LAPIN YLIOPISTO
UNIVERSITY OF LAPLAND

Henkilötietoa vai ei?
Pseudonymisointi ja anonymisointi henkilötietojen suojakeinoina EU:ssa

Oikeusinformatiikka
Maisteritutkielma

Julia Lyytinen

Kevät 2026
Lapin yliopisto

LAPIN YLIOPISTO
UNIVERSITY OF LAPLAND

Lapin yliopisto
Tiedekunta: Oikeustieteiden tiedekunta
Työn nimi: Henkilötietoa vai ei? Pseudonymisointi ja anonymisointi henkilötietojen suojakeinoina EU:ssa
Tekijä: Julia Lyytinen
Koulutusohjelma / opetuskokonaisuus / oppiaine: Oikeusinformatiikka
Ohjaaja: Juhana Riekkinen
Työn laji: Maisteritutkielma
Sivumäärä, liitteiden lukumäärä: XVIII + 77
Vuosi: 2026

Tiivistelmä:

Henkilötietojen rooli digitaalisessa toimintaympäristössä on keskeinen, mutta niiden oikeudellinen luonne on yhä enenevissä määrin tulkinnanvarainen. Tutkimuksen tavoitteena on selvittää, miten pseudonymisoitujen tietojen tunnistettavuuden tulkinta sekä pseudonymisointi ja anonymisointi tietosuojatoimenpiteinä vaikuttavat rekisteröidyn oikeuksien toteutumiseen ja tietosuojasääntelyn tavoitteisiin. Tunnistettavuutta punnitaan erityisesti absoluuttisen ja suhteellisen henkilötiedon käsitteiden valossa. Samalla tutkimuksessa tarkastellaan pseudonymisoinnin ja anonymisoinnin välistä rajanvetoa. Tutkimuksessa arvioidaan voimassa olevan sääntelymallin tarkoituksenmukaisuutta suhteessa tietosuojasääntelyn kaksinaistavoitteeseen, eli henkilötietojen suojaan ja henkilötietojen vapaaseen liikkuvuuteen.

Tutkimus on pääasiassa lainopillinen, mutta siinä hyödynnetään myös oikeuspoliittista de lege ferenda -näkökulmaa. Lähdeaineisto pohjautuu pääosin EU:n yleiseen tietosuoja-asetukseen, EUT:n oikeuskäytäntöön, tietosuojaviranomaisten ohjeisiin ja kannanottoihin sekä oikeuskirjallisuuteen. Merkittävän painoarvon tutkimuksessa saa EUT:n ratkaisu asiassa C-413/23 P, joka on vahvistanut suhteellisen henkilötiedon käsitteen asemaa. Tutkimuksessa analysoidaan erityisesti myös Euroopan tietosuojaneuvoston pseudonymisointia koskevia suuntaviivoja 1/2025 ja Digital Omnibus -lainsäädäntöaloitetta. Tulkinnalliseksi apuvälineeksi ja henkilötiedon dynaamisen luonteen hahmottamiseksi tutkimuksessa on luotu relatiivisen avaimen käsite, jonka tarkoituksena on kattaa kaikki mahdolliset tunnistamiskeinot.

Tutkimus osoittaa, että pseudonymisoidun tiedon luonne ei ole yksiselitteinen, vaan sen arviointi riippuu kontekstista ja tunnistamisen mahdollisuuksista – eli relatiivisesta avaimesta. Pseudonymisoitu henkilötieto voi olla henkilötietoa yhdelle, mutta ei toiselle. Tällainen tulkinnanvaraisuus henkilötiedon käsitteeseen heijastuu ensinnäkin rekisteröidyn oikeuksien toteutumiseen ja sääntelyn tehokkuuteen. Rekisteröidyn oikeudet voivat pseudonymisoinnin johdosta toteutua porrasteisesti: täysimääräisesti, osittain tai ei lainkaan. Tietosuojan tavoitteiden tasapainon kannalta pseudonymisointi osoittautui tutkimuksessa anonymisointia tehokkaammaksi. Nykyinen sääntelymalli mahdollistaa tietosuojasääntelyn tavoitteiden tasapainon, mutta tulkinnanvaraisuus tunnistettavuuden arvioinnissa heikentää samalla oikeusvarmuutta ja ennakoitavuutta. Sääntelyssä on siten syytä korostaa riskiperusteista lähestymistapaa ja henkilötiedon dynaamista luonnetta.

Avainsanat: henkilötieto, anonyymi tieto, tietosuoja, pseudonymisointi, anonymisointi, tietosuoja-asetus, rekisteröidyn oikeudet, henkilötietojen suoja, henkilötietojen vapaa liikkuvuus

Sisällys

Lähteet

Aarnio 1997

Aarnio, Aulis: Oikeussäännösten systematisointi ja tulkinta, s. 35–56 teoksessa Häyhä, Juha (toim.): Minun metodini. WSLT Oy 1997.

Aarnio 2011

Aarnio, Aulis: Luentoja lainopillisen tutkimuksen teoriasta. Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisuja. Unigrafia Oy 2011.

Alapuranen ym. 2020

Alapuranen, Leena – Lehtonen, Lasse – Koskinen, Seppo – Wiberg, Matti: Henkilötietojen käsittely työelämässä. 3. uudistettu painos. Edita 2020.

Andersson 2024

Andersson, Jenna: Organisaation hyvä tietoturvan sääntelyjärjestelmä. Väitöskirja. Vaasan yliopisto 2024.

Bolognini – Bistolfi 2017

Bolognini, Luca – Bistolfi, Camilla: Pseudonymization and impacts of Big Data Processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation. Computer Law & Security Review 33, 2017, s. 171–181.

Bottis – Bouchagiar 2018

Bottis, Maria – Bouchagiar, George: Personal Data v. Dig Data in the EU Control Lost Discrimination Found. Open Journal Philosophy, 2018, s. 192–205.

Bäck – Keränen 2017

Bäck, Asta – Keränen, Janne: Anonymisointipalvelut – Tarve ja toteutusvaihtoehdot. Liikenne- ja viestintäministeriö 7/2017.

El Khoury 2017

El Khoury, Alessandro: Dynamic IP Addresses Can Be Personal Data, Sometimes. A Story of Binary Relations and Schrödinger's Cat. European Journal of Risk Regulation 8, 2017, s. 191–197.

Husa ym. 2008

Husa, Jaakko – Mutanen, Anu – Pohjolainen, Teuvo: Kirjoitetaan juridiikkaa. Ohjeita oikeustieteellisten kirjallisten töiden laatijoille. Talentum 2008.

Hintze 2018

Hintze, Mike: Viewing the GDPR through a de-identification lens: a tool for compliance, clarification and consistency. International Data Privacy Law, Volume 8(1), 2018.

Häyhä 1997

Häyhä, Juha: Johdanto, s. 15–34 teoksessa Häyhä, Juha (toim.) Minun metodini. WSLT Oy 1997.

Kangas 1997

Kangas, Urpo: Minun metodini, s. 90–109 teoksessa Häyhä, Juha (toim.) Minun metodini. WSLT Oy 1997.

Kolehmainen 2016

Kolehmainen, Antti: Tutkimusongelma ja metodi lainopillisessa työssä, s. 106–132 teoksessa Miettinen, Tarmo (toim.): Oikeustieteellinen opinnäyte – artikkeleita oikeustieteellisten opinnäytetöiden vaatimuksista, metodista ja arvostelusta. Edita 2016.

Koops 2014

Koops. Bert-Jaap: The trouble with European data protection law. International Data Privacy Law, Vol. 4(4), 2014, s. 250–261.

Korpisaari ym. 2022

Korpisaari, Päivi – Pitkänen, Olli – Warma-Lehtinen, Eija: Tietosuoja. 2. uudistettu painos. Alma Talent 2022.

Lindroos-Hovinheimo 2018

Lindroos-Hovinheimo, Susanna: Henkilötietojen suoja EU-oikeudessa – yksityisyyttä yhteisön kustannuksella? Lakimies 1/2018, s. 52–75.

Lynskey 2013

Lynskey, Orla: From Market-Making Tool to Fundamental Right: The Role of the Court of Justice in Data Protection's Identity Crisis teoksessa Gutwirh, Serge – Leenes, Ronald – de Hert, Paul – Poullet, Yves (toim.): European Data Protection: Coming of Age. Springer 2013, s. 59–84.

Lynskey 2015

Lynskey, Orla: The Foundations of EU Data Protection Law. Oxford University Press 2015.

Määttä – Paso 2022

Määttä, Tapio – Paso, Mirjami: Johdatus oikeudellisen ratkaisun teoriaan. Oikeuden perusteet 37. Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisuja 2022.

Neuvonen 2014

Neuvonen, Riku: Yksityisyyden suoja Suomessa. Lakimiesliiton kustannus 2014.

Ojanen 2004

Ojanen, Tuomas: EYTI C-112/00 Eugen Schmidberger Internationale Transporte Planzüge vastaan Itävallan tasavalta – Luzemburgin tuomarit tavaroiden vapaan liikkuvuuden ja perusoikeuksien välistä suhdetta pohtimassa. Lakimies 1/2004, s. 126–135.

Ollila 2014

Ollila, Riitta: Henkilötietojen suoja EU:n perusoikeutena. Defensor Legis N:o 5/2014, s. 814–824.

Poullet 2018

Poullet, Yves: Is the general data protection regulation the solution? Computer Law & Security Review 34(4), 2018, s. 773–778.

Purtova 2018

Purtova, Nadezhda: The law of everything. Broad concept of personal data and future of EU data protection law. Law, Innovation and Technology Volume 10(1), 2018, s. 40–81.

Raitio 2016

Raitio, Juha: Euroopan unionin oikeus. Alma Talent 2016.

Raitio 2017

Raitio, Juha: Oikeusvaltion ääriviivat. Alma Talent 2017.

Rauhanen 2025

Rauhanen, Riku: Henkilötiedon käsitteen kehitys: olemmeko siirtyneet suhteellisten henkilötietojen aikakauteen? Defensor Legis 4/2025, s. 657–672.

Saarenpää 2000

Saarenpää, Ahti*:* Verkkoyhteiskunnan oikeutta – Johdatusta aiheeseen. Oikeus 1/2000, s. 3–14.

Saarenpää 2016

Saarenpää, Ahti: Oikeusinformatiikka, s. 67–273 teoksessa Niemi, Marja-Leena (toim.): Oikeus tänään, 4. uudistettu painos. Lapin yliopiston oikeustieteellisiä julkaisuja. Sarja C 64, 2016.

Saarenpää – Riekkinen 2023

Saarenpää, Ahti – Riekkinen, Juhana: Oikeusinformatiikan perusteet. Lapin yliopisto 2023.

Sartor – Gafioja 2020

Sartor, Giovanni – Gafioia, Francesca: The impact of the General Data Protection Regulation (GDPR) on artificial intelligence. European Parliament 2020.

Siltala 2003

Siltala, Raimo: Oikeustieteen tieteenteoria. Suomalainen Lakimiesyhdistys 2003.

Stalla-Bourdillon – Knight 2016

Stalla-Bourdillon, Sophie – Knight, Alison: Anonymous data v. Personal data – a false devate: An EU perspective on anonymisation, pseudonymisation and personal data. Wisconsin International Law Journal 2016.

Stalla-Bourdillon 2025

Stalla-Bourdillon, Sophie: Identifiability, as a Data Risk: IS a Uniform Approach to Anonymisation About to Emerge in the EU? European Journal of Risk Regulation 16, 2025, s. 1456–1474.

Talus – Penttinen 2016

Talus, Kim – Penttinen, Sirja-Leena: Eurooppaoikeudelliset oikeuslähteet ja niiden tulkinta oikeustieteellistä opinnäytettä kirjoittaessa, s. 223–245 teoksessa Miettinen, Tarmo (toim.): Oikeustieteellinen opinnäyte – Artikkeleita oikeustieteellisten opinnäytteiden vaatimuksista, metodista ja arvostelusta. Edita 2016.

Tarhonen 2016

Tarhonen, Laura: Pseudonymisation of Personal Data According to the General Data Protection Regulation. Viestintäoikeuden vuosikirja 2016, s. 10–32.

Tuori 1997

Tuori, Kaarlo: Ideologiakritiikistä kriittiseen positivismiin, s. 311–329 teoksessa Häyhä, Juha (toim.): Minun metodini. WSLT Oy 1997.

Tuori 2000

Tuori, Kaarlo: Kriittinen oikeuspositivismi. WSLT Oy 2000.

Tolonen 2003

Tolonen, Hannu: Oikeuslähdeoppi. WSOY Lakitieto 2003.

Voutilainen 2019

Voutilainen, Tomi: Oikeus tietoon. Informaatio-oikeuden perusteet. 2. uudistettu painos. Edita 2019.

Zuiderveen-Borgesius 2016

Zuiderveen Borgesius, Frederik: Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation. Computer Law & Security Review 32, 2016, s. 246–271.

Zuiderveen-Borgesius 2017

Zuiderveen Borgesius, Frederik: Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data Definition. European Data Protection Law Review, Volume 3(1), 2017, s. 130–137.

Virallislähteet

Kansainväliset sopimukset

Euroopan ihmisoikeussopimus

Euroopan neuvoston yleissopimus ihmisoikeuksien ja perusvapauksien suojaamiseksi (4.11.1950, SopS 18/1990).

Euroopan tietosuojayleissopimus

Euroopan neuvoston yleissopimus yksilöiden suojelusta henkilötietojen automaattisessa käsittelyssä (28.1.1981, SopS 36/1992).

OECD tietosuojasuositus

Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data. 23.8.1980. Päivitetty 11.7.2013.

Euroopan unionin primaarioikeus

Euroopan unionin perusoikeuskirja

Euroopan unionin perusoikeuskirjan konsolidoitu toisinto, EUVL C 202, 7.6.2016.

Sopimus Euroopan unionin toiminnasta (SEUT)

Euroopan unionin toiminnasta tehdyn sopimuksen konsolidoitu toisinto, EUVL C 202, 7.6.2016.

Sopimus Euroopan unionista (SEU)

Euroopan unionista tehdyn sopimuksen konsolidoitu toisinto, EUVL C 236, 26.10.2012.

Lissabonin sopimus

Lissabonin sopimus Euroopan unionista tehdyn sopimuksen ja Euroopan yhteisön perustamissopimuksen muuttamisesta, EUVL C 306, 17.12.2007.

Euroopan unionin sekundaarioikeus

Datasäädös

Euroopan parlamentin ja neuvoston asetus (EU) 2023/2854, annettu 13 päivänä joulukuuta 2023, datan oikeudenmukaista saatavuutta ja käyttöä koskevista yhdenmukaisista säännöistä ja asetuksen (EU) 2017/2394 ja direktiivin (EU) 2020/1828 muuttamisesta. EUVL L 2023/2854, 22.12.2023.

Digimarkkinasäädös

Euroopan parlamentin ja neuvoston asetus (EU) 2022/1925, annettu 14 päivänä syyskuuta 2022, kilpailullisista ja oikeudenmukaisista markkinoista digitaalialalla ja direktiivien (EU) 2019/1937 ja (EU) 2020/1828 muuttamisesta. EUVL L 265, 12.10.2022.

EHDS

Euroopan parlamentin ja neuvoston asetus (EU) 2025/327, annettu 11 päivänä helmikuuta 2025, eurooppalaisesta terveystietoalueesta sekä direktiivin 2011/24/EU ja asetuksen (EU) 2024/2847 muuttamisesta. EUVL L 2025/327, 5.3.2025.

Euroopan unionin toimielinten tietosuoja-asetus

Euroopan parlamentin ja neuvoston asetus (EU) 2018/1725, annettu 23 päivänä lokakuuta 2018, luonnollisten henkilöiden suojelusta unionin toimielinten, elinten ja laitosten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta sekä asetuksen (EY) N:o 45/2001 ja päätöksen N:o 1247/2002/EY kumoamisesta. EUVL L 295, 21.11.2018.

Henkilötietodirektiivi

Euroopan parlamentin ja neuvoston direktiivi 95/46/EY, annettu 24 päivänä lokakuuta 1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta (kumottu). EUVL L 281, 23.11.1995.

Tekoälysäädös

Euroopan parlamentin ja neuvoston asetus (EU) 2024/1689, annettu 13 päivänä kesäkuuta 2024, tekoälyä koskevista yhdenmukaistetuista säännöistä ja asetusten (EY) N:o 300/2008, (EU) N:o 167/2013, (EU) N:o 168/2013, (EU) 2018/858, (EU) 2018/1139 ja (EU) 2019/2144 sekä direktiivien 2014/90/EU, (EU) 2016/797 ja (EU) 2020/1828 muuttamisesta. EUVL L, 2024/1689, 12.7.2024.

Yleinen tietosuoja-asetus

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. EUVL L 119, 4.5.2016.

Muut virallislähteet

COM (92) 422 final

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. 28.10.1992.

COM (2015) 192 final

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A Digital Single Market Strategy for Europe. COM (2015) 192 final. 6.5.2015.

COM (2025) 837 final (Digital Omnibus)

Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018, 1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital framework and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024. COM (2025) 837 final. 19.11.2025.

EDPB 4/2019

Euroopan tietosuojaneuvosto: Ohjeet 4/2019 25 artiklan mukaisesta sisäänrakennetusta ja oletusarvoisesta tietosuojasta. 20.10.2020.

EDPB 28/2024

Euroopan tietosuojaneuvosto: Lausunto 28/2024 tietyistä henkilötietojen käsittelyyn tekoälymallien yhteydessä liittyvistä tietosuojanäkökohdista. 17.12.2024.

EDPB 1/2025

European Data Protection Board: Guidelines 1/2025 on pseudonymisation. 16.1.2025.

EDPB työohjelma 2026–2027

European Data Protection Board: Work Programme 2026–2027. 11.2.2026.

EDPB–EDPS 2026

European Data Protection Board – European Data Protection Supervisor: Joint Opinion 2/2026 on the Proposal for a Regulation as regards the simplification of the digital legislative framework.11.2.2026.

ENISA 2018

European Union Agency for Network and Information Security: Recommendations on shaping technology according to GDPR provisions. An overview on data pseudonymization 2018.

HE 309/1003 vp

Hallituksen esitys eduskunnalle perustuslakien perusoikeussäännösten muuttamisesta 309/1993 vp.

ICO 2012

Information Commissioner’s Office: Anonymisation: managing data protection risk code of practice 2012.

ICO 2022a

Information Commissioner's Office: Chapter: How do we ensure anonymisation is effective? Draft anonymisation, pseudonymisation and privacy enhancing technologies guidance 2022.

ICO 2022b

Information Commissioner's Office: Chapter 3: pseudonymisation. Draft anonymisation, pseudonymisation and privacy enhancing technologies guidance 2022.

PeVL 7/2026 vp

Perustuslakivaliokunnan lausunto asiasta U 81/2025 vp. Valtioneuvoston kirjelmä eduskunnalle komission ehdotuksista Euroopan parlamentin ja neuvoston asetusten ja direktiivien muuttamisesta digitaalisen lainsäädäntökehyksen yksinkertaistamisen osalta (digiomnibus) ja tekoälyä koskevien yhdenmukaistettujen sääntöjen täytäntöönpanon yksinkertaistamisen osalta (tekoälyomnibus).

STM periaatepäätös

Sosiaali- ja terveysministeriön periaatepäätös: Pseudonymisointi, anonymisointi ja suorien tunnisteiden käyttö sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain (522/2019) mukaan. STM103:00/2019.

STM 2024

Sosiaali- ja terveysministeriö: Kuva- ja signaalitiedon anonymisointi ja anonymiteetti sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain (522/2019) mukaisessa käsittelyssä. 28.3.2024.

Tietosuojavaltuutetun toimisto 4/2017

Tietosuojavaltuutetun toimisto: Miten valmistautua EU:n tietosuoja-asetukseen? Selvityksiä ja ohjeita 4/2017.

TSV 9.4.2021

Tietosuojavaltuutetun ratkaisu 9.4.2021. Diaarinumero 7158/163/18. Opiskelijanumeroihin yhdistettyjen arvosanojen ja tehtäväkohtaisten pisteiden vieminen yliopiston intranetiin.

TSV 23.6.2022

Tietosuojavaltuutetun ratkaisu 23.6.2022. Diaarinumero 3895/83/22. Potilastietojen käsittely ennaltaehkäisyn ja ennakoinnin tarkoituksissa sekä automatisoidut yksittäispäätökset.

U 81/2025 vp

Valtioneuvoston kirjelmä eduskunnalle komission ehdotuksista Euroopan parlamentin ja neuvoston asetusten ja direktiivien muuttamisesta digitaalisen lainsäädäntökehyksen yksinkertaistamisen osalta (digiomnibus) ja tekoälyä koskevien yhdenmukaistettujen sääntöjen täytäntöönpanon yksinkertaistamisen osalta (tekoälyomnibus).

WP136

WP 29: Opinion 4/2007 on the concept of personal data. Annettu 20.6.2007.

WP169

WP 29: Lausunto 1/2010 rekisterinpitäjän ja henkilötietojen käsittelijän käsitteistä. Annettu 16.2.2010.

WP216

WP 29: Opinion 5/2014 on Anonymisation Techniques. Annettu 10.4.2014.

WP217

WP 29: Lausunto 6/2014 direktiivin 95/46/EY 7 artiklan mukaisesta rekisterinpitäjän oikeutetun edun käsitteestä. Annettu 9.4.2014.

WP260

WP 29: Asetuksen 2016/679 mukaista läpinäkyvyyttä koskevat suuntaviivat. Annettu 29.11.2017. Tarkistettu 11.4.2018.

WP248

WP 29: Ohjeet tietosuojaa koskevasta vaikutuksenarvioinnista ja keinoista selvittää ”liittyykö käsittelyyn todennäköisesti” asetuksessa (EU) 2016/679 tarkoitettu korkea riski. Annettu 4.4.2017. Tarkistettu 4.10.2017.

Oikeuskäytäntö

Euroopan unionin tuomioistuin

Asia C-518/07, *Komissio v. Saksa*. Tuomio 9.3.2010.

Asia C-362/14, *Schrems v. Data Protection Commissioner*. Tuomio 6.10. 2015.

Asia C-582/14, *Breyer v. Saksan liittotasavalta*. Tuomio 19.10.2016.

Asia C-434/16, *Nowak v. Data Protection Commissioner*. Tuomio 20.12.2017.

Asia C-40/17, *Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV*. Tuomio 29.7.2019.

Asia C-154/21, *RW v. Österreichische Post AG*. Tuomio 12.1.2023.

Asia C-319/22, *Gesamtvernamd Autoheile-Handel eV v. Scania*. Tuomio 9.11. 2023.

Asia C-340/21, *VB v. Natsionalna agentsia za prihodite*. Tuomio 14.12.2023.

Asia C-479/22 P, *OC v. Komissio*. Tuomio 7.3.2024.

Asia C-604/22, *IAB Europe v. Gegevensbeschermingsautoriteit*. Tuomio 7.3.2024.

Asia C-757/22, *Meta Platform Ireland*. Tuomio 11.7.2024.

Asia C-413/23 P, *EDPS v. SRB*. Tuomio 4.9.2025.

Asia C-654/25, *US ja DR v. KY* (*Undelam)*. Ennakkoratkaisupyyntö jätetty 6.10.2025.

Euroopan unionin tuomioistuimen julkisasiamiehen ratkaisuehdotukset

Julkisasiamies Sánchez-Bordonan ratkaisuehdotus asiassa C-582/14. Annettu 12.5.2016.

Julkisasiamies Bobekin ratkaisuehdotus asiassa C-40/17. Annettu 19.12.2018.

Julkisasiamies Spielmannin ratkaisuehdotus asiassa C-413/23 P. Annettu 6.2.2025.

Muut tuomioistuinratkaisut

Puolan korkein hallinto-oikeus (Naczelny Sąd Administracyjny, ‘NSA’):

Asia III OSK 2595/22. Annettu 16.10.2025.

Ranskan korkein hallinto-oikeus (Conseil d'État):
Asia nro. 498628 GERS v. CNIL. Annettu 13.2.2026.

Ranskan korkein hallinto-oikeus (Conseil d'État):
Asia nro. 482872 Criteo v. CNIL. Annettu 4.3.2026.

Verkkolähteet

Craddock 2025

Craddock, Peter: When is data no longer personal? And what are the implications? LinkedIn article 5.9.2025. Saatavissa: https://www.linkedin.com/pulse/when-data-longer-personal-what-implications-peter-craddock-7bw4e/. (Tarkistettu 30.3.2026).

Komission verkkosivut: Terveystietojen uudelleenkäyttö

Euroopan komission verkkosivut: Terveystietojen uudelleenkäyttö. Saatavissa: https://health.ec.europa.eu/ehealth-digital-health-and-care/reuse-health-data_fi. (Tarkistettu 8.1.2026).

HSF Kramer 2026

Herbert Smith Freehills Kramer: French supreme court rules on pseudonymization vs. anonymization 20.3.2026. Saatavissa: https://www.hsfkramer.com/notes/data/2026-posts/french-supreme-court-rules-on-pseudonymisation-vs-anonymisation. (Tarkistettu 12.4.2026).

Konarski – Kupiec 2025

Konarski, Xawery – Kupiec, Mateusz: Polish Supreme Administrative Court requires DPAs to prove identifiability before treating IP addresses and cookie IDs as personal data. International Network of Privacy Law Professionals. 9.12.2025. Saatavissa: https://inplp.com/latestnews/article/polish-supreme-administrative-court-requires-dpas-to-prove-identifiabilitybefore-treating-ip-addresses-and-cookie-ids-as-personal-data/. (Tarkistettu 4.1.2026).

Purtova 2025

Purtova, Nadezda: Why simply redefining personal data narrowly does not solve the problem of the “law of everything”. Brussels Privacy Hub. 15.12.2025. Saatavissa: https://brusselsprivacyhub.com/why-simply-redefining-personal-data-narrowly-does-not-solve-the-problem-of-the-law-of-everything/. (Tarkistettu 12.4.2026).

Rowntree 2016

Rowntree, Lindsay: Pseudonymisation: What the Ad Tech Industry Needs to Know. Exchange Wire, 17.10.2016. Saatavissa: https://www.exchange-wire.com/blog/2016/10/17/pseudonymisation-ad-tech-industry-needs-know/. (Tarkistettu 16.3.2026).

Tanskan tietosuojavaltuutettu 2025.

Tanskan tietosuojaviranomainen: Mere nyt om EU-Domstolens afgørelse om pseudonymiserede personoplysninger. 22.10.2025. Saatavissa: https://www.datatilsy-net.dk/internationalt/internationalt-nyt/2025/okt/mere-nyt-om-eu-domstolens-afgoerelse-om-pseudonymiserede-personoplysninger. (Tarkistettu 4.1.2026).

Tietoarkiston verkkosivut

Tietoarkisto: Tunnisteellisuus ja anonymisointi. Saatavissa: https://www.fsd.tuni.fi/fi/palvelut/aineistonhallinta/tunnisteellisuus-ja-anonymisointi/. (Tarkistettu 4.1.2026).

Tietosuojavaltuutetun toimisto: Pseudonymisoidut ja anonymisoidut tiedot

Tietosuojavaltuutetun toimisto: Pseudonymisoidut ja anonymisoidut tiedot. Saatavissa: https://tietosuoja.fi/pseudonymisointi-anonymisointi. (Tarkistettu 4.1.2026).

Lyhenteet

Datasäädös	Asetus (EU) 2023/2854
Digimarkkinasäädös	Asetus (EU) 2022/1925
Digital Omnibus	Euroopan komission Digital Omnibus -asetusehdotus COM (2025) 837 final
EHDS	Asetus (EU) 2025/327
EIS	Euroopan ihmisoikeussopimus
ENISA	Euroopan unionin kyberturvallisuusvirasto (European Union Agency For Network and Information Security)
EU	Euroopan unioni
EU:n toimielinten tietosuoja-asetus	Asetus (EU) 2018/1725
EUT	Euroopan unionin tuomioistuin
HE	Hallituksen esitys
ICO	Yhdistyneen kuningaskunnan tietosuojaviranomainen (Information Commissioner's Office)
Lissabonin sopimus	Lissabonin sopimus Euroopan unionista tehdyn sopimuksen ja Euroopan yhteisön perustamissopimuksen muuttamisesta
NSA	Puolan korkein hallinto-oikeus (Naczelny Sąd Administracyjny)
OECD	Taloudellisen yhteistyön ja kehityksen järjestö (Organisation for Economic Co-operation and Development
Perustuslaki	Perustuslaki (731/1999)
PeVL	Perustuslakivaliokunnan lausunto
SEU	Sopimus Euroopan unionista
SEUT	Sopimus Euroopan unionin toiminnasta
SopS	Suomen säädöskokoelman sopimussarja
SRB	Asia C-413/23 P *EDPS v. SRB*
STM	Sosiaali- ja terveysministeriö
Hallitusmuoto	Suomen hallitusmuoto (94/1919)
Tietosuoja-asetus / TSA	Euroopan unionin yleinen tietosuoja-asetus (EU) 2016/679
Tietosuojalaki	Tietosuojalaki (1050/2018)

Tietosuojaneuvosto / EDPB	Euroopan tietosuojaneuvosto (European Data Protection Board)
Tietosuojatyöryhmä	Euroopan unionin tietosuojatyöryhmä (Article 29 Working Party)
Tietosuojavaltuutettu / EDPS	Euroopan tietosuojavaltuutettu (European Data Protection Supervisor)
Toisiolaki	Laki sosiaali- ja terveystietojen toissijaisesta käytöstä (552/2019)
TSV	Suomen tietosuojavaltuutettu
vp	Valtiopäivät

1 Johdanto

1.1 Tutkimuksen tausta

Yhteiskunnassa lähes jokainen toiminto rakentuu jossain määrin henkilötietojen varaan. Henkilötietojen vaihto on digitalisaation myötä huomattavasti lisääntynyt Euroopan unionissa (jäljempänä 'EU'). Niin yritykset kuin viranomaiset voivat hyödyntää henkilötietoja laajasti, mutta myös luonnolliset henkilöt saattavat henkilötietojaan julkisesti saataville esimerkiksi sosiaalisen median kautta.[1] Nykyinen digitaalinen toimintaympäristö luo paljon mahdollisuuksia, mutta myös paljon uhkakuvia henkilöiden tunnistettavuudelle. EU:n yleinen tietosuoja-asetus ((EU)2016/679, jäljempänä 'tietosuoja-asetus' tai 'TSA')[2] on luonut yhtenäisen sääntelykehyksen henkilötietojen käsittelylle. Asetuksen tavoitteena on samanaikaisesti turvata sekä luonnollisten henkilöiden perusoikeus henkilötietojen suojaan että henkilötietojen vapaa liikkuvuus unionin sisällä.[3]

Tietosuojasääntelyssä tehdään selkeä kahtiajako henkilötiedon ja anonyymin tiedon välille. TSA 4(1) artiklan mukaan henkilötiedoilla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja, jotka voidaan yhdistää tähän henkilöön suoraan tai epäsuorasti. Jos taas tietoa ei katsota henkilötiedoksi, on se anonyymiä tietoa eikä siihen sovelleta tietosuojasääntelyä.[4] Raja ei kuitenkaan ole yksiselitteinen. Henkilötiedon ja anonyymin tiedon rajanvedolla on siten suoraan vaikutus tietosuojasääntelyn aineelliseen soveltamisalaan.

Henkilötietojen suojaamiseksi on määritelty teknisiä ja organisatorisia toimenpiteitä, joista yksi on henkilötietojen pseudonymisointi. Pseudonymisoinnilla tarkoitetaan henkilötietojen käsittelemistä siten, ettei henkilötietoja voida enää yhdistää tiettyyn luonnolliseen henkilöön eli rekisteröityyn käyttämättä erillään säilytettäviä lisätietoja. Myös henkilötietojen anonymisointi on yksi suojatoimenpide. Anonymisoinnilla henkilötieto muutetaan pysyvästi muotoon, josta rekisteröityä ei voi tunnistaa. Sen sijaan pseudonymisoidusta tiedosta tunnistaminen on edelleen mahdollista lisätietojen avulla.[5] Tässä tutkimuksessa näitä lisätietoja kuvataan myös käsitteellä *relatiivinen avain*. Relatiivisen avaimen tarkoituksena on toimia niin sanottuna "kattoterminä" kaikille

[1] TSA johdanto-osa 5–6 kappaleet.
[2] 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).
[3] TSA johdanto-osa 2 kappale.
[4] TSA johdanto-osa 26 kappale. Ks. alueellisesta soveltamisalasta TSA 3 artikla.
[5] Ks. TSA johdanto-osa 26 kappale ja WP216, s. 3.

saatavilla oleville tunnistamiskeinoille.[6] Relatiivinen avain on siis tieto tai tietojoukko, jonka avulla luonnollinen henkilö voidaan tunnistaa.

Henkilötiedon käsite ja erityisesti kysymys siitä, onko pseudonymisoitu henkilötieto aina henkilötietoa, on herättänyt laajaa juridista keskustelua.[7] Oikeustieteellisissä keskusteluissa ei ole myöskään yhtenevää näkemystä siitä, tulisiko henkilötiedon käsitettä pitää absoluuttisena, jolloin henkilötieto on henkilötietoa aina kaikille vai suhteellisena, jolloin henkilötiedon luonne on kontekstisidonnaista.[8] Henkilötiedon käsitettä sekä pseudonymisointia ja anonymisointia on tutkittu runsaasti niin kansallisesti kuin kansainvälisesti niiden ollessa tietosuojan ydinkäsitteitä.

Euroopan unionin tuomioistuin (jäljempänä ’EUT’) on ottanut kantaa henkilötiedon tunnistettavuuteen useissa ratkaisuissaan. Syksyllä 2025 antamassaan ratkaisussa C-413/23 P *Euroopan tietosuojavaltuutettu v. Single Resolution Board* (EDPS v. SRB, jäljempänä ’SRB’) EUT on tarkastellut muun muassa pseudonymisoidun tiedon henkilötietoluonnetta sekä henkilötietoja luovuttaneen rekisterinpitäjän että tietojen vastaanottajan näkökulmista.[9] Ratkaisua on pidetty hyvin merkittävänä pseudonymisoidun henkilötiedon luonteen tulkinnan kannalta.[10] Lisäksi tammikuussa 2025 on Euroopan tietosuojaneuvosto (jäljempänä ’tietosuojaneuvosto’ tai ’EDPB’) antanut henkilötietojen pseudonymisointia koskevat suuntaviivat. EU:n Digital Omnibus -lainsäädäntöaloitepaketissa (jäljempänä ’Digital Omnibus’) on ehdotettu muutoksia henkilötiedon käsitteeseen ja pseudonymisoidun tiedon luonteeseen.[11] Nämä osoittavat, että pseudonymisoidun henkilötiedon tunnistettavuus on aiheena kiistanalainen, mikä tekee tutkimuskohteesta ajankohtaisen.

1.2 Tutkimuskysymykset ja rajaus

Rajanveto henkilötiedon ja anonyymin tiedon välillä vaikuttaa tietosuojasääntelyn soveltamisalaan, jolloin se vaikuttaa rekisteröidyn oikeuksiin ja toimijoihin kohdistuviin velvoitteisiin. Tutkimuksessa tarkastellaan pseudonymisoidun henkilötiedon luonnetta sekä pseudonymisoinnin ja

---

[6] Relatiivisen avaimen käsite tulee siten erottaa esimerkiksi salausavaimesta, joka on vain yhdenlainen relatiivisen avaimen muoto ja ilmentää teknistä toteutustapaa. Ks. pseudonymisoinnin teknisistä toteutustavoista esim. EDPB 1/2025.

[7] Ks. esim. Rauhanen 2025, s. 658. Ks. myös anonymisoinnista Stalla-Bourdillon 2025, s. 1.

[8] Ks. esim. Rauhanen 2025, s. 658. Ks. tarkemmin absoluuttisesta ja suhteellisesta henkilötiedon käsitteestä luku 2.2.

[9] TSA 4(7) mukaan rekisterinpitäjällä tarkoitetaan tahoa, joka yksin tai yhdessä toisen kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. TSA 4(9) mukaan vastaanottajalla tarkoitetaan tahoa, jolle henkilötietoja luovutetaan.

[10] Ks. Rauhanen 2025, s. 658 ja Craddock 2025.

[11] Ks. COM (2025) 837 final (Digital Omnibus). Ks. esitettävistä muutoksista luku 5.4.1.

anonymisoinnin vaikutusta rekisteröidyn oikeuksien toteutumiseen. Tietosuojasääntelyllä on kaksi keskenään jännitteisessä suhteessa olevaa tavoitetta: henkilötietojen suojan tavoite sekä henkilötietojen vapaan liikkuvuuden tavoite. Tutkimuksessa tarkastellaan myös pseudonymisoinnin ja anonymisoinnin merkitystä tavoitteiden toteutumisessa, ja myös sääntelymallin tarkoituksenmukaisuutta arvioidaan näitä tavoitteita vasten. Tutkimuksen tavoitteena on siten vastata seuraaviin kysymyksiin:

1. Miten pseudonymisoitujen tietojen tunnistettavuuden tulkinta sekä henkilötietojen pseudonymisointi ja anonymisointi tietosuojatoimenpiteinä vaikuttavat rekisteröidyn oikeuksien ja tietosuojasääntelyn tavoitteiden toteuttamiseen?
2. Onko pseudonymisointia ja anonymisointia koskeva sääntelymalli tarkoituksenmukainen suhteessa tietosuojan tavoitteisiin ja miten tavoitteiden toteutumista tulisi edistää *de lege ferenda*?

Pääasiallisiin tutkimuskysymyksiin vastataan seuraavien apukysymysten avulla: Missä tilanteessa pseudonymisoitu henkilötieto lakkaa olemasta henkilötietoa? Miten pseudonymisointi ja anonymisointi vaikuttavat rekisteröidyn oikeuksien tosiasialliseen toteutumiseen? Mikä on pseudonymisoinnin ja anonymisoinnin merkitys tietosuojan tavoitteiden kannalta?

Henkilötietoja käsitellään yhteiskunnassa monipuolisissa toiminnoissa, minkä vuoksi tutkimuskohteen ympärillä on laaja kehikko ja useita liittymäkohtia.[12] Tutkimuksen ulkopuolelle jääviä asioita ei sen vuoksi ole tarkoituksenmukaista tyhjentävästi luetella. Tutkimuksen ulkopuolelle rajataan ainakin pseudonymisoinnin ja anonymisoinnin teknisten toteutustapojen tarkempi tarkastelu.[13] Tarkemman tarkastelun ulkopuolelle rajataan myös pseudonymisoitujen henkilötietojen automaattiseen käsittelyyn ja profilointiin liittyvät kysymykset, eikä tarkastelua rajata sektorikohtaisesti. Myöskään henkilötietojen käsittelyn ja tekoälyn yhteyttä ei tutkimuksessa tarkemmin tarkastella, joskin sitä hieman sivutaan.

