# Biometrinen tunnistaminen Euroopan unionin oikeudessa

Eveliina Suvanto

Lapin Yliopisto

Oikeustieteiden tiedekunta

Maisteritutkielma

Eurooppaoikeus

Kevät 2026

**Lapin yliopisto**

Tiedekunta: Oikeustieteiden tiedekunta

Työn nimi: Biometrinen tunnistaminen Euroopan uninon oikeudessa

Tekijä: Eveliina Suvanto

Koulutusohjelma/oppiaine: Oikeustiede, Eurooppaoikeus

Työn laji: Maisteritutkielma

Sivumäärä: XII + 64

Vuosi: 2026

Tiivistelmä:

Biometrinen tunnistaminen ja erityisesti ihmisten automatisoitu tunnistaminen on yleistynyt viime vuosina. Kyseessä on teknologia, joka aiheuttaa merkittäviä riskejä yksityisyydellä, henkilötietojensuojalle sekä muille perus- ja ihmisoikeuksille. Huolia on noussut muun muassa yksityisyyden heikkenemisestä biometristen tietojen osalta tilanteissa, joissa biometrisiä tietoja hyödynnetään ilman riittävää sääntelyä ja valvontaa. Huolta ovat herättäneet erityisesti lainvalvontaviranomaisten käyttämät biometriset etävalvontajärjestelmät julkisilla paikoilla, jotka mahdollistavat suurien ihmismäärien tunnistamisen ilman heidän suostumustaan.

Euroopan unionissa hyväksyttiin vuonna 2024 tekoälyasetus, jonka tavoitteena on edistää luotettavien ja ihmiskeskeisten tekoälyjärjestelmien kehittämistä ja käyttöä siten, että samalla turvataan perusoikeuksien ja unionin arvojen toteutuminen. Sääntelyn keskeisenä periaatteena toimii riskiperusteisuus, jonka tarkoituksena on varmistaa, että erityisesti suurempia riskejä esimerkiksi yksityisyydelle ja muille perusoikeuksille aiheuttavat järjestelmät asetetaan tiukempien vaatimusten ja velvoitteiden alaisiksi.

Tutkielmassa systemoidaan biometristen tunnisteiden ja biometrisen tunnistamisen kannalta keskeiset säännökset. Näihin lukeutuvat erityisesti perus- ja ihmisoikeussääntely sekä Euroopan unionin tietosuojasääntelyyn kuuluvat yleinen tietosuoja-asetus ja rikosasioiden tietosuojadirektiivi. Lisäksi tutkielmassa tarkastellaan, miten tekoälyasetus huomioi perus- ja ihmisoikeuksien suojelun biometrisen tunnistamisen yhteydessä. Tarkastelun perusteella asetuksessa voidaan havaita useita merkittäviä perus- ja ihmisoikeussuojaan liittyviä puutteita ja tulkinnanvaraisuuksia. Erityisiä huolenaiheita aiheuttavat esimerkiksi reaaliaikaisen ja jälkikäteisen biometrisen etätunnistamisen välinen epäselvä rajanveto sekä asetukseen sisältyvät laajat poikkeukset muutoin kiellettyihin tekoälyjärjestelmiin. Nämä poikkeukset voivat käytännössä heikentää asetuksen tavoitetta turvata yksityisyys, kokoontumisvapaus ja muut keskeiset perusoikeudet sekä mahdollistaa sellaisten valvontakäytäntöjen käytön, joita asetuksella on lähtökohtaisesti pyritty rajoittamaan.

Avainsanat: Biometrinen tunnistaminen, tekoälyasetus, yksityisyys

X Tutkielma ei sisällä muita kuin tekijän omia henkilötietoja

# Sisällys

# LÄHTEET

## KIRJALLISUUS

*Bradford, Anu:* The Brussels effect. Northwestern University Law Review, Vol. 107, No. 1, Columbia Law and Economics Working Paper No. 533, 2012.

*Bradford, Anu*: The False Choice Between Digital Regulation and Innovation. Northwestern University Law Review, Vol. 118, Issue 2, 2024.

*Brey, Philip:* Ethical Aspects of Face Recognition Systems in Public Places. Journal of Information, Communication & Ethics in Society, 2:2, 97-109, 2004.

*Bräutigam, Tobias – Cunningham, Francine – Toivanen, Meeri – Aholainen, Maria – Geus, Marjolein*: Sitra työpaperi: EU-sääntely rakentaa reilumpaa datataloutta. PunaMusta Oy 2022.

*Caruana, Mireille M. – Borg, Roxanne Meilas:* Regulating Artificial Intelligence in the European Union. Teoksessa The EU Internal Market in the Next Decade – Quo Vadis? Toim. Ivan Sammut ja Ivan Mifsud. Brill 2025.

*Garfinkel, Simson:* Database Nation: The Death of Privacy in the 21st Century. O'Reilly Media 2000.

*Gelb, Alan – Clark, Julia*: Identification for Development: The Biometrics Revolution. Working paper 315 January 2013. Center for Global Development Washington 2013.

*Gomez-Barrero, Marta – Drozdowski, Pawel – Rathgeb, Christian – Patino, Jose – Todisco, Massimiliano – Nautsch, Andreas – Damer, Naser – Priesnitz, Jannier – Evans, Nicholas – Busch, Christoph*: Biometrics in the Era of COVID-19: Challenges and Opportunities, s. 1-15, 2022.

*Hirvelä, Päivi – Heikkilä, Satu:* Ihmisoikeudet: Käsikirja EIT:n oikeuskäytäntöön. Alma Talent Oy 2017.

*Hirvonen, Ari:* Mitkä metodit? Opas oikeustieteen metodologiaan. Helsingin yliopisto, Oikeustieteellinen tiedekunta 2011.

*Heinonen, Risto*: Digitaalinen minä. Edita 2001.

*Israel, Olatunji*: Ethical Implications of Constant Biometric Surveillance. ResearchGate 2024.

*Jain, Anil K. – Pankanti, Sharath – Hong, Lin – Ross, Arun – Wayman, James L:* Biometrics: A Grand Challenge. Cambridge UK 2004.

*Keller, Milla*: Mitä on tietosuoja? Alma Talent Helsinki 2023.

*Keller, Milla*: Datajuridiikka. Paremmat pelisäännöt datataloudelle. Alma Insights 2025.

*Kindt, Els:* Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis. Springer 2013.

*Kindt, Els:* A First Attempt at Regulating Biometric Data in the European Union. Teoksessa Regulating Biometrics: Global Approaches and Urgent Questions. Toim. Amba Kak. AI Now Institute 2020.

*Koillinen Mikael*: Henkilötietojen suoja itsenäisenä perusoikeutena. Oikeus 2012 (42); 2: 171–193.

*Koops, Bert-Jaap*: The concept of function creep. Law, Innovation and Technology 2021, Vol 13, No. 1, 29-56.

*Korhonen, Rauno:* Poliisin valtontakeinot ja kansalaisten yksityisyyden suoja. Edita Publishing Oy 2005.

*Korja, Juhani:* Biometrinen tunnistaminen ja henkilötietojen suoja: tutkimus biometristen tunnisteiden lainsäädännöllisestä asemasta. Lapin yliopisto 2016.

*Korpisaari, Päivi*: Tietosuoja. Alma Talent 2022.

*Korpisaari, Päivi – Pitkänen, Olli – Warma-Lehtinen, Eija*: Uusi tietosuojalainsäädäntö. Alma Talent 2018.

*Koula, Aikaterini*: AI-Driven Mass Surveillance at 2024 Olympics: The Human Rights Issues and Recommendations. Manchester Metropolitan University (ei päivätty)

*Kujala, Tero*: Euroopan unionin perusoikeuskirja – perusoikeudet ja lainkäyttö, s. 123–146. Teoksessa Ervo, Laura – Lahti, Raimo – Siro, Jukka (toim.): Perus- ja ihmisoikeudet rikosprosessissa. Helsingin hovioikeus, Helsinki 2012.

*Kusche, Isabel:* Possible harms of artificial intelligence and the EU AI act: fundamental rights and risk. Journal of Risk Research. Routledge, 2024.

*Lasek-Markey, Marta – Hogan, Linda:* Delivering on the Promise of the Fundamental Rights Impact Assessments in the EU AI Act: Intersectionality and Vulnerability. European Journal of Law and Technology, Vol. 16 No. 2, 2025.

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

*Lindroos-Hovinheimo, Susanna – Koivisto, Ida – Koulu, Riikka – Sankari, Suvi*: Tekoälyn sääntely. Alma Insights, Helsinki 2025.

*Loideain Ni Nora:* EU Data Privacy Law and Serious Crime: Dara Retention and Policymaking, Chapter 2: The Approach of the European Court of Human Rights to the Interceptions of Communications. Oxford University Press 2025.

*Neuwirth, Rostam Josef*: Prohibited Artificial Intelligence Practices in the Proposed EU Artificial Intelligence Act. SSRN 2022.

*Nikula, Paavo*: Euroopan unionin perusoikeuskirja. Oikeus 4/2000 s. 524–526.

*Paula, Ana:* Unlocking Security the Impact of Biometric Intelligence Analysts. Journal of Biometrics & Biostatistics 15 (2024): 210.

*Penttinen, Sirja-Leena*: Avaimet EU-oikeuteen. Edita Publishing Oy 2017.

*Pugliese, Joseph*: Biometrics: Bodies, Technologies, Biopolitics. Routledge 2010.

*Pöysti, Tuomas*: Oikeudellisen tiedon niukkuus ja henkilötietojen suoja s. 303–329. Teoksessa Aarnio, Aulis – Kangas, Urpo – Korhonen, Rauno – Mattila Heikki – Mikkola Tuulikki (toim.): Syntymästä kuolemaan, oikeudesta informaatioon. Suomalainen Lakimiesyhdistys, Helsinki 2006.

*Raitio, Juha – Tuominen Tomi*: Euroopan unionin oikeus. Alma Talent 2020.

*Saarenpää, Ahti – Korhonen, Rauno – Råman, Jari – Hyvänen, Mari*: Sähköinen viestintä, tietoturvallisuus ja perusoikeudet. Lapin yliopisto, Rovaniemi 2004.

*Saarenpää Ahti*: Henkilö- ja persoonallisuusoikeus. Teoksessa Oikeusjärjestys osa I. Lapin yliopiston oikeustieteellisiä julkaisuja sarja C 59, Rovaniemi 2012.

*Saarenpää, Ahti – Riekkinen, Juhani*: Oikeusinformatiikan perusteet. Lapin yliopisto, Rovaniemi 2023

*Saarenpää Ahti*: (Ei päivätty) Näkökulmia yksityisyyteen, tietoturvaan ja valvontaan. Verkkoteksti osoitteessa https://www.ulapland.fi/loader.aspx?id=35185384-e21d-406b-96cc-1abe9705623d. (Käyty 3.3.2025)

*Sankari, Valtteri – Wiberg, Matti*: GDPR ei toimi. Tietosuojakäytännöt eivät noudata asetusta. Yhteiskuntapolitiikka -lehti 84:3 2019.

*Walkila, Sonya*: Ajankohtaista eurooppa-oikeutta – Aktuellt inom europarätten: Euroopan unionin perusoikeuskirja EU-tuomioistuimen oikeuskäytännössä. Defensor Legis N:o 6/2011, s. 813–820.

*Wong-Toropainen, Sanna*: Euroopan unionin datasääntely - käsikirja viiteen asetukseen. Edilex Lakitieto Oy 2025.

*Zaccaroni, Giovanni:* Facing the Golem: Disruptive Technologies vs Democracy in the EU Digital Single Market. Teoksessa: The EU Internal Market in the Next Decade – Quo Vadis? Brill 2025.

**VIRANOMAISJULKAISUT**

C(2025) 5052 final. Euroopan komissio: Komission suuntaviivat asetuksella (EU) 2024/1689 (tekoälysäädös) kielletyistä tekoälyyn liittyvistä käytännöistä. 29.7.2025.

COM (2020) 65 final. Euroopan komissio: Valkoinen kirja tekoälystä – Eurooppalainen lähestymistapa huippuosaamiseen ja luottamukseen.

COM (2021) 206 final. Euroopan komissio: Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts.

Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu: Yhteinen lausunto 5/2021 ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi tekoälyä koskevista yhdenmukaistetuista säännöistä. 18.6.2021.

European Data Protection Supervisor: Opinion 6/2015: A further step towards comprehensive EU data protection. EDPS recommendations on the Directive for data protection in the police and justice sectors. 28.10.2015.

Euroopan unionin perusoikeusvirasto: Facial recognition technology: fundamental rights considerations in the context of law enforcement. 2019.

Euroopan unionin neuvosto. 2021/0106(COD): Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - General approach.

**MUUT LÄHTEET**

Amnesty International: EU: European Parliament adopts ban on facial recognition but leaves migrants, refugees and asylum seekers at risk, 14.6.2023. saatavilla https://www.amnesty.org/en/latest/news/2023/06/eu-european-parliament-adopts-ban-on-facial-recognition-but-leaves-migrants-refugees-and-asylum-seekers-at-risk/

ARTICLE 19: When Bodies Become Data: Biometric Technologies and Freedom of Expression, 2021.

Article 29 Working Party, WP248: Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679, 4.4.2017.

Bird & Bird,*Nora Santalu*: What is an Emotion Recognition System under the EU's Artificial Intelligence Act? Part 1 - A Machine That "Understands" Your Monday Blues! 4.11.2024. saatavilla: https://www.twobirds.com/en/insights/2024/global/what-is-an-emotion-recognition-system-under-the-eus-artificial-intelligence-act-part-1

Elisa Oyj, blogikirjoitus 27.6.2025: Cyber Security Outlook 2025: Trendejä, uhkia ja ratkaisuja tulevaisuuteen. saatavilla: https://yrityksille.elisa.fi/ideat/cybersecurity-outlook-2025/

European Center for Not-for-Profit Law: Hungary's new Biometric Surveillance Laws Violate the AI Act, 28.4.2025. saatavilla: https://ecnl.org/news/hungarys-new-biometric-surveillance-laws-violate-ai-act

European Data Protection Board: Guidelines 05/2022 on the Use of Facial Recognition technology in the Area of Law Enforcement, 12.5.2022.

European Digital Rights (EDRi): Ban Biometric Mass Surveillance – A Set of Fundamental Rights Demands for the European Commission and EU Member States, Bryssel 2020.

European Digital Rights (EDRi): About Clearview AI's Mockery of Human Rights, Those Fighting It, and the Need for the EU to Intervene**.** saatavilla https://edri.org/our-work/we-need-to-talk-about-clearview-ai/

European Parliament: Artificial Intelligence Act: Deal on Comprehensive Rules for Trustworthy AI. 9.12.2023. saatavilla https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai

European Parliamentary Research Service (EPRS): Artificial Intelligence: From Ethics to Policy. Scientific Foresight Unit (STOA), 2020

European Parliamentary Research Service (EPRS): Person Identification, Human Rights and Ethical Principles. Rethinking Biometrics in the Era of Artificial Intelligence, 2021.

European Union Agency for Fundamental Rights (FRA): Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU. Volume II: Field Perspectives and Legal Update, 2017.

European Union Agency for Fundamental Rights (FRA): Assessing High-risk Artificial Intelligence: Fundamental Rights Risks 2025.

*Giannini, Alice – Tas, Sarah*: AI Act and the Prohibition of Real-Time Biometric Identification: Much Ado About Nothing? Verfassungsblog 10.12.2024. saatavilla https://verfassungsblog.de/ai-act-and-the-prohibition-of-real-time-biometric-identification

The Guardian, *Carole Cadwalladr – Emma Graham-Harrison*: Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach. 17.3.2018. saatavilla https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

International Organization for Migration (IOM): International Migration Law No. 5 – Biometrics and International Migration, 2005.

International Organization for Migration (IOM): Introduction to Biometrics, 2024.

IPOL Study: *Wendehorst, Christiane – Duller, Yannic*: Biometric Recognition and Behavioural Detection: Assessing the Ethical Aspects of Biometric Recognition and Behavioural Detection Techniques with a Focus on their Current and Future Use in Public Spaces, 2021.

Joint Civil Society Recommendations for an EU Artificial Intelligence Act for Fundamental Rights Biometrics, Part 1: Article 3(36) and Article 5(1)(d), ei päivätty. saatavilla chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://edri.org/wp-content/uploads/2022/05/Prohibit-RBI-in-publicly-accessible-spaces-Civil-Society-Amendments-AI-Act-FINAL.pdf

Kansalaisjärjestöjen yhteinen lausunto: EU's AI Act Fails to Set Gold Standard for Human Rights, 3.4.2024. saatavilla chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.amnesty.eu/wp-content/uploads/2024/04/EUs-AI-Act-fails-to-set-gold-standard-for-human-rights.pdf

National Institute of Standards and Technology, NISTIR 8280: Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, 2019. saatavilla https://www.nist.gov/publications/face-recognition-vendor-test-part-3-demographic-effects?utm_source=chatgpt.com

*Nóra Ni Loideain*: A Trustworthy Framework that Respects Fundamental Rights? The Draft EU AI Act and Police Use of Biometrics. Information Law and Policy Centre 4.8.2021, saatavilla https://infolawcentre.blogs.sas.ac.uk/2021/08/04/a-trustworthy-framework-that-respects-fundamental-rights-the-draft-eu-ai-act-and-police-use-of-biometrics/

A Policy Framework for Responsible Limits on Facial Recognition Use Cases: Law Enforcement Investigations. Insight Report, 2022.

Reclaim Your Face: kampanjan verkkosivut. Saatavilla https://reclaimyourface.eu/

Teknologiateollisuus ry: Lausunto luonnoksesta hallituksen esitykseksi tekoälyasetuksen toimeenpanoa koskevaksi lainsäädännöksi 2024.

Tekoälyä käsittelevä korkean tason asiantuntijaryhmä: Luotettavaa tekoälyä koskevat eettiset ohjeet, 2019.

Yle artikkeli, Teemu Hallamaa: Analyysi: EU yrittää tekoälyasetuksella toisintaa Bryssel-efektiä, mutta muu maailma ei välttämättä seuraa nyt perässä, 14.6.2023. saatavilla https://yle.fi/a/74-20036826

YK:n lapsen oikeuksien komitea: Yleiskommentti nro 25 (2021) digitaaliseen ympäristöön liittyvistä lapsen oikeuksista (CRC/C/GC/25).

## OIKEUSKÄYTÄNTÖ

### Euroopan ihmisoikeustuomioistuin

Euroopan ihmisoikeustuomioistuin, *P.G. ja J.H. v. Yhdistynyt kuningaskunta*, no. 44787/98, tuomio 25.9.2001

Euroopan ihmisoikeustuomioistuin, *Peck v. Yhdistynyt kuningaskunta*, no. 44647/98, tuomio 28.1.2003

Euroopan ihmisoikeustuomioistuin, *Liberty ja muut v. Yhdistynyt kuningaskunta*, no. 58234/00 tuomio 1.7.2008

Euroopan ihmisoikeustuomioistuin suuren jaoston ratkaisu *S. ja Marper v. Yhdistynyt kuningaskunta,* no. 30562/05, 30566/04, tuomio 4.12.2008.

Euroopan ihmisoikeustuomioistuin, *Shimovolos v. Venäjä,* no. 30194/09, tuomio 21.6.2011

Euroopan ihmisoikeustuomioistuin, *M.K v. Ranska*, no. 19522/09, tuomio 18.4.2013

Euroopan ihmisoikeustuomioistuin*, Gaughran v. Yhdistynyt kuningaskunta*, no. 45245/15, tuomio 13.2.2020

Euroopan ihmisoikeustuomioistuin, *Big Brother Watch ja muut v. Yhdistynyt kuningaskunta,* no. 58170/13, 62322/14 ja 24960/15, tuomio 25.5.2021

Euroopan ihmisoikeustuomioistuin, *Glukhin v. Venäjä*, no. 11519/20, tuomio 4.7.2023

**Euroopan unionin tuomioistuin**

Yhdistetyt asiat C-293/12 ja C-594/12 *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Irlanti ja The Attorney General, Irish Human Rights Commission,* ECLI:EU:C:2014:238

Asia C-362/14 *Maximillian Schrems v. Data Protection Commissioner,* ECLI:EU:C: 2015:650

Asia C-205/21 *Ministerstvo na vatreshnite raboti Glavna direktsia za borba s organiziranata prestapnost v. V. S,* ECLI:EU:C: 2023:49

**Tietosuojaviranomaisten ratkaisut**

Ruotsin tietosuojaviranomaisen ratkaisu DI-2020-2719, annettu 10.2.2021.

# Lyhenneluettelo

| | |
|---|---|
| EU | Euroopan unioni |
| EUT | Euroopan unionin tuomioistuin |
| EIS | Euroopan ihmisoikeussopimus |
| EIT | Euroopan ihmisoikeustuomioistuin |
| SEU | Sopimus Euroopan unionista |
| SEUT | Sopimus Euroopan unionin toiminnasta |

# 1 Johdanto

## 1.1 Aiheen taustaa

Teknologian kehitys on tuonut mukanaan välineitä ja sovelluksia arjen kaikille osa-alueille, joita vielä muutama vuosikymmen sitten ei olisi voitu kuvitellakaan. Erityisesti biometrinen teknologia, kuten kasvojentunnistus ja sormenjälkitunnistus, on kehittynyt nopeasti mahdollistaen yksilöiden entistä tarkemman ja jatkuvan valvonnan sekä syrjinnän. Tämä kehitys on herättänyt laajaa keskustelua sekä kotimaisessa että kansainvälisessä oikeustieteessä, kuten Aarnio (*Häviääkö yksityisyyden suoja*), Heinonen (*Digitaalinen minä*) ja Garfinkel (*Database Nation*) ovat omissa teoksissaan todenneet[1]. Teknologiaa on syytetty ”yksityisyyden kuolemasta”. Kyse ei ole uudesta väitteestä, sillä jo vuonna 1890 bostonilaiset lakimiehet *Samuel Warren* ja *Louis Brandeis* kirjoittivat *Harvard Law Review* -lehden artikkelissaan, että uusien keksintöjen ja liiketoimintasuunnitelmien myötä yksityisyys on hyökkäyksen kohteena.[2] Huoli yksityisyyden heikkenemisestä tai jopa sen täydellisestä katoamisesta on noussut keskiöön biometristen tietojen osalta tilanteissa, joissa biometrisiä tietoja hyödynnetään ilman riittävää sääntelyä ja valvontaa.[3]

Euroopan unioni on pyrkinyt vastaamaan näihin haasteisiin luomalla sääntelykehystä, joka turvaisi teknologian eettisen ja turvallisen käytön sekä suojaisi kansalaisten perusoikeuksia. Vuonna 2024 hyväksyttiin Euroopan unionin tekoälyasetus.[4] Euroopan komissio totesi vuonna 2020 valkoisessa kirjassaan, että sääntelyn tavoitteena on mahdollistaa luotettavan ja turvallisen tekoälyn kehittäminen Euroopassa kunnioittaen unionin kansallisia arvoja ja oikeuksia. Tavoitteena on luoda ”luottamuksen ekosysteemi”.[5]

## 1.2 Tutkimuskysymykset ja tutkielman rakenne

Tutkielman tarkoituksena on selvittää, miten Euroopan unionissa pyritään turvaamaan biometristen tunnistamisen ihmis- ja perusoikeuksia kunnioittava käyttö. Tutkimuskysymykset voidaan tiivistää seuraavasti:

---

[1] ks. Aarnio Häviääkö yksityisyyden suoja, s. 51–57, Heinonen digitaalinen minä s. 151–155 ja Garfinkel, Database Nation. The Death of Privacy in the 21st Century.
[2] Garfinkel 2000, s. 6.
[3] Esimerkiksi ARTICLE19 (2021) ja Amnesty International 14.6.2023.
[4] Euroopan parlamentin ja neuvoston asetus (EU) 2024/1689, annettu 13.6.2024, 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)
[5] COM (2020) 65 final, s. 3.

1) *Miten tekoälyasetus muuttaa biometristen tunnistamisen sääntelyä Euroopan unionissa?*
2) *Miten perus- ja ihmisoikeuksien suojan toteutuminen pyritään tekoälyasetuksessa takaamaan?*

Tutkielman rakenne etenee johdannon jälkeen siten, että toisessa luvussa käsittelen biometristä tunnistamista. Tutkielmassa biometrisen tunnistamisen tekniseen puoleen ei syvennytä enempää kuin on tarpeen ilmiön oikeudellisen tarkastelun ja ymmärtämisen kannalta. Luvun tarkoituksena on hahmotella, mistä biometrisessä tunnistamisessa on kysymys sekä mitä riskejä ja haasteita sen käytöstä aiheutuu. Riskien ymmärtäminen on keskeistä, jotta voidaan hahmottaa sääntelyn tarvetta. Kolmannessa luvussa tarkastellaan biometristen tunnistamisen kannalta keskeisiä perus- ja ihmisoikeuksia, yksityisyyttä ja henkilötietojen suojaa, Euroopan unionin perusoikeuskirjan ja Euroopan ihmisoikeussopimuksen valossa.

Jotta ensimmäiseen tutkimuskysymykseen voidaan vastata, tulee hahmottaa biometrisiä tietoja ja tunnistamista koskeva unionitason sääntely ennen tekoälyasetuksen voimaantuloa. Neljännessä luvussa systematisoin biometrisen tunnistamisen kannalta relevanttia EU-sääntelyä.

Viidennessä luvussa tarkastellaan lähemmin tekoälyasetuksen biometrisiin tunnisteisiin ja tunnistamiseen liittyvää sääntelyä sekä sitä, miten perus- ja ihmisoikeusnäkökulma otetaan huomioon. Viimeisessä, kuudennessa luvussa esitetään tutkielman keskeiset johtopäätökset.

Tutkielman keskeinen lähde on tekoälyasetus sekä relevantti perus- ja ihmisoikeussääntely. Tekoälyasetuksen osalta keskiössä ovat ihmis- ja perusoikeuksien suojaa koskevat tavoitteet sekä asetuksen mukainen järjestelmien jaottelu riskiluokkiin. Hyödynnän tutkielman lähdeaineistona sekä oikeuskirjallisuutta ja artikkeleita että virallislähteitä. Lisäksi käytän lähdeaineistona Euroopan ihmisoikeustuomioistuimen ja Euroopan unionin tuomioistuimen oikeuskäytäntöä sekä tietosuojaviranomaisten lausuntoja, siltä osin kuin ne soveltuvat.

## 1.3 Tutkielman oikeudellinen viitekehys ja metodiset valinnat

Oikeustieteellisen tutkimuksen keskeinen metodi eli tutkimusmenetelmä on lainoppi, jota kutsutaan myös oikeusdogmaattiseksi metodiksi. Lainopin tutkimuskohteena on voimassa oleva oikeus, ja perinteisesti lainopin keskeisiä tehtäviä ovat sekä lain tulkinta että systematisointi. Voimassa olevien oikeusnormien sisältöä pyritään selvittämään tulkinnan ja systematisoinnin

avulla. Lainoppi metodina tutkii siis voimassa olevan oikeuden sisältöä ja sitä, mikä merkitys laista ja muista oikeuslähteistä saatavalla aineistolla on.[6]

Tutkielman aihe on eurooppaoikeudellinen, ja tutkielman keskiössä on Euroopan unionin oikeuden sääntely. Tämän vuoksi tulee ottaa huomioon EU-oikeuden erityispiirteet. Erityispiirteisiin lukeutuvat muun muassa EU-oikeuden jatkuva kehittyminen, soveltumisalan laajentumien sekä lainsäädäntötyön hitaus. Perussopimuksissa ei ole määritelty sitä, mitä tulkintametodia esimerkiksi unionin tuomioistuimen tulee noudattaa. Lähtökohtana voidaan pitää sanamuodon mukaista tulkintaa. Lisäksi Eurooppaoikeudelle on tyypillistä teleologinen eli tarkoitusperäopillinen tulkinta, jossa normia lähestytään sen tarkoituksen ja päämäärän kautta. Teleologinen tulkinta on EU-oikeudessa perusteltua, koska se mahdollistaa normien tarkoituksen toteutumisen muuttuvassa toimintaympäristössä.[7]

Tutkielmassa teleologinen tulkinta korostuu erityisesti arvioitaessa tekoälyasetuksen biometrisiä tunnisteita ja tunnistamista koskevia säännöksiä suhteessa asetuksen tavoitteisiin. Tekoälyasetuksen keskeisenä tarkoituksena on yhtäältä edistää luotettavan ja turvallisen tekoälyn kehittämistä Euroopan unionissa ja toisaalta turvata yksilöiden perus- ja ihmisoikeudet.[8] Täten tutkielmassa tarkastellaan paitsi sitä, mitä tekoälyasetuksessa säädetään biometrisestä tunnistamisesta, myös sitä, miten sääntely pyrkii toteuttamaan asetuksen taustalla olevia tavoitteita. Teleologisen tulkinnan avulla arvioin esimerkiksi sitä, miten riskiperusteinen sääntelymalli, kiellettyjä tekoälykäytäntöjä koskevat säännökset sekä korkean riskin järjestelmille asetetut velvoitteet edistävät perusoikeuksien toteutumista ja luottamuksen rakentamista tekoälyjärjestelmiin.

Vaikka tutkielma käsittelee Euroopan unionin oikeutta, tutkielmassa on myös oikeusinformatiikkaan liittyvä näkökulma. Oikeusinformatiikalle tunnusomaisia piirteitä ovat riskien tunnistaminen, lainsäädännön muutostarpeiden, informaation yhteiskunnallisen merkityksen, tietojärjestelmien ja tietoverkkojen käyttömahdollisuuksien sekä oikeudellisten tietovarantojen ja käytön tutkimus. Yhteiskunnan kehittyminen oikeudellisesta informaatioyhteiskunnasta nykyiseksi digitaaliseksi verkkoyhteiskunnaksi on lisännyt alan lainopillista tutkimusta. Oikeusinformatiikan alaan liittyvä tutkimus ei kuitenkaan ole perinteistä taaksepäin katsovaa lainoppia, vaan oikeudenalalla on eteenpäin katsova luonne.[9]

---

[6] Hirvonen 2011, s. 21–23.
[7] Penttinen 2017, s. 27–28, 32.
[8] Tekoälyasetuksen johdanto-osan 1 perustelukappale.
[9] Saarenpää – Riekkinen 2023, s. 35–36.

