

TEKOÄLYÄ JA ALGORITMIPERUSTEISTA SYRJINTÄÄ KOSKEVAT EUROOPPALAISET SUUNTAVIIVAT

yhdenvertaisuuselimille ja muille
kansallisille ihmisoikeustoimijoille



Yhteistyössä:

Interfederal Centre for Equal Opportunities (Unia), Belgia,
Yhdenvertaisuusvaltuutettu (YVV), Suomi, ja
Commission for Citizenship and Gender Equality (CIG), Portugali

Kris Shrishak
Soizic Pénicaud

Euroopan unionin
yhteisrahoittama



EUROOPAN UNIONI

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

Euroopan neuvoston
yhteisrahoittama ja toteuttama

**TEKOÄLYÄ JA
ALGORITMIPERUSTEISTA
SYRJINTÄÄ KOSKEVAT
EUROOPPALAISET
SUUNTAVIIVAT**
yhdenvertaisuuselimille
ja muille kansallisille
ihmisoikeustoimijoille

**Kris Shrishak
Soizic Pénicaud**

Tämä julkaisu on laadittu Euroopan unionin ja Euroopan neuvoston taloudellisella tuella. Sen sisällöstä vastaavat yksinomaan sen kirjoittajat. Tässä julkaisussa esitettyjen näkemysten ei voida missään tapauksessa katsoa edustavan Euroopan unionin tai Euroopan neuvoston virallista kantaa.

Otteiden (enintään 500 sanaa) jäljentäminen on sallittua kaupallisia tarkoituksia lukuun ottamatta, kunhan tekstin eheys säilyy, otetta ei käytetä asiayhteydestään irrotettuna, ote ei tarjoa epätäydellisiä tietoja eikä lukijaa muutoin johdeta harhaan tekstin luonteen, laajuuden tai sisällön suhteen. Lähdeteksti on aina mainittava seuraavasti: "© Euroopan neuvosto, julkaisuvuosi". Kaikki muut asiakirjan tai sen osan jäljentämistä/kääntämistä koskevat pyynnöt on osoitettava Euroopan neuvoston julkaisuista ja visuaalisesta ilmeestä vastaavalle osastolle (Publications and Visual Identity Division) (F-67075 Strasbourg Cedex tai publishing@coe.int).

Kaikki muu tätä asiakirjaa koskeva kirjeenvaihto on osoitettava Euroopan neuvoston osallisuuden ja syrjinnän torjunnan osaston vihapuhetta, viharikoksia ja tekoälyä käsittelevälle yksikölle: Hate Speech, Hate Crime and Artificial Intelligence Unit of the Council of Europe's Inclusion and Anti-Discrimination Programmes Division, Council of Europe, F-67075 Strasbourg Cedex, sähköposti: anti-discrimination@coe.int

Alkuperäinen englanninkielinen teksti on Euroopan neuvoston laatima. Tämä suomenkielinen käännös on julkaistu Euroopan neuvoston suostumuksella, mutta sen sisällöstä vastaavat yksin kääntäjät. Euroopan neuvoston julkaisujen ja visuaalisen ilmeen osaston toimitusyksikkö ei ole korjannut tämän suomenkielisen julkaisun typografisia tai kieliopillisia virheitä.

Kannen suunnittelu: Publications and Visual Identity Division (DPiV), Euroopan neuvosto
Englanninkielisen julkaisun taitto: Jouve, Paris
Suomenkielisen julkaisun taitto: Vida Design, Pori
Käännös: ALM Translations
Käännöksen oikeudellinen tarkastus: Waltter Roslin, 1001 Lakes
Kuvat: Shutterstock

Sisällys

LYHENTEET	7
KIITOKSET	9
TIIVISTELMÄ	10
JOHDANTO	12
Suuntaviivojen tausta	12
Suuntaviivojen tavoite	13
Menetelmä	14
Suuntaviivojen rakenne	15
OSA I	17
1. TEKÖÄLYASETUKSEN YLEINEN TAUSTA	18
2. KIELLOT	21
2.1. Kiellettyjen tekoälyyn liittyvien käytäntöjen johdanto	21
2.2. Tekoälyjärjestelmät, jotka manipuloivat, harhaanjohtavat tai hyödyntävät ihmisten haavoittuvuuksia	24
2.3. Sosiaalinen pisteytys	28
2.4. Rikokseen syyllistymisen riskinarviointi	32
2.5. Kasvokuvien harvointi kasvontunnistustietokantojen luomiseksi tai laajentamiseksi	34
2.6. Tunteentunnistus	36
2.7. Biometrinen luokittelu	38
2.8. Biometrinen etätunnistus	40
3. SUURIRISKISET TEKÖÄLYJÄRJESTELMÄT	46
3.1. Suuririskisten tekoälyjärjestelmien luokittelu	46
3.2. Suuririskisten käyttötapauksen luettelon muuttaminen	50
3.3. Riskinhallintajärjestelmän vaatimukset	53
3.4. Datanhallinnan vaatimukset	55
3.5. Perusoikeusvaikutusten arviointi (FRIA)	59
3.6. EU:n tietokanta liitteessä III luetelluista suuririskisistä tekoälyjärjestelmistä	63
4. TEKÖÄLYJÄRJESTELMIEN VAATIMUSTEN AVOIMUUS	70
4.1. Tausta ja merkittävyys	70
5. TÄYTÄNTÖÖNPANO	73
5.1. Perusoikeuksia suojelevien viranomaisten valtuudet	73
5.2. Oikeussuojakeinot	78
5.3. Yhteistyömekanismit	81
OSA II	87
6. DIREKTIIVIT YHDENVERTAISUUSELIMIÄ KOSKEVISTA NORMEISTA	88
6.1. Yleinen tausta	88
6.2. Toimivaltuuksien ja resursoinnin muutokset	89
6.3. Valtuuksien muutokset	93
7. TEMAATTISET PAINOPISTEET	101
7.1. Temaattinen painopiste: lainvalvonta ja muuttoliikkeen, turvapaikka-asoiden ja rajavalvonnan hallinta	101
7.2. Temaattinen painopiste: koulutus	106
7.3. Temaattinen painopiste: työllisyys	108
7.4. Temaattinen painopiste: sosiaaliturva- ja työnvälityspalvelut	110
LÄHDEVIITTEET	114

Lyhenteet

ADM	automaattinen päätöksenteko
AFAR	Algorithmic fairness for asylum seekers and refugees -tutkimushanke
AI	tekoäly
Tekoälyasetus	Euroopan parlamentin ja neuvoston asetus (EU) 2024/1689, annettu 13 päivänä kesäkuuta 2024, tekoälyä koskevista yhdenmukaistetuista säännöistä
AVMSD	audiovisuaalisia mediapalveluja koskeva direktiivi (2010/13/EU)
CCTV	kameravalvonta
EUT	Euroopan unionin tuomioistuin
CNIL	La Commission nationale de l'informatique et des libertés (Ranskan tietosuojaviranomainen)
Komissio	Euroopan komissio
Yleissopimus 108+	Euroopan neuvoston uudistettu yleissopimus nro 108 yksilöiden suojelusta henkilötietojen käsittelyssä
CSO:t	kansalaisjärjestöt
DMA	digimarkkinasäädös
DPA	tietosuojaviranomainen
DPIA	tietosuojaa koskeva vaikutustenarviointi
DSA	digipalvelusäädös
EB	yhdenvertaisuuselin
ECRI	Euroopan rasismien ja suvaitsemattomuuden vastainen komissio
ETA	Euroopan talousalue
Equinet	kansallisten yhdenvertaisuuselinten eurooppalainen verkosto
EU	Euroopan unioni
FARI	AI for the Common Good Institute -aloite
Puiteyleissopimus	tekoälyä ja ihmisoikeuksia, demokratiaa ja oikeusvaltioperiaatetta koskeva Euroopan neuvoston puiteyleissopimus (CETS nro. 225)
FRIA	perusoikeusvaikutusten arviointi

GDPR	yleinen tietosuoja-asetus (asetus (EU) 2016/679)
HUDERIA	menetelmä, jolla arvioidaan tekoälyjärjestelmistä aiheutuvia ihmisoikeuksiin, demokratiaan ja oikeusvaltioperiaatteeseen kohdistuvia riskejä ja vaikutuksia
LEA	lainvalvontaviranomainen
LED	direktiivi lainvalvontatarkoituksessa käsiteltyjen henkilötietojen suojasta
Lääkinnällisistä laitteista annettu asetus	Euroopan parlamentin ja neuvoston asetus (EU) 2017/745, annettu 5. päivänä huhtikuuta 2017, lääkitieteellisten laitteiden
MSA	markkinavalvontaviranomainen
NHRS	kansallinen/kansalliset ihmisoikeustoimija/-toimijat
OCR	optinen merkitunnistus
Unia	liittovaltion yhdenvertaisuuskeskus
PEReN	Le Pôle d'expertise de la régulation numérique (Digitaalisten alustojen sääntelyn asiantuntijakeskus)
RBI	biometrinen etätunnistusjärjestelmä
STEM	luonnontieteet, matematiikka, tekniikka ja teknologiat

Katso sanasto EU:n tekoälyasetuksen määritelmiä koskevasta [3 artiklasta](#)

Kiitokset

Tämä raportti laadittiin hankkeen ”Upholding equality and non-discrimination by Equality bodies regarding the use of artificial intelligence in public administrations” yhteydessä. Hankkeen rahoittajina toimivat Euroopan unioni teknisen tuen välineen kautta sekä Euroopan neuvosto. Hankkeen toteuttamisesta vastaa Euroopan neuvosto yhteistyössä Euroopan komission, Belgian yhdenvertaisuustyöhön erikoistuneen instituution (Interfederal Centre for Equal Opportunities, Unia), Suomen yhdenvertaisuusvaltuutetun (YVV) ja Portugalin kansalaisuuksien ja sukupuolten tasa-arvoa käsittelevän komission (Commission for Citizenship and Gender Equality, CIG) kanssa.

Raportin ovat laatineet Kris Shrishak (kansainvälinen konsultti, Euroopan neuvosto) ja Soizic Pénicaud (kansainvälinen konsultti, Euroopan neuvosto).

Euroopan neuvosto haluaa kiittää hankkeeseen osallistuneita instituutioita ja Euroopan komissiota jatkuvasta sitoutumisesta raportin laatimisprosessin ajan sekä erityisesti seuraavia henkilöitä: Nele Roekens ja Nadine Brauns (Belgian Interfederal Centre for Equal Opportunities, Unia); Tiina Valonen ja Ville Rantala (Suomen yhdenvertaisuusvaltuutettu, YVV); Carla Peixe, Ana Martinho Fernandes, Alexandra Andrade ja Susana Miguel (Portugalin Commission for Citizenship and Gender Equality, CIG) ja Massimiliano Santini (Euroopan komission uudistus- ja investointityöryhmän pääsihteeri) sekä Menno Ettema, Sara Haapalainen, Ayça Dibekoğlu ja Delfine Gaillard (Euroopan neuvoston syrjinnän ehkäisemistä käsittelevä osasto).

Erityiskiitokset kuuluvat Louise Hooperille (kansainvälinen konsultti, Euroopan neuvosto) hänen asiantuntijapanoksestaan ja luonnoksen vertaisarvioinnista sekä Milla Vidinalle (Equinet, kansallisten yhdenvertaisuuselinten eurooppalainen verkosto) hänen antamastaan rakentavasta palautteesta.

Raportissa hyödynnettiin myös haastatteluihin keväällä 2025 osallistuneiden yhdenvertaisuuselinten ja kansalaisjärjestöjen kansallisten asiantuntijoiden panosta. Heidän näkemyksensä rikastuttivat näiden suuntaviivojen analyttisiä ja toiminnallisia osia.



YHDENVERTAISUUSVALTUUTETTU
NON-DISCRIMINATION OMBUDSMAN



Tiivistelmä

Tekoälyä ja algoritmiperusteista syrjintää koskevissa eurooppalaisissa poliittisissa suuntaviivoissa esitetään, miten yhdenvertaisuuselimet ja tarvittaessa muut kansalliset ihmisoikeustoimijat voivat käyttää EU:n lainsäädäntökehyksen – erityisesti tekoälyä koskevista yhdenmukaistetuista säännöistä annetun asetuksen (EU) 2024/1689 (EU:n tekoälyasetus) – mukaisia valtuuksiaan perusoikeuksien turvaamiseksi ja syrjintäriskien torjumiseksi tekoälyn ja automaattisten päätöksentekojärjestelmien (ADM) käyttöönotossa erityisesti julkisella sektorilla. Näillä instituutioilla on ratkaisevan tärkeä rooli perusoikeuksien turvaamisessa ja syrjinnän riskien torjumisessa aikana, jolloin tällaisia järjestelmiä otetaan yhä enemmän käyttöön julkisella ja yksityisellä sektorilla.

Suuntaviivat on jaettu kahteen pääosaan. Ensimmäisessä osassa keskitytään EU:n tekoälyasetuksen keskeisiin säännöksiin, jotka ovat olennaisimpia yhdenvertaisuuselinten ja kansallisten ihmisoikeustoimijoiden kannalta, ja selitetään, miten niitä voidaan soveltaa käytännössä:

1. Kielletyt tekoälyjärjestelmät: Suuntaviivoissa selitetään 5 artiklassa kielletyt tekoälyyn liittyvät käytännöt, joiden katsotaan olevan ristiriidassa unionin arvojen ja perusoikeuksien, kuten oikeuden syrjimättömyyteen, kanssa. Kiellot koskevat muun muassa ja tietyin edellytyksin tekoälyjärjestelmiä, jotka manipuloivat, huijaavat, hyödyntävät haavoittuvuuksia, harjoittavat sosiaalista pisteytystä tai rikosriskien arviointia ja jotka haravoivat kuvia kasvontunnistustietokantojen luomiseksi tai laajentamiseksi, sekä järjestelmiä, joilla tunnistetaan tunteita, luokitellaan biometrisiä tietoja ja suoritetaan reaaliaikaista biometristä etätunnistusta.
2. Suuririskiset tekoälyjärjestelmät: Suuntaviivoissa selvitetään, miten tekoälyjärjestelmät, joita käytetään kriittisillä aloilla, kuten biometriikassa, lainvalvonassa, sosiaaliturvassa, työllisyydessä, koulutuksessa ja keskeisten palvelujen saatavuudessa, voidaan luokitella ”suuririskisiksi” järjestelmiksi, ja miten niihin voidaan näin ollen soveltaa tiukkoja riskinhallintaa, tietohallintoa, dokumentaatiota, ihmisen suorittamaa valvontaa ja perusoikeusvaikutusten arviointia koskevia vaatimuksia. Suuntaviivoissa esitetään, mitä yhdenvertaisuuselinten ja kansallisten ihmisoikeustoimijoiden tulisi ottaa huomioon, kun ne käsittelevät luokituspäätöksiä ja tarkastelevat näiden velvoitteiden noudattamista yhdenvertaisuuden ja syrjimättömyyden näkökulmasta.
3. Avoimuus ja tietokannat: Suuntaviivoissa kuvataan, miten uudet avoimuusvaatimukset ja EU-tason tietokannat – erityisesti EU:n tiettyjä suuririskisiä tekoälyjärjestelmiä koskeva tietokanta – voivat luoda valvontamahdollisuuksia. Rekisteröinti- ja kirjaamisvelvoitteet voivat auttaa yhdenvertaisuuselimiä ja kansallisia ihmisoikeustoimijoita tunnistamaan, missä tekoälyjärjestelmiä käytetään, niiden seurantaa ja tutkintaa varten sekä tukemaan henkilöitä, joihin nämä järjestelmät ovat saattaneet vaikuttaa.
4. Täytäntöönpano: Suuntaviivoissa tarkastellaan tekoälyasetuksen 77 artiklassa lueteltujen perusoikeuksia suojelevien elinten roolia, yksilöiden käytettävissä olevia oikeussuojakeinoja sekä yhdenvertaisuuselinten, tietosuojaviranomaisten, markkinavalvontaviranomaisten ja muiden valvontaviranomaisten ja toimijoiden

välillä olevia yhteistyömekanismeja ja -mahdollisuuksia. Suuntaviivoissa annetaan poliittisia suosituksia siitä, miten yhdenvertaisuuselimet ja kansalliset ihmisoikeustoimijat voivat käyttää kantelujen käsittelyyn, tutkimuksiin, oikeudenkäynteihin, neuvontaan ja tietoisuuden lisäämiseen liittyviä valtuuksiaan algoritmisen syrjinnän ehkäisemiseksi,

Ensimmäisessä osassa määritellään yhdenvertaisuuselinten ja kansallisten ihmisoikeustoimijoiden tehtävät ja vastuut sekä annetaan kohdennettuja toimintapoliittisia suosituksia siitä, miten nämä elimet voivat ehkäistä ja havaita algoritmista syrjintää ja reagoida siihen esimerkiksi edistämällä yhdenvertaisuutta, lisäämällä tietoisuutta, tukemalla valituksia, ryhtymällä oikeustoimiin ja tekemällä tiivistä yhteistyötä tekoälyn laajempaan valvontajärjestelmään kuuluvien kansallisten toimivaltaisten viranomaisten kanssa.

Suuntaviivojen toinen osa koostuu kahdesta pilarista. Ensimmäisenä analysoidaan EU:n uusia yhdenvertaisuuselinten normeja koskevia direktiivejä ("direktiivit yhdenvertaisuuselimistä koskevista normeista") ja selitetään, miten niiden toimivaltaa, riippumattomuutta, resursseja ja valtuuksia (mukaan lukien edistämistä, oikeus-suojan saatavuutta ja tiedonkeruuta koskevia valtuuksia) koskevia säännöksiä voidaan hyödyntää tekoäly- ja ADM-järjestelmiin liittyvien syrjintäriskien torjumiseksi. Toiseksi se tarjoaa temaattisia lähtökohtia tekoälyn käytölle aloilla, jotka usein kuuluvat yhdenvertaisuuselinten toimivallan piiriin: lainvalvonta, maahanmuutto, turvapaikka-asiat ja rajavalvonta, sosiaaliturva, työllisyys ja koulutus. Suuntaviivoissa yhdistetään konkreettiset tekoälyn käyttötapaukset tekoälyasetuksen sovellettaviin säännöksiin (kiellot, suuren riskin luokitukset, avoimuus- ja rekisteröintivaatimukset) kunkin alan osalta ja hahmotellaan, missä tapauksissa alakohtaiset suojatoimet sekä yhdenvertaisuuselinten ja kansallisten ihmisoikeustoimijoiden osallistuminen on olennaisen tärkeää.

Suuntaviivat on suunniteltu mukautettaviksi erilaisiin kansallisiin olosuhteisiin ja tukemaan yhdenvertaisuuselimistä ja kansallisia ihmisoikeustoimijoita poliittisten päättäjien ja valvontaviranomaisten neuvonnassa, Euroopan neuvoston standardien, kuten yleissopimuksen 108+ ja tekoälyä ja ihmisoikeuksia, demokratiaa ja oikeusvaltioperiaatetta koskevan Euroopan neuvoston puiteyleissopimuksen, noudattamisessa sekä sen varmistamisessa, että tekoäly- ja ADM-järjestelmiä kehitetään ja käytetään eurooppalaisen yhdenvertaisuus-, tasa-arvo- ja syrjimättömyyslainsäädännön mukaisesti.



Johdanto

Suuntaviivojen tausta

Julkishallinnot eri puolilla Eurooppaa käyttävät tekoälyjärjestelmiä ja/tai automaattista päätöksentekoa (ADM) hyödyntäviä järjestelmiä monilla eri toiminta-alueilla, kuten maahanmuuton, hyvinvoinnin, oikeuden, koulutuksen, työllisyyden, verotuksen, lainvalvonnan tai terveydenhuollon apuna. Tällaisia järjestelmiä käytetään myös yksityisen sektorin kriittisillä aloilla, kuten pankki- (esimerkiksi luottopisteytys) ja vakuutusala. Vaikka tekoäly- ja ADM-järjestelmiin liittyy merkittäviä syrjäntäriskejä, näiden riskien tunnistamisessa ja lieventämisessä on edelleen haasteita. Hiljattain julkaistussa raportissa ”Legal protection against algorithmic discrimination in Europe: Current frameworks and remaining gaps” (Xenidis 2025), joka on laadittu osana Euroopan unionin ja Euroopan neuvoston hanketta, nostetaan esiin kriittisiä ongelmia: syrjäntäriskeihin liittyvä tietoisuuden puute, avoimuuden ja merkityksellisen tiedon puute viranomaisten tekoäly-/ADM-järjestelmien käyttöä koskien, oikeussuojan käytettävyyden haasteet sekä standardoitujen hallintokäytäntöjen puute. Näin ollen yhdenvertaisuuselimillä (EB:t) ja muilla kansallisilla ihmisoikeustojärjestöillä (NHRs:t) on keskeinen rooli tekoäly- ja ADM-järjestelmien perusoikeuksien mukaisessa käyttöönotossa julkisen sektorin organisaatioissa.

Uusilla oikeudellisilla kehyksillä, kuten tekoälyä ja ihmisoikeuksia, demokratiaa ja oikeusvaltioperiaatetta koskevalla Euroopan neuvoston puiteyleissopimuksella¹ ja Euroopan unionin tekoälyasetuksella,² pyritään suojelemaan perusoikeuksia ja estämään tekoälyjärjestelmien harjoittamaa syrjintää. Lisäksi Euroopan unioni on antanut kaksi uutta direktiiviä, joilla otetaan käyttöön vähimmäisvaatimukset yhdenvertaisuuselinten aseman ja valmiuksien vahvistamiseksi Euroopassa (jäljempänä ”direktiivit yhdenvertaisuuselimistä koskevista normeista”).³ Näiden uusien säädösten asianmukainen täytäntöönpano on avainasemassa niiden tehokkuuden varmistamisessa.

Suuntaviivojen tavoite

Tätä taustaa vasten näillä suuntaviivoilla pyritään antamaan yhdenvertaisuuselimille ja muille kansallisille ihmisoikeustoimijoille, erityisesti Euroopan unionin sisäisille elimille, valmiudet puuttua tekoäly- ja ADM-järjestelmien harjoittamaan syrjintään

- ▶ tiedottamalla niille niiden tekoälyä koskevan sääntely-ympäristön luomista muuttuvista velvoitteista, mukaan lukien siitä, miten muutokset vaikuttavat suoraan tai välillisesti niiden toimivaltaan
- ▶ tarjoamalla niille erityisiä ohjeita, suosituksia ja esimerkkejä hyvistä käytännöistä uusien asetusten soveltamisen ja täytäntöönpanon valvomiseksi ja yhdistämällä ne olemassa oleviin säädöksiin
- ▶ toimimalla yhdenvertaisuuselinten ja kansallisten ihmisoikeustoimijoiden tukena, joka auttaa ja neuvoa kansallisia sidosryhmiä, kuten poliittisia päättäjiä ja valvontaviranomaisia, ihmisoikeuksiin, yhdenvertaisuuteen ja syrjimättömyyteen liittyvissä kysymyksissä.

Näissä suuntaviivoissa keskitytään erityisesti julkisen sektorin tekoäly- ja ADM-järjestelmiin.

1. Tekoälyä ja ihmisoikeuksia, demokratiaa ja oikeusvaltioperiaatetta koskeva Euroopan neuvoston puiteyleissopimus (Vilna, 5. syyskuuta 2024), jäljempänä ”Euroopan neuvoston puiteyleissopimus”.
2. Euroopan parlamentin ja neuvoston asetukset (EU) 2024/1689, annettu 13 päivänä kesäkuuta 2024, tekoälyä koskevista yhdenmukaistetuista säännöistä ja asetusten (EY) N:o 300/2008, (EU) N:o 167/2013, (EU) N:o 168/2013, (EU) 2018/858, (EU) 2018/1139 ja (EU) 2019/2144 sekä direktiivien 2014/90/EU, (EU) 2016/797 ja (EU) 2020/1828 muuttamisesta, jäljempänä ”tekoälyasetus”.
3. Neuvoston direktiivi (EU) 2024/1499, annettu 7 päivänä toukokuuta 2024, normeista tasa-arvoelimille, jotka toimivat asioissa, jotka koskevat henkilöiden rodusta tai etnisestä alkuperästä riippumatonta yhdenvertaista kohtelua, uskonnosta tai vakaumuksesta, vammaisuudesta, iästä tai seksuaalisesta suuntautumisesta riippumatonta yhdenvertaista kohtelua työssä ja ammatissa ja naisten ja miesten yhdenvertaista kohtelua sosiaaliturvaa koskevista asioissa ja tavaroiden ja palvelujen saatavuuden ja tarjonnan osalta sekä direktiivien 2000/43/EY ja 2004/113/EY muuttamisesta, ja Euroopan parlamentin ja neuvoston direktiivi (EU) 2024/1500, annettu 14 päivänä toukokuuta 2024, tasa-arvoelimiä koskevista normeista naisten ja miesten yhdenvertaiseen kohteluun ja yhtäläisiin mahdollisuuksiin työssä ja ammatissa liittyvissä asioissa sekä direktiivien 2006/54/EY ja 2010/41/EU muuttamisesta, jäljempänä ”direktiivit yhdenvertaisuuselimistä koskevista normeista”.

Menetelmä

Näissä suuntaviivoissa annetaan yleiskatsaus yhdenvertaisuuselinten ja kansallisten ihmisoikeustoimijoiden uusien säädösten mukaisiin uusiin tehtäviin, toimivaltuuksiin ja mahdollisuuksiin, sekä laajat suuntaviivat, joita voidaan mukauttaa kansallisten olosuhteiden mukaan.

Suuntaviivat perustuvat seuraaviin:

- ▶ asiakirjatutkimus ja oikeudellinen analyysi
- ▶ Euroopan unionin ja Euroopan neuvoston hankkeen yhteydessä laaditun raportin tulokset (Xenidis 2025)
- ▶ viisi kansalaisjärjestöjen ja yhdenvertaisuuselinten edustajien osittain jäseneltyä haastattelua, joissa haastateltavat valittiin aiheeseen liittyvän asiantuntemuksensa perusteella.

EU on hiljattain antanut muitakin digitaalisen hallintoon liittyviä asetuksia. Esimerkkinä verkkopalvelujen sääntelyyn keskittyvä digitaalisia palveluita koskeva säädöspaketti, joka koostuu digipalvelusäädöksestä⁴ (DSA) ja digimarkkinasäädöksestä⁵ (DMA). Näissä asetuksissa ja erityisesti digipalvelusäädöksessä käsitellään myös tarvetta suojella perusoikeuksia digitaali-alalla riskien tunnistamisen ja lieventämisen suhteen. Esimerkiksi sekä digipalvelusäädöksen 34 artikla, jossa käsitellään erittäin suurten verkkoalustojen ja erittäin suurten verkossa toimivien hakukoneiden tarjoajien suorittamaa riskinarviointia, että 35 artikla, jossa käsitellään näiden riskien vähentämistä, sisältävät syrjinnästä johtuvat riskit. Digipalvelusäädöksessä ja digimarkkinasäädöksessä ei kuitenkaan käsitellä tekoälyjärjestelmien käyttöä julkisella sektorilla. Koska näissä suuntaviivoissa keskitytään erityisesti julkisen sektorin tekoäly- ja ADM-järjestelmien käyttöön, ne eivät ole suorassa yhteydessä digipalvelusäädöksen tai digimarkkinasäädöksen.

4. Euroopan parlamentin ja neuvoston asetus (EU) 2022/2065, annettu 19 päivänä lokakuuta 2022, digitaalisten palvelujen sisämarkkinoista ja direktiivin 2000/31/EY muuttamisesta, jäljempänä "digipalvelusäädös".

5. Euroopan parlamentin ja neuvoston asetus (EU) 2022/1925, annettu 14 päivänä syyskuuta 2022, kilpailullisista ja oikeudenmukaisista markkinoista digitaali-alalla ja direktiivien (EU) 2019/1937 ja (EU) 2020/1828 muuttamisesta, jäljempänä "digimarkkinasäädös".

Suuntaviivojen rakenne

Suuntaviivojen ensimmäinen osa on jäsennelty niiden tekoälyasetuksen artiklojen ympärille, jotka ovat yhdenvertaisuuselinten ja muiden kansallisten ihmisoikeustoi-
mijoiden kannalta kriittisimpiä joko siksi, että ne vaikuttavat suoraan tai välillisesti
niiden toimivaltaan, tai siksi, että ne muodostavat merkittäviä muutoksia muille ins-
tituutioille, valvontaviranomaisille tai hallintorakenteille. Kullakin artiklalla on yhteys
voimassa oleviin tietosuoja-asetuksiin (Euroopan unionin yleinen tietosuoja-asetus⁶,
Euroopan unionin lainvalvontadirektiivi⁷ ja Euroopan neuvoston yleissopimus 108+
yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä) sekä
Euroopan neuvoston puiteyleissopimukseen.

Suuntaviivojen toisessa osassa esitetään yleiskatsaus direktiiveistä, jotka käsittävät
yhdenvertaisuuselimiä koskevia normeja. Nämä direktiivit ovat yhdenvertaisuuselinten
kannalta merkityksellisiä mitä tulee tekoälyjärjestelmien yhdenvertaisuuteen. Lisäksi
toisessa osassa käsitellään asiaa lainvalvonnan, maahanmuuton, turvapaikanhaun ja
rajavalvonnan, hyvinvoinnin ja sosiaaliturvan, työllisyyden sekä koulutuksen alojen
kannalta, missä tekoälyjärjestelmien käyttö aiheuttaa merkittäviä syrjintäriskejä.
Kunkin aihealueen yhteydessä mainitaan alan kannalta merkitykselliset tekoäly-
asetuksen artiklat.

-
6. Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta, jäljempänä ”yleinen tietosuoja-asetus” tai ”GDPR”.
 7. Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680, annettu 27 päivänä huhtikuuta 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 puitepäättöksen 2008/977/YOS kumoamisesta, jäljempänä ”direktiivi lainvalvontatarkoituksessa käsiteltyjen henkilötietojen suojasta” tai ”LED”.

OSA I



AI ACT

1. Tekoälyasetuksen yleinen tausta

Tekoälyasetuksen tarkoituksena on ”parantaa sisämarkkinoiden toimintaa vahvistamalla yhtenäinen oikeudellinen kehys erityisesti unionin arvojen mukaiselle tekoälyjärjestelmien kehittämiseksi, markkinoille saattamiselle, käyttöönotolle ja käytölle unionissa, edistää ihmiskeskeisen ja luotettavan tekoälyn käyttöönottoa varmistaen samalla Euroopan unionin perusoikeuskirjassa vahvistettu terveyden, turvallisuuden ja perusoikeuksien, mukaan lukien demokratia, oikeusvaltio ja ympäristönsuojelu, suojelun korkea taso”⁸

Tekoälyasetus astui voimaan 2. elokuuta 2024, ja sen eri vaatimuksia sovelletaan asteittain, kunnes ne pannaan täysimääräisesti täytäntöön vuonna 2030. Koska kyseessä on asetus, se on sovellettavissa sellaisenaan, eikä siitä tarvitse säätää kansallisella lainsäädännöllä. Monien vaiheiden, kuten kansallisen hallinto- ja valvontajärjestelmän perustamisesta, on kuitenkin päätettävä kansallisen täytäntöönpanolainsäädännön kautta. Tätä kirjoitettaessa tekoälyasetuksen täytäntöönpano on vasta alkuvaiheessa, ja sen suhteen tulee tehdä vielä paljon selvitystyötä.

8. Tekoälyasetus, johdanto-osan 1 kohta.

Vaikka tekoälyasetus tarjoaa yhdenvertaisuuselimille ja kansallisille ihmisoikeustoimijoille uusia mahdollisuuksia ehkäistä ja korjata syrjintää tekoälyjärjestelmissä, näitä suuntaviivoja lukiessa on syytä pitää mielessä useita sen ominaispiirteitä.

Ensiksi on syytä käsitellä tekoälyjärjestelmien määritelmää. Komissio antoi 6. helmikuuta 2025 suuntaviivat tekoälyasetuksen mukaisen tekoälyjärjestelmän tulkinnasta. Kuten useat kommentoijat ovat todenneet, nämä suuntaviivat eivät ole sitovia ja saattavat täten aiheuttaa sekaannuksia.⁹ Organisaatiot saattavat väittää, että jotkin julkisella sektorilla käytettävät ADM-järjestelmät¹⁰ jäävät tekoälyasetuksen soveltamisalan ulkopuolelle, vaikka niihin liittyykin syrjimättömyyteen kohdistuvia riskejä.¹¹ Tällaiset väitteet saattavat perustua määritelmän väärään tulkintaan. Tekoälyasetuksessa todetaan esimerkiksi, että tekoälyjärjestelmässä ”voi ilmetä mukautuvuutta”,¹² että ne ”on suunniteltu toimimaan käyttöönoton jälkeen vaihtelevilla autonomian tasoilla”¹³ ja että ”yksi tekoälyjärjestelmien keskeisistä piirteistä on niiden päättelykyky”.¹⁴ Yhdenvertaisuuselimiä ja kansallisia ihmisoikeustoimijoita kehoitetaan vahvasti käyttämään tekoälyjärjestelmien määritelmää, joka tulkitsee niiden olevan riippumattomia tietystä tekoälytekniikasta (kuten koneoppimisesta tai luonnollisen kielen käsittelystä) ja joka katsoo niiden itsenäisyyden ja mukautuvuuden valinnaisiksi ominaisuuksiksi.¹⁵

Toiseksi tutkimus ja kehittäminen eivät kuulu tekoälyasetuksen soveltamisalaan: ”Tätä asetusta ei sovelleta mihinkään tekoälyjärjestelmiä tai tekoälymalleja koskevaan tutkimus-, testaus- ja kehittämistoimintaan ennen niiden markkinoille saattamista tai käyttöönottoa”.¹⁶ Näin ollen jopa kiellettyjä tekoälyyn liittyviä käytäntöjä voidaan tutkia, testata ja kehittää, kunhan niitä ei saateta markkinoille tai oteta käyttöön. Kun tekoälyyn liittyvä käytäntö on saatettu markkinoille tai otettu käyttöön, se kuuluu kuitenkin tämän asetuksen soveltamisalaan. Pelkkä käyttöönoton lokeroiminen kokeiluksi tai tutkimukseksi ei kuitenkaan riitä tutkimus- ja kehittämispoikkeuksen soveltamiseen. Suuririskisten tekoälyjärjestelmien – ei kiellettyjen tekoälyyn liittyvien käytäntöjen – ”testaus todellisissa olosuhteissa”¹⁷ tekoälyn sääntelyn testiympäristöjen ulkopuolella voidaan tilapäisesti sallia, eikä tällaista testausta pidetä markkinoille saattamisena tai käyttöönottona, jos tietyt edellytykset täyttyvät.¹⁸ Näin ollen on

9. Kris Shrishak (2025), *EU's AI Act: Tread the Guidelines Lightly*, Tech Policy Press, saatavilla osoitteessa www.techpolicy.press/eu-ai-act-tread-the-guidelines-lightly/; Algorithm Audit (helmikuu 2025) 'Implementation of the AI Act: definition of an AI system', saatavilla osoitteessa https://algorithmaudit.eu/knowledge-platform/knowledge-base/guidelines_ai_act_implementation/.