1.3 Tutkimusmenetelmä

Metodi nähdään tapana ajatella yhteiskunnasta ja oikeudesta,[14] ja sen avulla hankitaan tietoa ja perustellaan sen merkitys.[15] Tässä tutkimuksessa pääasiallisena metodina käytetään lainoppia

[12] Tutkimuksessa keskitytään tarkastelemaan tutkimuskysymyksiä EU:n yleisen tietosuoja-asetuksen valossa, mutta samat tulkinnat sinänsä pätevät myös EU:n toimielinten tietosuoja-asetukseen (2018/1725), sillä asetukset vastaavat pitkälti toisiaan. Ks. esim. EUT:n ratkaisu C-413/23 P (SRB).
[13] Näihin liittyen ks. EDPB 1/2025 ja WP216.
[14] Kangas 1997, s. 91.
[15] Häyhä 1997, s. 24.

eli oikeusdogmatiikkaa.[16] Lainopilla on kaksi tehtävää: selvittää oikeussääntöjen sisältö eli tulkita niitä, ja systematisoida oikeussäännöksiä.[17] Lainopin tiedonintressi kohdistuu siten systeemiin ja sen sisältöön.[18] Lainopin tulkintatehtävää voidaan kutsua käytännölliseksi lainopiksi ja systematisointitehtävää teoreettiseksi lainopiksi.[19] Teoreettisella lainopilla voidaan esimerkiksi vastata siihen, millaisen oikeudellisen käsitteistön avulla oikeutta on tarkoituksenmukaista kuvata.[20] Lainoppi tuottaa perusteltuja tulkintakannanottoja ja mahdollisimman varmaa informaatiota oikeusjärjestyksen sisällöstä.[21] Käytännöllinen ja teoreettinen lainoppi toimivat tiiviissä vuorovaikutussuhteessa ja molemmilla on tehtävänsä oikeusjärjestyksen hahmottamisessa.[22]

Ensimmäisen tutkimuskysymyksen kohdalla tiedonintressi on lainopillinen. Apukysymyksen *missä tilanteessa pseudonymisoitu henkilötieto lakkaa olemasta henkilötietoa* osalta menetelmä on enemmän tulkintapainotteinen eli käytännöllinen lainoppi. Tämän apukysymyksen kohdalla on kuitenkin teoreettisen lainopin elementtejä, kun tulkinnalliseksi apuvälineeksi ja tunnistamisen mahdollistavien keinojen luonteen hahmottamiseksi luodaan *relatiivisen avaimen* käsite.[23] *Apukysymykset miten pseudonymisointi ja anonymisointi vaikuttavat rekisteröidyn oikeuksien toteutumiseen ja toimijoiden rooleihin näiden toteuttamisessa* sekä *mikä on pseudonymisoinnin ja anonymisoinnin merkitys tietosuojan tavoitteiden kannalta* liittyvät enemmän toimenpiteiden tarkasteluun sääntelykokonaisuudessaan, jolloin näillä on enemmän systematisointipainotteinen intressi. Ensimmäisen tutkimuskysymyksen kohdalla hyödynnetään siten sekä käytännöllistä että teoreettista lainoppia. Tutkimus on pääosin *de lege lata* -tutkimusta eli painopisteenä on voimassa olevan oikeuden tutkiminen.[24]

Toinen tutkimuskysymys pohjautuu näihin aiempiin tulkinnallisiin ja systematisoiviin analyyseihin, ja liittyy sääntelysystematiikan ja sääntelyn toimivuuden arviointiin. Sääntelymallin tarkoituksenmukaisuutta arvioidaan tietosuojan jopa ristiriitaisia tavoitteita vasten. Tämän tutkimus-

---

[16] Ks. oikeusdogmaattisesta tutkimuksesta tarkemmin esim. Husa ym. 2008, s. 20.
[17] Aarnio 1997, s. 36–37.
[18] Aarnio 1997, s. 48; Hirvonen 2011, s. 19.
[19] Aarnio 1997, s. 40. Ks. myös Tuori 2000, s. 303. Tuori käyttää käytännöllisen lainopin sijasta sanaa ”tulkintalainoppi”.
[20] Siltala 2003, s. 124. Siltala on kuvannut teoreettisen lainopin olevan käytännöllistä abstraktimpaa.
[21] Aarnio 1997, s. 49; Aarnio 2011, s. 12.
[22] Aarnio 1997, s. 37 ja 104. Aarnion mukaan käytännöllisen lainopin tehtävänä on testata teoreettisen lainopin luomia systematisointeja ja teorioita. Tuori taas näkee käytännöllisen lainopin liikkuvan oikeusjärjestyksestä antamillaan tulkintakannanotoillaan oikeuden pintatasolla. Teoreettinen lainoppi taas systematisoidessaan muotoilee ja kehittää oikeuskulttuurin tasolle sijoittuvia oikeudenalojen yleisiä oppeja. Ks. oikeuden tasoteoriaan liittyen Tuori 1997, s. 327.
[23] Ks. tarkemmin relatiivisen avaimen käsitteestä luku 3.1.
[24] Siltala 2003, s. 606.

kysymyksen kohdalla hyödynnetään oikeuspoliittista eli de lege ferenda -näkökulmaa. Näkökulmalla arvioidaan erilaisia lainsäädännöllisiä ratkaisuja, joihin tuleva lainsäädäntö voisi perustua.[25] Tällainen de lege ferenda -kannanotto syntyy yleensä lainopin sivutuotteena.[26] Tutkimuksessa de lege ferenda -analyysin kohteena on, millaisen henkilötietoa ja pseudonymisointia koskevan sääntelyn tulisi olla, jotta se vastaisi tietosuojasääntelyn molempia tavoitteita, tai miten näitä tavoitteita voitaisiin parhaiten toteuttaa *de lege ferenda*.

Tutkimuksessa on myös piirteitä oikeushistoriallisesta näkökulmasta, vaikka tutkimus itsessään ei ole oikeushistoriallinen. Oikeushistoria tarkastelee voimassa olevan sääntelyn syntyyn johtanutta kehitystä.[27] Tutkimuksessa taustoitetaan ja tarkastellaan tietosuojan kehitystä erityisesti tietosuojan tavoitteiden taustan kuvaamiseksi.

Normit on myös aina annettu jotakin tarkoitusta ja päämäärää varten.[28] EUT kehittää EU-oikeutta erityisesti tulkitsemalla lainsäädäntöä teleologisesti ottamalla huomioon säädöksen tavoitteet ja päämäärän.[29] Myös tässä tutkimuksessa hyödynnetään teleologista tulkintametodia. Teleologisessa tulkinnassa selvitetään ensin sääntelyn tavoitteet, jonka jälkeen arvioidaan eri tulkintavaihtoehtojen tosiasialliset seuraukset. Näistä vaihtoehdoista valitaan sääntelyn tavoitteita parhaiten edistävä vaihtoehto.[30] Teleologisen tulkintametodin voidaan siten täydentävän tutkimuksen de lege ferenda -analyysiä.

1.4 Tutkimuksen oikeudenalakehys ja lähdeaineisto

Tutkimus sijoittuu oikeusinformatiikan alalle, tarkemmin sen alle kuuluvan informaatio-oikeuden piiriin.[31] Informaatio-oikeuden kohteena on erilaisissa muodoissa oleva tieto.[32] Tietosuoja on yksi

---

[25] Kolehmainen 2016, s. 108. Ks. myös Siltala 2003, s. 106. Siltalan mukaan de lege ferenda -tutkimus soveltaa oikeuden yhteiskunnallisiin vaikutuksiin perustuvaa lähestymistapaa tulevaan lainsäädäntöön. Pyrkimykseltään oikeuskäytäntöön vaikuttavaa tutkimusta kutsutaan de sententia ferenda -tutkimukseksi, johon tällä tutkimuksella ei pyritä. Ks. tästä tarkemmin Siltala 2003, s. 132 ja 279.
[26] Kolehmainen 2016, s. 116.
[27] Husa ym. 2008, s. 21.
[28] Aarnio 2011, s. 19–20.
[29] Talus – Penttinen 2016, s. 224–225; Hirvonen 2011, s. 40. EUT:n teleologinen tulkinta ilmenee myös tässä tutkimuksessa käsitellyissä EUT:n ratkaisuissa.
[30] Hirvonen 2011, s. 40.
[31] Oikeusinformatiikan luonteesta itsenäisenä oikeudenalana on oikeuskirjallisuudessa esitetty eriäviä näkemyksiä. Esim. Voutilainen on pitänyt oikeusinformatiikkaa enemmän tutkimuksellisena ilmiönä oikeudellisten ilmiöiden tarkasteluun. Ks. Voutilainen 2019, s. 53. Saarenpää ja Riekkinen ovat puolestaan pitäneet oikeusinformatiikkaa itsenäisenä, merkittävänä ja välttämättömänä oikeudenalana. Ks. Saarenpää – Riekkinen 2023, s. 7.
[32] Voutilainen 2019, s. 23.

informaatio-oikeudellisista tutkimuskohteista.[33] Informaatio-oikeuden tehtävänä on lisäksi systematisoida hajautunutta lainsäädäntöä.[34] Se myös tutkii oikeudellista sääntelyä ja sen mahdollisuuksia.[35] Näihin informaatio-oikeuden tehtäviin ja tutkimuskohteisiin tällä tutkimuksella pyritään antamaan vastauksia. Informaatio-oikeus on suomalaisessa oikeusjärjestelmässä kehittynyt omaksi kokonaisuudekseen vahvasti 1980-luvulta lähtien yhteiskunnallisten muutosten myötä, jolloin tietovarannoista on tullut merkityksellisempiä.[36] Oikeusinformatiikan voidaan katsoa olevan siten oikeudenalana verraten nuori ja dynaaminen, sekä sillä on paljon historiallista merkitystä.[37]

Informaatio-oikeudella on lisäksi useita yhteyksiä eri oikeudenaloihin.[38] Tutkimus keskittyy pääosin EU-oikeudellisten lähteiden tulkintaan, sillä informaatio-oikeus saa huomattavia vaikutteita EU-oikeudesta juuri tietosuojasääntelyn kautta.[39] Tutkimuksen voidaan siten katsoa olevan myös eurooppaoikeudellinen. Tutkimuksessa tehdyt tulkinnat koskettavat siten kaikkia EU:n jäsenvaltioita.

Tutkimuksessa tärkeimpänä oikeuslähteenä on tietosuoja-asetus. Tämän lisäksi hyödynnetään myös muita EU:n primaari- ja sekundaarioikeuteen kuuluvia säädöksiä, sekä muita EU:n virallislähteitä. EUT toimii ennakkoratkaisutuomioistuimena, jonka ratkaisut ovat merkittäviä EU-oikeuden tulkintakysymyksissä.[40] EUT:n antamilla ennakkoratkaisuilla on vakiintuneesti ollut huomattava merkitys oikeuslähteenä. EUT:n tulkintakannanotto, *ratio decidendi,* voidaan katsoa sitovaksi oikeusohjeeksi siitä huolimatta, että ahtaasti tulkiten se sitookin vain pyytänyttä kansallista tuomioistuinta.[41] Näin ollen EUT:n ratkaisukäytännöllä on olennainen rooli tässä tutkimuksessa. Lisäksi oikeuslähteinä hyödynnetään julkisasiamiesten ratkaisuehdotuksia.[42]

---

[33] Ks. Voutilainen 2019, s. 24 ja Saarenpää 2016, s. 75.
[34] Voutilainen 2019, s. 75.
[35] Korhonen 2003, s. 29.
[36] Voutilainen 2019, s. 21.
[37] Ks. Saarenpää – Riekkinen 2023, s. 7–8 ja 27–34; Ks. myös Saarenpää 2016, s. 67, jonka mukaan oikeusinformatiikkaa voidaan pitää merkittävänä oikeudenalana.
[38] Voutilainen 2019, s. 59. Ks. oikeusinformatiikan ja informaatio-oikeuden liitäntäkohdista muihin oikeudenaloihin ks. esim. Saarenpää – Riekkinen 2023.
[39] Voutilainen 2019, s. 59.
[40] Ks. sopimus Euroopan unionista (SEU) 19 artikla ja sopimus Euroopan unionin toiminnasta (SEUT) 267 artikla.
[41] Raitio 2017, s. 2; Raitio 2016, s. 199; Ks. myös Talus – Penttinen 2016, s. 231, jonka mukaan annettu ennakkoratkaisu on asetettava myös muun kuin sitä pyytäneen tuomioistuimen ratkaisun pohjaksi, sillä EUT:n tehtävänä on varmistaa EU-oikeuden yhdenmukainen soveltaminen.
[42] Ks. SEUT 252(2) artikla, jonka mukaan julkisasiamiehet ovat täysin puolueettomia ja riippumattomia, ja heidän tehtävänään on esittää EUT:lle perusteltuja ratkaisuehdotuksia.

Merkittävinä oikeuslähteinä hyödynnetään myös neuvoa-antavien elinten eli Euroopan tietosuojaneuvoston ja tätä edeltäneen henkilötietodirektiivin (95/46/EY)[43] aikaisen Euroopan tietosuojatyöryhmän WP 29 lausuntoja ja suuntaviivoja. Näiden oikeuslähdeopilliseen asemaan on kuitenkin syytä kiinnittää huomiota. Soft law -tasoisina oikeuslähteinä nämä eivät ole muodollisesti sitovia,[44] mutta niiden käytännön merkitys on suuri ja niitä tosiasiallisesti noudatetaan. Tietosuojatyöryhmän lausunnot ovat *de facto* vaikuttaneet tietosuojalainsäädännön tulkintaan.[45] Tietosuojatyöryhmän lausunnoille voidaan edelleen antaa painoarvoa tietosuojasääntelyn tulkinnassa, sillä henkilötiedon määritelmän ei ole katsottu TSA:n myötä ainakaan kaventuneen.[46] Tietosuojaneuvoston roolin on arvioitu olevan edeltäjäänsä suurempi, vaikka molemmilla on muodollisesti ollut neuvoa-antava rooli.[47] EUT ei kuitenkaan ole nimenomaisesti näihin lähteisiin viitannut.[48] Näiden lisäksi tulkinnassa hyödynnetään aiheeseen liittyvää oikeuskirjallisuutta ja verkkoaineistoa, sekä jäsenvaltioiden ratkaisuja ja muita virallislähteitä. EU:n etusijaperiaatteesta johtuen kansallisilla lähteillä ei ole suurta painoarvoa muuten kuin tulkinnan tukena.

1.5 Tutkielman rakenne

Tutkimus etenee systemaattisesti siten, että ensin luvussa kaksi taustoitetaan tutkimuksen kannalta relevantteja käsitteitä ja konsepteja. Luvussa käsitellään ensinnäkin tietosuojasääntelyn soveltamisalaa sekä tietosuojasääntelyn tavoitteita. Tämän jälkeen avataan henkilötiedon ja anonyymin tiedon välistä rajanvetoa. Lisäksi tarkastellaan pseudonymisoinnin taustan ymmärtämiseksi henkilötiedon käsittelyä ohjaavia periaatteita, riskiperusteista lähestymistapaa sekä teknisiä ja organisatorisia toimenpiteitä. Luvun lopussa avataan tutkimuksessa tarkasteltavat rekisteröidyn oikeudet ja eri toimijoiden roolit henkilötietojen käsittelyssä.

---

[43] Euroopan parlamentin ja neuvoston direktiivi (95/46/EY), annettu 25 päivänä lokakuuta 1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta.
[44] Raitio 2016, s. 206. Raition mukaan soft law -oikeuslähteiden luonnetta juridisen sitovuuden kannalta ei ratkaise otsikko vaan sisältö.
[45] Zuiderveen Borgesius 2016, s. 259.
[46] Korpisaari ym. 2022, s. 60, jossa lisäksi todetaan, että henkilötiedon käsitteen voidaan katsoa korkeintaan laajentuneen, kun uuden teknologian tunnistamiskeinot on otettu sanamuodossa huomioon. Ks. myös Saarenpää – Riekkinen 2023, s. 236, jossa korostetaan, että tietosuojatyöryhmän lausuntoja hyödynnettäessä on aina tarkoin pohdittava niiden yksityiskohtaista soveltuvuutta.
[47] Poullet 2018, s. 774. Ks. henkilötietodirektiivin 29(1) artikla tietosuojatyöryhmän neuvoa-antavasta roolista.
[48] Purtova 2018, s. 59–60, jossa myös korostetaan, että EUT on usein päätynyt jopa päinvastaisiin ratkaisuihin. Julkisasiamiehet ovat kuitenkin hyödyntäneet näitä ratkaisuehdotustensa perusteluissa. Ks. esim. C-40/17 (FashionID), kohdat 46 ja 48.

Luvuissa kolme ja neljä syvennytään tarkastelemaan ensimmäiseen tutkimuskysymykseen vastaamisen kannalta relevanttia tunnistettavuuden määräytymistä. Tämä toimii pohjana tutkimuksessa tehdylle muulle analyysille. Kolmannessa luvussa tutkitaan henkilötiedon tunnistettavuutta ja kohtuullisen todennäköisiä keinoja tunnistamiseksi. Samassa yhteydessä avataan myös relatiivisen avaimen käsitettä tunnistettavuuden määrittäjänä. Lisäksi käsitellään pseudonymisointia ja anonymisointia henkilötietojen suojakeinoina sekä näiden välistä rajanvetoa. Neljännessä luvussa tarkastellaan tietosuojatyöryhmän, tietosuojaneuvoston ja EUT:n sekä muiden jäsenvaltioiden tulkintalinjaa pseudonymisoidun henkilötiedon tunnistettavuudesta ja toimijoiden rooleista.

Viidennessä luvussa analysoidaan pseudonymisoidun tiedon muuttuvaa luonnetta, tämän vaikutuksia rekisteröidyn oikeuksiin, pseudonymisoinnin ja anonymisoinnin merkitystä tietosuojasääntelyn tavoitteiden toteutumisessa sekä arvioidaan nykyistä ja tulevaa sääntelymallia. Viidennessä luvussa siten tarkastellaan molempia tutkimuskysymyksiä pohjautuen tutkimuksen aiempaan analyysiin. Lopuksi kootaan yhteen tutkimuksen aikana tehdyt johtopäätökset ja mahdolliset muutosehdotukset sääntelyyn.

2 Henkilötieto EU:n tietosuojasääntelyssä

2.1 Tietosuojasääntelyn soveltamisala ja kaksinaistavoite

2.1.1 TSA:n soveltamisalasta ja tavoitteista

Ennen tietosuoja-asetusta jäsenvaltioilla oli omat säädöksensä henkilötietodirektiivin implementoimiseksi. Henkilötietodirektiivin mahdollistama liikkumavara mahdollisti siten hajanaisen täytäntöönpanon, mikä nähtiin mahdollisena esteenä taloudelliselle toiminnalle, kilpailun vääristymiselle ja viranomaisten toiminnalle näiden suorittaessa velvollisuuksiaan.[49] Teknologian kehittymisen vuoksi EU:ssa nähtiin tarve yhdenmukaistaa sääntelyä ja täytäntöönpanoa, jotta luottamusta voitiin rakentaa niin digitaalitalouden kehittymiseen sisämarkkinoilla kuin luonnollisten henkilöiden henkilötietojen valvontaan.[50] TSA tuli voimaan 24.5.2016 ja sitä on sovellettu 25.5.2018 alkaen. TSA on EU:n asetuksena suoraan sovellettavaa oikeutta eli sitä sovelletaan sel-

[49] TSA johdanto-osa 9 kappale; Voutilainen 2019, s. 87.
[50] TSA johdanto-osa 7 kappale.

laisenaan kaikissa EU:n jäsenvaltioissa. TSA kuitenkin mahdollistaa tietyssä määrin jäsenvaltioille liikkumavaraa täsmentää asetusta, mutta edellyttäen ettei henkilötietojen vapaata kulkua unionissa vaikeuteta.[51] Suomessa TSA:ta täydennetään useilla säädöksillä, kuten tietosuojalailla (1050/2018).[52] TSA:ta sovelletaan EU:n alueella tapahtuvaan luonnollisten henkilöiden henkilötietojen käsittelyyn kansalaisuudesta ja asuinpaikasta riippumatta.[53] Tästä syystä henkilötiedon käsitteen ja tunnistettavuuden tulkinta määrittää koko sääntelyn soveltamisalan, ja pienetkin erot tulkintalinjoissa voivat johtaa merkittäviin seurauksiin.

EU:n tietosuojasääntelyllä on jo henkilötietodirektiivin aikaan ollut kaksi tavoitetta: korkeatasoinen henkilötietojen suojelu ja henkilötietojen vapaa liikkuvuus.[54] Tietosuojasääntelyllä tasapainotellaan siten perusoikeudellisten ja taloudellisten intressien välillä, eikä kumpaakaan ole sinänsä nostettu toista painavammaksi.[55] TSA:n tavoitteena on johdanto-osan 2 kappaleen mukaan tukea vapauden, turvallisuuden ja oikeuden alueen ja sen talousunionin kehittämistä, taloudellista ja sosiaalista edistystä, talouksien lujittamista ja lähentämistä sisämarkkinoilla sekä luonnollisten henkilöiden hyvinvointia. Tietosuojasääntelyn kaksinaistavoitetta on oikeuskirjallisuudessa kritisoitu sekavaksi ja vaikeasti ymmärrettäväksi näiden keskinäisen monimutkaisen ja ristiriitaisen suhteen vuoksi.[56] Vaikeaselkoiseksi luonnehditun TSA:n tulkintaa voidaan helpottaa tulkitsemalla säännöksiä tietosuojaperiaatteiden kautta osana laajempaa kokonaisuutta.[57] Tietosuojaperiaatteet toimivatkin siten eräänlaisina tulkintatyökaluina.

2.1.2 Henkilötietojen suoja perusoikeutena

Yhteiskunnassa heräsi kiinnostus henkilötietojen suojaan liittyviin ongelmiin 1970-luvun alussa.[58] Tällöin alettiin laatimaan myös henkilötietojen suojaa koskevia dokumentteja. Taloudellisen kehityksen ja yhteistyön järjestö OECD hyväksyi vuonna 1980 tietosuojasuosituksen,[59] joka

---

[51] TSA johdanto-osa 10 ja 53 kappaleet.
[52] Tietosuojalaissa pseudonymisointi mainitaan vain kerran 6 §:n erityisiä henkilötietoryhmiä koskevan käsittelyn yhteydessä. Anonymisointia ei mainita kertaakaan.
[53] Ks. tarkemmin aineellisesta ja alueellisesta soveltamisalasta TSA 2–3 artiklat. Ks. myös TSA johdanto-osan 14, 18 ja 27 kappaleet. Muun muassa oikeushenkilöihin ja kuolleisiin henkilöihin kohdistuvien tietojen käsittely sekä henkilökohtaiseen toimintaan käyttäminen rajautuvat soveltamisalan ulkopuolelle.
[54] TSA johdanto-osa 3 ja 10 kappaleet.
[55] Ks. C-518/07 (Komissio v. Saksa), kohta 24 ja C-362/14 (Schrems), kohta 42, joiden mukaan valvontaviranomaisen on huolehdittava, että perusoikeuden ja henkilötietojen vapaan liikkuvuuden välillä saavutetaan oikea tasapaino.
[56] Ks. Lynskey 2015, s. 87–88 ja Koops 2014.
[57] Korpisaari ym. 2022, s. 28. Ks. myös Lindroos-Hovinheimo 2018, s. 61. Ks. tietosuojaperiaatteista tarkemmin luku 2.3.1.
[58] Alapuranen ym. 2020, s. 12. Ks. myös Saarenpää – Riekkinen 2023, s. 31.
[59] Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (23.8.1980).

sisältää toisiaan täydentäviä yleisperiaatteita koskien henkilötietojen keräämistä ja laatua, rekisteröidyn tiedonsaantioikeutta, tietoturvaa ja kansainvälistä tiedonsiirtoa.[60] Samaan aikaan yhteistyössä valmisteltiin perusperiaatteiltaan suositusta lähellä oleva Euroopan neuvoston tietosuojayleissopimus[61], joka hyväksyttiin vuonna 1981.[62] Tämän tarkoitus on varmistaa jokaisen yksilön perusoikeuksien ja -vapauksien kunnioittaminen, erityisesti oikeus yksityisyyteen henkilötietojen automaattisessa käsittelyssä.[63] Tästä kehityksestä voidaan huomata, että henkilötietojen suoja perusoikeutena on kehittynyt reaktiona teknologiseen ja yhteiskunnalliseen muutokseen.

Euroopan neuvoston ihmisoikeussopimuksen (jäljempänä 'EIS')[64] 8 artiklan 1 kohdan mukaan jokaisella on oikeus nauttia yksityis- ja perhe-elämäänsä, kotiinsa ja kirjeenvaihtoonsa kohdistuvaa kunnioitusta. Tämän on katsottu sisältävän myös oikeuden henkilötietojen suojaan.[65] EU:n perusoikeuskirjan 7 artikla on käytännössä tämän kanssa yhtenevä. Perusoikeuskirjan 8 artiklan mukaan jokaisella on oikeus henkilötietojensa suojaan ja tutustua hänestä kerättyihin tietoihin ja saada ne oikaistuiksi. [66] Perusoikeuskirjan 8 artikla edellyttää tietojen käsittelyn asianmukaisuutta sekä asianmukaisen henkilön suostumusta taikka laissa säädettyä oikeusperustetta henkilötietojen käsittelylle. Oikeus henkilötietojen suojaan löytyy myös Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT) 16 artiklan 1 kohdasta. TSA:lla käytännössä siten konkretisoidaan EU:n primaarilähteistä löytyvä perusoikeudellinen henkilötietojen suoja.

Vuonna 2009 voimaan tulleen Lissabonin sopimuksen[67] myötä EU:n perusoikeuskirjasta tuli osa EU:n primaarioikeutta. Tällöin henkilötietojen suojasta tuli EU-oikeuden mukainen perusoikeus. Ennen Lissabonin sopimusta EUT ei ollut ottanut ratkaisuissaan kantaa henkilötietojen suojaa koskevaan henkilötietodirektiivin tavoitteeseen, vaan se korosti sisämarkkinoiden kehittämisen

---

[60] Korhonen 2003, s. 93; OECD:n tietosuojasuositus osa 2.
[61] Euroopan neuvoston yleissopimus yksilöiden suojelusta henkilötietojen automaattisessa käsittelyssä (28.1.1981, SopS 36/1992).
[62] Korhonen 2003, s. 93. Vaikka tutkimuksessa ei automaattista henkilötietojen käsittelyä tarkastellakaan tutkimuksen rajatun laajuuden vuoksi, on sillä merkittävä rooli henkilötietojen suojaan liittyvissä kysymyksissä. Pseudonymisoitujen henkilötietojen automaattinen käsittely olisikin potentiaalinen tutkimuskohde.
[63] Euroopan neuvoston tietosuojayleissopimus 1 artikla.
[64] Euroopan neuvoston yleissopimus ihmisoikeuksien ja perusvapauksien suojaamiseksi (4.11.1950, SopS 18/1990).
[65] Ks. Neuvonen 2014, s. 51. Neuvosen mukaan EIS:n tulkinnassa nämä elementit muodostavat yhtenäisen yksityisyyden suojan kokonaisuuden. Ks. myös Korpisaari ym. 2022, s. 8–9, jonka mukaan henkilötietojen suoja kattaa kuitenkin yksityiselämän suojaa laajemman alan.
[66] Perusoikeuskirjan 8 artiklan myötä henkilötietojen suoja siten erotettiin yksityisyyden suojasta.
[67] Lissabonin sopimus Euroopan unionista tehdyn sopimuksen ja Euroopan yhteisön perustamissopimuksen muuttamisesta, allekirjoitettu Lissabonissa 13.12.2007.

tavoitetta.[68] Tämä johtui siitä, ettei EU:lla ollut riittävää toimivaltaa säätää perusoikeuksista ennen Lissabonin sopimusta, sillä vasta tämän voimaantulon myötä EU:n perusoikeuskirja sai saman oikeudellisen arvon kuin EU:n perussopimukset.[69] Ennen tätä EU:lla ei siten ollut edellytyksiä puuttua henkilötietojen suojaa koskeviin kysymyksiin, vaan ainoastaan sisämarkkinoiden kehitykseen. Lissabonin sopimuksen voimaantulon jälkeen EUT:n on katsottu perusteluissaan painottavan perusoikeuksia markkinoiden harmonisoinnin ja henkilötietojen vapaan liikkuvuuden painottamisen sijaan.[70]

Henkilötietojen suojaa on pidetty yhtenä yksityisyyden suojan osa-alueena, joita ovat lisäksi yksityiselämän suoja, kotirauha ja luottamuksellinen viestintä.[71] On kuitenkin perusteltua mieltää henkilötietojen suoja itsenäiseksi perusoikeudeksi, kuten se erotetaan myös EU:n perusoikeuskirjassa.[72] Tietosuojatyöryhmä on korostanut, että henkilötietojen käsittelyssä tulee aina huomioida säännösten tarkoitus suojata yksilöiden perusoikeuksia ja -vapauksia.[73] Tässä yhteydessä on syytä nostaa esiin myös tiedollinen itsemääräämisoikeus, jota pidetään informaatio-oikeudellisena periaatteena ja lähtökohtana henkilötietojen suojalle.[74] Tiedollisella itsemääräämisoikeudella tarkoitetaan henkilötietojen suojaan liittyvien aineellisten ja menettelyllisten oikeuksien kokonaisuutta.[75] TSA korostaa tiedollista itsemääräämisoikeutta muun muassa siten, että luonnollisten henkilöiden on voitava valvoa omia henkilötietojaan ja niiden käsittelytoimia.[76] Tiedollisen itsemääräämisoikeuden voidaankin katsoa koostuvan erilaisista rekisteröidyn oikeuksia ilmentävistä oikeuksista.[77] Tiedolliseen itsemääräämisoikeuteen sisältyvät oikeudet eivät kuitenkaan

---

[68] Lynskey 2015, s. 51. Kuitenkin tuomiossa C-112/00 Schmidberger EYT painotti perusoikeuksien kunnioittamista tavaroiden vapaata liikkuvuutta enemmän. Ks. tarkemmin Ojanen 2004.
[69] SEU 6(1) artikla.
[70] Ollila 2014, s. 815; Lynskey 2013. Ks. esim. julkisasiamies Bobekin ratkaisuehdotus asiassa C-40/17 (FashionID), kohta 72. Julkisasiamies on todennut, että EU:n oikeuskäytäntöä on leimannut pyrkimys tehokkaan henkilötietojen suojan varmistamiseen.
[71] Ks. esim. Neuvonen 2014. Suomen perustuslain (731/1999) 10 §:ssä henkilötietojen suoja on sisällytetty yksityiselämän suojan kanssa samaan momenttiin, ja se on ollut saman muotoisena myös perustuslakia edeltäneen hallitusmuodon (94/1919) 8 §:ssä. Ks. HE 309/1993 vp, s. 52–55, jossa todetaan henkilötietojen suojaa koskevan lainsäädännöllisen tasovaatimuksen tulleen Euroopan neuvoston tietosuojayleissopimuksesta.
[72] Ks. Korpisaari ym. 2022, s. 16–17.
[73] WP136, s. 24.
[74] Voutilainen 2019, s. 36. Voutilaisen mukaan tiedollinen itsemääräämisoikeus pohjautuu saksalaiseen 1980-luvun oikeuskäytäntöön.
[75] Voutilainen 2019, s. 82. Voutilainen kuvaa tiedollista itsemääräämisoikeutta eräänlaiseksi sateenvarjoksi yksilön tietoihin kohdistuviin oikeuksiin.
[76] Alapuranen ym. 2020, s. 31.
[77] Voutilainen 2019, s. 82. Voutilaisen mukaan tiedollinen itsemääräämisoikeus koostuu oikeuksista pitää salassa itseään koskeva tieto, saada itseään koskeva tieto, tarkastaa itseään koskevat tiedot ja korjauttaa niissä olevat virheet, vaikuttaa itseään koskevien tietojen keräämiseen ja luovuttamiseen sekä julkistaa tai antaa itseään koskevia tietoja.

ole ehdottomia, mikä ilmenee myös rekisteröidyn oikeuksia koskevissa poikkeussäännöksissä. Tämä johtuu siitä, että henkilötietojen käsittelyyn liittyvien oikeuksien sääntelyä on pitänyt kehittää niin rekisteröidyn kuin rekisterinpitäjän näkökulmista.[78] Tämäkin ilmentää tietosuojasääntelyn tavoitteiden tasapainottelua sekä eri oikeuksien ja intressien punnintaa. TSA:n johdanto-osan 4 kappaleen mukaan henkilötietojen suojan on oltava oikeassa suhteessa sen tehtävään yhteiskunnassa sekä muihin perusoikeuksiin nähden.

2.1.3 Henkilötietojen vapaan liikkuvuuden tavoite

Teknologia helpottaa entisestään henkilötietojen jakamista, henkilötietojen vapaata kulkua unionissa sekä tietojen siirtämistä kolmansiin maihin ja kansainvälisille järjestöille, mutta samalla se varmistaa henkilötietojen suojan korkean laadun.[79] Euroopan komission mukaan korkeatasoista henkilötietojen suojaa on tarvittu muun muassa siksi, että voitaisiin hyödyntää digitaalitalouden kaikki mahdollisuudet ja parantaa talouskasvua.[80] Tieto nähdään siten hyödykkeenä, jonka käytölle on oltava säännökset niin yksilöiden suojelemiseksi kuin sisämarkkinoiden toimivuuden varmistamiseksi, sillä rajoitukset vapaaseen liikkuvuuteen voivat estää sisämarkkinoiden kehitystä.[81] Koko Euroopan unionin alkuperäinen tavoite onkin ollut taloudellinen integraatio.[82]

Jotta sisämarkkinat toimisivat EU:n alueella moitteetta, henkilötietojen vapaata liikkuvuutta ei unionin sisällä rajoiteta eikä kielletä syistä, jotka liittyvät luonnollisten henkilöiden suojeluun henkilötietojen käsittelyssä.[83] Myös henkilötietojen siirrot kolmansiin maihin ja kansainvälisille järjestöille ovat useille organisaatioille tavanomaisia.[84] Henkilötietojen siirrot unionin ulkopuolelle ovat tarpeen kansainvälisen kaupan ja yhteistyön kehittämiseksi. Tällaisen lisääntyminen aiheuttaa puolestaan henkilötietojen suojaan liittyviä haasteita.[85] Tietosuojasääntelyllä pyritäänkin löytämään tasapaino näiden kahden tavoitteen, henkilötietojen suojan ja henkilötietojen vapaan liikkuvuuden välillä.

---

[78] Voutilainen 2019, s. 84.
[79] TSA johdanto-osa 6 kappale.
[80] COM 2015 (192) final, s. 3.
[81] Voutilainen 2019, s. 65.
[82] Ks. lisää esim. Tolonen 2003, s. 112. Ennen Euroopan unionia kyse oli Euroopan yhteisöstä, mutta selvyyden vuoksi koko tutkimuksessa käytetään näistä ensimmäistä.
[83] TSA johdanto-osa 13 kappale. Ks. myös Lynskey 2015, s. 51.
[84] Korpisaari ym. 2022, s. 466–467.
[85] TSA johdanto-osa 101 kappale. Ks. henkilötietojen siirrosta kolmansiin maihin tai kansainvälisille järjestöille erityisesti TSA luku V.

2.2 Henkilötieto ja anonyymi tieto

TSA 4(1) artiklan mukaan henkilötiedoilla tarkoitetaan

> *– – kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja. Tunnistettavissa olevana puolestaan pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa tunnistetietojen, esimerkiksi nimen, henkilötunnuksen, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurisen tai sosiaalisen tekijän perusteella.*

Tieto katsotaan EUT:n vakiintuneen oikeuskäytännön mukaan henkilötiedoksi, kun se liittyy tunnistettuun tai tunnistettavissa olevaan henkilöön sisältönsä, tarkoituksensa tai vaikutuksensa vuoksi.[86] Henkilötiedon käsite on myös niin sanotusti teknologianeutraali, eli se kattaa kaikenlaisessa muodossa olevat tiedot, joista henkilö on tunnistettavissa.[87] Teknologisen kehityksen seurauksena ympäristöstä kerätään laajasti tietoja, joiden avulla henkilöitä on entistä helpompi tunnistaa. Kaikista teknologian mahdollistamista tunnistamistavoista emme välttämättä ole edes tietoisia.[88]

Erityiset henkilötietoryhmät on määritelty TSA 9 artiklassa. Sellaisten henkilötietojen käsittely on kiellettyä, joista ilmenee rotu tai etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus taikka ammattiliiton jäsenyys. Lisäksi kiellettyä on geneettisten tai biometristen tietojen käsittely henkilön yksiselitteistä tunnistamista varten tai terveyttä koskevien tietojen taikka luonnollisen henkilön seksuaalista käyttäytymistä ja suuntautumista koskevien tietojen käsittely. Näitä tietoja voidaan kuitenkin käsitellä TSA 9 artiklassa määritellyin poikkeuksin.