Tutkielman tavoitteena on selvittää ja systematisoida voimassa olevaa biometristä tunnistamista koskevaa lainsäädäntöä. Tutkielman käsitellessä unionin oikeutta on perusteltua hyödyntää erityisesti perus- ja ihmisoikeussuojan osalta lainopin lisäksi teleologista tulkintaa sen selvittämiseksi, miten tekoälyasetus pyrkii turvaamaan perus- ja ihmisoikeuksien toteutumisen myös rakenteellisesti esimerkiksi riskiperusteisen sääntelymallin sekä kiellettyjä tekoälykäytäntöjä koskevien säännösten kautta. Tavoitteen saavuttamiseksi hyödynnän lainoppia sekä teleologista tulkintaa. Oikeustieteessä vallitsee metodinen pluralismi, joka tarkoittaa metodista moninaisuutta ja moniarvoisuutta.[10] Tämänkin vuoksi moninainen näkökulma on perusteltu.

[10] Hirvonen 2011, s. 15.

# 2 Biometriset tunnisteet ja biometrinen tunnistaminen

## 2.1 Mitä biometrinen tunnistaminen on?

Biometria tarkoittaa alun perin elollisten ilmiöiden mittaamista ja tilastollista tutkimusta. Sana tulee kreikan kielen sanoista ”*bios*” (elämä) ja ”*metron*” (mitta). Biometristen tunnisteiden yleistyminen automaattisessa tunnistamisessa on muuttanut termin merkityssisältöä.[11] Jo sivilisaation alkuajoista lähtien kanssaihmisten tunnistamisella on ollut merkittävä rooli yhteiskunnan rakenteessa. Ihmisten tunnistaminen on olennainen osa infrastruktuuria, jota tarvitaan eri liiketoiminnan aloilla, kuten rahoituksessa, terveydenhuollossa, lainvalvonnassa, kulunvalvonnassa sekä hallinnossa ja viestinnässä. Yhteiskunnan muuttuessa yhä globaalimmaksi on syntynyt tarve suorittaa luotettava henkilötunnistus tarvittaessa etänä ja automaattisesti.[12]

Biometrinen data tarkoittaa henkilötietoja, jotka syntyvät luonnollisen henkilön fyysisiin, fysiologisiin tai käyttäytymiseen liittyviin ominaisuuksiin kohdistuvasta erityisestä teknisestä käsittelystä ja joiden avulla voidaan tunnistaa kyseinen henkilö yksilöllisesti tai varmistaa hänen henkilöllisyytensä. Biometrisillä teknologioilla tarkoitetaan puolestaan erilaisia teknologioita, joilla mitataan tai analysoidaan ihmisten yksilöllisiä ominaisuuksia, kuten DNA:ta, sormenjälkiä, ääntä tai silmän verkkokalvoja. Yksi tällaisista teknologioista on kasvojentunnistus.[13]

Teknisestä näkökulmasta biometrisen datan ensisijaisena tarkoituksena on yksilön henkilöllisyyden määrittäminen tai varmentaminen hänen yksilöllisten ominaisuuksiensa perusteella. Biometrinen data palvelee kahta erillistä käyttötarkoitusta: biometriseen tunnistamiseen (*identification*) ja biometriseen todentamiseen (*authentication / verification*). Todentaminen vastaa kysymykseen, onko henkilö se, joka hän väittää olevansa. Järjestelmä vertaa aiemmin tallennettua biometristä mallia tai näytettä henkilöön, joka haluaa todentaa henkilöllisyytensä.[14]

Biometriset todennusteknologiat tarjoavat perinteisiä todennustapoja, kuten salasanoja, turvallisemman vaihtoehdon, sillä ne perustuvat yksilöllisiin biometrisiin ominaisuuksiin, joita on vaikeampi jäljitellä ja väärentää.[15]Arkielämän esimerkkejä ovat muun muassa lentokentän passintarkastusportit, pankkipalveluihin kirjautuminen kasvojentunnistuksen tai sormenjäljen

[11] Korja 2016, s. 141 alaviite.
[12] Jain ym. 2004, s. 1.
[13] ARTICLE 19 2021, s. 8
[14] IOM 2024, s. 2.
[15] Paula 2024, s. 1. Tosin huolta herättävät ääntä ja ulkonäköä jäljittelevät *deepfake*t eli syvävääreennökset, jotka kehittyvät nopeasti. Niitä käytetään huijauksissa sekä poliittisessa vaikuttamisessa. Tulevaisuudessa esimerkiksi kasvojentunnistusta tunnistautumismenetelmänä ei pidetä riittävänä, koska generatiivisen tekoälyn nopeaan kehityksen vuoksi ne voivat olla murrettavissa jo parin vuoden sisällä. Ks. Elisa Oyj: Cyber security Outlook 2005.

avulla ja älypuhelimen avaaminen kasvojentunnistustoiminnolla. Tässä tutkielmassa keskitytään biometrisen tunnistamiseen, joten biometrinen todentaminen ei syvennytä tarkemmin.

Biometrinen tunnistaminen puolestaan vastaa kysymykseen ”kuka olet”, jolloin henkilö tunnistetaan muiden joukosta.[16] Henkilö tunnistetaan automaattisesti erityisen ohjelmiston tai laitteen avulla henkilön uniikkien piirteiden perusteella. Tunnistuksessa käytettävät tunnisteet voidaan jakaa fysiologiseen biometriseen tunnistamiseen ja käyttäytymispiirteeseen perustuvaan biometriseen tunnistamiseen. Ensimmäisessä tunnistaminen perustuu ihmisen fysiologisista ominaispiirteistä saatavaan informaatioon, kuten kasvoihin, sormenjälkiin ja silmän iiriksiin. Jälkimmäisessä tunnistaminen perustuu ihmisen käyttäytymispiirteisiin liittyvään informaatioon, joka perustuu epäsuorasti myös ihmiskehosta saatavaan tietoon. Tällaisia ovat esimerkiksi kävelytapa, kirjoitustapa ja kasvojen liikkeet, kuten huulien liikkeet puhuttaessa.[17]

Tunnistamiseen hyödynnettävän ominaispiirteen tulee ensinnäkin olla yleinen eli sen tulee esiintyä kaikilla ihmisillä. Toiseksi ominaispiirteen tulee olla yksilöllinen, jolloin piirre eroaa eri henkilöiden välillä, ja kolmanneksi pysyvä eli ajan kuluessa muuttumaton. Lisäksi ominaispiirteen tulee olla koneellisesti luettavissa ja analysoitavissa.[18]

Viranomaiset ja yksityiset toimijat hyödyntävät biometristä tunnistamista ja teknologioita monin eri tavoin. Teknologioiden käyttöä perustellaan muun muassa kansallisen turvallisuuden suojaamisella, terrorismin torjunnalla sekä rikollisuuden ehkäisemisellä ja torjunnalla.[19] Automatisoitu tunnistaminen mahdollistaa tunnistuksen kokonaan ilman ihmisen osallistumista. Ihmisen sijaan tunnistuksen suorittaa tietokone erilaisten ohjelmistojen ja laitteiden avulla.[20] Automatisoitu tunnistus mahdollistaa suurtenkin ihmisjoukkojen tunnistuksen.[21] Kiinnostus muun muassa kasvojentunnistusteknologiaa kohtaan perustuu sen tehokkuuteen ja skaalaavuuteen.[22]

Biometristä tunnistamista voidaan käyttää monimuotoisilla tavoilla, kuten tunnistamattoman henkilön etsimiseen tietokannasta hänen henkilöllisyytensä selvittämiseksi. Lisäksi henkilön liikkeitä voidaan seurata julkisissa tiloissa vertaamalla hänen kasvojaan valvonta-alueella aiemmin tallennettuihin biometrisiin tietoihin, esimerkiksi rikoksen selvittämiseksi. Biometriaa voidaan hyödyntää myös henkilöiden liikkeiden ja kontaktien jälkikäteiseen rekonstruointiin. Yksi

[16] IOM 2024, s. 2.
[17] IOM 2024, s. 4.
[18] Korja 2016, s. 142. Valokuvat voivat olla biometrisiä tietoja vain tilanteissa, joissa niitä käsitellään sellaisin erityisin teknisin menetelmin, jotka mahdollistavat luonnollisen henkilön yksilöllisen tunnistamisen tai todentamisen. Ks. Korpisaari ym. 2018, s. 73.
[19] ARTICLE 19 2021, s. 9.
[20] Korja 2016, s. 141–142.
[21] Korhonen 2005, s. 190.
[22] Euroopan tietosuojaneuvoston ohjeet 05/2022, s. 8.

käyttötarkoitus on etsintäkuulutettujen henkilöiden tunnistaminen julkisissa tiloissa. Tällöin videovalvontakameroiden tallentamia kasvoja verrataan reaaliaikaisesti viranomaisten tietokantoihin.[23] Lisäksi seulonnan avulla voidaan huomaamattomasti arvioida, kuuluuko henkilö esimerkiksi tarkkailulistalle.[24]

Julkisen sektorin lisäksi esimerkiksi kasvojentunnistus kiinnostaa myös yksityisellä sektorilla. Teknologiaa käytetään laajasti esimerkiksi mainonnassa, markkinoinnissa ja muissa tarkoituksissa, joissa sen avulla asiakkaita voidaan tunnistaa ja profiloida, jotta heidän mieltymyksiään voidaan ennustaa esimerkiksi kasvonilmeiden perusteella. Työelämässä kasvojentunnistusta voidaan käyttää analysoimaan työnhakijoiden ilmeitä[25] työhaastattelun aikana. Nämä käyttötavat herättävät kysymyksiä yksityisyydestä, syrjinnästä ja henkilötietojen käytön näkyvyydestä.[26]

## 2.2 Biometrisen tunnistamisen kehitys

Biometristen tunnisteiden historia juontaa juurensa tuhansien vuosien taakse. Jo muinaisessa Babyloniassa ja Kiinassa hyödynnettiin sormenjälkiä asiakirjojen sinetöintiin ja henkilöiden tunnistamiseen. Kiinassa allekirjoituksia vahvistettiin sormenjälkien avulla jo 200-luvulla eaa.[27]

Modernin biometrisen tunnistamisen kehitys alkoi 1800-luvulla. Ranskalainen poliisi ja biometrian tutkija *Alphonse Bertillon* kehitti menetelmän, jossa rikollisia tunnistettiin kehon mittojen perusteella ajatuksen kehon mittojen käyttämisestä rikollisten tunnistamiseen.[28] Tätä ajankohtaa pidetään biometrisen tunnistamisen ensimmäinen sukupolven alkuna.[29] Nämä tekniikat vaativat paljon aikaa ja asiantuntijoita tekemään manuaalisia mittauksia ja vertamaan pieniä yksityiskohtia. Manuaalisen vertailun tarkkuutta heikensivät muun muassa inhimilliset virheet.[30]

1800-luvulta lopulla lainvalvontaviranomaiset alkoivat hyödyntää sormenjälkiä järjestelmällisemmin, jolloin ne syrjäyttivät aiemmat kehon mittauksiin perustuvat tunnistusjärjestelmät.

---

[23]Euroopan tietosuojaneuvoston ohjeet 05/2022, s. 12–13.
[24] Jain ym. 2004, s. 2.
[25] Tunnereaktioiden tunnistamisella tarkoitetaan biometristä teknologiaa, jossa koneoppimisen avulla pyritään tunnistamaan yksilön tunnetiloja ja luokittelemaan ne erilaisiin kategorioihin, kuten viha, pelko ja onnellisuus. ARTICLE 19, s. 8.
[26] EU:n perusoikeusvirasto, Facial recognition technology: fundamental rights considerations in the context of law enforcement 2019, s. 2.
[27] Pugliese 2010, s. 26 ja Kindt 2013, s. 15–16.
[28] Jain ym. 2004, s. 2
[29] Korja 2016, s. 146.
[30] Gelb – Clark 2013, s. 1.

Brittiläinen virkamies *William Herchel* käytti sormenjälkiä henkilöiden tunnistamiseen Intiassa, ja häntä pidetäänkin ensimmäisenä eurooppalaisena, joka tunnisti sormenjälkien merkityksen tunnistamisessa.[31] Vuonna 1893 Yhdistyneen kuningaskunnan sisäministeriön toimisto hyväksyi, että kahdella henkilöllä ei ole samoja sormenjälkiä.[32]

1900-luvun alkuvuosikymmeninä biometrinen tunnistus kehittyi entisestään. Vuonna 1901 Sir *Edward Henry* kehitti Henry-luokittelujärjestelmän, joka mahdollisti sormenjälkien systemaattisen arkistoinnin ja tunnistamisen poliisityössä. 1920-luvulle mennessä sormenjälkitunnistusta käyttivät lainvalvojat ympäri maailmaa.[33] Toisen sukupolven alkuna pidetään 1900-luvun jälkipuoliskoa, jolloin nykymuodossaan tunnetut biometrisen tunnistamisen menetelmät yleistyivät.[34] Sormenjälki- ja kasvojentunnistuksen rinnalle kehittyi uusia menetelmiä, kuten iiriksen tunnistaminen, ja markkinoille tuotiin ensimmäisiä kaupallisia biometrisiä järjestelmiä.[35]

2000-luvun aikana biometrinen tunnistus yleistyi laajasti arkielämässä. Syyskuun 2001 terrori-iskut kiihdyttivät biometristen järjestelmien käyttöönottoa turvallisuuden, maahanmuuton ja matkustusasiakirjojen valvonnassa.[36] Biometrinen tunnistaminen nähtiin tehokkaana tapana parantaa turvallisuutta ja tehostaa viranomaisten välistä tiedonvaihtoa.[37] Vaikka biometrisiä passeja oli suunniteltu jo ennen terrori-iskuja, tapahtumat nopeuttivat niiden laajamittaista käyttöönottoa.[38]

Pelkkä poliittinen ilmapiiri ei olisi riittänyt käynnistämään biometrisen tunnistamisen teknologian yleistymistä. Teknologinen kehitys on alentanut kustannuksia sekä parantanut järjestelmien tarkkuutta, käytettävyyttä ja saatavuutta. Digitalisoituvassa maailmassa on lisääntynyt tarve tehokkaille ja luotettaville tunnistusmenetelmille.[39] Viimeisen vuosikymmenen aikana tekoälyn ja sensoreiden kehitys on vauhdittanut muun muassa kasvojentunnistusteknologian kehitystä.[40] Esimerkiksi biometrisessä etätunnistamisessa (*remote biometric identification*)

---

[31] Kindt 2013, s. 16.
[32] Jain ym. 2004, s. 2. Tästä seuraava tapahtumaketju johti ensimmäisen Automatic Fingerprint Identification System (AFIS) -järjestelmän syntymiseen 1960-luvulla
[33] Kindt 2013, s. 18.
[34] Korja 2016, s. 147.
[35] Kindt 2013, s. 18.
[36] Korja 2016, s. 148.
[37] IOM 2005, s. 5.
[38] IOM 2005, s. 9. Yksi käyttötarkoitus oli matkustamisen helpottaminen antamalla usein matkustaville mahdollisuus ilmoittaa biometriset tietonsa ja käyttää sitten lentokentällä pikakaistaa lähdettäessä ja saapuessaan. Tällaiset järjestelmät perustuivat tietojen vapaaehtoiseen ilmoittamiseen, ja niitä käytettiin henkilökohtaisen mukavuuden ja käsittelyn nopeuden vuoksi. Turvallisuussyistä biometrisiä järjestelmiä käytettiin ensisijaisesti lentokenttien rajoitetuille alueille pääsyyn.
[39] Korja 2016, s. 148.
[40] Ks. A Policy Framework for Responsible Limits on Facial Recognition Use Case: Law Enforcement Investigations 2022. s. 5.

tekoälyjärjestelmää hyödynnetään henkilön tunnistamiseen etäältä hänen biometrisiä tietojaan käyttämällä, usein ilman että henkilö tietää tunnistamisesta.[41]

Myös COVID-19-pandemia vaikutti biometrisen tunnistamisen kehitykseen. Kasvomaskien käyttö heikensi esimerkiksi kasvojentunnistusjärjestelmien tarkkuutta ja tämä herätti mielenkiinnon muun muassa periokulaarista tunnistusta kohtaan, jossa hyödynnetään silmänympärysalueen piirteitä henkilön tunnistamiseksi.[42]

## 2.3 Biometrisen tunnistamisen riskit

### 2.3.1 Yleistä biometrisen tunnistamisen riskeistä

Biometrinen tunnistaminen on herättänyt huolta muun muassa kansalaisjärjestöjen[43] ja tietosuojaviranomaisten[44] keskuudessa. Useat kansalaisjärjestöt ovat yhdessä luoneet *Reclaim Your Face* -kampanjan, jonka tavoitteena on massavalvontaan perustuvan biometrisen tunnistamisen kieltäminen.[45] Myös tekoälyasetuksen valmisteluvaiheessa Euroopan komissio tunnisti valkoisessa kirjassaan, että tekoälyn käyttö voi johtaa perusoikeuksien loukkauksiin.[46]

Tietosuojavaltuutetun toimiston entinen ylitarkastaja *Risto Heinonen* on todennut, että biotunnisteisiin sisältyy tavallisesti enemmän tietoa kuin henkilön tunnistamisen kannalta olisi tarpeen. Tiedot voivat olla arkaluonteisia ja paljastaa esimerkiksi henkilön terveydentilaan liittyviä yksityisiä tietoja. Lisäksi biotunnisteen tai kokonaisen biotunnisterekisterin varastaminen ja väärinkäyttö voi johtaa mittaviin haitallisiin seurauksiin. Yksityisyyden suojan näkökulmasta ongelmallista on se, että biometrinen tunnistaminen mahdollistaa henkilön tunnistamisen automaattisesti myös hänen tietämättään.[47]

Tietojen kerääminen automatisoidun tietojenkäsittelyn, profiloinnin ja joukkovalvonnan kautta, voi johtaa siihen, että erityisesti haavoittuvassa asemassa olevien yksilöiden oikeuksiin puututaan mielivaltaisesti tai lainvastaisesti. Esimerkiksi lasten kohdalla vaikutukset voivat ulottua

---

[41] Ks. Joint civil society recommendations for an EU Artificial Intelligence Act for Fundamental Rights Biometrics Part 1: Article 3(36) and Article 5(1)(d), s. 1.
[42] Gomez-Barrero ym. 2022, s. 1–5. Pandemian hallintatoimia olivat esimerkiksi karanteeni- ja kontaktien jäljitystyssovellukset sekä poliisien käyttämät valvontalaitteet, kuten kypärät, jotka mittaavat kuumetta julkisissa tiloissa ohikulkijoilta. Ks. Kansainvälinen ihmisoikeusjärjestö ARTICLE 19 linjaus 2021, s. 7,22.
[43] Esimerkiksi ARTICLE 19 ja IOM ovat ilmaisseet huolensa biometristen teknologioiden vaikutuksista perus- ja ihmisoikeuksiin. European union agency for fundamental rights (FRA) on koonnut tekoälyn ja algoritmien aiheuttumia riskejä yksityisyydellä ja henkilötietojen suojalle.
[44] Euroopan tietosuojaneuvoston ja Euroopan tietosuojavaltuutetun yhteinen lausunto 5/2021.
[45] ks. Reclaim Your Face verkkosivut.
[46] COM (2020) 65 final, s. l0.
[47] Korhonen 2005, s. 189.

pitkälle tulevaisuuteen.[48] Biometrisen tunnistamisen teknologiaa ei käytetä vain henkilöiden tunnistamiseen, vaan enenevissä määrin myös henkilöiden valvontaan ja tarkkailuun. Fyysisten toimintaympäristön rinnalla toimii digitaalinen toimintaympäristö. Digitaalisessa ympäristössä perus- ja ihmisoikeuksien loukkaaminen on helpompaa, minkä vuoksi perus- ja ihmisoikeuksien merkitys korostuu.[49]

Biometristen tunnisteiden erityispiirteet aiheuttavat useita yksityisyyden suojaan ja henkilötietojen käsittelyyn liittyviä riskejä, joita tarkastellaan seuraavaksi.

### 2.3.2 Tietojen kerääminen, tallentaminen ja säilyttäminen sekä tietoturvariskit

Biometristen teknologioiden kehittäminen ja käyttöönotto edellyttävät suurten henkilötietomäärien keräämistä ja käsittelyä. Biometriset tiedot kuuluvat erityisiin henkilötietoihin, sillä ne voivat paljastaa yksilöstä hyvin arkaluonteisia tietoja, kuten sormenjälkiä, silmän skannauksia sekä tietoja etnisestä taustasta tai sukupuolesta. Tämän vuoksi niiden käsittely edellyttää korostettuja suojatoimia ja tietosuojaa.[50]

Jo lähtökohtaisesti biometrinen teknologia on luonteeltaan varsin tunkeilevaa. Lisäksi tietoaineistoja kerätään usein puutteellisin tai vinoutunein menetelmin, jolloin ne eivät välttämättä edusta väestöä kokonaisuutena ja voivat vahvistaa olemassa olevia yhteiskunnallisia stereotypioita. Ongelmallista on lisäksi biometrisen datan laaja ja usein rajoittamaton säilyttäminen, joka ei aina täytä välttämättömyyden ja suhteellisuuden vaatimuksia. Tietojen käsittelijät säilyttävät biometrisiä tietoja usein pidempään kuin alkuperäinen käyttötarkoitus edellyttäisi.[51]

Tietomurtoihin liittyvät riskit korostuvat erityisesti keskitetysti hallituissa tietokannoissa. Tietokantojen tietomurtojen havaitseminen on vaikeaa ja niiden korjaaminen on erittäin kallista. Lisäksi yksilöillä on usein rajalliset mahdollisuudet saada hyvitystä kärsimästään vahingosta. Toisin kuin salasanat, biometriset tiedot eivät ole vaihdettavissa tietomurron jälkeen, vaan niitä voidaan käyttää yksilön tunnistamiseen ja seuraamiseen koko elämän ajan. Riskit kohdistuvat erityisesti haavoittuvissa asemissa oleviin ryhmiin ja valtioihin, joissa tietoturvainfrastruktuuri on puutteellista tai kehittymätöntä. Tällaisessa ympäristössä biometrisen datan säilyttäminen viranomaisten tai yksityisten toimijoiden hallussa voi herättää merkittäviä luottamukseen liittyviä huolia.[52]

---

[48] YK:n lapsen oikeuksien komitean yleiskommentti nro 25 (2021), s. 16.
[49] Korja 2016, s. 69–70.
[50] ARTICLE 19 2021, s. 16.
[51] ARTICLE 19 2021, s. 16.
[52] ARTICLE 19 2021, s. 16-17.

Biometrisiä tietoja, kuten muitakin henkilötietoja, voidaan kerätä myös oikeudettomasti ilman henkilön suostumusta. Lisäksi riskinä on tietojen tarpeeton kerääminen. Pelkästään teknologian saatavuus voidaan nähdä riittävänä perusteena sen käytölle ilman asianmukaista arviota välttämättömyydestä ja suhteellisuudesta.[53]

### 2.3.3 Oikeudeton käyttö

Käyttötarkoituksen laajeneminen (*function creep*) on ilmiö, jossa rajattuun tarkoitukseen suunniteltu teknologia voi saada vähitellen uusia, odottamattomia käyttötarkoituksia tai toimintoja. Tämä voi tapahtua virallisesti käyttöä laajennettaessa päätöksillä tai epävirallisesti järjestelemän väärinkäytön kautta.[54] Vaikka käyttötarkoituksen laajentuminen tapahtuisi alun perin hyväksyttävistä syistä, siihen saattaa liittyä merkittäviä oikeudellisia ja eettisiä ongelmia. Jos alun perin tiettyä tarkoitusta varten annettua toimivaltaa käytetään muihin tarkoituksiin, voi syntyä legitimiteettiongelmia. Tällöin ei välttämättä ole selkeää oikeusperustaa sille, miten valtaa käytetään uudessa tarkoituksessa, eikä lainsäädännössä ole huomioitu tarvittavia valvonta- ja tarkastusmekanismeja.[55]

Käyttötarkoituksen laajeneminen voi ilmetä esimerkiksi siten, että alun perin turvallisuuteen tai terveyden seurannan välineeksi kehitetty järjestelmä muuttuu vähitellen yleiseksi valvontavälineeksi. Esimerkiksi pandemian hallintaa varten kerättyjä biometrisiä tietoja voisivat myöhemmin käyttää lainvalvontaviranomaiset, vakuutusyhtiöt tai työnantajat muihin tarkoituksiin.[56]

Käyttötarkoituksen laajentuminen voi ilmetä useilla eri tavoilla. Tietokantoja voidaan ensinnäkin laajentaa lisäämällä niihin henkilökategorioita alkuperäisen käyttötarkoituksen ulkopuolelta. Toiseksi käyttötarkoitus voi laajentua.[57] Tällöin teknologian käyttötarkoitus laajenee koskemaan sellaisia toimintoja ja tiedonkeruuta, joita ei alun perin ole hyväksytty.[58] Esimerkiksi rikollisten tunnistamiseen tarkoitettua teknologiaa voidaan hyödyntää väkijoukkojen analysointiin, käyttäytymisen ennustamiseen tai yksilöiden jatkuvaan seurantaan. Lisäksi käyttäjäkunta tai käyttöympäristö voi muuttua. Järjestelmää voivat alkaa käyttää uudet toimijat, mikä lisää väärinkäytön riskiä. Järjestelmiä voidaan ottaa käyttöön uusilla alueilla, kuten siirtyä

[53] ARTICLE 19 2021, s. 18.
[54] Brey 2004, kappale Function creep.
[55] Koops 2021, s. 47.
[56] Israel 2024, s. 3.
[57] Brey 2004, kappale Function Creep.
[58] ARTICLE 19 2021, s. 16.

julkisista tiloista yksityisiin ympäristöihin. Käyttötarkoituksen laajentuminen on yleinen ilmiö uutta teknologiaa käytettäessä. Sitä voidaan rajoittaa sääntelyllä, mutta ei kokonaan estää.[59]

Biometrinen data mahdollistaa myös profiloinnin. Profiloinnilla tarkoitetaan prosessia, jossa tietokannoista etsitään eri tietojen välisiä yhteyksiä ja näiden perusteella muodostetaan profiileja, joiden avulla henkilö voidaan tunnistaa, kuvata tai sijoittaa tiettyyn ryhmään.[60]

### 2.3.4 Massavalvonta

Euroopan neuvosto määrittelee massavalvonnan valvonnaksi, joka ei kohdistu tiettyyn yksilöityyn henkilöön, vaan yleisöön kokonaisuutena. Euroopan unionin perusoikeusvirasto puolestaan korostaa, että kohdentamaton valvonta käynnistyy ilman ennakkoperustetta tai epäilyä. Täten siihen liittyy ennakoiva elementti, jonka tarkoituksena on pikemminkin tunnistaa vaara kuin tutkia tunnettua uhkaa. Käytännössä tällaiset valvontatoimet kohdistuvat usein suhteettomasti ryhmiin, jotka ovat jo valmiiksi tarkkailun kohteena, kuten maahanmuuttajiin, vähävaraisiin yhteisöihin ja rodullisiin ryhmiin, mikä voi syventää rakenteellista syrjintää. [61]

Vuosikymmeniä sitten valvontakameroita otettiin käyttöön ympäri maailmaa rikollisuuden ehkäisemisen nimissä. Nykyisin samoihin järjestelmiin voidaan integroida biometrisen analyysin ominaisuuksia, mikä laajentaa merkittävästi etävalvonnan ulottuvuutta: pelkkien tapahtumien havainnoinnin sijaan on mahdollista seurata myös toimijoiden henkilöllisyyttä ja liikkumista.[62] Teknologian kehitys on johtanut entistä parempiin mahdollisuuksiin valvoa ihmisiä ja heidän elämänpiiriään välittömästi ja välillisesti. Valvonta ei rajoitu vain julkisen vallan toimintaan, vaan myös yksityiset toimijat hyödyntävät biometrisiä järjestelmiä toiminnan tehostamiseen.[63]

Kasvojentunnistukseen perusturva massavalvonta voi estää anonyymin liikkumisen julkisilla paikoilla. Esimerkiksi Ranska hyväksyi lain, joka mahdollisti laajamittaisen tekoälypohjaisen videovalvonnan laajamittaisen käytön vuoden 2024 olympialaisten aikana. Tekoälypohjaisessa

---

[59] Brey 2004, kappale Function Creep.
[60] Neuwirth 2022, s. 12.
[61] ks. EDRi Ban Biometric Mass Surveillance 2020, s. 10. Myös kohdennetun valvonnan kohdalla yksityisyyden suojan ja oikeudenmukaisen menettelyn periaatteet edellyttävät, että viranomaisilla on laillinen peruste ja perusteltu epäily henkilöä kohtaan ennen kuin valvontaan ryhdytään.
[62] EDRi Ban Biometric Mass Surveillance 2020, s. 10–11. Jopa valvontakameroiden kannattajien on ollut vaikea esittää vakuuttavaa näyttöä niiden tehokkuudesta rikosten ennaltaehkäisyssä; lähinnä on voitu todeta, että niistä voi olla hyötyä rajatuissa ja erityisissä tilanteissa rikostutkinnan tai syyteharkinnan tukena.
[63] Saarenpää 2012, s. 226, 244. Toukokuuhun 2020 mennessä ainakin 15 Euroopan maata oli kokeillut biometrisiä teknologioita, kuten kasvojentunnistusta, julkisissa tiloissa tarkoituksiin, jotka johtavat massavalvontaan. Näihin maihin kuuluu muun muassa Tanska, Ruotsi, Saksa, Italia ja Ranska. Kyseisiä järjestelmiä on usein otettu käyttöön ilman riittävää avoimuutta ja vastuullisuutta. Monissa tapauksissa puuttuvat myös asianmukaiset arviot toimien välttämättömyydestä ja suhteellisuudesta, samoin kuin riittävä julkinen tiedottaminen ja laajempi yhteiskunnallinen keskustelu. Ks. EDRi: Ban Biometric Mass Surveillance 2020, s. 7.