10. Lighthouse Reports (2023), *France's Digital Inquisition*, saatavilla osoitteessa www.lighthousereports.com/investigation/frances-digital-inquisition/, viitattu 7. marraskuuta 2025.

11. Yksityiskohtainen analyysi aiheesta; ks. Xenidis 2025.

12. Tekoälyasetus, 3 artiklan 1 kohta.

13. Tekoälyasetus, 3 artiklan 1 kohta.

14. Tekoälyasetus, johdanto-osan 12 kohta.

15. Kris Shrishak (2025), *EU's AI Act: Tread the Guidelines Lightly*, Tech Policy Press, saatavilla osoitteessa www.techpolicy.press/eu-ai-act-tread-the-guidelines-lightly/; katso myös Algorithm Audit (2025), AI Act Implementation Tool, saatavilla osoitteessa <https://algorithmaudit.eu/technical-tools/implementation-tool/>.

16. Tekoälyasetus, 2 artiklan 8 kohta.

17. Tekoälyasetus, 3 artiklan 57 kohta.

18. Tekoälyasetus, 60 artiklassa määritetään kaikki ehdot, joiden on täyttyvä ennen testausta todellisissa olosuhteissa.

tärkeää, että yhdenvertaisuuselimet käsittelevät suuririskisten tekoälyjärjestelmien testausta jo olemassa olevan oikeudellisen työkalupakin pohjalta.

Kolmanneksi tekoälyasetusta sovelletaan ainoastaan järjestelmiin, jotka on saatettu markkinoille tai otettu käyttöön asetuksen yleisen soveltamispäivän jälkeen, ja se estää jo käytössä olevien tekoälyjärjestelmien ”merkittävän muutoksen”. Poikkeuksena ovat suuririskiset tekoälyjärjestelmät, jotka on tarkoitettu viranomaisten käyttöön ja joiden osalta toimijoiden tulee noudattaa tekoälyasetuksen vaatimuksia 2. elokuuta 2030 mennessä.¹⁹

Neljänneksi tekoälyasetuksen riskiperusteisessa lähestymistavassa määritetään erilaiset säännöt ja velvoitteet tekoälyjärjestelmien riskitasosta riippuen. Käytännössä jotkin käytännöt ovat kiellettyjä (katso [5 artikla](#)), joitakin tekoälyjärjestelmiä pidetään suuririskisinä ja niiden toimijoihin sovelletaan sen vuoksi uusia velvoitteita (katso [6 artikla](#)), ja avoimuusvaatimuksia sovelletaan tiettyihin tekoälyjärjestelmiin (katso [50 artikla](#)). Tämän soveltamisalan ulkopuolelle jääviin järjestelmiin ei sovelleta samoja vaatimuksia, jolloin on vaarana, että tekoälytoimijat voivat hyödyntää ”etiikkapesun” (Equinet 2025) ja ”riskien vähentämisen” (Xenidis 2025) käytäntöjä välttääkseen näiden vaatimusten soveltamisen. Tätä riskiperusteista lähestymistapaa olisi kuitenkin tarkasteltava tekoälytoimijoiden perusoikeuksien ja syrjinnänvastaisen lainsäädännön kunnioittamisvelvoitteen valossa.

19. Tekoälyasetus, johdanto-osan 177 kohta.



2. Kiellot

2.1. Kiellettyjen tekoälyyn liittyvien käytäntöjen johdanto

2.1.1. Tausta ja merkitys

Asetuksen 5 artiklassa luetellaan tekoälyasetuksen nojalla kielletyt tekoälyjärjestelmät, koska ”ne ovat ihmisarvon kunnioittamista, vapautta, *tasa-arvoa*, demokratiaa ja oikeusvaltiota koskevien unionin arvojen sekä perusoikeuskirjassa vahvistettujen perusoikeuksien vastaisia, *mukaan lukien oikeus syrjimättömyyteen*, tietosuoja ja yksityisyyden suoja sekä lapsen oikeudet”.²⁰ Sellaiset tekoälyyn liittyvät käytännöt, joita ei pidetä tekoälyasetuksen nojalla kiellettyinä, voivat olla sitä unionin muun lainsäädännön nojalla.²¹

Nämä kiellot ovat olleet voimassa 2. helmikuuta 2025 alkaen. Euroopan komissio julkaisi 6. helmikuuta 2025 suuntaviivat tällaisiin kiellettyihin käytäntöihin liittyen

20. Tekoälyasetus, johdanto-osan 28 kohta [korostus lisätty].

21. Tekoälyasetus, 5 artiklan 8 kohta.

tekoälyasetuksen 96 artiklan 1 kohdan b alakohdan mukaisesti.²² Vaikka suuntaviivoissa voidaan antaa ohjeita siitä, mitkä käytännöt olisi kiellettävä ja mitkä ei, suuntaviivoja on kritisoitu niiden epäselvyydestä.²³ Epäselvyyksien riskinä on se, että tekoälytoimijat hyödyntävät ”riskien vähentämisen strategioita” eli epäselvissä tapauksissa katsovat, että tiettyä käytäntöä ei ole kielletty. Lisäksi tällaiset suuntaviivat eivät ole sitovia, ja vasta oikeustapaukset mahdollistavat kieltojen selkeyttämisen.

Markkinaavalvontaviranomaiset raportoivat vuosittain Euroopan komissiolle (jäljempänä ”komissio”) kyseisenä vuonna esiintyneistä kielletyistä käytännöistä ja toteutetuista toimenpiteistä.²⁴ Komissio arvioi kerran vuodessa ”kiellettyjen tekoälyyn liittyvien käytäntöjen luettelon muutostarpeen”²⁵ ja toimittaa tulokset Euroopan parlamentille ja neuvostolle.²⁶

Euroopan komission yhteyteen perustetun tekoälytoimiston odotetaan kehittävän ”puolueettoman ja osallistavan menetelmän riskitason arvioimiseksi asiaankuuluviissa artikloissa esitettyjen perusteiden pohjalta ja uusien järjestelmien sisällyttämiseksi” 5 artiklaan.²⁷

Yhteys muihin asetuksiin

Euroopan neuvoston puiteyleissopimuksessa määrätään myös, että puiteyleissopimuksen sopimuspuoli voi asettaa lykkäyksen tai kiellon, ”jos se katsoo, että tällaiset käyttötavat ovat ristiriidassa ihmisoikeuksien kunnioittamisen, demokratian toiminnan tai oikeusvaltioperiaatteen kanssa”.²⁸

22. Euroopan komissio (2025), ”Komission suuntaviivat asetuksella (EU) 2024/1689 (tekoälysäädös) kielletyistä tekoälyyn liittyvistä käytännöistä”, saatavilla osoitteessa <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act>, viitattu 11. marraskuuta 2025. Jäljempänä ”tekoälyasetuksen kieltosuuntaviivat”.

23. Katso esim. Autoriteit Persoonsgegevens (2025), ”Summary and next steps call for input on prohibition on AI systems for emotion recognition in the areas of workplace or education institutions”, saatavilla osoitteessa www.autoriteitpersoonsgegevens.nl/en/documents/summary-and-next-steps-call-for-input-on-prohibition-on-ai-systems-for-emotion-recognition-in-the-areas-of-workplace-or-education-institutions (2025), viitattu 11. marraskuuta 2025.

24. Tekoälyasetus, 74 artiklan 2 kohta.

25. Tekoälyasetus, 112 artiklan 1 kohta.

26. Vaikka tekoälyasetuksessa säädetään, että Euroopan komissio voi arvioida tarvetta muuttaa kiellettyjen käytäntöjen luetteloa, se ei anna komissiolle mahdollisuutta päivittää tekoälyasetuksen kyseistä luetteloa. Tällaisen päivityksen tekeminen edellyttäisi erillistä lainsäädäntömenettelyä.

27. Tekoälyasetus, 112 artiklan 11 kohdan b alakohta.

28. Euroopan neuvoston puiteyleissopimus, 16 artiklan 4 kohta.

2.1.2. Yhdenvertaisuuselinten ja muiden kansallisten ihmisoikeustoimijoiden rooli kiellettyjen tekoälyyn liittyvien käytäntöjen käsittelyssä

Tässä osassa käsitellään yhdenvertaisuuselinten ja kansallisten ihmisoikeustoimijoiden mahdollista roolia kiellettyjen tekoälyyn liittyvien käytäntöjen suhteen. Seuraavissa osissa korostetaan toimia, joita yhdenvertaisuuselimet ja kansalliset ihmisoikeustoimijat voivat toteuttaa tiettyjen kieltojen osalta.

Yhdenvertaisuuselimet ja kansalliset ihmisoikeustoimijat voivat kaikkien kieltojen osalta

- ▶ valvoa kiellettyjä käytäntöjä kokoamalla yhteen esimerkkejä tapauksista, jotka on arvioitu tai jotka olisi arvioitava 5 artiklan nojalla. Nämä esimerkit auttavat havainnollistamaan nykyisten kiellettyjen käytäntöjen merkitystä ja mahdollista tarvetta laajentaa kieltoa muihin käytäntöihin niiden perusoikeuksiin, erityisesti yhdenvertaisuuteen ja syrjimättömyyteen, kohdistuvien riskien vuoksi. Esimerkkejä voidaan kerätä tekemällä yhteistyötä kansalaisjärjestöjen ja tällaisia järjestelmiä tutkineiden tutkijoiden kanssa, analysoimalla yhdenvertaisuuselinten ja kansallisten ihmisoikeustoimijoiden vastaanottamia valituksia sekä seuraamalla riita-asioita, mukaan lukien yksityisiä oikeudenkäyntejä. Yhteistyötä EU:n perusoikeusviraston kanssa voi myös harkita.
- ▶ osallistua 112 artiklan mukaiseen komission vuosittaiseen arviointiin. Osallistuminen voi tapahtua jakamalla komissiolle näyttöä kielletyistä käytännöistä ja vaarallisista tekoälyjärjestelmistä, joita ei ole vielä kielletty tekoälyasetuksella.
- ▶ osallistua tekoälytoimiston osallistavaan riskitasojen arviointimenetelmään.
- ▶ edistää markkinavalvontaviranomaisten kieltojen toimeenpanoa muun muassa käyttämällä valvonnan kautta kerättyjä esimerkkejä.
- ▶ tarjota yhdenvertaisuuteen ja syrjimättömyyteen liittyvää asiantuntemusta markkinavalvontaviranomaisille, joiden on arvioitava perusoikeuksiin kohdistuvien haittojen vuoksi asetettuja kieltoja.
- ▶ vastaanottaa yleisöltä valituksia, jotka voivat koskea yksityisten toimijoiden käyttöönottoja.

2.2. Tekoälyjärjestelmät, jotka manipuloivat, harhaanjohtavat tai hyödyntävät ihmisten haavoittuvuuksia

2.2.1. Tausta ja merkitys

Tekoälyasetuksen 5 artiklan 1 kohdan a ja b alakohdassa kielletään haitalliset tekoälyjärjestelmät, jotka manipuloivat, harhaanjohtavat tai hyödyntävät ihmisten haavoittuvuuksia. Tämä kieltö suojaa monia vaarassa olevia perusoikeuksia: oikeutta ihmisarvoon, yksilöiden itsemääräämisoikeutta, vammaisten oikeuksia sekä iästä (lapsen oikeudet, ikääntyneiden henkilöiden oikeudet) tai sosioekonomisesta tilanteesta johtuvaa oikeutta syrjimättömyyteen.

On epätodennäköistä, että julkisen sektorin organisaatiot ottaisivat tarkoituksellisesti käyttöönsä manipuloivia tekoälyjärjestelmiä. Näin voi kuitenkin vahingossa käydä esimerkiksi käyttöön otettavien chattibottien myötä.

Esimerkkejä

Chattibotteja käytetään yhä enenevässä määrin julkisella sektorilla, muun muassa julkisten palveluiden tiedottamistarkoituksiin. Vuonna 2024 New Yorkin kaupungin käyttämä chattibotti antoi virheellistä tietoa työlainsäädännöstä.²⁹ Tällaisia välineitä käytetään todennäköisesti myös pankki- ja vakuutusallalla.

Tämä chattibotti voitaisiin kieltää 5 artiklan 1 kohdan a ja/tai b alakohdan nojalla:

- ▶ Jos tällainen chattibotti erehdyttää ihmisiä antamalla harhaanjohtavaa tietoa, minkä seurauksena henkilö tekee päätöksen, joka aiheuttaa haittaa, kuten rohkaisee henkilöä tekemään itsemurhan,³⁰ chattibotti voitaisiin kieltää 5 artiklan 1 kohdan a alakohdan nojalla.
- ▶ Jos chattibotti taas käyttää hyväkseen henkilön sosioekonomista asemaa eikä anna tietoa (tai antaa virheellisiä tietoja) tietyistä olennaisista palveluista, kuten tarveharkintaisten sosiaalietuuksien saamisesta, mikä johtaa taloudellisiin vaikeuksiin, se voitaisiin kieltää 5 artiklan 1 kohdan b alakohdan nojalla, koska kyseinen tekoälyjärjestelmä hyödyntää henkilön sosioekonomista tilannetta (ks. jäljempää). Olosuhteista riippuen jälkimmäiseen tilanteeseen voidaan soveltaa myös 5 artiklan 1 kohdan a alakohtaa.

Näitä kahta kieltoa tarkastellaan yhdessä, koska 5 artiklan 1 kohdan b alakohtaa voidaan pitää erityissäännöksenä, kun sillä on päällekkäisyyksiä 5 artiklan 1 kohdan a alakohdan kanssa.³¹

29. Offenhartz J. (2024), "NYC's AI chatbot was caught telling businesses to break the law. The city isn't taking it down", *AP News*, saatavilla osoitteessa <https://apnews.com/article/new-york-city-chatbot-misinformation-6ebc71db5b770b9969c906a7ee4fae21>, viitattu 10. marraskuuta 2025.

30. Walker, L. (2023), "Belgian man dies by suicide following exchanges with chatbot", *Brussels Times*, saatavilla osoitteessa www.brusselstimes.com/430098/belgian-man-commits-suicide-following-exchanges-with-chatgpt, viitattu 10. marraskuuta 2025.

31. Tekoälyasetuksen kieltosuuntaviivat.

5 artiklan 1 kohdan a ja b alakohtien mukaisten kieltojen arviointi

Sen arvioiminen, onko tekoälyjärjestelmä 5 artiklan 1 kohdan a alakohdan nojalla kielletty, edellyttää viisivaiheista arviointia, joka täyttää kaikki seuraavat vaiheet:

1. Onko tekoälyjärjestelmä saatettu markkinoille, otettu käyttöön tai käytössä?³²
2. Käyttääkö tekoälyjärjestelmä ”subliminaalisia tekniikoita, joita henkilö ei havaitse tietoisesti, tai tarkoituksellisesti manipuloivia tai harhaanjohtavia tekniikoita” tai näiden yhdistelmää?
3. Onko tekoälyjärjestelmän käyttöönoton ”tavoitteena vääristää tai [se] olennaisesti vääristää henkilön tai henkilöryhmän käyttäytymistä”?
4. Onko tekoälyjärjestelmä käyttäytymistä vääristämällä saanut henkilön tai henkilöryhmän ”tekemään päätöksen, jota tämä ei olisi muussa tapauksessa tehnyt”?
 - a. Onko henkilön/ryhmän itsenäisyyttä merkittävästi heikennetty (muutenkin kuin lailliseen suostutteluun perustuvan vaikuttamisen kautta)?
5. Onko tämä henkilön tai henkilöryhmän päätös aiheuttanut tai ”kohtuullisella todennäköisyydellä aiheuttaa kyseiselle henkilölle, toiselle henkilölle tai henkilöryhmälle merkittävää haittaa”?
 - a. Millaista haittaa heille aiheutui? Fyysistä, psykologista, taloudellista?
 - b. Oliko haitta merkittävä³³? Vakavuus perustuu haittojen yhdistelmään, kumulatiivisiin vaikutuksiin, laajuuteen, palautettavuuteen ja keston.³⁴

Sen arvioiminen, onko tekoälyjärjestelmä 5 artiklan 1 kohdan b alakohdan nojalla kielletty, edellyttää nelivaiheista arviointia, joka täyttää kaikki seuraavat vaiheet:

1. Onko tekoälyjärjestelmä saatettu markkinoille, otettu käyttöön tai käytössä?
2. Hyödyntääkö tekoälyjärjestelmä ”luonnollisen henkilön tai tietyn henkilöryhmän haavoittuvuuksia, jotka liittyvät heidän ikäänsä, vammaansa tai erityiseen sosiaaliseen tai taloudelliseen tilanteeseensa”?
 - a. Ikä: lapset ja ikääntyneet henkilöt.
 - b. Vamma: käsittää fyysiset, henkiset, älylliset ja aistivammat, jotka estävät yksilön täysimääräisen osallistumisen yhteiskuntaelämään.³⁵

32. Tekoälyasetus, 3 artiklan 9–11 kohta. Katso komission tulkinta ”markkinoille saattamisesta, käyttöönotosta tai käytöstä” Sinisen opas – EU:n tuotesääntöjen täytäntöönpano-oppaan 2022, 2022/C247/01 kohdasta 2.

33. Unionin tuomioistuin, 7.9.2004, *Waddenvereniging ja Vogelbeschermingsvereniging*, C-127/02, EU:C:2004:482, ja 11.4.2013, *Sweetman ja muut.*, C-258/11, EU:C:2013:220.

34. Tekoälyasetuksen kieltosuuntaviivat, 92 kohta.

35. Euroopan parlamentin ja neuvoston direktiivi (EU) 2019/882, annettu 17 päivänä huhtikuuta 2019, tuotteiden ja palvelujen esteettömyysvaatimuksista (EUVL L 151, 7.6.2019, s. 70).

- c. Sosiaalinen tai taloudellinen tilanne: kattaa äärimmäisessä köyhyydessä elävät henkilöt, etniset tai uskonnolliset vähemmistöt.³⁶
3. Onko tekoälyjärjestelmän käyttöönoton "tavoitteena vääristää tai [se] olen-
naisesti vääristää henkilön tai kyseiseen henkilöryhmään kuuluvan henkilön
käyttäytymistä"?
4. Onko tekoälyjärjestelmä käyttäytymistä vääristämällä aiheuttanut "tai kohtuul-
lisella todennäköisyydellä aiheuttaa kyseiselle henkilölle tai toiselle henkilölle
merkittävää haittaa"?

Mitä tulee 5 artiklan 1 kohdan a alakohtaan, jotkin tärkeät konseptit eivät ole itsestään selviä. Tekoälyasetuksessa ei ole määritelty "subliminaalisia tekniikoita, joita henkilö ei havaitse tietoisesti", "tarkoituksellisesti manipuloivia" ja "harhaanjohtavia tekniikoita".

- ▶ Subliminaaliset tekniikat, joita henkilö ei havaitse tietoisesti, voivat olla ärsyke-
keitä, joita ihmiset eivät tietoisesti havaitse, mutta joita aivot kuitenkin käsit-
televät ja jotka voivat vaikuttaa heidän käyttäytymiseensä. Tällaiset ärsykkeet
voivat olla ääni- tai näköärsykeitä tai aikakäsityksiä muuttavia ärsykeitä.³⁷
Subliminaalisia tekniikoita voisivat olla esimerkiksi "aivojen ja tietokoneen
rajapinnat tai virtuaalitodellisuus".³⁸ Mitä tulee audiovisuaaliseen kaupalliseen
viestintään,³⁹ audiovisuaalisia mediapalveluja koskeva direktiivi (AVMSD)
kieltää jo ennestään subliminaalisten tekniikoiden käytön.⁴⁰ Näin ollen teko-
älyasetuksessa asetettu kieltö, jota sovelletaan vain silloin, kun kyseessä on
tekoälyjärjestelmä, on AVMSD:n kiellon erityistapaus. Subliminaalisia tekniikoita
voidaan pitää esimerkkeinä manipulatiivisista tekniikoista.
- ▶ Tarkoituksellisesti manipuloivia tekniikoita voidaan käyttää "taivuttelemaan
henkilöitä haitallisiin käyttäytymismalleihin", hyödyntämällä heidän ennako-
luulojaan tai tunnetilaansa "suuntaamalla heitä tekemään päätöksiä tavalla, joka
horjuttaa ja heikentää heidän itsenäisyyttään, päätöksentekoaan ja valinnan-
vapauttaan".⁴¹ Tällaista manipulointia voi olla henkilötietojen hyödyntäminen
personoitujen viestien, kuten kohdennettujen mainosten, lähettämiseksi.
- ▶ Harhaanjohtavilla tekniikoilla esitetään vääriä ja harhaanjohtavia tietoja.
Harhautus voi tapahtua audiovisuaalisen sisällön, kuten syvävääreännösten
tai harhaanjohtavien chattibottien kautta. Tekniikan harhaanjohtavuutta
arvioitaessa tulee ottaa huomioon 50 artiklan avoimuusvelvoitteet, koska
niiden avulla harhaanjohtaminen voidaan estää ilmoittamalla käyttäjille, että

36. Tekoälyasetus, johdanto-osan 29 kohta: "Lisäksi tekoälyjärjestelmissä voidaan myös muutoin hyödyntää henkilön tai tietyn henkilöryhmän haavoittuvuuksia, jotka liittyvät heidän ikäänsä, Euroopan parlamentin ja neuvoston direktiivissä (EU) 2019/882 tarkoitettuun vammaan tai erityiseen sosiaaliseen tai taloudelliseen tilanteeseen, joka todennäköisesti saattaa nämä henkilöt haavoittuvammiksi hyväksikäytölle, kuten äärimmäisessä köyhyydessä elävät henkilöt tai etniset tai uskonnolliset vähemmistöt" (korostus lisätty).

37. Tekoälyasetuksen kielto-suuntaviivat, 64–66 kohta.

38. Tekoälyasetus, johdanto-osan 29 kohta.

39. Euroopan parlamentin ja neuvoston direktiivi 2010/13/EU, annettu 10 päivänä maaliskuuta 2010, audiovisuaalisten mediapalvelujen tarjoamista koskevien jäsenvaltioiden tiettyjen lakien, asetusten ja hallinnollisten määräysten yhteensovittamisesta (EUVL L 95, 15.4.2010, s. 1); AVMSD:n 1 artiklan h alakohta.

40. AVMSD:n 9 artiklan 1 kohdan b alakohta.

41. Tekoälyasetus, johdanto-osan 29 kohta.

he ovat vuorovaikutuksessa tekoälyjärjestelmän kanssa. Avoimuusvelvoitteista huolimatta tekniikat voivat kuitenkin edelleen olla manipuloivia.

Kieltoa sovelletaan silloin, kun tekoälyjärjestelmän käyttöönoton ”tavoitteena on vääristää tai jotka olennaisesti vääristävät henkilön tai henkilöryhmän käyttäytymistä”. Tämä tarkoittaa, että käyttäytymisen olennaisen vääristämisen *aikomus* ei ole välttämätön, vaan sen *vaikutus* riittää. Euroopan komissio toteaa suuntaviivoissaan, että jo vaikutuksen todennäköisyys⁴², joka johtuu esimerkiksi tietojen esittämisestä,⁴³ ilman todisteita vaikutuksesta sen jälkeen, kun haitta on toteutunut, riittää. Komission mukaan vaikutus tai vaikutuksen todennäköisyys voi kohdistua

1. keskivertokuluttajaan,⁴⁴ mukaan lukien sen tunnustaminen, että hänen päätösten-tekokykyään voivat heikentää rajoitukset, kuten kognitiiviset ennakkoluulot,⁴⁵ ja
2. yksilöihin tai ryhmiin, jotka ovat saattaneet joutua erityiseksi kohteeksi tai joita on syrjitty.

On kuitenkin välttämätöntä, että tekniikoiden, joiden ”tavoitteena on vääristää tai jotka olennaisesti vääristävät” ja subliminaalisten, tarkoituksellisesti manipuloivien tai harhaanjohtavien tekoälyjärjestelmän käyttämien tekniikoiden välillä on uskottava todennäköisyys.

Merkittävän haitan kohtuullisen todennäköisyyden arvioimiseksi on otettava huomioon fyysisten, psykologisten ja taloudellisten vahinkojen eri muodot.⁴⁶ Lisäksi on arvioitava haittojen merkittävyyttä,⁴⁷ esimerkiksi haittojen yhdistelmään perustuvaa vakavuutta, haittojen kumulatiivisia vaikutuksia, haittojen laajuutta (esimerkiksi kansallisella tasolla julkisella sektorilla käyttöönotetut chattibotit, jolloin on todennäköistä, että niitä käyttävät useat ihmiset), haittojen palautettavuutta ja haittojen kestoa.⁴⁸

42. Unionin tuomioistuimen tuomio (viides jaosto) 26.10.2016. *Canal Digital Denmark A/S*. EU:C:2016:800, tapaus C-611/14, 73 kohta.

43. Unionin tuomioistuimen tuomio 19.12.2013, *Trento Sviluppo ja Centrale Adriatica*, C-281/12, EU:C:2013:859.

44. Komission tiedonanto – Ohjeet sopimattomista elinkeinonharjoittajien ja kuluttajien välisistä kaupallisista menettelyistä sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston direktiivin 2005/29/EY tulkintaa ja soveltamista varten (EUVL C 526, 29.12.2021, s. 1). Ks. myös keskivertokuluttajan määritelmä direktiivin 2005/29/EY johdanto-osan 18 kohdasta: ”valistunut, kohtuullisen tarkkaavainen ja huolellinen keskivertokuluttaja, ottaen huomioon sosiaaliset, kulttuuriset ja kielelliset tekijät”.

45. *Compass Banca SpA vs. Autorità Garante della Concorrenza e del Mercato (AGCM)*, tapaus C-646/22, EU:C:2024:957.

46. Tekoälyasetus, johdanto-osan 29 kohta.

47. Unionin tuomioistuin, 7.9.2004, *Waddenvereniging ja Vogelbeschermingsvereniging*, C-127/02, EU:C:2004:482, ja 11.4.2013, *Sweetman ja muut.*, C-258/11, EU:C:2013:220.

48. Tekoälyasetuksen kieltosuuntaviivat, 92 kohta.

2.2.2. Yhdenvertaisuuselinten ja muiden kansallisten ihmisoikeustoimijoiden rooli sellaisten tekoälyjärjestelmien käsittelyssä, jotka manipuloivat, harhaanjohtavat tai käyttävät hyväksi henkilön haavoittuvuutta

- ▶ Lisätä tietoisuutta tästä kiellosta ja korostaa henkilölle aiheutuvaa haittaa kuluttajan sijasta, sillä henkilön oikeudet ulottuvat kuluttajan oikeuksia laajemmalle, kun taas komission suuntaviivoissa viitataan nimenomaan tämän kiellon osalta ”keskivertokuluttajaan” (katso kohta 2.2 edellä). Tähän voidaan ryhtyä yhdenvertaisuuselinten ja kansallisten ihmisoikeustoimijoiden julkisen viestinnän sekä niiden ja markkinavalvontaviranomaisten välisen viestinnän kautta.
- ▶ Varmistaa ennakoivasti, että haitan ”merkittävydessä” otetaan huomioon perusoikeudet ja erityisesti yhdenvertaisuus ja syrjimättömyys. Yhdenvertaisuuselimet voivat arvioida haitan ”merkittävyyttä” syrjimättömyyttä koskevan, voimassa olevan oikeuskäytännön perusteella. Rajaa, jonka jälkeen vahinkoa pidetään riittävän merkittävänä kiellon asettamiseksi, tulee arvioida.
 - On tärkeää, että yhdenvertaisuuselimet keräävät esimerkkejä. Kansalaisjärjestöt (CSO:t) voivat olla tässä hyödyllisenä apuna. Lisäksi yhdenvertaisuuselinten on seurattava siviilioikeudenkäyntejä.
- ▶ Varmistaa, että haavoittuvuuksien ”hyödyntämisessä” otetaan huomioon perusoikeudet ja erityisesti yhdenvertaisuus ja syrjintä laatimalla ohjeita ja toimittamalla ne markkinavalvontaviranomaisille, jotka vastaavat haittojen arvioinnista. Erityistä huomiota tulee kiinnittää siihen, voidaanko näihin kriteereihin sisällyttää välillinen syrjintä.

2.3. Sosiaalinen pisteytys

2.3.1. Tausta ja merkitys

Tekoälyasetuksen 5 artiklan 1 kohdan c alakohdassa kielletään julkisia ja yksityisiä toimijoita suorittamasta ihmisten sosiaalista pisteytystä, koska se voi johtaa ”syrjiviin tuloksiin ja tiettyjen ryhmien syrjäytymiseen”⁴⁹ ja koska se loukkaa oikeutta ihmisarvoon ja syrjimättömyyteen.

Esimerkkejä sosiaaliseen pisteytykseen perustuvista järjestelmistä

Tämä kiello on erityisen tärkeä julkisella sektorilla, jolla luokittelu ja arviointi on yleistä, esimerkiksi työllisyyden ja sosiaaliturvan, verotuksen, maahanmuuton, lainvalvonnan tai oikeuslaitoksen aloilla. Luokitus- ja arviointijärjestelmiä käytetään

49. Tekoälyasetus, johdanto-osan 31 kohta.

myös vakuutus- ja pankkialalla. Esimerkiksi Saksassa käytetään Schufa-järjestelmää, jonka avulla ihmisille annetaan luottopisteytys.⁵⁰

Esimerkiksi Itävallassa työvoimatoimisto kehitti algoritmin, jonka avulla työllistymismahdollisuuksia voidaan ennustaa ja tukiresursseja jakaa työnhakijoille. Prototyypin osoitettiin syrjivän naisia (erityisesti yksinhuoltajaäitejä) ja maahanmuuttaja-taustaisia työnhakijoita.⁵¹ Alankomaissa havaittiin, että petosten ennustamiseen käytetty järjestelmä oli syrjinyt edunsaajia etnisen alkuperän ja kansalaisuuden perusteella.⁵² Puolassa työvoimatoimiston käyttämästä järjestelmästä luovuttiin lopulta, koska sitä pidettiin perustuslain vastaisena.⁵³ ADM- ja tekoälyjärjestelmiä käytetään tai käytettiin myös edunsaajien valvontaan useissa maissa (esimerkiksi Ranska,⁵⁴ Alankomaat,⁵⁵ Tanska,⁵⁶ Belgia⁵⁷), ja ne ovat olleet syrjiviä ja ylivalvoneet haavoittuvassa tilanteessa olevia henkilöitä. Tällaiset järjestelmät perustuvat yleensä henkilökohtaisien ominaisuuksien ja persoonallisuusominaisuuksien sekä edunsaajien ja julkisten työvoimatoimistojen välisiä vuorovaikutussuhteita koskevien tietojen ja joskus yksityisyrittäksiltä (kuten sähkötyhtiöiltä) saatujen tietojen yhdistelmään.

Luokittelu- ja arviointijärjestelmät voivat perustua myös muunlaisiin tietoihin. Esimerkiksi pakolaisleirin osittain automatisoitu valvontajärjestelmä voi analysoida kameroista ja liiketunnistimista saatuja tietoja ja selvittää, ovatko tietyt henkilöt (kuten siirtolaiset) vaarassa yrittää poistua leiriltä.⁵⁸

50. AlgorithmWatch (2018), "SCHUFA, a black box: OpenSCHUFA results published", saatavilla osoitteessa <https://algorithmwatch.org/en/schufa-a-black-box-openschufa-results-published/>, ja C-634/21 SCHUFA Holding (Scoring) EU:C:2023:957.
51. Allhutter D. et al. (2020), "Algorithmic profiling of job seekers in Austria: How austerity politics are made effective", *Frontiers in Big Data*, 3, saatavilla osoitteessa <https://doi.org/10.3389/fdata.2020.00005>, viitattu 11. marraskuuta 2025.
52. De Rechtspraak (2019), "SyRI legislation in breach of European Convention on Human Rights", *De Rechtspraak*, saatavilla osoitteessa www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Rechtbanken/Rechtbank-Den-Haag/Nieuws/Paginas/SyRI-legislation-in-breach-of-European-Convention-on-Human-Rights.aspx, viitattu 11. marraskuuta 2025. SyRI-järjestelmän katsottiin myös loukanneen kohtuuttomasti loppukäyttäjien oikeutta yksityisyyteen, koska se käsitteli eri valtion virastoilta saatuja henkilötietoja.
53. Szymielewicz K. et al. (2015), "Profiling the unemployed in Poland: social and political implications of algorithmic decision making", Fundacja Panoptykon, saatavilla osoitteessa <https://en.panoptykon.org/profiling-unemployed-poland-report>, viitattu 11. marraskuuta 2025.
54. Romain et al. (2023).
55. Mehrotra D. et al. (2023), "Inside the suspicion machine", *WIRED*, saatavilla osoitteessa www.wired.com/story/welfare-state-algorithms/.
56. Geiger G. (2023), "How Denmark's welfare state became a surveillance nightmare", *WIRED*, saatavilla osoitteessa www.wired.com/story/algorithms-welfare-state-politics/ and Amnesty International (2024), "Denmark: AI-powered welfare system fuels mass surveillance and risks discriminating against marginalized groups – report", saatavilla osoitteessa www.amnesty.org/en/latest/news/2024/11/denmark-ai-powered-welfare-system-fuels-mass-surveillance-and-risks-discriminating-against-marginalized-groups-report/.
57. Degraeve E. (2020), "The use of secret algorithms to combat social fraud in Belgium", *European Review of Digital Administration & Law* 1–2: 167–78.
58. Tekoälyasetuksen kieltosuuntaviivojen 155 kohdassa annettu esimerkki.