Henkilötiedon käsittelyllä tarkoitetaan TSA 4(2) artiklan mukaan *”henkilötietojen keräämistä, tallettamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista.”* Toisin sanoen henkilötietojen käsittelyä ovat kaikki henkilötietoihin kohdistuvat toiminnot.[89] Näin ollen tutki-

---

[86] Ks. esim. C-413/23 P (SRB), kohta 55; C-434/16 (Nowak), kohta 35 ja C-479/22 P (OC v. Komissio), kohta 45.
[87] WP136, s. 7; TSA johdanto-osa 26 kappale; Purtova 2018, s. 44.
[88] Ks. Purtova 2018, s. 44.
[89] Ks. myös Alapuranen ym. 2020, s. 41, jonka mukaan tietosuojalainsäädäntö on koko informaation elinkaaren kattavaa lainsäädäntöä, sillä sääntely koskettaa kaikkia eri tietojenkäsittelyn vaiheita.

muksen kannalta relevantit tietosuojatoimenpiteet eli henkilötietojen pseudonymisointi ja anonymisointi ovat molemmat henkilötietojen käsittelyä. Erityisiin henkilötietoryhmiin kuuluvia tietoja ei lähtökohtaisesti käsitellä ja niitä on suojeltava erityisen tarkasti.[90]

Tietosuojatyöryhmä on katsonut henkilötiedon rakentuvan neljästä elementistä: 1) kaikenlaiset tiedot 2) jotka liittyvät 3) tunnistettuun tai tunnistettavissa olevaan 4) luonnolliseen henkilöön.[91] Näistä kolmannen kohdan voidaan katsoa olevan tutkimuksen kannalta merkityksellisin, sillä tunnistettavuus määrittää sen, onko pseudonymisoitu tai anonymisoitu tieto katsottava henkilötiedoksi. Henkilötietoa voi olla kaikki tieto, jota käytetään minkä tahansa tiedon ilmaisemiseen edellyttäen, että tieto liittyy tunnistettavissa olevaan luonnolliseen henkilöön.[92] Henkilö voi olla suoraan tunnistettavissa esimerkiksi nimen ja syntymäajan perusteella. Henkilö voidaan myös epäsuorasti tunnistaa, jos tämä on mahdollista erottaa muista yhdistelemällä tietoja muihin tietoihin.[93] Henkilötiedon käsite kattaa niin objektiiviset tiedot, kuten verinäytteenoton tuloksena verestä löytyneet aineet, kuin myös subjektiiviset tiedot, esimerkiksi mielipiteet.[94] Myös esimerkiksi lääkemääräystietojen on katsottu olevan henkilötietoja sekä potilaan että lääkärin osalta.[95] Henkilötietojen ei kuitenkaan tarvitse olla tosia kuuluakseen määritelmän piiriin.[96] Henkilötieto voidaan siten mieltää hyvin laajaksi, joustavaksi ja mukautuvaksi käsitteeksi.[97]

EU:n lainsäätäjän alkuperäinen tarkoitus on ollut antaa henkilötiedolle laaja merkitys, jotta se kattaisi kaikki tunnistettavissa olevaa henkilöä koskevat tiedot. Tästä huolimatta henkilötiedon käsite ei ole rajaton.[98] Tietosuojatyöryhmä on todennut, ettei tietosuojasääntelyn soveltamisalaa tule laajentaa liikaa.[99] Henkilötiedon käsitettä ei kuitenkaan pidä supistaa vain sen vuoksi, että

---

[90] Käsittelykieltoon on kuitenkin tiettyjä poikkeuksia. Ks. näistä poikkeuksista TSA 9 artikla ja TSA johdantoosa 51 kappale. Erityisiin henkilötietoryhmiin kuuluvien arkaluonteisten tietojen käsittely voi aiheuttaa merkittäviä riskejä henkilön perusoikeuksille ja -vapauksille.

[91] WP136, s. 6. Tietosuojatyöryhmä käyttää sanan ”liittyvä” tilalla ”koskeva”. Tämä ilmenee myös henkilötietodirektiivin 2 artiklan määritelmässä. TSA:n mukaisen ilmaisun ”liittyvä” voidaan siten katsoa kattavan laajemman alan henkilötietodirektiivin määritelmään verrattuna.

[92] WP136, s. 6.

[93] WP136, s. 13–14. Ks. myös Korpisaari ym. 2022, s. 604.

[94] WP136, s. 6. Ks. mielipiteiden osalta EUT:n ratkaisu C-434/16 (Nowak).

[95] Ks. WP136, s. 7 ja Korpisaari ym. 2022, s. 602. Lääkemääräystietojen voidaan katsoa koskevan lääkkeen määrännyttä lääkäriä, vaikkei potilaan nimeä mainittaisi. Tietosuojatyöryhmän mukaan tunnistetun tai tunnistettavissa olevan lääkärin kirjoittamien lääkemääräysten tietojen toimittaminen valmistajille on henkilötietojen toimittamista sivullisille.

[96] WP136, s. 6. Tietosuojasääntelyssä on otettu huomioon virheellisten tietojen mahdollisuus, minkä vuoksi rekisteröidyllä on oikeus tarkastaa tiedot ja saada ne oikaistuiksi.

[97] Purtova 2018, s. 44. Purtova on kritisoinut henkilötiedon käsitteen laajuutta toteamalla TSA:n olevan niin sanottuna yleislakina “the law of everything”.

[98] WP136, s. 4 ja 24. Ks. myös COM (92) 422 final, s. 10.

[99] WP136, s. 5 ja 25. Tietosuojatyöryhmä on myös todennut, että on parempi olla aiheettomasti rajoittamatta henkilötietojen käsitteen määritelmän tulkintaa ja huomata, että soveltamisessa voidaan joustaa.

joidenkin henkilötietojen käsittely olisi sääntelyn asettamilta velvoitteilta kevyempää.[100] Oikeuskirjallisuudessa on myös argumentoitu, että laaja henkilötiedon käsite johtaa väistämättä tilanteisiin, jossa tietosuojasääntelyä sovelletaan tietosuojan ydinalueen ulkopuolelle. Samalla se kuitenkin tukee yksityisyyden suojaa varmistaen tietosuojasääntelyn soveltumisen joustavasti.[101] Laaja tulkinta voi kuitenkin johtaa kokonaisuudessaan tehottomaan sääntelyyn ja vaikeuttaa sen tarkoituksenmukaista kohdentamista, mutta johtaa myös muiden perusoikeuksien rajoittumiseen.[102]

Jos tieto ei ole henkilötietoa, on se anonyymiä tietoa. Tietosuojasääntely ei koske anonyymien tietojen käsittelyä.[103] Tämä korostaa tarvetta henkilötietojen ja anonyymien tietojen välisen rajanvedon selkeyteen, sillä käytännössä kyse on tietosuojasääntelyn soveltamisalan määrittelystä.[104] Suomen sosiaali- ja terveysministeriön mukaan anonyymin tiedon tulee käytännössä täyttää neljä ominaisuutta: anonyymistä tiedosta ei voida tunnistaa yksilöä, tehdä vain tiettyyn yksilöön kohdistuvia päätelmiä, tietoja ei pysty yhdistelemään muihin tietoihin ja tunnistettavuus on peruuttamaton tai ainakin kohtuuttoman vaikeasti saavutettavaa.[105]

Oikeustieteellisissä keskusteluissa on esiintynyt jakautuvia näkemyksiä siitä, tulisiko henkilötiedon käsitteen olla absoluuttinen vai suhteellinen. Absoluuttisella henkilötiedon käsitteellä tarkoitetaan, että jos yksikin taho pystyy yhdistämään tiedon luonnolliseen henkilöön, on se silloin henkilötietoa. Suhteellinen henkilötietokäsite on taas näkökulmariippuvainen siten, että jos osapuoli ei pysty yhdistämään tietoa luonnolliseen henkilöön, ei se silloin olisi kyseisen tahon näkökulmasta enää henkilötietoa.[106] Tiivistetysti tämä ero tarkoittaa, että absoluuttisesta näkökulmasta tieto on henkilötietoa kaikille, kun suhteellisesta se on vain osalle. Valittu lähestymistapa vaikuttaa siis suoraan tietosuojasääntelyn soveltamisalaan. Tämä konkretisoituu erityisesti pseudonymisoidun tiedon kohdalla ja on merkittävä myös tämän tutkimuksen kannalta arvioitaessa pseudonymisoidun tiedon henkilötietoluonnetta. Jos tiedon ei tietyssä tapauksessa katsota

---

[100] Korpisaari ym. 2022, s. 601.
[101] Rauhanen 2025, s. 663.
[102] Ks. Rauhanen 2025, s. 663; Ks. myös Purtova 2018 henkilötietokäsitteen laajuuteen kohdistuvasta kritiikistä.
[103] TSA johdanto-osa 26 kappale. Huomionarvoista kuitenkin, että anonyymiin tietoon voi kohdistua muuta sääntelyä.
[104] Stalla-Bourdillon – Knight 2016, s. 320–321.
[105] STM periaatepäätös, s. 2. Ks. myös ICO 2022a s. 5, jonka mukaan henkilötiedon ja anonyymin tiedon rajanvedon kolme keskeistä tekijää ovat erottaminen muista, yhdistettävyys ja päätelmät.
[106] Ks. esim. C-582/14 (Breyer); Rauhanen 2025, s. 658; Craddock 2025; Zuiderveen Borgesius 2017, s. 135. Suhteellisesta henkilötietokäsitteestä voidaan käyttää myös esimerkiksi ilmaisua relatiivinen tai objektiivinen henkilötietokäsite. Näillä tarkoitetaan kuitenkin samaa ilmiötä.

olevan henkilötietoa, sillä voi olla huomattavia vaikutuksia ensinnäkin henkilötietojen suojan mutta myös rekisteröidyn oikeuksien toteutumisen kannalta.

2.3 Tietosuojaperiaatteet ja riskiperusteinen lähestymistapa

2.3.1 Henkilötietojen käsittelyä ohjaavat periaatteet

TSA:n lähtökohtana on, että kaikkea ei ole pyritty sääntelemään ehdottomilla normeilla, vaan monissa tilanteissa henkilötietojen käsittelyä ohjaavat tietosuojaperiaatteet, joiden noudattaminen on rekisterinpitäjän vastuulla.[107] TSA 5 artiklan tietosuojaperiaatteet tulee huomioida myös pseudonymisoinnin ja anonymisoinnin kohdalla.

Lainmukaisuus, kohtuullisuus ja läpinäkyvyys. Henkilötietoja on ensinnäkin käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi. Luonnollisille henkilöille tulisi olla läpinäkyvää, miten heitä koskevia henkilötietoja käsitellään.[108] Erityisesti henkilötietojen käsittelyn tarkoitukset tulisi yksiselitteisesti ja lainmukaisesti ilmoittaa jo henkilötietojen keräämisen yhteydessä.[109] Lainmukaisuusvaatimus liittyy myös oikeusturvan ja hyvän hallinnon perusoikeuksien toteuttamiseen.[110] Jotta henkilötietojen käsittely olisi lainmukaista, tulisi sen perustua rekisteröidyn suostumukseen tai muuhun oikeutettuun perusteeseen.[111] Muita oikeutettuja perusteita ovat sopimuksen täytäntöönpano, rekisterinpitäjän lakisääteisen velvoitteen noudattaminen, elintärkeiden etujen suojaaminen, yleistä etua koskevan tehtävän suorittaminen sekä rekisterinpitäjälle kuuluvan julkisen vallan käyttäminen ja oikeutettujen etujen toteuttaminen.[112] Henkilötietojen käsittely rekisterinpitäjän oikeutetun edun perusteella edellyttää tasapainotestin tekemistä, jossa oikeutettu etu todetaan rekisteröidyn oikeuksia painavammaksi.[113] Suostumus

---

[107] Korpisaari ym. 2022, s. 28; Ks. TSA 5 luku. Rekisterinpitäjän osoitusvelvollisuus on yksi henkilötietojen käsittelyä ohjaavista periaatteista.
[108] TSA 5(2)a artikla; TSA johdanto-osa 39 kappale.
[109] Alapuranen ym. 2020, s. 54.
[110] Voutilainen 2019, s. 69. Ks. Saarenpää 2000, s. 14, jonka mukaan mm. oikeudet yksityisyyteen, tietoturvallisuuteen ja oikeusturvaan ovat keskeisiä informaatio-oikeudellisia metaperiaatteita. Ks. myös Voutilainen 2019, s. 25, jonka mukaan metaperiaatteet sijoittuvat oikeuden syvätasolle vaikuttaen tietosuojasäänTelyn taustalla turvaten oikeutta henkilötietojen suojaan.
[111] TSA johdanto-osa 40 kappale; EU:n perusoikeuskirjan 8(2) artikla; Ks. myös Voutilainen 2019, s. 85, jonka mukaan julkisen vallan käytössä suostumusta on pidetty monissa tilanteissa yhteensopimattomana.
[112] Korpisaari ym. 2022, s. 28–29. Ks. käsittelyn lainmukaisuudesta TSA 6 artikla, suostumuksesta 7–8 artiklat ja erityisistä henkilötietoryhmistä 9 artikla.
[113] Korpisaari ym. 2022, s. 132. Ks. EDPB 1/2025, s. 15 kohta 55. Ks. myös WP217, s. 74, jossa henkilötietojen kerääminen siten, että tiedot välittömästi anonymisoitiin ja niitä käytettiin vain tilastojen laatimiseen, auttoi tasapainotestissä kallistumaan enemmän rekisterinpitäjän oikeutetun edun puoleen.

tulee antaa selkeästi suostumusta ilmaisevalla toimella, kuten kirjallisesti tai suullisella lausumalla, josta käy ilmi, että suostumus on vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu. Suostumuksen olisi katettava kaikki sellaiset käsittelytoimet, jotka toteutetaan samaa tarkoitusta varten, ja suostumus tulee antaa jokaista käsittelytarkoitusta varten.[114] Rekisteröidyllä on TSA 7(3) artiklan mukaan oikeus peruuttaa suostumuksensa milloin tahansa. EUT on katsonut, että suostumuksen pätevyys riippuu siitä, onko henkilö saanut ennalta tiedot kaikista tietojen käsittelyyn liittyvistä olosuhteista, joihin hänellä on oikeus.[115]

Käyttötarkoitussidonnaisuus. Käyttötarkoitussidonnaisuuden periaatteen mukaan henkilötietoja on kerättävä tiettyä, nimenomaista ja laillista tarkoitusta varten, eikä niitä saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteensopimattomalla tavalla.[116] Käyttötarkoitussidonnaisuuden periaate vaikuttaa lähtökohtaisesti kaikissa tilanteissa ja se rajaa henkilötietojen myöhempää käyttöä.[117] Myös henkilötietojen pseudonymisoinnin ja anonymisoinnin kohdalla tulee arvioida käsittelyn yhteensopivuutta alkuperäisen tarkoituksen kanssa. Pseudonymisointia voidaan pitää keinona tietosuojariskien minimointiin, jolloin tehokkaasti toteutettuna se voisi mahdollistaa tasapainotestin kallistumisen siihen, että jatkokäsittelyä voidaan pitää yhteensopivana.[118] Vaikka anonymisoinnin lopputuloksena on anonyymi tieto, on itse anonymisointiprosessi vielä henkilötiedon käsittelyä. Anonymisointia voidaan lähtökohtaisesti pitää käyttötarkoituksiin nähden yhteensopivana, koska toimenpiteellä tunnistettavuus poistetaan. Anonyymiin tietoon itsessään ei käyttötarkoitussidonnaisuuskaan enää sovellu. Myöhempää käsittelyä yleisen edun mukaisia arkistointitarkoituksia taikka tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten ei katsota yhteensopimattomiksi alkuperäisten tietojen kanssa 89 artiklan 1 kohdan mukaisesti. Tämäkin edellyttää kuitenkin asianmukaisia teknisiä ja organisatorisia toimenpiteitä rekisteröidyn oikeuksien ja vapauksien turvaamiseksi.[119]

---

[114] TSA 4(11) artikla; TSA johdanto-osa 32 kappale.
[115] Ks. esim. C-757/22 (Meta Platforms Ireland), kohta 60.
[116] TSA 5(1)b artikla.
[117] Alapuranen ym. 2020, s. 58. Ks. kuitenkin TSA 6(4) artikla henkilötietojen käsittelystä muuhun kuin alkuperäiseen tarkoitukseen muissa kuin suostumukseen tai lakiin perustuvissa asioissa.
[118] Ks. Tarhonen 2016, s. 24; TSA 6 artikla 4 kohta.
[119] TSA 5(1)b artikla.

Tietojen minimointi. Tietojen minimoinnin periaatteen mukaan henkilötietojen on oltava asianmukaisia, olennaisia ja rajoitettuja siihen, mikä on tarpeellista suhteessa käsittelyn tarkoituksiin.[120] Tämä puolestaan edellyttää käsittelyn tarkoitusten määrittämistä. Henkilötietoja on käsiteltävä vain, jos käsittelyn tarkoitusta ei muilla keinoin voida toteuttaa.[121] Tietojen minimointi koskee siten sitä, kuinka paljon ja mitä tietoa käsitellään. Jos henkilötietoja ei enää tarvita, tulee ne poistaa tai anonymisoida.[122] Mikäli henkilötietojen käsittelyä ei organisaatiossa pystytä välttämään tai muutoin minimoimaan, pseudonymisointi on henkilötietojen suojaamiseksi huomionarvoinen toimenpide.[123] Henkilötietojen minimoinnilla on siten tiivis yhteys henkilötietojen pseudonymisointiin ja anonymisointiin. Voidaan todeta, että tietojen minimointi heijastaa pyrkimystä vähentää tietosuojariskejä jo ennalta. Pseudonymisoivan rekisterinpitäjän suorittama pseudonymisointi auttaa myös vastaanottavia rekisterinpitäjiä täyttämään esimerkiksi tietojen minimoinnin ja oletusarvoisen tietosuojan periaatteet.[124] Myös Suomen tietosuojavaltuutettu on pitänyt pseudonymisointia perusteltuna suojatoimena tietojen minimoinnin näkökulmasta.[125]

Täsmällisyys. Henkilötietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä. Henkilötietojen käsittelyssä on toteutettava kaikki mahdolliset kohtuulliset toimenpiteet sen varmistamiseksi, että käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä.[126] Tämä ilmentää osaltaan yksilön tiedollista itsemääräämisoikeutta siinä, että jokaisella on oikeus tulla arvioiduksi oikeiden tietojen valossa.[127] Tällä periaatteella on suora yhteys rekisteröidyn oikeuksiin saada tietonsa oikaistuiksi tai poistetuiksi.[128]

Säilytyksen rajoittaminen. Henkilötietojen säilyttämistä on rajoitettava, ja niitä on säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten.[129] Jos tunnistaminen ei ole enää tarpeellista, tulee

---

[120] TSA 5(1)c artikla.
[121] TSA johdanto-osa 39 kappale.
[122] Ks. EDPB 4/2019, s. 22 kohdat 73 ja 75.
[123] Andersson 2024, s. 321.
[124] Ks. EDPB 1/2025, s. 14 kohta 49.
[125] Ks. TSV 23.6.2022. Ratkaisu koski automatisoituja päätöksiä ja potilastietojen käsittelyä ennaltaehkäisyn ja ennakoinnin tarkoituksissa.
[126] TSA 5(1)d artikla.
[127] Alapuranen ym. 2020, s. 62.
[128] Ks. rekisteröidyn oikeuksista luku 2.4.
[129] TSA 5(1)e artikla. Henkilötietoja voidaan kuitenkin säilyttää pidempiä aikoja yleisen edun mukaisia arkistointitarkoituksia taikka tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten 89 artiklan 1 kohdan mukaisesti.

tiedot poistaa tai anonymisoida.[130] Tällä on yhteys myös tunnistamisen mahdollistaviin lisätietoihin eli relatiiviseen avaimeen, joka voi itsessään olla henkilötietoa.[131] Säilytyksen rajoittaminen koskee sitä, kuinka kauan tietoa säilytetään. Säilytyksen rajoittamisen ja tietojen minimoinnin periaatteet tukevat toisiaan, sillä pelkkä tietojen vähäinen määrä ei oikeuta niiden säilyttämistä rajattomasti eikä toisaalta lyhyt säilytysaika oikeuta keräämään rajattomasti tietoja.

Eheys ja luottamuksellisuus. Henkilötietoja on käsiteltävä tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus, mukaan lukien suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen asianmukaisia teknisiä ja organisatorisia toimia.[132] Esimerkiksi pseudonymisoinnin luvaton kumoutuminen voidaan katsoa tällaiseksi riskiksi, johon tulee varautua.[133] Tällainen tietoturvallisuus liittyy läheisesti riskiperusteiseen lähestymistapaan.[134] Tietoturvaa voidaankin kuvata tietosuojan toteuttamisen keinoksi. Tietojen suojaamisesta on huolehdittava koko henkilötietojen käsittelyn elinkaaren ajan, mikä edellyttää henkilötietojen käsittelyn seuraamista ja valvontaa.[135] Pseudonymisointi toimii vain, jos lisätiedot pidetään erillään ja pääsy niihin on rajattu. Näin eheyden ja luottamuksellisuuden vaatimuksella on selkeä yhteys pseudonymisoinnin tehokkuuteen, sillä tunnistaminen riippuu myös suojauksen tehokkuudesta ja toteutetuista tietoturvatoimenpiteistä.

2.3.2 Riskiperusteinen lähestymistapa sekä tekniset ja organisatoriset toimenpiteet

Riskiperusteista lähestymistapaa ei ole nimenomaisesti erikseen TSA:ssa määritelty, mutta se ilmenee useasta artiklasta.[136] Riskiperusteinen lähestymistapa tarkoittaa, että rekisterinpitäjän on arvioitava henkilötietojen käsittelyyn liittyvät riskit ja suhteutettava niihin tietosuojasääntelyn velvoitteet ja asianmukaiset toimenpiteet.[137] Näiden toimenpiteiden avulla varmistetaan asianmukainen turvallisuustaso ottaen huomioon uusin tekniikka ja toteuttamiskustannukset suhteessa henkilötietojen käsittelyn riskeihin ja suojeltavien henkilötietojen luonteeseen. Lisäksi tä-

---

[130] Ks. EDPB 4/2019, s. 22 kohdat 73 ja 75. Rekisterinpitäjän on säännöllisesti arvioitava, ovatko henkilötiedot yhä tarpeellisia.
[131] Ks. EDPB 1/2025, s. 9 kohta 20; Ks. relatiivisesta avaimesta tarkemmin luku 3.1.
[132] TSA 5(1)f artikla.
[133] Ks. TSA johdanto-osa 75 kappale.
[134] Alapuranen ym. 2020, s. 67; Tietosuojavaltuutetun toimisto 4/2017, s. 16.
[135] Alapuranen ym. 2020, s. 67.
[136] Riskiperusteinen lähestymistapa ilmenee TSA:ssa esimerkiksi artiklassa 24 (rekisterinpitäjän vastuu), 25 (sisäänrakennettu ja oletusarvoinen tietosuoja) ja 35 (tietosuojaa koskeva vaikutustenarviointi).
[137] Tietosuojavaltuutetun toimisto 4/2017, s. 16. Ks. TSA 35 artikla, joka koskee korkean riskin tilanteissa tehtäviä vaikutustenarviointeja.

män pohjalta toteutetaan henkilötietojen suojaamiseksi tarvittavat tekniset ja organisatoriset toimenpiteet.[138] Teknisiä ja organisatorisia toimenpiteitä on TSA 24 artiklan mukaan tarkistettava ja tarvittaessa päivitettävä. Riskiperusteinen henkilötietojen hallinta edellyttääkin jatkuvaa riskien kartoittamista ja niiden minimointiin liittyviä toimenpiteitä.[139]

TSA 25 artiklan sisäänrakennettu ja oletusarvoinen tietosuoja tarkoittaa systemaattista lähestymistapaa, jossa tietosuoja otetaan huomioon jo tietojärjestelmien ja henkilötietojen käsittelytoimien suunnittelussa.[140] Tämä tarkoittaa sitä, että rekisterinpitäjän tulisi sisäänrakennetun ja oletusarvoisen tietosuojan mukaisesti ottaa pseudonymisointi ja anonymisointi huomioon jo ennen varsinaisiin käsittelytoimiin ryhtymistä. Pseudonymisoinnin tehokkuus tietosuojaperiaatteiden täytäntöönpanossa riippuu suuresti siitä, keiltä pseudonymisoidun tiedon tunnistettavuus estetään.[141] Sisäänrakennettu ja oletusarvoinen tietosuoja kuvastaa siten ennakoivaa lähestymistapaa, jossa riskit pyritään ehkäisemään jo ennen niiden realisoitumista.

Tietosuojaa koskevasta vaikutustenarvioinnista säädetään TSA 35 artiklassa: ”[j]*os tietyntyyppinen käsittely etenkin uutta teknologiaa käytettäessä todennäköisesti aiheuttaa – – luonnollisen henkilön oikeuksien ja vapauksien kannalta korkean riskin, rekisterinpitäjän on ennen käsittelyä toteutettava arviointi suunniteltujen käsittelytoimien vaikutuksista henkilötietojen suojalle*.” Voidaankin todeta, että esimerkiksi tekoälyn hyödyntäminen aineiston analysointiin voi olla sellainen tekninen ratkaisu, joka voisi aiheuttaa korkean riskin ja johtaa vaikutustenarvioinnin tarpeellisuuteen. Vaikutuksenarviointi on tehtävä, jos käsittelytoimesta todennäköisesti aiheutuisi korkea riski. On huomioitava, että tietyn tasoista riskianalyysiä tulee tehdä jo pelkästään vaikutuksenarvioinnin suorittamistarpeen määrittämiseksi.

Luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit voivat TSA:n johdanto-osan 75 kappaleen mukaan aiheutua ensinnäkin henkilötietojen käsittelystä, joka voi aiheuttaa fyysisiä, aineellisia tai aineettomia vahinkoja, eritysesti jos käsittely saattaisi johtaa esimerkiksi pseudonymisoinnin luvattomaan kumoutumiseen tai aiheuttaa muuta merkittävää taloudellista tai sosiaalista vahinkoa. Riskejä voi aiheutua myös silloin, kun rekisteröidyltä evätään oikeuksia ja vapauksia, estetään tätä valvomasta omia henkilötietojaan, käsitellään erityisiin henkilötietoryhmiin kuuluvia tietoja, arvioidaan hen-

[138] TSA 32 artikla. Ks. myös Voutilainen 2019, s. 123–124.
[139] Voutilainen 2019, s. 124.
[140] Korpisaari ym. 2022, s. 311.
[141] Ks. EDPB 1/2025, s. 4.

kilökohtaisia ominaisuuksia tai kun käsitellään heikossa asemassa olevien tietoja tai suuria määriä henkilötietoja. Nämä vaihtelevat riskit korostavat tarvetta arvioida pseudonymisoitujen ja anonymisoitujen tietojen tunnistettavuutta huolellisesti.

Henkilötietojen käsittelyssä oikeuksien ja vapauksien suoja edellyttää asianmukaisten teknisten ja organisatoristen toimenpiteiden toteuttamista.[142] Pseudonymisointi on TSA:ssa määritelty tällaiseksi toimenpiteeksi, jonka avulla niin rekisterinpitäjät kuin henkilötietojen käsittelijät voivat vähentää rekisteröityihin kohdistuvia riskejä ja täyttää tietosuojasääntelyn mukaiset velvoitteensa.[143] Organisatorisiin toimenpiteisiin voidaan katsoa kuuluvan esimerkiksi toimintalinjaukset, periaatteet, organisaatiojärjestelyt, henkilöstön tehtävien ja vastuiden määrittelyt sekä ohjeistus, koulutus ja valvonta. Teknisiä toimenpiteitä ovat puolestaan esimerkiksi laitteille ja järjestelmiin pääsyn valvonta, tietojen ja järjestelmien luvattoman käytön esto, tapahtumien kirjaaminen, tietoliikenteen alkuperävalvonta ja reititysvalvonta, järjestelmien käyttöoikeuksien määrittely, ylläpitotoimien asianmukainen järjestäminen sekä tietojen ja järjestelmien suojaaminen tietoturvaa vaarantavilta tapahtumilta.[144]

2.4 Rekisteröidyn oikeudet henkilötietojen käsittelyssä

2.4.1 Rekisteröidyn oikeudet: erityisesti tiedonsaanti-, oikaisu- ja poistamisoikeus

Henkilötietojen käsittelyperuste vaikuttaa siihen, mitä oikeuksia rekisteröidyllä on suhteessa rekisterinpitäjään. EU:n perusoikeusulottuvuuden kehittymisen myötä ovat kehittyneet myös EUT:n rekisteröidyn oikeuksia koskevat tulkinnat.[145] Tässä tutkimuksessa rekisteröidyn oikeuksien toteutumista tarkastellaan erityisesti tiedonsaanti-, oikaisu- ja poistamisoikeuteen painottuen, sillä niiden avulla rekisteröity voi konkreettisesti vaikuttaa omiin tietoihinsa. Tiedonsaanti- ja oikaisuoikeudet turvataan TSA:n lisäksi myös EU:n perusoikeuskirjan 8(2) artiklassa.

Rekisteröidyllä on TSA 15 artiklan mukaan oikeus saada pääsy tietoihinsa eli niin sanottu tiedonsaantioikeus. Rekisteröidyllä on siten oikeus saada rekisterinpitäjältä vahvistus siitä, käsitelläänkö hänen henkilötietojaan ja saada tietoja henkilötietojensa käsittelyyn liittyvistä asioista

---

[142] TSA 32 artiklassa on esimerkinomaisesti lueteltu teknisiä ja organisatorisia toimenpiteitä, mutta lista ei ole tyhjentävä.
[143] EDPB 1/2025, s. 10 kohta 23.
[144] Korpisaari ym. 2022, s. 304.
[145] Ollila 2014, s. 821. Ennen Lissabonin sopimusta EUT tulkitsi rekisteröidyn oikeuksia henkilötietodirektiivin taloudellisten tavoitteiden ja henkilöiden perusoikeuksien ja -vapauksien yhteensovittamisen pohjalta. Ks. tästä lisää Ollila 2014, s. 820–821. Näin on siitä huolimatta, ettei EUT:llä ollut toimivaltuuksia puuttua perusoikeudellisella tasolla jäsenvaltioiden toimintaan.

sekä muista rekisteröidyn oikeuksista.[146] Tiedonsaantioikeuden toteutuessa rekisteröity pystyy arvioimaan henkilötietojensa käsittelyn lainmukaisuutta ja oikeellisuutta.[147] Tiedonsaantioikeus kytkeytyy siten myös tietosuojaperiaatteisiin. Rekisteröidyn tulee lisäksi pystyä käyttämään oikeuttaan vaivattomasti ja kohtuullisin väliajoin, eikä rekisteröidyn tarvitse esittää syytä omiin tietoihinsa tutustumiselle.[148] Käytännössä rekisterinpitäjä ilmoittaa rekisteröidylle henkilötietojen käsittelyyn liittyvistä asioista tietosuojaselosteessa.[149] Rekisteröidyn oikeus saada tietoja omista oikeuksistaan korostuu erityisiin henkilötietoryhmiin kuuluvien henkilötietojen ja yksityiselämän suojan ydinalueeseen kuuluvien henkilötietojen, esimerkiksi terveystietojen kohdalla.[150] EUT on katsonut, että rekisteröidylle toimitettujen tietojen on oltava mahdollisimman tarkkoja. EUT:n mukaan rekisteröidyllä on mahdollisuus saada rekisterinpitäjältä tietoja nimenomaisista vastaanottajista, tai vaihtoehtoisesti valita pyytää vain vastaanottajaryhmiä koskevia tietoja.[151] Kuitenkin tiedonsaantioikeutta voidaan rajoittaa koskemaan vastaanottajaryhmiä koskevia tietoja, jos rekisteröidylle on mahdotonta luovuttaa tietoja konkreettisista vastaanottajista.[152] Jos henkilötietoja koskevat muutokset ovat perustavanlaatuisia tai rekisteröidyn kannalta muuten olennaisia, rekisteröidylle on ilmoitettava näistä yksiselitteisesti hyvissä ajoin ennen niiden voimaantuloa. Näin rekisteröity pystyy arvioimaan muutoksen vaikutuksia ja käyttämään oikeuksiaan.[153] Läpinäkyvyysvaatimuksesta johtuen rekisterinpitäjän on annettava rekisteröidylle etukäteen riittävästi tietoa tämän oikeuksista tai oikeuksiin kohdistuvista mahdollisista rajoituksista, jotta ne eivät myöhemmin ilmene yllättäen rekisteröidyn yrittäessä käyttää oikeuksiaan suhteessa rekisterinpitäjään.[154]

Rekisteröidyllä on TSA 16 artiklan mukaan oikeus henkilötietojensa oikaisemiseen eli oikaisuoikeus. Rekisteröidyllä on oikeus vaatia, että rekisterinpitäjä oikaisee rekisteröityä koskevat epätarkat ja virheelliset henkilötiedot ilman aiheetonta viivytystä. Oikaisuoikeutta koskevaa TSA

---

[146] Rekisteröidyllä on esimerkiksi oikeus saada tiedot käsittelyn tarkoituksesta, kyseessä olevat henkilötietoryhmät, vastaanottajat tai vastaanottajaryhmät sekä mahdollisuuksien mukaan henkilötietojen säilytysaika tai sen määrittämiskriteerit. Ks. tarkemmin TSA 15 artikla.
[147] Alapuranen ym. 2020, s. 93.
[148] Alapuranen ym. 2020, s. 93; Voutilainen 2019, s. 101, jonka mukaan kohtuullista aikaväliä ei kuitenkaan TSA:ssa tarkemmin määritellä.
[149] Andersson 2024, s. 167. Tietosuojaseloste on eri asia kuin seloste käsittelytoimista, eikä tietosuojaseloste ole pakollinen dokumentti. Tietosuojaselosteella toteutetaan läpinäkyvyysvaatimusta suoraan rekisteröidylle.
[150] Voutilainen 2019, s. 95.
[151] C-154/21 (Österreichische Post), kohta 43; TSA 15 artikla.
[152] C-154/21 (Österreichische Post), kohdat 47–51. Näin on esimerkiksi, jos konkreettisista vastaanottajista on mahdotonta luovuttaa tietoa, koska ne eivät ole vielä tiedossa, taikka vastaanottajien tunnistaminen on mahdotonta tai rekisteröidyn pyyntö tutustua näihin tietoihin on ilmeisen perusteeton tai kohtuuton.
[153] WP260, s. 17.
[154] WP260, s. 35.

16 artiklaa on tulkittava yhdessä täsmällisyysperiaatteen kanssa, ja sen tarkoitus on ehkäistä väärien johtopäätösten tai päätösten tekemistä virheellisten tai epätarkkojen tietojen johdosta.[155] Rekisteröity voi tulla tietoiseksi virheellisistä tai puutteellisista tiedoista joko tarkastusoikeutensa nojalla, sattumalta tai kun tietojen pohjalta on ryhdytty toimenpiteisiin, kuten tehty rekisteröityä koskeva päätös.[156] Rekisterinpitäjällä on yleinen velvoite huolehtia, että henkilötiedot ovat täsmällisiä ja tarvittaessa päivitettyjä, mutta tietojen oikaisemiseen tulee ryhtyä myös rekisteröidyn pyynnöstä.[157] Rekisteröidyllä on oikeus siihen, että häntä koskevia tietoja käsitellään ajantasaisin tiedoin. Näin on etenkin silloin, jos käsiteltävillä tiedoilla on rekisteröidyn asemaan oikeudellisia vaikutuksia. Rekisterinpitäjällä ei kuitenkaan ole velvollisuutta oikaista tietoja, jos rekisteröity ei pysty virheellisyyttä osoittamaan. Sitä vastoin myös rekisterinpitäjällä on osoitusvelvollisuus siitä, että se käsittelee täsmällisiä ja ajantasaisia tietoja hyväksyttävällä syyllä.[158]

Rekisteröidyllä on TSA 17 artiklan mukaan oikeus tietojen poistamiseen eli toisin sanoen poistamisoikeus tai ”oikeus tulla unohdetuksi”. Rekisterinpitäjän tulee poistaa rekisteröityä koskevat tiedot tämän pyynnöstä ilman aiheetonta viivytystä esimerkiksi silloin, jos käsittelylle ei ole muuta laillista perustetta.[159] Tietosuojaneuvosto on todennut, että tiedot voidaan joko poistaa tai anonymisoida.[160] Henkilötietojen anonymisointi on siten vaihtoehto poistamiselle edellyttäen oleellisten tietojen huomioon ottamista ja uudelleentunnistamisen riskin todennäköisyyden ja vakavuuden säännöllistä arviointia.[161] Tämän jälkeen henkilötietoja ei enää käytännössä ole, sillä ne ovat anonyymejä. Kuitenkin tunnistamisen jäännösriski on aina olemassa, jolloin tiedoista voi vielä muuttua henkilötietoa.[162] Jos anonymisointi on epäonnistunut siten, että tiedot lopulta voidaan yhdistää henkilöön, poistamisoikeus voi tosiasiallisesti jäädä toteutumatta.

---

[155] Korpisaari ym. 2022, s. 242.
[156] Korpisaari ym. 2022, s. 242, jonka mukaan kyse voi olla tiedon kirjaamisesta väärän henkilön kohdalle taikka virheellisestä tai vanhentuneesta merkinnästä oikean henkilön kohdalle.
[157] Alapuranen ym. 2020, s. 95.
[158] Voutilainen 2019, s. 108.
[159] TSA 17 artiklan mukaan rekisterinpitäjällä on velvollisuus poistaa tiedot ilman aiheetonta viivytystä jos 1) henkilötietoja ei enää tarvita, 2) rekisteröity peruuttaa suostumuksensa tai vastustaa käsittelyä eikä käsittelyyn ole muuta laillista perustetta, 3) henkilötietoja on käsitelty lainvastaisesti, 4) ne on poistettava lakisääteisen velvoitteen noudattamiseksi tai 5) ne on kerätty tietoyhteiskunnan palvelujen tarjoamisen yhteydessä.
[160] Ks. EDPB 4/2019, s. 13 kohta 53.
[161] EDPB 4/2019, s. 14 kohta 54.
[162] Ks. C-319/22 (Scania), kohdat 46 ja 49. Itsessään anonyymit tiedot voivat muuttua henkilötiedoiksi, kun rekisterinpitäjä asettaa ne muiden henkilöiden saataville, joilla on relatiivinen avain.

2.4.2 Roolit ja velvollisuudet rekisteröidyn oikeuksien soveltamisessa

Rekisterinpitäjällä[163] tarkoitetaan TSA 4(7) artiklan mukaan ”*luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot*.” Kun vähintään kaksi rekisterinpitäjää määrittävät käsittelyn tarkoitukset ja keinot yhdessä, ovat ne TSA 26 artiklan mukaan yhteisrekisterinpitäjiä.[164] Rekisterinpitäjällä on pääasiallinen vastuu henkilötietojen käsittelystä ja TSA:n noudattamisesta.[165] Rekisterinpitäjän on TSA 12(2) artiklan mukaan helpotettava rekisteröidyn oikeuksien käyttöä, ellei TSA 11 ja 12 artikloista muuta johdu.[166]

Rekisterinpitäjä voi tarvita henkilötietojen käsittelyyn avukseen toisen tahon, henkilötietojen käsittelijän, esimerkiksi tarjoamaan rekisterinpitäjälle palvelualustan, teknistä tietojärjestelmän ylläpitoa tai tallennuskapasiteettia.[167] TSA 4(8) artiklan mukaan tällaisella henkilötietojen käsittelijällä tarkoitetaan ”*luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.*” Henkilötietojen käsittelijöitä ovat rekisterinpitäjästä erillisiä olevat toiset organisaatiot ja niissä työskentelevät henkilöt, jotka käsittelevät henkilötietoja rekisterinpitäjän ohjeiden mukaisesti.[168] Tyypillisesti kyse on toimeksianto- tai alihankintasuhteesta, jossa rekisterinpitäjä ulkoistaa jonkin osan käsittelystään.[169] Rekisterinpitäjään palvelussuhteessa olevat henkilöt eivät ole henkilötietojen käsittelijöitä, vaan ne toimivat osana rekisterinpitäjän toimintaa.[170] Henkilötietojen käsittelijä on myös vastuussa henkilötietojen käsittelystä, mutta sen vastuu on rekisterinpitäjää rajoitetumpi.[171] Pseudonymisoinnin ja anonymisoinnin voi suorittaa myös henkilötietojen käsittelijä, joka toimii rekisterinpitäjän lukuun. Rekisterinpitäjän on kuitenkin määriteltävä käsittelytarkoitukset ja on viime kädessä vastuussa kaikista sen lukuun tehdyistä käsittelytoimista.