valvonnassa hyödynnettiin algoritmeja, jotka analysoivat reaaliaikaista videokuvaa jo olemassa olevista valvontajärjestelmistä tunnistaakseen mahdollisia uhkia julkisissa tiloissa.[64]

Massavalvontaan liittyviä huolia heräsi myös *Clearview AI* tapauksessa. Yhdysvaltalainen yhtiö kehitti kasvojentunnistussovelluksen, joka vertaili käyttäjän syöttämää kuvaa laajaan internetistä kerättyyn kuvamateriaaliin. Kuvia oli kerätty muun muassa ihmisten sosiaaliseen mediaan ja verkostoitumistarkoituksiin lataamista kuvista. Sovellusta oli myyty muun muassa poliisiviranomaisille.[65] Muun muassa Ruotsissa poliisit olivat käyttäneet tätä sovellusta yksilöiden tunnistamiseen useissa eri tilanteissa. Käyttäessään sovellusta poliisi oli luvattomasti käsitellyt biometristä dataa kasvojen tunnistusta varten ja jättänyt tekemättä tietosuojavaikutusten arvioinnin.[66]

### 2.3.5 Virheellinen tulos

Biometristen järjestelmien keskeinen lupaus on niiden kyky tehdä oikeita päätöksiä tunnistustilanteissa. Käytännössä täydellistä takuuta ei voida antaa. Ensinnäkin järjestelmä voi antaa väärän osuman. Tämä voi tapahtua esimerkiksi silloin, kun järjestelmä yhdistää syötetyn tunnisteen tietokannassa olevaan väärään henkilöön. Toiseksi järjestelmä voi antaa väärän ei-vastauksen. Tässä tapauksessa järjestelmä ei tunnista oikeaa osumaa.[67] Onkin tärkeää muistaa, että biometriset tunnistusteknologiat eivät anna ehdotonta tulosta, vaan ne perustuvat todennäköisyyteen.[68]

EU:n perusoikeusvirasto on todennut vuoden 2019 raportissaan, että kasvojentunnistusohjelmistojen tarvittavan tarkkuuden määrittäminen on haastavaa, koska tarkkuutta voidaan arvioida monin eri tavoin muun muassa tehtävän, tarkoituksen ja käyttöyhteyden mukaan. Kun teknologiaa käytetään paikoissa, joissa liikkuu suuri ihmisjoukkoja, pienikin virheprosentti voi johtaa merkittävään määrään virheellisiä tunnistuksia. Lisäksi virheet eivät jakaudu tasaisesti, vaan tietyt ihmisryhmät voivat joutua muita useammin virheellisesti tunnistetuiksi. On myös hyvä huomioida järjestelmien alttius huijauksille, kuten väärennetyille kasvokuville. Tämä korostuu

[64] Koula (ei päivätty), s. 1.
[65] EDRi Ban Biometric Mass Surveillance 2020, s. 32.
[66] Ruotsin tietosuojaviranomaisen ratkaisu 10.2.2021, s. 2. Viranomainen määräsi asiassa sakon sekä poliisin tarjoamaan lisäkoulutusta työntekijöilleen vastaavien tapausten välttämiseksi. Toukokuussa 2021 joukko järjestöjä teki useita valituksia Clearview AI vastaan. Valituksia toimitettiin tietosuojaviranomaisille Ranskassa, Itävallassa, Italiassa, Kreikassa ja Yhdysvalloissa. ks. EDRi, About ClearviewAI's mockery of human rights, those fighting it, and the need for EU to intervene.
[67] Jain ym. 2004, s. 3.
[68] Euroopan tietosuojaneuvoston ohjeet 05/2022, s. 14.

erityisesti lainvalvonnassa, jossa virheellisillä tunnistuksilla ja väärinkäytöksillä voi olla vakavia seurauksia.[69]

Yhdysvaltain kansallisen standardien ja teknologian instituutin (NIST) vuonna 2019 julkaisema tutkimus osoitti, että väärien positiivisten tulosten erot ovat paljon suurempia kuin väärien negatiivisten tulosten erot. Eri väestöryhmissä väärien positiivisten tulosten määrä vaihtelee usein kymmenkertaisesti ja jopa yli satakertaisesti. Joidenkin algoritmien suorituskyvyssä havaittiin eroja tarkkuudessa muun muassa sukupuolen ja etnisen taustan perusteella.[70]

Tunnistusteknologian tarkkuus riippuu vahvasti käytetyn datan laadusta. Laatuun vaikuttaa esimerkiksi valaistus, kuvan tarkkuus, ikä ja sukupuoli. Esimerkiksi laadukkaat kontrolloiduissa olosuhteissa otetut kuvat, kuten passikuvat, tuottavat yleensä parempia tuloksia kuin heikkolaatuiset kuvat, esimerkiksi valvontakameroista.[71] Kasvojentunnistuksen osalta on huomattava, että kasvot muuttuvat merkittävästi ajan myötä ja voivat jopa vaihdella päivästä toiseen. Esimerkiksi ikääntyminen, kosmetiikka, plastiikkakirurgia, päihteiden väärinkäytön ja kuvakulma voivat kaikki vaikuttaa kasvojen ulkonäköön. Tästäkin syystä kasvojentunnistuksen tuloksia tulisi aina pitää tutkinnallisena johtolankana.[72]

Kasvojentunnistus perustuu usein valmiiksi koulutettuihin tekoälymalleihin, joiden toiminta riippuu koulutusdatan laadusta ja edustavuudesta. Jos koulutusdata ei sisällä riittävästi erilaisia ihmisryhmiä, järjestelmä voi toimia heikommin naisten ja ei-valkoihoisia henkilöiden kohdalla. Järjestelmien luetettavuutta haittaa myös koulutusdatan heikko läpinäkyvyys.[73]

Erityisesti lainvalvontaviranomaisten tulisi olla tietoisia näistä mahdollisista suorituskyvyn puutteista ja ottaa käyttöön asianmukaisia hallintoprosesseja niiden lieventämiseksi. Näin toimiessaan ne rajoittaisivat väärien tulosten riskiä ja mahdollisia henkilöiden perusteettomia pidätyksiä kasvojentunnistusteknologia -järjestelmän tulosten perusteella.[74]

---

[69] EU:n perusoikeusvirasto: Facial recognition technology: fundamental rights considerations in the context of law enforcement 2019, s. 9.
[70] NISTIR 8280, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, 2019, s. 2-3. Tutkimuksessa havaittiin esimerkiksi, että kaikissa algoritmeissa ja tietojoukoissa väärät positiiviset tunnistukset ovat korkeampia naisilla kuin miehillä. Lisäksi havaittiin kohonneita väärien positiivisten määriä iäkkäillä ja lapsilla; vaikutukset olivat suurempia vanhimmilla ja nuorimmilla ja pienimpiä keski-ikäisillä aikuisilla.
[71] EU:n perusoikeusvirasto: Facial recognition technology: fundamental rights considerations in the context of law enforcement 2019, s. 10.
[72]A Policy Framework for Responsible Limits on Facial Recognition Use Case: Law Enforcement Investigations 2022, s. 11.
[73] EU:n perusoikeusvirasto: Facial recognition technology: fundamental rights considerations in the context of law enforcement 2019, s. 10.
[74] A Policy Framework for Responsible Limits on Facial Recognition Use Case: Law Enforcement Investigations 2022, s. 5 - 6. Myös suuret yhdysvaltalaiset teknologiayritykset ovat muodostaneet kantansa tähän aiheeseen. Vuonna 2020 tapahtuneiden tapahtumien, kuten Clearview -tapauksen, seurauksena epäluottamus poliisilaitoksia kohtaan Yhdysvalloissa ja maailmanlaajuisesti lisääntyi. IBM ilmoitti, ettei se enää tarjoa, kehitä tai tutki

# 3 Yksityisyys ja henkilötietojen suoja

## 3.1 Perus- ja ihmisoikeudet Euroopan unionissa

Perus- ja ihmisoikeudet ovat keskeinen osa unionin oikeutta. Niiden merkitys näkyy esimerkiksi uutta unionin lainsäädäntöä valmisteltaessa sekä Euroopan unionin tuomioistuimen oikeuskäytännössä, jossa perusoikeusnäkökulma on saanut vahvempaa asemaa. Perus- ja ihmisoikeudet eivät ole erillinen osa oikeusjärjestystä, vaan ne vaikuttavat kaikilla unionin oikeuden alueilla.[75]

Perusoikeuksien kunnioittaminen demokratian ja oikeusvaltioperiaatteen puitteissa muodostaa vahvan perustan eettisten periaatteiden ja arvojen määrittelylle myös tekoälyn yhteydessä. Euroopan unionin perussopimukset ja perusoikeuskirja sisältävät useita perusoikeuksia, joita EU:n jäsenvaltioiden ja toimielinten on oikeudellisesti kunnioitettava pannessaan unionin lainsäädäntöä täytäntöön. Perusoikeudet muodostavat yhtäältä perustan lainmukaiselle tekoälysääntelylle ja toisaalta ne tarjoavat keskeisen viitekehyksen tekoälyn eettiselle arvioinnille.[76]

Euroopan unionin perus- ja ihmisoikeuksia sääntelevät keskeisesti Euroopan unionin perusoikeuskirja ja Euroopan ihmisoikeussopimus.

### 3.1.1 Euroopan ihmisoikeussopimus

Vuonna 1950 Euroopan neuvosto laati yleissopimuksen ihmisoikeuksien ja perusvapauksien suojaamisesta, joka tunnetaan vakiintuneesti Euroopan ihmisoikeussopimuksena. Sopimus velvoittaa Euroopan neuvoston jäsenmaita, jotka ovat sitoutuneet turvaamaan yleissopimuksen mukaiset oikeudet kaikille lainkäyttövaltansa piirissä oleville henkilöille heidän kansalaisuudestaan riippumatta.[77]

Euroopan ihmisoikeussopimuksessa turvatut oikeudet ja vapaudet sijoittuvat pääosin ihmisoikeuksien sukupolvijaottelun ensimmäisen sukupolven oikeuksiin eli klassisiin vapausoikeuksiin, joita kutsutaan myös kansalais- ja poliittisiksi oikeuksiksi. Näille oikeuksille on ominaista valtion negatiivinen velvollisuus pidättäytyä puuttumasta sopimuksessa suojattuihin oikeuksiin

---

kasvojentunnistusteknologiaa, kun taas Microsoft lupasi lopettaa kasvojentunnistusteknologia myynnin lainvalvontaviranomaisille Yhdysvalloissa, kunnes liittovaltion sääntely otettaisiin käyttöön. Vuonna 2022 Microsoft meni tätäkin pidemmälle ja asetti uusia rajoituksia ja suojatoimia kasvojentunnistusteknologian kaikelle käytölle osana laajempaa tekoälyperiaatteiden kokonaisuutta. Vuonna 2021 myös Amazon Web Services (AWS) jatkoi vuonna 2020 asettamaansa Rekognition-alustan poliisikäytön kieltoa.

[75] Penttinen 2017, s. 77.

[76] Tekoälyä käsittelevä korkean tason asiantuntijaryhmän laatimat eettiset ohjeet 2019, s. 12.

[77] Korpisaari 2022, s. 5.

ja vapauksiin. Kuitenkin Euroopan ihmisoikeustuomioistuin on oikeuskäytännössään katsonut lähes jokaisen artiklan osalta, että sopimuksesta on johdettavissa myös valtiolle positiivinen velvollisuus ryhtyä toimenpiteisiin, jotta oikeudet toteutuvat käytännössä tehokkaasti ja todellisesti.[78]

### 3.1.2 Euroopan unionin perusoikeuskirja

Euroopan unionin perusoikeuskirjaan koottiin unionin tasolla voimassa olevat perusoikeudet. Tavoitteena oli tuoda unionin oikeudessa tunnustetut oikeudet ja periaatteet paremmin unionin kansalaisten tietoisuuteen ja helpottaa niihin vetoamista, mikä vahvistaisi unionin oikeuteen perustuvaa oikeussuojaa.[79] Kaikilla perusoikeuskirjassa olevilla oikeuksilla on olemassa oleva oikeusperusta, joita ovat muun muassa Euroopan ihmisoikeussopimus ja muut kansainväliset ihmisoikeusasiakirjat. Kyseisten sopimusten ohella perusoikeuskirjaan pyrittiin tuomaan jäsenvaltioiden yhteisiin valtiosääntöperinteisiin pohjautuvia sekä Euroopan ihmisoikeustuomioistuimen ja Euroopan unionin tuomioistuimen oikeuskäytäntöön perustuvia oikeuksia.[80]

Ennen perusoikeuskirjan julkaisua EU:ssa ei ollut sitovasti määritelty unionin tai sen kansalaisten perusoikeuksia. Tästä huolimatta perusoikeuksilla on ollut vankka asema unionin tuomioistuimen oikeuskäytännössä, jossa on viitattu perusoikeuksien merkitykseen EU-oikeuden tulkinnassa jo 1960-luvulta lähtien. EU-tuomioistuimen oikeuskäytännöllä onkin ollut merkittävä rooli perusoikeuksien kehittämisessä unionissa.[81]

Perusoikeuskirjan määräykset sitovat sekä unionin toimielimiä ja laitoksia että jäsenvaltioita niiden soveltaessa EU-oikeutta. Perusoikeuskirja ei luonut Euroopan unionille uusia tehtäviä tai toimivaltuuksia, eikä sitä saa tulkita siten, että se rajoittaisi tai loukkaisi jäsenvaltioiden kansallisissa perustuslaeissa tunnustettuja perus- ja ihmisoikeuksia.[82]

Lissabonin sopimuksen myötä vuonna 2009 perusoikeuskirjan asema muuttui heikosti sitovasta soft law:sta osaksi unionin primaarioikeutta. Lissabonin sopimuksella lisättiin sopimukseen Euroopan unionista (SEU) 6 artiklan 1 kohta, jonka mukaan unioni tunnustaa Euroopan unionin perusoikeuskirjan sisältämät oikeudet, vapaudet ja periaatteet. Osana unionin primäärioikeutta perusoikeuskirja on sellaisenaan sitova ja suoraan sovellettavaa oikeutta. Perusoikeuskirjalla on sama oikeudellinen asema kuin perussopimuksilla, ja siihen viittaaminen argumentaatiossa

[78] Hirvelä – Heikkilä 2017, s. 5.
[79] Walkila 2011, s. 818.
[80] Nikula 2000, s. 524.
[81] Kujala 2012, s. 124–125.
[82] Nikula 2000, s. 525.

on tullut arkipäiväiseksi Euroopan unionin tuomioistuimessa. Ratkaisut sisältävät myös usein viittauksia muihin perus- ja ihmisoikeusasiakirjoihin, kuten Euroopan ihmisoikeussopimukseen ja EU:n yleisiin oikeusperiaatteisiin.[83]

Unionin perusoikeuskirjan takaamien perusoikeuksien merkitys ja ulottuvuus vastaavat pitkälti Euroopan ihmisoikeussopimuksen tasoa. Perusoikeuskirjan 52 artiklassa täsmennetään, että unioni voi myöntää Euroopan ihmisoikeussopimusta laajempaa suojaa. Näin ollen Euroopan ihmisoikeussopimus määrittää perusoikeuskirjan takaaman suojan vähimmäistason.

## 3.2 Yksityisyys ja henkilötietojen suoja ihmisoikeuksina

### 3.2.1 Yksityisyys käsitteenä

Ihmisillä on ollut aina tarve yksityisyyteen. Jo antiikin aikana tehtiin jakoa yksityiseen ja julkiseen, mutta oikeudellisena käsitteenä se on kuitenkin verrattain uusi. Englanninkielisenä käsitteenä yksityisyys jäi aluksi kehittymään Yhdysvalloissa. Euroopassa puolestaan omaksuttiin Euroopan ihmisoikeussopimukseen ilmaisu yksityiselämä 1950-luvulla. *Saarenpään* mukaan voidaan sanoa, että Euroopan ihmisoikeussopimuksen 8 artikla on kehityksen myötä muuttunut yksityiselämästä koskemaan laajemmin yksityisyyttä.[84]

Yksityisyyttä ei ole tarkasti määritelty lainsäädännössä. Kyse on suhdekäsitteestä, jonka määritelmä muuttuu ihmiskäsityksen ja yhteiskunnan muuttuessa. Liian täsmällinen määrittely johtaisi käsitteen keinotekoisuuteen ja edellyttäisi jatkuvaa lainsäädännön päivittämistä. *Saarenpään* mukaan riittävää on luonnehtia yksityisyys oikeudeksemme olla yksin suhteessa muihin yksilöihin, yhteisöihin ja yhteiskuntaan sekä oikeudeksemme päättää itse siitä, miten paljon, millä tavoin ja millä hinnalla yksityisyyttämme paljastetaan muille. Yksityisyys ei merkitse täten vain suojaa muilta, vaan lisäksi oikeutta päättää ja toimia.[85]

Yksityisyys liittyy läheisesti itsemääräämisoikeuteen, jolla tarkoitetaan yksilön oikeutta päättää itseään koskevista asioista sekä valvoa niiden toteutumista ja saada oikeusturvaa yhteiskunnassa. Digitaalisessa verkkoyhteisössä ulkoinen vapaus merkitsee enenevissä määrin oikeutta pysytellä moninaisten teknisten valvonnankeinojen ulkopuolella.[86] Fyysisen yksityisyyden lisäksi digitaalinen identiteettimme kuuluu itsemääräämisoikeuden piiriin.[87]

---

[83] Walkila 2011, s. 816–819.
[84] Saarenpää Näkökulmia yksityisyyteen, tietoturvaan ja valvontaan, s. 1.
[85] Saarenpää 2012, s. 241.
[86] Saarenpää 2012, s. 230–231.
[87] Saarenpää ym. 2004, s. 21.

Yksityisyys ei kuitenkaan ole ehdoton tai aukoton oikeus eikä se takaa meille mahdollisuutta täydelliseen vetäytymiseen muiden toimijoiden ulottumattomiin.[88] Oikeus on jatkuvassa muutosliikkeessä, johon vaikuttavat muun muassa eurooppalainen demokraattinen oikeusvaltio sekä yhteiskunnan ja teknologian kehitys.[89] Nauttiaksemme monista nyky-yhteiskunnan tarjoamista eduista, voimme joutua luopumaan yksityisyytemme jostain osasta. Kyse on ikään kuin vaihtokaupasta. Teknologia ei kuitenkaan itsessään loukkaa yksityisyyttä, vaan sitä käyttävien henkilöiden ja heidän noudattamistaan käytännöistä voi aiheutua oikeuden loukkauksia.[90]

### 3.2.2 Yksityisyys lainsäädännössä

Euroopan unionin perusoikeuskirjan 7 artiklan mukaan ”*jokaisella on oikeus siihen, että hänen yksityis- ja perhe-elämäänsä, kotiaan sekä viestejään kunnioitetaan*”. Henkilötietojen suojasta on säädetty erikseen 8 artiklassa. Sen mukaan jokaisella on oikeus henkilötietojen suojaan. Artiklan toisessa kohdassa on asetettu vaatimuksia tietojen käsittelylle.[91]

Euroopan ihmisoikeussopimuksen 8 artiklan mukaan

> ”*1. jokaisella on oikeus nauttia yksityis- ja perhe-elämäänsä, kotiinsa ja kirjeenvaihtoonsa kohdistuvaa kunnioitusta*”.
>
> *2. Viranomaiset eivät saa puuttua tämän oikeuden käyttämiseen, paitsi silloin kun laki sen sallii ja se on demokraattisessa yhteiskunnassa välttämätöntä kansallisen ja yleisen turvallisuuden tai maan taloudellisen hyvinvoinnin vuoksi, tai epäjärjestyksen ja rikollisuuden estämiseksi, terveyden tai moraalin suojaamiseksi, tai muiden henkilöiden oikeuksien ja vapauksien turvaamiseksi”.*

Euroopan ihmisoikeussopimuksen 8 artikla asettaa sekä negatiivisia että positiivisia velvoitteita. Artikla ei rajoitu vain viranomaisten toimiin perustuviin yksityiselämään kohdistuviin puuttumisiin, vaan sillä on tulkittu olevan horisontaalinen ulottuvuus eli ihmisoikeusvelvoitteet

---

[88] Saarenpää 2012, s. 241.
[89] Saarenpää Näkökulmia yksityisyyteen, tietoturvaan ja valvontaan, s. 1–2.
[90] Garfinkel 2000, s. 5–6. Yksityisyyttä loukkaava teknologia ei ole olemassa tyhjiössä, vaan tietoon, markkinoiden ja yhteiskunnan risteyksessä. *Garfinkelin* mukaan harvat insinöörit suunnittelevat järjestelmiä, jotka on suunniteltu loukkaamaan yksityisyyttä ja autonomiaa, ja harvat yritykset tai kuluttajat käyttäisivät tällaisia järjestelmiä, jos he ymmärtäisivät seuraukset. Usein uuden teknologian yksityisyys näkökulmat jäävät huomaamatta tai ne ymmärretään väärin.
[91] Euroopan unionin perusoikeuskirja 8 artikla. Tietojen käsittelyn tulee olla asianmukaista, tiettyä tarkoitusta varten tapahtuvaa, asianomaisen suostumukselle tai laissa säädetyn oikeuttavan perusteen nojalla tapahtuvaa. Jokaisella tulee olla oikeus tutustua niihin tietoihin, joita hänestä on kerätty.

ulottuvat välillisesti myös yksityiseen sektoriin. Valtion vastuu yksityisten toimijoiden aiheuttamista loukkauksista toteutuvat epäsuorasti positiivisten velvoitteiden kautta. Tämän merkitys on kuitenkin huomattava, kun otetaan huomioon yksityisen sektorin kasvava rooli julkisten palvelujen tuottamisessa dataan perustuvien tuotteiden ja järjestelmien avulla, erityisesti rikosoikeuden ja kansallisen turvallisuuden aloilla.[92] Artiklan kattavuus on ajan kuluessa laajentunut, sillä sitä on tulkittu joustavasti soveltaen sitä uusiin aihealueisiin.[93] Euroopan ihmisoikeussopimuksessa henkilötietojen suojasta ei ole erillistä mainintaa, mutta EIT:n tuomiosta *Leander v. Ruotsi* lähtien sen on katsottu kuuluvan yksityisyyden suojan turvaavaan 8 artiklan alaan.[94]

Yksityiselämän suoja ei rajoitu vain niin sanottuun ”ydinalueeseen”, vaan ulottuu myös yksilön vuorovaikutuksen muiden kanssa sekä hänen liikkumisensa, myös julkisissa tiloissa. Tämän vuoksi yksityiselämään kohdistuva puuttuminen voi toteutua jo silloin, kun henkilön sijaintia ja liikkumista koskevaa tietoa kerätään julkisesta ympäristöstä.[95] Euroopan ihmisoikeustuomioistuin on katsonut muun muassa poliisin suorittamaa ennaltaehkäisevää valvontaa ja matkustamisen seurantaa koskevassa ratkaisussa *Shimovolos v. Venäjä*, että valtion valvontatarkoituksiin kerätty ja tallennettu tieto henkilön liikkeistä junalla tai lentokoneella merkitsi puuttumista hänen yksityiselämäänsä.[96]

Euroopan ihmisoikeustuomioistuin on esimerkiksi tunnistanut keskeisten teknologisten kehitysten vaikutuksen siihen, miten laajasti viestinnän seuranta voi puuttua yksityiselämään. Euroopan ihmisoikeustuomioistuimen lähestymistapa kehittyviin teknologioihin ja niiden vaikutuksista yksityisyyteen on vaikuttanut myös siihen, että Euroopan ihmisoikeustuomioistuin on kehityksen valossa kumonnut ja arvioinut uudelleen merkittäviä aiempia johtopäätöksiä. Esimerkiksi asiassa *Liberty v. UK* tuomioistuin katsoi aiemmasta oikeuskäytännöstä poiketen, että samoja oikeusvaltioperiaatteeseen perustuvia arviointikriteerejä, joita käytetään kohdennetun

[92] Loideain 2025, s. 33, 35.
[93] Hirvelä – Heikkilä 2017, s. 628. Pysyäkseen ajan tasalla viestintäteknologian ja valvontakykyjen nopeassa kehityksessä Euroopan ihmisoikeustuomioistuin on kuitenkin hyödyntänyt Euroopan ihmisoikeussopimuksen 8 artiklan 1 kohdan laajaa tulkintaa laajentaakseen suojan soveltamisalaa. Yksityiselämän käsitteen on katsottu kattavan muun muassa pääsyn viestintätietoihin verkossa ja sen ulkopuolella, matkapuhelimet, sijaintitiedot ja massavalvontaohjelmat ks. Loideain 2025, s. 40.
[94] Koillinen 2012, s. 177.
[95] Loideain 2025, s. 38.
[96] EIS, *Shimovolos v. Venäjä* tuomio 21.6.2011, kappale 66. Tuomioistuin on tuomion kohdassa 65 viitannut aiempaan oikeuskäytäntöön tuomion tueksi. Esimerkiksi EIS *Peck v. UK* tuomiossa 28.1.2003 ja *P.G. ja J.H. v. UK* tuomiossa 25.9.2001 on todettu, että turvallisuuspalvelujen suorittama järjestelmällinen tietojen kerääminen ja tallentaminen tietyistä henkilöistä merkitsee puuttumista näiden henkilöiden yksityiselämään. Tähän ei vaikuta se, onko tiedot kerätty julkiselta paikalta tai koskevatko ne yksinomaan henkilön ammatillista ja julkista toimintaa.

viestinnän seurannan arvioinnissa, tulee soveltaa myös laajamittaiseen ja erottelemattomaan valvontaan.[97]

Euroopan ihmisoikeustuomioistuin ei ole kuitenkaan tarkastellut kovin syvällisesti yksityiselämän merkitystä kansallisen turvallisuuden yhteydessä, eteenkin laajamittaisten valvontaohjelmien kohdalla. Sen sijaan perusteellisempaa analyysiä on tehty lähinnä tilanteissa, joissa valvontaa tai tietojen säilyttämistä on käytetty rikollisuuden torjuntaan. Joissakin yksittäisissä tapauksissa tuomioistuin on tarkastellut yksityiselämän suojan laajuutta tarkemmin, erityisesti silloin kun kyse on ollut uusista valvonta- tai tietojenkäsittelytavoista. Tohtori *Nóra Ni Loideain* onkin pitänyt huolestuttavana, että vaikka 2000-luvulla kehittyneet ja laajamittaiset valvontajärjestelmät ovat ennennäkemättömän laajoja, on Euroopan ihmisoikeustuomioistuin poikennut perusteellisemmasta lähestymistavasta.[98]

Sekä Euroopan ihmisoikeussopimuksen että EU-lainsäädännön mukaan pelkkä valvontatoimenpiteitä mahdollistavan lainsäädännön olemassaolo on puuttumista yksityisyyden suojaan, ja eurooppalaiset tuomioistuimet ovat pitäneet tiedustelupalvelujen suorittamaa tiedonkeruuta puuttumisena. Tällaisen puuttumisen tulee olla välttämätöntä ja oikeasuhteista. Tiedustelualan edellyttämä tarve salassapitoon voi vaikuttaa oikeuksien valvonnan tehokkuuteen sekä yksilöiden kykyyn hakea oikeussuojakeinoja rikkomustilanteissa. Vaikka myös salaisen valvonnan kohdalla on oikeus hakea oikeussuojakeinoja, on tämä oikeus luonnostaan rajoitettu.[99]

Yksityisyyden suojan ja henkilötietojen suojan tehokkuus riippuu pitkälti siitä, miten ne on sisäistetty teknisessä infrastruktuurissa sekä liiketoiminnan ja hallinnon toimintamalleissa. Nämä seikat haastavat oikeusvarmuutta sekä ajatusta lain ajallisesta pysyvyydestä, sillä täsmälliset normit olisivat sidoksissa teknologiseen ympäristöön, joka muuttuu nopeasti.[100]

Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu korostavat, että päätöksenteon siirtäminen koneille datan perusteella aiheuttaa merkittäviä riskejä yksilöiden oikeuksille ja vapauksille. Ne painottavat, että oikeus yksityiselämään ja henkilötietojen suojaan ovat EU:n

---

[97] Loideain 2025, s. 32. EIS *Liberty v. UK* tuomio 1.7.2008 kappaleet 59–63. EIT katsoi tapauksessa, että 8 artiklaa oli rikottu

[98] Loideain 2025, s. 32, 43–44. Tutkijoiden mukaan tuomioistuimen aiemmin johdonmukainen ja tiukka arviointitapa on muuttunut vähemmän systemaattiseksi ja jäsennellyksi, mikä on johtanut epäselvempiin ja vähemmän perusteellisiin ratkaisuihin. Myös Euroopan ihmisoikeustuomioistuimen tuomarit ovat ilmaisseet huolensa tuomioistuimen tavasta arvioida viranomaisten laajoja valvontavaltuuksia. Erityisesti kritiikin kohteena on ollut nykyaikaisten laajamittaisten valvontajärjestelmien arviointi edelleen 1970-luvulla kehitettyjen standardien pohjalta. Esimerkiksi *Big Brother Watch v. UK 25.5.2021* ratkaisussa viitattiin useasti vuoden 1978 ratkaisuun *Klass and Others v. Saksa*, jossa vahvistettiin postin ja puhelinviestinnän valvontaa koskevat standardit (kappaleet 336, 337 ja 339)

[99] ks. EU Fundamental Rights Agency, p. 29 (2017), Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU -Volume II: field perspectives and legal update, s. 9-10.