Kieltojen arviointi 5 artiklan 1 kohdan c alakohdan nojalla

Sen arvioiminen, kuuluuko tekoälyjärjestelmä 5 artiklan 1 kohdan c alakohdan soveltamisalaan, edellyttää viisivaiheista arviointia, joka täyttää kaikki seuraavat vaiheet:

1. Onko tekoälyjärjestelmä saatettu markkinoille, otettu käyttöön tai käytössä?
2. Onko tekoälyjärjestelmän tarkoituksena "luonnollisten henkilöiden tai henkilöryhmien arvioiminen tai luokittelu" tai käytetäänkö sitä siihen?
3. Onko arviointi tai luokittelu tapahtunut "tietynä ajanjaksona"?
 - a. Kertaluontoista luokittelua ei ole kielletty, mutta kieltoa sovelletaan, jos kerran analysoidut tiedot kattavat tietyn ajanjakson.⁵⁹
4. Perustuuko arviointi tai luokittelu
 - a. luonnollisten henkilöiden tai henkilöryhmien sosiaaliseen käyttäytymiseen tai
 - b. "tunnettuihin, pääteltyihin tai ennakoituihin henkilökohtaisiin ominaisuuksiin tai luonteenpiirteisiin"?⁶⁰
5. Johtaako arviointi tai luokittelu sosiaaliseen pisteytykseen, joka johtaa "tiettyjen luonnollisten henkilöiden tai henkilöryhmien haitalliseen tai epäedulliseen kohteluun"
 - a. sosiaalisissa yhteyksissä, jotka eivät liity siihen asiayhteyteen, jossa tiedot alun perin tuotettiin tai kerättiin" ja/tai
 - b. "joka on perusteetonta tai suhteetonta heidän sosiaaliseen käyttäytymiseensä tai sen vakavuuteen nähden"?⁶¹

Luokittelu on arviointia laajempaa, ja se voi perustua tunnettuihin ominaisuuksiin, kuten ikään, sukupuoleen ja pituuteen, joiden perusteella luokittelu ei välttämättä ole profilointia.⁶² Arviointi liittyy läheisemmin "profilointiin", joka tarkoittaa:⁶³

59. Tekoälyasetuksen kieltoisuuntaviivat, 155 kohta. Kohta perustuu pakolaisleirillä käytetyn järjestelmän esimerkkiin, jossa analysoidut tiedot kattavat tietyn ajanjakson.

60. Tekoälyasetuksen kieltoisuuntaviivat, 158 kohta: ""Henkilökohtaisiin ominaisuuksiin" voi kuulua monia erilaisia henkilöön liittyviä tietoja, kuten sukupuoli, seksuaalinen suuntautuminen tai sukupuoliominaisuudet, sukupuoli, sukupuoli-identiteetti, rodullinen tai etninen alkuperä, perhetilanne, osoite, tulot, kotitalouden jäsenet, ammatti, työsuhte tai muu oikeudellinen asema, työsuoritus, taloudellinen tilanne, maksukyky, terveys, henkilökohtaiset mieltymykset, kiinnostuksen kohteet, luotettavuus, käyttäytyminen, sijainti tai liikkuminen, velan määrä ja auton tyyppi."

61. Alankomaiden lapsilisäskandaali on esimerkki, jossa molemmat 5 artiklan 1 kohdan c alakohdan vaatimukset täyttyvät. Ks. de Nationale ombudsman, "[Belastingdienst treft 232 gezinnen met onevenredig harde actie](#)", 27. marraskuuta 2019 [hollanniksi]. Ks. myös *ibid.* "[Geen powerplay maar fair play. Onevenredig harde aanpak van 232 gezinnen met kinderopvangtoeslag](#)", 9. elokuuta 2017, s. 32.

62. 29 artiklan mukainen tietosuojatyöryhmä. Suuntaviivat automatisoiduista yksittäispäätöksistä ja profiloinnista asetuksen (EU) 2016/679 täytäntöön panemiseksi, WP251rev.01, 6.2.2018, s. 7. Katso myös GDPR:n 4 artiklan 4 kohta.

63. *Ibid.*

tietojen keräämistä yksilöstä (tai ihmisryhmästä) ja heidän ominaisuuksiensa tai käyttäytymismallinsa arvioimista, jotta heidät voidaan sijoittaa tiettyyn kategoriaan tai ryhmään ja erityisesti analysoida ja/tai tehdä ennusteita esimerkiksi heidän

- ▶ kyvystään suoriutua tehtävästä
- ▶ kiinnostuksenkohteista
- ▶ todennäköisestä käyttäytymisestä.

Esimerkiksi Saksassa käytössä oleva luottopisteytysjärjestelmä Schufa, joka tuottaa ”todennäköisyyspisteytyksen” henkilön maksukyvyistä, on Euroopan unionin tuomioistuimen (EUT) mukaan ”profilointia”.⁶⁴

Pisteytyskäytäntö voi johtaa epäedulliseen kohteluun, vaikka siitä ei aiheutuisikaan erityistä haittaa (esimerkiksi yksilön erottaminen ylimääraisten tarkastusten kohteeksi, kun taas haitallinen kohtelu johtaa haittaan). Sekä haitallinen että epäedullinen kohtelu voidaan jo kieltää EU:n syrjimättömyyslainsäädännön nojalla, jolla suojellaan tiettyjä suojattuja ryhmiä esimerkiksi iän, etnisen ja rodullisen alkuperän⁶⁵, sukupuolen ja uskonnon perusteella. Tekoälyasetuksen kieltojen soveltamisala on kuitenkin laajempi, ja sitä sovelletaan kohteluun, joka ylittää EU:n syrjimättömyyslainsäädännön.⁶⁶

Jos pisteytys johtaa ”haitalliseen tai epäedulliseen kohteluun”, kieltoa sovelletaan, vaikka pisteytyksen tuottaisi muu organisaatio (yksityinen luottokelpoisuutta arvioiva yritys) kuin sitä käyttävä organisaatio (viranomainen).⁶⁷ Tämä kielto ei myöskään rajoitu pelkästään tekoälyjärjestelmän suorittamaan arviointiin tai luokitteluun. Kiellon soveltamisalaan kuuluvat pisteytyskäytännöt, joihin voi sisältyä ihmisen tekemiä arviointeja, kunhan tekoälyjärjestelmän tuotoksella on ”riittävän merkittävä rooli sosiaalisen pisteytyksen tuottamisessa”.⁶⁸ Esimerkiksi käyttö, jossa viranomainen käyttää tekoälyjärjestelmää pisteytykseen ja yhdistää tämän pisteytyksen tuloksen ihmisen suorittamaan lisätietojen arviointiin, olisi kielletty, jos tuloksena on haitallinen tai epäedullinen kohtelu.

2.3.2. Yhdenvertaisuuselinten ja muiden kansallisten ihmisoikeustoimijoiden rooli sosiaaliseen pisteytykseen liittyvien kieltojen käsittelyssä

- ▶ Seurata ja arvioida EU:n syrjimättömyyslainsäädännön ylittäviä pisteytyskäytäntöjä, jotka johtavat epäedulliseen ja haitalliseen kohteluun. Yhdenvertaisuuselinten on kehitettävä lisäasiantuntemusta, jotta ne voivat suorittaa tehokasta valvontaa.

64. Unionin tuomioistuimen tuomio 7.12.2023, *SCHUFA Holding (Scoring)*, C-634/21, EU:C:2023:957, 47 kohta.

65. Koska kaikki ihmiset kuuluvat samaan lajiin, Euroopan neuvoston ministerikomitea hylkää teorian, jotka perustuvat eri ”rotujen” olemassaoloon. Tässä julkaisussa termiä ”rotu” käytetään kuitenkin sen varmistamiseksi, etteivät henkilöt, joita yleisesti ja virheellisesti rodullistetaan, jää lainsäädännön tarjoaman suojan ja politiikan täytäntöönpanon ulkopuolelle.

66. Tekoälyasetuksen kieltosuuntaviivat, 165 kohta.

67. Unionin tuomioistuimen tuomio 7.12.2023, *SCHUFA Holding (Scoring)*, C-634/21, EU:C:2023:957, 42–51 ja 60–61 kohdat.

68. Tekoälyasetuksen kieltosuuntaviivat, 161 kohta.

2.4. Rikokseen syyllistymisen riskinarviointi

2.4.1. Tausta ja merkitys

Tekoälyasetuksen 5 artiklan 1 kohdan d alakohdassa kielletään yksilön rikokseen syyllistymisen riskin arviointi ja ennustaminen, joka ”perustuu yksinomaan luonnollisen henkilön profilointiin tai hänen persoonallisuuspiirteidensä ja persoonallisuussominaisuuksiensa arviointiin”⁶⁹ Tällä kiellolla pyritään rajoittamaan haittoja, jotka kohdistuvat oikeuteen ihmisarvoon, syrjimättömyyteen, oikeudenmukaiseen oikeudenkäyntiin, syyttömyysolettamaan, puolustukseen, tehokkaisiin oikeussuojakeinoihin, yksityisyyteen ja tietosuojaan.⁷⁰

Sen arvioiminen, sovelletaanko 5 artiklan 1 kohdan d alakohtaa tekoälyjärjestelmään, edellyttää kolmivaiheista arviointia, joka täyttää kaikki seuraavat vaiheet:

1. Onko tekoälyjärjestelmä saatettu markkinoille, otettu käyttöön tai käytössä?
2. Onko tekoälyjärjestelmän tarkoituksena tehdä luonnollisia henkilöitä koskevia riskinarviointia ”jotta voidaan arvioida tai ennustaa sen riskiä, että luonnollinen henkilö syyllistyy rikokseen”?
3. Perustuuko arvio tai ennuste ainoastaan
 - a. profilointiin,⁷¹ ja/tai
 - b. persoonallisuuspiirteiden ja persoonallisuussominaisuuksien, kuten kansallisuuden, syntymäpaikan, asuinpaikan, lasten lukumäärän, velkatason tai autotyypin, arviointiin.⁷²

Esimerkiksi lainvalvontaviranomaisen käyttämä tekoälyjärjestelmä, jolla voidaan ennustaa rikollista käyttäytymistä esimerkiksi terrorismirikosten suhteen pelkästään henkilön iän, kansallisuuden, osoitteen, autotyypin ja siviilisäädyn perusteella, olisi kielletty.⁷³

Esimerkkejä ei-kielletyistä käytöistä:

- ▶ ryhmän riskinarviointi (yksittäisen henkilön sijasta)⁷⁴
- ▶ kaikki muut ennakoivan poliisitoiminnan lähestymistavat, jotka eivät perustu yksinomaan profilointiin tai persoonallisuuspiirteiden ja persoonallisuussominaisuuksien arviointiin

69. Tekoälyasetus, 5 artiklan 1 kohdan d alakohta.

70. Tekoälyasetus, johdanto-osan 48 kohta.

71. Välilliseen tai välittömään syrjintään johtava profilointi on jo kielletty LED:n 11 artiklan 3 kohdassa. Ks. myös: 29 artiklan mukainen työryhmä. Suuntaviivat automatisoiduista yksittäispäätöksistä ja profiloinnista asetuksen (EU) 2016/679 täytäntöön panemiseksi, WP251rev.01, 6.2.2018, s.7; Euroopan unionin perusoikeusvirasto, *Preventing unlawful profiling today and in the future: a guide*, Handbook, 2018, s. 138.

72. Tekoälyasetus, johdanto-osan 42 kohta.

73. Tekoälyasetuksen kieltosuuntaviivat, 202 kohta.

74. Tekoälyasetuksen kieltosuuntaviivat, 196 kohta. On huomattava, että jos ryhmäprofilia käytetään yksittäisen henkilön samankaltaiseen rikokseen syyllistymisen riskin arviointiin ja ennustamiseen, tämä lasketaan profiloinniksi ja täten se kuuluu kiellon soveltamisalaan.

- tekoälyjärjestelmät, joita käytetään tukemaan ihmisen tekemää arviointia, joka perustuu objektiivisiin ja todennettavissa oleviin tosiseikkoihin, jotka liittyvät suoraan rikolliseen toimintaan⁷⁵
- sijaintiin perustuva ennakoiva poliisitoiminta⁷⁶
- tekoälyjärjestelmät, jotka tekevät yksittäisiä ennusteita, jotka ovat kansallisen ja EU:n lainsäädännön sallimia ja jotka liittyvät hallinnolliseen rikkomukseen (eivätkä rikokseen), vaikka seurauksena ”kerättäisiin tietoja luonnollisten henkilöiden mahdollisesta osallistumisesta rikoksiin”.⁷⁷

Tämä kielto on soveltamisalaltaan rajallinen, eikä se koske ennakoivaa poliisitoimintaa kokonaisuudessaan. Kun kieltoa sovelletaan, se on laajempi sen suhteen, milloin ja keneen sitä sovelletaan. Tekoälyasetus täydentää direktiiviä (EU) 2016/343, jolla suojataan oikeutta olettaa syyttömyys, kunnes syyllisyys on todistettu, ennen kuin virallinen rikostutkinta aloitetaan.⁷⁸ Direktiiviä (EU) 2016/343 sovelletaan vain silloin, kun henkilöä epäillään tai syytetään rikoksesta.

On tärkeää huomata, että kielto ei rajoitu lainvalvontaviranomaisiin tai niiden puolesta toimiviin tahoihin. Kaikki tahot, joilla on lakisääteinen velvollisuus ”arvioida tai ennustaa sen riskiä, että luonnollinen henkilö syyllistyy rikokseen”, kuuluvat kiellon soveltamisalaan. Veroviranomainen, joka luo profileja henkilöistä kansalaisuuden tai muiden tekoälyjärjestelmien avulla saatujen ominaisuuksien perusteella, kuuluu tämän kiellon soveltamisalaan.⁷⁹ Myös pankkilaitos, joka on yksityinen taho ja jonka tehtävänä on lain mukaan seuloa asiakkaita rikoksen, kuten rahanpesun, varalta, kuuluisi tämän kiellon soveltamisalaan, jos se käyttää tekoälyjärjestelmiä eikä noudata asetusta (EU) 2024/1624.⁸⁰

On myös tärkeää korostaa, että ”ryhmäprofiloinnin”⁸¹ kohdentaminen yksilöihin kuuluu tämän kiellon soveltamisalaan. Ryhmäprofiloinnissa luodaan profiili tietyistä ryhmästä, johon voi kuulua esimerkiksi terroristeja ja jengiläisiä. Tällaisia profileja voidaan käyttää arvioitaessa ja ennustettaessa muiden henkilöiden riskiä syyllistyä samanlaisiin rikoksiin. Tämä on kiellettyä.

75. Tekoälyasetuksen kieltoisuuntaviivat, 214 kohta.

76. Tekoälyasetuksen kieltoisuuntaviivat, 212–13 kohta. Tämä tarkoittaa sitä, että partioita voitaisiin sijoittaa runsaasti alueille sellaisten ennustavien algoritmien päätöksen perusteella, jotka perustuvat historiatietoihin ja jotka ylläpitävät lainvalvonnan syrjintää ja eriarvoisuutta. Ks. myös ”Cop out: automation in the criminal legal system”, Georgetown Law Centre on Privacy & Technology, saatavilla osoitteessa <https://copout.tech/>, viitattu 10. marraskuuta 2025.

77. Tekoälyasetuksen kieltoisuuntaviivat, 217 kohta. Ks. myös tekoälyasetuksen kieltoisuuntaviivojen alaviite 143, jossa käsitellään kriteerejä, joiden perusteella arvioidaan, onko rikkomus rikosoikeudellinen vai ei.

78. Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/343, annettu 9 päivänä maaliskuuta 2016, eräiden syyttömyysolettamaan liittyvien näkökohtien ja läsnäoloa oikeudenkäynnissä koskevan oikeuden lujittamisesta rikosoikeudellisissa menettelyissä.

79. Kieltoa ei sovelleta, kun veroviranomainen arvioi oikeushenkilön, kuten yrityksen, riskiä.

80. Euroopan parlamentin ja neuvoston asetusta (EU) 2024/1624, annettu 31 päivänä toukokuuta 2024, rahoitusjärjestelmän käytön estämisestä rahanpesuun tai terrorismin rahoitukseen, 20 artikla ja 76 artiklan 5 kohdan b alakohta.

81. EU:n perusoikeusvirasto (2018), *Preventing unlawful profiling today and in the future: a guide*, käsikirja, s. 21.

2.4.2. Yhdenvertaisuuselinten ja kansallisten ihmisoikeustoimijoiden rooli rikokseen syyllistymisen riskinarviointiin liittyvien kieltojen käsittelyssä

- ▶ Tutkia kiellon koko soveltamisalaa suorittamalla tai teettämällä tutkimuksia kiellon soveltamisalaan kuuluvista käyttökohteista, jotka eivät koske lainvalvontaviranomaisten riskinarvioinnin käyttöä yksittäisten rikosten ehkäisemiseksi (esimerkiksi veroviranomaiset tai rahanpesusta vastaavat laitokset).
- ▶ Edistää kiellon täytäntöönpanoa kouluttamalla ja valistamalla asianomaisia toimivaltaisia viranomaisia, jotka eivät välttämättä ole tekoälyasetuksen mukaisia toimivaltaisia viranomaisia, jotta ne voivat puuttua syrjinnän aiheuttamiin haittoihin.

2.5. Kasvokuvien haravointi kasvontunnistustietokantojen luomiseksi tai laajentamiseksi

2.5.1. Tausta ja merkitys

Tekoälyasetuksen 5 artiklan 1 kohdan e alakohdassa kielletään tarjoajia ja käyttöönottajia kehittämästä ja laajentamasta kasvontunnistustietokantoja ”haravoi-malla kasvokuvia kohdentamattomasti internetistä tai valvontakamerakuvista”⁸², koska se loukkaa oikeutta ihmisarvoon, syrjimättömyyteen, yksityisyyteen ja tietosuojaan.⁸³ Kieltoa sovelletaan tietokannan tallennusrakenteesta riippumatta. Kasvontunnistustietokantaa ei tarvitse keskittää yhteen sijaintiin tai yhden oikeushenkilön valvontaan. Tietokanta voi olla hajautettu. Kieltoa sovelletaan myös, jos tietokanta on väliaikainen tai lyhytaikainen.

Kasvokuvien kohdentamaton haravoiminen on kuitenkin jo nyt EU:n tietosuoja-lainsäädännön perusteella laitonta.⁸⁴ Haasteena on kuitenkin ollut kiellon täytäntöönpano, erityisesti ylikansallinen täytäntöönpano. Esimerkiksi yhdysvaltalaisen Clearview AI -yrityksen kaupallistaman kasvontunnistussovelluksen, joka perustui sosiaalisen median kasvokuvien kohdennettuun haravoimiseen, kerrottiin olevan useiden lainvalvontaviranomaisten käytössä eri puolilla Eurooppaa.⁸⁵

Sen arviointi, soveltuuko tekoälyjärjestelmä 5 artiklan 1 kohdan e alakohdan soveltamisalaan edellyttää nelivaiheista arviointia, joka täyttää kaikki seuraavat vaiheet:

1. Onko tekoälyjärjestelmä saatettu markkinoille, otettu käyttöön tai käytössä?

82. Tekoälyasetus, johdanto-osan 43 kohta.

83. Tekoälyasetuksen kielto-suuntaviivat, 226 kohta.

84. De Autoriteit Persoonsgegevens (2024), ”Dutch DPA imposes a fine on Clearview because of illegal data collection for facial recognition”, saatavilla osoitteessa www.autoriteitpersoonsgegevens.nl/en/current/dutch-dpa-imposes-a-fine-on-clearview-because-of-illegal-data-collection-for-facial-recognition, viitattu 10. marraskuuta 2025.

85. Euroopan tietosuojaneuvosto (10. kesäkuuta 2020), kirje Euroopan parlamentin jäsenille, saatavilla osoitteessa www.edpb.europa.eu/sites/default/files/files/file1/edpb_letter_out_2020-0052_facialrecognition.pdf, viitattu 10. marraskuuta 2025.

2. Suorittaako tämä tekoälyjärjestelmä ”kohdentamatonta haravointia” (katso jäljempää)?
3. Ovatko ”kasvokuvat” peräisin ”internetistä tai valvontakamerakuvista”?
4. Käytetäänkö tekoälyjärjestelmää ”kasvontunnistustietokantojen luomiseen tai laajentamiseen”?

Tekoälyasetus ei kiellä kaikkea haravointia. Se ei myöskään kiellä tietokantojen luomista muista tiedoista kuin kasvokuvista. Tällaista toimintaa, erityisesti biometrisiin tietoihin liittyvää toimintaa,⁸⁶ rajoitetaan jo EU:n tietosuojalainsäädännöllä.⁸⁷

Se, kunnioittaako verkkosivuja haravoiva yritys teknisiä estomekanismeja⁸⁸ ei vaikuta siihen, onko haravointi kohdentamatonta vai ei. Vain tiettyjen henkilöiden tai ennalta määritellyn henkilöryhmän kasvoja sisältävien kuvien tai videoiden kohdennettu haravointi ei ole kiellettyä.⁸⁹ Jos tällaista kohdennettua haravointia kuitenkin suoritetaan useiden henkilöiden tai ryhmien osalta tietyn ajanjakson aikana, haravointi vastaa kohdentamatonta haravointia ja on siten kiellettyä.⁹⁰

Lisäksi EU:n tietosuojalainsäädäntö suojaa julkisesti saatavilla olevia tietoja, vaikka henkilö olisi julkaissut kasvokuvansa sosiaalisen median verkkosivustolla. ”Pelkästään se, että henkilötiedot ovat julkisesti saatavilla, ei kuitenkaan tarkoita, että rekisteröity on nimenomaisesti saattanut kyseiset tiedot julkisiksi.”⁹¹

2.5.2. Yhdenvertaisuuselinten ja kansallisten ihmisoikeustoimijoiden rooli kasvontunnistustietokantojen luomiseen tai laajentamiseen liittyvään haravointiin liittyvien kieltojen käsittelyssä

- Tukea tämän kiellon täytäntöönpanoa erityisesti EU:n ulkopuolella sijaitsevista yrityksistä, jotka haravoivat kasvokuvia EU:n alueella asuvista henkilöistä, tekemällä jatkuvaa yhteistyötä markkinavalvontaviranomaisten ja tietosuojaviranomaisten kanssa.

86. Huomaa, että tekoälyasetuksen ”biometristen tietojen” määritelmä poikkeaa GDPR:n ja LED:n määritelmistä. Tekoälyasetus, 3 artiklan 34 kohdassa ”biometrisillä tiedoilla” tarkoitetaan ”kaikkia luonnollisen henkilön fyysisiin ja fysiologisiin ominaisuuksiin tai käyttäytymiseen liittyvällä teknisellä käsittelyllä saatuja henkilötietoja, kuten kasvokuvia tai sormenjälkitietoja”. GDPR:n 4 artiklan 14 kohdassa ja LED:n 3 artiklan 13 kohdassa ”biometrisillä tiedoilla” tarkoitetaan ”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”.

87. EDPB (2024), lausunto 28/2024 tietyistä henkilötietojen käsittelyyn tekoälymallien yhteydessä liittyvistä tietosuojanäkökohdista. Annettu 17. joulukuuta 2024, kohta 104–106.

88. Koster M. et al. (2022), ”Robots Exclusion Protocol”, RFC 9309, DOI 10.17487/RFC9309, saatavilla osoitteessa www.rfc-editor.org/info/rfc9309, viitattu 10. marraskuuta 2025.

89. Tekoälyasetuksen kieltosuuntaviivat, 229 kohta.

90. Tekoälyasetuksen kieltosuuntaviivojen 230 kohta.

91. EDPB (2024), ”Report of the work undertaken by the ChatGPT Taskforce”. Annettu 23. toukokuuta 2024, 18 kohta.

2.6. Tunteentunnistus

2.6.1. Tausta ja merkitys

”Erittäin epätoivoutuista syrjivistä ja ihmisarvoa loukkaavista seurauksista ja manipuloivista vaikutuksista”⁹² ja siitä, että tunteiden tunnistamisen toimivuudesta ei ole tieteellistä näyttöä⁹³, huolimatta,⁹⁴ tekoälyasetuksen 5 artiklan 1 kohdan f alakohdassa tunteiden tunnistus kielletään vain työpaikoilla ja oppilaitoksissa. Kaikkia muita tunteiden tunnistuksen käyttötarkoituksia pidetään suuririskisinä,⁹⁵ mutta niitä ei kielletä.

Esimerkkejä

Tunteiden tunnistus käsittää ”erilaisia teknologioita ja käsittelytoimintoja, joilla voidaan havaita, kerätä, analysoida, luokitella ja oppia tuntemaan henkilöiden tunteita, reagoida niihin ja olla vuorovaikutuksessa niiden kanssa”.⁹⁶ Tällaista teknologiaa voidaan käyttää työelämässä rekrytointiprosessin aikana tai työntekijöiden tunteiden seuraamiseen, terveydenhuollossa itsemurhien ehkäisemiseen tai lainvalvonnassa ”valheenpaljastimina” rajatarkastuksissa.⁹⁷

Sen arviointi, soveltuuko tekoälyjärjestelmä 5 artiklan 1 kohdan f alakohdan soveltamisalaan edellyttää kolmivaiheista arviointia, joka täyttää kaikki seuraavat vaiheet:

1. Onko tekoälyjärjestelmä saatettu markkinoille, otettu käyttöön tai käytössä?
2. Tunnistaako tai päättelee tekoälyjärjestelmä tunteita tai pystyykö se päättämään henkilöiden tunteita tai aikomuksia biometristen tietojen perusteella?
3. Onko tekoälyjärjestelmä käytössä ”työpaikoilla ja oppilaitoksissa”?

On tärkeää huomata, että tunteiden tunnistuksen käsitettä on rajoitettu tekoälyasetuksessa:

Tunteilla tai aikomuksilla tarkoitetaan tässä yhteydessä esimerkiksi onnellisuutta, surua, vihaa, yllättyneisyyttä, inhoa, häpeää, kiihtyneisyyttä, halveksuntaa, tyytyväisyyttä ja huvittuneisuutta. Ne *eivät sisällä fyysisiä olotiloja*, kuten kipua tai väsymystä, mukaan

92. Codagnone C. et al. (2022), *Identification and assessment of existing and draft EU legislation in the digital field*. Tekoälyä digitaalisella aikakaudella käsittelevän erityisvaliokunnan (AIDA) puolesta toteutettu tutkimus, talous-, tiede- ja elämänlaatupolitiikasta vastaava osasto, Euroopan parlamentti, Luxemburg, s. 62.

93. Tekoälyasetus, 3 artiklan 39 kohta: ”tunteentunnistusjärjestelmällä” [tarkoitetaan] tekoälyjärjestelmää, jonka avulla luonnollisten henkilöiden tunteita tai aikomuksia voidaan tunnistaa tai päätellä heidän biometristen tietojensa perusteella”.

94. Barrett L. F. et al. (2019), ”Emotional expressions reconsidered: challenges to inferring emotion from human facial movements”, *Psychological Science in the Public Interest*, 20(1), 1–68, saatavilla osoitteessa <https://doi.org/10.1177/1529100619832930>, viitattu 10. marraskuuta 2025.

95. Tekoälyasetus, liitteessä III olevan 1 kohdan c alakohda.

96. Tekoälyasetuksen kieltosuuntaviivat, 240 kohta.

97. Boffey D. (2018), ”EU border ‘lie detector’ system criticised as pseudoscience”, *The Guardian*, saatavilla osoitteessa www.theguardian.com/world/2018/nov/02/eu-border-lie-detection-system-criticised-as-pseudoscience, viitattu 10. marraskuuta 2025.

lukien esimerkiksi järjestelmät, joita käytetään ammattilientäjien tai -kuljettajien väsymyksen havaitsemiseen onnettomuuksien ehkäisemiseksi. Sillä *ei myöskään viitata pelkkään ilmeisen selvien ilmeiden, eleiden tai liikkeiden havaitsemiseen, ellei* niitä käytetä tunteiden tunnistamiseen tai pääättelemiseen. Tällaiset ilmeet voivat olla perusilmeitä, kuten rypistynyt otsa tai hymy, tai eleitä, kuten käsien, käsivarsien tai pään liikkeitä, tai henkilön äänen piirteitä, esimerkiksi korotettua ääntä tai kuiskaamista.⁹⁸

Edellä oleva kohta ei tarkoita, että nämä ovat laillisia käytäntöjä. Tunteiden tunnistaminen edellyttää biometristen tietojen käsittelyä, joka ilman pätevää oikeusperustaa on EU:n tietosuojalainsäädännön perusteella laitonta.⁹⁹

Vaikka työpaikan käsite sisältää rekrytointiprosessin ja suojaa työntekijöitä sekä itsenäisiä ammatinharjoittajia, Euroopan komission suuntaviivojen mukaan se ei sisällä muita henkilöitä. Esimerkiksi ”verkkokameroiden ja äänentunnistusjärjestelmien käyttäminen puhelinalvelukeskuksessa asiakkaiden tunteiden, kuten vihai-suuden tai kärsimättömyyden, seuraamiseksi ei ole kiellettyä” ja ”supermarketissa työntekijöiden tunteiden” seuraaminen on kiellettyä, mutta asiakkaiden tunteiden seuraaminen ei puolestaan ole.¹⁰⁰

Oppilaitoksen käsite koskee kaikkia julkisen tai yksityisen oppilaitoksen tasoja, jotka ovat ”asianomaisten kansallisten koulutusviranomaisten tai vastaavien viranomaisten akkreditoimia tai hyväksymiä”. Kielto koskee tunteiden tunnistuksen käyttöä oppilaitoksissa, myös sisänpääsyprosessien ja kokeiden aikana, mutta se ei koske kursseja, mukaan lukien verkkokursseja, joita tarjoavat yksiköt, joita ei pidetä oppilaitoksina.¹⁰¹

Työpaikoilla ja oppilaitoksissa tunteiden tunnistaminen on sallittua lääketieteellisistä tai turvallisuussyistä, jos se on ehdottoman välttämätöntä ja suhteellista. Lääketieteellisiin tarkoituksiin käytettävien tunteentunnistusjärjestelmien tulee olla asetuksen (EU) 2017/745 (lääkinnällisistä laitteista annettu asetus) sekä unionin ja kansallisen työlainsäädännön mukaisia, mukaan lukien työterveyttä ja -turvallisuutta koskevat lait, jotka saattavat rajoittaa järjestelmien käyttöä. Toisin sanoen CE-merkintä (Conformité Européenne)¹⁰², joka koskee lääkitieteellisten laitteiden asetuksen mukaista tunteiden tunnistusjärjestelmää, on välttämätön mutta ei riittävä edellytys kyseisen järjestelmän tekoälyasetuksen mukaiselle käytölle työpaikoilla ja oppilaitoksissa.

Lisäksi tällainen käyttö edellyttää ”tiettyä käyttötapausta varten etukäteen annettava[a] kirjalli[sta] ja perusteltu[a] asiantuntijalausunto[a, jonka] tarvetta tulisi arvioida objektiivisesti suhteessa lääketieteelliseen ja turvallisuuteen liittyvään tarkoitukseen sen sijaan, että viitataan työnantajan tai oppilaitoksen ”tarpeisiin”. Arvioinnissa olisi selvitettävä, onko olemassa vähemmän yksityisyyteen puuttuvia vaihtoehtoisia keinoja, joilla saavutettaisiin sama lopputulos.”¹⁰³

98. Tekoälyasetus, johdanto-osa, 18 kohta (*korostus lisätty*).

99. GDPR, 6 artikla (käsittelyn lainmukaisuus) ja 9 artikla (erityiset henkilötietoryhmät).

100. Tekoälyasetuksen kieltosuuntaviivat, 254 kohta.

101. Tekoälyasetuksen kieltosuuntaviivat, 257 kohta.

102. Euroopan komissio (n.d.), *CE Marking*, saatavilla osoitteessa https://single-market-economy.ec.europa.eu/single-market/ce-marking_en, viitattu 10. marraskuuta 2025.

103. Tekoälyasetuksen kieltosuuntaviivat, 259 kohta.

Liitteessä III olevan 1 kohdan c alakohdan mukaan ei-kielletyt tunteidentunnistusjärjestelmät katsotaan suuririskisiksi tekoälyjärjestelmiksi. Esimerkkeinä voidaan mainita,¹⁰⁴ jos ja vain jos järjestelmän käytölle on olemassa pätevä oikeusperusta:

- ▶ tilastoviranomaiset, jotka käyttävät tunteiden tunnistusta äänestyskopeissa selvittääkseen ihmisten suhtautumista demokratiaan (esimerkiksi viha, tyytyväisyys)
- ▶ yritys, joka käyttää tunteiden tunnistusta käyttävää chattibottia reagoidakseen asianmukaisesti erittäin tyytymättömiin asiakkaisiin
- ▶ lainvalvontaviranomainen, joka käyttää tunteiden tunnistusjärjestelmää epäilyn kuulustelussa.

Huomaa, että kaikissa tapauksissa tämä viittaa biometristen tietojen käyttämiseen tunteiden päättelyyn tai tunnistamiseen.