TSA 28 artiklan mukaan rekisterinpitäjän ja henkilötietojen käsittelijän välillä on sovittava henkilötietojen käsittelystä sopimuksella tai muulla unionin tai kansallisen lainsäädännön mukaisella oikeudellisella asiakirjalla. TSA siten vaatii, että rekisterinpitäjä ja käsittelijä sopivat kirjallisessa

---

[163] Oikeuskirjallisuudessa on esitetty rekisterinpitäjän termin olevan epäonnistunut. Ks. esim. Saarenpää – Riekkinen 2023, s. 220 ja Korpisaari ym. 2022, s. 34 ja 36.
[164] TSA 26 artikla. Ks. Korpisaari ym. 2022, s. 325, jonka mukaan käsittelytarkoitusten ei tarvitse olla täysin samat, vaan riittää, että tarkoitukset ovat läheisesti toisiinsa liittyviin tai toisiaan täydentäviin tarkoituksiin.
[165] Korpisaari ym. 2022, s. 34; Ks. EDPB 4/2019, s. 20 kohdat 86–87.
[166] TSA 12 artikla; EDPB 1/2025, s. 4.
[167] Korpisaari ym. 2022, s. 34–35.
[168] Andersson 2024, s. 161.
[169] Alapuranen ym. 2020, s. 43–44. Yleensä rekisterinpitäjät ovat ulkoistaneet esimerkiksi palkanmaksun.
[170] Voutilainen 2019, s. 46.
[171] Korpisaari ym. 2022, s. 34–35.

muodossa henkilötietojen käsittelystä.[172] Jos käsittelijä kuitenkin tosiasiassa päättää henkilötietojen käsittelystä tai käyttää tietoja omiin tarkoituksiinsa, käsittelijästä tulee rekisterinpitäjä, vaikka tämä henkilötietojen käsittelysopimuksessa käsittelijäksi määriteltäisiin.[173] Jos rekisterinpitäjä tarvitsee useampaa henkilötietojen käsittelijää, on rekisterinpitäjän tehtävänä huolehtia, että ne muodostavat johdonmukaisen kokonaisuuden eivätkä eri käsittelijöiden kanssa tehdyt sopimukset ole keskenään ristiriidassa.[174] TSA 29 artiklan mukaan henkilötietojen käsittelijä taikka sen tai rekisterinpitäjän alaisuudessa toimiva henkilö ei lähtökohtaisesti saa käsitellä henkilötietoja muuten kuin rekisterinpitäjän ohjeen mukaisesti, ellei lainsäädännössä niin vaadita. Myös henkilötietojen käsittelijän tulee pystyä osoittamaan, että se on noudattanut tälle osoitettuja velvoitteita.[175] Siirrettäessä henkilötietoja kolmansiin maihin tai kansainvälisille järjestöille sekä rekisterinpitäjän että henkilötietojen käsittelijän on varmistettava, että TSA:n edellytyksiä noudatetaan.[176] Jos henkilötietojen käsittelijä sijaitsee kolmannessa maassa, tulee rekisterinpitäjän ja käsittelijän myös aina laatia TSA 28 artiklan mukainen henkilötietojen käsittelysopimus.[177]

Vastaanottajalla tarkoitetaan TSA 4(9) artiklassa ”*luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, jolle luovutetaan henkilötietoja, oli kyseessä kolmas osapuoli tai ei*.”[178] Kolmannella osapuolella puolestaan tarkoitetaan 10 kohdan mukaan ”*luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta toimielintä kuin rekisteröityä, rekisterinpitäjää, henkilötietojen käsittelijää ja henkilöä, joilla on oikeus käsitellä henkilötietoja suoraan rekisterinpitäjän tai henkilötietojen käsittelijän välittömän vastuun alaisena*.” Toisin sanoen kolmannella osapuolella tarkoitetaan muita henkilöitä kuin niitä, joilla on oikeus käsitellä henkilötietoja suoraan rekisterinpitäjän tai henkilötietojen käsittelijän välittömän vastuun alaisena. Kolmannet osapuolet eivät ole rekisterinpitäjän palveluksessa eivätkä kuulu sen määräysvaltaan, toisin kuin henkilötietojen käsittelijät.[179] Vastaanottaja voi siten olla myös esimerkiksi toinen rekisterinpitäjä.[180] Tarvittaessa rekisterinpitäjän on tehtävä vastaanottajan kanssa sitova sopimus,

---

[172] Korpisaari ym. 2022, s. 34–35.
[173] Ks. TSA 28 artikla 10 kohta; EDPB 7/2020, s. 14; WP169, s. 14; Ks. lisäksi Korpisaari ym. 2022, s. 76, jossa kuvataan esimerkkinä, että henkilötietojen käsittelijä lähettää rekisteröidyille omaa markkinointipostiaan tai muutoin käsittelee rekisterinpitäjän antamien ohjeiden vastaisesti.
[174] Korpisaari ym. 2022, s. 34–35.
[175] Alapuranen ym. 2020, s. 43–44.
[176] Korpisaari ym. 2022, s. 466–467.
[177] Korpisaari ym. 2022, s. 480.
[178] Tällaisia ei kuitenkaan ole saman artiklan mukaan viranomaiset, jotka mahdollisesti saavat henkilötietoja tietyn tiedustelun puitteissa laillisesti.
[179] C-340/21 (VB), kohta 66.
[180] Ks. WP169, s. 30. Henkilötietoja vastaanottava sivullinen voi olla uusi rekisterinpitäjä edellyttäen, että muut rekisterinpitäjäksi määrittelemisen edellytykset täyttyvät.

jolla varmistetaan, että vastaanotettuja henkilötietoja käsitellään asianmukaisesti.[181] Selvyyden vuoksi todettakoon, että vaikka vastaanottaja voi myös olla rekisterinpitäjä, ei tällainen tietojen luovuttaminen vastaanottajalle tee näistä yhteisrekisterinpitäjiä. Käytettävän terminologian kannalta huomionarvoista on myös, että yksinomaan anonyymiä tietoa käsittelevä vastaanottaja ei ole TSA:n tarkoittamalla tavalla rekisterinpitäjä.

Rekisterinpitäjän on TSA 19 artiklan mukaan ilmoitettava kaikenlaisista henkilötietojen oikaisuista, poistoista tai käsittelyn rajoituksista jokaiselle vastaanottajalle, jolle henkilötietoja on luovutettu, paitsi jos ilmoitusvelvollisuuden toteuttaminen osoittautuu mahdottomaksi tai vaatii kohtuutonta vaivaa. Rekisterinpitäjän on ilmoitettava rekisteröidylle näistä vastaanottajista, jos rekisteröity sitä pyytää. Jos rekisterinpitäjällä on velvollisuus poistaa henkilötiedot, on sen käytettävissä oleva teknologia ja toteuttamiskustannukset huomioon ottaen toteutettava kohtuulliset toimenpiteet ilmoittaakseen muille rekisterinpitäjille rekisteröidyn pyynnöstä.[182] Tämäkään ilmoitusvelvollisuus ei ole ehdoton ja riippuu tilannetekijöistä, sillä ”kohtuulliset toimenpiteet” viittaavat tapauskohtaiseen arviointiin. Tietoja ei kuitenkaan ole lähtökohtaisesti tarpeen poistaa, mikäli käsittely on tarpeen yleisen edun mukaisia arkistointitarkoituksia taikka tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten 89 artiklan 1 kohdan mukaisesti, jos oikeus tietojen poistamiseen estää kyseisen käsittelyn tai vaikeuttaa sitä suuresti.[183] Tätä voidaan pitää poikkeuksena rekisteröidyn oikeuksien toteutumiselle, mikä puolestaan ilmentää henkilötietojen suojan ja henkilötiedon vapaan liikkuvuuden välistä jännitettä.

Rekisterinpitäjällä on TSA 5(2) artiklan mukaan osoitusvelvollisuus. Rekisterinpitäjä vastaa tietosuojasääntelyn noudattamisesta. Rekisterinpitäjän on toteutettava kaikki tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että käsittelyssä noudatetaan TSA:ta.[184] Rekisterinpitäjän on ylläpidettävä vastuillaan olevista käsittelytoimista kirjallista selostetta.

[181] EDPB 1/2025, s. 18–19 kohta 75.
[182] TSA johdanto-osa 66 kappale; Ks. TSA 17 artikla. Ks. Korpisaari ym. 2022, s. 315, jonka mukaan rekisterinpitäjän tulee seurata yleistä teknistä kehitystä ja pitää käyttämänsä teknologia ajan tasalla ymmärtäen teknologiasta aiheutuvat riskit ja mahdollisuudet.
[183] TSA 17(2) artikla.
[184] TSA 24 artikla.

Myös henkilötietojen käsittelijän on pidettävä selostetta kaikista rekisterinpitäjän lukuun suoritettavista henkilötietojen käsittelytoimista.[185] Rekisterinpitäjä voi noudattaa osoitusvelvollisuutensa esimerkiksi dokumentoimalla toimintaan liittyviä toimia, arvioita ja käytänteitä.[186] Dokumentoinnin yksityiskohtaisuus riippuu käsiteltävän asian luonteesta ja käsittelytarkoituksesta.[187]

Rekisterinpitäjä saattaa käsitellä sellaisia henkilötietoja, jotka eivät edellytä rekisteröidyn tunnistamista. TSA 11 artiklan 1 kohdan mukaan *"[j]os henkilötietojen käsittelyn tarkoitus ei edellytä tai ei enää edellytä rekisteröidyn tunnistamista, ei rekisterinpitäjällä ole velvollisuutta säilyttää, hankkia tai käsitellä lisätietoja rekisteröidyn tunnistamista varten, jos tämä olisi tarpeen vai tämän asetuksen noudattamiseksi."* Lisäksi 2 kohdan mukaan *"[j]os tämän artiklan 1 kohdassa tarkoitetuissa tapauksissa rekisterinpitäjä pystyy osoittamaan, ettei se pysty tunnistamaan rekisteröityä, rekisterinpitäjän on ilmoitettava asiasta rekisteröidylle, jos tämä on mahdollista. Tällaisissa tapauksissa 15–20 artiklaa ei sovelleta, paitsi jos rekisteröity näiden artikloiden mukaisia oikeuksia käyttääkseen antaa lisätietoja, joiden avulla hänet voidaan tunnistaa."*[188] Rekisterinpitäjällä on siten velvollisuus osoittaa, ettei se pysty tunnistamaan henkilöä hyötyäkseen 11 artiklan rekisteröidyn oikeuksia koskevista kevennyksistä. Tässä yhteydessä korostuu sopivien pseudonymisointitekniikoiden merkitys.[189] Tämä osoitusvelvollisuus koskee siten käytännössä relatiivisen avaimen hallussapitoa.

3 Pseudonymisointi, anonymisointi ja tunnistettavuus

3.1 Tunnistettavuus ja kohtuullisen todennäköisesti käytettävissä olevat keinot

Monet tietosuojaan liittyvät asiat riippuvat olosuhteista.[190] TSA:ssa viitataan kaikkiin keinoihin, joita rekisterinpitäjä tai muu taho voi kohtuullisen todennäköisesti käyttää luonnollisen henkilön

[185] TSA 30 artikla. Tällaiset velvollisuudet eivät kuitenkaan koske yritystä tai järjestöä, jossa on alle 250 työntekijää, paitsi jos sen suorittama käsittely todennäköisesti aiheuttaa riskin rekisteröidyn oikeuksille ja vapauksille, käsittely ei ole satunnaista tai käsittely kohdistuu erityisiin henkilötietoryhmiin tai rikostuomioita tai rikkomuksia koskeviin henkilötietoihin.
[186] Alapuranen ym. 2020, s. 67–70.
[187] Korpisaari ym. 2022, s. 30.
[188] Hintze 2018, s. 95–96 on todennut, että tällaisesta voidaan ilmoittaa esimerkiksi näkyvällä tai helposti löydettävällä ilmoituksella.
[189] ENISA 2018, s. 17.
[190] Tarhonen 2016, s. 15.

tunnistamiseen.[191] Julkisasiamies Spielmann on kuvannut näitä kohtuullisen todennäköisiä keinoja ”epäsuoraksi pääsyksi” tunnistetietoihin.[192] Tämä muodostaa myös pseudonymisoidun tai anonymisoidun tiedon luonteen arvioinnin lähtökohdan: onko tietoa hallussaan pitävällä taholla kohtuullisen todennäköisiä keinoja henkilön tunnistamiseksi?

Oikeuskirjallisuudessa on katsottu, että pelkästään mahdollisuus henkilön tunnistamisesta voi johtaa tietosuojalainsäädännön soveltamiseen.[193] Tämä kuvastaa TSA:n henkilötiedon määritelmän ”tunnistettavissa oleva” -kohtaa, eikä tunnistamisen tarvitse konkreettisesti edes tapahtua. Kuitenkaan käytännössä ei ole katsottu olevan merkitystä sillä, katsotaanko henkilö tunnistetuksi vai tunnistettavissa olevaksi, sillä tietosuojasääntely soveltuu molempiin tilanteisiin.[194] Jälkimmäisen osalta arviointi ei kuitenkaan ole suoraviivaista, vaan vaaditaan enemmän tulkintaa siitä, onko luonnollinen henkilö tosiasiallisesti mahdollista tunnistaa. Näin ollen ”tunnistettavissa oleva” on pseudonymisoitujen ja anonymisoitujen tietojen aseman arvioinnin ytimessä.

Luonnollinen henkilö voidaan tietosuojatyöryhmän mukaan katsoa tunnistetuksi, jos hän erottuu joukosta sekä silloin, jos hänet on mahdollista tunnistaa, vaikkei tunnistamista olisi vielä tapahtunut.[195] Tietosuojatyöryhmä on myös katsonut, että henkilön tunnistaminen riippuu tilanteesta ja kontekstista.[196] Myös rekisterinpitäjän tarkoitus tietojen käsittelylle on olennainen tekijä arvioitaessa sitä, onko henkilön tunnistamiseksi kohtuullisesti toteutettavissa olevia keinoja.[197] Esimerkiksi hyvin yleisen sukunimen perusteella ei voida erottaa tiettyä henkilöä koko valtion väestöstä, mutta sillä voidaan tunnistaa tietty oppilas luokan kaikkien oppilaiden joukosta.[198]

Tunnistettavuuden määrittämiseksi on otettava huomioon kaikki keinot, joita rekisterinpitäjä tai muu taho voi kohtuullisen todennäköisesti käyttää luonnollisen henkilön tunnistamiseen suoraan tai välillisesti. Tällöin tulisi ottaa huomioon kaikki objektiiviset tekijät, joita ovat esimerkiksi tunnistamisesta aiheutuvat kulut, tunnistamiseen tarvittava aika, käsittelyajankohtana käytettävissä oleva teknologia ja tekninen kehitys.[199] Näillä arvioidaan sitä, onko toimijalla kohtuullisen

---

[191] TSA johdanto-osa 26 kappale. Tunnistamisen kohtuullisuus on nostettu esille myös COM (92) 422 final, s. 10 siten, että erityistapauksissa tilastomuotoon koottuja henkilötietoja ei voida pitää henkilötietoina, jos tietojen kohteena olevia henkilöitä ei voida enää kohtuudella tunnistaa.
[192] Julkisasiamies Spielmannin ratkaisuehdotus asiassa C-413/23 P (SRB), alaviite 25.
[193] Bolognini – Bistolfi 2017, s. 174.
[194] Hintze 2018, s. 89.
[195] WP136, s. 12.
[196] Ks. WP136, s. 12–13.
[197] WP136, s. 16.
[198] WP136, s. 12–13; Korpisaari ym. 2022, s. 603.
[199] TSA johdanto-osa 26 kappale; Jos tietojen ajatellaan koskevan esimerkiksi julkisuuden henkilöitä, on kohtuullisen todennäköisesti käytettävissä olevien keinojen arviointi katsottava korkeammaksi. Ks. tarkemmin ICO 2022a, s. 11.

todennäköisiä keinoja saada relatiivinen avain haltuunsa. Jos tietoja on tarkoitus säilyttää pidemmän aikaa, rekisterinpitäjän on otettava huomioon tunnistamisen mahdollisuus tulevaisuudessa ja voitava mukauttaa toimintaa kehityksen mukaisesti.[200]

Kaikilla käytössä olevilla tunnisteilla ei yksinään ole mahdollista tunnistaa henkilöä. Henkilö saattaa siitä huolimatta olla tunnistettavissa, jos tieto yhdistettynä muihin tietoihin mahdollistaa henkilön erottamisen muista.[201] Tietosuojatyöryhmän mukaan tällaisten muiden tietojen ei välttämättä tarvitse olla rekisterinpitäjän hallussa, vaan tietoja voi olla saatavilla myös muista tietolähteistä.[202] Tällaisena muuna tietona voidaan pitää esimerkiksi henkilön ammattia, vaikkei siitä yksinään pystyisi henkilöä tunnistamaan.[203] Myös kansainvälisten henkilötunnusten avulla on helppoa yhdistellä yksilöä koskevia erilaisia tietoja toisiinsa.[204] TSA ei aseta rajoja anonyymien tietojen käsittelylle. Sinänsä anonyymeinä pidettävien tietojen yhdisteleminen voi kuitenkin mahdollistaa sen, että luonnollinen henkilö lopulta olisikin tunnistettavissa, mikä johtaa sääntelyn soveltamisalan piiriin. Tämä osoittaa, että tietojen yhdistelemisestä aiheutuvaa tunnistamista erityisesti teknologian mahdollistamana on pidettävä yhtenä keskeisimmistä tietosuojariskeistä.

Tunnistettavuutta tulee arvioida ottamalla huomioon kaikki tunnistamiseen vaikuttavat tekijät, eikä pelkkä teoreettinen tunnistamisen mahdollisuus riitä.[205] Mikäli mikä tahansa hypoteettinen tunnistamismahdollisuus riittäisi, henkilötiedon käsite laajentuisi rajattomasti.[206] Jos rekisterinpitäjän tarkoituksena ei ole tunnistaa rekisteröityä hallussaan olevista tiedoista, ja tunnistamisen estämiseksi on toteutettu asianmukaiset tekniset ja organisatoriset toimenpiteet, ei tunnistaminen ole välttämättä mahdollista.[207]

Henkilötietoja ovat lähtökohtaisesti myös staattiset IP-osoitteet, sillä ne koskevat tunnistettavissa olevia henkilöitä.[208] Näin ei kuitenkaan ole esimerkiksi yleisissä tiloissa, sillä internetpalveluntarjoaja ei kykene täysin varmasti erottamaan, mahdollistaako kyseinen IP-osoite tunnistamisen vai ei. Tietosuojatyöryhmän mukaan tällaisissa tilanteissa palveluntarjoajan on varmuuden

---

[200] WP136, s. 15.
[201] WP136, s. 15. Erityisesti nykyisessä toimintaympäristössä, esimerkiksi sosiaalisessa mediassa, voi esiintyä käyttäjänimiä tai muita tietoja, joiden perusteella henkilö ei suoraan ole tunnistettavissa.
[202] WP136, s. 13; WP216, s. 24; Ks. myös Korpisaari ym. 2022, s. 604.
[203] Ks. esim. EDPB 1/2025, s. 23 kohta 101.
[204] WP136, s. 15.
[205] WP136, s. 15. Ks. myös ICO 2022a, s. 12.
[206] Kuitenkin EUT on katsonut, että hypoteettisessa tulevaisuuden tilanteessa on kohtuullisen todennäköiset keinot, jos välikäden avulla pystytään saamaan tarvittava relatiivinen avain. Ks. C-582/14 (Breyer), kohdat 47–48.
[207] WP136, s. 16.
[208] WP136, s. 16.

vuoksi käsiteltävä kaikkia IP-osoitteita henkilötietoina.[209] Kuitenkin suhteellisesta näkökulmasta tarkastellen: jos samaa tietokonetta ja siten samaa IP-osoitetta käyttää käytännössä rajoittamaton joukko, ei erottaminen ole kohtuullisin keinoin mahdollista ainakaan internetpalveluntarjoajan näkökulmasta.[210] IP-osoitteet eivät siten aina ole henkilötietoja esimerkiksi yleisissä paikoissa, joissa laitteita on usean mahdollista käyttää.[211] Tunnistamisen arvioinnissa teknologisoituvassa toimintaympäristössä korostuukin siten sekä teknisen että oikeudellisen asiantuntemuksen tarve.

Tietosuojalainsäädäntöä on tulkittu siten, ettei henkilötietoja ole mitenkään kategorisoitu,[212] lukuun ottamatta erityisiä henkilötietoryhmiä. Pseudonymisoitujen tietojen käsittely ei siten eroa muusta henkilötietojen käsittelystä. Henkilötiedon käsitteen laajuus osoittaa, että tunnistettavuuden ja kohtuullisten keinojen arviointi vaatii kokonaisharkintaa ja tapauskohtaista oikeudellista arviointia.[213] Koska henkilötiedon käsite ei ole rajaton, tunnistettavuutta ei tule arvioida puhtaasti hypoteettiselta pohjalta.[214] Tunnistettavuuden arviointi ”kohtuullisin keinoin” jättää tilaa vaihteleville tulkinnoille, mikä korostaa soft law -tasoisten joustavien ohjeistusten merkitystä.

Tunnistettavuuden mahdollisuutta laajentaa erityisesti se, ettei tunnistettavuuden mahdollistavien lisätietojen tarvitse olla pelkästään rekisterinpitäjän tai ylipäänsä vain yhden tahon hallussa.[215] Lisätietoja voi olla saatavilla myös muualla, eri muodoissa ja eri toimijoilla. Juuri tämä kuvastaa *relatiivisen avaimen* käsitteen tarpeellisuutta. Relatiivinen avain on suhteellinen myös aineiston kokoon nähden ja merkityksellistä on, mistä avain koostuu ja kenen hallussa se on. Relatiivinen avain voi olla saatavissa laajasti erilaisista lähteistä, eikä sen saaminen edellytä välttämättä aktiivisia toimia. Relatiivinen avain voi itsessään olla henkilötietoa samalla, kun se on toiselle anonyymiä tietoa.[216] Se myös kuvastaa suhteellisen henkilötiedon käsitteen ajattelutapaa siten, että yhdellä avain voi avata tunnistettavuuden lukon, kun toisella se on vain tieto muiden

---

[209] WP136 s. 16–17.
[210] Erottaminen taas voisi olla mahdollista ainakin jonkun tahon näkökulmasta, jos esimerkiksi tietokoneelle täytyy kirjautua tai tietokoneen käytöstä maksetaan digitaalisen jalanjäljen jättävällä pankkikortilla.
[211] Ks. kuitenkin WP136, s. 17, jonka mukaan internetin palveluntarjoajan on varmuuden vuoksi käsiteltävä kaikkia IP-osoitteita henkilötietoina, sillä se ei pysty täysin varmasti erottamaan mahdollistaako IP-osoite tunnistamisen vai ei.
[212] Hintze 2018, s. 89. Ks. myös ICO 2022b, s. 4, jonka mukaan TSA tekee selväksi, että pseudonymisoitu henkilötieto säilyy henkilötietona.
[213] Yhdistyneen kuningaskunnan tietosuojaviranomainen (ICO) on ottanut käyttöön niin sanotun motivoituneen tunkeutujan testin, jolloin tunnistamisriskin arvioinnissa otetaan huomioon tunnistamisen mahdollisuus, jos olisi motivaatiota yrittää. Arviointitaso asettuu käytännössä suhteellisen kokemattoman ja merkittävää asiantuntemusta omaavan henkilön väliin. Ks. lisää ICO 2022a, s. 15–21.
[214] Ks. esim. WP136, s. 4 ja C-413/23 P (SRB), kohdat 85–86.
[215] Ks. C-582/14 (Breyer), kohta 43.
[216] Ks. EDPB 1/2025, s. 9 kohta 20.

joukossa. Relatiivisen avaimen käsite on siten omiaan kuvaamaan niin lisätiedon kuin ylipäänsä tunnistettavuuden dynaamista luonnetta, ja se pitää sisällään kaikki mahdolliset keinot, joiden avulla tietty luonnollinen henkilö on kohtuudella mahdollista tunnistaa.

3.2 Pseudonymisointi ja anonymisointi henkilötietojen suojakeinoina

EU:n sääntelyssä henkilötietojen pseudonymisointi määriteltiin ensimmäistä kertaa TSA:ssa.[217] Siitä huolimatta pseudonymisointia on käytetty jo aiemmin, mikä ilmenee niin EUT:n ratkaisuista, tietosuojatyöryhmien lausunnoista kuin useista muista lähteistä.[218] Pseudonymisoinnin käyttöönotolla pyrittiin alkujaan tuomaan joustavuutta tietosuojavelvoitteiden keventämiseksi.[219] Pseudonymisointi määritellään TSA 4(5) artiklassa prosessina seuraavasti:

> *[Pseudonymisoimisella tarkoitetaan] henkilötietojen käsittelemistä siten, että henkilötietoja ei voida enää yhdistää tiettyyn rekisteröityyn käyttämättä lisätietoja, edellyttäen että tällaiset lisätiedot säilytetään erillään ja niihin sovelletaan teknisiä ja organisatorisia toimenpiteitä, joilla varmistetaan, ettei henkilötietojen yhdistämistä tunnistettuun tai tunnistettavissa olevaan luonnollisen henkilöön tapahdu.*

Pseudonymisoinnin määritelmän mukaan tieto tulee olla yhdistettävissä ”tiettyyn” luonnolliseen henkilöön. Tunnistettavuutta tulee arvioida sillä tarkkuudella, onko tieto mahdollista yhdistää vain yhteen henkilöön.[220] Lisätiedot säilytetään erillään ja niihin sovelletaan teknisiä ja organisatorisia toimenpiteitä, joilla varmistetaan, ettei henkilötietoja pysty yhdistämään tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön.[221] Tietosuojaneuvosto on kutsunut pseudonymisointiprosessin toteuttavaa tahoa pseudonymisoivaksi rekisterinpitäjäksi.[222] Pseudonymisoiva rekisterinpitäjällä relatiivinen avain on se alkuperäinen lisätieto, joka on syntynyt

---

[217] Tarhonen 2016, s. 10.
[218] Ks. esim. Hintze 2018, s. 89, jonka mukaan Saksan liittovaltion tietosuojalaissa (Bundesdatenschutzgesetz) on jo pitkään kannustettu pseudonymisointiin tietojen minimoimiseksi.
[219] Julkisasiamies Spielmannin ratkaisuehdotus asiassa C-413/23 P (SRB), alaviite 23, jonka mukaan tämä pyrkimys ei kuitenkaan näy TSA johdanto-osan 26 kappaleessa, jossa pseudonymisointia ja anonymisointia avataan.
[220] Ks. Tarhonen 2016, s. 14, jonka mukaan tällainen arviointitilanne voi olla esimerkiksi osoitteiden kohdalla, joissa asuu enemmän kuin yksi henkilö.
[221] Esimerkiksi TSV 21.4.2021 ratkaisussa on katsottu, että opintosuoritusten arvosanat voi julkistaa opiskelijanumeroon yhdistettynä yliopiston sisäisessä intranetissä ilman rekisteröidyn suostumusta. Rekisterinpitäjän on tällöin huolehdittava teknisin ja organisatorisin toimenpitein, että kolmansilla osapuolilla ei ole pääsyä listoihin tai muuhun opiskelijan nimen ja opiskelijanumeron yhdistävään lisätietoon. Ilmoittaja oli kertonut, että muiden opiskelijoiden on ollut helppo saada haltuunsa toisten opiskelijanumeroita esimerkiksi ryhmätöiden kautta.
[222] EDPB 1/2025, s. 9 kohta 18.

prosessin yhteydessä. Relatiivinen avain voi olla esimerkiksi pseudonymisoinnin johdosta yksittäinen salanimi tai taulukko. Tietosuojatyöryhmä on katsonut, että jos lisätiedot ovat kadonneet eivätkä ole kohtuullisin keinoin löydettävissä, tiedot eivät enää viittaa tunnistettavissa oleviin henkilöihin.[223]

Pseudonymisoinnilla vähennetään rekisteröityihin kohdistuvia riskejä.[224] Se toimii riskienhallintakeinona sekä teknisenä ja organisatorisena toimenpiteenä.[225] Henkilötietojen pseudonymisointi toteuttaa muun muassa tietojen minimoinnin sekä sisäänrakennetun ja oletusarvoisen tietosuojan periaatteita, ja sen avulla varmistetaan asianmukainen ja riskiin suhteutettu tietoturvan taso.[226] Pseudonymisoinnilla pyritään siis turvaamaan henkilötietojen suojaa. Pseudonymisoinnilla ei ole haluttu poissulkea muita tietosuojatoimenpiteitä kuten tietojen minimointia.[227] Vaikka pseudonymisointi on tehokas ja merkityksellinen toimenpide, on sitä kuitenkin tietosuojaneuvoston mukaan täydennettävä muilla toimenpiteillä.[228]

Pseudonymisoitua tietoa on vakiintuneesti pidetty henkilötietona.[229] Tämä tulkinta perustuu siihen, että tunnistettavuus ei poistu, vaan tunnistaminen edellyttää lisätietoja eli relatiivista avainta. On myös argumentoitu, että pseudonymisoidut tiedot sijoittuvat henkilötietojen ja anonyymien tietojen välimaastoon niin sanotulle harmaalle alueelle.[230] Tietosuojatyöryhmän mukaan pseudonymisoidut tiedot ovat epäsuorasti tunnistettavissa olevia henkilötietoja, jotka voivat olla jäljitettävissä.[231] Peitenimen eli pseudonyymin käyttäminen tarkoittaa, että se voidaan jäljittää henkilöön, mutta vain ennalta määritellyissä oloissa. Kuitenkin tietosuojatyöryhmän mukaan tunnistamisen riski on yleensä pieni epäsuorasti tunnistettavissa olevan tiedon kohdalla, jolloin tietosuojasäännöksiä on perusteltua soveltaa joustavammin kuin suoraan tunnistettavissa olevia henkilöitä koskevia tietoja käsiteltäessä.[232] Pseudonymisointi on muun muassa tutkimus-, tilastointi- tai arkistointitarkoituksissa hyvä apuväline henkilötietojen käsittelyyn liittyvien riskien pienentämiseksi, muttei se kuitenkaan vapauta TSA:n velvoitteista.[233] Tietosuojatyöryhmä

---

[223] WP136, s. 19.
[224] TSA johdanto-osa 28 kappale. Ks. Saarenpää – Riekkinen 2023, s. 228, jonka mukaan pseudonymisointia voidaan pitää merkittävänä osana tietoturvallisuuden suunnittelua ja riskienhallintaa.
[225] KS. TSA 25 artikla sisäänrakennetusta ja oletusarvoisesta tietosuojasta.
[226] EDPB 1/2025, s. 3.
[227] TSA johdanto-osa 28 kappale.
[228] EDPB 1/2025, s. 8.
[229] Ks. esim. ENISA 2018, s. 13–14; Voutilainen 2019, s. 41–42; Korpisaari ym. 2022, s. 717–718; Tarhonen 2016, s. 10 ja Andersson 2024, s. 321.
[230] Tarhonen 2016, s. 10; El Khoury 2017, s. 192.
[231] WP136, s. 18.
[232] WP136, s. 18.
[233] Korpisaari ym. 2022, s. 717–718.

on kuvannut ”erityiseksi salakuopaksi” sitä, että pseudonymisoituja tietoja saatetaan pitää anonyymeinä tietoina.[234] Tietosuojatyöryhmä on siten tunnistanut jo ennen TSA:n voimaantuloa pseudonymisoinnin ja anonymisoinnin välisen rajanvedon ongelman. Siitä huolimatta, että pseudonymisointi on nykyään osa tietosuojasääntelyä, ei rajanveto ole vieläkään selkeä. Tietosuojatyöryhmän mukaan pseudonymisoituja tietoja ei voida rinnastaa anonyymeihin tietoihin, koska yksilö on edelleen mahdollista erottaa joukosta. Tätä on tietosuojatyöryhmä pitänyt merkityksellisenä erityisesti tutkimustoiminnassa.[235]

Anonymisointia ei TSA:ssa nimenomaisesti mainita, mutta johdanto-osan 26 kappaleessa sitä kuvataan tunnistettavuuden poistamisena siten, ettei rekisteröityä voi enää tunnistaa. Anonymisoinnilla tunnistettavuus poistetaan peruuttamattomasti niin, että tunnistettavuus on peruuttamatonta myös yhdistettäessä tietoja toisiin tietoihin – olivat ne julkisia tai ei.[236] Tehokkaasta anonymisoinnista seuraa, ettei tietosuojasääntelyä sovelleta enää jatkokäsittelyyn.[237] Anonymisointiprosessissa tulee poistaa riittävästi elementtejä niin, ettei yksikään taho pysty yhdistämään tietoa luonnolliseen henkilöön.[238] Tämän voi toteuttaa esimerkiksi karkeistamalla tiedot yleiselle tasolle tai muuttamalla ne sellaiseen muotoon, ettei yksittäistä henkilöä koskevat tiedot ole enää tunnistettavassa muodossa.[239] Anonymisointi on onnistunut, kun tunnistaminen on estynyt peruuttamattomasti siten, ettei yksikään toimija voi enää palauttaa tietoja takaisin tunnistettavaksi eli saada relatiivista avainta.

Mikään anonymisointitekniikka ei ole täydellinen.[240] Tietosuojatyöryhmän mukaan anonymisoinnin luonteeseen kuuluu riskin olemassaolo.[241] Rekisterinpitäjän tulee siten säännöllisesti uudelleenarvioida jäännösriskiä.[242] Tietosuojatyöryhmän mukaan jäännösriski on liian korkea silloin, jos rekisteröidyt voivat joutua kärsimään huomattavista tai peruuttamattomista seurauksista, joita he eivät välttämättä pysty torjumaan.[243] Anonymisoinnin ja pseudonymisoinnin tehokkuutta tuleekin arvioida riskiperusteisesta lähestymistavasta. Jos rekisterinpitäjä tai muu taho pystyy

---

[234] WP216, s. 11; Ks. myös ICO 2022b, s. 4–5 ja ENISA 2018, s. 13; Ks. peitenimillä suojaamisesta WP216, s. 20 ja EDPB 1/2025.
[235] WP216, s. 11.
[236] WP216, s. 3. Ks. myös ICO 2012, s. 18.
[237] Saarenpää – Riekkinen 2023, s. 219, jonka mukaan samaa seurausta ei ole pelkällä tietojen pseudonymisoinnilla.
[238] WP216, s. 6.
[239] Tietosuojavaltuutetun toimisto: Pseudonymisoidut ja anonymisoidut tiedot.
[240] WP216, s. 12.
[241] WP216, s. 3.
[242] WP216, s. 4.
[243] WP248, s. 22.

peruuttamaan anonymisoinnin, on anonymisointi epäonnistunut ja tietoja on käsiteltävä henkilötietoina.[244] Epäonnistunut anonymisointi voi vaikuttaa myöhemmin haitallisesti ja jopa peruuttamattomasti rekisteröityihin.[245] On etenkin huomioitava erityisten henkilötietoryhmien kohdalla, että henkilö voi olla välillisesti tunnistettavissa yksityiskohtaisesta tiedosta, kuten harvinaisesta sairaudesta. Anonymisointia onkin pidetty ongelmallisena esimerkiksi potilasturvallisuuden kannalta.[246]

Samalla tavoin myös pseudonymisointi on epäonnistunut, jos jollakin taholla on pääsy relatiiviseen avaimeen.[247] Julkisasiamies Sánchez-Bordona on todennut, että *”missään tilanteessa ei voida todeta ehdottoman varmasti, ettei ole olemassa sivullista, jonka hallussa on lisätietoja, jotka voidaan yhdistää kyseisiin tietoihin ja joiden avulla voidaan näin paljastaa tietyn henkilön henkilöllisyys.”*[248] Toimenpiteiden mahdollisesta epäonnistumisesta ja jäännösriskistä johtuen rekisterinpitäjän tulee varautua, että anonymisointi ja pseudonymisointi voivat teknisen kehityksen myötä heikentyä, ja relatiivisia avaimia voi uusissa muodoissa syntyä ajan kuluessa.

Kun arvioidaan henkilötiedon ja anonyymin tiedon rajanvetoa, nousee esiin myös kysymys, voiko pseudonymisoinnin avulla anonymisoida tietoa. Pseudonymisointia ei ole kuitenkaan tarkoitettu anonymisointitekniikaksi.[249] Rekisterinpitäjän on vaikea määritellä, milloin tieto on anonymisoitu asianmukaisesti ja siksi on myös vaikeaa arvioida, onko anonymisointi pseudonymisoinnin tuloksena mahdollista.[250] Pseudonymisointi kuitenkin estää vain välittömän tunnistamisen, minkä vuoksi se ei tee tiedosta anonyymiä.[251]

Pseudonymisoinnilla ja anonymisoinnilla on olennainen asema myös osana muuta sääntelyä. Eurooppalaista terveystietoaluetta koskevan asetuksen ((EU) 2025/327, EHDS)[252] johdanto-osan

---

[244] Ks. WP216, s. 6 ja Hintze 2018, s. 90, joissa käsitellään AOL (America on Line) -tapausta. AOL julkaisi vuonna 2006 tietoja 650 000 käyttäjästä, joiden tunnistettavuus oli peitetty numeerisilla tunnisteilla. Tästä huolimatta murto-osa henkilöistä oli mahdollista tunnistaa. Tapausta on laajalti pidetty Hintzen sanoin ”yksityisyyden suojan katastrofina”, vaikka prosessin epäonnistumisprosentti oli vain 0,001. Tämä selvästi korostaa, että yksityisyyteen on suhtauduttu vakavasti.
[245] WP216, s. 9.
[246] Saarenpää – Riekkinen 2023, s. 60.
[247] Tällainen tilanne voi olla esimerkiksi, kun henkilötunnuksen loppuosa peitetään, mutta syntymäaika jää vahvaksi epäsuoraksi tunnisteeksi. Ks. Tietoarkiston verkkosivut.
[248] Julkisasiamies Sánchez-Bordonan ratkaisuehdotus asiassa C-582/14 (Breyer), kohta 65.
[249] WP216, s. 3; Ks. kuitenkin ENISA 2018, s. 14, jonka mukaan anonymisointitekniikoita voidaan hyödyntää tehokkaan pseudonymisoinnin saavuttamisessa.
[250] Tarhonen 2016, s. 18.
[251] Bäck-Keränen 2017, s. 7.
[252] Euroopan parlamentin ja neuvoston asetus (EU) 2025/327, annettu 11 päivänä helmikuuta 2025, eurooppalaisesta terveystietoalueesta sekä direktiivin 2011/24/EU ja asetuksen (EU) 2024/2847 muuttamisesta.