[100] Pöysti 2006, s. 305, 315.

keskeisiä arvoja. Nämä oikeudet voivat joutua ristiriitaan sen oletuksen kanssa, että koneet voivat tehdä itsenäisiä päätöksiä tekoälyn avulla.[101] Biometristen tietojen käsittely kaikissa tilanteissa puuttuu vakavasti perusoikeuskirjan 7 ja 8 artiklaan riippumatta siitä, johtaako käsittely esimerkiksi positiiviseen tunnistustulokseen.[102]

### 3.2.3 Henkilötietojen suoja

Henkilötietojen suoja tai tietosuoja ymmärretään varsin vakiintuneesti osaksi yksityiselämän suojaa. Perus- ja ihmisoikeutena henkilötietojen suojan asema on kasvanut yksityisyyden ja yksityiselämän suojan eräänlaisena sovellutuksena.[103] Toisin kuin yksityisyys, henkilötiedot eivät ole olemassa ennen niiden keräämistä tai dokumentointia. Niiden kerääminen ja käsittely on sallittua, mikäli se tapahtuu sääntelyn määrittelemällä tavalla. Sääntelyn tarkoituksena ei ole suojata ihmistä kaikilta mahdollisilta tietojenkäsittelyn muodoilta, vaan epäoikeutetulta tietojen keräämiseltä, säilyttämiseltä ja käytöltä. Henkilötietojen suojasääntely määrittää siten ne ehdot, joiden puitteissa tietoja voidaan laillisesti käsitellä.[104]

Euroopassa henkilötietojen suojaa koskevaa sääntelyä alettiin kehittää 1960- ja 70-luvuilla.[105] Tarve lakien säätämiseen heräsi automaattisen tietojenkäsittelyn herättämästä huolesta.[106] Huolta herätti erityisesti se, että uusi teknologia voisi vaarantaa yksityisyyden suojaa. Niinpä Euroopan neuvosto määritteli periaatteet ja normit henkilötietojen epäoikeudenmukaisen käsittelyn estämiseksi ja antoi asiassa suosituksen vuonna 1968. Samalla tunnistettiin merkittävä tarve kansallisten lakien yhdenmukaistamiseen. Tältä ajalta ovat peräisen monet nykyisen tietosuojasääntelyn keskeiset periaatteet, kuten käyttötarkoitussidonnaisuus ja tietojen oikeellisuus.[107] Henkilötietojen suoja otettiin virallisesti eurooppalaiseksi perusoikeudeksi vuonna 2000 ja sitä voidaan pitää eurooppalaisessa oikeusvaltiossa perusoikeuksien ydinalaan kuuluvana.[108]

Euroopan unionin tuomioistuimen ratkaisut *Digital Rights Ireland* ja *Schrems* korostavat korkeatasoisen tietosuojan merkitystä erityisesti lainvalvonnan ja kansallisen turvallisuuden yhteydessä. Molemmissa ratkaisuissa perusoikeuskirjan 7 ja 8 artikloja käsiteltiin yhdessä. *Digital*

---

[101] Euroopan tietosuojaneuvoston ja Euroopan tietosuojavaltuutetun yhteinen lausunto 5/2021, s. 6.
[102] Euroopan tietosuojaneuvoston ohjeet 05/2022, s. 5.
[103] Koillinen 2012, s. 171, 174. Henkilötietojen suojan asemasta on käyty keskustelua itsenäisenä perusoikeutena. Aihetta on muun muassa käsitellyt Koillinen 2012 ja Keller 2023, s. 85–88.
[104] Lindroos-Hovinheimo 2018, s. 58.
[105] Korpisaari 2022, s. 5.
[106] Koillinen 2012, s. 172.
[107] Korpisaari 2022, s. 5.
[108] Saarenpää – Riekkinen 2023, s. 217.

*Rights Ireland* -ratkaisussa otettiin kantaa siihen, miten yksityisen ja yleisen edun välinen raja tulisi hahmottaa. Asiassa tuomioistuin totesi, että tietojen säilyttäminen voi luoda ihmisille tunteen siitä, että heidän yksityiselämäänsä seurataan jatkuvasti.[109] *Schrems* -ratkaisussa tuomioistuin puolestaan katsoi, että viranomaisten yleinen pääsy sähköisen viestinnän sisältöön voi loukata yksityisyyden suojan ydintä.[110] Euroopan unionin tuomioistuin on täten painottanut, että laajamittainen ja yleinen valvonta voi olla vakava uhka perusoikeuksille, erityisesti oikeudelle yksityisyyteen.[111] Näistä ratkaisujen perusteella voidaan katsoa, että yksityisyys ja erityisesti henkilötietojen suoja ovat oikeuspoliittisesti tärkeitä. Unionin tuomioistuin on korostanut henkilötietojen suojan asemaa perusoikeutena yksityisyyden rinnalle Euroopan ihmisoikeustuomioistuinta selkeämmin ja aiemmin.[112]

Henkilötietojen suojaan liittyvä sääntely osoittaa, ettei oikeusvaltiossa ole kyse ainoastaan yksilön ja valtion välisestä suhteesta. Keskeistä on yksilön oikeus määrätä itseään koskevasta informaatiosta.[113] Henkilötietojen suoja liittyy läheisesti myös muihin perusoikeuksiin, kuten sananvapauteen ja kokoontumisvapauteen, ja toimii usein niiden toteutumisen keskeisenä edellytyksenä.[114]

### 3.2.4 Perus- ja ihmisoikeuksien rajoittaminen

Poliisilla ja muilla viranomaisilla tulee olla riittävät ja tehokkaat keinot rikollisuuden, terrorismin ja muiden uhkien torjumiseksi, eikä tietosuojan ja yksityisyyden ole tarkoitus estää tätä. Näille keinoille tulee kuitenkin olla tietyt rajat, sillä kaikkiin varmuuden vuoksi kohdistuva valvonta ei ole hyväksyttävää demokraattisessa yhteiskunnassa.[115]

Kuten todettu, biometristen tietojen käsittely merkitsee jo itsessään vakavaa puuttumista perusoikeuksiin. Pelkkä tietojen käsittely on puuttumista, vaikka biometrinen malli poistettaisiin heti vertailun jälkeen eikä vastaavuutta löytyisi.[116]

Perusoikeuksiin voidaan puuttua lainsäädännöllä, viranomaistoiminnalla tai tilanteissa, joissa yksityiselle toimijalle on annettu julkisen vallan käyttöön liittyviä tehtäviä.[117] Euroopan

---

[109] Yhdistetyissä asioissa C-293/12 ja C-549/12 *Digital Rights Ireland Ltd*, kappale 37. Ratkaisussa
[110] Asia C-362/14 *Schrems,* kappale 94. Asiassa oli pääasiassa kyse siitä, millä ehdoilla unionin kansalaisen tietoja voidaan siirtää käsiteltäväksi kolmansiin maihin, tässä asiassa Yhdysvaltoihin.
[111] European Data Protection Supervisor Opinion 6/2015, s. 4.
[112] Lindroos-Hovinheimo 2018, s. 52, 65.
[113] Korja 2016, s. 76.
[114] Euroopan tietosuojaneuvoston ohjeet 05/2022, s. 9.
[115] Keller 2023, s. 173.
[116] Euroopan tietosuojaneuvoston ohjeet 05/2022, s. 15.
[117]European Data Protection Supervisor Opinion 6/2015, s. 15.

ihmisoikeussopimuksen mukaan yksityiselämään puuttuminen on sallittua vain, jos se perustuu lakiin, se on tarpeen tiettyjen etujen turvaamiseksi ja puuttuminen on välttämätöntä demokraattisessa yhteiskunnassa.[118]

Perusoikeuskirja asettaa samansuuntaiset vaatimukset perusoikeuksien rajoittamiselle. Lisäksi kyseisten oikeuksien ja vapauksien keskeistä sisältöä tulee kunnioittaa. Rajoitusten tulee olla suhteellisuusperiaatteen mukaisia eli välttämättömiä ja vastattava tosiasiallisesti unionin tunnustamia yleisen edun mukaisia tavoitteita tai tarvetta suojella muiden henkilöiden oikeuksia ja vapauksia. Lisäksi perusoikeuskirjan 54 artikla kieltää sellaisen toiminnan, jonka tarkoituksena on tehdä tyhjäksi jokin perusoikeuskirjassa tunnustettu oikeus tai vapaus taikka rajoittaa sitä laajemmalti kuin perusoikeuskirjassa on sallittu.[119]

Esimerkiksi Euroopan ihmisoikeustuomioistuimen tapauksessa *M.K. v. Ranska* tuomioistuimen mielestä suojan tarve oli tavanomaista suurempi, jos kyse on automaattisesta tietojenkäsittelystä ja erityisen suuri, jos tietoja käytettiin poliisivoimien tarkoituksiin. Lain tuli taata, että vain tarpeellisia tietoja tallennettiin ja että ne olivat sellaisessa muodossa, että tiedon kohdetta ei voi tunnistaa kauemmin kuin rekisteröinnin tarkoitus edellyttää. Lainsäädännössä tulee myös olla takeet tietojen sopimatonta ja loukkaavaa käyttämistä vastaan.[120]

Myös esimerkiksi biometrisen tunnisteen tyypillä voi olla vaikutusta siihen, miten vakavasti sen katsotaan puuttuvan yksityisyyteen. Esimerkiksi Euroopan ihmisoikeustuomioistuimen suuren jaoston ratkaisussa *S. ja Marper v. Yhdistynyt kuningaskunta* tuomioistuin piti solunäytteiden ja DNA-profiilien säilyttämistä vakavampana puuttumisena yksityiselämän suojaan kuin sormenjälkien tallettamista, koska ne itsessään paljastivat henkilöstä enemmän kuin sormenjäljet, ja vaara niiden myöhemmästä väärinkäytöstä erilaisin teknologian mahdollistamin keinoin oli suurempi.[121]

Myös Euroopan unionin tuomioistuimen *Schrems* ratkaisussa tuomioistuin toteaa, että henkilötietojen käsittelyä koskevien säännösten tulee olla selkeitä ja täsmällisiä. Säännöissä tulee asettaa vähimmäisvaatimukset, jotta henkilötietojen käsittelyn kohteena olevilla henkilöillä on riittävät takeet tietojensa suojaamiseksi väärinkäytöksiltä sekä laittomalta saannilta ja käytöltä. Myös EUT korostaa tällaisten takeiden merkitystä erityisesti silloin, kun henkilötietoja käsitellään automaattisesti ja on olemassa huomattava vaara laittomasta pääsystä näihin tietoihin. Lisäksi tuomiossa huomautetaan, että yksityiselämän kunnioitusta koskevan perusoikeuden suoja

[118] Euroopan ihmisoikeussopimus 8 artiklan 2 kohta.
[119] Raitio – Tuominen, 2025, s. 340–341.
[120] EIT M.K v. Ranska tuomio 18.4.2013, kappale 35.
[121] EIT S ja Marper v. Yhdistynyt kuningaskunta 4.12.2008, kappale 75.

unionin tasolla edellyttää, että henkilötietojen suojaa koskevat poikkeukset ja rajoitukset toteutetaan sen rajoissa, mikä on ehdottomasti tarpeen.[122]

Euroopan ihmisoikeustuomioistuimen *Glukhin v. Venäjä* tuomiossa arvioitiin, oliko tietojen käsittely sallittua ihmisoikeussopimuksen 8 artiklan 2 kohdan perusteella. Tapauksessa *Glukhin* oli järjestänyt mielenosoituksen yksin Moskovan metrossa. Protestissaan hän käytti vain pahvifiguuria, joka esitti aiemmin pidätettyä aktivistia. *Glukhin* otettiin kiinni, kun hänet oli tunnistettu metron valvontakameroiden kautta. Tuomioistuin hyväksyi *Glukhin* väitteen siitä, että reaaliaikaista ja jälkikäteistä kasvojentunnistusta oli käytetty, koska nopeaa tunnistusta ei voitu selittää muulla tavalla. Tuomioistuin tunnusti rikosten torjunnan olevan hyväksyttävä tavoite, mutta katsoi, että kasvojentunnistusteknologian käyttö ja siitä seuranneet toimenpiteet olivat suhteettomia. Tuomioistuin korosti, että valvontaan käytettävän kasvojentunnistusteknologia edellyttää korkeaa perustelutasoa, jotta sen käyttö voidaan katsoa välttämättömäksi. Tämä korostuu reaaliaikaisen kasvojentunnistusteknologian kohdalla. Tapauksessa painavaa yhteiskunnallista tarvetta teknologian käytölle ei ollut, eikä sen katsottu olevan välttämätöntä demokraattisessa yhteiskunnassa.[123]

Tuomioistuin ei kuitenkaan arvioinut, onko kasvojentunnistusteknologia luonteeltaan lähtökohtaisesti yhteensopimaton EIS:n 8 artiklan ydinalueen kanssa. Se ei myöskään tarkastele sitä, onko kyseinen teknologia kategorisesti ristiriidassa ihmisoikeussopimuksen kanssa esimerkiksi suhteellisuusperiaatteen näkökulmasta. Se keskittyi arvioimaan, oliko tietojen käsittelyn oikeutettua artiklan 2 kohdan perusteella.

Yhteenvetona voidaan todeta, että vaikka viranomaisille on taattava riittävät keinot turvallisuuden varmistamiseksi, tulee huomioida perus- ja ihmisoikeussäännösten asettamat vaatimukset. Biometristen tietojen käsittely ja tunnistaminen merkitsevät lähtökohtaisesti merkittävää puuttumista yksityisyyteen ja henkilötietojen suojaan. Tästä johtuu, että niiden on perustuttava selkeään ja täsmälliseen lainsäädäntöön, oltava välttämättömiä hyväksyttävän tavoitteen saavuttamiseksi ja suhteellisuusperiaatteen mukaisia. Yksilöille tulisi taata riittävät oikeusturvakeinot väärinkäytöksiä vastaan. Reaaliaikaisen tunnistamisen käyttö on epäilemättä herkin käyttötapaus.

[122] Asia C-362/14 *Schrems,* kappale 91–92.
[123] EIT Glukhin v. Venäjä 4.7.2023, kappaleet 6–8, 86–88.

# 4 Biometrinen tunnistaminen yleisessä tietosuoja-asetuksessa ja rikosasioiden tietosuojadirektiivissä

## 4.1. Euroopan unionin toimivalta

Euroopan unioni on oma, ainutlaatuinen oikeusjärjestelmänsä, joka eroaa järjestelmänä valtioista sekä valtioiden välisistä kansainvälisistä järjestöistä. Unioni ei ole suvereeni kuten valtio, vaan sen toimivalta on johdettu jäsenvaltioiden suvereenista toimivallasta. Unionin jäsenvaltiot ovat antaneet unionille toimivallan perussopimuksissa. Toimivalta, jota ei ole perussopimuksissa luovutettu unionille, kuuluu SEU 5 artiklan mukaisesti jäsenvaltioille.[124]

Unionin toimivalta jaetaan perussopimuksissa yksinomaiseen, jaettuun ja tukevaan toimivaltaan. Kun unionilla on yksinomainen toimivalta tietyllä alalla SEUT 2 artiklan 1 kohdan mukaan, on ainoastaan unionilla toimivalta antaa oikeudellisesti velvoittavia säännöksiä. Kyseinen artikla sisältää pääsäännön lisäksi poikkeuksen, jonka mukaan yksinomaisen toimivallan alalla jäsenvaltiot voivat antaa velvoittavia säännöksiä unionin valtuuttamina tai unionin antamien säädösten täytäntöön panemiseksi. Unionin yksinomaiseen toimivaltaan kuuluvat alat on lueteltu SEUT 3 artiklassa. Näitä ovat muun muassa tulliliitto, sisämarkkinat ja eurovaltioiden rahapolitiikka.[125]

Jaetun toimivallan aloilla unioni ja jäsenvaltiot voivat toimia lainsäätäjänä ja antaa oikeudellisesti velvoittavia säädöksiä. Jäsenvaltiot voivat käyttää kyseisellä alalla toimivaltaansa siltä osin kuin unioni ei ole käyttänyt omaansa. Jaetun toimivallan alalla unionin lainsäädäntötoimien katsotaan syrjäyttävän jäsenvaltioiden mahdollisuuden säädellä asiassa. Toisaalta toimivalta voi siirtyä takaisin jäsenvaltioille, jos unioni on lakannut käyttämästä toimivaltaansa. SEUT 4 artiklan mukaan jaettuun toimivaltaan kuuluvat muut toimialat paitsi yksinomaiseen toimivaltaan kuuluvat alat sekä SEUT 6 artiklassa mainitut tukevaan toimivaltaan kuuluvat alat. Jaettua toimivaltaa pidetään toimivallan pääsääntönä.[126]

SEUT 2 artiklan 5 kohdan mukaan tukeva toimivalta tarkoittaa jäsenvaltioiden toimintaa tukevia, yhteensovittavia ja täydentäviä toimia, jotka eivät kuitenkaan syrjäytä jäsenvaltioiden toimivaltaa. Tukevan toimivallan alalla unioni ei voi yhdenmukaistaa jäsenvaltioiden lainsäädäntöä. Tukevan toimivallan alat on listattu SEUT 6 artiklassa. Tämän toimivallan alle kuuluvat

[124] Raitio – Tuominen 2020, s. 206–217. Keskeisessä Euroopan unionin tuomioistuimen ennakkopäätöksessä *Van Gend en Loos* unionin tuomioistuin painotti EU-oikeuden erityistä luonnetta, joka erottaa sen muusta kansainvälisestä oikeudesta.
[125] Raitio – Tuominen 2020, s. 217–218.
[126] Raitio – Tuominen 2020, s. 218–219.

ihmisten terveyden suojelu, teollisuus, kulttuuri, matkailu, koulutus, pelastuspalvelu ja hallinnollinen yhteistyö.[127]

Tekoälyasetus harmonisoi unionin sisämarkkinoille tuotaville ja siellä käytettäville tekoälyjärjestelmille asetetut vaatimukset. Unionin toimivalta tekoälyasetuksen säätämiseen on johdettu SEUT-sopimuksen 114 artiklasta, jonka mukaan komissio voi säännellä sisämarkkinoiden toimintaa ja täten taata sen tehokkaan toiminnan. Asetuksen tavoitteena on välttää eriävää kansallista sääntelyä, joka haittaisi tekoälyjärjestelmiin liittyvien tuotteiden ja palveluiden vapaata liikkuvuutta ja käyttöönottoa unionin sisämarkkinoilla. Eriävä kansallinen sääntely aiheuttaisi lisäkustannuksia ja -esteitä yrityksille EU:n markkinoille pääsemisessä.[128] SEUT 114 artikla kuuluu jaetun toimivallan alaan. Käytettäessä tätä artiklaa sääntelyn oikeusperustana, unionin toimivalta syrjäyttää kansallisen toimivallan. EU-oikeuden systematiikassa asetus sijoittuu pääosin tuotesääntelyyn.[129]

Edellä mainitun SEUT 114 artiklan lisäksi asetuksen toinen oikeusperusta on SEUT 16 artikla siltä osin kuin asetus sisältää henkilötietojen käsittelyn erityissääntöjä, joilla rajoitetaan tekoälyjärjestelmien käyttöä lainvalvontatarkoituksessa esimerkiksi biometrisessa etätunnistamisessa, luonnollisia henkilöitä koskevissa riskinarvioinneissa ja biometrisessa luokittelussa.[130] Yleinen tietosuoja-asetus ja rikosasioiden tietosuojadirektiivi on myös annettu SEUT 16 artiklan perusteella.[131] Säännöillä pyritään takaamaan henkilötietojen käsittelyn korkea vaatimustaso ja suojaamaan henkilöjen oikeus yksityisyyteen.[132] Euroopan unionin tuomioistuimen oikeuskäytännön mukaisesti SEUT 16 artikla on asianmukainen oikeusperusta silloin, kun henkilötietojen suoja on keskeinen osa EU-lainsäädäntöä. Kyseisen artiklan soveltaminen edellyttää myös, että henkilötietojen käsittelyä valvotaan riippumattomasti. Tähän velvoittaa myös EU:n perusoikeuskirjan 8 artikla, jossa turvataan oikeus henkilötietojen suojaan.[133]

---

[127] Raitio – Tuominen 2020, s. 219.
[128] Wong-Toropainen 2025, s. 83. Lainsäädäntöinstrumentin valinnan voidaan kertovan komission siirtyneen reaktiivisesta alakohtaisesta sääntelystä kohti yleisluontoisempaa ennakkosääntelyä eli *ex ante* -sääntelyä. Ks. Sitra työpaperi 2022, s. 17.
[129] Lindroos-Hovinheimo ym. 2025, s. 319–320. Tekoälyasetuksen lainsäädäntöprosessin aikana käytiin keskusteluja siitä, onko unionilla 114 artiklan pohjalta riittävä toimivalta antaa näin merkittävää ja kattavaa sääntelyä. Asiaa tarkasteltiin myös EU-oikeuden periaatteiden, suhteellisuus- ja toissijaisuusperiaatteiden, valossa. *Lindroos-Hovinheimon* mukaan voidaan vieläkin kysyä, edellyttäkö sisämarkkinoiden toteuttaminen niin kauaskantoisia ratkaisuja ja niin laajaa toimivallan siirtoa EU:lle kuin tekoälyasetuksessa annettiin. Hän kuitenkin huomauttaa, että jäsenvaltiot hyväksyivät asetuksen, joten ilmeisesti toimivaltaa ei ollut niiden näkökulmasta ylitetty, tai jos ylitetiin, tapahtui se jäsenvaltioille hyväksyttävällä tavalla. Viime sijassa Euroopan unionin tuomioistuin ratkaisee kysymyksen siitä, pysyykö asetus EU:n toimivallan rajoissa, mikäli tätä koskeva asia tulisi siellä vireille.
[130] Tekoälyasetus johdanto-osa 3 perustelukappale.
[131] EPRS 2021, s. 23.
[132] Wong-Toropainen 2025, s. 83.
[133] Euroopan tietosuojaneuvoston ja Euroopan tietosuojavaltuutetun yhteinen lausunto 5/2021, s. 2.

## 4.2 Biometristen tunnisteiden sääntely kehitys Euroopan unionissa

Vuonna 1995 hyväksytty tietosuojadirektiivi[134] oli henkilötietojen käsittelyä koskeva perustavanlaatuinen oikeudellinen kehys. Direktiivissä ei nimenomaisesti viitattu biometrisiin tietoihin, vaikka sen säännöksien on tulkittu kattavan myös biometrisen datan.[135] Vuonna 2004 tuli voimaan EU:n passiasetus[136], joka velvoitti jäsenvaltiot tallentamaan kansalaisten passeihin ja matkustusasiakirjoihin kasvokuvat ja sormenjäljet. Samoihin aikoihin unioniin perustettiin laajoja tietokantoja turvapaikan- ja viisuminhakijoiden biometrisiä tietoja varten sekä tietojärjestelmä Schengen-alueen suojaamiseksi.[137]

Vaikka biometriselle teknologialle tunnistettiin monia hyötyjä, Euroopan neuvosto varoitti jo varhain, että biometrisiä tietoja tulisi pitää ”arkaluonteisina” tietoina, joihin liittyy riskejä. Ne voivat paljastaa tietoja esimerkiksi terveydestä, mahdollistaa henkilöiden tunnistamisen ja helpottaa eri tietojen yhdistelemistä ja ovat lisäksi luonteeltaan peruuttamattomia.[138]

Riskeistä huolimatta yleinen tietosuojakehys ja useimpien valtioiden kansallinen lainsäädäntö eivät pitkään sisältäneet erityisiä säännöksiä biometrisen datan käytöstä ja käsittelystä. Samalla ohjeistus jäi rajalliseksi, vaikka teknologia kehittyi nopeasti. Näiden puutteiden paikkaamiseksi osa kansallisista tietosuojaviranomaisista laati omia kehyksiään biometrisen datan käytölle. Niissä korostettiin data arkaluonteisuutta, tietokantoihin liittyviä riskejä sekä niin sanottua käyttötarkoituksen laajenemista (*function creep*). Tietosuojaviranomaiset arvioivat myös, täyttikö biometrisen datan käyttö suhteellisuusperiaatteen vaatimukset. Tämä jätti kuitenkin paljon harkintavaltaa ja johti käytännössä vaihteleviin ja vaikeasti ennakoitaviin ratkaisuihin jäsenvaltioissa.[139]

Tätä taustaa vasten Euroopan unioni hyväksyi vuonna 2016 yleisen tietosuoja-asetuksen sekä rikosasioiden tietosuojadirektiivin[140]. Vuoden 1995 henkilötietodirektiivi määritteli vaatimuksia jäsenvaltioiden lainsäädännöille tietosuojan toteuttamiseksi, mikä johti tulkintaeroihin jäsenvaltioiden välillä. Vuonna 2018 voimaan tulleella yleisellä tietosuoja-asetuksella pyrittiin

---

[134] Euroopan parlamentin ja neuvoston direktiivi 95/46/EY, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta.
[135] EPRS 2021, s. 24.
[136] Neuvoston asetus (EY) 2252/2001 jäsenvaltioiden myöntämien passien ja matkustusasiakirjojen turvatekijöitä ja biometriikkaa koskevista vaatimuksista. EU:n passiasetusta on muutettu Euroopan parlamentin ja neuvoston asetuksella (EY) N.o 444/2009.
[137] Kindt 2020, s. 62.
[138] Kindt 2020, s. 62.
[139] Kindt 2020, s. 63.
[140] Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680, luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäätöksen 2008/977/YOS kumoamisesta.

harmonisoimaan tietosuojalainsäädäntöä.[141] Asetus sisältää säännökset sekä julkisen että yksityisen sektorin biometrisen datan käsittelystä. Rikosasioiden tietosuojadirektiivi puolestaan koskee henkilötietojen käsittelyä rikosten ennaltaehkäisyssä, havaitsemissa, tutkinnassa ja syytteeseen asettamisessa lainvalvontaviranomaisten toimesta.[142] Näin ollen EU:n tietosuojalainsäädännössä alettiin vasta 2016 säännellä biometrisen datan käyttöä nimenomaisesti.[143]

Tekoälyasetus on jatkumoa edellä mainitulle sääntelylle sekä osa EU:n laajempaa datastrategiaa.[144] Unionin tekoälyasetus on maailman ensimmäisiä tekoälyyn liittyvä lainsäädäntöinstrumentteja, joka sääntelee tekoälyjärjestelmiä horisontaalisesti eikä esimerkiksi sektorikohtaisesti, kuten Kiinassa.[145] Euroopan unionin haluaa tekoälyasetuksen myötä toimia suunnannäyttäjänä uusien teknologioiden sääntelijänä. Columbian yliopiston professori *Anu Bradfortin* luoma termi Bryssel-efekti kuvaa ilmiötä, jossa EU merkittävänä markkina-alueena pystyy sisämarkkinoidensa kautta luomaan globaaleja standardeja. Koska yritysten on helpoin toimia yhdellä tavalla, toimittaisiin EU:n sääntöjen mukaan maailmanlaajuisesti.[146]

Tekoälyasetuksen on odotettu jatkavan yleisen tietosuoja-asetuksen käynnistämää digitaalista Bryssel-efektin sarjaa. Sen mahdollisuudet saavuttaa yleisen tietosuoja-asetuksen kaltainen globaali vaikutusvalta voivat olla kuitenkin rajalliset. Yleinen tietosuoja-asetus syntyi poikkeuksellisessa tilanteessa, jossa esimerkiksi *Cambridge Analytica* -skandaali nosti henkilötietojen käytön ja tietosuojan laajaan julkiseen keskusteluun. Tekoälyn kehitys puolestaan liittyy vahvasti suurvaltapolitiikkaan ja sen kehitys tapahtuu pääosin EU:n ulkopuolella.[147]

Euroopassa onkin syntynyt verrattain vähän maailmanlaajuisesti tunnettuja teknologia yrityksiä verrattuna Yhdysvaltoihin ja Kiinaan. Vaikka EU ei ehkä pysty luomaan maailman johtavia

---

[141] Sankari – Wiberg 2019, s. 340.
[142] Kindt 2020, s. 63.
[143] EPRS tutkimus 2021, s. 24.
[144] Wong-Toropainen 2025, s. 8–9. Datastategiaa seuranneita lainsäädäntötoimia on kutsuttu muun muassa sääntelytsunamiksi, joka aiheuttaa rasitteita yrityksille ja hidastaa teknologian kehittämistä Euroopassa. Sääntelyn laajuutta kuvaa *Bruegelin* kokoama kaavio EU:n digitalisaatiota koskevasta lainsääntökehyksestä. Kaavio sisältää 78 säädöstä, jotka oli hyväksytty kesäkuuhun 2024 mennessä ja lisäksi 34 säädöstä, joita valmisteltiin vuonna 2024. EU:n kilpailullisuutta koskevassa *Margo Dragin* raportissa vuonna 2024 vahvistettiin, että digitaalialan lainsäädäntö nähdään epäjohdonmukaisena ja rajoittavana, josta johtuu, että monet eurooppalaiset yritykset ovat hakeneet investointeja Yhdysvalloista ja pyrkineet skaalautumaan amerikkalaisilla markkinoilla.
[145] Wong-Toropainen 2025, s. 1, 3.
[146] Bradfort 2012, s. 3–5.
[147] Yle artikkeli 14.6.2023: Analyyi: EU yrittää tekoälyasetuksella toisintaa Bryssel-efektiä, mutta muu maailma ei välttämättä seuraa nyt perässä. *Cambridge Analytica* on vuonna 2018 paljastunut skandaali, jossa brittiläinen data analytiikkayritys *Cambridge Analytica* keräsi luvattomasti Facebook-käyttäjien henkilötietoja. Kerättyjä tietoja käytettiin poliittiseen profilointiin. Tiedonkeruun avulla saatiin kerättyä yli 50 miljoonaa yksittäistä profiilia, jotka voitiin yhdistää äänestäjäluetteloihin ja yhdistämällä näitä persoonallisuustestien tuloksiin ja Facebookin dataan rakennettiin algoritmi, jonka avulla pystyttiin tunnistamaan mahdolliset liikkuvat äänestäjät sekä muotoilemaan viestejä, jotka todennäköisesti vetoavat heihin. Näitä tietoja käytetiin muun muassa vuoden 2016 USA:n presidentin vaaleissa. Lisä yritys työskenteli yhdessä Brexit äänestyksen voittaneen osapuolen kanssa. ks. The Guardian artikkeli 17.3.2018.

teknologiayrityksiä, on se osoittanut olevansa enemmän kuin kykenevä luomaan säännöksiä näiden yritysten ohjaamiseksi. *Bradford* onkin kuvannut unionia perusoikeuslähtöiseksi sääntelyvallaksi, kun taas Yhdysvalloissa tai Kiinassa sääntely on joko markkina- tai valtiovetoista.[148]

## 4.3 Yleinen tietosuoja-asetus

### 4.3.1 Biometrinen tunnistamisen määritelmä yleisessä tietosuoja-asetuksessa

Yleisen tietosuoja-asetuksen myötä EU-oikeudessa määriteltiin ensimmäisen kerran biometrinen tieto[149]: ”*kaikkia luonnollisen henkilön fyysisiin ja fysiologisiin ominaisuuksiin tai käyttäytymiseen liittyvällä teknisellä käsittelyllä saatuja henkilötietoja, kuten kasvokuvia tai sormenjälkitietoja, joiden perusteella kyseinen luonnollinen henkilö voidaan tunnistaa tai kyseisen henkilön tunnistaminen voidaan varmistaa*”.