2.6.2. Yhdenvertaisuuselinten ja kansallisten ihmisoikeustoimijoiden rooli tunteiden tunnistamiseen liittyvien kieltojen käsittelyssä

- ▶ Kerätä näyttöä syrjinnän aiheuttamista haitoista ja riskeistä, jotka johtuvat tunteiden tunnistamisesta muualla kuin työpaikoilla ja oppilaitoksissa. Yhdenvertaisuuselimet ja kansalliset ihmisoikeustoimijat voivat erityisesti valvoa tekoälyasetuksen liitteessä III olevan 1 kohdan c alakohdan mukaisia suuririskisinä tekoälyjärjestelminä pidettyjä tunteentunnistusjärjestelmiä, jotka rekisteröidään suuririskisten tekoälyjärjestelmien tietokantaan (katso [49 artikla](#)).
- ▶ Kerätä näyttöä tekoälytoimijoiden perusteluista, joiden mukaan tunteiden tunnistuksen käyttö lääketieteellisistä ja turvallisuussyistä on välttämätöntä ja suhteellista lainsäädännön noudattamisen varmistamiseksi.
- ▶ Suojata asiakkaita ja muita ihmisiä, jotka ovat vuorovaikutuksessa muiden ihmisten kanssa heidän työpaikallaan, koska tätä ei ole kielletty 5 artiklan 1 kohdan f alakohdassa.

2.7. Biometrinen luokittelu

2.7.1. Tausta ja merkitys

Tekoälylain 5 artiklan 1 kohdan g alakohdassa kielletään luonnollisten henkilöiden *yksilöllinen* luokittelu "heidän biometristen tietojensa perusteella rodun, poliittisten mielipiteiden, ammattiliiton jäsenyyden, uskonnollisen tai filosofisen vakaumuksen, seksuaalisen käyttäytymisen tai seksuaalisen suuntautumisen perusteella",¹⁰⁵ koska tällainen luokittelu loukkaa oikeuksia ihmisarvoon, syrjimättömyyteen, yksityisyyteen

104. Wendeorst C. and Duller. Y (2021), *Biometric Recognition and Behavioural Detection: Assessing the ethical aspects of biometric recognition and behavioral detection techniques with a focus on their current and future use in public spaces*. Oikeudellisten asioiden valiokunnan ja vetoomusvaliokunnan puolesta suoritettu tutkimus, Euroopan parlamentti, s. 66.

105. Tekoälyasetus, 5 artiklan 1 kohdan g alakohta.

ja tietosuojaan. On huomattava, että jäljempänä selitetty biometrinen luokittelu eroaa biometrisestä (etä)tunnistuksesta, jota käytetään henkilöiden tunnistamiseen (katso kohta 2.8).

Termistä ”biometrinen luokittelujärjestelmä” poiketen termiä ”biometrinen luokittelu” ei ole määritelty tekoälyasetuksessa, mutta se voidaan ymmärtää seuraavasti:

Prosessi, jossa määritetään, kuuluvatko yksilön biometriset tiedot ryhmään, jolla on jokin ennalta määritelty ominaisuus, jotta tietty toimenpide voidaan toteuttaa. Tässä tapauksessa *ei ole tärkeää tunnistaa tai todentaa henkilöä*, vaan luokitella hänet automaattisesti tiettyyn luokkaan. Esimerkiksi mainostaulu voi näyttää erilaisia mainoksia sen katsojan iän tai sukupuolen perusteella.¹⁰⁶ [korostus lisätty]

Esimerkkejä

Muita esimerkkejä biometrisestä luokittelusta ovat ohjelmistojen käyttö ihmisten automaattiseen luokitteluun etnisen alkuperän tai sukupuolen mukaan tai tekoälyjärjestelmä, joka analysoi henkilön sosiaalisen median kuvia ja olettaa niiden perusteella hänen poliittisen suuntautumisensa ja lähettää hänelle kohdennettuja viestejä tai olettaa niiden perusteella hänen seksuaalisen suuntautumisensa ja lähettää hänelle kohdennettua mainontaa.

Biometrinen luokittelu on profiloinnin muoto.¹⁰⁷ GDPR:n 22 artiklan 1 kohdassa sekä lainvalvontadirektiivin (LED) 11 artiklan 3 kohdassa kielletään jo ennestään profilointiin perustuva välillinen tai välitön syrjintä.

Sen arvioiminen, kuuluuko tekoälyjärjestelmä 5 artiklan 1 kohdan g alakohdan soveltamisalaan, edellyttää viisivaiheista arviointia, jossa arvioidaan seuraavat:

1. Onko tekoälyjärjestelmä saatettu markkinoille, otettu käyttöön tai käytössä?
2. Perustuuko tekoälyjärjestelmä ”biometrisiin tietoihin”?
3. Onko tekoälyjärjestelmä ”biometrinen luokittelujärjestelmä” sellaisena kuin se on määritelty 3 artiklan 40 kohdassa?
4. Luokitellaanko henkilöitä tämän ”biometrisen luokittelujärjestelmän” avulla?
 - a. Onko tekoälyjärjestelmän ensisijainen tarkoitus ”luokitella luonnollisia henkilöitä heidän biometristen tietojensa perusteella tiettyihin ryhmiin”?
5. Käytetäänkö tekoälyjärjestelmää luokittelemaan ihmisiä ”rodun, poliittisten mielteiden, ammattiliiton jäsenyyden, uskonnollisen tai filosofisen vakaumuksen, seksuaalisen käyttäytymisen tai seksuaalisen suuntautumisen perusteella”?

106. 29 artiklan mukainen tietosuojatyöryhmä. Opinion 3/2012 on developments in biometric technologies, WP193, 27. huhtikuuta 2012, s. 6.

107. 29 artiklan mukainen tietosuojatyöryhmä. Suuntaviivat automatisoiduista yksittäispäätöksistä ja profiloinnista asetuksen (EU) 2016/679 täytäntöön panemiseksi, WP251rev.01, 6.2.2018, s. 7. Katso myös GDPR:n 4 artiklan 4 kohta.

Kiellon soveltamisalan ulkopuolelle jäävät seuraavat liitteessä III olevan 1 kohdan b alakohdan mukaiset suuririskiset toimet:

- ▶ ”laillisesti hankittujen biometristen tietoaaineistojen, kuten kuvien, merkitsemistä tai suodattamista biometristen tietojen perusteella lainvalvonta-alalla”¹⁰⁸
- ▶ biometrinen luokittelu, joka on ”toisen kaupallisen palvelun oheistoiminto ja se on ehdottoman välttämätön objektiivisista teknisistä syistä”¹⁰⁹

On kuitenkin huomattava, että tällainen käyttö voi kuitenkin olla kiellettyä GDPR:n ja LED:n nojalla, jos käsittelyn tarkoitus ei ole laillinen tai jos biometristen tietojen käsittelystä johtuva ihmisten perusoikeuksiin puuttuminen ei ole välttämätöntä ja suhteellista.

2.7.2. Yhdenvertaisuuselinten ja kansallisten ihmisoikeustoimijoiden rooli biometriseen luokitteluun liittyvien kieltojen käsittelyssä

- ▶ Koota näyttöä biometrisestä luokittelusta johtuvista syrjinnän haitoista ja jakaa ne markkinavalvontaviranomaisten ja Euroopan komission kanssa 5 artiklan ja liitteen III vuosittaiseen arviointiin osallistumiseksi 112 artiklan mukaisesti konkreettisten esimerkkien avulla. Erityisesti yhdenvertaisuuselimet ja kansalliset ihmisoikeustoimijat voivat tehdä yhteistyötä kansalaisjärjestöjen ja markkinavalvontaviranomaisten kanssa kiinnittääkseen erityistä huomiota lainvalvonnan alalla tapahtuvaan suuririskisten järjestelmien käyttöön, jotka rekisteröidään suuririskisten tekoälyjärjestelmien tietokannan ei-julkiseen versioon (katso 49 artikla).

2.8. Biometrinen etätunnistus

2.8.1. Tausta ja merkitys

Tekoälyasetuksen eri artikloissa käsitellään biometrisiä etätunnistusjärjestelmiä (RBI).¹¹⁰ Liitteessä III olevan 1 kohdan a alakohdan mukaan kaikkia kansallisen tai unionin lainsäädännön nojalla sallittuja biometrisiä etätunnistusjärjestelmiä¹¹¹ pidetään suuririskisinä tekoälyjärjestelminä. Koska biometriset etätunnistusjärjestelmät käsittelevät biometrisiä tietoja, jotka ”kaikissa tilanteissa puuttuvat vakavasti [Euroopan unionin perusoikeuskirjassa taattuihin oikeuksiin]”,¹¹² tällainen puuttuminen edellyttää

108. Tekoälyasetus, 5 artiklan 1 kohdan g alakohta.

109. Tekoälyasetus, 3 artiklan 40 kohta.

110. Tekoälyasetus, 3 artiklan 41 kohta: ”biometrisellä etätunnistusjärjestelmällä” [tarkoitetaan] tekoälyjärjestelmää, jonka avulla luonnolliset henkilöt voidaan tunnistaa ilman heidän aktiivista osallistumistaan – tyypillisesti etäältä – vertaamalla henkilön biometrisiä tietoja viitetietokantaan sisältyviin biometrisiin tietoihin”. Katso myös tekoälyasetuksen 3 artiklan 35 kohta ja tekoälyasetuksen kieltosuuntaviivojen 306 kohta.

111. Tällaisia järjestelmiä voivat olla esimerkiksi kasvojen etätunnistusjärjestelmät, äänen etätunnistusjärjestelmät ja kävelyntunnistusjärjestelmät.

112. EDPB (2022), Ohjeet 05/2022 kasvojentunnistusteknologian käytöstä lainvalvonnan alalla, s. 5.

oikeusperustaa. Kasvon- ja puheentunnistustekniikat ovat kaksi yleistä esimerkkiä biometrisistä etätunnistusjärjestelmistä. Biometrisen tunnistuksen käyttö muihin tarkoituksiin kuin lainvalvontaan on jo nyt yleisesti kielletty.¹¹³

Lainvalvontatarkoituksessa oikeusperustan luomiseksi ei riitä, jos ”lainvalvontadirektiivin 10 artiklan yleinen lauseke vain saatettaisiin osaksi kansallista lainsäädäntöä”¹¹⁴. Myöskään tekoälyasetus ei muodosta oikeusperustaa tällaiselle puuttumiselle.¹¹⁵ Näin ollen biometristen tietojen käsittely, myös biometristen etätunnistusjärjestelmien suorittama käsittely lainvalvontatarkoituksiin, on kielletty EU-maissa, ellei erityistä oikeusperustaa ole. Ainakin kahdessa maassa, Alankomaissa¹¹⁶ ja Italiassa¹¹⁷, ei ole vielä muodostettu tällaista oikeusperustaa.

Reaaliaikaiset biometriset etätunnistusjärjestelmät

Tekoälyasetuksessa erotetaan toisistaan reaaliaikaiset biometriset etätunnistusjärjestelmät ja jälkikäteiset biometriset etätunnistusjärjestelmät.¹¹⁸ Jälkimmäinen määritellään biometriseksi etätunnistusjärjestelmäksi, joka ei ole reaaliaikainen järjestelmä. Reaaliaikaisten biometristen etätunnistusjärjestelmien käyttö voi ”synnyttää tunteen jatkuvasta valvonnasta ja *estää välillisesti kokoontumisvapauden ja muiden perusoikeuksien käyttämisen*”, ja se voi johtaa ikään, etniseen tai rodulliseen alkuperään, sukupuoleen tai vammaisuuteen perustuvaan syrjintään.¹¹⁹

Ongelman ratkaisemiseksi 5 artiklan 1 kohdan h alakohdassa kielletään reaaliaikaisen biometrisen etätunnistusjärjestelmän käyttö *lainvalvontatarkoituksiin* julkisissa tiloissa. Tämä tarkoittaa, että kieltoa ei sovelleta ainoastaan silloin, kun lainvalvontaviranomaiset¹²⁰ käyttävät reaaliaikaista biometristä etätunnistusjärjestelmää, vaan sitä sovelletaan myös silloin, kun jokin muu taho, kuten julkista liikennettä harjoittava yritys tai urheiluseura, käyttää sitä lainvalvontatarkoituksiin. Tällainen tilanne on kyseessä, jos lainvalvontaviranomainen delegoi käyttöönoton näille tahoille.¹²¹

113. Tekoälyasetus, johdanto-osa, 39 kohta. Ks. myös GDPR:n 9 artiklan 1 kohta ja EUDPR:n 10 artiklan 1 kohta.

114. EDPB (2022), Ohjeet 05/2022 kasvojen tunnistusteknologian käytöstä lainvalvonnan alalla, s. 5.

115. Tekoälyasetus, johdanto-osa, 38 kohta.

116. Galič M. and Stevens L. (2023), ”Regulating police use of facial recognition technology in the Netherlands: The complex interplay between criminal procedural law and data protection law”, *New Journal of European Criminal Law* 14(4), 459-78, saatavilla osoitteessa <https://doi.org/10.1177/20322844231212834>, viitattu 10. marraskuuta 2025.

117. ”Garante per la protezione dei dati personali” (2021), *Riconoscimento facciale: Sari Real Time non è conforme alla normativa sulla privacy*, saatavilla osoitteessa www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9575842, viitattu 10. marraskuuta 2025.

118. Tekoälyasetus, 3 artiklan 42 ja 43 kohta. 3 artiklan 42 kohdassa todetaan, että ”reaaliaikaisella biometrisellä etätunnistusjärjestelmällä” [tarkoitetaan] 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”.

119. Tekoälyasetus, johdanto-osa, 32 kohta (*korostus lisätty*)

120. Tekoälyasetus, 3 artiklan 45 kohta.

121. Tekoälyasetus, 3 artiklan 46 kohta: ”lainvalvonnalla” [tarkoitetaan] toimia, joita lainvalvontaviranomaiset toteuttavat tai joita toteutetaan niiden puolesta rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten, mukaan lukien yleiseen turvallisuuteen kohdistuvilta uhkilta suojelu ja tällaisten uhkien ehkäisy”.

Tämän kiellon osalta tekoälyasetusta sovelletaan erityissäännöksenä LED-direktiivin 10 artiklaan.¹²²

Sen arviointi, soveltuuko tekoälyjärjestelmä 5 artiklan 1 kohdan h alakohdan soveltamisalaan edellyttää viisivaiheista arviointia, joka täyttää kaikki seuraavat vaiheet:

1. Onko tekoälyjärjestelmä 3 artiklan 41 kohdan mukainen biometrinen etätunnistusjärjestelmä?
2. Onko biometrinen etätunnistusjärjestelmä käytössä?
 - Tällä viitataan siihen, että kiello koskee ainoastaan käyttöönottajia (eikä toimijoita, kuten muut kiellot).
3. Käytetäänkö biometristä etätunnistusjärjestelmää ”julkisissa tiloissa”?
4. Onko biometrinen etätunnistusjärjestelmä ”reaaliaikainen”?
5. Käytetäänkö reaaliaikaista biometristä etätunnistusjärjestelmää lainvalvontatarkoituksiin?

Tämä kiello ei kuitenkaan ole ehdoton. Reaaliaikaisten biometrinen etätunnistusjärjestelmien käyttö lainvalvontatarkoituksiin *voitaisiin* sallia, jos se on ehdottoman välttämätöntä seuraaviin tarkoituksiin:

1. kolmen erityisen vakavan rikoksen uhrien kohdennettu etsintä¹²³ ja kadonneiden henkilöiden kohdennettu etsintä
2. ihmishenkeen tai fyysiseen turvallisuuteen kohdistuvan välittömän uhan tai todellisen terrori-iskun uhan torjuminen
3. tiettyihin rikoksiin syyllistyneiden epäiltyjen ja rikoksentekijöiden paikantaminen tai tunnistaminen.¹²⁴

Tekoälyasetus ei muodosta oikeusperustaa tällaiselle käytölle. Näissä poikkeustapauksissa reaaliaikaista biometristä etätunnistusjärjestelmää voidaan käyttää lainvalvontatarkoituksiin vain seuraavissa tapauksissa:

- ▶ Annettu kansallinen laki muodostaa oikeusperustan reaaliaikaisen biometrinen etätunnistusjärjestelmän käytölle ja sallii yhden tai useamman kolmesta tapauksesta.
- ▶ Lainvalvontaviranomainen on suorittanut 27 artiklan mukaisen perusoikeusvaikutusten arvioinnin (FRIA) välttämättömyyden ja suhteellisuuden arvioimiseksi.¹²⁵

122. Tekoälyasetus, johdanto-osa, 38 kohta.

123. Nämä kolme vakavaa rikosta ovat kaappaus, ihmiskauppa ja seksuaalinen hyväksikäyttö.

124. Tekoälyasetus, 5 artiklan 1 kohdan h alakohdan iii alakohta: Rikokset kuuluvat soveltamisalaan, jos ne täyttävät seuraavat edellytykset: (1) rikos on lueteltu tekoälyasetuksen liitteessä II, ja (2) ”näistä rikoksista voi asianomaisessa jäsenvaltiossa seurata vapaudenmenetyksen käsittävä rangaistus tai turvaamistoimenpide, jonka enimmäisaika on vähintään neljä vuotta.”

125. Tekoälyasetus, 5 artiklan 2 kohta.

- ▶ Jos lainvalvontaviranomainen (tai sen puolesta toimiva taho) haluaa käyttää reaaliaikaista biometristä etätunnistusjärjestelmää, sen on kunkin käyttö-tarkoituksen osalta täytettävä seuraavat vaatimukset:¹²⁶
 - Se on hankkinut luvan oikeusviranomaiselta tai riippumattomalta hallinto-viranomaiselta, jonka päätös on sitova kyseisessä EU-maassa (paitsi hätä-tilanteessa, jolloin tarvitaan jälkikäteinen hyväksyntä).
 - Se ilmoittaa asiasta markkinavalvontaviranomaiselle (MSA) ja tietosuoja-viranomaiselle (DPA).
 - Se lisää käyttötiedot ei-julkiseen EU:n tietokantaan 49 artiklan 4 kohdan mukaisesti.
- ▶ Tietosuojaviranomaisen ja markkinavalvontaviranomaisen tulee toimittaa Euroopan komissiolle vuosiraportti, jossa ilmoitetaan muun muassa reaali- aikaisen biometrisen etätunnistusjärjestelmän käyttötiheys maassa. Nämä tahot voivat halutessaan lähettää yhteisen raportin.¹²⁷
- ▶ Euroopan komission tulee julkaista tietosuojaviranomaisten ja markkina- valvontaviranomaisten raportteihin pohjautuvat vuosiraportit.¹²⁸

Jos oikeusperustan muodostamiseksi laaditaan kansallinen laki, suuririskisiä teko- älyjärjestelmiä koskevia sääntöjä sovelletaan tällaiseen lainvalvontatarkoituksiin käytettävään käyttöön.

Jos kansallinen lainsäädäntö ei muodosta oikeusperustaa biometrisen etätunnis- tusjärjestelmän käytölle, joka edellyttää ensin oikeusperustaa biometristen tietojen käsittelylle, reaaliaikaisen biometrisen etätunnistusjärjestelmän käyttö julkisissa tiloissa lainvalvontatarkoituksiin on kielletty yleiskiellolla 2. helmikuuta 2025 alkaen. Jäsenvaltioilla ei ole määräaikaa tällaisen kansallisen lain säätämiselle. Tämän raportin kirjoitushetken mennessä yksikään EU-maa ei ole säätänyt tällaista kansallista lakia. EU:n jäsenvaltiot voivat tukea yleiskieltoa siten, että ne eivät säädä asiaa koskevaa kansallista lakia.

Yhteenvetona voidaan todeta, että reaaliaikaiset biometriset etätunnistusjärjestelmät ovat kiellettyjä, ellei kansallinen laki salli niiden käyttöä lainvalvontatarkoituksiin. Tällaisessa laissa käyttö sallitaan tiettyjä tavoitteita varten, ja käytön suhteellisuutta ja välttämättömyyttä tulee tarkastella. Muutoin käyttö on kiellettyä, koska se puuttuu useisiin perusoikeuksiin, kuten oikeuteen syrjimättömyyteen.

126. Tekoälyasetus, 5 artiklan 2–5 kohta.

127. Tekoälyasetus, 5 artiklan 6 kohta.

128. Tekoälyasetus, 5 artiklan 7 kohta.

**Esimerkkitapaus Euroopan ihmisoikeustuomioistuimesta: *Glukhin v. Venäjä*
– hakemusno 11519/20 (2023)**

Poliisi löysi rutiininomaisen Internet-valvonnan aikana julkisella Telegram-kanavalla julkaistuja valokuvia ja videota, joissa kantaja piti yksin mielenosoitusta Moskovan metrossa. Kantajan mukaan poliisi käytti kasvontunnistusteknologiaa hänen tunnistamiseensa kanavan kuvakaappauksista, keräsi videotallenteita Moskovan metroasemille asennetuista valvontakameroista, joiden ohi hän oli kulkenut, ja useita päiviä myöhemmin käytti reaaliaikaista kasvontunnistusteknologiaa hänen paikallistamiseensa ja pidättämiseensä kantajan matkustaessa metrossa.

Kuvakaappauksia käytettiin todisteina hallinnollista rikkomusta koskevissa oikeudenkäynneissä kantajaa vastaan. Kantaja tuomittiin oikeudenkäynneissä.

Euroopan ihmisoikeustuomioistuin totesi, että tapauksessa oli rikottu 10 ja 8 artiklaa.

Kasvontunnistusteknologian käyttö hallinnollisissa oikeudenkäynnissä rauhanomaisen mielenosoittajan tunnistamiseksi, paikantamiseksi ja pidättämiseksi oli omiaan vaikuttamaan lamaannuttavasti sananvapauteen ja oikeuteen kokoontua rauhanomaisesti (10 artikla). Kasvontunnistusteknologian käyttöönotossa tarvitaan seuraavat:

- ▶ toimenpiteiden soveltamisalaa ja käyttöä koskevat tarkat säännöt
- ▶ vahvat suojatoimet väärinkäytösten ja mielivaltaisuuden riskiä vastaan.

Tuomioistuin totesi, että tämä tarve lisääntyi, kun käytettiin reaaliaikaista kasvontunnistusteknologiaa. Vaikka tuomioistuin ei sulkenut pois tällaisen teknologian käyttöä täysin, se totesi, että Glukhinia koskevassa asiassa teknologian käyttö Glukhinin löytämiseksi, paikantamiseksi ja pidättämiseksi ei vastannut ”pakottavaa yhteiskunnallista tarvetta” eikä sitä voitu pitää ”demokraattisessa yhteiskunnassa välttämättömänä”.

Tuomioistuimen New technologies -tiedote:

https://www.echr.coe.int/d/fs_new_technologies_eng

Jälkikäteiset biometriset etätunnistusjärjestelmät (RBI)

Biometrisiä etätunnistusjärjestelmiä, joita ei ole kielletty tekoälyasetuksessa tai muussa kansallisessa tai unionin lainsäädännössä, pidetään suuririskisinä. Määritelmän mukaan näihin kuuluvat kaikki kansallisen tai unionin lainsäädännön nojalla sallitut jälkikäteiset biometriset etätunnistusjärjestelmät (sallittujen reaaliaikaisten biometristen etätunnistusjärjestelmien lisäksi).

Näihin jälkikäteisiin biometrisiin etätunnistusjärjestelmiin sovelletaan kaikkia suuririskisiä tekoälyjärjestelmiä koskevia sääntöjä. Jälkikäteisten biometristen etätunnistusjärjestelmien käyttö lainvalvonnassa sisältää käyttöönottajille *lisävelvoitteen*.

Jälkikäteisten biometristen etätunnistusjärjestelmien, jotka on tarkoitettu "[r]ikoksesta epäillyn tai tuomitun henkilön kohdennett[uun] etsintää[n]"¹²⁹, käyttöönottajien on saatava lupa järjestelmän käyttöön oikeusviranomaiselta tai riippumattomalta hallintoviranomaiselta, jonka päätös on sitova kyseisessä EU-maassa. Tällainen lupa on hankittava vähintään 48 tuntia ennen jokaista järjestelmän käyttökertaa. Kukin tällainen käyttökerta on "rajoitettava siihen, mikä on ehdottoman välttämätöntä kyseessä olevan rikoksen tutkintaa varten".¹³⁰

2.8.2. Yhdenvertaisuuselinten ja muiden kansallisten ihmisoikeustoimijoiden rooli biometriseen etätunnistukseen liittyvien kieltojen käsittelyssä

- Hallituksia on kannustettava pitämään voimassa yleinen kieltä käyttä reaaliaikaisia biometrisiä etätunnistusjärjestelmiä lainvalvontatarkoituksiin.

129. Tekoälyasetus, 26 artiklan 10 kohta.

130. Tekoälyasetus, 26 artiklan 10 kohta.



3. Suuririskiset tekoälyjärjestelmät

3.1. Suuririskisten tekoälyjärjestelmien luokittelu

3.1.1. Tausta ja merkitys

Tekoälyasetuksen 6 artiklassa kuvataan säännöt asetuksen soveltamisalaan kuuluvien suuririskisten tekoälyjärjestelmien luokitteluun. Erityisen merkityksellisiä yhdenvertaisuuselinten kannalta ovat liitteessä III luetellut sovellukset, jotka kattavat seuraavat alat:

- ▶ biometriikka¹³¹
- ▶ kriittinen infrastruktuuri (digitaalinen infrastruktuuri, tieliikenne ja vesi-, kaasuja sähköhuolto)¹³²
- ▶ yleissivistävä ja ammatillinen koulutus¹³³

131. Tekoälyasetus, liitteessä III oleva kohta 1 ja johdanto-osan kappale 54.

132. Tekoälyasetus, liitteessä III oleva kohta 2 ja johdanto-osan kappale 55.

133. Tekoälyasetus, liitteessä III oleva kohta 3 ja johdanto-osan kappale 56.

- ▶ työllistäminen, henkilöstöhallinto ja itsenäisen ammatinharjoittamisen mahdollistaminen¹³⁴
- ▶ välttämättömien yksityisten palvelujen ja välttämättömien julkisten palvelujen ja etuuksien saatavuus ja käyttö (esimerkiksi sosiaaliturva, luottopisteytys, vakuutukset, terveydenhuolto ja hätäpalvelut)¹³⁵
- ▶ lainvalvonta¹³⁶
- ▶ muuttoliikkeen hallinta, turvapaikka-asiat ja rajavalvonta¹³⁷
- ▶ oikeudenhoito ja demokraattiset prosessit.¹³⁸

Tekoälyasetuksen näitä aloja koskevissa johdanto-osan kappaleissa korostetaan, että riskin käsite ei rajoitu pelkästään teknologisiin ominaisuuksiin, vaan se on tiiviisti sidoksissa yhteiskunnalliseen kontekstiin, ja varoitetaan mahdollisuudesta lisätä rakenteellista eriarvoisuutta.

Muihin tekoälyjärjestelmiin verrattuna suuririskisiin tekoälyjärjestelmiin sovelletaan enemmän dokumentointi-, laadunvarmistus- ja avoimuusvelvoitteita, joiden tarkoituksena on torjua syrjintää.

Näiden alojen tekoälyjärjestelmien tarjoajat voivat kuitenkin luokitella järjestelmän muuksi kuin suuririskiseksi, jos katsotaan, että järjestelmä ei aiheuta ”merkittävää riskiä” (katso jäljempää). Näin ollen järjestelyn ulkopuolelle jättäytyvien tarjoajien ei tarvitse noudattaa suuririskisiä järjestelmiä koskevia velvoitteita.

Tämä poisjättäytyminen perustuu tarjoajien itsearviointeihin, joita tarjoajat eivät ole velvollisia julkaisemaan (katso jäljempää). Tämä aiheuttaa riskin siitä, että tiettyjä sääntelemättömiä suuririskisiä tekoälyjärjestelmiä käytetään virheellisesti muina kuin suuririskisinä.

Liitteessä III luetelluilla aloilla käytettäviä tekoälyjärjestelmiä koskevat suuririskisten tekoälyjärjestelmien säännöt tulevat voimaan elokuussa 2026. Tekoälytoimiston odotetaan laativan suuntaviivat tekoälyjärjestelmien luokittelulle suuririskisiksi järjestelmiksi 2. helmikuuta 2026 mennessä.¹³⁹ Suuntaviivojen tulisi sisältää ”käytännön esimerk[kejä] sellaisten tekoälyjärjestelmien käyttötapauksista, jotka ovat suuririskisiä ja muita kuin suuririskisiä”.¹⁴⁰ Suuririskisten tekoälyjärjestelmien luokittelusääntöjä koskevan 6 artiklan 6–8 kohdan mukaan delegoiduilla säädöksillä voidaan lisätä, poistaa tai muuttaa 6 artiklan 3 kohdan ehtoja, mutta ne ”eivät saa heikentää tässä asetuksessa säädetyn terveyden, turvallisuuden ja perusoikeuksien suojelun yleistä tasoa”.¹⁴¹

134. Tekoälyasetus, liitteessä III oleva kohta 4 ja johdanto-osan kappale 57.

135. Tekoälyasetus, liitteessä III oleva kohta 5 ja johdanto-osan kappale 58.

136. Tekoälyasetus, liitteessä III oleva kohta 6 ja johdanto-osan kappale 59.

137. Tekoälyasetus, liitteessä III oleva kohta 7 ja johdanto-osan kappale 60.

138. Tekoälyasetus, liitteessä III oleva kohta 8 ja johdanto-osan kappale 61.

139. Tekoälyasetus, 6 artiklan 5 kohta.

140. Ibid.

141. Tekoälyasetus, 6 artiklan 8 kohta.

Merkittävä riski ja poisjättäytymisen ehdot

Vaikka termiä ”merkittävä riski” ei ole määritelty tekoälyasetuksessa, sen voidaan tulkita vaikuttavan haitallisesti perusoikeuksiin, joihin kuuluvat ”oikeus ihmisarvoon, yksityis- ja perhe-elämän kunnioittaminen, henkilötietojen suoja, sananvapaus ja tiedonvälityksen vapaus, kokoontumis- ja yhdistymisvapaus, oikeus syrjimättömyyteen, oikeus koulutukseen, kuluttajansuoja, työntekijöiden oikeudet, vammaisten oikeudet, *sukupuolten tasa-arvo*, teollis- ja tekijänoikeudet, oikeus tehokkaisiin oikeussuojakeinoihin ja puolueettomaan tuomioistuimeen, oikeus puolustukseen ja syyttömyysolettama sekä oikeus hyvään hallintoon”¹⁴² sekä lasten oikeudet ja oikeus korkeaan ympäristönsuojelun tasoon.¹⁴³ Arvioinnissa voidaan ottaa huomioon haitan vakavuus ja todennäköisyys.

”Merkittävää riskiä” on arvioitava erityisesti niiden neljän ehdon suhteen, joihin tekoälyjärjestelmien tarjoajat voivat vedota jättäessään järjestelmän vaatimusten ulkopuolelle:¹⁴⁴

- a. tekoälyjärjestelmän tarkoituksena on suorittaa suppea menettelyllinen tehtävä (esimerkiksi tekoälyjärjestelmä, joka luokittelee saapuvat asiakirjat eri luokkiin)
- b. tekoälyjärjestelmän tarkoituksena on parantaa aiemmin suoritettua ihmisen toiminnan tulosta (esimerkiksi tekoälyjärjestelmä, jonka tarkoituksena on parantaa aiemmin laadituissa asiakirjoissa käytettyä kieltä)
- c. tekoälyjärjestelmän tarkoituksena on havaita päätöksentekotapoja tai poikkeamia aiemmista päätöksentekotavoista, eikä sen tarkoituksena ole korvata aiemmin tehtyä ihmisen tekemää arviota tai vaikuttaa siihen ilman asianmukaista ihmisen suorittamaa arviota (esimerkiksi tekoälyjärjestelmät, joiden avulla voidaan ”tietyn opettajan arvostelutapojen pohjalta tarkistaa jälkikäteen, onko kyseinen opettaja mahdollisesti poikennut arvostelutavoista”)
- d. tekoälyjärjestelmä on tarkoitettu suorittamaan valmistelutehtävä, joka koskee liitteessä III lueteltujen käyttötapauksen kannalta merkityksellistä arviointia (esimerkiksi alkuperäisten asiakirjojen kääntämiseen käytettävät tekoälyjärjestelmät).

EU:n tietosuojalainsäädännössä määriteltyä ”profilointia”¹⁴⁵ pidetään jo nyt ”merkittävänä riskinä”. Liitteen III mukaisia tekoälyjärjestelmiä, joita käytetään profilointiin, pidetään aina suuririskisinä.¹⁴⁶

Suuririskisten tekoälyjärjestelmien järjestelyn ulkopuolelle jättäytymisen seuraukset

1. Jos tekoälyjärjestelmien tarjoajat päättävät itse jättäytyä järjestelyn ulkopuolelle, niiden on

142. Tekoälyasetus, johdanto-osan kappale 48. (*Korostus lisätty*)

143. EU:n perusoikeuskirja, 37 artikla.

144. Tekoälyasetus, 6 artiklan 3 kohta ja johdanto-osan kappale 53. Nämä ehdot eivät estä tekoälyjärjestelmän kieltämistä.

145. GDPR, 4 artiklan 4 kohta, ja direktiivi lainvalvontatarkoituksessa käsiteltävien henkilötietojen suojasta, 3 artiklan 4 kohta.

146. Tekoälyasetus, 6 artiklan 3 kohdan kolmas alakohta.

- dokumentoitava tiivistelmä syistä, joiden perusteella tekoälyjärjestelmän ei katsota olevan suuririskinen, ennen järjestelmän saattamista markkinoille tai käyttöönottoa
 - rekisteröitävä järjestelmä EU:n tietokantaan 49 artiklan 2 kohdan, 71 artiklan ja liitteessä VIII olevan B jakson tietojen mukaisesti. Vaaditut tiedot eivät ole yhtä yksityiskohtaisia kuin liitteessä VIII olevassa A jaksossa (49 artiklan 1 kohdan mukaisesti) vaaditut tiedot suuririskisille järjestelmille. Tietoihin sisältyy kuitenkin "[t]ämän asetuksen 6 artiklan 3 kohdan mukainen edellytys tai sen mukaiset edellytykset, joiden perusteella tekoälyjärjestelmän ei katsota olevan suuririskinen".¹⁴⁷
2. Tekoälyjärjestelmien tarjoajien ei tarvitse julkaista itsearviointejaan. Niitä pyydetään kuitenkin toimittamaan arviointiasiakirjat pyynnöstä kansallisille toimivaltaisille viranomaisille.¹⁴⁸
 3. Markkinavalvontaviranomaiset voivat arvioida tekoälyjärjestelmiä määrittääkseen, ovatko tekoälyjärjestelmät suuririskisiä, ja tarvittaessa vaatia tarjoajaa toteuttamaan korjaavia toimia.¹⁴⁹ Markkinavalvontaviranomainen voi sakottaa tarjoajaa, jos tarjoaja luokittelee tekoälyjärjestelmän virheellisesti muuksi kuin suuririskiseksi järjestelmäksi tekoälyasetuksen vaatimusten kiertämiseksi.¹⁵⁰ (Katso [77 artikla](#).)