53 kappaleen mukaan ”*[s]ähköisten terveystietojen toissijainen käyttö perustuu pseudonymisoituihin tai anonymisoituihin tietoihin, jotta rekisteröityjen tunnistaminen estettäisiin*.” Eurooppalaisella terveystietoalueella pyritään muun muassa pseudonymisoitujen ja anonymisoitujen terveystietojen helpompaan saatavuuteen tutkimusta ja innovointia varten, kuitenkin asettaen tiukat ehdot tietojen käsittelylle ja antaen yksityishenkilöille mahdollisuuden kieltää tietojensa toisiokäytön.[253] Tarkemmalla sääntelyllä pyritään siten mahdollistamaan ensinnäkin korkeatasoinen henkilötietojen suoja, erityisesti näiden arkaluonteisina pidettävien terveystietojen osalta. Lisäksi pyritään turvaamaan tietojen hyödynnettävyys tutkimus- ja innovaatiotoiminnassa.[254] Tämä osoittaa, että henkilötietojen suojan ja henkilötietojen vapaan liikkuvuuden tasapainoon pyritään myös muissa EU:n säädöksissä, eikä pelkästään ”yleislakina” pidettävässä TSA:ssa.[255]

Pseudonymisoinnilla ja anonymisoinnilla on siten merkittävä rooli tutkimustoiminnan kannalta. TSA:n 89(1) artiklan mukaan yleisen edun mukaisia arkistointitarkoituksia taikka tieteellisiä ja historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten tapahtuvaan käsittelyyn sovelletaan rekisteröidyn oikeuksia ja vapauksia koskevia asianmukaisia suojatoimia. Esimerkiksi pseudonymisoinnilla ja muilla suojatoimilla on varmistettava, että on toteutettu tekniset ja organisatoriset toimenpiteet, joilla taataan etenkin tietojen minimoinnin periaatteen noudattaminen.[256]

---

[253] Ks. Komission verkkosivut: Terveystietojen uudelleenkäyttö; Ks. esim. EDHS johdanto-osa 72 kappale, jonka mukaan on muun muassa käytettävä uusimpia pseudonymisointi- ja anonymisointitekniikoita ja -standardeja sekä varmistettava mahdollisimman hyvin, ettei uudelleentunnistusta ole mahdollista tehdä tai yrittää. Ks. myös laki sosiaali- ja terveystietojen toissijaisesta käytöstä (552/2019, toisiolaki)

[254] Terveystietojen toisiokäytöllä tutkimus- ja innovaatiotoiminnassa voidaan katsoa olevan niin yksityiset kuin yhteiskunnalliset intressit. sillä esimerkiksi tutkimustulosten myötä luonnollinen henkilö itse saattaa saada parempaa hoitoa, kun samalla saadaan tietoa yleisesti kansanterveydestä.

[255] Ks. TSA:sta yleislakina ja siihen kohdistuvasta kritiikistä Purtova 2018 ja Purtova 2025 ja luku 5.4.

[256] TSA 89(1) artikla.

Pseudonymisoinnilla ja anonymisoinnilla on merkitystä myös esimerkiksi datasäädöksessä ((EU) 2020/1828)[257], jossa anonymisointi- ja pseudonymisointivelvoitteet kohdistuvat tyypillisesti luovutettavaan tietokopioon.[258] Myös digimarkkinasäädös ((EU) 2022/1925)[259] velvoittaa hakukoneiden portinvartijat anonymisoimaan henkilötiedot ennen niiden jakamista.[260] Digimarkkinasäädöksessä korostetaan, että anonymisointi tulisi toteuttaa henkilötietojen suojaamiseksi ilman tiedon laadun tai käyttökelpoisuuden merkittävää heikentymistä.[261] On kuitenkin huomioitava, että vaikka eri säädöksissä käytetään samaa terminologiaa, niiden merkityssisältö ja tavoiteltu henkilötietojen suojan taso ei automaattisesti ole yhtenevä. Arviointi tietosuojaa turvaavien toimenpiteiden merkityksestä ja tehokkuudesta tulisi siten tehdä TSA:n asettamien vähimmäisedellytysten pohjalta siten, ettei tietosuojan tasoa ainakaan heikennetä.

Henkilötietojen käsittelyssä on hyödynnettävä ensisijaisesti anonymisointia, jos teknisesti ja tietojenkäsittelyn tarkoitus huomioiden se on mahdollista. Pseudonymisointia hyödynnetään toissijaisesti, mikäli tunnistettavuuden poistaminen kokonaan ei ole tarkoituksenmukaista.[262] Jatkokäsittelyn yhteydessä rekisterinpitäjän on säännöllisesti arvioitava, ovatko henkilötiedot yhä asianmukaisia, oleellisia ja tarpeellisia, vai onko tiedot joko poistettava tai anonymisoitava.[263] Anonymisoinnin lopputuloksen tulee olla yhtä pysyvää kuin tietojen poistaminen.[264] Anonymisoidun aineiston hyödynnettävyys heikkenee kuitenkin nopeasti, kun tietoa on jouduttu liikaa karkeistamaan.[265] Vaikeus anonymisoinnin tehokkuudessa heijastuu varovaisuutena hyödyntää aineistoja

[257] Euroopan parlamentin ja neuvoston asetus (EU) 2023/2854, annettu 13 päivänä joulukuuta 2023, datan oikeudenmukaista saatavuutta ja käyttöä koskevista yhdenmukaisista säännöistä ja asetuksen (EU) 2017/2394 ja direktiivin (EU) 2020/1828 muuttamisesta (EU:n datasäädös).
[258] Ks. datasäädös 18 artikla.
[259] Euroopan parlamentin ja neuvoston asetus (EU) 2022/1925, annettu 14 päivänä syyskuuta 2022, kilpailullisista ja oikeudenmukaisista markkinoista digitaalialalla ja direktiivien (EU) 2019/1937 ja (EU) 2020/1828 muuttamisesta (EU:n digimarkkinasäädös).
[260] Ks. digimarkkinasäädös 6(11) artikla.
[261] Digimarkkinasäädös johdanto-osa 61 kappale. Ks. kuitenkin anonymisoitujen tietojen hyödynnettävyyden heikentymisestä esim. Bäck – Keränen 2017, s. 24.
[262]Anonymisoinnin ensisijaisuus suhteessa pseudonymisointiin ilmenee esim. EHDS 66 artiklasta, jonka mukaan terveystiedot annetaan lähtökohtaisesti anonymisoidussa muodossa, ja vasta toissijaisesti pseudonymisoituina. Sama etusija korostuu myös esim. datasäädöksen 18(4) artiklassa.
[263] EDPB 4/2019, s. 22 kohdat 73 ja 75. Tämä kuvastaa suoraan TSA:n tietosuojaperiaatteita.
[264] WP216, s. 6.
[265] Bäck – Keränen 2017, s. 24; Esimerkiksi räätälöityjen kampanjoiden rakentamiseksi pseudonymisointia pidetään markkinointialalla parempana vaihtoehtona kuin anonymisointia. Ks. tarkemmin Rowntree 2016.

oman organisaation ulkopuolella.[266] Pseudonymisoinnin tavoitteena on estää rekisteröityjen tunnistaminen pelkkien pseudonymisoitujen tietojen avulla.[267] Jos siis tunnistaminen on vielä tarpeen, henkilötiedot on pseudonymisoitava, jotta pienennetään rekisteröityihin kohdistuvia riskejä.[268]

Tietosuojatyöryhmä on anonymisointitekniikoita koskevassa lausunnossaan kuvannut peitenimellä suojaamisen menetelmää, jonka tarkoituksena on vähentää tietojen yhdistämisen mahdollisuutta.[269] Anonymisointia koskeva lausunto koskee siten osittain myös pseudonymisointia. Tämä osoittaa, että vaikka toimenpiteet ovat erillisiä, ovat ne silti hyvin lähellä toisiaan. Keskeinen ero pseudonymisoinnin ja anonymisoinnin välillä on, että pseudonymisointi säilyttää yhteyden luonnolliseen henkilöön vähintään yhden toimijan näkökulmasta, kun taas anonymisointi katkaisee sen kokonaan. Mitä tehokkaammin pseudonymisointi estää tunnistamisen, sitä lähemmäs anonymisointia se käytännössä sijoittuu. Mikäli relatiivinen avain on jollakin taholla olemassa, ei pseudonymisoitu henkilötieto voi olla anonyymiä kaikille.[270] Teoriassa pseudonymisoitu aineisto voisi kuitenkin muuttua anonyymiksi edellyttäen, että tunnistamisen mahdollistavat lisätiedot poistetaan ja tehdään tunnistamisesta peruuttamatonta. Jos siis pseudonymisoidusta tiedosta haluttaisiin tehdä anonyymiä, tulisi pseudonymisoitu aineisto vielä myöhemmin anonymisoida, Toimenpiteet siten täydentävät toisiaan: ensin henkilötietojen keräämistä ylipäänsä minimoidaan, henkilötietojen turvaamiseksi ja hyödynnettävyydeksi ne pseudonymisoidaan ja lopulta ne anonymisoidaan, kun tunnistamiselle ei ole enää tarvetta. Pseudonymisoitu henkilötieto voi siten lakata olemasta henkilötietoa erillisen anonymisointiprosessin jälkeen, jos anonyymiyden edellytykset muutoin täyttyvät.[271]

---

[266] Bäck – Keränen 2017, s. 25.
[267] C-413/23 P (SRB), kohta 74. EUT on viitannut EU:n toimielinten tietosuoja-asetuksen ((EU) 2018/1725) 3(6) artiklaan, jonka mukaan teknisillä ja organisatorisilla toimenpiteillä varmistetaan, ettei henkilötietojen yhdistämistä tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön tapahdu.
[268] EDPB 4/2019, s. 22 kohta 75. Tietosuojaneuvosto on todennut pseudonymisoinnilla vähennettävän rekisteröidyn oikeuksiin kohdistuvia riskejä. Sopivampaa olisi kuitenkin puhua henkilötietojen suojaan kohdistuvista riskeistä. Ks. tutkielman luku 5.1, jossa käsitellään pseudonymisoinnin vaikutusta rekisteröidyn oikeuksiin.
[269] WP216, s. 3. Suomenkielisessä käännösversiossa termiä ”pseudonymisointi” ei ole käytetty, mutta englanninkielisessä versiossa on. Ks. myös EDPB 28/2024, s. 30, jonka mukaan peitenimillä suojaaminen voi olla erityisen tarkoituksenmukaista esimerkiksi tekoälymallien kouluttamisessa.
[270] Ks. C-413/23 P (SRB), kohta 73.
[271] EDPB 1/2025, s. 10 kohta 22.

4 Pseudonymisoidun tiedon tunnistettavuudesta ja toimijoiden rooleista

4.1 Tietosuojatyöryhmän tulkintalinjaa

Tietosuojatyöryhmä on käyttänyt esimerkkiä lääketieteellisiä tutkimuksia varten käsitellyistä henkilötiedoista, jolloin potilaiden tietoja siirretään yrityksille lääketieteellisiä tutkimuksia varten. Potilaista ei käytetty nimiä, vaan tapauksiin on liitetty satunnainen sarjanumero. Potilaiden henkilöllisyys oli tiedossa kuitenkin vain salassapitovelvollisuuden omaavalla lääkärillä. Tietoihin ei sisältynyt lisäyksityiskohtia, joita yhdistämällä olisi pystynyt luomaan relatiivisen avaimen potilaiden tunnistamiseksi. Lisäksi oli toteutettu kaikki muut oikeudelliset, tekniset ja organisatoriset toimenpiteet tunnistamisen estämiseksi. Tällaisessa tilanteessa voi tietosuojatyöryhmän mukaan katsoa, että lääkeyritysten suorittama tietojenkäsittely ei sisältänyt kohtuullisesti toteutettavissa olevia keinoja, joiden avulla potilaat olisi voitu tunnistaa.[272] Esimerkissä korostuu henkilötietokäsitteen tapauskohtainen harkinta ja kontekstisidonnaisuus.

Tietosuojatyöryhmä on esittänyt myös toisen terveystietoja koskeva esimerkin, jossa tutkija kokoaa tiedot potilaan tutkimuksista ja yksilöi potilaat edellisen esimerkin tapaan koodeilla. Tutkija lähettää lääkeyrityksille ja muille toimeksiantajille tiedot vain koodatussa muodossa. Tutkija kuitenkin säilyttää koodiavaimen tunnistamisen mahdollistaakseen, sillä mikäli lääkkeet osoittautuvat vaarallisiksi, tutkijan on potilaiden terveyden suojelemiseksi pystyttävä tarvittaessa tunnistamaan henkilöt hoitaakseen heidät asianmukaisesti.[273] Tietosuojatyöryhmä totesi, että samaa aineistoa käsittelevä toimija ei kuitenkaan välttämättä käsittele henkilötietoja, jos uudelleentunnistamisen mahdollisuus on nimenomaisesti poissuljettu ja tätä varten on toteutettu asianmukaiset tekniset toimenpiteet.[274] Tunnistamisen mahdollisuuden nimenomainen poissulkeminen voisi sinänsä viitata sekä pseudonymisointiin että anonymisointiin. Kontekstista päätellen voidaan kuitenkin tulkita, että koska tutkijalla on vielä tarpeen tunnistaa henkilö, on tietosuojatyöryhmä tarkoittanut kuvata suhteellista lähestymistapaa pseudonymisoituun tietoon. Tässä esi-

[272] WP136, s. 15—16.
[273] WP136, s 19; Ks. myös Tarhonen 2016, s. 20; Tämä on yksi esimerkki siitä, miksi pseudonymisointi on joissakin tilanteissa anonymisointia tarkoituksenmukaisempaa myös rekisteröityjen omien etujen kannalta.
[274] WP136, s. 19.

merkissä koodiavain kuvastaa yhtä relatiivisen avaimen muotoa. Jos toimeksiantajan on kuitenkin mahdollista esimerkiksi yhdistellä tietoja potilaalla olevan harvinaisen sairauden vuoksi, toimii tietojen yhdisteleminen relatiivisena avaimena tunnistettavuuden lukon avaamiseksi.

Tietosuojatyöryhmä on kuvannut viininjuontitottumusten tilastointiin liittyvän tilanteen, jossa yksittäisen henkilön nimen sijasta käytetään koodia. Nimiä ja koodeja säilytetään toisistaan erillään. Tilastointilaitoksen osalta yksilöihin liitettäviä tietoja voidaan pitää henkilötietoina, sillä tätä koodiavainta on mahdollista käyttää kohtuullisesti toteutettavissa olevin keinoin, koska heillä on nämä avaimet hallussaan. Työryhmä nostaa kuitenkin esille tämän tutkimuksenkin kannalta relevantin ongelman: tilastot viininjuontitavoista toimitetaan seuraavaksi viinintuottajajärjestölle, jotta se voi esittää tilastotietoja esimerkiksi markkinoimiseen. Henkilötietoaseman ratkaisemiseksi on arvioitava, voidaanko yksittäiset viininkuluttajat tunnistaa ottaen huomioon kaikki kohtuullisen todennäköiset relatiiviset avaimet, joita rekisterinpitäjä tai joku muu voi käyttää.[275] Tässäkin esimerkissä korostuu henkilötietokäsitteen suhteellisuus ja olosuhdetekijät.

Tietosuojatyöryhmän esimerkit korostavat suhteellista lähestymistapaa ja toimijakohtaista arviointia. Huomionarvoista on, että tietosuojatyöryhmä on tulkinnut myös arkaluonteisena pidettävien terveystietojen tunnistettavuutta suhteellisesta lähestymistavasta. Terveystietojen ja muiden erityisiin henkilötietoryhmiin kuuluvien tietojen kohdalla tulisi kuitenkin relatiivisen avaimen saatavuuteen kiinnittää korostuneesti huomiota.

4.2 Tietosuojaneuvoston pseudonymisointia koskevat suuntaviivat

TSA:n tultua voimaan tietosuojatyöryhmän on korvannut Euroopan tietosuojaneuvosto.[276] Tietosuojaneuvosto on julkaissut tammikuussa 2025 henkilötietojen pseudonymisointia koskevat suuntaviivat, joiden tarkoituksena on auttaa rekisterinpitäjiä valitsemaan tehokkaita tekniikoita alkuperäisten henkilötietojen muokkaamiseen, suojaamaan pseudonymisoituja tietoja luvattomalta yhdistämiseltä sekä hallinnoimaan käyttöoikeuksia pseudonymisoituja tietoja käsiteltäessä.[277]

Tietosuojaneuvosto lähtee siitä, että pseudonymisoidut tiedot, jotka voidaan yhdistää henkilöön lisätiedolla, ovat edelleen henkilötietoja.[278] Tietosuojaneuvosto ei siis nimenomaisesti väitä, että

[275] WP136, s. 18.
[276] TSA johdanto-osa 139 kappale; Ks. tarkemmin tietosuojaneuvoston roolista TSA 64–76 artiklat.
[277] EDPB 1/2025, s. 4. Tietosuojaneuvosto käsittelee suuntaviivoissaan erilaisia pseudonymisoinnin toteutustapoja, joita ei tutkimuksen laajuuden vuoksi ole tarkoituksenmukaista lähteä avaamaan.
[278] EDPB 1/2025, s. 8.

pseudonymisoitu henkilötieto olisi aina ja kaikille henkilötietoa, vaan se riippuu tunnistamismahdollisuudesta. Näin on tietosuojaneuvoston mukaan myös silloin, kun pseudonymisoidut tiedot ja lisätiedot eivät ole saman tahon hallussa.[279] Tämä puolestaan korostaa henkilötiedon ja anonyymin tiedon välisessä rajanvedossa kohtuullisen todennäköisesti käytettävissä olevan relatiivisen avaimen olemassaoloa. Jos pseudonymisoidut henkilötiedot ja relatiivinen avain voidaan yhdistää toisiinsa ottaen huomioon ne keinot, joita rekisterinpitäjä tai muu taho todennäköisesti käyttää, ovat pseudonymisoidut tiedot henkilötietoja. Vaikka pseudonymisoivan rekisterinpitäjän hallussa ollut relatiivinen avain olisi poistettu, pseudonymisoitu henkilötieto muuttuu anonyymiksi vain, jos anonyymiyden edellytykset täyttyvät.[280]

Pseudonymisoivan rekisterinpitäjän tai henkilötietojen käsittelijän säilyttämä relatiivinen avain on suojattava teknisin ja organisatorisin toimenpitein, jottei tietoja voida yhdistää tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön. Relatiivista avainta ei saa luovuttaa pseudonymisoituja tietoja käsitteleville henkilöille eikä niitä saa käyttää.[281] Tämä tekisi pseudonymisoinnin käytännössä merkityksettömäksi. Relatiivinen avain voi olla myös itsessään henkilötietoa.[282] Pseudonymisoinnin tehokkuuden arvioinnissa tulee huomioida, että lisätietoja voi olla pseudonymisoivan rekisterinpitäjän tai henkilötietojen käsittelijän välittömän valvonnan ulkopuolellakin. Esimerkiksi sosiaalisesta mediasta voi saada tällaisia tietoja.[283] Pseudonymisoitujen tietojen virtausta on valvottava tiukasti, kuten kaikkia henkilötietoja.[284]

Pseudonymisointi on usein tehokkainta, kun sitä täydennetään lisätoimenpiteillä. Rekisterinpitäjän tuleekin arvioida toimenpiteiden kokonaisuutta siten, että ne riittävät täyttämään tietosuojavaatimukset.[285] Pseudonymisoinnin luvaton kumoutuminen on tietoturvaloukkaus, johon sovelletaan TSA:n tietoturvaloukkausta koskevia säännöksiä.[286] Luvatonta purkamista voi vaikeuttaa,

---

[279] EDPB 1/2025, s. 10 kohta 22.
[280] EDPB 1/2025, s. 10 kohta 22.
[281] EDPB 1/2025, s. 9 kohta 20.
[282] EDPB 1/2025, s. 9 kohta 20.
[283] EDPB 1/2025, s. 10 kohta 21. Sosiaalinen media on yksi esimerkki relatiivisen avaimen monipuolisesta ulottuvuudesta, sillä esimerkiksi sosiaalisessa mediassa tietoja voidaan jakaa monilla eri tavoilla, niin rajatulle ihmismäärälle kuin avoimesti saataville ja yhdistää esimerkiksi toisilta käyttäjiltä löytyviin tietoihin.
[284] EDPB 1/2025, s. 25 kohta 112.
[285] EDPB 1/2025, s. 13 kohta 44.
[286] Ks. EDPB 1/2025, s. 19 kohta 80. Ks. myös s. 25 kohta 113, jonka mukaan rekisterinpitäjän on varmistettava lisätietojen ja pseudonymisoidun tiedon käsittelyyn käytettyjen järjestelmien ja palvelluiden jatkuva luottamuksellisuus, eheys ja vikasietoisuus.

jos pseudonymisointi on suoritettu kahteen kertaan.[287] Tietoturvaloukkauksena pidetään myös lisätietojen katoamista siten, ettei rekisterinpitäjällä ole tietoihin enää pääsyä.[288]

Tehokas pseudonymisointi vähentää luottamuksellisuusriskejä: se estää rekisteröityjen suorien tunnisteiden paljastamisen, mutta myös vähentää riskin vakavuutta tilanteessa, jossa pseudonymisoitu tieto paljastetaan tai pääsee luvattomasti toisen käsiin.[289] Esimerkiksi Suomessa suurimpana tietomurtotapauksena tunnetussa Vastaamo-tapauksessa tehokkaasti pseudonymisoidut tiedot olisivat voineet huomattavasti vähentää asianomistajiin kohdistuvia haittoja. Toisistaan hyvin poikkeavien salanimien antaminen samankaltaisia ominaisuuksia omaaville henkilöille voi parantaa luottamuksellisuutta sekä vähentää riskiä siitä, että tiedot tai kohteet liitetään virheellisesti vääriin rekisteröityihin.[290]

Yksi tapa yhdistää tiedot luonnolliseen henkilöön on tarkastella useita tiedoissa olevia ominaisuuksia, jotka paljastavat tietoa rekisteröidyn identiteetistä. Näitä ovat esimerkiksi ikä, sukupuoli, siviilisääty, perhetilanne ja ammattiin liittyvät tiedot. Tällaisten niin kutsuttujen kvasitunnisteiden yhdistelmä riittää mahdollistamaan ainakin osan pseudonymisoitujen tietojen yhdistämisen rekisteröityyn. Pseudonymisoituja tietoja käsittelevät henkilöt saattavat siten pystyä yhdistämään näiden perusteella tiedot henkilöihin ilman yksittäisten lisätietojen käyttöä.[291] Tämä korostaa relatiivisen avaimen laajempaa ulottuvuutta perinteiseen lisätiedon käsitteeseen verrattuna. Kyseisessä esimerkissä kvasitunnisteiden yhdistelemistä voidaan pitää relatiivisen avaimen muotona.[292]

Tietosuojaneuvosto on ottanut käyttöön uuden käsitteen: pseudonymisointialueen. Tämä käytännössä tarkoittaa sen määrittämistä, keneltä kielletään pseudonymisoitujen tietojen yhdistäminen rekisteröityyn.[293] Rekisterinpitäjä voi pseudonymisoinnin tavoitteesta riippuen määritellä pseudonymisointialueen kattamaan esimerkiksi vain yhden rekisterinpitäjän organisaation yksikön, yhden ulkoisen vastaanottajan, kaikki valtuutetut tai ennakoidut lailliset vastaanottajat

[287] Ks. EDPB 1/2025, s. 28 kohta 128.
[288] Korpisaari ym. 2022, s. 381–382.
[289] EDPB 1/2025, s. 11 kohta 27.
[290] Ks. EDPB 1/2025, s. 11 kohta 29. Tietosuojaneuvosto on siten tunnistanut väärien yhdistämisten mahdollisuuden.
[291] EDPB 1/2025, s. 23 kohta 101. Ks. myös kohta 102, jonka mukaan kvasitunnisteet voidaan kuitenkin poistaa, muokata tai satunnaistaa.
[292] Esimerkiksi sukupuolen ja ammatin yhdistelmällä on pienemmällä paikkakunnalla todennäköisempää tunnistaa tietty henkilö kuin suurkaupungissa, minkä vuoksi relatiivisen avaimen olemassaolo vaihtelee näkökulmasta riippuen.
[293] EDPB 1/2025, s. 8.

taikka joukon tai kaikki ulkoiset tahot, jotka voivat yrittää saada pääsyn tietoihin.[294] Jos pseudonymisointia halutaan käyttää luottamuksellisuusriskien vähentämiseksi, pseudonymisointialueeseen on sisällytettävä tällaiset luvattomat kolmannet osapuolet ja arvioitava keinot, joita nämä todennäköisesti tunnistamiseen käyttäisivät.[295]Tietosuojaneuvoston mukaan erityisesti kaikkien pseudonymisoitujen tietojen vastaanottajien on voitava osoittaa, että pseudonymisoituja tietoja ei luovuteta luvattomille vastaanottajille.[296] Luvattomasta kolmannesta osapuolesta johtuvia luottamuksellisuusriskejä vähentääkseen rekisterinpitäjän tai henkilötietojen käsittelijän on sisällytettävä kolmannet osapuolet pseudonymisointialueeseen ja arvioitava todennäköiset relatiivisen avaimen mahdollisuudet. Tällöin on tietosuojaneuvoston mukaan suositeltavaa ottaa huomioon sekä vilpittömässä että vilpillisessä, kuten rikollisessa tarkoituksessa tehdyt toimet.[297]

Pseudonymisoivan rekisterinpitäjän on arvioitava ja varmistettava, että pseudonymisointialueella tunnistamisriski on merkityksetön.[298] Näin ollen tunnistamisen ei tarvitse olla teoriassa ehdottomasti mahdotonta. Kaikkien asianomaisten toimijoiden on valittava asianmukaiset tekniset ja organisatoriset keinot, joilla varmistetaan, etteivät pseudonymisoidut tiedot poistu pseudonymisointialueelta eikä alueelle pääse relatiivista avainta.[299] Lopuksi rekisterinpitäjien tulee rajoittaa pseudonymisoidun tiedon käsittelyä siinä määrin kuin se on tarpeen jäännösriskin lieventämiseksi.[300]

Vaikka tunnistamisen riski on pseudonymisoivan rekisterinpitäjän sisäisessä käsittelyssä pieni, kolmannelle osapuolelle siirrettäessä sitä tulee arvioida uudelleen. Tällöin on vähintään tunnistettava ja otettava huomioon vastaanottajalla käytettävissä olevat tunnistamiskeinot. Tietosuojaneuvoston mukaan tämä korostuu etenkin, jos siirto olisi laillista vain silloin, jos tiedot pysyvät vastaanottajalla pseudonymisoituina.[301] Rekisterinpitäjän tulee myös arvioida, pitäisikö riskien minimoimiseksi esimerkiksi muokata tai korvata salanimiä ennen tietojen luovuttamista. Jos vastaanottaja on itsenäinen rekisterinpitäjä, on tietosuojaneuvosto pitänyt hyvänä käytäntönä, että

[294] EDPB 1/2025, s. 12 kohta 38.
[295] EDPB 1/2025, s. 13 kohta 42.
[296] Ks. EDPB 1/2025, s. 14 kohta 51.
[297] EDPB 1/2025, s. 12 kohta 42.
[298] EDPB 1/2025, s. 30 kohta 131.
[299] Ks. EDPB 1/2025, s. 12 kohta 39 ja s. 30 kohta 134.
[300] EDPB 1/2025, s. 30 kohta 135.
[301] EDPB 1/2025, s. 17 kohta 70.

vastaanottava rekisterinpitäjä ilmoittaa luovuttavalle rekisterinpitäjälle omaan käsittelyynsä liittyvistä riskeistä.[302] Tähän ei kuitenkaan tietosuojasääntely velvoita, mutta käytäntö voi olla asianmukainen myös vastaanottajan omien riskien minimoimiseksi.

Tietosuojaneuvoston mukaan unionin tai jäsenvaltion lainsäädännössä voidaan säätää, että henkilötietoja käsitellään ainoastaan pseudonymisoidussa muodossa. Tällöin vastaanottajan olisi varmistettava, että pseudonymisoiva rekisterinpitäjä eli luovuttaja soveltaa relatiiviseen avaimeen teknisiä ja organisatorisia toimenpiteitä estääkseen tietojen yhdistämisen luonnolliseen henkilöön.[303] Tällaisessa tilanteessa vastaanottajalla on siis intressi saada tiedot tunnistamattomassa muodossa, eikä vastaanottajalla ole tarkoitustakaan hyödyntää pseudonymisoitua tietoa tietosuojasääntelyn velvoitteita kiertäen. Tietosuojaneuvosto on todennut, että siltä osin kuin on tarpeen varmistaa lisätietojen asianmukainen käsittely, vastaanottajan olisi tehtävä näiden osapuolten kanssa oikeudellisesti sitova sopimus, joka mahdollistaisi tällaisen käsittelyn täytäntöönpanon.[304] Tarvittaessa myös rekisterinpitäjän on tehtävä vastaanottajan kanssa sitova sopimus varmistaakseen, että vastaanotettuja tietoja käsitellään asianmukaisesti.[305] Sopimuksen tekeminen luovuttajan ja vastaanottajan välillä palvelee siten molempia osapuolia.

Vastaanottajien on voitava osoittaa, ettei pseudonymisoituja tietoja luovuteta luvattomille vastaanottajille.[306] Jos kuitenkin tieto on vastaanottajan näkökulmasta anonyymiä, voi tilanne johtaa siihen, että vastaanottaja rajoituksetta luovuttaa pseudonymisoitua aineistoa eteenpäin tai hyödyntää sitä itse muulla tavoin. Tällä puolestaan on suora vaikutus henkilötietojen suojaan aiheuttaen merkittäviä riskejä rekisteröidyille. On kuitenkin otettava huomioon, että tällaiseen tietoon mahdollisesti sovelletaan jotain muuta sääntelyä. Jos lainsäädännöllisiä rajoituksia ei kuitenkaan ole, on rajoituksia tietojen hyödyntämiselle ja luovuttamiselle luvattomille vastaanottajille mahdollista määritellä sopimuksellisin keinoin. Tietosuojaneuvoston mukaan aina kun pseudonymisointialueen on tarkoitus koostua määritellystä vastaanottajajoukosta, kaikkien osapuolten vastuut tulisi määritellä sopimuksella, mieluiten sopimusmuodossa. Näiden järjestelyjen tulisi heijastaa tarvetta pitää pseudonymisoitu aineisto pseudonymisointialueen sisällä ja rajoittaa sellaisten tietojen sisäänvirtausta tai pääsyä tietoihin, jotka saattaisivat mahdollistaa pseudonymisoidun tiedon yhdistämisen rekisteröityihin.[307] Toisin sanoen sopimusjärjestelyillä pyrittäisiin mahdollistamaan pseudonymisoinnin tehokkuus siten, ettei relatiivisia avaimia ilmene

[302] EDPB 1/2025, s. 18 kohta 72.
[303] EDPB 1/2025, s. 18 kohta 73.
[304] EDPB 1/2025, s. 18 kohta 73.
[305] EDPB 1/2025, s. 18–19 kohta 75.
[306] EDPB 1/2025, s. 14 kohta 51.
[307] EDPB 1/2025, s. 25 kohta 114.

pseudonymisointialueen sisällä. Sopimusjärjestelyjä ei luonnollisestikaan ole mahdollista toteuttaa, jos vastaanottajia ei ole määritelty. Suuntaviivoissa avoimeksi kysymykseksi kuitenkin jää, onko suhteellista henkilötiedon käsitettä mahdollista soveltaa saman pseudonymisointialueen sisällä siten, että sama aineisto on jollekin henkilötietoa ja jollekin anonyymiä.

Asianomaisten rekisterinpitäjien tulee soveltaa säilyttämiinsä lisätietoihin suunniteltuja teknisiä ja organisatorisia toimenpiteitä.[308] Kaikkien vastaanottajien tulee puolestaan soveltaa asianmukaisia teknisiä ja organisatorisia toimenpiteitä varmistaakseen, ettei pseudonymisoitu aineisto poistu pseudonymisointialueelta sekä varmistaa, ettei alueelle pääse relatiivista avainta.[309] Näin voidaan katsoa olevan ainakin silloin, kun pseudonymisoitu tieto on vastaanottajan käsissä henkilötietoa. Rekisterinpitäjän tulee rajoittaa pseudonymisoidun tiedon käsittelyä siinä määrin kuin se on pseudonymisoinnin kumoutumisriskin eli niin sanotun jäännösriskin lieventämiseksi tarpeen.[310]

Huomionarvoista on, että tietosuojaneuvoston suuntaviivat, lausunnot ja ohjeistukset ovat soft law -aineistoa, eikä niillä ole samaa velvoittavuutta kuin EUT:n ratkaisuilla. Niillä on kuitenkin merkittävä käytännön ohjausvaikutus.[311] On siten pidettävä mielessä, että mikäli suuntaviivat olisivat ristiriidassa esimerkiksi EU:n ratkaisukäytännön kanssa, on jälkimmäistä vahvasti velvoittavana oikeuslähteenä noudatettava. Tietosuojaneuvoston suuntaviivat korostavat huolellisen riskiarvioinnin merkitystä sekä käytännössä korkeaa kynnystä tulkita pseudonymisoitu henkilötieto anonyymiksi, vaikkei tätä suoranaisesti mainita.

Käytännössä henkilötiedoksi tulkitsemisen määrää ainoastaan se, onko tietty luonnollinen henkilö tunnistettavissa.[312] TSA:sta sekä sitä edeltäneiden tietosuojatyöryhmien ja oikeuskirjallisuudessa esitetyistä kannanotoista voidaan todeta, että kun arvioidaan kohtuullisen todennäköisesti toteutettavissa olevia keinoja luonnollisen henkilön tunnistamiseksi, tulee näitä aina peilata yksittäistapauksen olosuhteisiin ja tehdä tapauskohtaista harkintaa. Huomionarvoista on kuitenkin, että tällainen tapauskohtaisen harkinnan mahdollisuus on aina omiaan johtamaan jopa hyvinkin erilaisiin tulkintoihin.[313]

---

[308] EDPB 1/2025, s. 30 kohta 133.
[309] EDPB 1/2025, s. 30 kohta 134.
[310] EDPB 1/2025, s. 30 kohta 135.
[311] Ks. Määttä – Paso 2022, s. 30–31; Ks. myös Saarenpää – Riekkinen 2023, s. 237, jossa todetaan, että tietosuojaneuvostolla on vahva tulkinta-asema.
[312] WP136, s. 4; Ks. myös Stalla-Bourdillon – Knight 2016, s. 320—321.
[313] Ks. Voutilainen 2019, s. 87. Myös TSA:ssa on direktiivin piirteitä siinä, että se mahdollistaa liikkumavaraa ja erilaisia tulkintoja.

4.3 Tunnistettavuus ja toimijoiden roolit ratkaisukäytännössä

4.3.1 EUT:n merkittävät tunnistettavuutta koskevat ratkaisut

Aiemmissa luvuissa on todettu, että pseudonymisoidun tiedon oikeudellinen asema määräytyy tunnistettavuuden perusteella. Keskeinen kysymys onkin, missä tilanteessa henkilö ei ole pseudonymisoiduista tiedoista enää tunnistettavissa. Toinen keskeinen kysymys on, mitkä katsotaan ”kohtuullisen todennäköisiksi keinoiksi” tunnistettavuuden arvioinnissa. Olennaista on myös huomioida, miten eri toimijoiden tulee suhtautua pseudonymisoituun aineistoon rekisteröidyn oikeuksien ja tietosuojatavoitteiden toteuttamiseksi.

EUT on vuonna 2016 antamassaan ratkaisussa C-582/14 (Breyer vs. Saksan liittotasavalta) ottanut kantaa henkilötiedon tunnistettavuuteen.[314] Tapauksessa oli kyse siitä, olivatko dynaamiset IP-osoitteet[315] henkilötietoja verkkosivuston ylläpitäjän näkökulmasta silloin, kun tunnistamisen mahdollistavat tiedot eivät olleet saman tahon hallussa. Breyerin internetpalveluntarjoajalla oli hallussa tiedot, joiden perusteella Breyer oli mahdollista tunnistaa tämän dynaamisen IP-osoitteen perusteella. Tapauksessa EUT otti käytännössä kantaa siihen, tuliko henkilön tunnistettavuutta arvioida absoluuttisen vai suhteellisen kriteerin kautta.[316] Suhteellisesta näkökulmasta dynaaminen IP-osoite olisi henkilötietoa ainoastaan Breyerin internetpalveluntarjoajan näkökulmasta, kun taas objektiivisesta näkökulmasta ne olisivat henkilötietoja kaikille osapuolille.[317] EUT ratkaisi asian siten, että dynaaminen IP-osoite on henkilötieto ”jos palveluntarjoajalla on käytettävissään oikeudelliset keinot, joiden perusteella se voi tunnistaa kyseisen henkilön sellaisten lisätietojen avulla, jotka ovat tämän henkilön internetyhteyden tarjoajan käytettävissä.”[318]

Breyer-ratkaisussa on otettu kantaa myös siihen, mitä kohtuullisen todennäköisillä keinoilla tarkoitetaan. Kohtuulliset keinot voivat olla sellaisia, joissa relatiivinen avain saadaan sivullisilta kohtuullisella tavalla. Laittomia tai käytännössä mahdottomia keinoja ei kohtuullisen todennäköisillä keinoilla tarkoiteta.[319] Mahdottomilla keinoilla tarkoitetaan sellaisia, joilla tunnistaminen

---

[314] Ks. Stalla-Bourdillon 2025, s. 1468, jossa Breyer-tapauksen on kuvattu olevan “the main CJEU case touching upon the concept of identifiability”.
[315] Dynaamiset IP-osoitteet vaihtuvat jokaisen uuden internetyhteyden ottamisen myötä, toisin kuin staattiset IP-osoitteet. Ks. C-582/14 (Breyer), kohta 16.
[316] El Khoury 2017, s. 2. EUT on käyttänyt ilmauksia objektiivinen ja suhteellinen.
[317] Zuiderveen Borgesius 2017, s. 131–132.
[318] C-582/14 (Breyer), kohdat 49 ja 65.
[319] Julkisasiamiehen Sánchez-Bordonan ratkaisuehdotus asiassa C-582/14 (Breyer), kohta 68.

vaatii suhteettomia ponnisteluja resursseihin nähden.[320] Tunnistamisen ei siten tarvitse olla helppoa, mutta sen on oltava realistisesti toteutettavissa ilman suhteettomia ponnistuksia. Relatiivisen avaimen käsitteen voidaan kuitenkin sinänsä katsoa pitävän sisällään myös laittomat ja mahdottomat keinot, mutta rekisterinpitäjän velvollisuutta arvioida tällaisten niin avainten olemassaoloa ei voida pitää kohtuullisena. Jäännösriskin arvioinnissa on tällaiset otettava kuitenkin huomioon henkilötietojen suojaamiseksi.[321]

Oikeuskirjallisuudessa on analysoitu, että EUT vaikuttaisi Breyer-ratkaisun perusteella painottavan absoluuttista lähestymistapaa tunnistettavuuden arvioinnissa.[322] Breyer-ratkaisu kuitenkin osoittaa, ettei henkilötietokäsite ole täysin absoluuttinen, vaan se vaatii tilannekohtaista arviointia. EUT ei erityisesti korosta toimijakohtaisuutta, mutta se ilmenee kohtuullisen todennäköisten keinojen arvioinnissa.[323] EUT on Breyer-ratkaisussa vahvistanut suhteellista lähestymistapaa, mutta pitänyt anonyymiksi tulkitsemisen kynnyksen korkealla.[324] Oikeuskirjallisuudessa on myös esitetty näkemys siitä, että Breyer-ratkaisulla asetettiin luonnollisen henkilön tunnistamisen standardi niin tiukalle, että suhteellisen henkilötiedon käsitteelle ei käytännössä jäänyt paljoa tilaa.[325] EUT asetti kohtuullisen todennäköisten keinojen arvioinnin korkealle katsoen, että tunnistaminen on kohtuullisin keinoin mahdollista hypoteettisessa tulevaisuuden tilanteessa välikäsiin tukeutuen.[326] Voidaan kuitenkin todeta, että tästä korkeasta kynnyksestä huolimatta EUT on tunnustanut suhteellisen henkilötietokäsitteen olemassaolon.