Määritelmän osatekijä ”teknisellä käsittelyllä” sulkee käytännössä pois tietokantoihin tallennetun ja säilytetyn ”raakadatan”, kuten valvontakameroiden tallentamat kasvokuvat ja äänitallenteet sekä tilanteet, joissa data julkaistaan verkkosivustolla tai sosiaalisessa mediassa.[150] Täten valokuvat eivät kuulu biometristen tietojen määritelmän piiriin, paitsi jos niitä käsitellään erityisin teknisin menetelmin, jotka mahdollistavat luonnollisen henkilön yksilöllisen tunnistamisen tai todentamisen.[151]

Määritelmän muotoilusta johtuen se, milloin tiedoista tulee biometrisiä, määräytyy tietojen käytön eikä niiden arkaluonteisuuden tai tunnistettavuuden perusteella. Lisäksi biometrisen datan keräämiseen liittyviä riskejä ei kateta. Tiedot, joiden tulisi saada erityissuojaa, voivat jäädä sen ulkopuolelle, koska niitä ei käsitellä asetuksen mukaan biometrisesti. Tämä on ongelmallista, koska tietojen myöhempi käyttö, erityisesti lainvalvontaviranomaisten toimesta, voi olla vähemmän läpinäkyvää ja rajoitettu sekä tietoja voidaan hyödyntää ilman, että asianomaisille henkilöille tai yleisölle ilmoitetaan asiasta. Esimerkiksi valokuvien rajautuminen määritelmän ulkopuolelle merkitsee, että yritykset ja viranomaiset voivat kerätä laajoja kuvakantoja, kuten *Clearview AI* tapauksessa.[152]

Määritelmä ei ole myöskään täysin linjassa Euroopan ihmisoikeustuomioistuimen kanssa, joka on katsonut, että yksilöllisten inhimillisten ominaisuuksien tallentaminen tietokantoihin

[148] Bradford 2024, s. 378, 383, 385–387.
[149] Kindt 2020, s. 63.
[150] Kindt 2020, s. 64.
[151] Yleisen tietosuoja-asetuksen johdanto-osan 51 perustelukappale.
[152] Kindt 2020, s. 66.

puuttuu oikeuteen nauttia yksityiselämän kunnioitusta.[153] Esimerkiksi *Gaughran v. Yhdistynyt kuningaskunta* tuomiossa Euroopan ihmisoikeustuomioistuin katsoi, että hakijan DNA-profiilin, sormenjälkien ja valokuvien säilyttäminen merkitsi puuttumista hänen yksityiselämäänsä.[154]

*Kindtin* mukaan asianmukaisen määritelmän tulisi turvata oikeudellinen suoja sellaisille yksilöllisille inhimillisille ominaisuuksille, jotka mahdollistavat tunnistamisen tai joita voidaan hyödyntää automatisoiduissa prosesseissa. Lisäksi sääntelyssä tulisi asettaa rajoituksia näiden tietojen tallentamiselle tietokantoihin.[155]

### 4.3.2 Biometrinen tunnistaminen ja biometriset tunnisteet yleisessä tietosuoja-asetuksessa

Kuten muidenkin henkilötietojen osalta, biometristen tietojen käsittely on sallittua vain, jos jokin yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan käsittelyperusteista täyttyy. Käsittely voi olla esimerkiksi oikeutettua, jos rekisteröity antaa suostumuksensa tai jos se on tarpeen lakisääteisen velvoitteen noudattamiseksi.[156]

Koska biometristen tietojen käsittely voi aiheuttaa merkittäviä riskejä rekisteröidyn perusoikeuksille, asetuksen 9 artiklan 1 kohdan mukaan biometristen tietojen käsittely henkilön yksiselitteistä tunnistamista varten on lähtökohtaisesti kielletty. Kieltoon on kuitenkin monia poikkeuksia, jotka on lueteltu kyseisen artiklan 2 kohdassa. Esimerkiksi käsittely on sallittua, jos rekisteröity on antanut nimenomaisen suostumuksensa tai rekisteröity on nimenomaisesti saattanut tiedot julkisiksi. Käsittely voi olla sallittua myös silloin, jos se on tarpeen tärkeän yleisen edun vuoksi ”unionin oikeuden tai jäsenvaltion lainsäädännön nojalla, edellyttäen että se on oikeasuhteinen tavoitteeseen nähden, siinä noudatetaan keskeisiltä osin oikeutta henkilötietojen suojaan ja siinä säädetään asianmukaisista ja erityisistä toimenpiteistä rekisteröidyn perusoikeuksien ja etujen suojaamiseksi”.[157] Biometristen tietojen käsittelyn edellytyksenä on kuitenkin myös 6 artiklan 1 kohdan edellytysten täyttyminen.[158]

---

[153] Kindt 2020, s. 66.
[154] EIT *Gaughran v. Yhdistynyt kuningaskunta* 13.2.2020, kappale 63. Tuomioistuin viittasi tuomiossa S. ja Marper ratkaisuun, jossa suuri jaosto oli todennut, että yksityiselämän käsite kattaa myös henkilön oikeuteen omaan kuvaansa liittyviä ulottuvuuksia (kappale 66).
[155] Kindt 2020, s. 66.
[156] Yleisen tietosuoja-asetuksen 6 artikla 1 kohta.
[157] Yleisen tietosuoja-asetuksen 9 artikla 1 ja 2 kohta.
[158] Yleisen tietosuuoja-asetuksen johdanto-osan 51 perustelukappale.

Asetus rajoittaa myös automatisoitua yksittäistä päätöksentekoa. Asetuksen 22 artiklan 1 kohdan mukaan rekisteröidyillä on oikeus olla joutumatta sellaisen päätöksen kohteeksi, joka perustuu yksinomaan automaattiseen käsittelyyn, mukaan lukien profilointi, ja jolla on oikeusvaikutuksia tai joka vaikuttaa heihin vastaavalla merkittävällä tavalla. Täysin automatisoidulla päätöksellä tarkoitetaan tilannetta, jossa ihmisen osallistuminen puuttuu eikä päätöksen lopputulosta tarkasteta vastuuhenkilön toimesta. Myös automatisoituihin yksittäispäätöksiin liittyy poikkeuksia, jotka on määritelty asetuksen 22 artiklan 2 kohdassa. Biometrisiin tietoihin perustuvaan automatisoituun päätöksentekoon sovelletaan vielä tiukempia rajoituksia. Artiklan 22(4) mukaan tällainen päätöksenteko on sallittua ainoastaan, jos rekisteröity on antanut nimenomaisen suostumuksensa tai jos käsittely on tarpeen merkittävän yleisen edun vuoksi.[159]

Asetuksen 9 artiklan poikkeukset ovat osin tulkinnanvaraisia ja epämääräisiä, kuten käsite ”tärkeä yleinen etu”. Lisäksi poikkeuksia on paljon, minkä vuoksi yleinen tietosuoja-asetus sallii biometrisen datan käsittelyn monissa tilanteissa. Asetuksessa ei myöskään oteta huomioon erilaisten biometrisen järjestelmien toimintatapoja tai sitä, miten tietoja käsitellään. Esimerkiksi 9 artikla ei tee eroa biometristen todentamisen ja tunnistamisen välillä. Todentaminen ei edellytä tietokannan käyttöä toisin kuin tunnistaminen, joten se sisältää vähemmän riskejä. Asianmukaisen sääntelyn tulisi huomioida eri toiminnallisuuksien suhteelliset riskit sekä rajoittaa tai kieltää aidosti riskialttiit käyttötavat ja samalla edistää yksityisyyttä paremmin suojaavia ratkaisuja.[160]

Laajat poikkeukset ja sääntelyn epämääräisyys jättävät tilaa riskialttiille biometrisen datan käyttötavoille, kuten reaaliaikaiselle kasvojentunnistukselle. Asetuksen poikkeukset ovat luonteeltaan yleisiä, ja niihin sisältyy esimerkiksi mahdollisuus käsitellä biometrisiä tietoja “tärkeän yleisen edun” perusteella lain nojalla.[161]

Yleisen tietosuoja-asetuksen mukaan rekisterinpitäjän on ennen käsittelyä toteutettava vaikutustenarviointi, jos tietyntyyppinen käsittely, erityisesti uutta teknologiaa käytettäessä, todennäköisesti aiheuttaa luonnollisen henkilön oikeuksien ja vapauksien kannalta korkean riskin.[162] Asetuksen riskiperusteisen lähestymistavan mukaan velvollisuus tehdä vaikutustenarviointi muodostuu, kun yksilöiden oikeuksiin ja vapauksiin kohdistuu korkea riski. [163] Asetuksessa on nostettu yksilöiden profilointi ja yleisölle avoimen alueen järjestelmällinen valvonta tilanteiksi,

[159] IPOL study 2021, s. 26–27.
[160] Kindt 2020, s. 65, 67. Tunnistaminen tuo lisäriskejä, kuten biometrisen tiedon laajamittaisen keräämisen ja tallentamisen tietokantoihin, mahdollisesti virheelliset osumat sekä yksityisyyden ja valvonnan lisääntymiseen liittyvät riskit.
[161] Kindt 2020, s. 67.
[162] Yleinen tietosuoja-asetus 35 artiklan 1 kohta.
[163] Keller 2023, s. 89.

joissa vaaditaan vaikutustenarviointi sekä erityisiin henkilötietoryhmiin kohdistuva laajamittainen käsittely.[164] Riskienhallinnan näkökulmasta vaikutustenarvioinnin tavoitteena on "hallita riskejä", jotka kohdistuvat luonnollisten henkilöiden oikeuksiin ja vapauksiin kolmen vaiheen kautta. Ensimmäisessä vaiheessa määritellään käsittelyn konteksti eli arvioidaan käsittelyn luonne, laajuus, asiayhteys, tarkoitus ja riskien lähteet. Toisessa vaiheessa arvioidaan riskien todennäköisyys ja vakavuus. Kolmannessa vaiheessa arvioidaan suojatoimia ja mekanismeja, joilla riskejä voidaan lieventää, henkilötietojen suoja varmistaa ja asetuksen noudattaminen osoittaa.[165]

Vaikka viittaus rekisteröityjen oikeuksiin ja vapauksiin koskee ensisijaisesti oikeutta yksityisyyteen, se voi kattaa myös muita perusoikeuksia, kuten sananvapauden, liikkumisvapauden ja syrjinnän kiellon.[166] Korkeaa riskiä ei siis arvioida vain tietosuojan tai yksityisyyden näkökulmasta, vaan organisaatioiden tulee huomioida myös muut yksilön oikeudet ja vapaudet.[167]

Asetuksen mukaisen vaikutustenarvioinnin laatimatta jättäminen, virheellinen toteuttaminen tai toimivaltaisen valvontaviranomaisen kuulemisen laiminlyönti silloin, kun sitä asetuksen mukaan edellytetään, voivat kukin johtaa hallinnolliseen seuraamusmaksuun.[168]

## 4.4 Rikosasioiden tietosuojadirektiivi

Rikosasioiden tietosuojadirektiivissä[169] biometriset tiedot määritellään samoin kuin yleisessä tietosuoja-asetuksessa. Koska määritelmät vastaavat toisiaan, myös asetuksen määritelmään liittyvät ongelmakohdat koskevat direktiivin määritelmää.

Rikosasioiden tietosuojadirektiivissä ei kuitenkaan, tosin kuin yleisessä tietosuoja-asetuksessa, säädetä henkilötietojen käsittelyn oikeusperusteista, vaan siinä asetetaan yleiset periaatteet lainvalvontaviranomaisten toiminnalle.[170] Biometristen tietojen käsittelylle ei ole asetettu yleistä kieltoa, mutta käsittely on sallittua vain tietyin edellytyksin. Käsittelyn on ensinnäkin oltava ehdottoman välttämätöntä, ja siihen on liityttävä asianmukaiset suojatoimet rekisteröidyn oikeuksien ja vapauksien turvaamiseksi. Lisäksi yhden seuraavista edellytyksistä on täytyttävä:

---

[164] Yleinen tietosuoja-asetus 35 artiklan 3 kohta.
[165] Article 29 WP 248, s. 15.
[166] Article 29 WP 248, s. 15.
[167] Keller 2023, s. 89.
[168] Article 29 WP 248, s. 4.
[169] Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680, annettu 27.4.2016, luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäätöksen 2008/977/YOS kumoamisesta.
[170] IPOL study 2021, s. 27.

käsittely on sallittua unionin tai jäsenvaltion lainsäädännössä, se on tarpeen rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi tai käsittely koskee tietoja, jotka rekisteröity on nimenomaisesti saattanut julkisiksi.[171]

Rikosasioiden tietosuojadirektiivi on esteenä sellaiselle kansalliselle lainsäädännölle, jossa säädetään sellaisen henkilön biometristen ja geneettisten tietojen järjestelmällisestä keräämisestä rekisteröintiä varten, jonka osalta on aloitettu esitutkinta virallisen syytteen alaisesta tahallisesta rikoksesta. Tällainen sääntely ei ole sallittua, jos viranomaisilta ei edellytetä arviointia ja perusteluja siitä, onko tietojen kerääminen ehdottoman välttämätöntä kyseissä tilanteessa ja voitaisiinko sama tavoite saavuttaa vähemmän yksilön oikeuksiin puuttuvilla keinoilla. Tietojen kerääminen ei siten voi olla automaattista, vaan sen tarpeellisuus ja oikeasuhtaisuus on arvioitava tapauskohtaisesti.[172]

Automatisoidun päätöksenteon osalta direktiivin 11 artiklan mukaan käsittely on sallittua vain, jos käytössä on riittävät suojatoimet rekisteröityjen oikeuksien ja vapauksien turvaamiseksi, erityisesti oikeus saada inhimillinen osallistuminen päätöksentekoon. Biometrisiin tietoihin perustuvien automatisoitujen päätösten osalta direktiivin rajoitukset ovat vähemmän täsmällisiä kuin yleisessä tietosuoja-asetuksessa. Direktiivissä edellytetään ainoastaan, että käytössä on asianmukaiset toimenpiteet rekisteröidyn oikeuksien, vapauksien ja oikeutettujen etujen suojaamiseksi. Lisäksi artiklassa täsmennetään, että profilointi, joka johtaa luonnollisten henkilöiden syrjintään arkaluontoisten tietojen perusteella, on kielletty.[173]

Direktiivin 29 artiklassa edellytetään, että jäsenvaltiot toteuttavat asianmukaiset tietoturvatoimet sekä asianmukaiset tekniset ja organisatoriset toimenpiteet sen varmistamiseksi, että riskit vastaavat vaadittua turvallisuustasoa erityisesti biometristen tietojen kaltaisten erityisten henkilötietoryhmien osalta.[174] Tietosuojariskejä arvioitaessa olisi otettava huomioon tietojenkäsittelyyn liittyvät riskit, kuten henkilötietojen tahaton tai tahallinen tuhoaminen, häviäminen tai muuttaminen sekä luvaton luovuttaminen tai pääsy tietoihin, mikä voi aiheuttaa etenkin fyysisiä, aineellisia tai aineettomia vahinkoja.[175]

---

[171] Rikosasioiden tietosuojadirektiivi 10 artikla.
[172] Asia C-205/21 *Ministerstvo na vatreshnite raboti v. V. S,* kappale 135.
[173] Rikosasioiden tietosuojadirektiivi 11 artikla 1–3 kohdat.
[174] Rikosasioiden tietosuojadirektiivin 29 artikla.
[175] Rikosasioiden tietosuojadirektiivin johdanto-osa 60 perustelukappale.

## 4.5 Yleisen tietosuoja-asetuksen ja rikosasioiden tietosuojadirektiivin välinen suhde

Euroopan unionin tuomioistuimen ennakkoratkaisussa *Ministerstvo na vatreshnite raboti v. V. S* tuomioistuin on kommentoinut yleisen tietosuoja-asetuksen ja rikosasioiden tietosuojadirektiivin suhdetta. Asiassa oli kyse Bulgarian viranomaisten käytännöstä kirjata rikoksesta epäiltyjen henkilöiden biometrisiä tietoja poliisirekisteriin. V.S oli vastustanut tietojen keräämistä. Unionin tuomioistuimelta pyydettiin selvennystä siihen, onko tällaisten biometristen ja geneettisten tietojen kerääminen sallittua ja millä edellytyksillä rikosasioiden tietosuojadirektiivin sekä perusoikeuskirjan mukaan.[176]

Sekä yleinen tietosuoja-asetus että rikosasioiden tietosuojadirektiivi sisältävät säännöksiä arkaluonteisiksi katsottujen erityisten henkilötietoluokkien, kuten geneettisten ja biometristen tietojen käsittelystä. Unionin tuomioistuin kuitenkin korosti, että asetus ja direktiivi eivät ole samanlaisia. Direktiivi sallii arkaluonteisten tietojen käsittelyn vain, jos se on ehdottoman välttämätöntä ja jos rekisteröidyn oikeudet turvataan asianmukaisesti. Yleinen tietosuoja-asetus lähtee siitä, että tällaisten tietojen käsittely on periaatteellisesti kielletty, mutta sallittua tietyissä poikkeustapauksissa. Tästä seuraa, että vaikka toimivaltaisen viranomaisen suorittama biometristen ja geneettisten tietojen käsittely direktiivin soveltamisalaan kuuluvissa tilanteissa voi olla sallittua direktiivissä asetettujen vaatimusten täyttyessä, näin ei välttämättä kuitenkaan ole yleisen tietosuoja-asetuksen soveltamisalaan kuuluvan näiden samojen tietojen käsittelyn osalta.[177]

Tuomioistuin katsoi, että rikosasioiden tietosuojadirektiiviä, luettuna perusoikeuskirjan 52 artiklan valossa, on tulkittava siten, että poliisiviranomaiset saavat käsitellä biometrisiä ja geneettisiä tietoja rikollisuuden torjumiseksi ja yleisen järjestyksen ylläpitämiseksi, jos tästä on säädetty riittävän selkeästi ja täsmällisesti jäsenvaltion laissa. Vaikka kansallisessa laissa viitattaisiin yleiseen tietosuoja-asetukseen eikä suoraan rikosasioiden tietosuojadirektiiviin, tietojen käsittely voi silti olla sallittua. Edellytyksenä on, että lainsäädännöstä kokonaisuutena käy selvästi, täsmällisesti ja yksiselitteisesti ilmi, että kyseinen käsittely kuuluu nimenomaan kyseisen direktiivin soveltamisalaan eikä yleisen tietosuoja-asetuksen piiriin. Samassa laissa voi olla molempiin sääntelyihin kuuluvia tilanteita, mutta lainsäätäjän on varmistettava, ettei synny epäselvyyttä siitä, kumpaa sääntelyä sovelletaan.[178]

---

[176] Asia C-205/21 *Ministerstvo na vatreshnite raboti v. V. S*, tuomio 26.1.2023, kohdat 35–39.
[177] Asia C-205/21 *Ministerstvo na vatreshnite raboti v. V. S*, kappaleet 62–63.
[178] Asia C-205/21 *Ministerstvo na vatreshnite raboti v. V. S*, kappale 76.

## 4.6 Yhteenvetoa biometrisen tiedon sääntelystä ennen tekoälyasetusta

Yhteenvetona voidaan todeta, että yleisen tietosuoja-asetuksen ja rikosasioiden tietosuojadirektiivin biometrisen tiedon määritelmä on herättänyt kritiikkiä erityisesti siksi, että se sulkee soveltamisalan ulkopuolelle niin sanotun ”raakadatan”, kuten kasvokuvat. Määritelmä poikkeaa myös Euroopan ihmisoikeustuomioistuimen oikeuskäytännöstä, jossa yksityisyyden suojan on katsottu ulottuvan jo tietojen keräämiseen. Lisäksi sääntelyn laajat poikkeukset ja tulkinnanvaraisuus ovat mahdollistaneet biometrisen tiedon riskialttiita käyttötapoja, kuten reaaliaikainen kasvojentunnistuksen.

EU:n tietosuojalainsäädännössä erityisiin henkilötietoryhmiin liittyviä käsittelysääntöjä on pidetty epäselvinä ja niistä on laadittu huomattava määrä konsultaatioita tietosuojaviranomaisille. Tietosuojaviranomaiset ovat lausuntojen julkaisemisen lisäksi toteuttaneet aloitteita ja tehneet biometrisen datan käsittelyyn liittyviä päätöksiä. Esimerkiksi vuonna 2019 Ranskan tietosuojaviranomainen julkaisi raportin, jossa se esitti useita suosituksia erityisesti liittyen kasvojentunnistuksen kokeiluihin julkisissa tiloissa. Ruotsissa tietosuojaviranomainen määräsi sakon kunnalle, joka oli käyttänyt kasvojentunnistusteknologiaa oppilaiden läsnäolon valvontaan koulujen pilottihankkeessa.[179]

Lisäksi yleisesti tietosuojalainsäädäntöön liittyen on todettu, että koneoppimisen ja siihen liittyvien tekoälyteknologioiden yleistyminen voi hämärtää arkaluonteisten ja muiden henkilötietojen välistä eroa, koska ne mahdollistavat arkaluonteisia ominaisuuksia koskevien päätelmien tekemisen yhdistämällä yksittäin harmittomilta vaikuttavia tietoja muihin tietoihin niiden elinkaaren aikana.[180] Näiden kehityskulkujen vuoksi unionissa on nähty tarvetta aiempaa täsmällisemmälle biometrisen tunnistamisen sääntelylle.

[179] EPRS Study 2021, s. 26.
[180] EPRS Study 2021, s. 27.

# 5 Tekoälyasetus

## 5.1 Yleistä

Euroopassa ei ole annettu yksinomaan biometriaan kohdistuvaa sääntelyä. Keskeisimmät erityissäännöt on annettu EU:n tietosuojalainsäädännössä. Lisäksi EU:n perusoikeusjärjestelmä soveltuu täysimääräisesti biometristen teknologioiden käyttöön. Tämän oikeudellisen kehyksen tarkastelu osoittaa, että teknologinen kehitys etenee osin olemassa olevien oikeuksien ja periaatteiden puitteissa ja toisinaan jopa niistä huolimatta. Näin ollen näitä oikeuksia ja periaatteita voi olla tarpeen vahvistaa, selkeyttää tai ainakin täsmentää.[181]

Tekoälyn käyttö voi vaikuttaa unionin keskeisiin arvoihin ja johtaa useiden perusoikeuksien, rikkomiseen. Nämä riskit voivat johtua esimerkiksi järjestelmien suunnitteluvirheistä, ihmisen suorittaman valvonnan puuttumisesta tai vinoutuneesta datasta. Tekoäly myös lisää mahdollisuuksia seurata ja analysoida ihmisten päivittäisiä tottumuksia ja riskiä siitä, että valtion viranomaiset ja muut toimijat hyödyntävät sitä laajamittaiseen valvontaan.[182] Äärimmäisimmissä näkemyksissä tekoäly voisi alistaa tai jopa tuhota ihmiskunnan. Maltillisempien näkemysten mukaan tekoäly on ihmisten luoma ja hallitsema, mutta sen käyttö voi johtaa joidenkin ihmisten alistamiseen. *Caruanan* ja *Borgin* mukaan järjestelmiä voidaan suunnitella alusta alkaen turvaamaan perus- ja ihmisoikeuksia, koska tekoälyn kehitys on ihmisten käsissä.[183]

Jotta tekoälyn mahdollisuuksiin ja haasteisiin voidaan vastata, tulee EU:n toimia yhtenäisesti ja määrittää eurooppalaisten arvojen pohjalta oma tapansa edistää tekoälyn kehittämistä ja käyttöönottoa.[184] Tämän tavoitteen saavuttamiseksi hyväksyttiin EU:ssa keväällä 2024, jota on pidetty maailman ensimmäisenä tekoälyä kattavasti sääntelevänä oikeudellisena instrumenttina. Asetus tuli voimaan 1. elokuuta 2024 ja se tulee sovellettavaksi vaiheittain kolmen vuoden aikana.[185]

Tekoälyasetuksella tavoitellaan kahta keskeistä päämäärää: toisaalta siinä korostetaan tekoälyjärjestelmiin liittyviä mahdollisia merkittäviä riskejä turvallisuudelle ja perusoikeuksille, ja toisaalta pyritään edistämään tekoälyn kehitystä ja käyttöönottoa EU:ssa sekä yksityisellä että julkisella sektorilla.[186]

---

[181] EPRS study 2021, johdanto-osa sivu II.
[182] COM (2020) 65 final, s. 13.
[183] Caruana – Borg 2025, s. 113–114.
[184] COM (2020) 65 final, s.4.
[185] Lindroos-Hovinheimo ym. 2025, s. 3,7.
[186] Lindroos-Hovinheimo ym. 2025. 11.

Lainsäädäntöprosessi venähti ja kesti paljon odotettua kauemmin.[187] Asetuksen valmisteluvaiheessa käytiin runsaasti keskustelua erityisesti biometrisiin tietoihin perustuvasta kasvojentunnistuksesta ja biometrisistä luokittelujärjestelmistä.[188] Biometristen tunnistusteknologioiden sääntely on jakanut eurooppalaisia toimielimiä. Tekoälyasetuksen valmistelun yhteydessä Euroopan komissio ja Euroopan unionin neuvosto ovat kannattaneet rajattujen poikkeusten säilyttämistä reaaliaikaisen kasvojentunnistuksen käytön kiellosta lainvalvontatarkoituksissa.[189] Euroopan parlamentti yhdessä kansalaisjärjestöjen kanssa, kuten *Amnesty Internationalin* ja *Article 19*, tuki täyskieltoa.[190] Kasvojentunnistusteknologian ei nähdä olevan yhteensopiva eurooppalaisten ja demokraattisten arvojen kanssa. Myöhemmin parlamentti lievensi lähestymistapaansa ja hyväksyi rajoitettuja poikkeuksia reaaliaikaisen kasvojentunnistuksen kieltoon lainvalvontaviranomaisten osalta.[191]

Asetus soveltuu sellaisiin järjestelmiin, jotka käyttävät tekoälyä. Asetuksella on laaja aineellinen ja alueellinen soveltamisala.[192] Tekoälyasetuksen 2 artiklan mukaan asetus soveltuu järjestelmiin, jotka saatetaan EU:n markkinoille, otetaan käyttöön, tuodaan tai jaetaan EU:ssa tai joita käyttää sellainen käyttöönottaja, jonka sijoittumispaikka tai sijaintipaikka on EU:ssa. Asetuksen johdanto-osan 22 kappaleen mukaan asetuksen kiertämisen estämiseksi ja unionissa sijaitsevien luonnollisten henkilöiden tehokkaan suojelun varmistamiseksi asetusta tulee soveltaa myös kolmanteen maahan sijoittuneisiin tekoälyjärjestelmien tarjoajiin ja käyttöönottajiin, mikäli kyseisten järjestelmien tuottamaan tulosta on tarkoitus käyttää unionissa.[193] Asetuksen laajasta alueellisesta ulottuvuudesta johtuu, että se soveltuu esimerkiksi amerikkalaiseen tekoälyjärjestelmän tarjoajaan, jos järjestelmän vaikutukset kohdistuvat esimerkiksi Suomessa asuvaan henkilöön.[194]

## 5.2 Määritelmiä

### 5.2.1 Tekoälyn määritelmä

Tekoäly on yleistermi teknologioille, jotka voivat jäljitellä, automatisoida tai mahdollisesti jopa ylittää ihmisen älyllisiä kykyjä. Tällaisia ovat esimerkiksi symbolinen tekoäly, koneoppiminen

[187] Lindroos-Hovinheimo ym. 2025 s. 8.
[188] Bräutigam ym. 2022, s. 25.
[189] Euroopan unionin neuvosto 2021/0106 (COD) s. 4 ja COM/2021/206 final, kohta 5.2.2.
[190] Amnesty International: EU: European Parliament adopts ban on facial recognition but leaves migrants, refugees and asylum seekers at risk, 14.6.2023.
[191] ks. European Parliament News: Artificial Intelligence Acr: deal on comprehensive rules for trustworthy AI, 9.12.2023.
[192] Lindroos-Hovinheimo 2025, s. 57.
[193] Tekoälyasetus johdanto-osa 22 perustelukappale.
[194] Lindroos-Hovinheimo ym. 2025, s. 58.

tai tilastolliset menetelmät. Kun esimerkiksi mediassa puhutaan tekoälyn suurista edistysaskeleista tai vastaavasti keskustellaan tekoälyn vaaroista, viitataan useimmiten juuri koneoppimiseen. Esimerkiksi kuvien luokittelu ja kasvojentunnistus perustuvat koneoppimiseen.[195]

Tekoälyasetuksessa tekoälyjärjestelmä määritellään konepohjaiseksi järjestelmäksi, joka on suunniteltu toimimaan käyttöönoton jälkeen vaihtelevilla autonomian tasoilla ja jossa voi ilmetä mukautuvuutta käytön aikana. Se päättelee vastaanottamansa syötteen perusteella, eksplisiittisiä tai implisiittisiä tavoitteita varten, miten tuottaa tuotoksia - kuten ennusteita, sisältöä, suosituksia tai päätöksiä - jotka voivat vaikuttaa fyysisiin tai virtuaalisiin ympäristöihin.[196]

Koneoppimisen keskeinen piirre on sen kyky oppia ja mukautua. Toisin kuin esimerkiksi symbolinen tekoäly, joka toimii ennalta määriteltyjen sääntöjen varassa eikä muutu kokemuksen myötä, koneoppiminen hyödyntää dataa ja kehittää toimintaansa sen perusteella. Koulutusvaiheessa algoritmille syötetään harjoitusdataa, jonka avulla se oppii tunnistamaan oikeita toimintatapoja. Mikäli algoritmi tekee virheen, se mukauttaa toimintaansa niin, että virhe vältetään vastaisuudessa. Lisäksi koneoppimisjärjestelmät voivat jatkaa oppimista varsinaisen koulutusvaiheen jälkeen eli mukautua uusiin tilanteisiin ja muuttuvaan ympäristöön käytön aikana.[197]

Koneoppiminen eroaa symbolisesta tekoälystä myös siinä, ettei se perustu ihmisten ennalta ohjelmoimiin sääntöihin. Symbolinen tekoäly voi matkia ihmisen älykkyyttä yhdistämällä suuren joukon sääntöjä yhdeksi algoritmiksi. Mitä monimutkaisempi sääntökokonaisuus, sitä suurempi älykkyyden illuusio. Koneoppiminen luo vahvemman vaikutelman älykkyydestä: se ei ainoastaan noudata sääntöjä, vaan muodostaa ne itse ja pystyy muuttamaan niitä kohdatessaan uutta dataa.[198]

Kolmas keskeinen ero liittyy läpinäkyvyyteen. Symbolisen tekoälyn toiminta voidaan yleensä kuvata selkeästi sääntöjen ja päätöspuiden avulla. Sen sijaan koneoppimisalgoritmien muodostamat säännöt eivät ole ihmisille helposti ymmärrettävässä muodossa ja vaikka sen toimintaa pystyttäisiin teknisesti avaamaan, sen logiikka ei välttämättä olisi ihmiselle ymmärrettävää. Tämä tekee koneoppimisesta sekä tehokasta että ongelmallista. Vaikka koneoppimisella on potentiaali olla erittäin tehokas työkalu vaikuttavaan päätöksentekoon, sen kyvyttömyys selittää, miksi tiettyyn lopputulokseen on päädytty voi jättää päätöksenteon perusteet epäselviksi.[199]

---

[195] European Parliamentary Research Service, Artificial intelligence: From ethics to policy 2020, s. 5.
[196] Tekoälyasetuksen 3 artikla 1 kohta.
[197]European Parliamentary Research Service, Artificial intelligence: From ethics to policy 2020 s. 5-6.
[198] European Parliamentary Research Service, Artificial intelligence: From ethics to policy 2020, s. 6.
[199]European Parliamentary Research Service, Artificial intelligence: From ethics to policy 2020, s. 6.