Riskien vähentämiskäytäntöihin liittyvät ongelmat

Järjestelyn ulkopuolelle jättäytymisen itsearvioinnin, "merkittävän riskin" määritelmän puuttuminen ja 6 artiklan 3 kohdassa kuvattujen ehtojen yhdistelmä luo riskin, että tarjoajat ryhtyvät "riskien vähentämiskäytäntöihin". Tämä tarkoittaa, että tarjoajat jättäytyvät suuririskisten järjestelmien luokittelun ulkopuolelle, vaikka järjestelmät todellisuudessa aiheuttavat merkittävän riskin, ja välttävät siten suuririskisille tekoälyjärjestelmille asetetut velvoitteet.

Käytännön esimerkkien kattavan luettelon puuttuminen tällä hetkellä lisää tätä riskiä. Esimerkiksi ansioluetteloiden analysointiin käytettävät tekoälyjärjestelmät,¹⁵¹ jotka voivat vaikuttaa siihen, kuka pääsee työhaastatteluun, voivat jäädä sääntelemättä, jos niitä pidetään suppeana menettelyllisenä tai valmistelevana tehtävänä. Sama koskee tekoälyjärjestelmää, jota käytetään turvapaikkahakemuksiin liittyvien asiakirjojen kääntämiseen. Tällaiset järjestelmät eivät välttämättä käännä kaikkia kieliä riittävän hyvin, mikä voi johtaa väärinkäsityksiin ja haitallisiin vaikutuksiin

147. Liite VIII, jaksossa B oleva 6 kohta.

148. Tekoälyasetus, 6 artiklan 4 kohta. Yhdenvertaisuuselimillä ei pidetä tekoälyasetuksen 6 artiklan 4 kohdassa tarkoitettuina kansallisina toimivaltaisina viranomaisina. Yhdenvertaisuuselimillä on kuitenkin mahdollisuus saada samat tiedot niiden valtuuksien nojalla, jotka on kuvattu tekoälyasetuksen 77 artiklassa. Lisäksi yhdenvertaisuuselimien normeja koskevien direktiivien 8 artiklassa niille annetaan tutkintavaltuudet ja oikeus saada tietoja toimeksiantonsa täyttämiseksi.

149. Tekoälyasetus, 80 artiklan 1–2 kohta.

150. Tekoälyasetus, 80 artiklan 7 kohta.

151. HrFlow.ai, saatavilla osoitteessa <https://hrflow.ai/parsing/>, viitattu 12. marraskuuta 2025.

turvapaikanhakijoiden kannalta.¹⁵² Näin ollen yhdenvertaisuuselimet ja kansalliset ihmisoikeustoimijat ovat keskeisessä asemassa varmistettaessa, ettei suuririskisiä tekoälyjärjestelmiä koskevia velvoitteita kierretä. Näiden elinten on osallistuttava tulevien suuntaviivojen ja delegoitujen säädösten laadintaan.

3.1.2. Yhdenvertaisuuselinten ja kansallisten ihmisoikeustoimijoiden rooli suuririskisten tekoälyjärjestelmien luokittelussa

- ▶ Arvioida suuririskisten järjestelmien järjestelyn ulkopuolelle jäävien tarjoajien itsearvioinneissa annettuja tietoja sen varmistamiseksi, voidaanko annettujen tietojen perusteella analysoida asianmukaisesti yhdenvertaisuuteen ja syrjimättömyyteen kohdistuvia vaikutuksia.
- ▶ Laatia luettelo tekoälyjärjestelmistä, joiden tarjoajat ovat jättäytyneet 6 artiklan 3 kohdan mukaisen suuririskisten järjestelmien järjestelyn ulkopuolelle mutta joihin liittyy merkittävä riski. Tällaisia esimerkkejä voidaan kerätä suuririskisten tekoälyjärjestelmien EU:n tietokannasta,¹⁵³ yhdenvertaisuuselinten saamista valituksista ja kansalaisjärjestöjen kanssa tehdystä yhteistyöstä saaduista tiedoista (katso yhteistyötä koskeva kohta).
- ▶ Julkaista tämä luettelo ja viestiä siitä suoraan markkinavalvonta- ja tietosuoja-viranomaisille sekä Euroopan komissiolle tietoisuuden lisäämiseksi ja Euroopan komission suuntaviivojen kehittämiseksi.
- ▶ Kehittää ohjeita tekoälyjärjestelmien aiheuttamista syrjintä- ja yhdenvertaisuusriskeistä. Ohjeet voidaan laatia edellä mainitun esimerkkiluettelon perusteella.
- ▶ Yhdenvertaisuuselinten on tehtävä yhteistyötä markkinavalvontaviranomaisten kanssa ja avustettava niitä, kun arvioidaan, aiheuttaako suuririskisten järjestelmien järjestelyn ulkopuolelle jätetty tekoälyjärjestelmä merkittävän riskin perusoikeuksille.

3.2. Suuririskisten käyttötapauksen luettelon muuttaminen

3.2.1. Tausta ja merkittävyys

Tekoälyasetuksen 7 artiklan mukaisesti Euroopan komissiolla on valta antaa delegoituja säädöksiä

1. **liitteen III** muuttamiseksi lisäämällä siihen suuririskisiä tekoälyjärjestelmiä koskevia käyttötapauksia tai muokkaamalla niitä¹⁵⁴

152. Bhuiyan J. (2023), "Lost in AI translation: growing reliance on language apps jeopardizes some asylum applications", *The Guardian*, saatavilla osoitteessa www.theguardian.com/us-news/2023/sep/07/asylum-seekers-ai-translation-apps, viitattu 10. marraskuuta 2025.

153. On epäselvää, onko yhdenvertaisuuselimillä oikeus tarkastella tietokannan ei-julkista osaa.

154. Tekoälyasetus, 7 artiklan 1 kohdan ensimmäinen alakohta.

2. **liitteessä III** olevan luettelon muuttamiseksi poistamalla siitä suuririskisiä tekoälyjärjestelmiä.¹⁵⁵

Näiden kahden vaihtoehdon välisen eron ymmärtämiseksi voi olla hyödyllistä tarkastella liitteessä III olevaa esimerkkiä:¹⁵⁶

Työllistäminen, henkilöstöhallinto ja itsenäisen ammatinharjoittamisen mahdollistaminen:

- (a) Tekoälyjärjestelmät, jotka on tarkoitettu käytettäväksi luonnollisten henkilöiden rekrytoinnissa tai valinnassa, erityisesti kohdennettujen työpaikkailmoitusten esittämiseen, työhakemusten analysointiin ja suodattamiseen sekä hakijoiden arviointiin.
- (b) Tekoälyjärjestelmät, jotka on tarkoitettu käytettäväksi työsuhteen ehtoja, uralla etenemistä ja työhön liittyvien sopimussuhteiden päättämistä koskevien päätösten tekemiseen, tehtävien jakamiseen yksilöllisen käytöksen tai personallisuuspiirteiden tai henkilön ominaisuuksien perusteella tai tällaisissa suhteissa olevien henkilöiden suorituksen ja käyttäytymisen seurantaan ja arviointiin.

Tässä esimerkissä tekoälyjärjestelmä katsotaan suuririskiseksi ”työllistämi[sen], henkilöstöhallin[non] ja itsenäisen ammatinharjoittamisen mahdollistami[sen]” alalla kahdessa a ja b alakohdassa olevassa käyttötapauksessa.

Suuririskisten käyttötapausten lisäys tai muuttaminen

Komissio voi delegoiduilla säädöksillä muuttaa mitä tahansa a ja b alakohdissa esitettyistä käyttötapauksista tai lisätä uusia käyttötapauksia lisäämällä c, d jne. alakohtien järjestelmiä tekoälyjärjestelmiin, jotka ”aiheuttavat terveys- ja turvallisuushaitan riskin tai perusoikeuksiin kohdistuvan kielteisen vaikutuksen riskin, joka on vähintään yhtä suuri kuin liitteessä III jo tarkoitettujen suuririskisten tekoälyjärjestelmien aiheuttaman haitan tai kielteisen vaikutuksen riski”.¹⁵⁷ Komissio ei kuitenkaan voi lisätä uutta alaa liitteessä III lueteltuihin kahdeksaan suuririskisten tekoälyjärjestelmien aloihin.

Suuririskisten käyttötapausten poisto

Jos komissio katsoo delegoidussa säädöksessä, että tekoälyjärjestelmien käyttö ”työllistämi[sen], henkilöstöhallin[non] ja itsenäisen ammatinharjoittamisen mahdollistami[sen]” alalla ei enää aiheuta merkittäviä riskejä eikä heikennä perusoikeuksien, terveyden tai turvallisuuden suojelua,¹⁵⁸ tällä alalla käytetyt tekoälyjärjestelmät ja kaikki käyttötapaukset voidaan poistaa liitteestä III.

Jos komissio haluaa lisätä tai muuttaa käyttötapauksia tai poistaa suuririskisiä tekoälyjärjestelmiä liitteestä III, sen on otettava huomioon monia kriteerejä. Näitä ovat seuraavat:¹⁵⁹

- ▶ ”tekoälyjärjestelmän käsittelemien ja käyttämien tietojen luonne ja määrä”
- ▶ ”missä määrin ihmisen on mahdollista kumota [tekoälyjärjestelmän] päätös tai suositukset, jotka voisivat aiheuttaa mahdollista haittaa”

155. Tekoälyasetus, 7 artiklan 3 kohdan ensimmäinen alakohta.

156. Tekoälyasetus, liitteessä III oleva 4 kohta.

157. Tekoälyasetus, 7 artiklan 1 kohdan b alakohta.

158. Tekoälyasetus, 7 artiklan 3 kohdan a ja b alakohta.

159. Tekoälyasetus, 7 artiklan 2 kohta.

- ▶ nykyinen näyttö tai "missä määrin tekoälyjärjestelmän käyttö on... herättänyt merkittävää huolta tällaisen haitan tai kielteisen vaikutuksen todennäköisyydestä" perusoikeuksille, "mikä käy ilmi esimerkiksi kansallisille toimivaltaisille viranomaisille toimitetuista raporteista tai dokumentoiduista väitteistä taikka muista asianmukaisista raporteista"
- ▶ mahdollinen haitallinen vaikutus perusoikeuksiin ja "tällaisen haitan tai tällaisen haitallisen vaikutuksen mahdollinen laajuus, erityisesti sen voimakkuus ja kyky vaikuttaa useisiin henkilöihin tai vaikuttaa suhteettomasti erityiseen henkilöryhmään"
- ▶ riippuvuuden laajuus: "missä määrin henkilöt, joille mahdollisesti aiheutuu haittaa tai joihin mahdollisesti kohdistuu kielteinen vaikutus, ovat riippuvaisia tekoälyjärjestelmän tuottamasta tuloksesta, erityisesti koska käytännöllisistä tai oikeudellisista syistä ei ole kohtuudella mahdollista olla noudattamatta tätä tulosta"
- ▶ vallan epätasapaino: "missä määrin henkilöt, joille mahdollisesti aiheutuu haittaa tai kohdistuu kielteinen vaikutus, ovat haavoittuvassa asemassa tekoälyjärjestelmän käyttöönottajaan nähden, erityisesti aseman, valta-aseman, tietämyksen, taloudellisten tai sosiaalisten olosuhteiden tai iän vuoksi"
- ▶ tekoälyjärjestelmän avulla tuotetun tuloksen korjattavuus tai peruutettavuus, "kun otetaan huomioon korjaukseen tai peruuttamiseen käytettävissä olevat tekniset ratkaisut, jolloin tulosten, joilla on haitallisia vaikutuksia terveyteen, turvallisuuteen tai perusoikeuksiin, ei katsota olevan helposti korjattavissa tai peruutettavissa"
- ▶ missä määrin voimassa olevassa unionin oikeudessa (ei kansallisessa lainsäädännössä) säädetään "tekoälyjärjestelmän aiheuttamiin riskeihin liittyvistä tehokkaista oikeussuojakeinoista, lukuun ottamatta vahingonkorvausvaateita", ja "tehokkaista toimenpiteistä kyseisten riskien ehkäisemiseksi tai vähentämiseksi merkittävästi".

Nämä kriteerit osoittavat selvästi, että perusoikeudet ja syrjimättömyys ovat keskeisiä kaikissa liitteen III muutoksissa.

3.2.2. Yhdenvertaisuuselinten ja kansallisten ihmisoikeustoimijoiden rooli suuririskisten käyttötapauksen luettelon muuttamisessa

- ▶ Dokumentoida ja julkaista raportteja, joissa tuodaan esiin tekoälyjärjestelmien haitalliset vaikutukset perusoikeuksiin. Raporteissa on erotettava toisistaan
 1. tekoälyjärjestelmät, jotka on jo luokiteltu liitteessä III suuririskisiksi
 2. käyttötarkoitukset, joita ei ole vielä lueteltu liitteessä III, mukaan lukien 6 artiklan 3 kohdan mukaiset vapautetut käyttötarkoitukset.
- ▶ Kohdan 1 näyttö korostaa, että on tärkeää säilyttää liitteessä III olevat suuririskisten tekojärjestelmien alueet eikä poistaa niitä. Kohdan 2 näyttö korostaa tarvetta muuttaa liitteessä III olevia käyttötapaauksia tai lisätä niitä siihen. Kohdan 2 osalta yhdenvertaisuuselinten on priorisoitava tekoälyjärjestelmät,

joiden käyttötapauksissa on vallan tasapainoa käyttöönottajien, kuten viranomaisten, ja asianosaisten henkilöiden välillä. Tämä tarkoittaa tilannetta, jossa henkilöillä ei ole mahdollisuutta olla käyttämättä järjestelmiä (esimerkiksi muuttoliikkeen hallinta tai maan sosiaaliturvajärjestelmä) ja jossa perusoikeuksia loukkaavien päätösten lopputulosta ei voida helposti peruuttaa. Tällaiset raportit voivat perustua kansalaisjärjestöjen keräämään näyttöön erityisesti järjestelmistä, joita ei vielä ole lueteltu liitteessä III. Kansalaisjärjestöistä voi olla apua myös ensisijaisten tutkimus- ja selvitysalueiden määrittämisessä.

- ▶ Lähettää nämä raportit jäsenvaltioiden kansallisille toimivaltaisille viranomaisille tietoisuuden lisäämiseksi sekä Euroopan komissiolle, jotta ne otetaan huomioon, kun komissio suunnittelee delegoitujen säädösten laatimista ja hyväksymistä.
- ▶ Suorittaa tai teettää tutkimusta, jossa tuodaan esiin unionin lainsäädännön puutteet tekoälyjärjestelmien käytöstä johtuvien syrjintäriskien "ehkäisemiseksi tai vähentämiseksi merkittävästi"¹⁶⁰ sekä tehokkaiden oikeussuojamekanismien tarjoamiseksi henkilöille, joita tekoälyjärjestelmän aiheuttamat riskit koskevat, komission huomioitavien kriteerien mukaisesti. Tällaista tutkimusta voidaan tehdä yhteistyössä eri yhdenvertaisuuselinten kesken kansallisten tasa-arvoelinten eurooppalaisen verkoston (Equinet) mahdollisen koordinoinnin kautta.

3.3. Riskinhallintajärjestelmän vaatimukset

3.3.1. Tausta ja merkitys

Tekoälyasetuksen 9 artiklassa edellytetään, että suuririskisten tekoälyjärjestelmien tarjoajat perustavat ja panevat täytäntöön riskinhallintajärjestelmän sekä dokumentoivat ja pitävät sitä yllä "suuririskisen tekoälyjärjestelmän koko elinkaaren ajan", ja järjestelmää "on säännöllisesti ja järjestelmällisesti tarkastettava ja saatettava ajan tasalle".¹⁶¹ Tämän on sisällettävä seuraavat:

- ▶ "[N]iiden tunnettujen ja kohtuudella ennakoitavissa olevien riskien tunnistaminen ja analysointi",¹⁶² joita suuririskinen tekoälyjärjestelmä voi aiheuttaa perusoikeuksille, ja erityisesti "haitallinen vaikutus alle 18-vuotiaisiin henkilöihin ja tarvittaessa muihin haavoittuvassa asemassa oleviin ryhmiin".¹⁶³ Myös käyttöönoton jälkeen syntyvät riskit on arvioitava.¹⁶⁴
- ▶ "[S]ellaisten asianmukaisten ja kohdennettujen riskinhallintatoimenpiteiden hyväksyminen, joiden tarkoituksena on puuttua... tunnistettuihin riskeihin"¹⁶⁵ siten, että "suuririskisten tekoälyjärjestelmien kokonaisujohtamisen riskin katsotaan olevan hyväksyttävällä tasolla".¹⁶⁶ Näihin toimenpiteisiin kuuluvat seuraavat:

160. Tekoälyasetus, 7 artiklan 2 kohdan k alakohdan ii alakohta.

161. Tekoälyasetus, 9 artiklan 1 kohta.

162. Tekoälyasetus, 9 artiklan 2 kohdan a alakohta.

163. Tekoälyasetus, 9 artiklan 9 kohta.

164. Tekoälyasetus, 9 artiklan 2 kohdan c alakohta.

165. Tekoälyasetus, 9 artiklan 2 kohdan d alakohta.

166. Tekoälyasetus, 9 artiklan 5 kohdan ensimmäinen alakohta.

- ”määritettyjen ja arvioitujen riskien poistaminen tai vähentäminen siinä määrin kuin se on teknisesti mahdollista suuririskisen tekoälyjärjestelmän asianmukaisella suunnittelulla ja kehittämisellä”¹⁶⁷
- ”asianmukaisten riskinvähentämis- ja valvontatoimenpiteiden toteuttaminen sellaisiin riskeihin puuttumiseksi, joita ei voida poistaa”¹⁶⁸
- avoimuus ja tiedotus käyttöönottajille.¹⁶⁹

On tärkeää korostaa, että 9 artiklassa ”tarkoitettut riskit koskevat ainoastaan niitä, joita voidaan kohtuudella lieventää ja poistaa suuririskisen tekoälyjärjestelmän kehittämisen tai suunnittelun avulla tai asianmukaisten teknisten tietojen antamisella”.¹⁷⁰ EU:n perusoikeuskirjan 52 artiklan 1 kohdassa todetaan kuitenkin, että ”[t]ässä perusoikeuskirjassa tunnustettujen oikeuksien ja vapauksien käyttämisestä voidaan rajoittaa ainoastaan lailla, ja kyseisten oikeuksien ja vapauksien olennaista sisältöä noudattaen” ja ”[s]uhteellisuusperiaatteen mukaisesti rajoituksia voidaan tehdä ainoastaan, jos ne ovat välttämättömiä ja vastaavat tosiasiallisesti unionin tunnustamia yleisen edun mukaisia tavoitteita tai tarvetta suojella muiden henkilöiden oikeuksia ja vapauksia”. Kaiken kaikkiaan on mahdollista, että syrjintään liittyviä haittoja ei voida perustellusti sisällyttää 9 artiklan mukaisiin riskinhallintajärjestelmiin, jos niitä ei voida lieventää tai poistaa teknisin keinoin. Lieventämättömät ja jatkuvat riskit on kuitenkin sisällytettävä tekniseen dokumentaatioon tekoälyasetuksen 11 artiklan mukaisesti.¹⁷¹ Näin on erityisesti siksi, että syrjinnän jäännösriski ei välttämättä ole hyväksyttävä.

Yhteys muihin oikeudellisiin kehyksiin

Euroopan neuvoston puiteyleissopimuksen 16 artiklassa määrätään myös riskin- ja vaikutustenhallintajärjestelmän käyttöönotosta ja ylläpitämisestä. Tätä varten Euroopan neuvosto on kehittänyt ”menetelmä[n], jolla varmistetaan yhdenmukainen lähestymistapa [tekoälyjärjestelmien] riskien tunnistamiseen, analysointiin ja arviointiin sekä vaikutusten arviointiin ihmisoikeuksien toteutumisen, demokratian toiminnan ja oikeusvaltioperiaatteiden noudattamisen kannalta”. Tähän menetelmään viitataan nimellä HUDERIA.¹⁷² HUDERIA-menetelmässä ehdotetaan kontekstiin perustuvan riskianalyysin ja sidosryhmien sitouttamisprosessin kautta tehtävää riskien ja vaikutusten arviointia, jossa käytetään erilaisia elementtejä ”riskien ja vaikutusten tunnistuksen, arvioinnin, ehkäisyn ja lieventämisen porrastetulla ja eriytetyllä lähestymistavalla suhteessa siihen, kuinka vakavia ja todennäköisiä ihmisoikeuksiin, demokratiaan ja oikeusvaltioperiaatteen kohdistuvat riskit ja vaikutukset ovat”.

167. Tekoälyasetus, 9 artiklan 5 kohdan a alakohta.

168. Tekoälyasetus, 9 artiklan 5 kohdan b alakohta.

169. Tekoälyasetus, 9 artiklan 5 kohdan c alakohta.

170. Tekoälyasetus, 9 artiklan 3 kohta.

171. Tekoälyasetus, 11 artikla ja liitteessä IV olevan 2 kohdan g alakohta ja kohta 3.

172. Euroopan neuvoston tekoälykomitea (2022), *Outline of Huderia risk and impact assessment methodology*, Strasbourg, saatavilla osoitteessa <https://rm.coe.int/cai-bu-2022-03-outline-of-huderia-risk-and-impact-assessment-methodology/1680a81e14>, viitattu 10. marraskuuta 2025; ja Euroopan neuvoston tekoälykomitea (2024), ”Methodology for the risk and impact assessment of artificial intelligence systems from the point of view of human rights, democracy and the rule of law (Huderia methodology)”, Euroopan neuvosto, Strasbourg, saatavilla osoitteessa <https://rm.coe.int/cai-2024-16rev2-methodology-for-the-risk-and-impact-assessment-of-arti/1680b2a09f>, viitattu 10. marraskuuta 2025.

Menetelmässä myös edellytetään arvioinnin iteratiivista tarkistusta. Se ei kuitenkaan ole oikeudellisesti sitova eikä puiteyleissopimuksen tulkintaohjeiden lähde, eikä HUDERIAN noudattaminen ole pakollista puiteyleissopimuksen velvoitteiden täyttämiseksi.

3.3.2. Yhdenvertaisuuselinten ja kansallisten ihmisoikeustoimijoiden rooli riskinhallintajärjestelmien vaatimuksissa

- ▶ Tehdä yhteistyötä oikeustieteilijöiden kanssa sen selvittämiseksi, kuuluvatko syrjintähaitat 9 artiklan soveltamisalaan, kun otetaan huomioon viittaukset hyväksyttävään jäännösrisktiin ja riskeihin, joihin voidaan puuttua teknisin keinoin. Tällainen yhteistyö on hyödyllistä siihen saakka, että unionin tuomioistuin antaa asiasta oikeudellisesti sitovan tulkinnan.
- ▶ Laatia väliaikaiset ohjeet siitä, onko syrjinnän riski sisällytettävä 9 artiklan mukaiseen riskinarvointiin. Tällaiseen ohjeeseen voi sisältyä vaatimus selittää riskin tunnistus, riskin arviointi ja asianmukaisten riskinhallintatoimenpiteiden toteuttaminen.
- ▶ Väliaikaisissa ohjeissa on selvennettävä, että suuririskisen tekoälyjärjestelmän tunnistetut syrjintäriskit on sisällytettävä tekniseen dokumentaatioon, vaikka niitä ei voitaisi lieventää.

3.4. Datanhallinnan vaatimukset

3.4.1. Tausta ja merkitys

Data on olennainen osa tekoälyjärjestelmien kehittämistä. Asetuksen 10 artiklassa säädetään suuririskisten tekoälyjärjestelmien tarjoajien datanhallintavelvoitteista. Tarjoajat voivat täyttää nämä velvoitteet suunnittelemalla oman lähestymistapansa, tekninen toteutus mukaan luettuna. Valitusta lähestymistavasta riippumatta näiden velvoitteiden täyttäminen on välttämätöntä, mutta se ei kuitenkaan yksin riitä tekoälyjärjestelmien syrjimättömyysriskien rajoittamiseen. Tämä johtuu siitä, että data on vain yksi tekoälyjärjestelmien vinoumien ja syrjinnän lähteistä. Tekoälyjärjestelmät voivat olla syrjiviä sekä algoritmien että niiden arviointien vuoksi.¹⁷³

Suuririskisten tekoälyjärjestelmien tarjoajien on seurattava vinoumia ja toteuttava ”asianmukaiset toimenpiteet... mahdollisten vinoutumien havaitsemiseksi, ehkäisemiseksi ja lieventämiseksi”¹⁷⁴ datajoukoissa,¹⁷⁵ jotka todennäköisesti ”vaikuttavat

173. Shrishak K. (2025), ”Bias evaluation, AI-complex algorithms and effective data protection supervision”, EDPB, saatavilla osoitteessa www.edpb.europa.eu/our-work-tools/our-documents/support-pool-experts-projects/ai-complex-algorithms-and-effective-data_en, viitattu 10. marraskuuta 2025.

174. Tekoälyasetus, 10 artiklan 2 kohdan g alakohta.

175. Tekoälyasetuksen 3 artiklan 29–33 kohdassa määritellään koulutus-, validointi- ja testausdatajoukot. Tekoälyjärjestelmiä voidaan kehittää käyttämällä kaikkia kolmea datajoukkoa tai vain yhtä niistä tekniikasta riippuen. Kummassakin tapauksessa 10 artiklan 1 ja 6 kohdan ja 10 artiklan 2–5 kohdan velvoitteita sovelletaan.

kielteisesti perusoikeuksiin tai johtavat unionin oikeudessa kiellettyyn syrjintään”.¹⁷⁶ Tämän velvoitteen täyttämiseksi on olennaisen tärkeää, että tarjoajat toimivat seuraavasti:

- ▶ tekevät ”asiaankuuluvat suunnitteluvalinnat”¹⁷⁷
- ▶ keräävät ja käyttävät laadukasta dataa, joka perustuu hyvin muotoiltuihin oletuksiin¹⁷⁸
- ▶ varmistavat, että datajoukot ovat ”riittävän edustavia”¹⁷⁹ ”niiden henkilöiden tai henkilöryhmien osalta, joihin liittyen suuririskistä tekoälyjärjestelmää on tarkoitus käyttää”¹⁸⁰, ja että niissä otetaan huomioon ”ominaisuudet tai osatekijät, jotka ovat ominaisia sille maantieteelliselle, viitekehystenä olevalle, käyttäytymiseen liittyvälle tai toiminnalliselle ympäristölle, jossa suuririskistä tekoälyjärjestelmää on tarkoitus käyttää”¹⁸¹
- ▶ suorittavat ”asiaankuuluvat tietojenkäsittelytoimet, kuten huomautusten ja tunnisteiden lisääminen, puhdistus” ja niin edelleen.¹⁸²

On tärkeää korostaa, että monien tekoälyjärjestelmien suorituskyvylle olennaisen tärkeät huomautusten ja tunnisteiden lisäystoimet ulkoistetaan usein nimettömille toimijoille, jotka eivät edusta tekoälyjärjestelmän käyttöönottopopulaatiota.¹⁸³ Näin ollen ei ole harvinaista, että datajoukoissa on virheellisiä tunnisteita. Joissakin tapauksissa tunnisteiden lisäysprosessin aikana datajoukkoon lisätään rasistisia herjauksia ja halventavia ilmaisuja.¹⁸⁴ Tätä ongelmaa voi esiintyä myös yleiskäyttöisissä tekoälyjärjestelmissä ja tilanteissa, joissa niitä käytetään tiettyihin sovelluksiin.¹⁸⁵ Näin ollen huomautusten ja tunnisteiden lisäys voi olla tekoälyjärjestelmien kehittämisessä käytetyn datan vinoumien lähde.

Vaikka erilaisten teknisten lähestymistapojen käyttö ”mahdollisten vinoutumien havaitsemiseksi, ehkäisemiseksi ja lieventämiseksi”¹⁸⁶ ei kuulu tämän raportin piiriin,¹⁸⁷ on tärkeää korostaa seuraavaa:

176. Tekoälyasetus, 10 artiklan 2 kohdan f alakohta.

177. Tekoälyasetus, 10 artiklan 2 kohdan a alakohta.

178. Tekoälyasetus, 10 artiklan 2 kohdan d alakohta.

179. Tekoälyasetus, 10 artiklan 3 kohta.

180. Ibid.

181. Tekoälyasetus, 10 artiklan 4 kohta.

182. Tekoälyasetus, 10 artiklan 2 kohdan c alakohta.

183. C. G. Northcutt et al. (2021), ”Pervasive label errors in test sets destabilize machine learning benchmarks”, saatavilla osoitteessa <https://labelerrors.com>, viitattu 10. marraskuuta 2025.

184. Birhane A. ja Prabhu V. U. (2021), ”Large image datasets: A pyrrhic win for computer vision?” WACV (2021 IEEE Winter Conference on Applications of Computer Vision), 1536-46; Crawford K. ja Paglen T. (2021), ”Excavating AI: The politics of images in machine learning training sets”, *AI & SOCIETY* 36, 1105-16.

185. Vaikka yleiskäyttöisiin tekoälyjärjestelmiin ei lisättäisi tunnisteita alkuvaiheen koulutuksen aikana, jotkin yritykset luottavat kehitysprosessin myöhemmässä vaiheessa ihmispalautteeseen perustuvaan vahvistavaan oppimiseen, mikä luo vinoumia järjestelmään.

186. Tekoälyasetus, 10 artiklan 2 kohdan g alakohta.

187. Jos haluat lisätietoja vinoumien arvioinnista, katso Shrishak K. (2025), ”Bias evaluation, AI-complex algorithms and effective data protection supervision”, EDPB.

- ▶ Tekoölyjärjestelmät ovat sosioteknisiä, eivätkä puhtaasti tekniset lähestymistavat pysty täysin puuttumaan vinoumiin.¹⁸⁸
- ▶ Arkaluontoisten muuttujien poistaminen datajoukoista ei yksin riitä, koska data sisältää yleensä sijaismuuttujia, jotka voivat edelleen aiheuttaa vinoumia.¹⁸⁹

Tekoölyasetuksen 10 artiklan 5 kohta

Yleinen tietosuoja-asetus kieltää yleisesti henkilötietojen erityisryhmien käsittelyn,¹⁹⁰ ellei poikkeusta sovelleta. Tekoölyasetuksen 10 artiklan 5 kohdassa kuvataan yleisen tietosuoja-asetuksen poikkeus, jossa ”käsittely on tarpeen tärkeää yleistä etua koskevasta syystä”.¹⁹¹ Tekoölyasetuksen mukainen tärkeä syy on ”vinoutumien havaitsemisen ja korjaamisen varmistami[nen]”.¹⁹²

Tekoölyasetuksen 10 artiklan 5 kohtaa sovelletaan ainoastaan tekoölyjärjestelmien tarjoajiin, ei käyttöönottajiin tai muihin kolmansiin osapuoliin. Seuraavassa on kaksi esimerkkitilannetta, jotka auttavat ymmärtämään tämän seurauksia:

- ▶ Viranomainen tarjoajana ja käyttöönottajana: Jos viranomainen kehittää (tarjoajana) tekoölyjärjestelmän itse ja käyttää sitä sosiaaliturvaetuuksien arviointiin, se voi tarjoajana vedota 10 artiklan 5 kohtaan.
- ▶ Viranomainen vain käyttöönottajana: Jos yritys (tarjoaja) kehittää tekoölyjärjestelmiä, joita käytetään sosiaaliturvaetuuksien arviointiin, ja viranomainen (käyttöönottaja) ostaa tämän tekoölyjärjestelmän ja käyttää sitä, vain yritys voi vedota 10 artiklan 5 kohtaan. Eri viranomaiset voivat käyttää yrityksen kehittämää tekoölyjärjestelmää sosiaaliturvaetuuksien arviointiin useissa eri maissa. Viranomaiset, joilla voi olla enemmän maantieteellistä ja asiayhteyteen liittyvää tietoa, eivät kuitenkaan pysty keräämään ja käsittelemään erityisryhmiin kuuluvia tietoja, jotta vinoumat voitaisiin havaita ja korjata. Tämä tarkoittaa, että viranomaisia saatetaan kannustaa olemaan kehittämättä itse suuririskisiä tekoölyjärjestelmiä, koska tämä asettaisi niille suuremman vastuun (järjestelmän tarjoajana).

Tekoölyjärjestelmien tarjoajat voivat vedota 10 artiklan 5 kohtaan vain silloin, kun erityisryhmään kuuluvien tietojen käsittely on ehdottoman välttämätöntä vinoumien havaitsemiseksi ja korjaamiseksi ja muut kuin erityisryhmien tiedot ovat tehottomia.¹⁹³ Tarjoajien lähestymistapaa ”olisi tarkasti rajoite[ttava] säännöksillä,

188. Buyl M. ja De Bie T. (2024), ”Inherent limitations of AI fairness”, *Communications of the ACM*, 67(2), 48-55, saatavilla osoitteessa <https://doi.org/10.1145/3624700>, viitattu 10. marraskuuta 2025; Schwartz R. et al. (2022). ”Towards a standard for identifying and managing bias in artificial intelligence” (National Institute of Standards and Technology, Special Publication 1270).

189. Dwork C. et al. (2012), ”Fairness through awareness”, *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*, 214-26; Kamiran F. ja Calders T. (2012), ”Data preprocessing techniques for classification without discrimination”, *Knowledge and Information Systems*, 33(1), 1-33.