EUT on antanut joulukuussa 2017 ratkaisun C-434/16 (Nowak vs. Data Protection Commissioner), jossa oli kyse muun muassa siitä, ovatko hakijan laatimat koevastaukset sekä tarkastajan kokeeseen tekemät merkinnät osallistujaan liittyviä henkilötietoja. EUT katsoi, että kokeen tarkastajan antamat kommentit sisälsivät ensinnäkin osallistujaan liittyviä tietoja, sillä kommentit

---

[320] C-582/14 (Breyer), kohta 46.
[321] Ks. myös EDPB 1/2025, s. 12 kohta 42.
[322] Ks. esimerkiksi Zuiderveen Borgesius 2017, s. 135. Absoluuttisen sijaan on kuitenkin käytetty termiä ”objektiivinen”, johon myös EUT viittaa Breyer-ratkaisussaan.
[323] Ks. esim. C-582/14 (Breyer), kohta 49, jonka mukaan dynaaminen IP-osoite on palveluntarjoajaan nähden henkilötieto, jos palveluntarjoajalla on käytettävissään oikeudelliset keinot, joiden perusteella se voi tunnistaa kyseisen henkilön sellaisten lisätietojen avulla, jotka ovat tämän henkilön internetyhteyden tarjoajan käytössä.
[324] Ks. Hintze 2018, s. 89, jonka mukaan kaikki tiedot, jotka eivät ylitä tätä EUT:n vahvistamaa korkeaa kynnystä, ovat edelleen henkilötietoja.
[325] Rauhanen 2025, s. 662.
[326] Ks. C-582/14 (Breyer), kohdat 47–48. EUT katsoi, että toimijalla oli kohtuullisen todennäköiset keinot tunnistamiseen, jos tämä kääntyy mahdollisessa kyberhyökkäystilanteessa viranomaisen puoleen, joka puolestaan hankkii tiedot internetpalveluntarjoajalta; Ks. ulkopuolisiin apuihin tukeutumisesta myös C-604/22 (IAB Europe), kohta 78.

sisälsivät tarkastajan mielipiteitä ja arvioita kyseisestä osallistujasta ja hänen koesuoriutumisestaan. Toiseksi näiden kommenttien katsottiin liittyvän myös tarkastajaan, sillä kommentit sisälsivät tämän mielipiteitä.[327] EUT nosti esille, että mikäli tiedot eivät olisi olleet henkilötietoa, ei näihin sovellettaisi tietosuojalainsäädäntöä. Tämä taas olisi johtanut siihen, että vastauksia ja kommentteja voisi mahdollisesti jakaa kolmansille osapuolille ilman rajoitteita.[328] Vaikka Nowak-ratkaisu ei koskenut pseudonymisointia, ratkaisu korostaa tulkintaa, jossa henkilötietokäsitteelle annetaan laaja merkitys perusoikeussuojan turvaamiseksi.

EUT on katsonut maaliskuussa 2024 antamassaan ratkaisussa C-479/22 P (OC v. komissio), että Euroopan petostentorjuntaviraston lehdistötiedotteessa esitetyt tiedot voivat muodostaa henkilötietoja, mikäli henkilö on tunnistettavissa objektiivisen tarkastelun perusteella tai kohtuullisen todennäköisillä keinoilla, joita joku lukijoista voisi käyttää.[329] EUT on todennut, että henkilön epäsuoraan tunnistamiseen liittyy olennaisesti lisätiedot, joiden ei tarvitse olla asianomaisten tietojen käsittelystä vastaavan rekisterinpitäjän hallussa.[330] EUT huomioi siten mahdollisuuden, että laajasta joukosta jollakin saattaa olla relatiivinen avain hallussaan. Näin ollen pseudonymisoituja ja anonymisoituja henkilötietoja jakaessaan toimijan tulee huomioida relatiivisen avaimen esiintymisen mahdollisuus laajasti henkilötietojen suojan turvaamiseksi.

4.3.2 SRB-ratkaisu: suhteellisen henkilötiedon käsitteen vahvistaja

EUT on antanut 4. syyskuuta 2025 merkittävänä pidettävän ja kritisoidun[331] ratkaisun C-413/23 P Euroopan tietosuojavaltuutettu (jäljempänä ’EDPS’ tai ’tietosuojavaltuutettu’) v. Single Resolution Board (kriisinratkaisuneuvosto).[332] Kriisinratkaisuneuvosto oli kerännyt pankin entisiltä osakkeenomistajilta ja velkojilta huomautuksia, jotka pseudonymisoitiin korvaamalla henkilötiedot satunnaisilla koodeilla. Kriisinratkaisuneuvosto kuitenkin säilytti rekisterinpitäjänä erilliset lisätiedot, joiden avulla huomautusten antajat oli mahdollista tunnistaa. Pseudonymisoidut huomautukset sitten siirrettiin konsulttiyhtiölle ratkaisun arvioimiseksi. [333] Tapauksessa tietojen kerääminen rekisteröidyltä perustui suostumukseen.[334]

---

[327] C-434/16 (Nowak), kohdat 42–44.
[328] C-434/16 (Nowak), kohdat 48–50.
[329] C-479/22 P (OC v. Komissio), kohta 64.
[330] C-479/22 P (OC v. Komissio), kohta 55.
[331] Ratkaisua on kritisoitu mm. avoimeksi jätetyistä kysymyksistä. Ks. esim. Rauhanen 2025.
[332] Tapauksessa sovellettiin EU:n toimielinten TSA:n säännöksiä, mutta C-413/23 P (SRB) kohdassa 52 todetaan, että tapauksen havainnot soveltuvat yhtä lailla TSA:n soveltamisalaan.
[333] Ks. C-413/23 P (SRB), kohdat 22–28, joissa on kuvattu pseudonymisoidun tiedon käsittelyyn ja luovuttamiseen liittyvää menettelyä.
[334] C-413/23 P (SRB), kohta 106.

Tietosuojavaltuutettu argumentoi perusteluissaan, että henkilötietojen käsitteen laaja tulkinta on välttämätöntä, jotta tietosuojaa koskevalla oikeudella olisi tehokas vaikutus.[335] Tietosuojavaltuutettu piti pseudonymisoitua tietoa automaattisesti henkilötietona kaikkien tahojen osalta eikä ollut miettinyt vastaanottajan tosiasiallista tunnistamisen mahdollisuutta, mikä selvästi osoittaa absoluuttista lähestymistapaa.[336] Tietosuojavaltuutettu on katsonut unionin lainsäätäjän selventäneen pseudonymisoinnin käsitteen käyttöönotolla, ettei henkilötietoja voida jättää tietosuojasääntelyn ulkopuolelle pelkästään erottamalla ne lisätiedoista.[337] Tietosuojavaltuutettu on huomauttanut, että pseudonymisoitujen tietojen pitäminen anonyymeinä on omiaan vaarantamaan unionin lainsäätäjän tavoitteleman ja perusoikeuskirjassa edellytetyn korkeatasoisen suojan.[338] Myös tietosuojaneuvosto on ottanut asiaan kantaa nostamalla esiin, että pseudonymisoituja tietoja voitaisiin tällöin käsitellä rajoituksetta, esimerkiksi jakamalla, julkaisemalla tai siirtämällä kolmansiin maihin. [339]

EUT on SRB-ratkaisussaan linjannut, ettei pseudonymisoitujen tietojen voida katsoa olevan kaikissa tilanteissa ja kaikkien henkilöiden osalta henkilötietoja, koska pseudonymisointi voi käsiteltävän asian olosuhteiden mukaan tosiasiallisesti estää muita henkilöitä kuin rekisterinpitäjää tunnistamasta rekisteröityä siten, ettei tämä ole enää näiden henkilöiden tunnistettavissa.[340] Rekisterinpitäjällä säilyi relatiivinen avain, jolla yhdistäminen tiettyyn rekisteröityyn oli mahdollista.[341] Näin ollen aineisto pysyi rekisterinpitäjän näkökulmasta henkilötietona ja tämän tuli noudattaa tietosuojasääntelyä. EUT kuitenkin erotti ratkaisussaan selkeästi toisistaan rekisterinpitäjän ja vastaanottajan näkökulmat. EUT:n mukaan pseudonymisoitu aineisto ei vastaanottajan näkökulmasta ole välttämättä henkilötietoa, jos yhdistäminen rekisteröityyn ei ole kohtuudella mahdollista.[342] Tämä merkitsee sitä, että sama tieto voi siis olla henkilötietoa yhdelle, muttei toi-

---

[335] C-413/23 P (SRB), kohta 66.
[336] Ks. C-413/23 P (SRB), kohdat 66 ja Rauhanen 2025, s. 672.
[337] C-413/23 P (SRB), kohta 65.
[338] C-413/23 P (SRB), kohta 66; Ks. myös kohta 64: Unionin yleisen tuomioistuimen tulkinta on ollut, että henkilötiedot muuttuisivat luonteeltaan silloin, kun ne siirretään ulkopuolelle sellaiselle taholle, jolla ei ole tunnistamisen mahdollistavaa lisätietoa.
[339] C-413/23 P (SRB), kohta 66; TSA johdanto-osan 101 kappaleen mukaan henkilötietojen siirroilla ei saa vaarantaa henkilötietojen suojan tasoa, ja siirtoja voidaan toteuttaa ainoastaan tietosuoja-asetusta kaikilta osin noudattaen.
[340] C-413/23 P (SRB), kohta 86.
[341] C-413/23 P (SRB), kohta 76.
[342] C-413/23 P (SRB), erityisesti kohdat 85–87. Oikeuskirjallisuudessa on tarkasteltu tapausta jo ennen EUT:n antamaa ratkaisua siten, että tietojen suunniteltu käyttö puoltaisi henkilötietoluonteen säilymistä vastaanottajan hallussa. Ks. Stalla-Bourdillon 2025, s. 1465. EUT on kuitenkin päätynyt vastakkaiseen ratkaisuun.

selle. Ratkaisua on pidetty EUT:n ratkaisukäytännössä ensimmäisenä, jossa EUT vahvistaa henkilötiedon suhteellisen käsitteen siten, että riittävän vahvasti pseudonymisoidut tiedot eivät ole kaikille tahoille välttämättä henkilötietoa.[343]

EUT katsoi, että siltä osin kun ei voida sulkea pois sitä, että kolmansilla osapuolilla on kohtuulliset keinot yhdistää pseudonymisoidut tiedot rekisteröityyn, rekisteröityä on pidettävä tunnistettavissa sekä luovuttavan että kolmansien osapuolten suorittaman myöhemmän käsittelyn osalta.[344] Vastaanottajan ei siten tarvitse pitää pseudonymisoitua tietoa henkilötietona, jos se ei pysty tunnistamaan henkilöä kohtuullisin ja laillisin keinoin, eikä se luovuta pseudonymisoitua tietoa relatiivisen avaimen omaavalle taholle.[345] Näin ollen, vaikka toimija ei itse pystyisi tunnistamaan henkilöä, on tieto kuitenkin tämän hallussa henkilötietoa, jos vastaanottaja pystyy henkilön tunnistamaan.[346] EUT:n ratkaisun perusteella herää kysymys siitä, miten pitkälle rekisterinpitäjän tulee miettiä vastaanottajan tunnistamisvaihtoehtoja. Käytännössä pseudonymisoidun tiedon vastaanottajan realistiset tunnistamiskeinot vaikuttavat suoraan myös luovuttajana toimivan rekisterinpitäjän velvollisuuksiin. Tietosuojaneuvoston suuntaviivojen mukaan rekisterinpitäjän on pseudonymisoinnin tehokkuuden varmistamiseksi suunniteltava tunnistamiseen tarvittavat lisätiedot siten, etteivät pseudonymisointialueella olevat toimijat hallitse niitä tai pysty niitä kohtuullisin keinoin hankkimaan.[347] Jos luvaton toimija voi helposti hankkia pääsyn relatiiviseen avaimeen, pseudonymisoinnin turvallisuusetu voi olla merkityksetön tai olematon.[348]

EUT totesi, että henkilötiedon käsitteen tulee olla laaja, muttei rajaton.[349] EUT:n mukaan relatiivisen avaimen olemassaolo ei sinänsä tarkoita, että pseudonymisoituja tietoja olisi pidettävä kaikissa tapauksissa ja kaikkien tahojen osalta henkilötietoina.[350] Tätä kannanottoa on pidetty hyvin merkittävänä, sillä EUT selvästi omaksui suhteellisen henkilötietokäsitteen katsoessaan, että

---

[343] Rauhanen 2025, s. 657.
[344] C-413/23 P (SRB), kohta 85.
[345] C-413/23 P (SRB), kohta 85; Ks. myös Craddock 2025. Ks. tähän liittyen Digital Omnibusista luku 5.4.1.
[346] Esimerkiksi pseudonymisoiva rekisterinpitäjä A luovuttaa pseudonymisoidut henkilötiedot vastaanottajalle B. B kuitenkin katsoo, ettei sillä ole kohtuullisen todennäköisesti relatiivista avainta ja tulkitsee tiedon anonyymiksi. B luovuttaa tiedot edelleen C:lle olettaen, ettei tällä ole kohtuullisen todennäköisiä keinoja tunnistaa henkilöä. Mikäli C kuitenkin saa haltuunsa relatiivisen avaimen, tieto muuttuu sen hallussa takaisin henkilötiedoksi. Tällaisessa ketjussa B jää ainoaksi toimijaksi, joka ei pysty tunnistamaan henkilöä. Tällöin korostuisi kriittinen arviointi siitä, olisiko B:llä kuitenkin tosiasiallisesti kohtuulliset keinot tunnistaa henkilö.
[347] Ks. EDPB 1/2025, s. 16 kohta 60.
[348] EDPB 1/2025, s. 16 kohta 61.
[349] C-413/23 P (SRB), kohta 88.
[350] C-413/23 P (SRB), kohta 82.

sama aineisto voi olla toisen toimijan osalta henkilötietoa, muttei se sitä ole välttämättä toiselle.[351] Vaikka pseudonymisoidut tiedot olisivat lähtökohtaisesti henkilötietoja, voivat ne lakata olemasta henkilötietoa vastaanottajan näkökulmasta, jos asianmukaiset tekniset ja organisatoriset toimet estävät tunnistamisen.[352] EUT:n mukaan pseudonymisoitujen tietojen anonyymi asema vastaanottajan hallussa edellyttää sitä, ettei tämä pysty peruuttamaan pseudonymisointia tai turvautumaan muihin tunnistamiskeinoihin.[353] Tieto on siten EUT:n tulkinnan mukaan anonyymiä vain, jos vastaanottajalla ei ole realistista pääsyä relatiiviseen avaimeen.

Näin ollen ratkaisevaa on arvioida, onko tietojen yhdistäminen rekisteröityyn vastaanottajan näkökulmasta objektiivisesti arvioituna kohtuudella mahdollista ottaen huomioon tekniset ja organisatoriset toimenpiteet. Keino ei ole kuitenkaan kohtuullisen todennäköisin keinoin käytettävissä rekisteröidyn tunnistamiseen, jos tunnistaminen on lailla kielletty tai jos se veisi suhteettoman paljon aikaa tai resursseja.[354] EUT totesi, että sinänsä anonyymit tiedot voivat muuttua henkilötiedoiksi rekisterinpitäjän antaessa ne muiden tahojen käyttöön, joilla on kohtuullisen todennäköisesti pääsy relatiiviseen avaimeen.[355] Yksi SRB-ratkaisun myötä avoimeksi jäänyt kysymys on, että tarvitaanko pseudonymisoitujen tietojen luovuttamiseen vastaanottajalle oikeusperuste.[356]

EUT:n mukaan ratkaisussa ei ole kyse henkilötietojen suojan heikentämisestä vaan suojatasolle jo asetettujen rajoitusten vahvistamisesta.[357] Julkisasiamies Spielmannin ratkaisuehdotuksen mukaan jos henkilöt eivät ole tunnistettavissa, voidaan pseudonymisointia pitää riittävänä suojakeinoina, vaikkei lisätietoja olisi poistettu kokonaan.[358] Julkisasiamies on myös nostanut absoluuttisen ja suhteellisen henkilötietokäsitteen esiin toteamalla, että on olemassa *"kaksi hyvin erilaista tietosuojasääntöjen soveltamisalan ulottuvuutta koskevaa lähestymistapaa"*.[359] Julkisasiamies on todennut, että mikäli tunnistamisriskiä ei ole tai tunnistamisriski on merkityksetön,

[351] Ks. esim. Rauhanen 2025.
[352] C-413/23 P (SRB), kohdat 75 ja 77.
[353] C-413/23 P (SRB), kohta 77.
[354] C-413/23 P (SRB), kohta 82. EUT on viitannut C-479/22 P (OC v. Komissio) 51 kohtaan.
[355] C-413/23 P (SRB), kohta 84. EUT viittasi Scania-ratkaisun (C-319/22), 46 kohtaan, jonka mukaan ajoneuvon valmistenumero ei sellaisenaan ole henkilötietoa, mutta se voi relatiivisen avaimen myötä muuttua henkilötiedoksi.
[356] Ks. Craddock 2025, V.5.
[357] Ks. C-413/23 P (SRB), kohdat 88 ja 89. Ks. myös Craddock 2025.
[358] Julkisasiamies Spielmannin ratkaisuehdotus asiassa C-413/23 P (SRB), 51 kohta.
[359] Julkisasiamies Spielmannin ratkaisuehdotus asiassa C-413/23 P (SRB), kohta 43.

voidaan tietoa pitää anonyyminä.[360] Julkisasiamiehen lähestymistapaa voidaan siten pitää painotukseltaan EUT:n kantaa tiukempana.

EUT vahvisti SRB-ratkaisussa, että rekisterinpitäjällä säilyy muun muassa ilmoitusvelvollisuus pseudonymisoitujen henkilötietojen vastaanottajista siitä huolimatta, ovatko tiedot vastaanottajalle henkilötietoa vai ei. Tiedot mahdollisista vastaanottajista ovat EUT:n mukaan välttämättömiä, jotta rekisteröity voi myöhemmin puolustaa oikeuksiaan näitä vastaanottajia vastaan.[361] Tämä kanta on kuitenkin ristiriidassa pseudonymisoidun tiedon muuttuvan henkilötietoluonteen kanssa, sillä rekisteröidyllä ei ole oikeuksia anonyymiin tietoon. Kuitenkin rekisteröidyn kannalta voi olla merkityksellistä saada tieto konkreettisista vastaanottajista mahdollisten henkilötietoluonteen virheellisten tulkintojen ja tulevaisuudessa henkilötietojen suojan vaarantumisen vuoksi. EUT totesi lisäksi, että TSA:n velvoitteita ei voida asettaa sellaiselle tahoille, jotka eivät millään tavoin pysty tunnistamaan rekisteröityä.[362] Jos tunnistaminen on käytännössä mahdotonta, ei voida pitää kohtuullisena velvoitteiden kohdentamista tällaisiin tahoihin.[363] Tämä on merkittävä huomio nimenomaan puoltamaan suhteellista henkilötiedon käsitettä. Voitaisiin myös ajatella, että TSA 11 artiklan sallima poikkeus rekisteröidyn oikeuksien soveltamiseen ilmentäisi samanlaista velvoitteiden kohtuullistamista tilanteessa, jossa velvoitteet ja käytännön toimet ovat tunnistamattomuudesta johtuen epäsuhdassa.

SRB-ratkaisussa EUT näyttäisi selkeästi omaksuvan henkilötiedon käsitteeseen suhteellisen lähestymistavan. Oikeuskirjallisuudessa on todettu, että SRB-ratkaisu tuo uuden ja merkittävän näkökulman, sillä se on EUT:n tuomioista ensimmäinen, jossa selvästi vahvistetaan pseudonymisoitujen tietojen suhteellisuus.[364] Oikeuskirjallisuudessa on kuitenkin aiemmin luonnehdittu Breyer-ratkaisua yhdeksi suurimmista läpimurroista tietosuojasääntelyssä, sillä siinä on tunnistettu harmaa alue, jossa tiedot voivat olla samaan aikaan henkilötietoa ja ei-henkilötietoa.[365] Käytännössä SRB-ratkaisussa vahvistettu linja ei siten poikkea ainakaan merkittävästi aiemmasta tulkintalinjasta.[366]

---

[360] Julkisasiamies Spielmannin ratkaisuehdotus asiassa C-413/23 P (SRB), kohta 57. Julkisasiamies on siten tulkinnut asiaa samalla tavoin kuin EDPB pseudonymisointia koskevissa suuntaviivoissaan. Ks. EDPB 1/2025, s. 30 kohta 131.
[361] C-413/23 P (SRB), kohta 109.
[362] C-413/23 P (SRB), kohta 89.
[363] Julkisasiamies Spielmannin ratkaisuehdotus asiassa C-413/23 P (SRB), kohta 58.
[364] Rauhanen 2025, s. 658; Ks. myös Craddock 2025.
[365] Ks. El Khoury 2017, s. 192.
[366] Myös Suomen Sosiaali- ja terveysministeriö on nostanut henkilötiedon subjektiivisuuden esiin jo vuonna 2024 antamassaan linjauksessaan toteamalla, että henkilötietoluonteen toimijakohtaisuus rakentuu henkilötiedon käsitettä koskevaan EUT:n ratkaisukäytäntöön viitaten Breyer- ja Scania -ratkaisuihin. Ks. STM 2024, s. 3.

4.3.3 EU:n jäsenvaltioiden tuoretta tulkintaa

Myös Puolan korkein hallinto-oikeus (Naczelny Sąd Administracyjny, jäljempänä ’NSA’) on tarkastellut ratkaisussaan III OSK 2595/22 IP-osoitteiden ja evästeiden henkilötietoluonnetta. NSA:n mukaan tietosuojaviranomainen ei voi olettaa, että IP-osoitteet ja evästeiden tunnisteet olisivat aina henkilötietoja. Tietosuojaviranomaisen on osoitettava tapauskohtaisesti, että luonnollinen henkilö on TSA:n tarkoittamalla tavalla tunnistettavissa. NSA tulkitsi siten, että tunnistettavuus on tapauskohtaista eikä IP-osoitteen tai evästeiden käsittely johda aina luonnollisen henkilön tunnistamiseen.[367] Esimerkiksi IP-osoitteiden osalta pysyvien eli staattisten osoitteiden avulla pystytään välillisesti tunnistamaan sen käyttäjä, kun taas dynaamisten osoitteiden kohdalla vaaditaan internetpalveluntarjoajalta lisätietoja.[368]

NSA:n mukaan tunnistamisen mahdollisuuden arviointi on tehtävä tietojenkäsittelyn ajankohtana vallinneiden olosuhteiden perusteella. NSA on ratkaisunsa yhteenvedossa todennut, ettei viranomainen ollut asianmukaisesti selvittänyt olennaisia olosuhteita eikä osoittanut riittävästi, että kyseessä oli henkilötietojen käsittely. NSA on todennut, että vaikka IP-osoitteet ja evästeet ovat käytännössä usein henkilötietoja, ei tällaista johtopäätöstä voida tehdä ilman asianmukaista analyysiä. Tämä heijastaa myös EUT:n esittämää kantaa siitä, ettei tietosuojaviranomainen voi automaattisesti olettaa tiedon olevan henkilötietoa.[369] Tämä puolestaan herättää näyttötaakkaan liittyvän kysymyksen siitä, onko toimijan osoitettava tiedon olevan tälle anonyymiä, vai onko viranomaisen tehtävä osoittaa tiedon olevan henkilötietoa.

Saksan liittovaltion tuomioistuin on puolestaan jättänyt elokuussa 2025 EUT:lle ennakkoratkaisupyynnön asiassa C-654/25 (Undelam). Kansallinen tuomioistuin on pyytänyt EUT:ta selventämään, onko dynaaminen IP-osoite henkilötietoa, jos kolmas osapuoli voi tunnistaa käyttäjän vai onko tunnistettavuutta arvioitava henkilötietojen luovutukseen osallistuvien rekisterinpitäjän tai vastaanottajan näkökulmista. Lisäksi kansallinen tuomioistuin on pyytänyt EUT:n kannanottoa

---

[367] III OSK 2595/22; Ks. myös Konarski – Kupiec 2025. NSA tulkitsi asiaa linjassa SRB-ratkaisun kanssa.
[368] III OSK 2595/22. NSA on argumentointinsa tueksi vedonnut juuri Breyer-tapaukseen, jossa dynaamiset IP-osoitteet katsottiin henkilötiedoiksi vain, kun rekisterinpitäjä pystyi tosiasiallisesti ja realistisesti hankkimaan tunnistamista varten tarvittavia lisätietoja.
[369] C-413/23 P (SRB), kohta 47.

siihen, edellyttääkö tunnistettavuus hypoteettisia tunnistamiskeinoja vai tosiasiallista tunnistamista yksittäistapauksissa.[370] EUT ei ole antanut ennakkoratkaisupyyntöön vielä ratkaisua. Esitettyihin kysymyksiin vastatessaan EUT pystyy kuitenkin joko vahvistamaan suhteellista lähestymistapaa entisestään tai viemään tulkintaa painotukseltaan henkilötietojen suojan suuntaan.

Ranskan korkein hallinto-oikeus (Conseil d'État) on arvioinut pseudonymisoitujen henkilötietojen tunnistettavuuden kohtuullisen todennäköisiä keinoja. Ensinnäkin laajojen aineistojen yhdisteltävyys voi johtaa siihen, että ainakin osa rekisteröidyistä on tosiasiallisesti tunnistettavissa.[371] Lisäksi erilaisien kvasitunnisteiden ja muiden tietojen yhdisteleminen saattaisi kohtuullisin keinoin mahdollistaa tunnistamisen.[372] Tanskan tietosuojavaltuutettu on myös ottanut kantaa pseudonymisoidun henkilötiedon luonteeseen, mutta henkilötietojen käsittelijän näkökulmasta. Tietosuojavaltuutetun mukaan, jos rekisterinpitäjä on pseudonymisoinut henkilötiedon ja rekisterinpitäjällä säilyy relatiivinen avain, on tieto henkilötietoa myös henkilötietojen käsittelijälle niin kauan kuin se suorittaa käsittelytoimia rekisterinpitäjän lukuun.[373] Jos käsittelijä haluaa ryhtyä käsittelemään pseudonymisoitua tietoa omiin tarkoituksiinsa itsenäisenä rekisterinpitäjänä, pseudonymisoivan rekisterinpitäjän on varmistettava, että henkilötietojen luovuttamiseen on lainmukainen peruste. Tietosuojavaltuutettu antoi siten kannanottonsa SRB-ratkaisusta avoimeksi jääneeseen kysymykseen pseudonymisoitujen tietojen luovuttamisen oikeusperusteen tarpeellisuudesta. Tietosuojavaltuutetun mukaan on pseudonymisoivan rekisterinpitäjän tehtävänä huolehtia menettelyn lainmukaisuudesta ennen kuin se jakaa pseudonymisoitua tietoa käsittelijälle.[374]

5 Pseudonymisointi ja anonymisointi suhteessa rekisteröidyn oikeuksiin ja tietosuojan tavoitteisiin

5.1 Henkilötietoa vai ei? Pseudonymisoidun tiedon muuttuva luonne

Pseudonymisoinnin vaikutukset rekisteröidyn oikeuksien toteutumiseen pohjautuvat kysymykseen siitä, missä tilanteessa pseudonymisoitu henkilötieto lakkaa olemasta henkilötietoa. Pseudonymisoitu henkilötieto asettuu henkilötiedon ja anonyymin tiedon välimaastoon ja haastaa

[370] Ks. ennakkoratkaisupyyntö C-654/25 (Undelam), kohta 2. Ks. myös Konarski – Kupiec 2025.
[371] Conseil d'État asiat nro. 482872 (Criteo), kohta 12.
[372] Conseil d'État asiat nro. 498628 (GERS), kohdat 10–11. Ks. myös GERS-tapaukseen liittyvää analyysiä HSF Kramer 2026, jonka mukaan ratkaisussa kohtuullisen todennäköisiä keinoja tulkittiin tiukasti.
[373] Tanskan tietosuojavaltuutettu 2025.
[374] Tanskan tietosuojavaltuutettu 2025.

näiden välisen kahtiajaon. Toisin kuin anonymisointi, pseudonymisointi ei lähtökohtaisesti poista tiedon henkilötietoluonnetta, vaan ainoastaan vähentää tunnistettavuutta ja siihen liittyviä riskejä. Tuore oikeuskäytäntö viittaa siihen, että EU:ssa henkilötiedon ja anonyymin tiedon sekä samalla pseudonymisoidun ja anonymisoidun tiedon välinen rajanveto on kaventumassa.

Tietosuojaneuvoston pseudonymisointia koskevia suuntaviivoja sekä EUT:n antamaa SRB-ratkaisua on syytä verrata toisiinsa. SRB-ratkaisu vahvistaa henkilötiedon kontekstisidonnaisuuden. Tietosuojaneuvosto puolestaan korostaa, että pseudonymisoitu tieto on henkilötietoa niin kauan kuin tunnistaminen on mahdollista. Tietosuojaneuvosto painottaa kokonaisharkintaa sekä korostaa myös lisätietojen eli relatiivisen avaimen olemassaolon merkitystä. EUT:n tulkinta nojaa siihen, ettei TSA:n velvoitteita voida asettaa tahoille, jotka eivät tosiasiallisesti pysty tunnistamaan rekisteröityä. Tietosuojaneuvosto puolestaan korostaa perusoikeussuojan tehokkuutta sekä tunnistamisriskiä. SRB-ratkaisu luo pseudonymisoidun tiedon tulkintaan joustavuutta, mutta lisää samalla tulkinnallista epävarmuutta. Tietosuojaneuvoston suuntaviivat kuitenkin pyrkivät vähentämään epävarmuutta antamalla konkreettisia ohjeistuksia.[375] Erityisesti on kiinnitettävä huomiota, että EUT on ratkaisussaan selvästi painottanut enemmän henkilötietojen vapaan liikkuvuuden tavoitetta, kun tietosuojaneuvosto painottaa korkeatasoista henkilötietojen suojaa. Jos organisaatiot tulkitsevat SRB-ratkaisua liian laajasti ja kirjaimellisesti, ne voivat vedota relatiivisen avaimen puuttumiseen, vaikka tunnistamisriski olisi tosiasiassa olemassa.[376] Tällaisessa tilanteessa suuntaviivojen rooli voi olla tasapainottava. Näin ollen näitä voidaan pitää osin toisiaan täydentävänä.

Pseudonymisoitu henkilötieto voi muuttua anonyymiksi kahdella tavalla. Ensinnäkin se voidaan myöhemmin anonymisoida, jolloin anonyymiyden edellytysten täyttyessä siitä tulee anonyymiä kaikille.[377] On kuitenkin huomioitava, ettei pseudonymisointi itsessään ole anonymisointitekniikka, eikä tieto siten ”muutu” anonyymiksi, vaan se tarkoituksellisesti muutetaan sellaiseksi erillisellä toimenpiteellä. Toisaalta pseudonymisoitu henkilötieto voi lakata olemasta henkilötietoa tilanteessa, jossa pseudonymisoitua tietoa hallussaan pitävällä toimijalla ei ole kohtuullisen

---

[375] Suuntaviivat pääosin keskittyvät kuitenkin teoreettiseen ja tekniseen puoleen, eikä anna konkreettisia ja suoria vastauksia. Organisaatiot saattaisivat kaivata selkeämpää kriteeristöä, jotta suhteellisen henkilötietokäsitteen soveltaminen olisi kaikin puolin tarkoituksenmukaista.

[376] Kärjistettynä esimerkkinä tällaisesta tulkinnasta on seuraava: tietosuojalain 29.5 §:n mukaan rekisteröidyn henkilön tunnistamiseen ei saa käyttää yksinomaan henkilötunnusta tai henkilötunnuksen ja rekisteröidyn nimen yhdistelmää. Äärimmillään voitaisiin ajatella, että jos pelkän henkilötunnuksen avulla ei taholla olisi kohtuullisen todennäköisiä keinoja tunnistaa henkilöä, ei henkilötunnus näiden käsissä olisi enää henkilötietoa. Tällaista tulkintaa on kuitenkin pidettävä varsin epätodennäköisenä, sillä henkilötunnusta pidetään kuitenkin varsin vahvana tunnisteena.

[377] Ks. EDPB 1/2025, s. 10 kohta 22.

todennäköisesti toteutettavia keinoja eli relatiivista avainta yhdistää tietoa tiettyyn luonnolliseen henkilöön. Samalla on huomattava, että sinänsä anonyyminä pidettävä tieto voi myöhemmin muuttua takaisin henkilötiedoksi, jos relatiivinen avain tulee saataville. Näin voi tapahtua myös ilman toimijan aktiivista toimintaa, mikä korostaa riskiperusteista suhtautumista myös relatiiviseen avaimeen.

Sellaisen vastaanottajan näkökulmasta, jolla ei ole kohtuullisia keinoja saada relatiivista avainta, ei eroa pseudonymisoidun ja anonymisoidun tiedon osalta käytännössä ole. Vastaanottaja ei välttämättä edes ole tietoinen käytetystä toimenpiteestä, ellei sitä ole erikseen ilmoitettu. Tällä tiedolla on kuitenkin merkitystä vastaanottajan näkökulmasta ensinnäkin kohtuullisen todennäköisten keinojen, mutta myös jäännösriskin todennäköisyyden arvioimiseksi. Jotta vastaanottaja voi olla tietoinen siitä, käsitteleekö se pseudonymisoitua vai anonymisoitua tietoa, tulisi luovuttavan rekisterinpitäjän ilmoittaa vastaanottajalle, mikäli sillä on relatiivinen avain hallussaan. Mikäli vastaanottajan ei ole kohtuullisin keinoin mahdollista saada relatiivista avainta, ei tietosuojasääntelyä tarvitse soveltaa kummassakaan tapauksessa.

Jos pseudonymisoinnin jälkeen rekisteröityä ei voida tunnistaa ilman relatiivista avainta, toimenpidettä voidaan pitää onnistuneena. Tehokas pseudonymisointi voi kuitenkin johtaa siihen, että tieto jää tietosuojasääntelyn soveltamisalan ulkopuolelle. Jos siten tehokkaasta pseudonymisoinnista voi aiheutua vastaanottajan näkökulmasta anonymisointiin rinnastuva lopputulos, on perusteltua pohtia pseudonymisoinnin todellista merkitystä tietosuojatoimenpiteenä. Pseudonymisointi ja anonymisointi ovat erillisiä prosesseja, joilla tavoitellaan eri tasoisia intressejä.[378]

Vallitsevana oikeustilana voidaan pitää seuraavaa: pseudonymisoitu henkilötieto ei automaattisesti lakkaa olemasta henkilötietoa, muttei se myöskään ole henkilötietoa automaattisesti kaikille toimijoille. Ratkaisevaa on tapauskohtainen tunnistettavuuden arviointi, joka perusoikeusulottuvuutensa vuoksi edellyttää riskiperusteista lähestymistapaa. Suhteellista tulkintaa on sovellettu käytännössä jo ennen SRB-ratkaisua, minkä vuoksi ratkaisu ei itsessään merkittävästi muuta oikeustilaa ainakaan teoriassa. Käytännön vaikutukset voivat kuitenkin olla toisenlaisia. Oikeuskirjallisuudessa on esitetty, että kynnys tulkita pseudonymisoitu henkilötieto anonyymiksi

[378] Ks. pseudonymisoinnin ja anonymisoinnin merkityksestä tietosuojan tavoitteiden kannalta luku 5.3.

tiedoksi on SRB-ratkaisun jälkeen madaltunut. [379] Tämä voi vaikuttaa siihen, miten toimijat suhtautuvat henkilötiedon tunnistettavuuden arviointiin, ja hyödynnetäänkö pseudonymisoitua mutta anonyymiksi tulkittua tietoa ilman rajoituksia.