Yhä useammin uudet biometristen teknologioiden sovellukset perustuvat koneoppimiseen, joka muodostaa keskeisen haasteen vastuunalaisuudelle ja oikeussuojalle automatisoidun päätöksenteon yhteydessä. Kun päätöksen taustalla oleva logiikka ja oletukset eivät ole selkeitä, muun muassa tuomioistuinten on vaikeaa arvioida esitettyjen todisteiden paikkansapitävyyttä.[200]

### 5.2.2 Biometrisiin teknologioihin liittyvät käsitteet tekoälyasetuksessa

Biometrinen tieto on pääpiirteiltään määritelty tekoälyasetuksessa samoin kuin yleisessä tietosuoja-asetuksessa ja rikosasioiden tietosuojadirektiivissä: ” *kaikkia luonnollisen henkilön fyysisiin ja fysiologisiin ominaisuuksiin tai käyttäytymiseen liittyvällä teknisellä käsittelyllä saatuja henkilötietoja, kuten kasvokuvia tai sormenjälkitietoja*”. Tekoälyasetukseen ei ole otettu yleisen tietosuoja-asetuksen määritelmään sisältyvää lisäedellytystä siitä, että niiden perusteella henkilö voidaan tunnistaa tai kyseisen henkilön tunnistaminen voidaan varmistaa.

Tosin kuin yleisessä tietosuoja-asetuksessa ja rikosasioiden tietosuojadirektiivissä, tekoälyasetuksessa on määritelty erikseen biometrinen tunnistus ja todennus. Tunnistus on määritelty asetuksessa ihmisten fyysisten, fysiologisten, käyttäytymiseen liittyvien ja psykologisten ominaisuuksien automaattiseksi tunnistamiseksi luonnollisen henkilön henkilöllisyyden toteamiseksi. Tunnistuksessa verrataan kyseisen henkilön biometrisiä tietoja tietokantaan tallennettuihin toisten yksilöiden biometrisiin tietoihin.[201] Koska asetusten määritelmissä on eroja, voidaan biometrisillä tiedoilla asiayhteydestä riippuen tarkoittaa hieman eri asiaa. Nämä erot voivat aiheuttaa päänvaivaa tilanteessa, jossa molemmat asetukset tulevat sovellettaviksi.[202]

Asetuksessa säädetään säännöistä, jotka koskevat monenlaisia tekoälyjärjestelmiä. Biometrisen teknologioiden keskeinen merkitys ilmenee siinä, että tekoälyasetus määrittelee kolme tekoälyjärjestelmätyyppiä suoraan niiden biometriseen dataan perustuvan luonteen pohjalta ja asettaa niille erityiset säännöt. Näitä ovat biometriset etätunnistusjärjestelmät, tunteentunnistusjärjestelmät ja biometriset luokittelujärjestelmät.[203]

Biometrisellä etätunnistusjärjestelmällä tarkoitetaan tekoälyjärjestelmää, jonka avulla luonnollinen henkilö voidaan tunnistaa ilman hänen aktiivista osallistumistaan, tyypillisesti etäältä, vertaamalla hänen biometrisiä tietojaan viitetietokantaan tallennettuihin biometrisiin tietoihin. Tällaista järjestelmää käytettäessä henkilö ei välttämättä tiedä, että häntä tunnistetaan.[204]

---

[200] ARTICLE 19 2021, s. 17.
[201] Tekoälyasetuksen 3 artiklan 34 ja 35 alakohta.
[202] Lindroos-Hovinheimo ym. 2025, s. 141.
[203] EPRS study 2021, johdanto-osa sivu I.
[204] EPRS study 2021, s. 4.

Biometristen etätunnistusjärjestelmien kohdalla asetuksessa määritellään ero reaaliaikaisten ja jälkikäteisten järjestelmien välillä. Asetuksessa nämä järjestelmät on määritelty seuraavasti:

> *42) ”reaaliaikaisella biometrisellä etätunnistusjärjestelmällä” biometristä etätunnistusjärjestelmää, jossa biometristen tietojen kerääminen, vertailu ja tunnistaminen tapahtuvat ilman merkittävää viivettä ja joka kattaa välittömän tunnistamisen lisäksi myös vähäiset viiveet, joilla pyritään ehkäisemään harhaanjohtamista;*
>
> *43) ”jälkikäteisellä biometrisellä etätunnistusjärjestelmällä” muuta kuin reaaliaikaista biometristä etätunnistusjärjestelmää.* [205]

Tekoälyasetuksen johdanto-osassa on myös selvennetty eroa järjestelmien välillä. Reaaliaikaisissa järjestelmissä biometriset tiedot kerätään, vertaillaan ja tunnistetaan välittömästi, lähes välittömästi tai joka tapauksessa ilman merkittävää viivettä. Tämän vuoksi sääntelyä ei tulisi voida kiertää käyttämällä vähäisiä viivästyksiä. Käytännössä reaaliaikaiset järjestelmät perustuvat kameran tai muun vastaavan laitteen tuottamaan suoraan tai lähes suoraan materiaaliin. Jälkikäteisissä järjestelmissä kyse on esimerkiksi valvontakameroiden tai yksityisten laitteiden tuottamasta kuva- tai videomateriaalista, joka on tallennettu ennen kuin sitä käytetään henkilöiden tunnistamiseen.[206]

Tunteentunnistusjärjestelmä on määritelty tekoälyjärjestelmäksi, jonka avulla luonnollisten henkilöiden tunteita ja aikomuksia voidaan tunnistaa tai päätellä henkilöiden biometristen tietojen perusteella.[207] Biometrinen luokittelujärjestelmä on asetuksessa määritelty tekoälyjärjestelmäksi, jonka avulla luonnolliset henkilöt luokitellaan heidän biometristen tietojensa perusteella tiettyihin ryhmiin, lukuun ottamatta tilanteita, joissa tällainen luokittelu on toisen kaupallisen palvelun oheistoiminto ja ehdottoman välttämätöntä objektiivisista teknisistä syistä.[208]

## 5.3 Tekoälyasetuksen suhde aiempaan EU:n tietosuojalainsäädäntöön

Valmisteluvaiheessa korostettiin, että sääntelyssä on vältettävä ristiriitoja jo voimassa olevan sääntelyn kanssa, erityisesti yleisen tietosuoja-asetuksen ja rikosasioiden tietosuojadirektiivin

[205] Tekoälyasetuksen 3 artiklan 42 ja 43 kohta.
[206] Tekoälyasetuksen johdanto-osan 17 perustelukappale.
[207] Tekoälyasetuksen 3 artiklan 39 alakohta.
[208] Tekoälyasetuksen 3 artiklan 40 alakohta.

kanssa. Tämä on tärkeää oikeusvarmuuden vuoksi sekä sen varmistamiseksi, ettei tekoälyasetus heikennä suoraan tai välillisesti henkilötietojen suojaa koskevaa perusoikeutta.[209]

Tekoälyasetuksen mukaan asetusta ei sovelleta tietosuojakysymyksissä. Henkilötietojen suojaa, yksityisyyttä ja viestinnän luottamuksellisuutta koskevaa unionin oikeutta sovelletaan henkilötietoihin, joita käsitellään tekoälyasetuksessa säädettyjen oikeuksien ja velvoitteiden yhteydessä. Tekoälyasetus ei vaikuta muun muassa yleisen tietosuoja-asetuksen ja rikosasioiden tietosuojadirektiivin soveltamiseen.[210] Pääsäännön mukaan niitä sovelletaan tekoälyasetuksen sijaan silloin, kun kyseiset säädökset tulevat sovellettaviksi omien soveltamisalasäännöstensä perusteella.[211]

Pääsääntöön on kuitenkin poikkeuksia. Siinä määrin kuin se on ehdottoman välttämätöntä, voidaan suuririskisten tekoälyjärjestelmien vinoutumien havaitsemisen ja korjaamisen varmistamiseksi poikkeuksellisesti käsitellä erityisiä henkilötietoryhmiä.[212] Edellytyksenä on, että luonnollisten henkilöiden perusoikeudet ja -vapaudet turvataan asianmukaisilla suojatoimilla. Tällainen käsittely edellyttää myös asetuksen 10 artiklan 5 kohdan mukaisten erityisten ehtojen täyttymistä. Poikkeuksesta johtuu, että tietyissä ehdottoman välttämättömissä tilanteissa erityisiä henkilötietoryhmiä, kuten biometrisiä tietoja, voidaan käsitellä tietosuojasääntelystä poikkeavalla tavalla tekoälyasetuksen 10 artiklan 5 kohdan asettamin ehdoin.[213]

Toinen poikkeus liittyy niin sanottuihin sääntelyhiekkalaatikoihin tai testiympäristöihin. Tekoälyasetuksen 59 artikla mahdollistaa tietyin ehdoin ja edellytyksin sen, että tietosuojasääntelystä voidaan poiketa tekoälyjärjestelmien kehitys-, koulutus- ja testaustilanteissa.

Tekoälyasetuksessa ei nimenomaisesti määritellä, miten sen ja tietosuojasääntelyn välinen suhde käytännössä rakentuu. Sen 2 artiklan soveltamisalaa koskevista säännöksistä käy kuitenkin ilmi, että tietosuojasääntely, käytännössä tietosuoja-asetus, soveltuu aina, kun kyse on henkilötietojen käsittelystä. Koska monet tekoälyjärjestelmät käsittelevät laajoja tietomääriä, mukaan lukien henkilötietoja, tietosuoja-asetus tulee usein sovellettavaksi myös tekoäly-yhteyksissä.

Tekoälyasetus sääntelee siten monin osin toimintaa, josta on jo säädetty yleisessä tietosuoja-asetuksessa. Lähtökohtaisesti näitä säädöksiä sovelletaan rinnakkain. Mikäli niiden välillä kuitenkin ilmenee ristiriitaa, etusija annetaan tietosuoja-asetukselle. Tähän liittyy myös se, ettei

[209] Euroopan tietosuojaneuvoston ja Euroopan tietosuojavaltuutetun yhteinen lausunto 5/2021, s. 19.
[210] Tekoälyasetuksen 2 artiklan 7 kohta.
[211] Lindroos-Hovinheimo ym. 2025, s. 66.
[212] Tekoälyasetuksen 2 artiklan 7 kohta.
[213] Lindroos-Hovinheimo ym. 2025, s. 66.

teosta, josta on määrätty yleisen tietosuoja-asetuksen perusteella seuraamusmaksu, voida määrätä tekoälyasetuksen mukaista seuraamusmaksua.[214]

Komission tiedonannon mukaan tekoälyasetuksella ei rajoiteta erityisesti perusoikeuksien suojelua, kuluttajansuojaa, työllisyyttä, työntekijöiden suojelua ja tuoteturvallisuutta. Asetus perustuu ennaltaehkäisevään ja turvallisuutta korostavaan sääntelylogiikkaan: tiettyjä tekoälyjärjestelmiä ei saa saattaa markkinoille tai käyttää tietyillä tavoilla. Samalla tekoälyasetus ei rajoita muiden EU-oikeuden säännösten soveltamista. Näin ollen silloinkin, kun tekoälyjärjestelmää ei ole kielletty tekoälyasetuksessa, voi sen käyttö olla kiellettyä tai laitonta unionin muun primaari- tai sekundaarioikeuden perusteella. Näin voi olla esimerkiksi silloin, jos henkilötietojen käsittelylle ei ole tietosuojalainsäädännön edellyttämää oikeusperustaa tai jos järjestelmän käyttö johtaa unionin oikeudessa kiellettyyn syrjintään. Siten pelkkä tekoälyasetuksen mukaisten kieltojen noudattaminen ei riitä osoittamaan, että tekoälyjärjestelmien tarjoajat tai käyttöönottajat täyttävät myös muun unionin oikeuden asettamat vaatimukset.[215]

## 5.4 Tekoälyasetuksen riskiperusteinen lähestymistapa

Tekoälyasetuksen keskeinen periaate on riskiperusteinen lähestymistapa, jonka tavoitteena on varmistaa, että säännöt ovat tehokkaita ja oikeasuhteisia. Tässä lähestymistavassa tekoälyjärjestelmiin kohdistuvat vaatimukset määräytyvät niiden aiheuttamien riskien perusteella: mitä suurempi riski, sitä tiukempi sääntely.[216] Riskiperusteinen lähestymistapa ilmenee asetuksessa siten, että sääntelyä on lähinnä kielletyille ja suuririskisille järjestelmille sekä yleiskäyttöisille tekoälymalleille. Euroopan komission tekoälyn korkean tason asiantuntijaryhmän vuonna 2019 julkaisemasta ohjeistuksesta sekä Euroopan komission vuonna 2020 julkaisemasta valkoisesta kirjasta lähtien tekoälyn sääntely on rakentunut riskien tunnistamiseen.[217]

Tekoälyasetus määrittelee riskin 3 artiklassa haitan esiintymisen todennäköisyyden ja haitan vakavuuden yhdistelmäksi. Myös tietosuoja-asetuksen keskeinen periaate on riskiperusteinen lähestymistapa.[218] Lainsäädäntö sisältää sekä oikeuksia että velvollisuuksia, mutta tuoteturvallisuuteen liittyvä sääntely, kuten tekoälyasetus, painottuu ennen kaikkea toimijoille asetettaviin velvollisuuksiin.[219]

---

[214] Lindroos-Hovinheimo ym. 2025, s. 67.
[215] Komission tiedonanto C (2025) 5052 final, s. 16.
[216] Tekoälyasetuksen johdanto-osan 26 perustelukappale.
[217] COM (2020) 65 final, s. 10.
[218] Korpisaari 2022, s. 30–31.
[219] Caruana – Borg 2025, s. 111.

Tekoälyasetus asettaa erilaisia velvoitteita riskitason perusteella.

1) Kielletyt järjestelmät: tekoälyjärjestelmät, jotka aiheuttavat perusoikeuksiin ja unionin arvioihin kohdistuvia kohtuuttomia riskejä.
2) Suuririskiset tekoälyjärjestelmät: aiheuttavat suuria riskejä terveydelle, turvallisuudelle ja perusoikeuksille. Tähän luokkaan kuuluviin järjestelmiin sovelletaan tiettyjä vaatimuksia ja velvoitteita.
3) Avoimuuteen kohdistuva riski: tekoälyjärjestelmiin, joiden aiheuttama avoimuusriski on vähäinen, sovelletaan tekoälyasetuksen 50 artiklan mukaisia avoimuusvelvoitteita.
4) Minimaalinen riski tai ei riskiä: tekoälyjärjestelmä aiheuttaa minimaalisen riskin tai ei lainkaan riskejä. Näitä ei asetuksessa säännellä, mutta järjestelmien tarjoajat ja käyttöönottajat voivat halutessaan noudattaa vapaaehtoisia käytännesääntöjä.[220]

Riskiperusteisen lähestymistavan valitseminen esimerkiksi suorien kieltojen tai sääntelyhiekkalaatikoihin tukeutumisen sijaan edesauttaa joustavien mekanismien luomisessa. Niiden avulla voidaan mukauttaa sääntelyä teknologian kehittyessä ja uusien ongelmatilanteiden ilmetessä.[221] Tästä näkökulmasta Euroopan unionin valitsema horisontaalinen ja riskiperusteinen sääntelymalli on perusteltu.[222] *DigitalEurope* on arvioinut, että oikein tehtynä keskittyminen tekoälyjärjestelmien käytön todelliseen tarkoitukseen varmistaa, että uudet velvoitteet liittyvät tapauksiin, joissa todellakin voi olla uusia riskejä. Samalla vältetään lisäsääntely matalan riskin ja toissijaisten tekoälyjärjestelmien osalta jo ennestään vankan EU:n turvallisuuslainsäädännön ulkopuolella. Tekoälyasetus paitsi mukauttaa jo olemassa olevaa tuoteturvallisuuslainsäädäntöä, myös asettaa oman luokkansa korkean riskin käyttötapauksille.[223]

Luotettavan tekoälyn ajatus nojautuu pitkälti perusoikeuksiin nojaavaan lähestymistapaan. Ajatuksena on, että tekoälyjärjestelmään voidaan luottaa, jos se kunnioittaa yksilön perusoikeuksia. Tekoälyjärjestelmien katsotaan aiheuttavan riskejä perusoikeuksille ja niiden katsotaan edellyttävän erityistä suojaa. Perusoikeudet eroavat sellaisista normeista, jotka suoraan kieltävät tai määräävät tiettyjä tekoja. Ne ovat normatiivisia odotuksia, jotka on kirjattu kansallisiin perustuslakeihin ja vastaaviin ylikansallisiin sopimuksiin, kuten Euroopan unionin perusoikeuskirja. Ne ovat sääntöjen sijasta ennemmin periaatteita. Kun tuomioistuimet ratkaisevat asioita, ne soveltavat suhteellisuusperiaatetta arvioidakseen, rajoittaako jokin oikeussääntö perusoikeuksia.

[220] Komission tiedonanto C (2025) 5052 final, s. 1.
[221] Kusche 2024, s. 5.
[222] Neuwirth 2022, s. 15.
[223] DIGITALEUROPE 2021, s. 2–3.

Tällainen rajoitus voidaan hyväksyä, jos sääntely edistää tavoiteltua päämäärää oikeassa suhteessa eikä käytettävissä ole vähemmän rajoittavaa keinoa.[224]

Jo ennen tekoälyn yleistymistä oikeusjärjestelmä ei tuntenut normeja, jotka estäisivät kaikki perusoikeuksien rajoitukset. Ratkaisevaa on ollut tuomioistuinten tapauskohtainen arvio siitä, milloin perusoikeuteen on tosiasiallisesti puututtu hyväksyttävyyden rajat ylittäen. Riskiperusteisessa sääntelyssä tätä arviointia tehdään osittain etukäteen riskien kautta. Vaikka riskiarviointi voi olla osa oikeudellista menettelyä, kyse ei ole perinteisestä intressien ja periaatteiden välisestä punninnasta.[225]

Koska biometriset tekoälyjärjestelmien perusoikeusvaikutukset voivat olla merkittävät, kuuluvat ne tavanomaisesti kiellettyihin tai suuririskisten tekoälyjärjestelmien luokkaan. Tämän vuoksi tässä tutkielmassa keskitytään näistä vain kahteen ensimmäiseen.

### 5.4.1 Kielletyt tekoälyyn liittyvät käytännöt

#### *5.4.1.1 Tunteiden tunnistusjärjestelmät*

Käytännöt, joilla tunnistetaan tunteita työpaikoilla tai oppilaitoksilla, ovat kiellettyjä asetuksen 5 artiklan 1 kohdan ensimmäisen alakohdan f alakohdan nojalla. Poikkeuksena kieltoon on tällaisten järjestelmien lääketieteellinen ja turvallisuuteen liittyvä käyttö. Tunteilla ja aikomuksilla tarkoitetaan esimerkiksi onnellisuutta, surua, vihaa, häpeää ja tyytyväisyyttä. Ne eivät kata fyysisiä olotiloja, kuten kipua tai väsymystä.[226] Asetuksessa ei kuitenkaan juuri selvennetä, mitä ”aikomuksella” tarkoitetaan. Asetuksen johdanto-osassa esitettyjä esimerkkejä ei tavallisesti luokitella aikomuksiksi, sillä aikomuksiin liittyy tyypillisesti ennakoiva ja tulevaisuuteen suuntaava ulottuvuus. Johdannossa mainitut esimerkit kuvaavat pikemminkin yksilöiden tämänhetkisiä reaktioita tilanteisiin tai ympäristöihin.[227]

Tunteidentunnistusta voidaan käyttää useilla eri aloilla, kuten kohdennetussa mainonnassa, lääketieteessä esimerkiksi masennuksen havaitsemiseen sekä koulutuksessa oppilaiden tarkkaavaisuuden ja osallistumisen seuraamiseen. Lainvalvonnassa ja yleiseen turvallisuuteen liittyen tunteentunnistusta voidaan käyttää valheenpaljastimina ja tunteiden seurantaan muun muassa suurissa tapahtumissa.[228] Viittaukset valheenpaljastimiin eivät lisää luottamusta sääntelyyn,

[224] Kusche 2024, s. 6, 10.
[225] Kusche 2024, s. 6.
[226] Tekoälyasetuksen johdanto-osan 18 perustelukappale.
[227] Bird & Bird: “What is an Emotion Recognition System under the EU’s Artificial Intelligence Act? Part 1 - A machine that “understands” your Monday blues!” 4.11.2024.
[228] Komission tiedonanto C(2025) 5052 final, s. 91.

vaikka niitä on käytetty pitkään lainvalvonnassa muun muassa Yhdysvalloissa. Niiden kykyä havaita valheita pidetään tieteellisesti kiistanalaisena.[229]

Tunteiden ilmaisutavat vaihtelevat huomattavasti kulttuurien ja tilanteiden välillä, ja suurta vaihtelua voi esiintyä myös henkilön omassa tunteiden ilmaisussa. Näiden järjestelmien keskeisiä puutteita ovatkin heikko luotettavuus, puutteellinen tarkkuus ja heikko yleistettävyys.[230] Virheriski korostuu erityisesti arkisissa ympäristöissä, kuten julkisilla paikoilla, joissa järjestelmiä mahdollisesti käytetään.[231]

#### *5.4.1.2 Biometriset luokittelujärjestelmät*

Tekoälysäädöksen 5 artiklan 1 kohdan ensimmäisen alakohdan g alakohta kieltää biometriset luokittelujärjestelmät, joissa luonnollisia henkilöitä luokitellaan heidän biometristen tietojensa perusteella siten, että niistä päätellään tai johdetaan tietoja esimerkiksi rodusta, poliittisista mielipiteistä, ammattiliiton jäsenyydestä, uskonnollisesta tai filosofisesta vakaumuksesta taikka seksuaalisesta käyttäytymisestä tai suuntautumisesta. Kielto ei kuitenkaan koske sellaista biometrisiin tietoihin perustuvaa merkitsemistä, suodattamista tai luokittelua, joka perustuu unionin tai kansallisen lainsäädännön mukaisesti hankittuihin tietoihin ja jota voidaan hyödyntää esimerkiksi lainvalvonnassa.[232]

Biometrinen luokittelu voi kohdistua esimerkiksi kasvojen piirteisiin tai ihonväriin taikka DNA:han tai käyttäytymiseen liittyviin seikkoihin, kuten näppäinpainallusten analyysiin tai kävelytyyliin. Kyseiset luokittelujärjestelmät loukkaavat ihmisarvoa ja aiheuttavat merkittäviä riskejä muille perusoikeuksille, kuten yksityisyyden suojalle ja syrjimättömyydelle.[233]

#### *5.4.1.3 Reaaliaikaiset biometriset etätunnistusjärjestelmät*

Tekoälyasetus kieltää reaaliaikaisten biometristen etätunnistusjärjestelmien käytön yleisölle avoimissa tiloissa lainvalvontatarkoituksiin. Kielto ei ole absoluuttinen, sillä se sallii tiettyjä merkittäviä poikkeuksia. Jälkikäteiset biometriset etätunnistusjärjestelmät luokitellaan liitteen

---

[229] ks. Loideain verkkoartikkeli: A Trustworthy Framework that Respects Fundamental Rights? The Draft EU AI Act and Police Use of Biometrics, 2021. Yhdysvaltojen korkein oikeus on todennut, että niiden valheenpaljastimen luotettavuudesta ei ole yksimielisyyttä.
[230] Komission tiedonanto C (2025) 5052 final, s. 91.
[231] ks. Loideain 2021.
[232] Tekoälyasetuksen 5 artiklan 1 kohdan ensimmäisen alakohdan g alakohta.
[233] Komission tiedonanto C (2025) 5052 final, s. 103.

III mukaisesti korkean riskin tekoälyjärjestelmiksi.[234] Kun valvontajärjestelmä kattaa julkisesti saavutettavan tilan, se tarkoittaa käytännössä sitä, että jokaisen alueen läpi kulkevan henkilön biometriset tiedot skannataan. Vaikka kasvojentunnistus on todennäköisesti yleisin biometrisen etätunnistuksen muoto, tunnistaminen voidaan tehdä myös muiden biometristen tietojen avulla. Muita henkilön yksilöiviä piirteitä ovat esimerkiksi henkilön kävelytyyli ja korvan muoto.[235]

Tekoälyasetuksen johdanto-osan 32 kappaleessa myönnetään, että reaaliaikaisten biometristen etätunnistusjärjestelmien käyttäminen julkisissa tiloissa lainvalvontatarkoituksessa puuttuu erityisen pitkälle menevällä tavalla asianomaisten henkilöiden oikeuksiin ja vapauksiin, koska se voi vaikuttaa suuren väestönosan yksityiselämään, synnyttää tunteen jatkuvasta valvonnasta ja estää välillisesti kokoontumisvapauden ja muiden perusoikeuksien käyttämisen.[236]

Kyseisten järjestelmien epätarkkuudet voivat johtaa vinoutuneisiin tuloksiin ja aiheuttaa syrjiviä vaikutuksia. Lisäksi näiden järjestelmien käyttöön liittyvien vaikutusten välittömyys ja rajalliset mahdollisuudet lisätarkastuksiin tai korjauksiin lisäävät asianomaisten henkilöiden oikeuksiin tai vapauksiin kohdistuvia riskejä lainvalvonnan yhteydessä.[237]

Reaaliaikaisen ja jälkikäteisen järjestelmätyypin erottelua ovat kyseenalaistaneet muun muassa kansalaisjärjestöt ja tutkijat. Molemmat järjestelmät voivat aiheuttaa samanlaisia riskejä yksilöiden joutumisesta jatkuvan seurannan kohteeksi. Biometrisen etätunnistuksen käyttö julkisissa tiloissa, reaaliaikainen tai jälkikäteinen, on yksi keskeinen tapa, joka on johtanut massavalvontaan, koska tällainen laajamittainen ja kohdentamaton valvonta on luonteeltaan suhteetonta.[238]

*Giannini* ja *Tas* esittävät, että jälkikäteiset järjestelmätyypit voivat vaikuttaa jossain tilanteissa enemmän perusoikeuksiin ja -vapauksiin kuin reaaliaikainen biometrinen etätunnistusjärjestelmä. Koska ne hyödyntävät laajempia tietoaineistoja ja niillä on enemmän aikaa analysoida tietoa, niiden avulla voidaan tunnistaa henkilöitä pitkän ajan kuluttua tapahtumista. Tällaisella käytöllä voi olla vaikutusta esimerkiksi sananvapauden ja kokoontumisvapauden harjoittamiseen, jos ihmiset pelkäävät joutuvansa tunnistetuiksi mielenosoituksissa tai muussa julkisessa tilaisuudessa vielä pitkänkin ajan kuluttua.[239] Myös tohtori *Nóra Ni Loideain* on kysynyt, miksi

---

[234] Tekoälyasetus 5(1) h.
[235] EPRS study 2021, s. 16.
[236] Tekoälyasetuksen johdanto-osan 32 perustelukappale.
[237] Tekoälyasetuksen johdanto-osan 32 perustelukappale.
[238] ks. kansalaisjärjestöjen yhteinen lausunto:" EU's AI Act fails to set gold standard for human rights" 3.4.2024. Järjestöt ovat lisäksi todenneet, että EU:n lainsäätäjien tulisi vastustaa biometrisen valvonnan infrastruktuurien laajentamista. Tällaisia hankkeita ovat esimerkiksi Prüm II -järjestelmän laajentamista, EURODAC-asetuksen kehittäminen ja EU:n laajempi yhteen toimivien tietokantojen infrastruktuuri.
[239] ks. Giannini – Tas verkkoartikkeli: *AI Act and the Prohibition of Real-Time Biometric Identification: Much ado about nothing?* 2024.

ajallinen viive kuvan tai muun biometrisen tiedon keräämisen ja sen myöhemmän käsittelyn välillä määrittäisi puuttumisen vakavuuden.[240]

Samoilla linjoilla ovat olleet myös Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu. Eurooppalaiset tietosuojaviranomaiset ovat pitäneet epäselvänä sitä, mitä ”merkittävällä viiveellä” tarkoitetaan sekä miksi sitä pidetään lieventävänä tekijänä, kun otetaan huomioon, että massatunnistusjärjestelmällä voidaan tunnistaa tuhansia ihmisiä jo muutamassa tunnissa. Lisäksi käsittelyn tunkeutuvuus ei riipu pelkästään käsittelyn tarkoituksesta. Vaikka järjestelmää käytettäisiin esimerkiksi yksityiseen turvallisuuteen, se voi silti aiheuttaa samanlaisia uhkia perusoikeuksille. Lisäksi on huomattavaa, että rajoituksista huolimatta, rikoksista epäiltyjen tai rikosten tekijöiden mahdollinen määrä on usein riittävän suuri, että tekoälyjärjestelmien käyttö epäiltyjen havaitsemiseen voidaan helposti oikeuttaa huolimatta 5 artiklassa asetetuista lisäehdoista.[241]

Komission tiedonannossa on vahvistettu, että ilmausta ”ilman merkittävää viivettä” ei ole määritelty asetuksessa, vaan se on arvioitava tapauskohtaisesti. Koska reaaliaikaiseen tunnistamiseen ja jälkikäteiseen etäältä tapahtuvaan tunnistamiseen käytetään usein samoja laitteita, ero niiden välillä on ajallinen. Viivettä voidaan tiedonannon mukaan pitää merkittävänä ainakin silloin, kun henkilö on todennäköisesti jo poistunut paikasta, jossa biometriset tiedot kerättiin.[242]

#### *5.4.1.4 Kiellon poikkeukset*

Kuten todettu, reaaliaikaiset biometriset etätunnistusjärjestelmät lainvalvontatarkoituksiin ovat tekoälyasetuksen mukaan pääsääntöisesti kiellettyjä. Kielto ei ole ehdoton. Asetuksen 5 artiklan 1 kohdan h alakohdan mukaan tämän teknologian käyttö on sallittua, jos se on ehdottoman välttämätöntä seuraaviin tarkoituksiin: (i) kaappauksen, ihmiskaupan ja seksuaalisen hyväksikäytön uhrien kohdennettu etsintä sekä kadonneiden henkilöiden etsintä; (ii) luonnollisten henkilöiden henkeen tai fyysiseen turvallisuuteen kohdistuvan erityisen, merkittävän ja välittömän uhan taikka aidon ja välittömän tai aidon ja ennakoitavissa olevan terrori-iskun uhan ehkäiseminen; ja (iii) rikoksesta epäillyn henkilön paikantaminen tai tunnistaminen, kun se on tarpeen tutkintaa, syytteeseenpanoa tai rangaistuksen täytäntöönpanoa varten, edellyttäen, että rikos on

---

[240] ks. Nóra Ni Loideain verkkoartikkeli ’A Trustworthy Framework that Respects Fundamental Rights? The Draft EU AI Act and Police Use of Biometrics, 4.8.2021.