190. GDPR, 9 artiklan 1 kohta, ja Euroopan parlamentin ja neuvoston asetukset (EU) 2018/1725, 10 artiklan 1 kohta.

191. GDPR, 9 artiklan 2 kohdan g alakohta, ja Euroopan parlamentin ja neuvoston asetukset (EU) 2018/1725, 10 artiklan 2 kohdan g alakohta.

192. Tekoölyasetus, 10 artiklan 5 kohdan ensimmäinen alakohta.

193. Tekoölyasetus, 10 artiklan 2 kohdan a ja f alakohta.

joilla voidaan taata, että se todella rajoitetaan täysin välttämättömään”.¹⁹⁴ Tähän voi sisältyä dokumentointi, josta käy ilmi, miten erityisryhmiin kuuluvien tietojen käsittelyllä varmistetaan vinoumien havaitseminen ja korjaaminen sekä ehkäistään tehokkaasti syrjintää.

Lisäksi tarjoaja ei saa käyttää tätä henkilötietojen erityisryhmää muihin tarkoituksiin, sen on säilytettävä tietoja turvallisesti, eikä se saa jakaa tietoja muiden osapuolten kanssa tai antaa niitä muiden osapuolten käyttöön ja sen on poistettava tiedot, ”kun vinoutuma on korjattu tai kun henkilötietojen säilytysaika on päättynyt, sen mukaan kumpi ajankohdista on aikaisempi”.¹⁹⁵ Tämä tarkoittaa myös sitä, että tällaiset tiedot eivät ole yhdenvertaisuuselinten tai kansallisten ihmisoikeustoimijoiden saatavilla ainakaan 10 artiklan 5 kohdan perusteella.

On kuitenkin tärkeää korostaa, että yleisen tietosuoja-asetuksen erityiset henkilötietoryhmät ovat päällekkäisiä vain neljän syrjinnän vastaisella lainsäädännöllä kielletyn syrjintäperusteen kanssa: (1) vammaisuus, (2) uskonto tai vakaumus, (3) rodullinen tai etninen alkuperä ja (4) seksuaalinen suuntautuminen. Yleinen tietosuoja-asetus ei kiellä tarjoajia ja käyttöönottajia keräämästä tietoja muista ominaisuuksista, kuten iästä ja sukupuolesta.

Lisäksi tarjoajat voivat jo nyt käsitellä erityisryhmiin kuuluvia tietoja, jos ”rekisteröity on antanut nimenomaisen suostumuksensa kyseisten henkilötietojen käsittelyyn”.¹⁹⁶ Tekoälyasetuksen 10 artiklan 5 kohta on hyödyllinen vain, kun tarjoaja ei voida saada nimenomaista suostumusta rekisteröidyltä.

Yhteys muihin oikeudellisiin kehyksiin

Vaikka tekoälyasetuksen 10 artiklan 5 kohtaa sovelletaan vain tarjoajiin, yhdenvertaisuuselimet voivat hyödyntää [yhdenvertaisuuselimien normeja koskevien direktiivien](#) 21 artiklaa,¹⁹⁷ jonka mukaan yhdenvertaisuuselimet saavat käsitellä henkilötietojen erityisryhmiä. Jotta yhdenvertaisuuselimet voivat käyttää tätä mahdollisuutta, on välttämätöntä, että elinten jäsenvaltio saattaa yhdenvertaisuuselinten normeja koskevan direktiivin osaksi kansallista lainsäädäntöään panemalla täytäntöön yleisen tietosuoja-asetuksen 9 artiklan 2 kohdan g alakohdassa säädetyn poikkeuksen edellyttäen, että tätä poikkeusta ei ole jo taattu kansallisessa tietosuoja- tai muussa lainsäädännössä. Vaikka direktiivit yhdenvertaisuuselimiä koskevista normeista sallii yhdenvertaisuuselinten käsitellä erityisiä henkilötietoryhmiä, tekoälyasetus ja direktiivit yhdenvertaisuuselimiä koskevista normeista eivät kuitenkaan nimenomaisesti salli yhdenvertaisuuselinten kerätä tällaisia tietoja tekoälyn tarjoajilta.

194. Unionin tuomioistuimen tuomio, 8. huhtikuuta 2014, *Digital Rights Ireland Ltd*, C-293/12, ja C-594/12, ECLI:EU:C:2014:238, kohta 65.

195. Tekoälyasetus, 10 artiklan 5 kohdan e alakohta.

196. GDPR, 9 artiklan 2 kohdan a alakohta, ja Euroopan parlamentin ja neuvoston asetukset (EU) 2018/1725, 10 artiklan 2 kohdan a alakohta.

197. Direktiivit yhdenvertaisuuselimiä koskevista normeista, 21 artikla ja johdanto-osan kappale 48.

3.4.2. Yhdenvertaisuuselinten ja kansallisten ihmisoikeustoimijoiden rooli datanhallinnan vaatimuksissa

- ▶ Olla tietoinen vinoumien havaitsemiseen ja korjaamiseen liittyvien teknisten lähestymistapojen rajoituksista suuririskisten tekoälyjärjestelmien syrjintäriskien arvioinneissa. Tekoälyasetuksen ja sen 10 artiklan noudattaminen ei välttämättä riitä poistamaan suuririskisten tekoälyjärjestelmien aiheuttamaa syrjintäriskiä. Tällaisissa tilanteissa, kun 82 artiklan 1 kohdan mukaisia valtuuksiaan käyttävä markkinavalvontaviranomainen konsultoi yhdenvertaisuuselimiä, yhdenvertaisuuselimet voisivat pyytää valvontaviranomaista pakottamaan yritykset "toteuttamaan kaikki asianmukaiset toimenpiteet sen varmistamiseksi, että kyseinen tekoälyjärjestelmä ei... enää aiheuta kyseistä riskiä".¹⁹⁸
- ▶ Varmistaa, että EU:n yhdenvertaisuuselimiä koskevien direktiivien 21 artikla, jonka nojalla yhdenvertaisuuselimet saavat käsitellä henkilötietojen erityisryhmiä, saatetaan osaksi kansallista lainsäädäntöä, jos muu kansallinen lainsäädäntö ei vielä salli tätä.

3.5. Perusoikeusvaikutusten arviointi (FRIA)

3.5.1. Tausta ja merkitys

Yhdenvertaisuuselinten ja kansallisten ihmisoikeustoimijoiden on pidettävä FRIA-arviointia lähtökohtana, kun arvioidaan tekoälyjärjestelmiä, joita julkishallinnot ottavat käyttöön tai joita otetaan käyttöön julkishallinnon puolesta. FRIA-arvioinnin on sisällettävä erilaisia tietoja, jotka tuovat esiin mahdollisia puutteita ja haittoja oikeuksille, kuten syrjimättömyydelle. Suuririskisen tekoälyjärjestelmän käyttöönottoajan, ei tarjoajan, olisi tehtävä FRIA, koska oletetaan, että käyttöönottajalla on tämän arvioinnin kannalta olennaiset taustatiedot.

FRIA-arvioinnin on sisällettävä tiedot siitä, miten käyttöönottaja aikoo käyttää suuririskistä tekoälyjärjestelmää tarjoajan tarkoittamalla tavalla, kuinka kauan ja kuinka usein tekoälyjärjestelmää käytetään ja miten ihmisten suorittamat valvonta-toimenpiteet toteutetaan.¹⁹⁹ Ihannetapauksessa tämä edellyttäisi, että käyttöönottaja selittäisi tarjoajalta saatujen asiakirjojen perusteella ymmärrettävin sanoin, miten tekoälyjärjestelmä toimii, ja että tiedot linkitettäisiin EU:n tietokantaan rekisteröityyn suuririskiseen tekoälyjärjestelmään. Viranomaisten ei tule käyttää suuririskisiä tekoälyjärjestelmiä, joita tarjoajat eivät ole rekisteröineet EU:n tietokantaan.²⁰⁰

Lisäksi FRIA-arvioinnissa on kuvattava²⁰¹

- ▶ "niiden luonnollisten henkilöiden ja ryhmien luokat, joihin järjestelmän käyttö todennäköisesti vaikuttaa"

198. Tekoälyasetus, 82 artiklan 1 kohta.

199. Tekoälyasetus, 27 artiklan 1 kohdan a ja e alakohta.

200. Tekoälyasetus, 26 artiklan 8 kohta. Tämä koskee myös Euroopan unionin toimielimiä, elimiä, toimistoja ja virastoja.

201. Tekoälyasetus, 27 artiklan 1 kohdan c, d ja f alakohta.

- ▶ ”erityiset sellaisen haitan riskit, joka todennäköisesti kohdistuu” henkilön perusoikeuksiin, mukaan lukien syrjimättömyyteen, ottaen huomioon tarjoajan antamat tiedot
- ▶ tarjoajan toimenpiteet, ”jotka on toteutettava kyseisten riskien toteutuessa, mukaan lukien sisäistä hallintoa ja valitusmekanismeja koskevat järjestelyt”.

Kun henkilötietoja käsitellään, FRIA täydentää tietosuojaa koskevia vaikutustenarviointeja (DPIA), jotka tehdään EU:n tietosuojalainsäädännön mukaisesti.²⁰² Käyttöönottajien voidaan odottaa yhdistävän FRIA- ja DPIA-arvioinnit.

Tekoälyasetuksen johdanto-osan kappaleessa 96 todetaan, että ”suuririskisten tekoälyjärjestelmien käyttöönottajat *voisivat* ottaa asiaankuuluvat sidosryhmät, mukaan lukien sellaisten henkilöryhmien edustajat, joihin tekoälyjärjestelmä todennäköisesti vaikuttaa, riippumattomat asiantuntijat ja kansalaisjärjestöt, mukaan tällaisen vaikutustenarvioinnin toteuttamiseen sekä riskien toteutuessa toteutettavien toimenpiteiden suunnitteluun, etenkin jos tekoälyjärjestelmiä käytetään julkisella sektorilla” (*korostus lisätty*).

Yhteys muihin oikeudellisiin kehyksiin

Tietosuojalainsäädännössä säädetään tekoälyjärjestelmien vaikutustenarvioinnin tekemisestä. EU:n tietosuojalainsäädännössä säädetään DPIA-arvioinneista.²⁰³ Euroopan neuvoston uudistetussa yleissopimuksessa yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä (yleissopimus 108+) määrätään yleisestä velvollisuudesta tutkia tietojenkäsittelyn todennäköisiä vaikutuksia yksilöiden oikeuksiin ja perusvapauksiin ennen niiden käyttöä.²⁰⁴

Tekoälyasetuksen perusoikeusvaikutusten arviointia koskevat säännökset voidaan liittää riskinarviointia koskeviin velvoitteisiin, jotka on kuvattu Euroopan neuvoston puiteyleissopimuksessa ja HUDERIA-menetelmässä. Euroopan neuvoston puiteyleissopimuksessa edellytetään, että kukin sopimuspuoli ”ottaa käyttöön tai pitää voimassa toimenpiteet, joilla tunnistetaan ja arvioidaan tekoälyjärjestelmien aiheuttamat riskit ja ehkäistään ja lievennetään niitä ottamalla huomioon todelliset ja mahdolliset vaikutukset ihmisoikeuksiin, demokratiaan ja oikeusvaltioperiaatteeseen.”²⁰⁵ Puiteyleissopimuksen 16 artiklan 2 kohdan f alakohdassa edellytetään ”riskien, todellisten ja mahdollisten vaikutusten sekä riskinhallintaan sovellettavan lähestymistavan dokumentointi”. Lisäksi tällaisissa riskinarviointitoimenpiteissä on ”otettava tarvittaessa huomioon asiaankuuluvien sidosryhmien ja erityisesti niiden henkilöiden näkökulmat, joiden oikeuksiin voi kohdistua vaikutuksia”,²⁰⁶ ja ”niitä on sovellettava iteratiivisesti koko tekoälyjärjestelmän elinkaareen kuuluihin toimiin”.²⁰⁷

202. Tekoälyasetus, 27 artiklan 4 kohta. Katso myös GDPR, 35 artikla, ja LED, 27 artikla. Yleisen tietosuojasetuksen 35 artiklassa todetaan, että DPIA-arviointi on suoritettava, kun henkilötietojen käsittely todennäköisesti ”aiheuttaa... luonnollisen henkilön oikeuksien ja vapauksien kannalta korkean riskin”, ja varsinkin, jos se ”perustuu automaattiseen käsittelyyn, kuten profilointiin”.

203. GDPR, 35 artikla, ja LED, 27 artikla.

204. Euroopan neuvoston uudistettu yleissopimus yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä, 10 artiklan 2 kohta.

205. Euroopan neuvoston puiteyleissopimus, 16 artiklan 1 kohta.

206. Euroopan neuvoston puiteyleissopimus, 16 artiklan 2 kohdan c alakohta.

207. Euroopan neuvoston puiteyleissopimus, 16 artiklan 2 kohdan d alakohta.

FRIA-arviointien rajoitukset

Rajoitettu soveltamisala: FRIA-arvioinnin mahdollisesta tärkeydestä huolimatta velvollisuus suorittaa FRIA ennen käyttöönottoa koskee vain tiettyä suuririskisten tekoälyjärjestelmien käyttöönottajien joukkoa:

1. Muilla kuin kriittisen infrastruktuurin alan suuririskisillä tekoälyjärjestelmillä²⁰⁸ velvoite koskee seuraavia käyttöönottajia:
 - julkisoikeudelliset laitokset
 - julkisia palveluja tarjoavat yksityiset yksiköt.²⁰⁹
2. Kahteen käyttötarkoitukseen – luonnollisten henkilöiden luottokelpoisuuden arviointiin tai heidän luottopisteytyksensä määrittämiseen²¹⁰ ja riskinarviointiin ja hinnoitteluun sairaus- ja henkivakuutusten tapauksessa²¹¹ – tarkoitettujen suuririskisten tekoälyjärjestelmien osalta tämä velvoite koskee kaikkia käyttöönottajia.

Käytännössä tämä tarkoittaa, että yksityisten tahojen (jotka tässä tapauksessa olisivat käyttöönottajia) työllistämissektorilla käyttämät järjestelmät vapautetaan FRIA-velvoitteesta.

Lisäksi käyttöönottaja ei välttämättä tee FRIA-arviointia, koska tarjoaja on jättäytynyt suuririskisten järjestelmien järjestelyn ulkopuolelle. On myös mahdollista, että "[k]äyttöönottaja voi samanlaisissa tapauksissa tukeutua aiemmin tehtyyn perusoikeusvaikutusten arviointiin tai tarjoajan tekemään olemassa olevaan vaikutustenarviointiin".²¹² Tätä ei kuitenkaan pidä tulkita siten, että se vapauttaisi käyttöönottajat velvollisuudestaan tehdä FRIA-arviointi; se tarkoittaa vain, että käyttöönottajat voivat hyödyntää aiemmin suoritettua FRIA-arviointia sen sijaan, että aloittaisivat sen alusta.

Julkisen tiedon puute

Viranomaisten tai niiden puolesta toimivien henkilöiden, jotka ottavat käyttöön suuririskisiä tekoälyjärjestelmiä, "on rekisteröidyttävä, valittava järjestelmä ja rekisteröitävä sen käyttö... EU:n tietokantaan"²¹³ ja liitettävä mukaan yhteenveto FRIA-arvioinnin havainnoista.²¹⁴

Kuitenkin "lainvalvonnan, muuttoliikkeen, turvapaikka-asioiden ja rajavalvonnan aloilla"²¹⁵ sovelletaan seuraavia:

- EU:n tietokanta ei ole julkinen, ja siihen on pääsy vain Euroopan komissiolla ja tietosuojaviranomaisilla.²¹⁶

208. Tekoälyasetus, liitteessä III oleva 2 kohta.

209. Tekoälyasetus, 27 artiklan 1 kohdan ensimmäinen alakohta.

210. Tekoälyasetus, liitteessä III olevan 5 kohdan b alakohta.

211. Tekoälyasetus, liitteessä III olevan 5 kohdan c alakohta.

212. Tekoälyasetus, 27 artiklan 2 kohta. Tarjoaja voi myös olla kehittäjänsä tekoälyjärjestelmän käyttöönottaja. Tällaisessa tapauksessa tarjoaja on voinut tehdä FRIA-arvioinnin.

213. Tekoälyasetus, 49 artiklan 3 kohta.

214. Liite VIII, jaksossa C oleva 4 kohta.

215. Tekoälyasetus, 49 artiklan 4 kohdan ensimmäinen alakohta.

216. Tekoälyasetuksen 74 artiklan 8 kohdassa todetaan, että kansallisen viranomaisen tulee olla GDPR:n tai LED:n mukainen toimivaltainen viranomainen tai "mikä tahansa muu viranomainen, joka on nimetty samoin edellytyksin, jotka on määritelty... [LED:n] 41–44 artiklassa".

- FRIA-arvioinnin havaintoja ei sisällytetä EU:n tietokantaan.²¹⁷

Lisäksi, vaikka kaikki luonnollisten henkilöiden luottokelpoisuuden arvioinnin tai heidän luottopisteytyksensä määrittämisen²¹⁸ ja sairaus- ja henkivakuutusten riskinarvioinnin ja hinnoittelun käyttötapausten²¹⁹ käyttöönottajat ovat velvollisia tekemään FRIA-arvioinnin (katso jäljempää), ainoastaan ”käyttöönottajien, jotka ovat viranomaisia, unionin toimielimiä, elimiä, toimistoja tai virastoja tai niiden puolesta toimivia henkilöitä”,²²⁰ on rekisteröitävä tekoälyjärjestelmän käyttö tietokantaan. Yksityisten yritysten, jotka käyttävät tekoälyjärjestelmiä näihin käyttötarkoituksiin, ei siis tarvitse rekisteröidä järjestelmiä tietokantaan. Näin ollen niiden FRIA-arviointien yhteenvetoja ei ole saatavilla.

Syrjimättömyyteen kohdistuvien riskien arvioinnin tehottomuus

Vaikka käyttöönottajien on ilmoitettava FRIA-arviointien tuloksista markkinavalvontaviranomaisille, arviointi itsessään saattaa olla vain ruutujen rastittamista ilman merkityksellistä vaikutustenarviointia, koska käyttöönottaja voi täyttää ”kyselylomakkeen mallin”, jonka tekoälytoimisto laatii.²²¹ Yksi riski on, että FRIA-arvioinnit eivät anna riittävän tarkkoja tietoja, jotta voitaisiin arvioida, miten syrjintää on ehkäisty ja/tai lievennetty, mitä syrjintäperusteita on testattu ja miten mahdolliset oikeudellisesti suojellut ryhmät on määritelty riskinarviointimenettelyjen aikana.

3.5.2. Yhdenvertaisuuselinten ja kansallisten ihmisoikeustoimijoiden rooli perusoikeusvaikutusten arvioinnin (FRIA) vaatimuksissa

- **Käyttää EU:n tietokannassa olevia FRIA-yhteenvetoja lähtökohtana tekoälyjärjestelmien tutkimiselle.** Yhdenvertaisuuselinten on kartoitettava suuririskisten tekoälyjärjestelmien käyttöä EU:n tietokannan perusteella ja arvioitava FRIA-arviointien yhteenvetoja. Tämän jälkeen yhdenvertaisuuselimet voivat pyytää markkinavalvontaviranomaisilta FRIA-tulosten käyttöoikeutta. Näiden tietojen perusteella yhdenvertaisuuselimet voivat tehdä alustavan arvion syrjinnän vastaisen lainsäädännön rikkomuksista ja siitä, onko ryhdyttävä täysimittaiseen tutkintaan, mikä edellyttäisi arviointia käyttöönoton jälkeen (jota FRIA ei tarjoa).
- **Osallistua FRIA-arvioinnin kyselylomakkeen mallin laatimiseen.** Tekoälytoimiston on laadittava malli FRIA-arvioinnin kyselylomaketta varten. On tärkeää, että tässä mallissa esitetään asianmukaisia, tarkkoja kysymyksiä yhdenvertaisuuden ja syrjimättömyyden eri ulottuvuuksista, jotta annetut tiedot ja analyysi tarjoavat asianmukaisen arvioinnin ja riittävät suojatoimet sen sijaan, että kysymyksiin vastaaminen olisi vain ”ruutujen rastitusta”.

217. Tekoälyasetus, 49 artiklan 4 kohdan c alakohta.

218. Tekoälyasetus, liitteessä III olevan 5 kohdan b alakohta.

219. Tekoälyasetus, liitteessä III olevan 5 kohdan c alakohta.

220. Tekoälyasetus, 49 artiklan 3 kohta.

221. Tekoälyasetus, 27 artiklan 3 ja 5 kohta.

Tekoälytoimistolla ei ole määräaikaa mallin laatimiselle. Yhdenvertaisuuselimet ja kansalliset ihmisoikeustoimijat voivat edistää ennakoivasti tällaista täytännönpaanoa laatimalla tähän erityisohjeita. Ohjeet voidaan laatia Euroopan neuvoston kehittämän HUDERIA-menetelmän pohjalta.

► **Laatia seuraavia koskevia ohjeita:**

- Mitä merkitykselliset FRIA-arviointien tiivistelmät sisältävät?
- Kenen tulisi tehdä FRIA-arviointeja? Yhdenvertaisuuselinten ja kansallisten ihmisoikeustoimijoiden on korostettava perusoikeusasiantuntemuksen merkitystä ja tarpeellisuutta perusoikeusvaikutusten arviointeja tekevissä organisaatioissa.

- **Julkaista tapaustutkimuksia**, joissa tuodaan esiin syrjinnästä johtuvat "erityiset sellaisen haitan riskit", jotka on arvioitava osana FRIA-arviointeja. Tällaisissa tutkimuksissa on keskityttävä tarkkoihin esimerkkeihin, joissa käsitellään haittojen vakavuuteen ja laajuuteen liittyviä kysymyksiä. Tällaisia tutkimuksia voidaan tehdä yhteistyössä halukkaiden viranomaisten kanssa.

3.6. EU:n tietokanta liitteessä III luetelluista suuririskisistä tekoälyjärjestelmistä

3.6.1. Tausta ja merkittävyys

Tekoälyasetuksen 71 artiklan 1 kohdassa edellytetään, että komissio "perustaa yhteistyössä jäsenvaltioiden kanssa EU:n tietokannan... ja pitää sitä yllä". Tietokannan tulisi sisältää seuraavat tiedot:

1. liitteessä III luetellut suuririskiset tekoälyjärjestelmät
2. tekoälyjärjestelmät, jotka eivät tarjoajien itsearviointien mukaan ole 6 artiklan 3 kohdan mukaisia suuririskisiä järjestelmiä.

Tietokannan sisältämien tietojen tulee olla "helposti selattavia ja koneluettavia", ja tietokannan julkisen osion tulee myös olla "julkisesti saatavilla käyttäjäystävällisellä tavalla".²²² Saavutettavuuden laaja tulkinta merkitsisi, että tietojen tulisi olla toimintarajoitteisten käyttäjien käytettävissä ja johdanto-osan kappaleen 72 (joka koskee tekoälyn tarjoajien käyttöohjeita, jotka laaditaan tekoälyn käyttöönottajille) mukaisesti myös merkityksellisiä, kattavia, helposti saatavilla olevia ja ymmärrettäviä erilaisille yleisöille.²²³

Mahdollisuus avoimuuteen

Rekisteröintivelvoitteet ja EU:n tietokanta suuririskisistä tekoälyjärjestelmistä ovat erityisen hyödyllisiä yhdenvertaisuuselimille ja kansallisille ihmisoikeustoimijoille, jotta

222. Tekoälyasetus, 71 artiklan 4 kohta.

223. Equinet (2025) korostaa, että johdanto-osan kappaleessa on kyse tekoälyn tarjoajien avoimuusvaatimuksista tekoälyn käyttöönottajille (tekoälyasetus, 13 artikla), ja "näin ollen tätä määritelmää ei välttämättä voida soveltaa tässä yhteydessä". Se huomauttaa kuitenkin, että kyseessä on "ainoa selitys siitä, mitä "saavutettavuus" tarkoittaa tekoälyasetuksen dokumentaation kontekstissa".

ne voivat saada yleiskuvauksen julkisten elinten käyttämistä tekoälyjärjestelmistä, koska sellaista ei tällä hetkellä ole (Xenidis, 2025). Monet sidosryhmät ovat yhtä mieltä siitä, että tällaiset tietokannat ovat välttämättömiä, vaikka ne eivät yksin riitä sen varmistamiseksi, että tekoälyjärjestelmät kunnioittavat perusoikeuksia ja erityisesti oikeutta syrjimättömyyteen.²²⁴

EU:n tietokannasta on hyötyä yhdenvertaisuuselimille ja kansallisille ihmisoikeus-toimijoille, jotka voivat seurata tekoälyjärjestelmien markkinoille saattamista tai käyttöönottoa, sekä kansalaisjärjestöille ja toimittajille, jotka työskentelevät näiden kysymysten parissa, ja muille asianomaisille, jotta he voivat luoda yhteyksiä oman tilanteensa ja tekoälyjärjestelmien mahdollisen käytön välille.²²⁵

Rekisteröitävät järjestelmätyypit

Tekoälyjärjestelmät on rekisteröitävä EU:n tietokantaan seuraavassa neljässä tapauksessa:

<i>Rekisteröintivelvollinen taho</i>	<i>Rekisteröitävien tietojen yleiskuvauus</i> ²²⁶
1. Sellaisten liitteessä III lueteltujen alojen suuririskisten tekoälyjärjestelmien tarjoajat (tai tarvittaessa valtuutettu edustaja), lukuun ottamatta liitteessä III olevassa 2 kohdassa tarkoitettuja suuririskisiä tekoälyjärjestelmiä ("kriittinen infrastruktuuri"), jotka rekisteröidään kansallisella tasolla, ²²⁷ ennen järjestelmän markkinoille saattamista tai käyttöönottoa. ²²⁸	Tarjoajan nimi, osoite ja yhteystiedot. Järjestelmän ja sen osien käyttötarkoitus. Yleisluontoinen ja lyhyt kuvaus teknisistä tiedoista. Järjestelmän tila (esimerkiksi onko järjestelmä käytössä vai onko se vedetty pois markkinoilta). Sähköiset käyttöohjeet, jotka tarjoaja antaa käyttöönottajille 13 artiklan 2 kohdan mukaisesti (mukaan lukien "ominaisuudet, valmiudet ja suorituskyvyn rajoitukset", kuten "tarkkuuden... taso" ja ihmisten suorittaman valvonnan toimet ²²⁹).

224. IA Ciudadana (2025), "Making algorithm registers work for meaningful transparency", saatavilla osoitteessa <https://iaciudadana.org/2025/03/13/making-algorithm-registers-work-for-meaningful-transparency/>; Ada Lovelace Institute (2020), "Meaningful transparency and (in)visible algorithms: Can transparency bring accountability to public-sector algorithmic decision-making (ADM) systems?", saatavilla osoitteessa [www.adalovelaceinstitute.org/blog/meaningful-transparency-and-invisible-algorithms/](https://adalovelaceinstitute.org/blog/meaningful-transparency-and-invisible-algorithms/); lisäksi C. Cath ja F. Jansen (2022), "Dutch comfort: the limits of AI governance through municipal registers", *Techné Research in Philosophy and Technology*, 26(3), pp. 395-412, saatavilla osoitteessa <https://doi.org/10.5840/techné202323172>, kaikki viitattu 10. marraskuuta 2025.

225. IA Ciudadana (2025), "Making algorithm registers work for meaningful transparency", saatavilla osoitteessa <https://iaciudadana.org/2025/03/13/making-algorithm-registers-work-for-meaningful-transparency/>.

226. Tekoälyasetus, liitteet VIII ja IX, jotka sisältävät kattavan luettelon.

227. Tekoälyasetus, 49 artiklan 5 kohta.

228. Tekoälyasetus, 49 artiklan 1 kohta.

229. Tekoälyasetus, 13 artiklan 2 kohta.

<i>Rekisteröintivelvollinen taho</i>	<i>Rekisteröitävien tietojen yleiskuvaus²²⁶</i>
2. Sellaisten tekoälyjärjestelmien tarjoajat (tai tarvittaessa valtuutettu edustaja), joiden on todettu olevan muita kuin suuririskisiä, vaikka ne liittyvät liitteessä III lueteltuihin aloihin (6 artiklan 3 kohdan mukaisesti), ennen järjestelmän markkinoille saattamista tai käyttöönottoa.²³⁰	Samankaltaiset tiedot kuin suuririskisillä tekoälyjärjestelmillä mutta suppeammat vaatimukset. Esimerkiksi ”sähköisiä käyttöohjeita” ei tarvitse rekisteröidä. Tietoihin sisältyy myös lyhyt yhteenveto perusteista, joiden nojalla tekoälyjärjestelmää ei pidetä 6 artiklan 3 kohdassa tarkoitettua menettelyä sovellettaessa suuririskisenä.
3. Liitteessä III lueteltujen alojen suuririskisten tekoälyjärjestelmien käyttöönottajat (lukuun ottamatta kriittisen infrastruktuurin suuririskisiä tekoälyjärjestelmiä), jotka ovat ”viranomaisia, unionin toimielimiä, elimiä, toimistoja tai virastoja tai niiden puolesta toimivia henkilöitä”, ennen järjestelmän käyttöönottoa tai käyttöä.²³¹	Käyttöönottajan nimi, osoite ja yhteystiedot. Tekoälyjärjestelmän tarjoajan järjestelmästä EU:n tietokantaan kirjaamien tietojen URL-osoite. Yhteenveto 27 artiklan mukaisesti suoritettujen perusoikeusvaikutusten arvioinnin tuloksista. Yhteenveto tietosuoja-asetuksen mukaisesti tehdystä DPIA-arvioinnista.
4. Liitteessä III kuvattujen suuririskisten tekoälyjärjestelmien tarjoajat, jotka suorittavat testauksen tosielämän olosuhteissa tekoälyn sääntelyn testi-ympäristöjen ulkopuolella.²³²	Tosielämän olosuhteissa tapahtuvaan testaukseen osallistuvien tarjoajan tai mahdollisen tarjoajan ja käyttöönottajien nimi ja yhteystiedot. Lyhyt kuvaus tekoälyjärjestelmästä, sen käyttötarkoituksesta ja muista tiedoista, jotka ovat tarpeen järjestelmän tunnistamiseksi. Yhteenveto tosielämän olosuhteissa tapahtuvaa testausta koskevan suunnitelman keskeisistä ominaisuuksista. Tiedot tosielämän olosuhteissa tapahtuvan testauksen keskeyttämisestä tai päättämisestä.

230. Tekoälyasetus, 49 artiklan 2 kohta.

231. Tekoälyasetus, 49 artiklan 3 kohta. Katso myös tekoälyasetus, liitteessä III olevat kohdat 1, 6 ja 7.

232. Tekoälyasetus, 60 artiklan 4 kohdan c alakohta.

Tekoälyjärjestelmien käyttöönottajilla, joita velvoitteet eivät koske, *”olisi oltava oikeus”* rekisteröidä järjestelmänsä tietokantaan vapaaehtoisesti, ja tämä koskee myös yksityisiä käyttöönottajia.²³³

Käyttöönottajina toimivien viranomaisten on tarkistettava, onko tarjoaja rekisteröinyt suuririskisen järjestelmän tietokantaan. Jos järjestelmää ei ole rekisteröity, sitä ei saa käyttää ja siitä on ilmoitettava tarjoajalle tai jakelijalle.²³⁴

Tietokannan julkinen ja ei-julkinen osio

Tietokannassa on kaksi osiota: julkinen ja ”suojattu, ei-julkinen” osio.²³⁵ Tietokannan ei-julkinen osio sisältää tietoja seuraavista:

- ▶ suuririskiset tekoälyjärjestelmät, joita käytetään biometriikassa, lainvalvonnassa sekä muuttoliikkeen, turvapaikka-asioiden ja rajavalvonnan hallinnassa²³⁶
- ▶ suuririskiset tekoälyjärjestelmät, joita testataan 60 artiklan mukaisesti tosi-elämän olosuhteissa (ellei tarjoaja ole suostunut antamaan näitä tietoja julkisesti saataville).²³⁷

Perustamisen ja täytäntöönpanon aikataulu

- ▶ Komissio vastaa tietokannan toiminnallisten eritelmien laatimisesta kuullen ”asianomaisia asiantuntijoita”. Tietokannan toiminnallisten eritelmien päivittämisestä vastaa komissio kuullen tekoälyneuvostoa.²³⁸
- ▶ Tämän raportin laatimishetkellä Euroopan komissio ei ole vielä perustanut tietokantaa.
- ▶ Rekisteröityminen tietokantaan tulee pakolliseksi 2. elokuuta 2026. Rekisteröityminen ennen 2. elokuuta 2026 on vapaaehtoista mutta suositeltavaa.²³⁹

Yhteys muihin oikeudellisiin kehyksiin

Tekoälyasetuksen rekisteröintivelvoitteet voidaan liittää Euroopan neuvoston puiteyleissopimuksen 8 artiklaan, jonka mukaan sopimuspuolten on toteutettava tai pidettävä voimassa ”riittävät avoimuus- ja valvontavaatimukset” varmistavat toimenpiteet, sekä 9 artiklaan, jonka mukaan kukin sopimismies ”ottaa käyttöön tai pitää voimassa toimenpiteet varmistukseksi vastuuvollisuuden ja vastuun ihmisoikeuksiin, demokratiaan ja oikeusvaltioperiaatteeseen kohdistuvista haitallisista vaikutuksista”. Lisäksi puiteyleissopimuksen 14 artiklassa vaaditaan, että ”asiaankuuluvat tiedot tekoälyjärjestelmistä, jotka voivat vaikuttaa merkittävästi ihmisoikeuksiin, ja niiden merkityksellisestä käytöstä dokumentoidaan, toimitetaan elimille, joilla on valtuudet tutustua kyseisiin tietoihin, ja tarvittaessa ja soveltuvin osin asetetaan asianomaisten henkilöiden saataville tai annetaan heille tiedoksi”.