Toimijat voivat saada relatiivisia avaimia haltuunsa esimerkiksi tekoälyn avulla niin tarkoituksellisesti kuin myös vahingossa. Tekoälyn avulla on mahdollista yhdistää anonyymejä tietoja toisiinsa, jolloin yhdessä niistä voi muodostua henkilötietoa.[380] Tämä korostaa, että pseudonymisoidun tiedon vastaanottajan käytössä olevat tekniset menetelmät tulee olla suunniteltu ja rakennettu niin, ettei relatiivista avainta tahattomasti tai tarkoituksellisesti synny ja henkilötietojen suoja vaarannu. Tekoälysäädöksen ((EU) 2024/1689)[381] mukaan henkilötietojen suoja on taattava koko tekoälyjärjestelmän elinkaaren ajan.[382] Tekniset ja organisatoriset toimenpiteet tarkoittavat siten myös tekoälyn rakentamista, kouluttamista ja käyttöä ensinnäkin tietoturvallisella tavalla, mutta myös siten, että varaudutaan pseudonymisoidun tiedon dynaamiseen luonteeseen. Näin ollen tekoälyjärjestelmiä tulisi käsitellä kuten henkilötietoja eli riskiperusteisesta lähestymistavasta käsin. Tietosuojaneuvosto aikoo antaa tekoälysäädöksen ja TSA:n välistä vuorovaikutusta koskevat suuntaviivat, joissa olisi perusteltua huomioida pseudonymisoidun tiedon aiheuttamat tunnistamisriskit tekoälykontekstissa.[383]

5.2 Pseudonymisointi ja rekisteröidyn oikeudet

5.2.1 Pseudonymisoinnin vaikutus tiedonsaanti-, oikaisu- ja poistamisoikeuksiin

Suhteellinen henkilötietokäsite luo oikeudellista epävarmuutta sekä rekisteröidylle että pseudonymisoitua tietoa käsitteleville tahoille. Siinä missä anonymisointi poistaa tiedon tietosuojasääntelyn soveltamisalasta, [384] pseudonymisoinnin kohdalla ratkaisevaksi muodostuu tunnistettavuuden asteen arviointi, joka vaikuttaa suoraan rekisteröidyn oikeuksien toteutumiseen.

---

[379] Ks. Rauhanen 2025, s. 672.
[380] Ks. Sartor – Lagioia 2020, s. 36. Kyseinen tutkimus tarkastelee TSA:n ja tekoälyn välistä suhdetta; Ks. myös tekoälymallin anonymiteettiin liittyen EDPB 28/2024.
[381] Euroopan parlamentin ja neuvoston asetus (EU) 2024/1689, annettu 13 päivänä kesäkuuta 2024, tekoälyä koskevista yhdenmukaistetuista säännöistä ja asetusten (EY) N:o 300/2008, (EU) N:o 167/2013, (EU) N:o 168/2013, (EU) 2018/858, (EU) 2018/1139 ja (EU) 2019/2144 sekä direktiivien 2014/90/EU, (EU) 2016/797 ja (EU) 2020/1828 muuttamisesta (tekoälysäädös).
[382] Tekoälysäädöksen johdanto-osa 69 kappale.
[383] EDPB työohjelma 2026–2027, s. 7.
[384] On kuitenkin huomioitava, että jäännösriskin olemassaolon vuoksi toimija voi saada relatiivisen avaimen haltuunsa ja anonyymistä tiedosta voi vielä tulla henkilötietoa.

Tiedonsaantioikeuden osalta EUT on SRB-ratkaisussaan todennut, että rekisterinpitäjän velvollisuuksia on arvioitava jo henkilötietojen keräämisen yhteydessä.[385] Tässä arvioinnissa vastaanottajan mahdollisuuksilla saada käyttöönsä relatiivinen avain ei ole merkitystä. Rekisterinpitäjän velvollisuudet säilyvät siten riippumatta siitä, katsotaanko tieto vastaanottajan hallussa henkilötiedoksi. Pseudonymisoidun tiedon tunnistettavuudella ei näin ollen ole vaikutusta sellaisen rekisterinpitäjän velvollisuuksiin, joka pystyy tunnistamaan rekisteröidyn. EUT on pitänyt rekisterinpitäjän informointivelvollisuutta potentiaalisista vastaanottajista tärkeänä, jotta rekisteröity voi myöhemmin puolustaa oikeuksiaan suhteessa näihin ja päättämään tietoisena suostumuksensa antamisesta.[386] Tätä voidaan kuitenkin pitää ristiriitaisena, jos rekisteröidyn tulisi pystyä puolustamaan oikeuksiaan suhteessa vastaanottajaan niissäkin tilanteissa, joissa tieto nähdään anonyyminä.[387] Näin ollen voidaan todeta, että rekisteröidyn tiedonsaantioikeus toteutuu pseudonymisoitujen tietojen osalta suhteessa pseudonymisoivaan rekisterinpitäjään ja henkilötietojen käsittelijään, mutta oikeus ei välttämättä ulotu vastaanottajaan.

Oikaisuoikeuden toteutumista rajoittaa erityisesti se, miten rekisteröity voi osoittaa tiedon koskevan juuri häntä.[388] Vaikka vastaanottaja soveltaisi tietosuojasääntelyä, voi oikaisupyynnön toteuttaminen olla tosiasiassa haasteellista. Jos vastaanottaja ei pysty kohdistamaan oikaisupyyntöä oikeaan tietoon, aiheutuu siitä ensinnäkin riski kyseiselle rekisteröidylle, mutta väärän tiedon oikaisun vaikutukset saattavat myös ulottua toiseen henkilöön. Tämän vuoksi tietoja ei tule oikaista, ellei varmuudella voida yhdistää tietoa ja henkilöä toisiinsa.[389] Samalla on kuitenkin huomioitava, että myös tietojen oikaisematta jättäminen voi vaikuttaa niin rekisteröidyn kuin myös kolmansien oikeuksiin, sillä väärä tieto voi johtaa virheellisiin tunnistamisiin. Pseudonymisoidut tiedot tulee siten oikaista erityisesti silloin, jos tietojen käsittelyllä voi olla konkreettisia vaikutuksia henkilölle.

Poistamisoikeuden osalta pseudonymisointi voi ensinnäkin vähentää poistamisen tarvetta, koska rekisteröityyn kohdistuva riski on pienempi.[390] Tästä huolimatta rekisteröidyllä on oikeus saada tietonsa poistetuksi, ellei niiden säilyttämiselle ole muuta perustetta. Pseudonymisointi

---

[385] C-413/23 P (SRB), kohta 108.
[386] C-413/23 P (SRB), kohdat 108–109.
[387] Craddock 2025, luku IV; Ks. C-413/23 P (SRB), kohta 109.
[388] Ks. TSA 5 ja luku.
[389] Ks. Korpisaari ym. 2022, s. 202. TSA 12 artiklan mukaan rekisterinpitäjä voi pyytää rekisteröityä toimittamaan lisätiedot henkilöllisyytensä vahvistamiseksi. Tätä on pidettävä jopa velvollisuutena, jottei tiedonsaantioikeuteen nojaten anneta vääriä tietoja; Ks. myös Hintze 2018, s. 95.
[390] Näin on esimerkiksi, jos rekisterinpitäjä käsittelee pseudonymisoitua tietoa esimerkiksi oikeutetun edun perusteella.

toisaalta vaikeuttaa poistamista silloin, jos vastaanottaja ei tiedä, mitä tietoa tulisi poistaa. Poistamisoikeuden tosiasiallinen toteutuminen kytkeytyy samaan tunnistamisproblematiikkaan kuin tiedonsaanti- ja oikaisuoikeus; ilman relatiivista avainta rekisterinpitäjä ei kykene kohdistamaan pyyntöä oikeisiin tietoihin. Jos relatiivista avainta ei ole kohtuullisin keinoin mahdollista saada, on pseudonymisoitu henkilötieto toimijalle anonyymiä tietoa, eikä TSA:n mukaista velvollisuutta poistamiseen ole.

Toisaalta pseudonymisointi voi mahdollistaa tiettyjä poikkeuksia rekisteröidyn oikeuksiin myös tietosuojasääntelyn piirissä. TSA 11 artiklan mukaan rekisterinpitäjän ei tarvitse toteuttaa rekisteröidyn oikeuksia, jos se ei käsittelyn tarkoituksiin nähden tarvitse rekisteröidyn tunnistamista eikä sillä ole hallussaan relatiivista avainta ja se pystyy tämän osoittamaan. Tällainen tilanne voi syntyä esimerkiksi silloin, kun pseudonymisoitu henkilötieto luovutetaan vastaanottajalle, jolla ei ole käytännössä pääsyä relatiiviseen avaimeen.[391] Tämä tulee erottaa kohtuullisen todennäköisistä keinoista, joiden puuttuminen tekisi tiedosta toimijalle anonyymiä. TSA 11 artiklan mukainen tilanne on myös silloin, jos alkuperäinen rekisterinpitäjä tuhoaa lisätiedot, mutta tällä on vielä kohtuullisin keinoin pääsy relatiiviseen avaimeen.[392] Pseudonymisointi voi näin ollen mahdollistaa henkilötietojen hyödyntämisen ilman rekisteröidyn oikeuksien toteuttamista. Tämän voidaan katsoa osoittavan pseudonymisoinnin alkuperäistä tavoitetta keventää tietosuojasääntelyn velvoitteita. Rekisteröity voi kuitenkin vaikuttaa oikeuksiensa toteutumiseen toimittamalla lisätietoja. Tällöin oikeudet voivat tulla sovellettaviksi sekä TSA 11 artiklan tilanteissa, että anonyyminä pidettävän tiedon osalta. Lisäksi rekisterinpitäjä voi saada tiedon oikaisuista tai poistoista toisen rekisterinpitäjän kautta.[393]

Huomionarvoista on, miten suhteellinen lähestymistapa pseudonymisoituun henkilötietoon vaikuttaa arviointiin siitä, onko tieto a) tunnistamattomuudesta johtuen TSA 11 artiklan piirissä vai b) tunnistamattomuudesta johtuen anonyymiä. Ensimmäisen osalta ratkaisevaa on, että rekisterinpitäjällä ei ole arviointihetkellä relatiivista avainta hallussaan, mutta sellainen on kohtuullisin keinoin hankittavissa. Jälkimmäisen osalta arviointi perustuu puolestaan siihen, onko kohtuullisen todennäköisiä keinoja saada relatiivista avainta. Ensimmäisessä tilanteessa arvioidaan siten käytettävissä olevia keinoja, kun jälkimmäisessä myös potentiaalisia keinoja. Tämä osoittaa, että pseudonymisoidun tiedon henkilötietoluonne ei siten yksinään riitä takaamaan rekisteröidyn oi-

[391] Ks. Hintze 2018, s. 92.
[392] Ks. Hintze 2018, s. 92; Lisätietojen tuhoamisen osalta on huomioitava, että tämä ei automaattisesti muuta tietoja anonyymeiksi, minkä vuoksi TSA 11 artikla soveltuu tällaiseen tilanteeseen.
[393] TSA 19 artikla.

keuksien tehokasta toteutumista, vaan ratkaisevaa on aina tosiasiallinen tunnistettavuus. Pseudonymisointi voi toimia käytännössä mekanismina, joka rajoittaa rekisteröidyn oikeuksien toteutumista niin kauan kuin relatiivista avainta ei ole käytettävissä.

Pseudonymisoinnin vaikutus rekisteröidyn oikeuksiin on kaksijakoinen: yhtäältä se vahvistaa henkilötietojen suojaa, minkä vuoksi rekisteröidyn intressi tukeutua esimerkiksi oikaisu- tai poistamisoikeuteensa voi pienentyä, mutta toisaalta se voi heikentää rekisteröidyn oikeuksien tosiasiallista toteutumista. Rekisteröidyn oikeudet säilyvät selvästi suhteessa siihen toimijaan, jolla on pääsy relatiivinen avaimeen. Tällöin jopa kohtuullisin keinoin pääsy relatiiviseen avaimeen voi rajoittaa rekisteröidyn oikeuksia. Rekisteröidyn oikeudet katkeavat selvästi silloin, kun ei ole kohtuullisen todennäköisin keinoin mahdollista saada relatiivista avainta eli silloin, kun tieto muuttuu anonyymiksi. Rekisteröidyn mahdollisuus päästä oikeuksiinsa vaihtelee tunnistettavuuden asteesta riippuen. Voidaan katsoa, että mitä tehokkaammin pseudonymisointi suojaa yksityisyyttä, sitä vaikeampaa on rekisteröidyn päästä oikeuksiinsa.[394]

5.2.2 Toimijoiden roolit pseudonymisoidun tiedon käsittelyssä

Rekisteröidyn oikeudet toteutuvat suhteessa rekisterinpitäjään, jos tällä käytettävissään relatiivinen avain.[395] Tällaisessa tilanteessa rekisterinpitäjällä säilyy TSA:n rekisteröidyn oikeuksia koskevat velvoitteet. Jos rekisterinpitäjällä ei ole käytettävissä relatiivista avainta, mutta se on kohtuullisin keinoin saatavissa, rekisterinpitäjän velvollisuudet rekisteröidyn oikeuksien soveltamisessa rajoittuvat TSA 11 artiklan mukaisesti. Kohtuullisen todennäköisten keinojen puuttuessa toimija jää TSA:n soveltamisalan ulkopuolelle, jolloin tieto on rajoituksetta käytettävissä, ellei esimerkiksi sopimuksesta tai muusta sääntelystä muuta johdu. Tämä osoittaa, että toimijoiden rekisteröidyn oikeuksia koskevat velvollisuudet ovat tunnistettavuuden asteesta riippuen joko täysimääräisiä, osittaisia tai olemattomia.

Henkilötietojen käsittelijän osalta pseudonymisoidun tiedon on katsottu olevan henkilötietona, vaikkei käsittelijällä tosiasiassa olisi pääsyä relatiiviseen avaimeen.[396] Oikeuskirjallisuudessa on korostettu, että mikäli henkilötietojen käsittelijä ei enää tiedot vastaanotettuaan olisi henkilötie-

---

[394] On kuitenkin huomioitava, että koska henkilötiedolla on dynaaminen luonne, TSA:n säännökset voivat rekisteröidyn oikeuksia koskevine velvoitteineen tulla myöhemmin sovellettavaksi jäännösriskin myötä.

[395] SRB-ratkaisussa vastaanottajan näkökulma ei vaikuttanut luovuttajan ilmoitusvelvollisuuteen suhteessa rekisteröityyn. Näin ollen voidaan analogisesti tulkita, että luovuttajilla säilyvät myös muut TSA:n mukaiset velvollisuudet.

[396] Ks. Rauhanen 2025, s. 667–671. Ks. myös Tanskan tietosuojavaltuutettu 2025.

tojen käsittelijä, sille ei myöskään kohdistuisi käsittelijöille asetettuja velvoitteita, millä puolestaan voisi olla rekisteröidyn henkilötietojen suojalle vakavia seurauksia.[397] Tästä syystä henkilötiedon suhteellisuuden ei pitäisi ulottua rekisterinpitäjän jatkeena toimivaan henkilötietojen käsittelijään.[398] Päinvastainen tulkinta loisi mahdollisuuden kiertää henkilötietojen käsittelijöihin sovellettavia velvoitteita.[399] Tästä huolimatta pseudonymisointi voi merkittävästi supistaa henkilötietojen käsittelijöiden velvoitteita esimerkiksi rajoittamalla sen avustamisvelvollisuutta.[400] Suhteellisen henkilötietokäsitteen soveltuminen on perusteltua rajata koskemaan vain itsenäisiä toimijoita.[401] Tämän voidaan katsoa soveltuvan myös konsernin sisällä, koska konsernissa erillisten rekisterinpitäjien itsenäisyys on mahdollista.[402] TSA 28 artiklan mukainen henkilötietojen käsittelysopimus on tarpeellinen riippumatta siitä, onko käsittelijällä mahdollisuutta tunnistaa rekisteröityä.[403] Henkilötietojen käsittelijä voi saada relatiivisen avaimen esimerkiksi rekisterinpitäjän tietojärjestelmien kautta.[404] Näin on tilanteissa, joissa henkilötietojen käsittelijä toimii pseudonymisoivan rekisterinpitäjän tai sellaisen rekisterinpitäjän lukuun, jolla on relatiivinen avain. Jos kuitenkin henkilötietojen käsittelijä käsittelee pseudonymisoitua tietoa omiin tarkoituksiinsa tai rekisterinpitäjän ohjeiden vastaisesti, käsittelijä toimii itsenäisenä toimijana suhteessa tähän tietoon, jolloin arviointi kohdistuu siihen, onko sillä kohtuullisen todennäköiset keinot tunnistamiseen.[405]

---

[397] Rauhanen 2025, s. 659, esimerkkinä tällaisesta on rekisterinpitäjälle tietoturvaloukkauksista ilmoittamatta jättäminen.

[398] Craddock 2025, V.1.; Rauhanen 2025, s. 671. Rauhasen mukaan, jos rekisterinpitäjän ja käsittelijän väliseen suhteeseen sovellettaisiin suhteellista henkilötietokäsitettä, mahdollistaisi se keskeisten suojatoimien kuten tietoturvaloukkausten ilmoitusvelvollisuuden laiminlyönnin, ja tällä tavoin loisi aukon tietosuoja-asetuksen velvoiterakenteeseen. Tämä puolestaan olisi ristiriidassa TSA:n korkean tietosuojan tavoitteen kanssa. Suhteellisen henkilötietokäsitteen merkitys käsittelysopimusten osalta jää kuitenkin Rauhasen mukaan edelleen avoimeksi.

[399] Craddock 2025, V.1.

[400] Craddock 2025, V.1. Esimerkiksi pseudonymisoitujen tietojen kohdalla rekisterinpitäjä on jo huolehtinut turvallisuustoimista ennen tietojen jakamista henkilötietojen käsittelijälle, jolloin käsittelijän toteuttamien turvatoimenpiteiden laajuus voi olla rajatumpaa.

[401] Rauhanen 2025, s. 671. Ks. EDPB-EDPS 2/2026 s. 11, jossa sidosryhmät ovat kysyneet, että jos vastaanottaja käsittelee tietoja rekisterinpitäjän lukuun, onko se silti henkilötietojen käsittelijä, vaikkei tämä pysty tunnistamaan henkilöä.

[402] Craddock 2025, V.2. Craddock on todennut, että kilpailulainsäädännöstä johdetut periaatteet osoittavat konsernin sisäisen itsenäisyyden olevan mahdollista.

[403] Rauhanen 2025, s. 671.

[404] Rauhanen 2025, s. 671. Käsittelysopimusten tekeminen on siten nähty kannattavana, jotta voidaan varmistaa niin asianmukainen tietosuoja kuin riskienhallinta. Rauhanen on kannustanut käsittelysopimusten tekemiseen ainakin, kunnes EUT ottaa asiaan kantaa. Rauhanen on kuitenkin tuonut esiin sen mahdollisuuden, että EUT tulkitsisi asiaa toisin.

[405] Rauhanen on nostanut esille kriittisen kysymyksen siitä, soveltuuko suhteellisen henkilötietokäsitteen tulkinta myös tilanteisiin, joissa rekisterinpitäjä siirtää henkilötietojen käsittelijälle pseudonymisoitua aineistoa, ks. Rauhanen s. 658.

Luovuttavalla rekisterinpitäjällä on velvollisuus ilmoittaa rekisteröidylle vastaanottajista, jolloin rekisteröity tietää tietojensa siirtyneen pseudonymisoituina eteenpäin. Vastaanottaja ei kuitenkaan välttämättä kykene tunnistamaan rekisteröityä, eikä siten kohdentamaan rekisteröityä oikeisiin tietoihin – ei välttämättä edes rekisteröidyn toimittamilla lisätiedoilla. [406] Rekisteröity tarvitsee välikädeksi luovuttajan, joka puolestaan ilmoittaa oikaisuista tai poistoista vastaanottajalle TSA 19 artiklan mukaisesti. Mikäli vastaanottaja pitää tietoa henkilötietona, sillä on rekisterinpitäjänä tietosuojasääntelyn mukaiset velvoitteet. Sääntely ei kuitenkaan sovellu, jos vastaanottaja katsoo tiedon anonyymiksi, jolloin vastaanottaja voi sinänsä kieltäytyä vastaanottamasta relatiivista avainta tunnistamisen välttääkseen.[407] Tällaista voidaan hallita sopimuksellisin keinoin asettamalla vastaanottajalle velvoitteita ja rajoituksia pseudonymisoidun tiedon käyttämiselle.

Absoluuttinen tulkinta, jonka mukaan pseudonymisoitu henkilötieto olisi aina henkilötietoa kaikille toimijoille, voisi johtaa kohtuuttomiin ja vaikeasti toteutettaviin velvoitteisiin. [408] Tästä näkökulmasta on perusteltua, ettei rekisteröidyn oikeuksia tarvitse toteuttaa tilanteissa, joissa relatiivista avainta ei ole käytettävissä taikka kohtuudella käytettävissä. Tällainen on mahdollista jo nykysääntelyssä TSA 11 artiklan mukaisesti. Suhteellisen henkilötietokäsitteen korostuminen voi kuitenkin johtaa siihen, että toimijat tulkitsevat herkästi hallussaan olevan pseudonymisoidun tiedon anonyymiksi tiedoksi. Tällainen tulkinta voi aiheuttaa riskejä rekisteröidylle, mutta oikeudellisia seuraamuksia myös toimijalle itselleen. Tätä välttääkseen toimijat saattavat suhtautua pseudonymisoituihin tietoihin myös liian varovaisesti ja käsitellä pseudonymisoitua tietoa henkilötietona, jolloin toisaalta TSA 11 artikla keventää velvoitteita. Pseudonymisointi ja suhteellinen henkilötiedon käsite nostaa esiin myös kysymyksiä liittyen toimijoiden näyttötaakkaan pseudonymisoidun tiedon henkilötietoluonteesta. Tuoreen oikeuskäytännön perusteella tietosuojaviranomainen ei voi automaattisesti olettaa pseudonymisoidun tiedon olevan absoluuttisesti henkilötietoa kaikille toimijoille.[409] TSA 11 artiklan mukaisissa tilanteissa rekisterinpitäjällä on osoitusvelvollisuus siitä, ettei se kykene tunnistamaan rekisteröityä. Rekisterinpitäjällä on myös aina

[406] Ks. Craddock 2025, V.4. Ks. myös TSA 11 artikla rekisteröidyn oikeudesta toimittaa lisätietoja.
[407] Vrt. TSA 11 artikla, jonka mukaan rekisteröity voi oikeuksiinsa pääsemiseksi toimittaa rekisterinpitäjälle lisätietoja. Luovuttajan ilmoitus vastaanottajalle rekisteröidyn oikaisu- ja poisto-oikeuteensa vetoamisesta voi kuitenkin olla vastaanottajan kannalta merkittävä erityisesti jäännösriskin huomioimiseksi.
[408] Ks. julkisasiamies Spielmannin ratkaisuehdotus asiassa C-413/23 P (SRB), kohta 58.
[409] Ks. myös ICO 2022b, s. 5, jonka mukaan ei myöskään voi automaattisesti olettaa, että pseudonymisoitu henkilötieto on anonyymiä tietoa.

osoitusvelvollisuus siitä, että henkilötietojen käsittelyssä noudatetaan tietosuojasääntelyä. Mikäli tieto katsotaan toimijan hallussa anonyymiksi, tällaista osoitusvelvollisuutta ei kuitenkaan toimijalla ole.

5.3 Merkitys tietosuojasääntelyn tavoitteiden toteutumisessa

Tietosuojasääntelyn perusoikeudellinen ja taloudellinen tavoite ovat hyvin jännitteisessä suhteessa keskenään, koska niillä tavoitellaan vastakkaisia intressejä. Pseudonymisoinnilla vähennetään tunnistamisriskiä, kun anonymisoinnilla tunnistettavuus poistetaan. Molemmat ovat henkilötietojen suojaamiseen tarkoitettuja keinoja, mutta anonymisointia voidaan pitää henkilötietojen suojan kannalta tehokkaampana. Huomionarvoista on kuitenkin, että jäännösriski on olemassa niin pseudonymisoidun kuin anonymisoidunkin tiedon osalta, eikä anonymisointikaan ole siten täysin varmasti ja lopullisesti tunnistamatonta.

Pseudonymisoinnilla lähtökohtaisesti pyritään siihen, että tietoa voidaan myöhemmin hyödyntää. Anonymisoinnin jälkeen tiedon hyödynnettävyys muihin käyttötarkoituksiin heikkenee huomattavasti. Tästä hyödynnettävyyden näkökulmasta katsottuna pseudonymisoinnilla pyritään toteuttamaan henkilötietojen vapaan liikkuvuuden näkökulmaa. Suhteellisella suhtautumisella lisätään henkilötietojen laajaa hyödynnettävyyttä, mutta samalla se luo epäselvyyttä rekisterinpitäjille ja vastaanottajille omista velvollisuuksistaan tietosuojasääntelyn velvoitteiden toteuttamisessa.[410]

Absoluuttisen ja suhteellisen henkilötietokäsitteen rajanvedolla on merkitystä tietosuojan tavoitteiden painotuksen kannalta. Kuten todettu aiemmin, SRB-ratkaisulla on ollut enemmän henkilötietojen vapaan liikkuvuuden painotus, kun taas esimerkiksi tietosuojaneuvoston suuntaviivoilla on enemmän henkilötietojen suojaa painottava ote. Siten voidaan katsoa niiden täydentävän toisiaan, sillä tietosuojasääntelyssä ei ole asetettu tavoitteiden välille hierarkiaa. Jos pseudonymisoitua tietoa ei pidetä henkilötietona, ei myöskään esimerkiksi TSA 35 artiklan mukaista vaikutustenarviointia tarvitse tehdä. Tämän vuoksi esimerkiksi tekoälyn hyödyntäminen aiheuttaa henkilötietojen suojan kannalta merkittävän haasteen. Tekoälyn avulla toimija voi lopulta päätyä avaamaan tunnistettavuuden lukon, vaikkei sitä olisi edes tavoitellut.

Jännite tietosuojan tavoitteiden ja suhteellisen henkilötietokäsitteen välillä voi ilmetä käytännössä siten, että organisaatiot joko varmuuden vuoksi kohtelevat kaikkea tietoa henkilötietona,

---

[410] Ks. Rauhanen 2025, s. 672, jonka mukaan suhteellisen henkilötiedon käsitteen osalta on vallinnut epäselvyyttä, vaikka sillä onkin ollut vahva jalansija.

mikä rajoittaa tietojen hyödyntämistä, tai vaihtoehtoisesti käsittelevät tunnistettavissa olevaa tietoa anonyyminä, mikä vaarantaa henkilötietojen suojaa. Pseudonymisoinnilla on kuitenkin tarkoitus pyrkiä tavoitteiden tasapainon saavuttamisen. Myös TSA:ssa kannustetaan toimijoita hyödyntämään pseudonymisointia. Suhteellisen henkilötietokäsitteen mukainen pseudonymisoidun tiedon tulkinta on painotukseltaan enemmän henkilötietojen vapaan liikkuvuuden puolella. Suhteellisuuden voidaan katsoa turvaavan enemmän ei pelkästään EU:n sisämarkkinallista tavoitetta, vaan markkinalähtöistä ajattelua laajemmin.

Ennen Lissabonin sopimusta taloudellisella tavoitteella oli suurempi painotus EUT:n ratkaisukäytännössä, joskin tämä johtui EU:n toimivaltakysymyksistä perusoikeuksiin puuttumisessa.[411] Tämän jälkeen oikeuskirjallisuudessa on havaittu EUT:n painottavan enemmän perusoikeuksia.[412] Tähän on selvästi tullut muutos SRB-ratkaisun jälkeen, jossa painotus näyttää enemmän olevan henkilötietojen vapaan liikkuvuuden tavoitteessa. Näin ollen voidaan todeta, että suhteellisella henkilötiedon tulkinnalla palataan käytännössä lähemmäs taloudellisen painotuksen aikaan. Tunnistettavuuden arvioinnin kontekstisidonnaisuuden korostamista tulisi siten välttää, sillä liika korostaminen voi johtaa henkilötietojen vapaan liikkuvuuden painotukseen. Koska teknologia ja sitä myöten tunnistamisen mahdollisuudet kehittyvät koko ajan, on tällaisen painotuksen suhteen oltava varovainen. Tulee ennemmin painokkaammin korostaa, että pseudonymisoinnin tarkoituksena on turvata molempia tavoitteita samanaikaisesti, mutta punnintatilanteessa on vaakakupin kallistuttava henkilötietojen suojan puolelle perusoikeutena.

5.4 Sääntelymallin tarkoituksenmukaisuuden arviointi

5.4.1 Henkilötiedon käsite tulevaisuudessa: Digital Omnibus

Euroopan komission marraskuussa 2025 julkaistussa Digital Omnibus -lainsäädäntöaloitteessa ehdotetaan henkilötiedon käsitteen tarkentamista. Digital Omnibusissa on ehdotettu lisättävän TSA:n henkilötiedon määritelmään, että luonnollisia henkilöitä koskevat tiedot eivät välttämättä jonkun toisen tahon hallussa henkilötietoja, jos tällä ei ole tapoja tunnistaa luonnollista henkilöä. Lisäksi ehdotetaan, että tällaisista tiedoista ei tulisi kyseisen tahon kannalta henkilötietoja pelkästään sen vuoksi, että mahdollisella myöhemmällä vastaanottajalla on kohtuullisen todennäköiset keinot tunnistaa henkilö.[413] Käytännössä muutoksen taustalla on tahtotila kodifioida SRB-

[411] Ks. Raitio 2016, s. 202. Raitio on kuvannut EU:n tavoitteilla olleen ”talouspainotteinen pohjavire”.
[412] Ks. esim. Ollila 2014; Lynskey 2013; Lindroos-Hovinheimo 2018.
[413] COM (2025) 837 final, 3 artikla.

ratkaisussa vahvistettu lähestymistapa, mutta ratkaisun ja aloitteen julkistamisen välinen ajallinen yhteys viittaisi siihen, ettei pelkästään SRB-ratkaisu olisi muutoksen taustalla.[414] Kuten aiemmastakin oikeuskäytännöstä ja linjauksista on havaittavissa, on tällainen suhteellinen lähestymistapa ollut ainakin jossain määrin vallitseva oikeustila jo aiemmin – joskin SRB-ratkaisu on tätä vahvistanut.[415] Digital Omnibusilla on myös tarkoitus antaa komissiolle valta säätää täytäntöönpanosäädöksiä siitä, milloin pseudonymisoitua tietoa ei pidettäisi tiettyjen toimijoiden osalta henkilötietona.[416] Toisin sanoen komissiolle on ehdotettu annettavan valtaa säätää täytäntöönpanosäädöksillä tarkemmin tietosuojasääntelyn soveltamisalasta.

Euroopan tietosuojaneuvosto sekä Euroopan tietosuojavaltuutettu ovat helmikuussa 2026 antaneet yhteisen lausunnon Digital Omnibusista, jossa ovat esittäneet näkemyksensä muutosten vaikutuksista ihmisten perusoikeuksille, oikeusvarmuudelle ja tietosuojalainsäädännön käytännön soveltamiselle.[417] Lausunnossa tietosuojaneuvosto ja tietosuojavaltuutettu ovat ensinnäkin todenneet, että muutokset johtaisivat henkilötietokäsitteen merkittävään kaventumiseen ja muutoksilla luotaisiin epävarmuuksia niin käytännön soveltamiselle kuin rekisteröidyn oikeuksien toteutumiselle sekä vaarannettaisiin henkilötietojen suojaa.[418] Tämän lisäksi lausunnossa on tunnistettu, että ehdotettu muutos saattaisi kannustaa rekisterinpitäjiä etsimään porsaanreikiä tietosuojasääntelyn soveltamisesta.[419] Tunnistamista ja sääntelyä olisi entistä helpompi kiertää keinotekoisesti ja siitä huolimatta suorittaa käsittelytoimia.[420] Lausunnon mukaan komissiolle ei tulisi antaa valtuuksia säätää ehdotettuja täytäntöönpanosäädöksiä, sillä ne vaikuttaisivat myös komission velvoitteisiin.[421] Täytäntöönpanosäädösten käytännön vaikutus voisi luoda myös enemmän epäselvyyttä, mikä on ristiriidassa Digital Omnibusin sääntelyn yksinkertaistamistavoitteen kanssa.[422]

---

[414] Ehdotuksessa kuitenkin vedotaan oikeuskäytäntöön, kuitenkaan yksittäistapausta nimeämättä. Ks. COM (2025) 837 final, s. 10–11.
[415] Ks. myös Rauhanen 2025, s. 671—672, jonka mukaan emme ole siirtyneet SRB-tuomion jälkeen ”uuteen aikakauteen”, sillä se edellyttäisi merkittävää vallitsevan käsitteen muuttumista, mitä tässä tapauksessa ei ole tapahtunut.
[416] COM (2025) 837 final. 41 a artikla, jolla annettaisiin komissiolle valtuudet hyväksyä täytäntöönpanosäädöksiä, joissa vahvistettaisiin tekniset toimenpiteet ja arviointikriteerit pseudonymisoidun tiedon henkilötietoluonteen arvioimiseksi. Ks. täytäntöönpanosäädöksistä SEUT 291 artikla ja Talus – Penttinen 2016, s. 230.
[417] EDPB-EDPS 2/2026 s. 4.
[418] EDPB-EDPS 2/2026 s. 10 kohta 17 ja s. 8 kohta 6.
[419] EDPB-EDPS 2/2026 s. 10 kohta 17; Tässä on riski, että rekisterinpitäjät toteuttaisivat näennäisesti toimenpiteitä erottaakseen käsittelytoimet kohtuullisen todennäköisistä keinoista tunnistaa henkilö.
[420] Purtova 2025.
[421] Ks. EDPB-EDPS 2/2026 s. 12 kohta 23.
[422] Ks. EDPB-EDPS 2/2026 s. 12 kohta 24.

Lausunnossa myös korostetaan, ettei Digital Omnibusissa ehdotettu henkilötiedon käsitteen muutos olisi täysin linjassa EUT:n ratkaisukäytännön kanssa.[423] SRB-ratkaisussa esitetyt kannanotot ovat ensinnäkin annettu konkreettisesti jotakin taustaa vasten, kun Digital Omnibusin muutosta ehdotetaan sääntelyn tasolle soveltumaan kaikkiin tilanteisiin. SRB-ratkaisussa EUT on katsonut, että tieto on välillisesti henkilötietoa myös luovuttajalle, jos se on henkilötietoa vastaanottajalle.[424] Digital Omnibusilla tätä vastoin ehdotetaan, ettei luovuttajan osalta tieto muutu henkilötiedoksi vain siksi, että mahdollisella myöhemmällä vastaanottajalla on tai on kohtuullisin keinoin mahdollisuus saada relatiivinen avain. Voidaan siten todeta, että ehdotettu muutos on jopa SRB-ratkaisussa omaksuttua linjaa tiukempi.

Lausunnon mukaan ehdotetuilla muutoksilla on negatiivisia vaikutuksia oikeusvarmuuden kannalta.[425] Vaikka EU:ssa sääntelyä monesti tulkitaan teleologisen tulkinnan avulla, on sanamuotokin äärimmäisen tärkeä. Lausunnossa on esitetty huomio, että henkilötiedon käsitteen muuttamisella voi olla seurauksia myös muiden EU-lähteiden tulkintaa ajatellen ja voi näin vaikuttaa negatiivisesti koko EU-oikeuden koherenssiin.[426] Myös oikeuskirjallisuudessa on katsottu henkilötiedon käsitteen kaventamisen aiheuttavan pikemminkin uusia ongelmia, sillä merkittävä osa EU:n muusta digi- ja teknologiasääntelystä nojaa tietosuoja-asetukseen.[427]

Myös jäsenvaltiot ja sidosryhmät ovat ottaneet ehdotuksiin kantaa. Suomen valtioneuvosto suhtautuu lähtökohtaisesti myönteisesti anonymisointia ja pseudonymisointia koskevien tulkintaepävarmuuksien selventämiseen.[428] Valtioneuvosto ja perustuslakivaliokunta ovat kuitenkin todenneet, että huomiota tulee kiinnittää ensinnäkin henkilötietojen määritelmään, mutta myös anonymisointiin ja pseudonymisointiin liittyviin muutoksiin siten, että ne olisivat riittävän selkeitä ja tarkkarajaisia.[429] Henkilötiedon määritelmän muuttamisella voi olla laajoja vaikutuksia henkilötietojen suojalle, minkä vuoksi tulee huolellisesti arvioida uuden määritelmän seurauksia ja suhtautua muutokseen kriittisesti.[430] Täytäntöönpanovallan delegoimisesta komissiolle valtioneuvosto on korostanut, että myös sen tulee olla tarkoituksenmukaista, riittävän tarkkarajaista

---

[423] EDPB-EDPS 2/2026, s. 10 kohta 16; Ks. myös Purtova 2025. Purtovan näkemyksen mukaan ehdotetut muutokset eivät tosiasiassa kodifioisi SRB-ratkaisua, vaikka näin väitetään. Ks. esim. Konarski – Kupiec 2025.
[424] C-413/23 P (SRB) kohta 85.
[425] EDPB-EDPS 2/2026, s. 10 kohta 15.
[426] EDPB-EDPS 2/2026, s. 11 kohta 20.
[427] Purtova 2025; Ks. PeVL 7/2026 vp, kohta 7, jonka mukaan muutokset aiheuttavat heijastevaikutuksia sääntelyyn laajemmin.
[428] U 81/2025 vp, luku 6.1.
[429] PeVL 7/2026 vp, kohta 9.
[430] PeVL 7/2026 vp, kohta 9.

ja täsmällistä.[431] Perustuslakivaliokunta on tietosuojaneuvoston ja tietosuojavaltuutetun tavoin pitänyt kuitenkin ongelmallisena, että komissio pystyisi suoraan vaikuttamaan tietosuojasäänte-lyn soveltamisalaan, ja että ehdotuksella siirrettäisiin tapauskohtaisesti soveltamisalan määrit-tely kansallisilta tietosuojaviranomaisilta komissiolle.[432] Täytäntöönpanosäädöksiä ei ole pidetty asianmukaisena myöskään yksilön oikeuksien tai toimijoiden velvollisuuksien osalta.[433]

On syytä pohtia, onko tarkoituksenmukaista lähteä kodifioimaan suhteellista henkilötietokäsi-tettä lainkaan. Nykyinen tietosuojasääntely kuitenkin sallii suhteellisen lähestymistavan. EUT:n on mahdollista tehdä tulkintalinjauksia, joilla on vahva ohjausvaikutus jäsenvaltioissa, ja tieto-suojaneuvoston ohjeistuksilla on tyypillisistä soft law -aineistoista poiketen merkittävä rooli tul-kintakysymyksissä. Avoimilla normeilla lisätään tulkinnanvaraisuutta, joka voi ilmetä epäjohdon-mukaisina soveltamiskäytänteinä. Verkottuneessa yhteiskunnassa kuitenkin ilmenee jatkuvasti uusia relatiivisen avaimen muotoja, joten avoimilla normeilla pystytään varautumaan siihen, ett-eivät nämä jää tietosuojasääntelyn ulkopuolelle. Digital Omnibusin ehdotukset väistämättä tar-koittavat, että tahtotilana on painottaa taloudellista näkökulmaa perusoikeuspainotuksen si-jaan. Lopullista muutosta ja sanamuotoa on kuitenkin vielä hankala ennustaa, mutta ottaen huo-mioon ehdotuksesta annetut lausunnot, ei ehdotettu muutos henkilötiedon käsitteeseen toden-näköisesti astu voimaan.