[241] Euroopan tietosuojaneuvoston ja Euroopan tietosuojavaltuutetun yhteinen lausunto 5/2021, s. 13. Tekoälyasetuksen luonnoksen COM (2021) 206 final ja hyväksytyn version johdanto-osien perustelukappaleet liittyen merkittävään viiveeseen eivät poikkea toisistaan merkittävästi (asetusluonnoksessa kohta 8 ja hyväksytyssä asetuksessa kohta 17).

[242] Komission tiedonanto C (2025) 5052 final, s. 112.

liitteessä II tarkoitettu ja siitä voidaan määrätä kansallisen lain mukaan vähintään neljän vuoden enimmäisrangaistus.[243]

Näissä tilanteissa unionin lainsäätäjä on pyrkinyt tasapainottamaan yhteiskunnan turvallisuustarpeiden ja reaaliaikaisten biometristen etätunnistusjärjestelmien aiheuttamat riskit tunnistuksen kohteina olevien henkilöiden perusoikeuksille.[244]

Kaksi ensimmäistä alakohtaa vaikuttavat selkeiltä ja johdonmukaisilta, mutta viimeisen kohdalla saattaa olla eroja jäsenvaltioiden välillä. Keskeinen syy tähän on rikosten määrittelyyn liittyvät eroavuudet. Tekoälyasetuksen liitteessä II esitetään tyhjentävä luettelo kuudestatoista rikoksesta, joiden yhteydessä reaaliaikaisten biometristen etätunnistusjärjestelmien käyttö voidaan sallia. Luettelossa mainituille rikoksille ei ole olemassa yhtenäistä eurooppalaista määritelmää. Esimerkiksi raiskauksen määritelmä vaihtelee jäsenvaltioiden välillä. Osa jäsenvaltioista pitää suostumuksen puutetta rikoksen olennaisena osatekijänä, kun taas toiset eivät, kuten Ranska. Toinen esimerkki liittyy kansainvälisen rikostuomioistuimen toimivaltaan kuuluviin rikoksiin, kuten kansanmurhaan, rikoksiin ihmisyyttä vastaan ja sotarikoksiin. Jäsenvaltiot ovat sisällyttäneet nämä rikokset kansalliseen lainsäädäntöön eri tavoin. Osa valtioista, kuten Espanja, on sisällyttänyt kansainväliset rikokset rikoslakeihinsa, ja osa taas on säätänyt niitä varten erityisen lain, kuten Saksa. Sen sijaan esimerkiksi Italiassa ei ole tehty vastaavaa kattavaa sääntelyä. Tämä hajanaisuus rikosmääritelmissä jäsenvaltioiden välillä voi johtaa siihen, että reaaliaikaisten biometristen etätunnistusjärjestelmien käyttö on sallittua yhdessä jäsenvaltiossa, kun taas toisessa se on kielletty.

#### *5.4.1.5 Käytön laajentuminen*

Reaaliaikaisten biometristen etätunnistusjärjestelmien kiellon poikkeukset voivat johtaa paitsi tekoälyasetuksen käyttöönoton pirstaloitumiseen unionissa sekä niiden käyttöönoton laajaan ja vaaralliseen laajenemiseen.[245]

Vaaraa laajentumisesta on havaittavissa myös analysoitaessa tekoälyasetuksen vuorovaikutusta rikosasioiden tietosuojadirektiivin kanssa. Koska reaaliaikaisten biometristen etätunnistusjärjestelmien käyttö edellyttää biometrisen datan käsittelyä lainvalvontaviranomaisten toimesta, periaatteessa sen tulisi kuulua direktiivin soveltamisalaan ja erityisesti sen artiklaan 10, joka koskee erityisten tietoryhmien käsittelyä. Monet jäsenvaltiot, kuten Italia ja Alankomaat, eivät ole säätäneet erityistä kansallista lainsäädäntöä tämän arkaluonteisen tietoryhmän käsittelyn

[243] ks. Giannini - Tas 2024.Tällaisten käyttötapausten voidaan olettaa luokiteltavan korkean riskin järjestelmiksi, vaikka tätä ei suoraan artiklassa sanota. Tämä senkin vuoksi, että liitteessä III kaikki biometriset etätunnistusjärjestelmät luokitellaan korkean riskin järjestelmiksi.
[244] Komission tiedonanto C (2025) 5052 final, s. 118.
[245] Giannini - Tas 2024.

sääntelemiseksi lainvalvontaviranomaisten toimesta, vaan ne ovat saattaneet direktiivin 10 artiklan osaksi lainsäädäntöä.[246] Euroopan tietosuojaneuvosto on todennut, että yksinomaan täytäntöönpanoa ei voida käyttää oikeusperustana biometrisen datan käsittelylle, koska se ei täytä tarkkuuden eikä ennakoitavuuden vaatimuksia. Kansallisessa lainsäädännössä tulisi täten olla nimenomainen säännös, joka tarjoaa tällaisen oikeusperustan. Sen puuttuessa tietojen käsittely reaaliaikaisissa biometrisissä etätunnistusjärjestelmissä ei ole sallittua.[247]

Asetuksen reaaliaikaisia biometrisiä etätunnistusjärjestelmiä koskeva sääntely on erityissääntö (*lex specialis*) suhteessa rikosasioiden tietosuojadirektiivin artiklaan 10.[248] Reaaliaikaisten biometristen etätunnistusjärjestelmien käytön yhteydessä tehtävä biometrisen datan käsittely voi olla siten sallittua tekoälyasetuksen mukaan, vaikka sitä ei olisi sallittu tai säännelty kansallisessa lainsäädännössä. Tämän seurauksena tekoälyasetus voi käytännössä kiertää rajoituksia, jotka johtuvat siitä, että rikosasioiden tietosuojadirektiiviä ei ole pantu kunnolla täytäntöön kansallisella tasolla.[249]

Tilannetta voidaan korjata kansallisella lainsäädännöllä. Asetuksen 5(5) artikla antaa jäsenvaltioille mahdollisuuden säätää lailla, sallitaanko reaaliaikaisten biometristen etätunnistusjärjestelmien käyttö lainvalvonnassa kokonaan, osittain vai rajoitetaanko sitä vielä lisää. *Giannini* ja *Tas* argumentoivat, että samalla tällainen kansallinen laki loisi myös tarvittavan oikeusperustan biometrisen datan käsittelylle.[250]

Näistä säännöksistä muodostuva oikeudellinen kehys on melko monimutkainen. Vaikka tekoälyasetus on periaatteessa suoraan sovellettavaa oikeutta, jäsenvaltiot voivat *Gianninin* ja *Tasin* tulkinnan mukaan hyödyntää artiklan 5(1)(h) mukaisia poikkeuksia käytännössä vain, jos ne säätävät asiasta erikseen kansallisessa laissa.[251]

Tekoälyasetuksen voimaantulosta huolimatta Unkarissa hyväksyttiin vuonna 2025 lakimuutos, joka mahdollistaa aiempaa laajemman kasvojentunnistusjärjestelmien käytön, erityisesti rauhanomaisissa kokoontumisissa, kuten Budapest Priden yhteydessä. Muutoksen myötä kasvojentunnistusteknologiaa voidaan käyttää kaikenlaisissa rikkomusmenettelyissä, ei vain vakavien rikosten yhteydessä. Unkarissa käytössä olevan kasvojentunnistusjärjestelmä täyttää tekoälyasetuksen reaaliaikaiselle järjestelmälle asetetut kriteerit, mutta ei kiellon poikkeusten asettamia edellytyksiä. Muun muassa *EDRi* on katsonut, että tämä laajennettu

[246]Giannini - Tas 2024.
[247] EDPB Guidelines 05/2022, s. 3.
[248] Tekoälyasetuksen johdanto-osan 38 perustelukappale.
[249] Giannini - Tas 2024.
[250] Giannini - Tas 2024.
[251] Giannini - Tas 2024.

kasvojentunnistusjärjestelmän soveltaminen kiellettyihin Pride-tapahtumiin osallistuvien ja jopa vähäisiin rikkomuksiin syyllistyneiden henkilöiden seurantaan ja tunnistamiseen rikkoo tekoälyasetusta ja EU:n perusoikeuskirjaa.[252] Voidaankin todeta, että tekoälyasetus ei näytä täyttävän kaikkia niitä sääntelyaukkoja, joita tietosuojasäännökset ovat jättäneet biometrisen tunnistamisen osalta.

#### *5.4.1.6 Kohteena oleva henkilö ja suojatoimet*

Tekoälyasetuksen 5 artiklan 2 kohta koskee reaaliaikaisten biometrisen etätunnistusjärjestelmien käyttöönoton arviointia. Kohdassa mainitut edellytykset on otettava huomioon, jos jokin h alakohdan poikkeuksista tulee sovellettavaksi. Kyseissä artiklassa mainitaan joitakin huomioon otettavia tekijöitä, kuten tilanteen luonne, aiheutuvan vahingon vakavuus sekä vaikutukset asianomaisten henkilöiden oikeuksiin ja vapauksiin. Vaikka voidaan olettaa, että vastuu arvioinnista kuuluu lainvalvontaviranomaisille, artiklassa ei määritellä, kuka nämä tekijät arvioi, miten arviointi tehdään tai milloin arviointi tulisi suorittaa. Lainvalvontaviranomainen voi tarkoittaa eri toimijoita, kuten poliisia, syyttäjiä tai jopa yksityisiä tahoja, joille on annettu lainvalvontatehtäviä.[253]

Asetuksen 5 artiklan 2 kohdassa todetaan, että reaaliaikaisia biometrisia etätunnistusjärjestelmiä saa käyttää ainoastaan erityisesti kohteena olevan henkilön henkilöllisyyden vahvistamiseen. Tällä edellytyksellä on pyritty tasapainottamaan tilanteen vakavuus ja järjestelmän käyttämättä jättämisestä aiheutuva haitta sekä toisaalta teknologian vaikutukset yksilön oikeuksiin ja vapauksiin. Kohdentamalla reaaliaikaisen biometrisen etätunnistusjärjestelmän käyttö tiettyyn henkilöön pyritään välttämään joukkovalvontaa.[254]

Joissakin tilanteissa tällaisen henkilön määrittely voi olla helppoa. Esimerkiksi tilanteessa, jossa etsitään tiettyjen rikosten uhria, kuten ihmiskaupan uhria, kohdehenkilön henkilöllisyys on yleensä selkeä. Sen sijaan tilanteessa, jossa pyritään estämään uhka ihmisten hengelle tai fyysiselle turvallisuudelle, kuten terrori-isku, kohdehenkilön määrittely voi olla huomattavasti epävarmempaa. Esimerkiksi niin sanotussa ”tikittävä pommi” -skenaariossa voi olla vaikeaa yksilöidä tarkasti, kuka on se henkilö, johon toimenpiteet tulisi kohdistaa. Tämän vuoksi reaaliaikaisia biometrisiä etätunnistusjärjestelmiä saatetaan käyttää sellaisten henkilöiden tunnistamiseen, jotka eivät ole virallisesti rikostutkinnan kohteena, vaan ainoastaan yleisimmin

[252] ks. European Center for Not-for-Profit Law: Hungary’s new biometric surveillance laws violate the AI Act, 28.4.2025.
[253] Giannini - Tas 2024.
[254] Komission tiedonanto C (2025) 5052 final, s. 126.

tutkinnan piirissä.[255] Komission tiedonannon mukaan biometrisiä etätunnistusjärjestelmiä voidaan käyttää terroristijärjestöön kuuluvan rikoksentekijän tunnistamiseen, jos viranomaisilla on tosiasioihin perustuvaa näyttöä ja tietoja terroristijärjestön suunnitelmasta, iskun ajasta ja paikasta, mutta ei tietoa suunnitelman toteuttajasta. Tällöin lainvalvontaviranomaisten on tullut ennalta koota viitetietokannan, joka sisältää kyseisen järjestön jäsenten biometriset tiedot.[256]

Toiseksi asetuksen 5 artiklan 2 kohdan mukaan ennen järjestelmän käyttöä olisi arvioitava sen tarpeellisuus ja vaikutukset. Tällöin on punnittava mahdollisen käytön aiheuttaman tilanteen luonnetta ja verrattava erityisesti sen haitan vakavuutta, todennäköisyyttä ja laajuutta, joka luonnollisille henkilöille, yhteiskunnalle ja lainvalvontatarkoituksille aiheutuisi, jos järjestelmää ei käytettäisi, järjestelmän käytöstä aiheutuviin seurauksiin asianomaisten henkilöiden oikeuksille ja vapauksille ja erityisesti seurausten vakavuuteen, todennäköisyyteen ja laajuuteen. Vahingon ja seurausten vakavuuden, laajuuden ja todennäköisyyden arviointi tulee sisällyttää lainvalvontaviranomaisten tekemään perusoikeusvaikutusten arviointiin. Arviointi tulee tehdä tapauskohtaisesti.[257]

Tässä yhteydessä tulisi myös selvittää, olisiko käytettävissä vähemmän yksityisyyteen puuttuvia vaihtoehtoja. Esimerkiksi lainvalvontaviranomaiset eivät saa käyttää reaaliaikaisia kasvojentunnistusjärjestelmiä kaduilla yleisen turvallisuuden, rikosten ehkäisyn tai ruuhkautumisen perusteella, koska tämä edellyttäisi kaikkien henkilöiden jatkuvaa ja ajallisesti rajoittamatonta valvontaa. Tällainen käyttö ei täyttäisi asetuksen 5 artiklan 1 kohdan ensimmäisen alakohdan h alakohdan mukaisen kiellon poikkeusten edellytyksiä.[258]

Kolmanneksi kyseisen artiklan mukaan biometrisen etätunnistusjärjestelmän reaaliaikaisen käytön olisi oltava selvästi rajattua sen maantieteellisen laajuuden, keston ja kohteena olevan henkilön osalta. Näin pyritään varmistamaan, että järjestelmää käytetään vain, kun se on ehdottaman välttämätöntä. Biometrisen tunnistamisen osalta maantieteellisen rajoituksen on koskettava selkeästi rajattua aluetta, jossa on viitteitä tapahtuman toteutumisesta. Alue ei normaalisti saisi muodostua koko kaupungista tai valtiosta, vaan sen tulisi olla tarkemmin kohdennettu.[259]

Toinen suojatoimi liittyy asianomaisten henkilöiden ryhmien määrittelyyn. Tämä sulkee pois kohdentamattoman ja umpimähkäisen tunnistuksen tapauksissa, joissa ei ole viitteitä vaaratilanteista. Lisäksi käytön kesto on rajattava ehdottoman välttämättömään aikaan, vaikka sitä

[255] Giannini - Tas 2024.
[256] Komission tiedonanto C (2025) 5052 final, s. 126.
[257] Komission tiedonanto C (2025) 5052 final, s. 127.
[258] Komission tiedonanto C (2025) 5052 final, s. 127.
[259] Komission tiedonanto C (2025) 5052 final, s. 127–128.

voidaan tarvittaessa pidentää sovellettavien sääntöjen mukaisesti. Reaaliaikaisia biometrisiä etätunnistusjärjestelmiä ei saa käyttää toistaiseksi tai epämääräisen ajan. Ajanjakson on perustuttava konkreettisien viitteiden perusteella, jotka oikeuttavat järjestelmän käytön.[260]

*5.4.1.7 Ennakkolupa*

Tekoälyasetuksen 5 artiklan 3 alakohdan mukaan lainvalvonnan reaaliaikaisten biometrisen tunnistamisen järjestelmien käyttö edellyttää etukäteistä lupaa, jonka myöntää joko oikeusviranomainen tai riippumaton hallintoviranomainen kyseisessä jäsenvaltiossa. Poikkeuksena on perusteltu kiireellinen tilanne, jossa järjestelmän käyttö voidaan aloittaa ilman ennakkolupaa. Tässä tapauksessa lupa on pyydettävä ilman aiheetonta viivästystä ja viimeistään 24 tunnin kuluessa. Mikäli lupa evätään, käyttö on lopetettava välittömästi ja käyttöön liittyvät tulokset ja tuotokset on välittömästi poistettava.[261]

Voi olla vaikeaa varmistua siitä, että jäsenvaltiot eivät ota liikaa vapauksia, erityisesti tilanteissa, joissa biometrisen etätunnistusjärjestelmän ennakkolupamenettely voidaan ohittaa. Tällöin on olemassa riski siitä, että sääntelyn sallimia poikkeuksia tulkitaan laajasti ja järjestelmää aletaan käyttää ihmisten valvontaan laajemmin kuin tekoälyasetuksessa on tarkoitettu.[262]

Valvontajärjestelmä sisältää myös kaksi merkittävää elementtiä. Valvontaviranomaiset voivat myöntää lainvalvontaviranomaisille luvan käyttää reaaliaikaista biometristä etätunnistusjärjestelmää vain, jos ne katsovat sen olevan ”välttämätöntä ja oikeasuhteista” jonkin edellä mainitun h alakohdan tavoitteen saavuttamiseksi joko ”niiden käytettävissä olevan objektiivisen näytön tai selkeiden seikkojen perusteella”. Tämän voidaan katsoa olevan ainakin jossakin määrin ristiriidassa h alakohdan välttämättömyys- ja suhteellisuusvaatimuksen kanssa, jonka mukaan tällaisten järjestelmien käyttö sallitaan vain, jos se ”ehdottoman välttämätöntä”.[263]

Lisäksi 5 artiklan 3 kohta sisältää niin sanotun ohjaavan arviointivelvoitteen. Asetuksen mukaan toimivaltaisen viranomaisen on pyyntöä koskevaa päätöstä tehdessään otettava huomioon 2 kohdassa tarkoitetut seikat. Tästä seuraa, että valvontaviranomaisen on otettava huomioon myös se, mitä seurauksia luvan epäämisellä voi mahdollisesti olla lainvalvonnalle. Sen tulee siten arvioinnissa ottaa huomioon muun muassa mahdollisen käytön aiheuttaman tilanteen

[260] Komission tiedonanto C (2025) 5052 final, s. 127–128.
[261] Tekoälyasetuksen 5 artiklan 3 alakohta.
[262] Lindroos-Hovinheimo ym. 2025, s. 156.
[263] ks. Nóra Ni Loideain verkkoartikkeli ’A Trustworthy Framework that Respects Fundamental Rights? The Draft EU AI Act and Police Use of Biometrics, 4.8.2021. Kirjoittaja käsittelee artikkelissaan vuonna 2021 julkaistua luennosta tekoälyasetuksesta. Artikkelissa viitatut luonnoksen kohdat vastaavat hyväksyttyä asetusta.

luonne sekä erityisesti vahingon vakavuus, todennäköisyys ja laajuus siinä tapauksessa, että järjestelmää ei käytetä.[264]

Tohtori *Nóra Ni Loideain* on katsonut valvontajärjestelmän olevan linjassa EU:n perusoikeusvelvoitteiden, Euroopan unionin tuomioistuimen viimeaikaisen oikeuskäytännön ja yksityiselämän suojaa sekä salaista valvontaa koskevan Euroopan ihmisoikeussopimuksen 8 artiklan oikeuskäytännön kanssa.[265]

#### *5.4.1.8 Ilmoitusvelvollisuus ja raportointimenettely*

Reaaliaikaisen biometristen etätunnistusjärjestelmien kiellosta poikettaessa tällaisen järjestelmän jokaisesta käytöstä julkisissa tiloissa lainvalvontatarkoituksiin on ilmoitettava asianomaiselle markkinavalvontaviranomaiselle ja kansalliselle tietosuojaviranomaiselle. Tällä menettelyllä varmistetaan, että asianomaiset viranomaiset voivat hoitaa tehtävänsä asetuksessa ja kansallisessa lainsäädännössä asetettujen vaatimusten mukaisesti.[266]

Kansallisten markkinavalvonta- ja tietosuojaviranomaisten on ilmoitettuaan reaaliaikaisten biometristen etätunnistusjärjestelmien käytöstä lainvalvonnassa toimitettava komissiolle vuosittain raportti tällaisesta käytöstä. Komissio laatii tätä varten yhtenäisen mallin, joka sisältää tiedot toimivaltaisten oikeus- tai hallintoviranomaisten tekemien lupapäätösten määrästä ja niiden lopputuloksista. Komissio puolestaan julkaisee jäsenvaltioiden toimittamiin, yhdistettyihin tietoihin perustuvat vuosiraportit. Raportit eivät saa sisältää arkaluonteisia operatiivisia tietoja lainvalvontatoimista.[267]

### 5.4.2 Suuririskiset järjestelmät

#### *5.4.2.1 Suuririskisten tekoälyjärjestelmien luokittelu tekoälyasetuksessa*

Suuren riskin ryhmään luokitellaan tekoälyjärjestelmät, jotka vaikuttavat kielteisesti turvallisuuteen tai perusoikeuksiin. Ne jaetaan kahteen alakategoriaan: 1) tekoälyjärjestelmät, joita käytetään EU:n tuoteturvallisuussääntelyn piiriin kuuluvissa tuotteissa, jotka on määritelty liitteessä I. Näitä ovat muun muassa lelut, autot ja lääkinnälliset laitteet. 2) tekoälyjärjestelmät, joita käytetään tietynlaisiin käyttötarkoituksiin. Liitteessä III on lueteltu 8 tällaista

[264] Nóra Ni Loideain verkkoartikkeli 2021.
[265] Nóra Ni Loideain verkkoartikkeli 2021.
[266] Lindroos-Hovinheimo 2025, s. 152.
[267] Tekoälyasetuksen 5 artiklan 6 ja 7 alakohta.

käyttöaluetta. Kyseisen liitteen ensimmäinen kohta käsittelee biometristen tietojen hyödyntämistä tietyissä tilanteissa.[268]

Suuririskisiksi tekoälyjärjestelmiksi luokitellaan tekoälyasetuksessa ihmisten biometrinen etätunnistaminen, tunteentunnistaminen ja biometriseen luokitteluun tarkoitetut järjestelmät. Lainvalvontaviranomaisten käyttämä jälkikäteinen biometrinen etätunnistaminen luokitellaan suuririskiseksi toiminnaksi. Sellaisia biometrisiä järjestelmiä, joiden ainoa tarkoitus on varmistaa, että luonnollisen henkilön henkilöllisyys jonkin palvelun käyttämiseksi, laitteen lukituksen poistamiseksi tai valvottuun tilaan pääsemiseksi, eivät ole suuririskisiä. Lisäksi suuririskisiksi tekoälyjärjestelmiksi ei katsota biometrisiä järjestelmiä, joita on tarkoitus käyttää yksinomaan kyberturvallisuutta ja henkilötietojen suojaamista koskeviin toimiin.[269]

Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu kiinnittivät asetuksen valmisteluvaiheessa huomiota siihen, että ehdotuksessa esitettiin kattava luettelo suuririskisistä tekoälyjärjestelmistä. Luettelo on sisällytetty myös hyväksyttyyn asetukseen. Luettelon vaarana on, että suuren riskin tilanteiden vetovoima on heikko, mikä voi heikentää riskiperusteisen lähestymistavan tehokkuutta, jonka keskeinen ajatus on riskien asteittainen arviointi ja suhteuttaminen. Ne painottavat myös, että liitteet tulisi päivittää säännöllisesti, jotta niiden soveltamisalan asianmukaisuudesta voidaan varmistua.[270]

Asetuksen 5 artiklan mukaisia kiellettyjä tekoälykäytäntöjä on tarkasteltava yhdessä 6 artiklan suuririskisiä järjestelmiä koskevan luokittelun kanssa, erityisesti asetuksen liitteessä III mainittujen järjestelmien osalta. Käytännössä tämä tarkoittaa, että korkean riskin järjestelmäksi luokiteltu tekoälyjärjestelmä voi tietyissä tilanteissa täyttää myös kielletyn käytännön tunnusmerkit, jos 5 artiklan edellytykset täyttyvät. Toisaalta monet järjestelmät, jotka kuuluvat 5 artiklan kiellon poikkeusten piiriin, luokitellaan suuririskisiksi. Esimerkiksi tunteiden tunnistusjärjestelmät, jotka eivät täytä asetuksen 5 artiklan 1 kohdan f alakohdan kiellon ehtoja, luokitellaan asetuksen 6 artiklan ja III liitteen mukaan korkean riskin tekoälyjärjestelmiksi.[271]

Asetuksen 6 artiklan 3 alakohta sisältää poikkeukset suuririskisistä järjestelmistä. Poikkeusten tarkoituksena on sulkea suuririskisiä järjestelmiä koskevien velvoitteiden ulkopuolelle sellaiset järjestelmät, jotka eivät aiheuta merkittävää riskiä luonnollisten henkilöiden terveydelle, turvallisuudelle tai perusoikeuksille. Tämä merkitsee, että suuririskisiksi katsotaan vain liitteessä III luetellut järjestelmät, joihin liittyy merkittävä vahingon riski. Pelkkä vahingon mahdollisuus

[268] Keller 2025, s. 151–152.
[269] Tekoälyasetuksen johdanto-osan 54 perustelukappale.
[270] Euroopan tietosuojaneuvoston ja Euroopan tietosuojavaltuutetun yhteinen lausunto 5/2021, s. 10.
[271] Euroopan komission tiedonanto C (2025) 5052 final, s. 13.

ei siis riitä, vaan riskin on oltava olennaista tasoa. Asetus ei kuitenkaan täsmennä, mitä ”merkittävällä” riskillä tarkoitetaan. Pelkkä riski määritellään 3 artiklassa haitan todennäköisyyden ja vakavuuden yhdistelmäksi.[272]

Suuririskisten järjestelmien määrittely on poikkeuksellinen. Ensinnäkin perusoikeuksiin kohdistuva riski näyttäytyy ikään kuin kaksijakoisena: joko tällainen riski on tai sitä ei ole. Riskin suuruutta ei pyritä arvioimaan erikseen korkean riskin luokittelusta riippumatta. Toiseksi liitteeseen III sisällytettyjen tekoälyjärjestelmien valintaperusteita ei ole perusteltu tarkemmin.[273]

Tekoälyasetuksen riskiperusteisesta lähestymistavasta johtuu, että suuririskisille tekoälyjärjestelmille on asetettu eniten vaatimuksia ja velvoitteita. Valtaosa velvoitteista kohdistuu tarjoajiin eli järjestelmien kehittäjiin. Niille on asetettu sisällöllisiä vaatimuksia artikloissa 8–15, toimijoihin, kuten tarjoajiin ja käyttöönottajiin kohdistuvia velvoitteita artikloissa 16–27 sekä käytännesääntöjä ja standardeja näiden velvoitteiden täyttämisessä artikloissa 40–49.[274]

#### *5.4.2.2 Suuririskisten tekoälyjärjestelmille asetetuista vaatimuksista*

Tekoälyasetuksen 8 artiklan mukaan suuririskisten tekoälyjärjestelmien tulee täyttää kaikki kyseisessä jaksossa asetetut velvoitteet. Arvioinnissa on otettava huomioon sekä järjestelmän suunniteltu käyttötarkoitus että tekoälyteknologian yleisesti tunnistettu viimeisin kehitys. Lisäksi riskienhallintajärjestelmä on otettava huomioon vaatimustenmukaisuuden arvioinnissa.