233. Tekoälyasetus, johdanto-osan kappale 131 (*korostus lisätty*).

234. Tekoälyasetus, 26 artiklan 8 kohta.

235. Tekoälyasetus, 49 artiklan 4 kohta, ja tekoälyasetus, 71 artiklan 4 kohta.

236. Tekoälyasetus, 49 artiklan 4 kohta.

237. Tekoälyasetus, 60 artiklan 4 kohdan c alakohta.

238. Tekoälyasetus, 71 artiklan 1 kohta.

239. Tekoälyasetus, johdanto-osan kappale 179.

Puiteyleissopimuksen selitysmuistiossa tunnustetaan, että ”sopimuspuolten on löydettävä asianmukainen tasapaino [avoimuuden] ja erilaisten kilpailevien intressien”,²⁴⁰ kuten ”yksityisyyden, luottamuksellisuuden (mukaan lukien esimerkiksi liikesalaisuudet), kansallisen turvallisuuden, kolmansien osapuolten oikeuksien suojelun, yleisen järjestyksen ja oikeuslaitoksen riippumattomuuden”, välille. Termi ”riittävä” viittaa kuitenkin siihen, että avoimuuden vähimmäistaso on huomioitava erityisesti suuren yleisön kannalta ja myös sellaisten tekoälyjärjestelmien osalta, joiden tiedot on pidettävä yksityisinä.

Haasteet

Tietokantaan liittyy useita rajoituksia, jotka voivat haitata sen hyödyllisyyttä tekoälyjärjestelmissä esiintyvän syrjinnän tunnistamisessa ja lieventämisessä.

► Osa tiedoista on tietokannan ei-julkisessa osiossa:

- tiedot tekoälyjärjestelmistä, joita käytetään biometriikassa, lainvalvonnassa sekä muuttoliikkeen, turvapaikka-asioiden ja rajavalvonnan hallinnassa
- tiedot tosielämän olosuhteissa testatuista tekoälyjärjestelmistä.

► Joitakin tietoja ei tallenneta tietokantaan lainkaan:

- Tietokanta on rajattu koskemaan suuririskisiä tekoälyjärjestelmiä. Täten se ei välttämättä sisällä kaikkia viranomaisten käyttämiä sovelluksia, kuten chatti-botteja tai suoraan kansalaisten kanssa vuorovaikutuksessa olevia sovelluksia.
- Biometriikkaan, lainvalvontaan ja muuttoliikkeen, turvapaikka-asioiden ja rajavalvonnan hallintaan liittyvien suuririskisten tekoälyjärjestelmien tarjoajien ja käyttöönottajien on rekisteröitävä vähemmän tietoja tekoälyjärjestelmistään. Tarjoajien ei esimerkiksi tarvitse rekisteröidä sähköisiä käyttöohjeita, jotka annetaan käyttöönottajille. Käyttöönottajien ei tarvitse rekisteröidä FRIA-arviointien yhteenvetoja.
- Jos tekoälyjärjestelmien tarjoajat eivät pidä järjestelmiä 6 artiklan 3 kohdan mukaisina suuririskisinä järjestelminä, niiden käyttöönottajien ei tarvitse rekisteröidä niiden käyttöönottoa tai testausta tietokantaan.
- Vain käyttöönottajien, ”jotka ovat viranomaisia, unionin toimielimiä, elimiä, toimistoja tai virastoja tai niiden puolesta toimivia henkilöitä”,²⁴¹ on rekisteröidyttävä. Joidenkin suuririskisten tekoälyjärjestelmien käyttöönottajat voivat kuitenkin olla yksityisiä tahoja, kuten vakuutusyhtiöitä, ja tällaisten käyttöönottajien ei tarvitse rekisteröidä tekoälyjärjestelmäänsä EU:n tietokantaan. Tämä tarkoittaa, että kaikkia tietoja, kuten FRIA-arvioinnin yhteenvetoa, ei ole saatavilla näistä suuririskisistä tekoälyjärjestelmistä.
- Edes tietokannan julkiseen osioon rekisteröityjen suuririskisten tekoälyjärjestelmien osalta ei ole taattua, että rekisteröitävät tiedot ovat riittäviä

240. Euroopan neuvosto (2024), tekoälyä ja ihmisoikeuksia, demokratiaa ja oikeusvaltioperiaatetta koskeva puiteyleissopimus, selitysmuistio, kohta 62.

241. Tekoälyasetus, 49 artiklan 3 kohta.

syrynnän arviointiin. Käyttöönottajien on esimerkiksi toimitettava vain yhteen-
veto FRIA-arvioinneista, ei täydellisiä FRIA-arviointeja.

- Rekisteröityminen tietokantaan tulee pakolliseksi vasta 2. elokuuta 2026. Tämä tarkoittaa, että ennen kyseistä päivämäärää käyttöön otettuja tekoälyjärjestelmiä ei ole pakko kirjata tietokantaan, ellei niissä tapahdu ”huomattavia muutoksia”.²⁴²

Yhdenvertaisuuselinten ja kansallisten ihmisoikeustoimijoiden pääsy tietokannan ei-julkisessa osiossa oleviin tietoihin

Lainvalvonnassa sekä muuttoliikkeen, turvapaikka-asioiden ja rajavalvonnan hallinnassa käytettävillä tekoälyjärjestelmillä on ollut syrjiviä vaikutuksia ihmisiin (katso kohta 7.1: Temaattinen painopiste lainvalvonnassa ja muuttoliikkeen, turvapaikka-asioiden ja rajavalvonnan hallinnassa), ja pääsy tietokannan ei-julkiseen osioon sisältyvään dokumentaatioon on välttämätöntä, jotta yhdenvertaisuuselimet ja kansalliset ihmisoikeustoimijat voivat tehokkaasti täyttää tehtävänsä. Ilman pääsyä näihin tietoihin yhdenvertaisuuselimet ja kansalliset ihmisoikeustoimijat eivät saa yleiskuva näillä alueilla käytetyistä suuririskisistä tekoälyjärjestelmistä. On kuitenkin epäselvää, missä määrin yhdenvertaisuuselimet ja kansalliset ihmisoikeustoimijat voivat käyttää tietokannan ei-julkisessa osiossa olevia tietoja.

Tekoälyasetuksen 71 artiklan 4 kohdassa todetaan, että ”edellä olevan 60 artiklan mukaisesti rekisteröityjen [säätelyn testiympäristöjen ulkopuolella olevien suuririskisten tekoälyjärjestelmien] tietojen on oltava ainoastaan markkinavalvontaviranomaisten ja komission saatavilla, paitsi jos mahdollinen tarjoaja tai tarjoaja on antanut suostumuksensa näiden tietojen asettamiseen myös yleisön saataville”. Rekisteröintiä koskevassa 49 artiklan 4 kohdassa säädetään myös, että ”[a]inoastaan komissiolla ja 74 artiklan 8 kohdassa tarkoitetuilla kansallisilla viranomaisilla on pääsy” tietoihin, jotka koskevat biometriikassa, lainvalvonnassa sekä muuttoliikkeen, turvapaikka-asioiden ja rajavalvonnan hallinnassa käytettyjä suuririskisiä tekoälyjärjestelmiä.

Tekoälyasetuksen 77 artiklan 1 kohdassa todetaan, että ”[k]ansallisilla viranomaisilla tai elimillä, jotka valvovat tai panevat täytäntöön perusoikeuksien, mukaan lukien oikeus syrjimättömyyteen, suojelua koskevan unionin oikeuden mukaisia velvoitteita liitteessä III tarkoitettujen suuririskisten tekoälyjärjestelmien käytön yhteydessä, on oltava valtuudet pyytää ja saada käyttöönsä tämän asetuksen nojalla luotu tai ylläpidetty dokumentaatio ymmärrettävällä kielellä ja saavutettavassa muodossa, kun dokumentaation käyttö on tarpeen, jotta ne voisivat suorittaa tehokkaasti tehtävänsä omalla lainkäyttöalueellaan” (katso [77 artikla](#)).

Jos yhdenvertaisuuselinten / kansallisten ihmisoikeustoimijoiden, markkinavalvontaviranomaisten ja muiden 77 artiklan mukaisten elinten väliselle tietojen jakamiselle luodaan oikeusperustat (katso yhteistyötä koskeva kohta), yhdenvertaisuuselimet ja kansalliset ihmisoikeustoimijat voivat saada pääsyn markkinavalvontaviranomaisten 71 artiklan 4 kohdan ja 49 artiklan 4 kohdan nojalla saamiin tietoihin.

242. Tekoälyasetus, johdanto-osan 177 kohta.

3.6.2. Yhdenvertaisuuselinten ja kansallisten ihmisoikeustoimijoiden rooli liitteessä III lueteltujen suuririskisten tekoälyjärjestelmien EU:n tietokannassa

Tietokannan perustamisen aikana

- ▶ Osallistua asianomaisina asiantuntijoina²⁴³ (mahdollisesti Equinetin kautta tai muulla tavoin) tietokannan perustamiseen, mukaan lukien sen varmistaminen, että tietokanta täyttää esteettömyysvaatimukset.

Tietokannan käyttöönoton jälkeen

- ▶ Kannustaa viranomaisia rekisteröimään järjestelmiä tietokantaan vapaaehtoisesti, kun viranomaiset toimivat sellaisten tekoälyjärjestelmien käyttöönottajina, joita ei pidetä suuririskisinä. Tämä rekisteröintisuositus koskee myös yksityisiä tahoja, jotka toimivat suuririskisten tekoälyjärjestelmien käyttöönottajina (erityisesti vakuutus- ja pankkitoimintasektoreilla).
- ▶ Laatia koordinointimalli sellaisten kansallisten toimivaltaisten viranomaisten kanssa, joilla on pääsy tietokannan ei-julkiseen osioon.
- ▶ Edistää sitä, että tekoälyasetuksen täytäntöönpanon kansallisessa lainsäädännössä todetaan selkeästi, että yhdenvertaisuuselinten ja kansallisten ihmisoikeustoimijoiden tulee saada pääsy kansallisille viranomaisille annettuihin ja EU:n tietokannan ei-julkisen osion tietoihin.
- ▶ Seurata tietokantaan rekisteröityjä tekoälyjärjestelmiä sellaisten suuririskisten tekoälyjärjestelmien tunnistamiseksi, joita joko yhdenvertaisuuselinten tai markkinavalvontaviranomaisten on tutkittava tarkemmin niiden syrjintäriskin vuoksi (mahdollisesti yhteistyössä muiden sidosryhmien, kuten kansalaisjärjestöjen, kanssa).
- ▶ Seurata rekisteröityjä tekoälyjärjestelmiä, joita ei ole pidetty 6 artiklan 3 kohdan mukaisesti suuririskisinä, ja käyttää itsearviointien yhteenvedoja sen määrittämiseksi, olisiko tällaisia järjestelmiä pidettävä suuririskisinä. Jos näin on, asiasta on ilmoitettava markkinavalvontaviranomaiselle, ja sitä on pyydetävä suorittamaan arviointi 80 artiklan mukaisessa menettelyssä, joka koskee tarjoajien muuksi kuin suuririskiseksi luokittelemia järjestelmiä.
- ▶ Seurata tarjoajien rekisteröimiä luottopisteytyksiin ja vakuutuksiin liittyviä tekoälyjärjestelmiä ja tarvittaessa pyytää käyttöönottajilta tietoja, joita ei ole tietokannassa, kuten FRIA-arviointeja.
- ▶ Käyttää tietokannan julkista osiota tietoisuuden lisäämiseen siitä, miten tekoälyjärjestelmiä käytetään julkisella sektorilla.
- ▶ Seurata, miten kansalaisjärjestöt, toimittajat, yksityishenkilöt ja muut asiaan kuuluvat instituutiot käyttävät tietokantaa, ja ehdottaa päivityksiä komissiolle ja tekoälyneuvostolle. Erityisesti on seurattava, ovatko FRIA-arviointien yhteenvedojen sisältämät tiedot riittäviä syrjimättömyyteen kohdistuvien riskien arvioimiseksi.

243. Tekoälyasetus, 71 artiklan 1 kohta.



4. Tekoälyjärjestelmien vaatimusten avoimuus

4.1. Tausta ja merkittävyys

Tekoälyasetuksen 50 artiklassa säädetään tekoälyjärjestelmien tarjoajien ja käyttöönottajien avoimuusvelvoitteista. Sen mukaan tiedot on "annettava asiaankuuluville luonnollisille henkilöille selkeällä ja selvästi erottuvalla tavalla viimeistään ensimmäisen vuorovaikutuksen tai altistumisen yhteydessä",²⁴⁴ ja tietojen on oltava sovellettavien esteettömyysvaatimusten mukaisia.

Käyttöönottajien on ilmoitettava luonnollisille henkilöille, kun käyttöön otetaan

- ▶ tunteentunnistusjärjestelmä²⁴⁵ tai biometrinen luokittelujärjestelmä²⁴⁶
- ▶ syvävääreännöksiä tuottava tekoälyjärjestelmä²⁴⁷

244. Tekoälyasetus, 50 artiklan 5 kohta.

245. Tekoälyasetus, 3 artiklan 39 kohta.

246. Tekoälyasetus, 3 artiklan 40 kohta.

247. Tekoälyasetus, 3 artiklan 60 kohta: "syvävääreännöksellä" [tarkoitetaan] tekoälyllä tuotettua tai käsiteltyä kuva-, ääni- tai videosisältöä, joka muistuttaa olemassa olevia henkilöitä, esineitä, paikkoja, toimijoita tai tapahtumia ja joka antaa henkilölle valheellisen vaikutelman siitä, että se on aito tai totuudenmukainen".

- tekoälyjärjestelmä, ”joka tuottaa tai manipuloi tekstiä, jonka julkaisemisen tarkoituksena on tiedottaa yleisölle yleistä etua koskevista asioista.”²⁴⁸

Kun tarjoajat suunnittelevat ja kehittävät luonnollisten henkilöiden kanssa vuorovaikutuksessa olevia tekoälyjärjestelmiä, luonnollisten henkilöiden tulee olla tietoisia tästä vuorovaikutuksesta eikä heille voi luoda olettaa, että he ovat vuorovaikutuksessa ihmisen kanssa. Tätä velvoitetta sovelletaan, ”ellei tämä ole ilmeistä sellaisen luonnollisen henkilön näkökulmasta, joka on suhteellisen valistunut, tarkkaavainen ja huolellinen ottaen huomioon olosuhteet ja käytön asiayhteys.”²⁴⁹

Kun tekoälyllä tuotetaan sisältöä, tekoälyjärjestelmien tarjoajien on tarjottava ”tehokkaita, yhteentoimivia, vakaita ja luotettavia”²⁵⁰ teknisiä ratkaisuja, joiden koneluettavien merkintöjen avulla voidaan havaita, että sisältö on keinotekoisesti tuotettua tai manipuloitua. Tämä velvoite riippuu kuitenkin teknisestä toteutettavuudesta, yleisesti tunnustetusta alan viimeisimmästä kehityksestä ja tuotetun sisällön tyypeistä. Tämä velvoite koskee myös yleiskäyttöisten tekoälyjärjestelmien tarjoajia.²⁵¹

Euroopan komission yhteydessä toimiva Euroopan tekoälytoimisto voi myös ”kanustaa ja helpottaa käytäntönsääntöjen laatimista unionin tasolla”²⁵² keinotekoisesti tuotetun tai manipuloidun sisällön tunnistamista ja merkintää varten sekä antaa täytäntöönpanosäädöksiä kyseisten käytäntönsääntöjen hyväksymiseksi. Syyskuun 4. päivänä 2025 käynnistettiin kuuleminen, jonka tarkoituksena on aloittaa suunta- viivojen ja käytäntönsääntöjen laatimisprosessi.²⁵³ Jos tulevat käytäntönsäännöt eivät ole riittäviä, komissio voi antaa täytäntöönpanosäädöksiä, joissa täsmennetään yhteiset säännöt.

Kolme tärkeää seikkaa, jotka on muistettava:

1. tekoälyasetuksen 50 artiklaa sovelletaan kaikkiin tekoälyjärjestelmiin riippumatta siitä, ovatko ne suuririskisiä järjestelmiä vai eivät²⁵⁴
2. tekoälyasetuksen 50 artiklan noudattaminen ei tee tekoälyjärjestelmän käytöstä tai tuotoksesta laillista;²⁵⁵ esimerkiksi jotkin tekoälyjärjestelmät ovat kiellettyjä 5 artiklan nojalla
3. tekoälyasetuksen 50 artiklan velvoitteita ”ei sovelleta tekoälyjärjestelmiin, joita on lain mukaan sallittua käyttää rikosten paljastamiseen, estämiseen tai tutkimiseen ja rikoksiin liittyviin syytetoimiin.”²⁵⁶

248. Tekoälyasetuksen 50 artiklan 4 kohdan toisessa alakohdassa selvennetään, että käyttöönottajien ei tarvitse ilmoittaa yleisölle keinotekoisesti tuotetusta sisällöstä, ”jos tekoälyn tuottama sisältö on läpikäynyt ihmisen suorittaman arviointiprosessin tai toimituksellisen valvonnan ja jos luonnollisella henkilöllä tai oikeushenkilöllä on toimituksellinen vastuu sisällön julkaisemisesta.”

249. Tekoälyasetus, 50 artiklan 1 kohta.

250. Tekoälyasetus, 50 artiklan 2 kohta.

251. Tekoälyasetus, 3 artiklan 66 kohta.

252. Tekoälyasetus, 50 artiklan 7 kohta.

253. ”Commission launches consultation to develop guidelines and Code of Practice on transparent AI systems”; 4. syyskuuta 2025, saatavilla osoitteessa <https://digital-strategy.ec.europa.eu/en/news/commission-launches-consultation-develop-guidelines-and-code-practice-transparent-ai-systems>, viitattu 11. marraskuuta 2025.

254. Tekoälyasetus, 50 artiklan 6 kohta ja johdanto-osan kappale 132.

255. Tekoälyasetus, johdanto-osan kappale 137.

256. Tekoälyasetus, 50 artiklan 1 kohta.

Yhteys muihin oikeudellisiin kehyksiin

Avoimuus ja valvonta kuuluvat Euroopan neuvoston puiteyleissopimuksen periaatteisiin.²⁵⁷ Puiteyleissopimuksen 15 artiklan 2 kohdassa määrätään, että "[k]ukin sopimuspuoli pyrkii varmistamaan, sikäli kuin se on asiasyhteyden kannalta asianmukaista, että tekoälyjärjestelmien kanssa vuorovaikutuksessa oleville henkilöille ilmoitetaan, että he ovat vuorovaikutuksessa tällaisten järjestelmien eivätkä ihmisen kanssa."

4.1.1. Yhdenvertaisuuselinten ja kansallisten ihmisoikeustoimijoiden rooli tekoälyjärjestelmien vaatimusten avoimuudessa

Tätä artiklaa voidaan tarkastella 5 artiklassa lueteltujen kiellettyjen käyttötarkoitusten näkökulmasta:

- ▶ Kun 50 artiklaa tarkastellaan yhdessä 5 artiklan 1 kohdan a ja b alakohdan kanssa, voidaan puoltaa näiden alakohtien mukaisia kieltoja, kun artiklan mukainen avoimuusvelvoite on riittämätön perusoikeuksiin kohdistuvien haitallisten vaikutusten ehkäisyyn. Tämä pitäisi sisältää myös tilanteet, joissa tekoälyllä tuotetun ja manipuloidun sisällön tekniset ratkaisut ja yleisesti tunnetun viimeisimmän kehityksen mukaiset tunnistetut eivät ole "tehokkaita, yhteentoimivia, vakaita ja luotettavia".²⁵⁸
- ▶ Tekoälyasetuksen 50 artiklaa voidaan myös tarkastella yhdessä seuraavien kanssa: 5 artiklan 1 kohdan f alakohta, jossa kielletään tunteiden päättelemiseen työpaikalla ja oppilaitoksissa käytettävät järjestelmät, sekä 5 artiklan 1 kohdan g alakohta, jossa kielletään biometriset luokittelujärjestelmät, jos "luonnolliset henkilöt luokitellaan heidän biometristen tietojensa perusteella rodun, poliittisten mielipiteiden, ammattiliiton jäsenyyden, uskonnollisen tai filosofisen vakaumuksen, seksuaalisen käyttäytymisen tai seksuaalisen suuntautumisen perusteella".²⁵⁹ Asetuksen 50 artikla ei tee kielletyistä tekoälyjärjestelmistä laillisia.
- ▶ "Riskien vähentämiseen" liittyviä strategioita voidaan ehkäistä tekemällä tai teettämällä sellaisia tilanteita ja olosuhteita koskevia oikeudellisia tutkimuksia, joissa 50 artiklan mukaisia avoimuusvelvoitteita saatetaan käyttää 5 artiklan kieltojen kiertämiseen. Tällaiset tutkimukset olisi julkaistava, jotta tarjoajille ja käyttöönottajille voidaan tiedottaa, ettei heidän tule yrittää kiertää kieltoja. Tutkimuksia voidaan koordinoita yhdessä erilaisten yhdenvertaisuuselinten ja/tai kansallisten ihmisoikeustoimijoiden kanssa.

257. Euroopan neuvoston puiteyleissopimus, 8 artikla.

258. Tekoälyasetus, 50 artiklan 2 kohta.

259. Tekoälyasetus, 5 artiklan 1 kohdan g alakohta.



5. Täytäntöönpano

5.1. Perusoikeuksia suojelevien viranomaisten valtuudet

5.1.1. Tausta ja merkittävyys

Tekoälyasetuksen 77 artiklassa annetaan yhdenvertaisuuselimille uusia valtuuksia arvioida tekoälyjärjestelmien kautta tapahtuvaa syrjintää. Nämä valtuudet sisältävät oikeuden saada dokumentaatio käyttöön, oikeuden testata järjestelmiä ja oikeuden tehdä yhteistyötä markkinavalvontaviranomaisten ja tekoälyjärjestelmiin liittyvien toimijoiden kanssa. Yhdenvertaisuuselimiä ei kuitenkaan automaattisesti pidetä 77 artiklassa tarkoitettuina asiaankuuluvina eliminä.

Kumulatiiviset edellytykset sille, että yhdenvertaisuuselin voi olla 77 artiklan mukainen viranomainen

1. Niitä on pidettävänä "[k]ansallis[ina] viranomaisi[na] tai elimi[nä], jotka valvovat tai panevat täytäntöön perusoikeuksien, mukaan lukien oikeus syrjimättömyyteen, suojelua koskevan unionin oikeuden mukaisia velvoitteita"²⁶⁰

²⁶⁰. Tekoälyasetus, 77 artiklan 1 kohta.

2. Jäsenvaltion on pitänyt nimenomaisesti nimetä yhdenvertaisuuselin tai muu perusoikeuksia valvova elin tällaiseksi elimeksi, sisällyttää se komissiolle ja muille jäsenvaltioille ilmoitettavaan luetteloon ja julkaista luettelo 2. marraskuuta 2024 mennessä. Jäsenvaltioiden on ”pidettävä [luettelo] ajan tasalla”,²⁶¹ mikä osoittaa, että luetteloon voidaan myöhemmin lisätä yhdenvertaisuuselimiä tai muita perusoikeuksia valvovia elimiä, joita jäsenvaltiot eivät ole listanneet ensimmäisen ilmoituksen määräaikaan mennessä. Luettelosta voidaan myös poistaa yhdenvertaisuuselimiä ja muita elimiä.

Kun tässä osiossa ja muualla tässä asiakirjassa viitataan yhdenvertaisuuselimiin, termillä tarkoitetaan nimenomaan yhdenvertaisuuselimiä, jotka on nimetty sovellettavassa jäsenvaltiossa tekoälyasetuksen 77 artiklan mukaisiksi elimiksi.

Yhdenvertaisuuselinten rooli Euroopan neuvoston puiteyleissopimuksessa

Euroopan neuvoston puiteyleissopimuksen mukaan yhdenvertaisuuselimet ja ihmisoikeustoimijat ovat toimivaltaisia toimimaan osana valvontatoimenpiteitä, joilla varmistetaan puiteyleissopimuksen velvoitteiden noudattaminen.²⁶² Puiteyleissopimuksessa todetaan myös, että ”[k]ukin sopimuspuoli varmistaa, että tällaiset mekanismit hoitavat tehtävänsä riippumattomasti ja puolueettomasti ja että niillä on tarvittavat valtuudet, asiantuntemus ja resurssit, jotta ne voivat tehokkaasti hoitaa tehtävänsä valvoa tämän yleissopimuksen velvoitteiden noudattamista”.²⁶³ Tämä on merkittävä ero Euroopan neuvoston puiteyleissopimuksen ja tekoälyasetuksen välillä: tekoälyasetuksen mukaan valvonta ja täytäntöönpano kuuluvat markkinavalvontaviranomaisten tehtävään, kun taas yhdenvertaisuuselimet ja kansalliset ihmisoikeustoimijat on tunnustettu 77 artiklan mukaisiksi elimiksi, mutta ne eivät osallistu valvontatoimenpiteisiin. Euroopan neuvoston puiteyleissopimuksen mukaan yhdenvertaisuuselimet ja kansalliset ihmisoikeustoimijat voidaan kuitenkin nimetä osaksi valvonta- ja täytäntöönpanoviranomaisia.

Yhdenvertaisuuselinten valtuudet 77 artiklan nojalla

Oikeus pyytää ja saada käyttöön dokumentaatio

Yhdenvertaisuuselimillä ja kansallisilla ihmisoikeustoimijoilla on oltava ”liitteessä III tarkoitettujen suuririskisten tekoälyjärjestelmien käytön yhteydessä... valtuudet pyytää ja saada käyttöönsä tämän asetuksen nojalla luotu tai ylläpidetty dokumentaatio ymmärrettävällä kielellä ja saavutettavassa muodossa”.²⁶⁴ Yhdenvertaisuuselinten ja kansallisten ihmisoikeustoimijoiden tulisi tulkita ja testata tämän artiklan käyttöä, jotta ne voivat pyytää käyttöönsä tehtäviensä toteuttamiseen tarvittavaa tekoälyasetuksen mukaista dokumentaatiota. Yhdenvertaisuuselinten ja kansallisten ihmisoikeustoimijoiden on ilmoitettava maansa markkinavalvontaviranomaisille,

261. Tekoälyasetus, 77 artiklan 2 kohta.

262. Euroopan neuvosto (2024), tekoälyä ja ihmisoikeuksia, demokratiaa ja oikeusvaltioperiaatetta koskeva puiteyleissopimus, selitysmuistio, kohta 63.

263. Euroopan neuvoston puiteyleissopimus, 26 artikla.

264. Tekoälyasetus, 77 artiklan 1 kohta.

kun ne pyytävät dokumentaatiota. Tätä dokumentaatiota voidaan käyttää yksilöihin tai ryhmiin kohdistuvien syrjintähaittojen tunnistamiseen. Yksi esimerkki tästä on tilanne, jossa tekoälyjärjestelmä toimii tummaihoisilla naisilla muita heikommin ja estää heitä saamasta sosiaaliturvaetuksia, vaikka tekoälyjärjestelmä toimisi tummaihoisilla henkilöillä muuten hyvin.²⁶⁵

Oikeus testaukseen

Jos dokumentaatio on riittämätöntä ”sen selvittämiseen, onko perusoikeuksia suojaavan unionin oikeuden mukaisia velvoitteita rikottu,”²⁶⁶ yhdenvertaisuuselimet ja kansalliset ihmisoikeustoiijat voivat pyytää markkinavalvontaviranomaisia ”järjestä[mään] suuririskisen tekoälyjärjestelmän testau[ksen] teknisin keinoin... kohtuullisen ajan kuluessa”.²⁶⁷ Tällaisiin puutteisiin voi kuulua esimerkiksi se, että tarjoajat jättävät raportoimatta useiden oikeudenmukaisuusmittareiden tulokset tai määrittelevät vaikutusten piiriin kuuluvat ryhmät suppeasti, jolloin tiettyjen syrjinnän muotojen, erityisesti intersektionaalisen syrjinnän, arviointi on mahdotonta (Equinet, 2025). Yhdenvertaisuuselinten ja kansallisten ihmisoikeustoimijoiden on suositeltavaa tehdä tiivistä yhteistyötä markkinavalvontaviranomaisten kanssa testauksen aikana.

Oikeus yhteistyöhön markkinavalvontaviranomaisten ja tekoälyjärjestelmiin liittyvien toimijoiden kanssa

- ▶ Kun suuririskisten tekoälyjärjestelmien tarjoajat ilmoittavat markkinavalvontaviranomaisille vakavista vaaratilanteista,²⁶⁸ jotka rikkovat perusoikeuksien, kuten oikeuden syrjimättömyyteen, suojaamiseen tarkoitettua unionin lainsäädäntöä,²⁶⁹ markkinavalvontaviranomaisten on ilmoitettava siitä yhdenvertaisuuselimille ja kansallisille ihmisoikeustoimijoille.²⁷⁰
- ▶ Markkinavalvontaviranomaisten on arvioitava perusoikeuksille ”riskin aiheuttavat tekoälyjärjestelmät”²⁷¹, mukaan lukien järjestelmät, joiden riski kohdistuu haavoittuvassa asemassa oleviin ryhmiin.
 - Kun arviointeja tehdään, markkinavalvontaviranomaisten ”on ilmoitettava asiasta”²⁷² yhdenvertaisuuselimille ja kansallisille ihmisoikeustoimijoille ”ja tehtävä tiivistä yhteistyötä niiden kanssa”.

265. Jos tarvitset kattavamman analyysin siitä, 1) mitä asiakirjoja yhdenvertaisuuselimet voivat saada käyttöönsä ja 2) miten sovellettujen teknisten standardien perusteella kootun teknisen dokumentaation perusparametreja voidaan ymmärtää, katso Equinet, 2025.

266. Tekoälyasetus, 77 artiklan 3 kohta.

267. Ibid.

268. Tekoälyasetus, 73 artiklan 1 kohta.

269. Tekoälyasetus, 3 artiklan 49 kohta. Vakavalla vaaratilanteella tarkoitetaan ”vaaratilannetta tai tekoälyjärjestelmän toimintahäiriötä, joka suoraan tai välillisesti johtaa... c) perusoikeuksien suojaamiseen tarkoitettujen unionin oikeuden mukaisten velvoitteiden rikkomi[seen]”.

270. Tekoälyasetus, 73 artiklan 7 kohta.

271. Tekoälyasetus, 79 artiklan 1 kohta, ja Euroopan parlamentin ja neuvoston asetukset (EU) 2019/1020, 3 artiklan 19 kohta.

272. Tekoälyasetus, 79 artiklan 2 kohta.

- Myös asianmukaisten tekoälyjärjestelmiin liittyvien toimijoiden on tehtävä yhteistyötä markkinaevalvontaviranomaisten, yhdenvertaisuuselinten ja kansallisten ihmisoikeustoimijoiden kanssa.²⁷³
- Markkinaevalvontaviranomaiset voivat arviointinsa perusteella vaatia tekoälyjärjestelmiin liittyviä toimijoita ryhtymään korjaaviin toimiin, vetämään tekoälyjärjestelmän pois markkinoilta tai soveltamaan palautusmenettelyä.²⁷⁴
- ▶ Yhdenvertaisuuselinten ja kansallisten ihmisoikeustoimijoiden on tehtävä yhteistyötä markkinaevalvontaviranomaisten kanssa ja avustettava niitä, kun arvioidaan, aiheuttaako suuririskisten järjestelmien järjestelyn ulkopuolelle jätetty tekoälyjärjestelmä merkittävän riskin perusoikeuksille.
- ▶ Markkinaevalvontaviranomaisten on arvioitava, onko ”tekoälyjärjestelmä, jonka tarjoaja on luokitellut 6 artiklan 3 kohdan mukaisesti ei-suuririskiseksi... tosiasiaa suuririskinen”²⁷⁵ perusoikeuksiin kohdistuvan riskin vuoksi. Yhdenvertaisuuselimet voivat auttaa markkinaevalvontaviranomaisia tässä arvioinnissa.
- ▶ Markkinaevalvontaviranomaisten on konsultoitava yhdenvertaisuuselimiä ja kansallisia ihmisoikeustoimijoita myös silloin, kun suuririskinen tekoälyjärjestelmä on tekoälyasetuksen mukainen mutta aiheuttaa silti riskin perusoikeuksille.²⁷⁶

Näin ollen yhdenvertaisuuselimet ja kansalliset ihmisoikeustoimijat voivat osallistua markkinaevalvontaviranomaisten tutkimuksiin ja mahdollisesti ehdottaa asiaankuuluvia korjaavia toimia, kuten tekoälyjärjestelmän poistamista markkinoilta, koska ne voivat olla mukana avustamassa markkinaevalvontaviranomaisia sen selvittämisessä, onko mahdollisesti syrjivä tekoälyjärjestelmä tekoälyasetuksessa säädettyjen velvoitteiden vastainen.

Kun näitä valtuuksia käytetään, ne voivat olla tehokkaita tekoälyjärjestelmiin liittyvän syrjinnän arvioinnissa ja korjaamisessa.

Lisäksi on tärkeää korostaa, että tekoälyasetus ”ei rajoita perusoikeuksien suojelusta annetun unionin oikeuden soveltamista valvovien asiaankuuluvien kansallisten viranomaisten tai elinten, mukaan lukien tasa-arvoelimet..., toimivaltaa, tehtäviä, valtuuksia ja riippumattomuutta.”²⁷⁷ Toisin sanoen tutkimukset, joissa arvioidaan tekoälyasetuksen noudattamista, eivät vaikuta tutkimuksiin, joissa arvioidaan yhdenvertaisuuslainsäädännön noudattamista.²⁷⁸ Samoin asianomaisilla henkilöillä on oikeus tehdä valitus sekä tekoälyasetuksen 85 artiklan että yhdenvertaisuuslainsäädännön nojalla.

273. Ibid.

274. Huomaus: Euroopan parlamentin ja neuvoston asetus (EU) 2019/1020, 18 artikla: tekoälyjärjestelmiin liittyville toimijoille on annettava mahdollisuus tulla kuulluksi ennen tällaisia toimia.

275. Tekoälyasetus, 80 artiklan 1 kohta.

276. Tekoälyasetus, 82 artiklan 1 kohta.

277. Tekoälyasetus, johdanto-osan kappale 157.

278. Katso myös tekoälyasetuksen johdanto-osan kappale 45: tekoälyasetus ei vaikuta unionin syrjimättömyyslainsäädännön mukaisiin kieltoihin.