Euroopan tietosuojaneuvosto on myös julkaissut ohjelmansa vuosille 2026–2027 toteuttaakseen vuosien 2024–2027 strategiaansa.[434] Tietosuojaneuvoston yhtenä tavoitteena on turvata henkilö-tietojen suoja nykyisessä digitalisoituvassa ympäristössä.[435] Strategian mukaan tietosuojaneu-vosto laatii parhaillaan ohjeita muun muassa henkilötietojen anonymisoinnista ja pseu-donymisoinnista.[436] Näissä ohjeissa on tarkoitus huomioida myös SRB-ratkaisu antamalla lisä-ohjeita siitä, miten SRB-ratkaisu vaikuttaa esimerkiksi henkilötietojen siirtoihin kolmansiin mai-hin, yhteisrekisterinpitäjyyteen sekä henkilötietojen käsittelijän rooliin.[437] Julkisasiamies Spiel-mann on viitannut tietosuojatyöryhmän nimensä mukaisesti anonymisointitekniikoita koskevaan lausuntoon ”anonymisointi- ja pseudonymisointitekniikoita” koskevana lausuntona, [438] joka to-

[431] PeVL 7/2026 vp, kohta 12.
[432] PeVL 7/2026 vp, kohta 14.
[433] PeVL 7/2026 vp, kohta 15.
[434] EDPB työohjelma 2026–2027, s. 2.
[435] EDPB työohjelma 2026–2027, s. 7.
[436] EDPB työohjelma 2026–2027, s. 3.
[437] Ks. EDPB-EDPS 2/2026, s. 11 kohta 19.
[438] Julkisasiamies Spielmannin ratkaisuehdotus asiassa C-413/23 P (SRB), alaviite 20.

siasiassa kattaa molemmat toimenpiteet. Koska toimenpiteet ovat hyvin lähellään toisiaan – erityisesti suhteellisesta lähtökohdasta tulkiten – olisi perusteltua ennemmin antaa yhteinen lausunto koskien molempia toimenpiteitä. Näiden erillään pitäminen tuskin saa aikaan tavoiteltua lopputulosta ottaen huomioon myös, että merkittävimmät rajanveto- ja tulkintaongelmat liittyvät nimenomaan pseudonymisoituun tietoon.

5.4.2 Haastava yhtälö: toimiva sääntely vs. tavoitteiden tasapaino

Kaikille EU:n jäsenvaltioille yhteinen oikeusvarmuuden periaate edellyttää, että oikeussääntöjen tulee olla selviä, täsmällisiä ja vaikutuksiltaan ennakoitavia. EUT:n ratkaisukäytännössä oikeusvarmuuden määrittelyssä on erityisesti korostettu ennakoitavuutta etenkin silloin, kun sääntelyllä voi olla epäedullisia seurauksia luonnollisille henkilöille tai oikeushenkilöille.[439] Ennakoitavuudella on suuri merkitys henkilötietojen suojan näkökulmasta, sillä luonnollisten henkilöiden tulee voida arvioida henkilötietoihinsa kohdistuvia käsittelytoimia perusoikeuksiensa turvaamiseksi. Yleisesti EU:n asetuksilla pyritään poistamaan tulkintavaihtoehtoja ja yhdenmukaistamaan soveltamista jäsenvaltioissa,[440] minkä vuoksi toimijoiden tulee voida tunnistaa sovellettavat normit ja rekisteröityjen heille kuuluvat oikeudet. Sääntelyn ei tulisi olla reaktiivista, vaan sen tulisi ennakoivasti huomioida teknologisen toimintaympäristön muutoksista aiheutuvat uudet riskit henkilötietojen suojan turvaamiseksi.[441] Teknologinen kehitys luo niin sanotun lainsäätäjäriskin, jossa sääntely jää jälkeen ja vaatii nopeita muutoksia toimintaympäristön haasteisiin vastaamiseksi.[442] Tästä näkökulmasta henkilötiedon käsitteen kaventaminen ei ole perusteltu ratkaisu, sillä uusia tunnistamisen mahdollisuuksia syntyy jatkuvasti – emmekä ole kaikista vielä edes tietoisia.[443]

Nykyinen tietosuojasääntely rakentuu kahtiajakoon henkilötiedon ja anonyymin tiedon välillä.[444] Henkilötiedon käsitteen tulkinta on kehittynyt suhteellisempaan suuntaan, mikä on lisännyt joustavuutta, mutta samalla heikentänyt ennakoitavuutta. Tietosuojasäänteln tavoitteiden tasapai-

---

[439] Raitio 2017, s. 88; Ks. myös Raitio 2017, s. 84, jonka mukaan oikeusturvaodotukseen liittyy, että päätösten tulee vastata kyseessä olevan oikeuskulttuurin vakiintuneita arvoja ja tietoja todellisuudesta.
[440] Tämä on myös ollut tietosuoja-asetukseen siirtymisen taustalla.
[441] Ks. Andersson 2024, s. 359. Andersson on ottanut kantaa hyvään tietoturvan sääntelyjärjestelmään.
[442] Andersson 2024, s. 4. Andersson kuvaa lainsäätäjäriskiä Saarenpäätä ja Riekkistä (2023, s. 201–202) lainaten siten, että lainsäätäjä ei ole oikealla tavalla tai ajoissa havahtunut lainsäätämistarpeeseen.
[443] Purtova 2018, s. 44.
[444] Hintze on nähnyt kahtiajaon aiheuttavan ongelmia siten, että jos henkilötietoja ei ole käsittelytarkoitusten saavuttamiseksi mahdollista anonymisoida, ei rekisterinpitäjä ole välttämättä riittävän motivoitunut vähentämään tunnistamisriskejä pseudonymisoinnilla. Tällöin tiedot saatetaan säilyttää tarpeettomasti täysin tunnistettavassa muodossa, mikä vaikuttaa henkilötietojen suojaan. Ks. Hintze 2018, s. 89.

nolle on siten muodostunut haaste. Henkilötietojen suojaa ei voida heikentää kaventamalla henkilötiedon käsitettä. Samalla sääntelyn tulee mahdollistaa tietojen tehokas hyödyntäminen niin tutkimus- ja innovaatiotoiminnassa kuin markkinoilla liiketoiminnallisissa tarkoituksissa. Kyse on siten perusoikeudellisen ja taloudellisen tavoitteen välisestä intressipunninnasta.[445]

Oikeuskirjallisuudessa on esitetty kritiikkiä sekä henkilötiedon käsitteen laajuudesta että siitä, että TSA:sta on muodostunut eräänlainen yleislaki kaikkiin digitaalisiin ongelmiin. Tämä on johtanut epätarkkaan sääntelyyn.[446] Henkilötiedon määritelmää ei ole myöskään pidetty hyvänä ankkurina oikeussuojalle. Koko järjestelmä rakentuu henkilötiedon käsitteen varaan, vaikkeivat digitaaliset haitat tosiasiassa riipu aina tunnistettavuudesta.[447] Näin järjestelmästä voi muodostua epävakaa ja manipuloinnille altis.[448] Tämän vuoksi oikeuskirjallisuudessa on ehdotettu sääntelyn hajauttamista eri konteksteihin.[449] Digitaalisen ympäristön riskit tulisi siten ottaa laaja-alaisesti huomioon eri säädöksissä. Näiden huomioiminen pelkästään TSA:ssa ei riitä, sillä TSA niin sanottuna yleislakina ei voi ottaa huomioon yksityiskohtaisesti eri sektorien riskitekijöitä. Esimerkiksi tekoälyjärjestelmät voivat tunnistaa henkilön ja tehdä yksilöön vaikuttavia johtopäätöksiä, vaikka tekoälylle syötetyt tiedot olisivat anonyymejä. Pseudonymisoiduista ja anonymisoiduista tiedoista voidaan tehdä analyysejä, joiden haitat voivat kohdistua ihmisryhmiin ilman tietyn henkilön tunnistamista. Digitaaliset riskit voivat siten syntyä myös tilanteissa, joissa tunnistettavuus ei ole keskiössä.

TSA:n ollessa niin sanottu yleislaki kaikelle henkilötietojen käsittelylle, voidaan myös pohtia, onko tarkoituksenmukaista, että anonymisoinnin nimenomainen rooli on TSA:ssa lähes olematon. Anonymisointia käsitteenä ei ole mainittu TSA:ssa lainkaan, vaikka sen voidaan katsoa sisältyvän TSA 26 johdantokappaleeseen. Tästä huolimatta anonymisointi on merkittävä henkilötietojen suojaa turvaava toimenpide, ja muissa säädöksissä sitä on korostettu ensisijaisena toimenpiteenä suhteessa pseudonymisointiin. Vaikka kaikkia toimenpiteitä henkilötietojen suojaamiseksi ei ole tarkoituksenmukaista sääntelyn tasolla määritellä, voisi anonymisointiprosessin määritteleminen vähentää pseudonymisointiin ja anonymisointiin liittyviä tulkintaongelmia etenkin suhteellisen henkilötiedon käsitteen korostuessa.

---

[445] Ajatuksena tätä voisi verrata oikeutetun edun arvioinnissa tehtävään tasapainotestiin.
[446] Purtova 2025; Ks. myös Koops 2014, s. 256–259.
[447] Purtova 2025.
[448] Purtova 2025.
[449] Purtova 2025.

Oikeuskirjallisuudessa on esitetty ”potentiaalisen henkilötiedon” käsitettä, joka kuvastaisi henkilötiedon dynaamista luonnetta ja erityisesti pseudonymisoidun tiedon asemaa kahtiajaon välissä.[450] Tällainen välikategoria – jossa pseudonymisoitu henkilötieto on käytännössä jo ollut – voisi korostaa pseudonymisoinnin alkuperäistä tarkoitusta keventää tietosuojasääntelyn velvoitteita ja edistää tiedon hyödyntämistä ilman, että henkilötietojen suoja tai ennakoitavuus vaarantuu. Potentiaalisen henkilötiedon tunnustamisella olisi siten mahdollista nostaa pseudonymisoitu henkilötieto pois ”harmaalta alueelta”. Tällaisen kategorian käyttöönotto edellyttäisi kuitenkin huolellista arviointia sen oikeudellisesta asemasta ja riskeistä. Nopealla aikataululla syntyneet sääntelymuutokset voivat käytännön toiminnassa ilmetä tulkinnallisina ongelmina puutteellisen sääntelyn myötä.[451]

Pseudonymisoidun tiedon asettuminen henkilötiedon ja anonyymin tiedon välimaastoon lisää tulkinnallista epävarmuutta ja voi johtaa siihen, että samaa tietoa koskevat rekisteröidyn oikeuksia koskevat velvoitteet ovat eri toimijoilla joko täysimääräiset, osittaiset TSA 11 artiklan nojalla tai täysin olemattomat. Toimijoiden tulisi tunnistaa ja pitää säännöllisesti mielessä pseudonymisoidun tiedon dynaaminen luonne: sinänsä anonyymistä tiedosta voi tulla henkilötietoa ajan kuluessa ja teknologian kehittyessä. Jäännösriski on yhtä lailla olemassa myös anonymisoidun tiedon kohdalla, vaikka anonymisoinnin tarkoituksena on viedä henkilötietojen suoja pseudonymisointia pidemmälle. Pseudonymisoidun tiedon osalta tuleekin tunnistamisriskiin suhtautua vakavasti, sillä avain on lista tuoda sääntelyssä esiin, jotta korostettaisiin dynaamista luonteen riskejä henkilötietojen suojalle. Riskit kohdistuvat kuitenkin erityisesti pseudonymisoituun, mutta anonyyminä pidettävään tietoon, johon ei tietosuojasääntely sovellu.

Nykyisen pseudonymisoidun tiedon arviointikriteerin voidaan katsoa muodostuvan relatiivisen avaimen kautta: jos toimijalla on relatiivinen avain tai kohtuullisen todennäköisin keinoin pääsy relatiiviseen avaimeen, on pseudonymisoitu tieto henkilötietoa tälle toimijalle. Tämän arvioimiseksi ja virheellisten tulkintojen välttämiseksi olisi syytä antaa jatkossakin tietosuojaneuvoston ohjeistuksia.[452] Alati kehittyvässä toimintaympäristössä uusia tunnistamisen muotoja on hankala ennustaa, minkä vuoksi neuvoa-antavilla ohjeistuksilla on potentiaalia toimia tavoitteiden välisen tasapainon saavuttamisessa.

---

[450] Ks. Craddock 2025, V.3. Ks. ns. epäsuorasta henkilötiedosta myös El Khoury 2017, s. 192.
[451] Andersson 2024, s. 4.
[452] Kuten aiemmin todettu, neuvoa-antavana elimenä tietosuojaneuvoston antamilla ohjeistuksilla ei ole kuitenkaan sitovaa painoarvoa, toisin kuin Digital Omnibusissa esitetyillä komission täytäntöönpanosäädöksillä olisi.

Lisäksi voidaan kysyä, onko tarkoituksenmukaista, että arviointi onnistuneesta pseudonymisoinnista sekä henkilötiedon ja anonyymin tiedon välisestä rajanvedosta perustuisi pitkälti soft law -aineistoon – vaikka EUT:n ratkaisukäytännön merkitys tunnistettavuuden tulkinnassa onkin merkittävä. Tietosuojaneuvoston ohjeistuksilla on tosiasiallista merkitystä, vaikka ne soft law -aineistona ovatkin oikeuslähdehierarkiassa niin sanotun sallitun oikeuslähteen asemassa. Muuttuvassa toimintaympäristössä tulisi mahdollistaa sitovuudeltaan ja hierarkialtaan erilaisten normistojen toisiaan täydentävä ja johdonmukainen vuorovaikutus.[453] Koska nykyinen tietosuojasääntely sallii tällaisen dynaamisen ja suhteellisen henkilötiedon tulkinnan, ei käsitteen tai rajanvedon tarkentaminen sekundäärioikeuteen ole tarkoituksenmukaista.

Oikeuskirjallisuudessa on esitetty sopimuksellisia keinoja, joilla tunnistaminen kielletään tai vähintään muistutetaan vastaanottajaa tämän vastuusta varmistaa tietosuojasääntelyn noudattaminen siltä osin kuin se on tilanteeseen sovellettavissa.[454] Sopimuksella mahdollistettaisiin tarkoituksenmukainen rekisteröidyn oikeuksien turvaaminen, mutta myös rajattaisiin hyödyntämistä. Oikeuskirjallisuudessa on kuitenkin katsottu, ettei tällaiseen voi velvoittaa, sillä jos tiedot eivät ole toimijalle henkilötietoa, ei se kuulu TSA:n aineellisen soveltamisalan piiriin.[455] Sopimuksellisia keinoja olisi siten pidettävä vapaaehtoisina suojakeinoina.[456] Sopimuksen tekemistä voisi siten luonnehtia eräänlaiseksi organisatoriseksi toimenpiteeksi. Luovuttaja ja vastaanottaja voisivat siten sopia asiakirjalla, ettei vastaanottaja saa esimerkiksi käyttää relatiivisia avaimia tunnistamiseen. Sopimuksella suojattava intressi olisi siten luonnollisen henkilön perusoikeus. Aiheellista olisi kuitenkin arvioida sopimusrikkomustilanteista aiheutuvia seurauksia henkilötietojen suojalle ja vastuukysymyksiä tuottamuksen näkökulmasta. Sopimukselliset keinot voivat siten tasapainottaa henkilötietojen suojan ja henkilötietojen vapaan liikkuvuuden välistä suhdetta niin kauan, kun sopimusta noudatetaan. Lopulta kyse on laajemmasta verkosta, jossa myös ulkopuolisten tahojen tunnistamisen mahdollisuudet on henkilötietojen suojaamiseksi huomioitava.[457] Kuitenkaan kohtuuttomia velvoitteita ei voida toimijoille asettaa.[458]

---

[453] Andersson 2024, s. 360.
[454] Craddock 2025, V.3.
[455] Craddock 2025, V.3.; Ks. TSA 2, jonka mukaan asetusta sovelletaan henkilötietojen käsittelyyn. Jos kyse on anonyymien tietojen käsittelystä, ei TSA:lla voida siten asettaa sellaisen tiedon käsittelyyn kohdistuvia velvoitteita.
[456] Craddock 2025, V.3. Craddockin mukaan tästä huolimatta valvontaviranomaiset todennäköisesti pitäisivät toimenpiteiden puuttumista merkkinä laiminlyönnistä.
[457] Ks. C-479/22 P (OC v. komissio), kohdat 52–64. Kyse oli lehdistötiedotteesta, jossa oli tietoja henkilöstä, muttei kyseisen henkilön nimeä. Tapauksessa tutkittiin, onko yleisöllä tiedotteen tietojen perustella mahdollisuutta tunnistaa henkilö erityisetsi yhdistämällä muihin internetistä saataviin tietoihin.
[458] Ks. analogisesti julkisasiamies Spielmannin ratkaisuehdotus asiassa C-413/23 P (SRB), kohta 58.

Kyse on myös siitä, kuinka pitkälle tulevaisuuteen pseudonymisoidut tiedot luovuttavan rekisterinpitäjän tulee arvioida vastaanottajan tai myöhempien vastaanottajien tunnistamiskeinoja. Lisäksi on kyse siitä, missä määrin on kohtuullista huomioida tekninen kehitys, kun se on yksi objektiivisista kohtuullisen todennäköisten keinojen arviointikriteereistä.[459] Teknologisen kehityksen arvioinnissa voidaan hyödyntää kohtuullisuuden kriteeriä, jolloin rekisterinpitäjän velvollisuudet rajoittuvat kohtuullisesti ennakoitavissa olevaan kehitykseen. Mitä muuttuvampi toimintaympäristö on, sitä parempia avoimet normit ovat kattamaan eteen tulevia tilanteita. Tämän vuoksi tarkempaa rajoitusta sääntelyn tasolla ei olisi tarkoituksenmukaista määrittää. Käytännössä kohtuullisuuden rajat määrittyvät kuitenkin lopulta oikeuskäytännön myötä konkreettisiin tilanteisiin peilaten – ja näin on myös kohtuullisen todennäköisesti käytettävissä olevien tunnistamiskeinojen osalta.

Rekisterinpitäjän velvollisuuksia olisi kuitenkin syytä täsmentää pseudonymisoitujen henkilötietojen luovuttamistilanteissa. Rekisterinpitäjän tulisi tehdä tällaisen tiedon luovuttamisen osalta vaikutuksenarviointi erityisesti silloin, kun vastaanottajan kanssa ei ole tehty sopimusta tietojen luovuttamisesta. Erityisesti suhteellisen henkilötietokäsitteen vahvistumisen myötä syntyy riski siitä, että vastaanottaja ei ole tietosuojasääntelyn velvoitteiden piirissä. Tämä puolestaan johtaa rekisteröidyn oikeuksien ”katkeamiseen”, mutta aiheuttaa merkittäviä riskejä henkilötietojen suojalle. Kuitenkin jokaisen pseudonymisoituja tietoja käsittelevän tahon tulisi pyrkiä selvittämään, miten uudelleentunnistaminen parhaiten vältetään.[460]

Oikeuskirjallisuudessa on nostettu esiin mahdollisia lähestymistapoja vastaanottajien nimeämiseen tilanteissa, joissa henkilötietojen käsittelyperusteena on muu kuin suostumus. Yksi vaihtoehto olisi, ettei konkreettisia pseudonymisoitujen tietojen vastaanottajia tarvitsisi nimetä, vaan vastaanottajaryhmien nimeäminen riittäisi.[461] On huomioitava, että vaikka rekisteröidyn oikeudet sinänsä vaihtelevat käsittelyperusteen mukaan, on tiedonsaantioikeus niin sanottu portti myös muille rekisteröidyn oikeuksille. Tämän vuoksi konkreettisten tietojen saaminen mahdollisimman tarkasti on rekisteröidyn kannalta välttämätöntä. Vaikka käsittelyperusteena olisi muu kuin rekisteröidyn suostumus, ei se tarkoita, että rekisteröidyn oikeus saada tieto konkreettisista vastaanottajista olisi vähemmän merkityksellinen. Muiden käsittelyperusteiden kohdalla tiedonsaantioikeus konkreettisista vastaanottajista ennemminkin korostuu, jotta rekisteröidyllä on

[459] Rekisterinpitäjän velvollisuutta arvioida vastaanottajien tunnistamiskeinoja olisi syytä pohtia myös rikos- ja vahingonkorvausoikeudellisista näkökulmista. Tutkimuksen rajatun laajuuden vuoksi tätä ei kuitenkaan käsitellä enempää.
[460] Craddock 2025, V.3.
[461] Craddock 2025, V.4. Craddock on viitannut Österreichische Post -ratkaisun 36 kappaleen tulkintaan.

tieto henkilötietojensa liikkumisesta sekä mahdollisuus tarvittaessa puolustaa oikeuksiaan. Tiedonsaantioikeuden rajoittaminen muiden käsittelyperusteiden kohdalla olisi omiaan heikentämään luottamusta henkilötietojen suojaan ja tietosuojasääntelyn toimivuuteen ylipäänsä, ja vaikuttamaan siten esimerkiksi suostumuksen antamatta jättämisen kautta henkilötietojen liikkuvuuteen. Toinen esitetty vaihtoehto on, että rekisteröidylle voitaisiin ilmoittaa vastaanottajista, mikäli vastaanottaja on tietojen keräämisen hetkellä tiedossa ja mainita, ettei vastaanottajalla ole periaatteessa keinoja tunnistamiseen.[462] Tätä on pidettävä henkilötietojen suojan ja rekisteröidyn kannalta parempana vaihtoehtona. Ilmoittamisella rekisteröidylle pseudonymisointialueesta ja siitä, ettei sen sisällä periaatteessa ole pääsyä relatiiviseen avaimeen, toteutettaisiin tiedonsaantioikeutta ja samalla vähentää tilanteita, joissa rekisteröity yrittää käyttää oikeuksiaan suhteessa vastaanottajaan siinä onnistumatta.

Jos henkilötietoa arvioitaisiin absoluuttisesta näkökulmasta, olisi teknologian kehittyessä mahdollista tarkastella kaikkea tietoa henkilötietona.[463] Tällöin tietosuojan järjestelmästä tulisi kestämätön, eikä sillä pystyttäisi tavoittelemaan tietosuojan henkilötietojen vapaan liikkuvuuden tavoitetta. Jos henkilötietojen suojaa turvataan liian tiukasti, voi se johtaa tilanteeseen, jossa esimerkiksi kaikki tiedot salataan eikä mikään ole enää julkista. Myös tällaisella on vaikutuksensa oikeusvarmuudelle ja ennakoitavuudelle, esimerkiksi viranomaisten päätösten julkisuuden osalta. Näin ollen suhteellinen lähestymistapa pseudonymisoituun tietoon on perusteltu. Liian kapea henkilötiedon tulkinta voi tästä huolimatta aiheuttaa merkittävästi suurempia haittoja kuin liian laaja tulkinta.[464] Pseudonymisoidun henkilötiedon luonnetta ja ylipäätään tunnistettavuutta konseptina tulee lähestyä ennemmin siitä lähestymistavasta, että ”kaikki tieto on potentiaalisesti henkilötietoa, kunnes siitä ei pysty tunnistamaan” kuin ”kaikki tieto on anonyymiä, kunnes siitä voi potentiaalisesti tunnistaa”.

---

[462] Craddock 2025, V.4.

[463] Ks. tähän liittyvästä kritiikistä Purtova 2018 ja Purtova 2025.

[464] On kuitenkin huomioitava, ettei henkilöiden tunnistaminen ole aina huono asia eikä henkilötietojen suoja ole absoluuttinen oikeus. Esimerkiksi rikosepäiltyjen tunnistaminen on yhteiskunnallisesti painava intressi.

6 Päätäntö

6.1 Johtopäätökset

Tutkimuksessa on tarkasteltu pseudonymisoidun henkilötiedon tunnistettavuutta EU:n tietosuojakehyksessä, tämän vaikutuksia rekisteröidyn oikeuksiin ja toimijoiden velvollisuuksiin näiden toteuttamisessa sekä pseudonymisoinnin ja anonymisoinnin merkitystä tietosuojan kaksinaistavoitteen osalta. Arvioinnin ytimessä on ollut TSA 4(1) artiklan mukaisen henkilötiedon määritelmän ”tunnistettavissa oleva” luonnollinen henkilö sekä TSA:n vaatimus ottaa huomioon kaikki kohtuullisen todennäköisesti käytettävissä olevat keinot tunnistamisen tekemiseen.

Ensimmäiseen tutkimuskysymykseen vastaamisessa on apukysymyksenä käytetty sitä, *missä tilanteessa pseudonymisoitu henkilötieto lakkaa olemasta henkilötietoa*. Pseudonymisoitu henkilötieto on lähtökohtaisesti edelleen henkilötietoa, mutta sen luonne määräytyy viime kädessä kontekstin perusteella. Pseudonymisoitu henkilötieto lakkaa olemasta henkilötietoa silloin, kun kyseisen toimijan näkökulmasta rekisteröity ei ole tunnistettavissa ottaen huomioon kaikki käytettävissä olevat objektiivisesti arvioitavat, lailliset ja kohtuullisen todennäköiset keinot. Mikäli tällaista *relatiivista avainta* ei ole kohtuullisin keinoin käytettävissä, voi tieto olla kyseisen toimijan kannalta anonyymiä eikä tällöin kuulu TSA:n soveltamisalaan. Tunnistettavuus ei kuitenkaan riipu yksinomaan siitä, onko joku taho teoriassa kykenevä yhdistämään tiedon luonnolliseen henkilöön. Arvioinnissa on sen sijaan tarkasteltava, onko kyseisellä toimijalla tähän realistisia mahdollisuuksia. Pseudonymisoidun tiedon luonteen määrittely ei ole pelkästään tilannekohtaista, vaan riippuu ratkaisevasti siitä, miten tunnistettavuden kriteerit ymmärretään. Pseudonymisoidulla henkilötiedolla on hyvin dynaaminen luonne; se voi yhdessä hetkessä olla anonyymiä tietoa, mutta hetkessä muuttua henkilötiedoksi relatiivisen avaimen avulla. Tällainen tunnistettavuuden porrasteisuus puolestaan heikentää ennakoitavuutta ja oikeusvarmuutta niin luonnollisen henkilön kuin toimijoiden näkökulmista. Lisäksi se asettaa kyseenalaiseksi nykyisen tietosuojasääntelyn kahtiajaon henkilötiedon ja anonyymin tiedon välillä.

Tutkimuksessa on tarkasteltu *pseudonymisoinnin vaikutuksia rekisteröidyn oikeuksien toteutumiseen*. Pseudonymisoinnin alkuperäinen ajatus on ollut keventää tietosuojavelvoitteita, eikä sen tarkoitus ole ollut poistaa niitä kokonaan anonymisoinnin tavoin. Pseudonymisointi toimii siten riskienhallinnan välineenä, eikä sitä ole tarkoitettu anonymisointitekniikaksi. Rekisteröidyn oikeuksien toteutumisen kannalta on selvää, etteivät ne ulotu anonymisoituihin tietoihin. Pseudonymisointi puolestaan vaikuttaa rekisteröidyn oikeuksiin monella tapaa. Ensinnäkin TSA 11 ar-

tikla mahdollistaa rekisteröidyn oikeuksista poikkeamisen. Tämä tarkoittaa tilannetta, jolloin toimijalla katsotaan olevan kohtuullisen todennäköiset keinot tunnistaa henkilö, mutta se ei tosiasiallisesti pysty tunnistamaan. Jos toimijalla ei kuitenkaan ole kohtuullisen todennäköisiä keinoja eli relatiivista avainta, muuttuu tieto anonyymiksi tämän toimijan näkökulmasta ja jää siten tietosuojasääntelyn ulkopuolelle. Erona näiden kahden tilanteen välillä kuitenkin on, että ensimmäisessä rekisterinpitäjän tulee kuitenkin noudattaa muita tietosuojavelvoitteita, kun jälkimmäisessä toimija jää tietosuojasääntelyn ulkopuolelle. Tutkimus osoittaa, että pseudonymisoinnin myötä rekisteröidyn oikeuksien toteutuminen voi ”katketa” kahdessa tilanteessa: jos 1) jos rekisterinpitäjällä ei ole hallussaan relatiivista avainta TSA 11 artiklan mukaisessa tilanteessa tai 2) jos toimijalla ei ole kohtuullisin keinoin mahdollista saada relatiivista avainta. Näin ollen pseudonymisointi *de facto* kaventaa rekisteröidyn oikeuksien toteutumista.

Tutkimuksessa on tarkasteltu sitä, *miten pseudonymisointi ja anonymisointi suhteutuvat tietosuojasääntelyn tavoitteisiin*. Tietosuojan kaksinaistavoitteen osalta pseudonymisointi pyrkii toteuttamaan molempia. Anonymisointi puolestaan on painotukseltaan puhtaasti henkilötietojen suojaa turvaava, koska tällöin tietojen hyödynnettävyys on huomattavasti pseudonymisointia alhaisempi. Anonymisointi kuitenkin mahdollistaa tietojen vapaan käytön ilman tietosuojasääntelyn asettamia rajoituksia. Pseudonymisointi tukee erityisesti tietojen hyödyntämistä samalla estäen henkilön suoran tunnistamisen. Henkilötietojen suoja voi heikentyä pseudonymisoidun tiedon siirtyessä toimijalta toiselle erityisesti silloin, jos tiedon oikeudellinen asema vaihtelee. Anonymisoinnilla pyritään turvaamaan henkilötietojen suoja siten, että tunnistamisen mahdollisuus estetään kokonaan. Näin ollen anonymisoinnista ei lähtökohtaisesti ole henkilötietojen suojalle merkittävää riskiä, vaikka jäännösriskin olemassaolo on aina huomioitava. Edes anonymisoinnilla ei pystytä mahdollistamaan tilaa, jossa henkilötietojen suoja on turvattu täydellisesti. Suhteellisella henkilötiedon käsitteellä pyritään tavoittelemaan henkilötietojen vapaata liikkuvuutta, mutta se luo kuitenkin ennakoimattomia riskejä henkilötietojen suojalle ja rekisteröidyn oikeuksien toteutumiselle. Tutkimus kuitenkin osoittaa, että kaksinaistavoitteen tasapainon saavuttamiseksi suhteellinen henkilötietokäsite on välttämätön, vaikkakin ongelmallinen.

Tunnistettavuuden arviointi on tietosuojan tavoitteiden näkökulmasta painotukseltaan ristiriitaista eri oikeuslähteissä. EUT:n ratkaisukäytännössä korostuu tapauskohtainen ja suhteellinen arviointi, mikä ilmenee varsinkin tuoreessa oikeuskäytännössä henkilötietojen vapaan liikkuvuuden painottamisena. Tietosuojaneuvosto vuorostaan soveltaa varovaisempaa ja laajempaa tulkintalinjaa, painottaen siten henkilötietojen suojaa. Samanaikaisesti tulkiten lähteiden voidaan katsoa täydentävän toisiaan, mutta EUT:n korkeamman hierarkkisen aseman vuoksi voidaan todeta, että EU:ssa taloudellisille intresseille annetaan kasvava painoarvo.

Käytännössä koko tutkimuksen läpileikkaava kysymys on se, *onko pseudonymisointia ja anonymisointia koskeva sääntelymalli tarkoituksenmukainen suhteessa tietosuojan tavoitteisiin*. Nykyinen sääntelymalli ei kaikilta osin täytä oikeusvarmuuden ja ennakoitavuuden vaatimuksia, vaikka se lähtökohtaisesti mahdollistaa tietosuojan tavoitteiden tasapainon. Suhteellisen lähestymistavan korostuessa sääntely jättää merkittävää tulkinnanvaraa tunnistettavuuden arvioinnissa ja toimijoita koskevissa velvoitteissa. Tulkinnanvaraisuus puolestaan heikentää oikeusvarmuutta ja ennakoitavuutta, mikä väistämättä vaikuttaa luonnollisten henkilöiden luottamukseen henkilötietojen tehokkaasta suojasta. Toisaalta tällainen sääntely mahdollistaa tapauskohtaisen arvioinnin ja joustavuuden erityisesti teknologinen kehitys huomioiden, jolloin henkilötietoa voidaan hyödyntää niin yleisen kuin yksityisen edun mukaisissa toiminnoissa.

Tutkimuksessa on kehitetty tunnistamisen mahdollistavien lisätietojen ja kohtuullisen todennäköisten keinojen suhteellisuutta kuvaava käsite, *relatiivinen avain*. Relatiivinen avain ilmentää samaa ajattelumallia kuin suhteellinen henkilötietokäsite, ja se on siten henkilötiedon tavoin dynaaminen ja kontekstisidonnainen. Tutkimuksessa osoitetaan, että pseudonymisoidun ja anonymisoidun tiedon tunnistettavuus määrittyy siten aina *relatiivisen avaimen* mukaan, jolla *tunnistettavuuden lukko* avataan. Näin ollen relatiivinen avain määrittää myös rekisteröidyn oikeuksien tosiasiallisen toteutumisen, jäännösriskin tason sekä perusoikeudellisen henkilötietojen suojan tehokkaan toteutumisen.

Kokonaisuutena arvioiden tutkimus täyttää sille asetetut tavoitteet ja vastaa asetettuihin kysymyksiin. Lainopin ja teleologisen tulkinnan avulla oli mahdollista jäsentää henkilötiedon ja anonyymin tiedon välistä rajanvetoa sekä kytkeä nämä tulkinnat osaksi laajempaa systemaattista arviointia. Tutkimusta olisi ollut mahdollista syventää empiirisellä tutkimuksella siitä, miten tarkasteltuja teemoja sovelletaan käytännössä esimerkiksi rekisterinpitäjien toiminnassa. Kuitenkin sääntelyn, oikeuskäytännön ja muun lähdeaineiston tarkastelu lainopillisin keinoin mahdollisti tutkimustehtävän kannalta riittävän ja systemaattisen analyysin.

Jatkotutkimuksen kannalta tutkimus nostaa esiin useita kysymyksiä. Tutkimuksellisesti mielenkiintoinen kohde olisi esimerkiksi tarkastella tuottamuksen näkökulmasta rekisterinpitäjän mahdollisuuksia arvioida vastaanottajan tai muiden tunnistamiskeinoja sekä sitä, miten vastuukysymykset ja näyttötaakka määräytyvät suhteellisen henkilötietokäsitteen kontekstissa. Lisäksi olisi perusteltua tarkastella pseudonymisoinnin ja anonymisoinnin suhdetta tekoälyyn, profilointiin ja automaattiseen päätöksentekoon, erityisesti suhteellisen henkilötietokäsitteen ja henkilötietojen suojan näkökulmasta. Ajankohtaisena jatkotutkimusaiheena voidaan pitää myös pseu-

donymisoinnin ja anonymisoinnin asemaa terveystietojen toisiokäytössä. Tässä yhteydessä korostuvat sekä henkilötiedon dynaaminen luonne että terveystietojen arkaluonteisuus, jotka yhdessä asettavat merkittäviä haasteita voimassa olevan sääntelyn tulkinnalle.

6.2 De lege ferenda

Sääntelyn kehittämisessä tulisi ensisijaisesti vahvistaa oikeusvarmuutta ja ennakoitavuutta ilman, että henkilötiedon käsitettä kavennetaan perusoikeussuojaa heikentäen. Voimassa oleva sääntely mahdollistaa jo kontekstuaalisen ja toimijakohtaisen arvioinnin, mikä ilmenee myös EUT:n oikeuskäytännöstä. Suhteellista henkilötietokäsitettä ei ole siten tarkoituksenmukaista erikseen kodifioida. Liiallinen suhteellisuuden täsmentäminen kaventaisi henkilötiedon käsitettä ja tietosuojasääntelyn soveltamisalaa, mikä puolestaan heikentää oikeusvarmuutta ja ennakoitavuutta sekä vaarantaa henkilötietojen suojan.

Pseudonymisoinnin ja anonymisoinnin eron selventämiseksi TSA:ssa olisi syytä nimenomaisesti määritellä myös anonymisointiprosessi. Lisäksi sääntelyssä tulisi tunnistaa ja huomioida pseudonymisoidun tiedon dynaaminen luonne. Sääntelyssä tulee korostaa riskiperusteista lähestymistapaa. *De lege ferenda* olisi perusteltua edellyttää, että rekisterinpitäjä suorittaa ennen pseudonymisoitujen tietojen luovutusta vaikutustenarvioinnin, jossa arvioidaan tunnistettavuus eri toimijoiden näkökulmasta sekä jäännösriskin todennäköisyys.[465] Näin tulisi olla etenkin tilanteissa, joissa vastaanottajalle tieto olisi todennäköisesti anonyymiä tietoa eikä käsittelyä ole sopimuksellisilla keinoilla rajoitettu. TSA:ssa tulisi kannustaa toimijoita sopimuksellisiin mekanismeihin eräänlaisina teknisinä ja organisatorisina toimenpiteinä.

Pidemmällä aikavälillä voidaan arvioida myös niin sanotun potentiaalisen henkilötiedon kategorian käyttöönottoa. Tällainen välikategoria voisi paremmin kuvata pseudonymisoidun tiedon asemaa ja vähentää kahtiajaon aiheuttamaa tulkintaepävarmuutta. Potentiaalinen henkilötieto ei ole anonyymiä tietoa, joten se kuuluisi tietosuojasääntelyn soveltamisalaan mutta rajoitetuin velvoittein.[466] Kategorian käyttöönotto edellyttäisi kuitenkin huolellista ja kokonaisvaltaista arviointia luonnollisille henkilöille ja toimijoille kohdistuvista riskeistä sekä vaikutuksista tietosuojan tavoitteiden tasapainoon siten, että vältetään normiston monimutkaistuminen.

---

[465] ICO on myös korostanut tunnistettavuuden testaamista ja dokumentointia osana vaikutustenarviointia. Ks. ICO 2022a, s. 27.

[466] Tämä sinänsä kuvastaa TSA 11 artiklan mukaista tilannetta.

Lopuksi voidaan todeta, että tietosuojasääntelyn kehittämisessä on aina säilytettävä tasapaino henkilötietojen suojan ja vapaan liikkuvuuden välillä. Suhteellinen lähestymistapa on perusteltu, mutta sen liiallinen korostaminen voi johtaa henkilötietokäsitteen kaventumiseen perusoikeudellisen henkilötietojen suojan kustannuksella. Tämän vuoksi sääntelyä tulisi kehittää varovaisesti ja nimenomaan henkilötietojen suojan lähtökohdasta tarkasteltuna.