Suuririskiselle tekoälyjärjestelmälle tulee perustaa riskienhallintajärjestelmä, joka kattaa sekä riskien tunnistamisen ja arvioinnin että toimenpiteet niiden lieventämiseksi. Säännökseen sisältyy myös testaamista koskevia vaatimuksia.[275] Asetuksessa ei anneta yksityiskohtaista ohjeistusta riskienhallinnan toteuttamisesta. Riskienhallinnan tarkoituksena on suojata tekoälyjärjestelmän käyttäjiä sekä niitä henkilöitä, joihin järjestelmien vaikutukset kohdistuvat. Tästä huolimatta riskienhallintajärjestelmä on luonteeltaan ennen kaikkea organisatorinen kokonaisuus.[276] Riskienhallinta kohdistuu ennen kaikkea tunnettuihin ja ennakoitavissa oleviin riskeihin, joita voidaan kohtuudella lieventää ja poistaa teknisellä suunnittelulla tai asianmukaisella dokumentaatiolla. Lisäksi mahdolliseen väärinkäyttöön liittyvät riskit on otettava

[272] Lindroos-Hovinheimo ym. 2025, s. 181.
[273] Kusche 2024, s. 8.
[274] Lindroos-Hovinheimo ym. 2025, s. 190.
[275] Tekoälyasetuksen 9 artikla.
[276] Lindroos-Hovinheimo ym. 2025, s. 194.

huomioon siten, että tarkastellaan asetuksen vaatimusten keskinäisiä ja yhteisvaikutuksia. Tavoitteena on riskien kokonaisvaltainen minimointi.[277]

Asetuksen 10 artiklassa säädetään seikkaperäisesti suuririskisen tekoälyjärjestelmän datasta ja datanhallinnasta. Vaatimukset kohdistuvat aikaan ennen järjestelmän markkinoille saattamista. Korkeanlaatuinen data nähdään edellytyksenä vastuulliselle tekoälykehitykselle ja oikeus yksityisyyteen ja henkilötietojen suojaan onkin taattava koko tekoälyjärjestelmän elinkaaren ajan.[278] Artiklassa poiketaan säännöstä, jonka mukaan tekoälyasetus ei vaikuta yleisen tietosuoja-asetuksen soveltamiseen ja yleinen tietosuoja-asetus on etusijalla suhteessa tekoälyasetukseen. Yleisessä tietosuoja-asetuksessa erityisten henkilötietoryhmien käsittely on kiellettyä, mutta tekoälyasetuksen perusteella erityisiä henkilötietoryhmiä voidaan käsitellä, jos se on ehdottoman välttämätöntä vinoutumien havaitsemiseksi tai korjaamiseksi. Sekä yleisessä tietosuoja-asetuksessa että tekoälyasetuksessa asetettujen suojatoimien tulee kuitenkin täyttyä.[279]

Tämä herättää kysymyksiä näiden kahden asetuksen välisestä suhteesta. Tekoälyasetuksen 10 artiklassa viitataan siihen, että tietosuoja-asetuksen 9 artikla väistyy osittain, mutta ei täsmennetä miltä osin. Yleisen tietosuoja-asetuksen 9 artiklan 4 kohdassa jätetään kansallista liikkumavaraa lisäehtoja ja rajoituksien säätämiselle liittyen geneettisten, biometristen ja terveystietojen käsittelyyn. Ei ole kuitenkaan täysin selvää, koskeeko tämä liikkumavara myös tekoälyasetuksen 10 artiklassa tarkoitettuja tilanteita. Mikäli näin olisi, kyse olisi poikkeuksesta tekoälyasetuksen yleiseen linjaan, jonka mukaan asetuksessa ei jätetä juurikaan kansallista liikkumavaraa.[280]

Artiklassa 14 edellytetään, että suuririskiset järjestelmät on toteutettava siten, että ne mahdollistavat tehokkaan ihmisvalvonnan sekä valvojan tosiasiallisen mahdollisuuden keskeyttää järjestelmän toiminta. *FRA:*n mukaan kenttätutkimuksen tulokset osoittavat vahvaa tukeutumista ihmisvalvontaan riskien lieventämiskeinona. Ihmisvalvonnan tehokkuus riippuu kuitenkin siitä, miten se on suunniteltu ja toteutettu sekä siitä, onko otettu huomioon niin sanottu automaatiovinouma eli taipumus luottaa tekoälyjärjestelmän tuottamiin tuloksiin. Ihmisvalvonnan ei tule olla ainoa keino varmistaa perusoikeuksien toteutuminen. Tämä korostuu erityisesti silloin, kun ymmärrys tekoälyjärjestelmien toiminnasta on rajallista tai kun sekä järjestelmiin että niitä valvoviin ihmisiin voi liittyä vinoumia muiden perusoikeusnäkökohtien lisäksi.[281]

---

[277] Tekoälyasetuksen 9 artiklan 3 ja 4 kohta.
[278] Tekoälyasetuksen johdanto-osan 69 perustelukappale.
[279] Tekoälyasetuksen 10 artiklan 5 kohta.
[280] Lindroos-Hovinheimo ym. 2025, s. 202–203.
[281] ks. FRA: Assessing High-risk Artificial Intelligence: Fundamental Rights Risks 2025, s. 12.

Reaaliaikaisten ja jälkikäteisten biometristen etätunnistusjärjestelmien välillä on eroja lupamenettelyssä. Jälkikäteisten biometristen etätunnistusjärjestelmien osalta asetus edellyttää, että lupaa haetaan ennen käyttöä tai viimeistään 48 tunnin kuluessa käytöstä. Myöhäinen lupahakemus ei edellytä erityistä kiiretilannetta. Lupaa ei tarvita, jos järjestelmää käytetään mahdollisen epäillyn tunnistamiseen.[282]

Lupamenettelyn lisäksi asetuksessa on asetettu muita yleisiä velvollisuuksia korkean riskin tekoälyjärjestelmien tarjoajille ja käyttäjille, kuten rekisteröityminen EU:n tietokantaan (artikla 71). Lainvalvontakäytössä rekisteröintiä on kuitenkin rajoitettu: vain pieni osa tiedoista tallennetaan tietokannan ei-julkiseen osaan ja täten vain komissio ja kansalliset valvontaviranomaiset pääsevät tietoihin käsiksi, mikä heikentää avoimuutta ja demokraattista valvontaa.[283]

Kuten todettu, suuririskisille tekoälyjärjestelmille on asetettu asetuksessa paljon vaatimuksia ja velvoitteita, jotka liittyvät riskinhallintajärjestelmän luomiseen, koulutus- ja testausdatan laatuun ja sen hallintaan sekä teknisen dokumentaation laatimiseen ja ylläpitämiseen. Lisäksi asetus sisältää vaatimuksia liittyen tietojen säilyttämiseen, avoimuuteen, ihmisvalvontaan sekä luotettavuuteen ja kyberturvallisuuteen. Suurin osa näistä tulee ottaa huomioon järjestelmiä suunniteltaessa ja kehitettäessä, jolloin oikeudelliset periaatteet ikään kuin sisällytetään digitaalisiin teknologioihin. Suunnitteluprosessiin kohdistuvat vaatimukset ovat riskiperusteisen lähestymistavan mukaisia, sillä näin voidaan jo suunnitteluvaiheessa ehkäistä järjestelmiin liittyviä riskejä.[284]

Tekoälyasetuksen vaikutusten arviointia vaikeuttaa se, että kyse on täysin uudesta sääntelystä, joka liittyy nopeasti kehittyvään teknologiaperheeseen, jonka sovellusalueet ovat vielä muotoutumassa. Asetukseen on kytketty lukuisia EU:n yhdenmukaistettuja tuoteturvasäädöksiä, joiden tuoteryhmiin sovelletaan tietyin ehdoin suuririskisten tekoälyjärjestelmien vaatimuksia. Tämä lisää entisestään vaikutusten arvioinnin vaikeutta ja epävarmuuksia. *Teknologiateollisuus ry:n* arvion mukaan kyseessä on kompleksinen asetus, jossa kaikki laadukkaan lainvalmistelun kriteerit, kuten tarkkarajaisuus, oikeasuhteisuus ja ennustettavuus, eivät kaikilta osin täyty.[285]

*Gianninin* ja *Tasin* mukaan asetuksen suojakeinot vaikuttavat riittämättömiltä, kun otetaan huomioon korkean riskin järjestelmien vaikutukset perusoikeuksiin. Lisäksi ne voivat saada aikaan sen, että ihmiset alkavat rajoittaa käyttäytymistään valvonnan pelossa.[286] Yli 200

[282] Tekoälyasetuksen 26 artiklan 10 kohta.
[283] Giannini – Tas 2024.
[284] Lindroos-Hovinheimo ym. 2025, s. 222.
[285] Teknologiateollisuus ry:n lausunto 2024, s. 3.
[286] Giannini – Tas 2024.

kansalaisjärjestöä Euroopassa ja maailmanlaajuisesti sekä Euroopan tietosuojavaltuutettu, Euroopan tietosuojaneuvosto, Euroopan parlamentti ja YK:n ihmisoikeusvaltuutettu ovat kaikki korostaneet, että biometrisen etätunnistuksen käyttö julkisissa tiloissa muodostaa vakavan ja hyväksymättömän uhan perusoikeuksille. Näihin oikeuksiin kuuluvat muun muassa oikeus yksityisyyteen, henkilötietojen suojaan, yhdenvertaisuuteen ja syrjimättömyyteen, sanan- ja tiedonvapauteen, kokoontumis- ja yhdistymisvapauteen sekä syyttömyysolettamaan. Lisäksi biometrisen etätunnistamisen käyttö voi heikentää demokraattisia periaatteita, kuten median vapautta ja oikeusvaltioperiaatetta.[287]

### 5.4.3 Sanktiojärjestelmä

Jotta asetus olisi tehokas, jäsenvaltioiden tulee säätää seuraamuksia asetuksen rikkomisesta tai noudattamatta jättämisestä.[288] *DigitalEuropen* mukaan rikkomusten seuraamuksia koskevien sääntöjen tulisi olla yhdenmukaisia vastaavien säädösten, kuten yleisen tietosuoja-asetuksen, mukaisten käytäntöjen kanssa ja niiden tulisi olla johdonmukaisia kaikissa jäsenvaltioissa. [289]

Tekoälyasetuksen eri säännösten noudattamatta jättämisestä aiheutuvat seuraamukset perustuvat rikkomusten vakavuuden mukaiseen porrastukseen. Vakavimpina pidetään 5 artiklassa säädettyjen kieltojen rikkomuksia, minkä vuoksi niistä määrättävät seuraamukset ovat ankarimpia. Kiellettyihin tekoälykäytäntöihin osallistuville tarjoajille ja käyttöönottajille voidaan määrätä enintään 35 000 000 euron hallinnollinen sakko tai yritysten osalta enintään 7 prosenttia edeltävän tilikauden maailmanlaajuisesta vuotuisesta liikevaihdosta sen mukaan, kumpi määristä on suurempi.[290]

On mahdollista, että sama kielletty toiminta rikkoo samanaikaisesti useita asetuksen säännöksiä. Tällöin on noudatettava *ne bis in idem* -periaatetta, jonka mukaan samasta teosta ei saa rangaista useaan kertaan. Seuraamuksia määrättäessä on otettava huomioon asetuksen 99 artiklan 7 kohdassa säädetyt seuraamuksen määräämistä koskevat perusteet.[291]

---

[287] ks. Joint civil society recommendations for an EU Artificial Intelligence Act for Fundamental Rights, Biometrics Part 1: Article 3(36) and Article 5(1)(d), s. 2.
[288] Tekoälyasetuksen 99 artikla.
[289] DIGITALEUROPE 2021, s. 8.
[290] Komission tiedonanto C (2025) 5052 final, s. 20.
[291] Komission tiedonanto C (2025) 5052 final, s. 20.

## 5.5 Tekoälyasetuksen vaikutukset biometrisen tunnistamisen sääntelyyn

Tekoälyasetus merkitsee merkittävää muutosta biometrisen tunnistamisen sääntelyyn Euroopan unionissa. Asetus luo ensimmäistä kertaa unionitasoisen, suoraan sovellettavan sääntelykehyksen, jossa biometrisiä tekoälyjärjestelmiä arvioidaan niiden aiheuttamien riskien perusteella. Tekoälyasetuksessa biometriseen tunnistamiseen liittyvät määritelmät ovat yksityiskohtaisempia kuin tietosuojasääntelyssä. Tekoälyasetus erottelee muun muassa biometrisen tunnistamisen, biometrisen etätunnistamisen, reaaliaikaisen ja jälkikäteisen tunnistamisen sekä tunteiden tunnistamisen toisistaan. Tarkemmat määritelmät voivat edesauttaa sääntelyn kohdentamista oikeasuhteisesti tunnistamisesta aiheutuviin riskeihin kussakin tapauksessa. Tarkempi määrittely voi mahdollisesti tehdä vaikeammaksi sääntelyn kiertämisen teknisillä tai käsitteellisillä ratkaisuilla. Toisaalta yksityiskohtaiset määritelmät voivat lisätä sääntelyn monimutkaisuutta ja tulkinnanvaraisuutta.

Keskeinen muutos on se, että osa biometrisistä tekoälyjärjestelmistä kielletään kokonaan. Erityisesti reaaliaikainen biometrinen etätunnistaminen julkisissa tiloissa lainvalvontatarkoituksiin on lähtökohtaisesti kielletty, samoin tietyt tunteidentunnistus- ja biometriset luokittelujärjestelmät. Lisäksi biometriset järjestelmät, joita ei kielletä, luokitellaan usein suuririskisiksi tekoälyjärjestelmiksi, jolloin niihin kohdistuu laajoja velvoitteita esimerkiksi riskienhallinnasta, datan laadusta, dokumentaatiosta, ihmisvalvonnasta ja perusoikeusvaikutusten arvioinnista. Asetus vahvistaa myös ennakkovalvontaa, sillä reaaliaikaisten biometrisen etätunnistusjärjestelmien käyttö edellyttää pääsääntöisesti oikeusviranomaisen tai riippumattoman hallintoviranomaisen ennakkolupaa. Lisäksi sääntelyä tukee huomattava sanktiojärjestelmä, jossa vakavimmista rikkomuksista voidaan määrätä erittäin suuria hallinnollisia sakkoja.

Positiivisena kehityksenä voidaan pitää erityisesti sitä, että biometrisen tunnistamisen perusoikeusriskejä tunnistetaan aiempaa selkeämmin. Sääntely perustuu riskiperusteiseen lähestymistapaan, jonka avulla pyritään kohdistamaan ankarimmat velvoitteet kaikkein ongelmallisimpiin käyttötapoihin. Myös perusoikeuksien, kuten yksityiselämän suojan ja henkilötietojen suojan, korostaminen muodostaa tärkeän osan asetuksen rakennetta. Lisäksi asetuksen velvoitteet, kuten riskienhallintajärjestelmät, ihmisvalvonta ja dokumentointivaatimukset, voivat parhaimmillaan lisätä teknologian läpinäkyvyyttä ja vastuullisuutta jo järjestelmien suunnitteluvaiheessa.

Sääntelyyn liittyy kuitenkin myös merkittäviä ongelmia ja epävarmuuksia. Keskeinen heikkous liittyy reaaliaikaisen biometrisen etätunnistamisen kiellon poikkeuksiin, jotka ovat laajoja ja

osittain tulkinnanvaraisia. Perusoikeuksien suojelun ja biometriseen tunnistamiseen liittyvien riskien näkökulmasta ehdottomat kiellot olisivat olleet perustellumpi ratkaisu. Samalla voidaan kysyä, voidaanko reaaliaikaista biometristä etätunnistamista ylipäätään pitää demokraattiseen yhteiskuntaan sopivana teknologiana, kun sen käyttö mahdollistaa laajamittaisen ja jatkuvan julkisten tilojen valvonnan sekä voi heikentää yksilöiden yksityisyyttä, anonymiteettiä, kokoontumisvapautta ja sananvapautta.

Poikkeukset voivat mahdollistaa teknologian käytön hyvin erilaisissa tilanteissa jäsenvaltioiden kansallisten ratkaisujen perusteella, mikä voi johtaa sääntelyn pirstaloitumiseen unionissa. Asetuksessa on asetettu mekanismeja oikeuksia kunnioittavan käytön varmistamiseksi, mutta jo poikkeusten luonteesta johtuu, että ne mahdollistavat ihmisten oikeuksia loukkaavan käytön. Asetettujen mekanismien riittävyys selvinnee vasta, kun asetus on ollut sovellettavana pidemmän aikaa. Lisäksi reaaliaikaisen ja jälkikäteisen biometrisen etätunnistamisen välinen erottelu on herättänyt kritiikkiä, sillä myös jälkikäteiset järjestelmät voivat mahdollistaa laajamittaisen seurannan ja aiheuttaa vakavia vaikutuksia perusoikeuksille. Näiden kahden järjestelmän välistä erottelua ei nähdäkseni voida pitää täysin onnistuneena.

Ongelmallista on myös se, että asetus ei kaikilta osin täsmennä, miten tekoälyasetuksen ja tietosuojasääntelyn välinen suhde käytännössä rakentuu. Erityisesti biometrisen datan käsittelyä koskevat poikkeukset voivat synnyttää epäselvyyksiä suhteessa yleiseen tietosuoja-asetukseen ja rikosasioiden tietosuojadirektiiviin. Lisäksi osa asetuksen velvoitteista jää melko yleisluonteisiksi, jolloin niiden tehokkuus riippuu pitkälti kansallisesta täytäntöönpanosta, viranomaisten tulkinnoista ja käytännön valvonnasta.

Kokonaisuutena tekoälyasetus vahvistaa biometrisen tunnistamisen sääntelyä huomattavasti aiempaan verrattuna ja tuo perusoikeusnäkökulman keskeiseksi osaksi tekoälyn sääntelyä. Samalla asetukseen jää kuitenkin useita avoimia tulkintakysymyksiä ja poikkeuksia, joiden vuoksi ei ole vielä selvää, kuinka tehokkaasti se pystyy rajoittamaan biometriseen massavalvontaan ja syrjiviin käytäntöihin liittyviä riskejä käytännössä. Asetuksen epäselvät määritelmät voivat tulevaisuudessa tulla Euroopan unionin tuomioistuimen arvioitaviksi esimerkiksi silloin, kun niitä koskevia tulkintakysymyksiä nousee esiin kansallisten tuomioistuinten tekemissä ennakkoratkaisupyynnöissä.

## 5.6 Tekoälyasetus ja perusoikeusvaikutusten arviointi

### 5.6.1 Perus- ja ihmisoikeuksien suojelu tekoälyasetuksessa

Tekoälyasetuksen tarkoituksena on vahvistaa perusoikeuskirjassa vahvistettujen perusoikeuksien suojaa tekoälyjärjestelmien haitallisilta vaikutuksilta. Asetusta tulee soveltaa perusoikeuskirjassa vahvistettujen unionin arvojen mukaisesti, mikä helpottaa muun muassa demokratian ja oikeusvaltion suojelua.[292]

Tekoälyasetuksen soveltaminen ei saa rajoittaa perusoikeuksien toteutumista. Perus- ja ihmisoikeuksien suojelu on asetuksen keskeinen lähtökohta. Tämä ilmenee muun muassa kiellettyjä järjestelmiä koskevassa sääntelyssä, jonka tarkoituksena on suojata yksilöiden oikeuksia. Sama tavoite perustelee osaltaan myös suuririskisiä järjestelmiä koskevaa sääntelyä.[293]

Näitä arvoja pyritään suojelemaan myös tekoälyasetuksen mukaisella perusoikeusvaikutusten arvioinnilla.

### 5.6.2 Perusoikeusvaikutusten arviointi tekoälyasetuksen 27 artiklan mukaan

Tekoälyasetuksen 27 artiklaan sisältyy velvollisuus arvioida tekoälyjärjestelmien perusoikeusvaikutuksia. Velvollisuus koskee vain suuririskisiä tekoälyjärjestelmiä. Vaikutustenarviointi tulee suorittaa etukäteen, ja se sisältää useita osa-alueita. Näitä ovat muun muassa kuvaus käyttöönottajan prosesseista sekä siitä ajanjaksosta tai käyttötiheydestä, jolla kutakin korkean riskin tekoälyjärjestelmää on tarkoitus hyödyntää, sekä kuvaus niistä luonnollisten henkilöiden ja ryhmien luokista, joihin järjestelmän käyttö todennäköisesti vaikuttaa. Lisäksi arvioinnissa on tunnistettava erityiset haitalliset riskit, jotka voivat kohdistua näihin ryhmiin, sekä kuvattava toteutetut toimenpiteet, erityisesti siltä osin kuin ne ylittävät tavanomaiset riskienhallintatoimet.[294]

Säännös koskee lähtökohtaisesti vain julkisia toimijoita tai sellaisia toimijoita, joilla on yhteys julkisiin palveluihin. Tästä seuraa, että artiklan ulkopuolelle rajautuvat yksityiset toimijat, jotka eivät tarjoa julkisia palveluja. Rajauksesta johtuu, että suuri osa tekoälyjärjestelmistä on sellaisia, joiden käyttöönotossa ei ole ollut välttämätöntä arvioida perusoikeusvaikutuksia. Tämä ei silti tarkoita, että tekoälyjärjestelmien yhteydessä voitaisiin täysin sivuuttaa perusoikeussääntelyä, koska se tulee sovellettavaksi tekoälyasetuksen rinnalla.[295] Lisäksi artiklan ulkopuolelle

[292] Tekoälyasetuksen johdanto-osan 1–2 perustelukappaleet. Perusoikeuskirja on osa unionin primäärioikeutta ja tulisi täten sovellettavaksi, vaikka sitä ei erikseen asetuksessa mainittaisikaan.
[293]Lindroos-Hovinheimo ym. 2025, s. 283.
[294] Zaccaroni 2025, s. 197–198.
[295] Lindroos-Hovinheimo ym. 2025, s. 285.

rajatuilla toimijoilla on erillinen, mutta täydentävä velvollisuus arvioida perusoikeuksiin kohdistuvia riskejä osana suuririskisille tekoälyjärjestelmille edellytettyä kokonaisvaltaista riskienhallintaa tekoälyasetuksen 9 artiklan mukaisesti.[296] Rajaus vaikuttaa ongelmalliselta erityisesti siksi, että biometrisiä tunnistusjärjestelmiä voivat kehittää ja käyttää yksityiset toimijat. Käytännössä rajoituksesta johtuen merkittävä osa perusoikeusriskeistä jää siten varsinaisen perusoikeusvaikutuksien arvioinnin ulkopuolelle näissä tapauksissa.

Kun artiklan mukainen arviointi on suoritettu, käyttöönottajan tulee ilmoittaa markkinavalvontaviranomaiselle arvioinnin tuloksista ja toimitettava artiklassa tarkoitettu lomake.[297] Artiklan mukainen valvottavan ja valvojan välinen suhde voi muodostua erikoiseksi, sillä arviointia tekevät tavanomaisesti viranomaiset ja muut julkisoikeudelliset toimijat, kun taas arviointia valvovat markkinointiviranomaiset. Seurauksena voi olla erilaisia valvonnan päällekkäisyyksiä.[298]

Tekoälyasetus tunnistaa myös sen, ettei luotettavuus tarkoita samaa asiaa kuin matala riski. Sen 67 artiklan mukaan korkean riskin tekoälyjärjestelmä voi täyttää asetuksen vaatimukset ja silti aiheuttaa riskejä terveydelle, turvallisuudelle, perusoikeuksille tai muille yleisen edun kannalta keskeisille arvoille. Näin sääntelyyn syntyy sisäinen jännite: vaikka tavoitteena on ehkäistä perusoikeuksiin kohdistuvia haittoja, asetuksessa samalla myönnetään, ettei tätä tavoitetta voida täysin taata.[299] Tämä ilmentää riskiperusteisen sääntelymallin ongelmaa: järjestelmä voi täyttää kaikki asetuksessa asetetut tekniset ja hallinnolliset vaatimukset, mutta se voi silti aiheuttaa merkittäviä haittoja perusoikeuksille. Sääntelyssä keskitystään enemmin riskien hallintaan kuin niiden poistamiseen.

Käytännössä riskien arviointi jää pitkälti jäsenvaltioiden markkinavalvontaviranomaisten vastuulle. Tehtävä on kuitenkin vaativa, sillä arviointi perustuu suurelta osin palveluntarjoajien toimittamiin tietoihin, eikä viranomaisilla välttämättä ole riittäviä keinoja tehdä täysin itsenäistä arviota riskeistä.[300]

Artiklassa on joitakin puutteita, jotka heikentävät sen tehokkuutta. Arvioinnin sisältö jää perusoikeusnäkökulmasta puutteelliseksi. Edellytyksenä ei ole esimerkiksi niiden perusoikeuksien yksilöiminen, joita järjestelmän käyttöönotto rajoittaisi taikka minkäänlaista perusoikeuspunnintaa. Lisäksi luettelosta puuttuu vaatimus arvioida perusoikeuksien rajoitusedellytyksiä.[301] Perusoikeuksien punnintaa pidetään keskeisenä eurooppalaisessa perusoikeusjärjestelmässä.

[296] Lasek-Markey – Hogan 2025, s. 4.
[297] Tekoälyasetuksen 27 artiklan 3 kohta.
[298] Lindroos-Hovinheimo ym. 2025, s. 287.
[299] Kusche 2024, s. 10
[300] Kusche 2024, s. 10
[301] Lindroos-Hovinheimo ym. 2025, s. 287.

Koska asetuksessa ei edellytetä perusoikeuksien punnintaa, arviointi voi jäädä enemmänkin yleisluonteiseksi riskikartoitukseksi kuin oikeudelliseksi perusoikeusarvioinniksi.

Lisäksi epäselvyyttä voi liittyä 27 artiklan suhteeseen muuhun perusoikeussääntelyyn. Tekoälyasetuksen mukainen perusoikeusvaikutusten arviointi voi olla päällekkäinen tietosuojasääntelyssä edellytetyn tietosuojavaikutusten arvioinnin kanssa. Tämän vuoksi 27 artiklan 4 kohdassa säädetään, että jos velvoitteet on jo täytetty tietosuojavaikutusten arvioinnilla, riittää sen täydentäminen perusoikeusnäkökulmalla. Tämä toteutetaan yleisen tietosuoja-asetuksen 35 artiklan tai rikosasioiden tietosuojadirektiivin 27 artiklan mukaisesti.[302]

Kun otetaan huomioon tekoälyasetuksen yleinen tavoite suojella perusoikeuksia sekä se, kuinka paljon asetuksessa viitataan perusoikeuksiin, varsinaista perusoikeuksien suojaa koskevaa sääntelyä on kuitenkin verrattain vähän ja ne jäävät osittain yleisluonteisiksi. Voidaankin pohtia, rakentuuko tekoälyasetuksen perusoikeussuoja enemmänkin ennaltaehkäisevään hallinnolliseen sääntelyn kuin varsinaisten kieltojen varaan. Nähtäväksi jää, onko sääntely riittävä turvaamaan perusoikeuksien tehokkaan suojelun käytännössä.

[302] Lindroos-Hovinheimo ym. 2025, s. 289.

# 6 Johtopäätökset

Tekoälyasetus rakentuu osin perus- ja ihmisoikeuksien suojelulle. Biometrisen tunnistamisen sääntelyä ohjaa perusoikeuksien suojaa koskevat säädökset, kuten unionin perusoikeuskirja ja Euroopan ihmisoikeussopimus. Biometrisen tunnistamisen yhteydessä käsitellään erityisiä henkilötietoryhmiä, joihin biometriset tunnisteet kuuluvat. Näiden tietojen käsittelyä säännellään pääsääntöisesti yleisessä tietosuoja-asetuksessa ja rikosasioiden tietosuojadirektiivissä. Biometriikkaa on säännelty tekoälyasetuksessa tarkemmin kuin unionin tietosuojalainsäädännössä. Muun muassa määritelmät on määritelty hienojakoisemmin.

Voidaan nähdä myönteisenä kehityksenä, että unionissa on ryhdytty toimiin luotettavan ja perusoikeuksia kunnioittavan sääntelykehyksen luomiselle biometrisen tunnistamisen käytölle. Tekoälyasetuksessa sääntelyn keskeinen periaate on riskiperusteisuus. Perusoikeusvaikutusten arviointia edellytetään suuririskisten järjestelmien osalta. Lisäksi monissa säännöksissä on huomioitu perus- ja ihmisoikeudet, kuten oikeus yksityisyyteen. Tästä huolimatta tekoälyasetus sisältää merkittäviä puutteita.

Jokainen kielletty tekoälyjärjestelmä sisältää jo itsessään merkittäviä riskejä ihmisten oikeuksille. Lainvalvontaviranomaisten käyttämät biometriset etätunnistusjärjestelmät herättävät huolta reaaliaikaisen ja jälkikäteisen järjestelmien välisestä rajanvedosta. Lisäksi näiden järjestelmien käyttöä koskeva sääntely ei vastaa vakiintuneita EU:n perusoikeusvaatimuksia tai Euroopan unionin tuomioistuimen oikeuskäytäntöä. Tekoälyasetuksen tulkintaa monimutkaistavat tulkinnanvaraiset ilmaisut, kuten ”*merkittävä haitta*”. Näiden sisällön täsmentymistä joudutaan todennäköisesti odottamaa Euroopan unionin tuomioistuimen oikeuskäytännön kautta.

Ylipäätään biometristen järjestelmien käyttöedellytykset ja perusoikeusvaikutusten arviointi ovat paikoin liian väljiä, ristiriitaisia ja epämääräisiä. Reaaliaikainen kasvojentunnistus julkisilla paikoilla, biometrinen luokittelu ja tunteidentunnistus ovat kiellettyjä vain osittain ja saattavat mahdollistaa biometrisen massavalvonnan ja tekoälyyn perustuvan syrjinnän. Ongelman ydin liittyy siihen, mitä kasvojentunnistus ja muu biometrinen tietojenkäsittely merkitsevät yhteiskunnallemme. Kyse on siitä, miten nämä teknologiat voivat vahvistaa olemassa olevia eriarvoisuuksia ja syrjiviä rakenteita sekä siitä, ovatko ne ylipäätään yhteensopivia demokratian, vapauden, yhdenvertaisuuden ja yksityisyyden kaltaisten perusarvojen kanssa.