5.1.2. Yhdenvertaisuuselinten ja kansallisten ihmisoikeustoimijoiden rooli tekoälyasetuksen 77 artiklassa

- ▶ Puoltaa nimitystä 77 artiklan mukaisiksi elimiksi.
- ▶ Asetuksen 77 artiklan mukaisina eliminä käyttämällä oikeutta pyytää ja saada käyttöön dokumentaatio:
 - Laatia Equinetin työn pohjalta vankkoja perusteluja, jotka tukevat oikeutta saada tietoja käyttöön (katso Equinet, 2025). Muutoin yritykset ja viranomaiset todennäköisesti haastavat yhdenvertaisuuselimet ja kansalliset ihmisoikeustoimijat pyrkiessään estämään pääsyn tietoihin.
 - Kehittää käytettävissä olevien tietojen perusteella testitapauksia, joiden avulla voidaan selvittää, ovatko tiedot asianmukaisia toimeksiannon toteuttamisen kannalta.
 - Käyttää saatua dokumentaatiota syrjinnän aiheuttamien haittojen tutkimiseen.
 - Seurata mahdollista etiikkapesua ja arvioida, kuinka tekoälyjärjestelmiin liittyvät toimijat ovat määrittäneet ryhmät vinoumien testauksessa.
- ▶ Asetuksen 77 artiklan mukaisina eliminä testauksen kontekstissa:
 - Varmistaa, että niillä on riittävät resurssit tehokkaaseen yhteistyöhön testausta johtavien markkinaevalvontaviranomaisten kanssa. Tämä voi tarkoittaa sisäistä teknistä asiantuntemusta, muun kuin teknisen henkilöstön koulutusta yhteistyöhön teknisten asiantuntijoiden kanssa tai kumppanuuksien luomista ulkopuolisten toimijoiden kanssa (katso lisätietoja yhteistyötä koskevasta kohdasta).
 - Laatia malleja yhteistyöhön markkinaevalvontaviranomaisten kanssa.
- ▶ Asetuksen 77 artiklan mukaisina eliminä markkinaevalvontaviranomaisten täytäntöönpanotoimien kontekstissa:
 - Lisätä tietoisuutta tekoälyjärjestelmien syrjintäriskeistä esimerkiksi julkaisemalla päätöksiä.
 - Seurata ja julkaista toimia, jotka liittyvät rooliin 77 artiklan mukaisina eliminä, jotta voidaan lisätä yleistä tietoisuutta roolista ja havainnollistaa elinten tarpeellisuutta tekoälyjärjestelmiin liittyvän yhdenvertaisuuden ja syrjimättömyyden edistämiseksi.
- ▶ Antaa ohjeita ja edistää sitä, että Euroopan komissio huomioi perusoikeudet:
 - Euroopan komissio ”laatii yksinkertaistetun teknisen dokumentaatiolomakkeen, joka on suunnattu pienten ja mikroyritysten tarpeisiin.”²⁷⁹ Ihmisten oikeuksiin kohdistuvat haitat eivät korreloi suuririskisiä tekoälyjärjestelmiä kehittävien yritysten koon kanssa. Yhdenvertaisuuselinten ja kansallisten ihmisoikeustoimijoiden on korostettava, että välttämättömiä tietoja ei saa jättää pois dokumentaatiosta.
 - Euroopan komissiolle siirretään valta antaa delegoituja säädöksiä 97 artiklan mukaisesti (vallan siirto) liitteen IV muuttamiseksi (suuririskisten tekoälyjärjestelmien tekninen dokumentaatio).

279. Tekoälyasetus, 11 artiklan 1 kohdan toinen alakohta.

- Osallistua vakavien vaaratilanteiden raportointia koskevien Euroopan komission ohjeiden laatimiseen. Euroopan komission odotetaan laativan ohjeet vakavien vaaratilanteiden raportointiin 2. elokuuta 2025 mennessä.²⁸⁰ Näihin ohjeisiin sisältyy todennäköisesti koordinointi ja menettelyt tietojen siirtoon markkinavalvontaviranomaisilta yhdenvertaisuuselimille ja kansallisille ihmisoikeustoimijoille. Yhdenvertaisuuselinten tulisi harkita näiden ohjeiden laadintaan osallistumista Equinetin tai muiden elinten kautta.
- Katso myös näiden suuntaviivojen yhteydessä luetellut suositukset, jotka liittyvät esimerkiksi luokitteluun, suuririskisten ja kiellettyjen tekoälyjärjestelmien luettelon muuttamiseen ja perusoikeusvaikutusten arviointiin.

5.2. Oikeussuojakeinot

5.2.1. Tausta ja merkitys

Tekoälyasetus tarjoaa luonnollisille henkilöille ja oikeushenkilöille oikeuden tehdä valituksia markkinavalvontaviranomaisille ja luonnollisille henkilöille oikeuden saada selvitys. Kumpakaan näistä ei kuitenkaan voida sellaisenaan pitää tosiasiallisena oikeutena.

Oikeus tehdä valitus

Asianomainen henkilö voi tehdä valituksen markkinavalvontaviranomaiselle (85 artikla). Valitus ”on otettava huomioon markkinavalvontatoimien toteuttamisessa”²⁸¹ ja käsitellään ”markkinavalvontaviranomaisten sitä varten käyttöön ottamien menettelyjen mukaisesti”.²⁸² Markkinavalvontaviranomaisilla ei kuitenkaan ole yleistä velvollisuutta ryhtyä toimiin asianomaisen henkilön tekemän valituksen perusteella. Valituksen tekijällä ei ole asiavaltuutta prosessissa, vaikka valitus otetaan ”huomioon markkinavalvontatoimien toteuttamisessa”.²⁸³ Näin ollen tekoälyasetuksen mukaista valitusoikeutta voidaan pitää parhaimmillaankin vain osittaisena oikeutena. Tämä oikeus ei kuitenkaan rajoita muiden kansallisissa ja unionin lainsäädännöissä säädettyjen oikeussuojakeinojen käyttöä.²⁸⁴

Jos tekoälyjärjestelmä loukkaa henkilön perusoikeuksia, henkilön on harkittava valituksen tekemistä perusoikeuksia valvovalle elimelle, kuten yhdenvertaisuuselimelle, jos kyseessä on syrjintä. Kun kyse on henkilötiedoista, asianomaisella henkilöllä voi olla myös mahdollisuus tehdä valitus sovellettavalle tietosuojaviranomaiselle.²⁸⁵

280. Tekoälyasetus, 73 artiklan 7 kohta.

281. Tekoälyasetus, 85 artikla.

282. Euroopan parlamentin ja neuvoston asetus (EU) 2019/1020, 11 artiklan 7 kohdan a alakohta.

283. Tekoälyasetus, 85 artikla. Asianomainen osapuoli voi myös harkita muita muutoksenhakukeinoja, kuten Euroopan parlamentin ja neuvoston direktiiviä (EU) 2020/1828, annettu 25 päivänä marraskuuta 2020, kuluttajien yhteisten etujen suojaamiseksi nostettavista edustajakanteista ja direktiivin 2009/22/EY kumoamisesta. Katso myös tekoälyasetus, 110 artikla.

284. Tekoälyasetus, johdanto-osan kappale 170.

285. GDPR, 77–79 artikla.

Oikeus saada selvitys

Tekoälyasetus tarjoaa asianomaisille henkilöille myös oikeuden selvitykseen (86 artikla), kun käyttöönottaja tekee päätöksen ”liitteessä III luetellun suuririskisen tekoälyjärjestelmän tuotoksen perusteella ... ja [päätöksellä] on oikeusvaikutuksia tai... kyseiseen henkilöön vastaavanlainen merkittävä vaikutus, jonka kyseinen henkilö katsoo *vaikuttavan haitallisesti* hänen terveyteensä, turvallisuutensa tai *perusoikeuksiinsa*.”²⁸⁶ Selvityksen on sisällettävä ”selkeät ja merkitykselliset selitykset tekoälyjärjestelmän roolista päätöksentekomenettelyssä ja tehdyn päätöksen pääkohdista.”²⁸⁷

Milloin tekoälyasetuksen mukaista oikeutta selitykseen sovelletaan?

Tekoälyasetuksen mukaista oikeutta selitykseen sovelletaan kuitenkin vain, jos samasta oikeudesta ”ei ole muuta säädetty unionin oikeudessa”.²⁸⁸ Kun henkilötietojen käsittelyyn käytetään suuririskistä tekoälyjärjestelmää, sovelletaan GDPR:n 15 artiklan 1 kohdan h alakohdassa säädettyä oikeutta saada tietoja, jotka sisältävät ”merkitykselliset tiedot käsittelyyn liittyvästä logiikasta”²⁸⁹.

Lisäksi on tärkeää korostaa, että GDPR:n 22 artiklan 1 kohdassa määrätään rekisteröidyn oikeudesta olla joutumatta ”sellaisen päätöksen kohteeksi, joka perustuu pelkästään automaattiseen käsittelyyn, kuten profilointiin, ja jolla on häntä koskevia oikeusvaikutuksia tai joka vaikuttaa häneen vastaavalla tavalla merkittävästi”. Tämä tarkoittaa, että henkilötietoja käyttäviä suuririskisiä tekoälyjärjestelmiä, jotka tuottavat ”oikeusvaikutuksia tai... vaikutta[vat] asianomaisiin henkilöihin vastaavasti merkittävästi tavalla” voidaan käyttää vain tietyissä GDPR:n 22 artiklan 2 kohdan poikkeustilanteissa, kun käyttö

- (a) on välttämätön[tä] rekisteröidyn ja rekisterinpitäjän välisen sopimuksen tekemistä tai täytäntöönpanoa varten
- (b) on hyväksytty[ä] rekisterinpitäjään sovellettavassa unionin oikeudessa tai jäsenvaltion lainsäädännössä, jossa vahvistetaan myös asianmukaiset toimenpiteet rekisteröidyn oikeuksien ja vapauksien sekä oikeutettujen etujen suojaamiseksi
- (c) perustuu rekisteröidyn nimenomaiseen suostumukseen.

Lisäksi sanaa ”yksinomaan” on tulkittu Schufa-tapauksessa siten, että se kattaa myös automaattisen käsittelyn, joka saattaa olla vain osa päätöstä, mutta jolla on silti ”olennainen vaikutus”.²⁹⁰

286. Tekoälyasetus, 86 artiklan 1 kohta. (Korostus lisätty.)

287. Tekoälyasetus, 86 artiklan 1 kohta.

288. Tekoälyasetus, 86 artiklan 3 kohta.

289. GDPR, 15 artiklan 1 kohdan h alakohhta: ”Rekisteröidyllä on oikeus saada rekisterinpitäjältä vahvistus siitä, että häntä koskevia henkilötietoja käsitellään tai että niitä ei käsitellä, ja jos näitä henkilötietoja käsitellään, oikeus saada pääsy henkilötietoihin sekä seuraavat tiedot... h) automaattisen päätöksenteon, muun muassa 22 artiklan 1 ja 4 kohdassa tarkoitetun profiloinnin olemassaolo, sekä ainakin näissä tapauksissa merkitykselliset tiedot käsittelyyn liittyvästä logiikasta samoin kuin kyseisen käsittelyn merkittävyys ja mahdolliset seuraukset rekisteröidylle.”

290. Unionin tuomioistuimen tuomio 7 päivänä joulukuuta 2023, *SCHUFA Holding (Scoring)*, C-634/21, EU:C:2023:957, 50 kohta.

Näin ollen tekoälyasetuksen 86 artikla voi olla tarpeen kahdessa tilanteessa:

1. kun henkilötietoja ei käytetä suuririskisessä tekoälyjärjestelmässä (muutoin sovellettaisiin GDPR:n 15 artiklan 1 kohdan h alakohtaa)
2. kun käsittelyyn liittyy henkilötietoja ja suuririskistä tekoälyjärjestelmää hyödyntävällä automaattisella käsittelyllä ei ole "olennaista vaikutusta" päätökseen (katso edellä oleva EUT:n Schufa-päätös).

Mikä on merkityksellinen selitys?

Tekoälyasetuksessa vaaditaan "selkeät ja merkitykselliset selitykset tekoälyjärjestelmän roolista päätöksentekomenettelyssä ja tehdyn päätöksen pääkohdista."²⁹¹ Tapauksessa *CK v. Dun & Bradstreet* annetusta tuomiosta voi olla tässä kohtaa hyötyä. Tuomioissa selvennettiin, että GDPR:ssä mainitut "merkitykselliset tiedot käsittelyyn liittyvästä logiikasta"²⁹² tarkoittavat menettelyn periaatteita "tiiviisti esitetyssä, läpinäkyvässä sekä ymmärrettävässä ja helposti saatavilla olevassa muodossa..., joita tosiasiallisesti sovelletaan kyseisen henkilön henkilötietojen hyödyntämiseen automatisoidusti tietyn tuloksen... saavuttamiseksi kyseisten henkilötietojen perusteella."²⁹³ Kuitenkaan "monimutkaista selitystä siinä käytettävistä algoritmeista tai koko algoritmin paljastamista ei välttämättä edellytetä".²⁹⁴

Liikesalaisuuksien suoja

Tekoälyasetuksessa todetaan, että "[o]ikeutta selvityksen saamiseen ei pitäisi soveltaa sellaisten tekoälyjärjestelmien käyttöön, joita koskevat poikkeukset tai rajoitukset johtuvat unionin oikeudesta tai kansallisesta lainsäädännöstä".²⁹⁵ Yksi tällainen poikkeus voisi olla liikesalaisuuksien suoja.²⁹⁶ Oikeutta selitykseen on punnittava kuitenkin tapauksen *CK v. Dun & Bradstreet* tapaan immateriaalioikeuksien, mukaan lukien liikesalaisuuksien, suojan suhteen. Kyseisessä tapauksessa tuomioistuimien katsoi, että oikeuksien punnitseminen kuuluu valvontaviranomaiselle tai toimivaltaiselle tuomioistuimelle eikä yritykselle.²⁹⁷ Tekoälyasetuksen osalta voidaan esittää samanlainen analoginen perustelu.

291. Tekoälyasetus, 86 artiklan 1 kohta.

292. GDPR, 15 artiklan 1 kohdan h alakohta.

293. Yhteisöjen tuomioistuimen tuomio (ensimmäinen jaosto) 27 päivänä helmikuuta 2025. *CK v Dun & Bradstreet Austria GmbH ja Magistrat der Stadt Wien*, C-203/22, ECLI:EU:C:2025:117, 66 kohta.

294. *Ibid.*, 60 kohta.

295. Tekoälyasetus, johdanto-osan kappale 171.

296. Direktiivin 2016/943 2 artiklan 1 kohta.

297. Yhteisöjen tuomioistuimen tuomio (ensimmäinen jaosto) 27 päivänä helmikuuta 2025. *CK v Dun & Bradstreet Austria GmbH ja Magistrat der Stadt Wien*, C-203/22, ECLI:EU:C:2025:117, 76 kohta.

5.2.2. Yhdenvertaisuuselinten ja kansallisten ihmisoikeustoimijoiden rooli oikeussuojakeinojen osalta

- ▶ Tiedottaa kansalaisille heidän oikeuksistaan. Osana velvollisuuttaan avustaa syrjinnän uhreja (direktiivit yhdenvertaisuuselimä koskevista normeista mukaisesti) yhdenvertaisuuselinten on tiedotettava ihmisille heidän oikeudestaan selitykseen ja oikeudesta tehdä valitus markkinavalvontaviranomaiselle tekoälyasetuksen nojalla ja tietosuojaviranomaiselle EU:n tietosuojalainsäädännön nojalla. Tämä edellyttää henkilöstön kouluttamista, jotta he osaavat tunnistaa tapaukset, joissa oikeutta selitykseen sovelletaan.
- ▶ Henkilöille on tiedotettava, että tämä oikeus on lisätoimenpide eikä korvaa oikeudellisiin toimiin ryhtymistä.

5.3. Yhteistyömekanismi

5.3.1. Tausta ja merkitys

Jotta yhdenvertaisuuselimet ja kansalliset ihmisoikeustoimijat voisivat toimia tehokkaasti ja käyttää tekoälyasetuksen mukaisia valtuuksiaan, niiden on tehtävä yhteistyötä oman maansa markkinavalvontaviranomaisten sekä muiden 77 artiklan mukaisten elinten, kuten tietosuojaviranomaisten, kanssa. Lisäksi kansalaisjärjestöjen kuuleminen hyödyttää yhdenvertaisuuselinten työtä.

5.3.2. Yhdenvertaisuuselinten ja kansallisten ihmisoikeustoimijoiden rooli yhteistyössä eri sidosryhmien kanssa

77 artiklan mukaisten elinten välinen yhteistyö

Yhdenvertaisuuselinten ja kansallisten ihmisoikeustoimijoiden on vakuutettava jäsenvaltioilleen, että 77 artiklan mukaisten elinten väliselle tietojenvaihdolle on muodostettu selkeä oikeusperusta, jos niin ei ole vielä tehty. Tekoälyasetuksessa säädetään tietojen jakamisesta markkinavalvontaviranomaisten ja yhdenvertaisuuselinten/kansallisten ihmisoikeustoimijoiden välillä.²⁹⁸ Tietyissä tilanteissa yhdenvertaisuuselinten ja kansallisten ihmisoikeustoimijoiden on kuitenkin tehtävä yhteistyötä myös muiden maansa 77 artiklan mukaisten elinten kanssa, joka edellyttää erillistä oikeusperustaa tietojen jakamista varten.

²⁹⁸ Tekoälyasetus, 73 artiklan 7 kohta ja 79 artiklan 2 kohta.

Yhteistyö markkinavalvontaviranomaisten kanssa

Yhdenvertaisuuselinten ja kansallisten ihmisoikeustoimijoiden tulee niiden nimeämisen jälkeen luoda läheinen yhteistyösuhde markkinavalvontaviranomaisiin. Hallintorakenne voi vaihdella jäsenvaltioittain. On mahdollista, että jotkin maat valitsevat markkinavalvontaviranomaiseksi yhden valvontaviranomaisen, kun taas toiset valitsevat useita valvontaviranomaisia. Sekä Alankomaissa että Irlannissa suositaan useista valvontaviranomaisista koostuvaa kärrynpyörämallia, jossa johtava valvontaviranomainen tukee muita valvontaviranomaisia. Ranskassa puolestaan on otettu käyttöön koordinoitu hallintojärjestelmä: kilpailupolitiikan, kuluttaja-asoiden ja petostentorjunnan pääosasto (*Direction générale de la concurrence, de la consommation et de la répression des fraudes*) vastaa toiminnan koordinoinnista ja tekee yhteistyötä yritysasioista vastaavan pääosaston kanssa strategisen koordinoinnin osalta. Yli kymmenen muuta tahoa, kuten kansallinen tietosuojaviranomainen CNIL (*Commission nationale de l'informatique et des libertés*) ja mediasääntelyviranomainen Arcom (katso *Direction générale des Entreprises 2025*), vastaavat tekoälyasetuksen eri säännöksistä. Tällaisessa tilanteessa yhdenvertaisuuselinten on tehtävä yhteistyötä kaikkien markkinavalvontaviranomaisten kanssa ja asetettava etusijalle johtava markkinavalvontaviranomainen.

Muodostaa oikeusperusta tietojen jakamiselle

Yhdenvertaisuuselinten ja kansallisten ihmisoikeustoimijoiden tulee vakuuttaa jäsenvaltioidensa hallinto ja varmistaa, että jäsenvaltio on muodostanut laajan oikeusperustan tietojenvaihdolle 77 artiklan mukaisten elinten välillä sekä markkinavalvontaviranomaisten ja 77 artiklan mukaisten elinten välillä.²⁹⁹ Tällaisten oikeusperustojen olemassaolo on edellytys kahden- ja monenvälisen yhteistyösopimusten solmimiselle tietojen jakamiseksi. Tällaiset sopimukset on laadittava laaja-alaisesti siten, että ne kattavat 77 artiklan mukaisten elinten ja markkinavalvontaviranomaisten mandaatin. Näiden sopimusten on mahdollistettava tarvittaessa tapauskohtaisten kahdenvälisen lisäsopimusten solmiminen.³⁰⁰

Muodostaa yhdenvertaisuuteen keskittyviä työryhmiä

Yhdenvertaisuuselinten ja kansallisten ihmisoikeustoimijoiden on yhdessä markkinavalvontaviranomaisten kanssa perustettava työryhmiä, jotka voivat vaihtaa keskenään asiantuntemustaan tiettyihin aiheisiin liittyen. Aluksi tällaiset työryhmät voivat pyrkiä luomaan yhteistä ymmärrystä organisaatioiden välille. Työryhmä voi esimerkiksi keskittyä käsittelemään tekoälyjärjestelmien aiheuttaman syrjinnän aiheuttamiin haittoihin liittyviä parhaita käytäntöjä. Tästä voi olla apua yhdenvertaisuuselimille, kun ne laativat markkinavalvontaviranomaisille ohjeita syrjintään liittyvien haittojen tunnistamiseksi, jotta yhdenvertaisuuselimille voidaan ilmoittaa niistä.

299. De Autoriteit Persoonsgegevens (2024), *Final recommendation on supervision of AI: sector and centrally coordinated*, 37 kohta, saatavilla osoitteessa www.autoriteitpersoonsgegevens.nl/en/current/final-recommendation-on-supervision-of-ai-sector-and-centrally-coordinated, viitattu 11. marraskuuta 2025.

300. Ibid.

Luoda selkeät automaattiset laukaisevat tekijät, jotka velvoittavat markkinavalvontaviranomaisen tekemään yhteistyötä yhdenvertaisuuselinten ja kansallisten ihmisoikeustoimijoiden kanssa

On tärkeää, että markkinavalvontaviranomaisille tiedotetaan yhdenvertaisuuselinten ja kansallisten ihmisoikeustoimijoiden esimerkiksi syrjimättömyyteen ja yhdenvertaisuuteen liittyvästä asiantuntijuudesta. Markkinavalvontaviranomaisten tulisi automaattisesti ilmoittaa yhdenvertaisuuselimille, kun 73 artiklan 7 kohdan mukaisesta syrjimättömyyden vaarantavasta tapauksesta on ilmoitettu. Jos markkinavalvontaviranomaiset ovat epävarmoja siitä, onko syrjinnän riski olemassa, niiden tulee kuulla välittömästi yhdenvertaisuuselimiä, esimerkiksi tekoälyasetuksen 79 ja 80 artiklaan liittyvissä tapauksissa, jotta yhdenvertaisuuselin voi tarjota asiantuntemustaan. Väärien ilmoitusten tekeminen on parempi vaihtoehto kuin jättää huomiotta rikkomukset, jotka markkinavalvontaviranomaiset ovat jättäneet huomiotta asiantuntemuksen puutteen vuoksi.

Muiden EU-maiden vaatimustenvastaisuuksista ilmoittaminen

Jos markkinavalvontaviranomaiset havaitsevat vaatimustenvastaisuuksia, jotka eivät rajoitu niiden kansalliselle alueelle, niiden on "ilman aiheutonta viivytystä ilmoitettava komissiolle ja muille jäsenvaltioille arvioinnin tuloksista ja toimenpiteistä, jotka se ovat vaatinut toimijaa toteuttamaan"³⁰¹ ja ilmoitettava yksityiskohtaisesti, jos toimija ei noudata vaadittuja toimia.³⁰² Yhdenvertaisuuselinten ja kansallisten ihmisoikeustoimijoiden tulee korostaa markkinavalvontaviranomaisille ja EU:n tekoälylautakunnalle, että muiden jäsenvaltioiden yhdenvertaisuuselimille ja kansallisille ihmisoikeustoimijoille on tiedotettava ja ilmoitettava, kun vaatimustenvastaisuuden arviointiin liittyy perusoikeuksia, kuten syrjimättömyyttä, koskevia riskejä.

Oikeus tutustua asiakirjoihin

Yhdenvertaisuuselimet ja kansalliset ihmisoikeustoimijat voivat pyytää asiakirjoja suuririskisten tekoälyjärjestelmien toimittajilta.³⁰³ Yhdenvertaisuuselimet voivat saada asiakirjat myös markkinavalvontaviranomaisilta, jos markkinavalvontaviranomainen on jo saanut ne palveluntarjoajalta. Tämä voisi nopeuttaa asiakirjoihin tutustumista yhdenvertaisuuselinten ja kansallisten ihmisoikeustoimijoiden osalta. Kummassakin tapauksessa on tärkeää korostaa, että yritykset eivät voi estää markkinavalvontaviranomaisia jakamasta asiakirjoja yhdenvertaisuuselimien ja kansallisten ihmisoikeustoimijoiden kanssa liikesalaisuuden suojaan vedoten. Tuore tuomio osoittaa, että yritys ei voi päättää, voidaanko asiakirjoja jakaa vai ei, erityisesti silloin, kun yhdenvertaisuuselimet ja kansalliset ihmisoikeustoimijat pyytävät asiakirjoja markkinavalvontaviranomaisilta.³⁰⁴ Tällaisen päätöksen tekeminen kuuluu valvontaviranomaiselle tai tuomioistuimelle.

301. Tekoälyasetus, 79 artiklan 3 kohta.

302. Tekoälyasetus, 79 artiklan 5–6 kohta.

303. Tekoälyasetus, 77 artiklan 1 kohta.

304. Yhteisöjen tuomioistuimen tuomio (ensimmäinen jaosto) 27 päivänä helmikuuta 2025. *CK v. Dun & Bradstreet Austria GmbH ja Magistrat der Stadt Wien*, C-203/22, ECLI:EU:C:2025:117, s. 76.

Osallistuminen testaukseen

Kun yhdenvertaisuuselimet ja kansalliset ihmisoikeustoimijat katsovat, että palveluntarjoajien toimittamat asiakirjat eivät riitä varmistamaan, onko perusoikeuksia suojaavaa unionin lainsäädäntöä rikottu, ne voivat pyytää markkinavalvontaviranomaista ”järjestä[mään] suuririskisen tekoälyjärjestelmän testau[ksen] teknisin keinoin ... kohtuullisen ajan kuluessa”.³⁰⁵ Tekoälyasetuksessa todetaan, että markkinavalvontaviranomaisten on vastattava testien järjestämisestä. Tämä jättää varaa sille, että testit voi suorittaa kolmas osapuoli tai asiantuntija. Testaus on suoritettava yhdenvertaisuuselimien ja/tai kansallisten ihmisoikeustoimijoiden ”tiivillä myötävaikutuksella”.³⁰⁶

On tärkeää, että yhdenvertaisuuselimet ja kansalliset ihmisoikeustoimijat määrittävät seuraavat:

- ▶ Kuka suorittaa testin?
- ▶ Mitä testataan?
- ▶ ”Kohtuullisen ajan” tarkka määritelmä. Tämä on määritettävä mahdollisimman varhaisessa vaiheessa eikä vasta tapauksen syntyessä.
- ▶ Täsmällinen keskinäinen yhteisymmärrys yhdenvertaisuuselimien/kansallisten ihmisoikeustoimijoiden ja markkinavalvontaviranomaisten ”tiivistä myötävaikutuksesta”. Onko tapauksessa yhteyshenkilö, joka osallistuu suoraan testaukseen? Kuullaanko yhdenvertaisuuselimiä/kansallisia ihmisoikeustoimijoita testien vaiheista *a priori*?
- ▶ Kehitetäänkö toimijoiden välistä yhteistyötä varten suunnitelma?

Esimerkkejä ja hyviä käytäntöjä

Inspiraatiota voidaan ottaa yhdenvertaisuuselinten, kansallisten ihmisoikeustoimijoiden ja tietosuojaviranomaisten aiemmin tekemästä yhteistyöstä. Yhdistyneessä kuningaskunnassa yhdenvertaisuus- ja ihmisoikeuskomissio Equality and Human Rights Commission työskenteli paikallisen tietosuojaviranomaisen kanssa osana Fairness and Innovation Challenge -kilpailua korkeakoulutuksen, rahoituksen, terveydenhuollon ja rekrytoinnin testitapauksissa löytääkseen uusia tapoja puuttua tekoälyjärjestelmien tilastollisiin, inhimillisiin ja rakenteellisiin vinoumiin ja syrjintään. Kilpailun rahoitti Yhdistyneen kuningaskunnan tiedeministeriö.³⁰⁷ Norjassa yhdenvertaisuuselin on tehnyt yhteistyötä tietosuojaviranomaisen kanssa osana tekoälyn sääntelyn testiympäristöä.³⁰⁸

305. Tekoälyasetus, 77 artiklan 3 kohta.

306. Ibid.

307. Gov.uk (2024), lehdistötiedote: ”AI Fairness Innovation Challenge winners announced”, saatavilla osoitteessa www.gov.uk/government/news/ai-fairness-innovation-challenge-winners-announced, viitattu 11. marraskuuta 2025.

308. Ks. www.datatilsynet.no/en/regulations-and-tools/sandbox-for-artificial-intelligence/, viitattu 11. marraskuuta 2025.

Ranskassa Defender of Rights -yhdenvertaisuuselimen ja CNIL-tietosuojaviranomaisen välistä yhteistyötä helpottavat useat mekanismit: osapuolet ovat laatineet yhteysymmärryssopimuksena tehdyn pöytäkirjan ja Defender of Rights on myös CNIL:n hallituksen jäsen. Tämän rakenteellisen yhteyden ansiosta Defender of Rightsille ilmoitetaan kaikista CNIL:n vastaanottamista tapauksista.³⁰⁹

Yhteistyö muiden julkisten virastojen kanssa

Yhteistyötä on harkittava myös keinona yhdistää tiettyjä resursseja. Esimerkiksi Ranskassa on perustettu *PEReN* (Le Pôle d'expertise de la régulation numérique) -niminen datatieteen työryhmä, joka koostuu noin 20 datatieteilijästä ja jota johtaa elinkeinoministeriö. Työryhmä on kuitenkin kaikkien keskusvirastojen ja valvontaviranomaisten käytettävissä. Näin siis Ranskan Defender of Rights -yhdenvertaisuuselimellä on käytettävissään uusinta teknistä tietoa ja taitoa. On tärkeää, että tällaisessa yhteistyössä käytetään selkeitä yhteistyömekanismeja, joilla varmistetaan, että yhdenvertaisuuselinten tarpeet täytetään ja niiden riippumattomuus turvataan.

Yhteistyö kansalaisjärjestöjen ja muiden ulkoisten sidosryhmien kanssa

Perustaa kuhunkin jäsenvaltioon neuvoa-antava foorumi, joka koostuu kansalaisjärjestöjen jäsenistä, ruohonjuuritason järjestöistä sekä akateemikoista, jotka yhdessä yhdistävät kentältä saadun kokemuksensa ja asiantuntemuksensa yhdenvertaisuus- ja syrjimättömyyslainsäädännöstä sekä digitaalisista oikeuksista. Tämä neuvoa-antava foorumi voi tuoda esiin tekoälyn haitallisia käyttötapoja, joita jäsenvaltioiden yhdenvertaisuuselimet voivat tutkia ensisijaisesti. Foorumin tulee kokoontua säännöllisesti ja vaihtaa näkemyksiä yhdenvertaisuuselinten kanssa.

Jatkaa ja syventää nykyistä yhteistyötä kansalaisjärjestöjen kanssa

Equinet ja joidenkin jäsenvaltioiden yhdenvertaisuuselimet (esimerkiksi belgialainen Unia) ovat olleet säännöllisesti yhteydessä kansalaisjärjestöihin kutsumalla niitä tapahtumiin ja keskusteluihin. Tällaiset tapaamiset tarjoavat mahdollisuuden vaihtaa tietoja, jotka voivat hyödyttää molempia osapuolia. Näitä yhteyksiä voidaan syventää tekoälyn liittyvien näkökohtien osalta muodostamalla yhteyksiä muiden jäsenvaltioiden kansalaisjärjestöihin ja yhdenvertaisuuselimiin. Tämä edellyttäisi kuitenkin todennäköisesti lisähenkilöstöresursseja. Yksi keino tähän olisi laajentaa muissa sääntely-ympäristöissä jo olemassa olevia virallisia yhteistyörakenteita.

309. Tiedot perustuvat Defender of Rights -yhdenvertaisuuselimen haastatteluun.

Parantaa valitusten käsittelyä

Luoda selkeä ja suoraviivainen valitusten käsittelyprosessi tekoälyjärjestelmistä aiheutuvia syrjinnän haittoja varten.³¹⁰ Kertoo yhdenvertaisuuselinten/kansallisten ihmisoikeustoimijoiden prosessista, jolla ne vastaanottavat kanteluja toimivaltansa mukaisesti, ja kantelijan oikeuksista koko prosessin ajan. Kasvattaa kansalaisyhteiskunnan tietoisuutta prosessista ja jakaa esimerkkejä tapaustutkimuksista, jotka selventävät, millaisia valituksia yhdenvertaisuuselimet ja kansalliset ihmisoikeustoimijat voivat käsitellä toimivaltuuksiensa puitteissa. Voi olla hyödyllistä tuoda esiin myös tapauksia, jotka kuuluvat valvontaviranomaisten toimivaltaan tekoälyasetuksen ja/tai GDPR:n nojalla, sekä näiden lakien mukaisista kantelijoiden oikeuksista. Kannustaa kansalaisjärjestöjä jakamaan tätä tietoa ihmisille, jotka ovat kokeneet haittaa tekoälyjärjestelmien vuoksi, ja täten rohkaisemaan heitä tekemään valituksen.

Ulkopuoliset asiantuntijat voivat myös tarjota teknistä asiantuntemustaan

AI Equality by Design -hankkeessa professorit antoivat akateemista neuvontaa tekoälyä ja syrjintää koskevissa tapauksissa³¹¹. Rahoitusta saattaa olla tarpeen hakea hallitukselta, akateemisten tutkimusaloitteiden kautta, oikeudenkäyntejä rahoittavilta tahoilta tai muualta asiantuntijatodisteiden tai -neuvojen hankkimiseksi.

310. Ks. myös Equinet (2023), Minimal guidelines on improving complaints data collection by equality bodies, saatavilla osoitteessa <https://equineteurope.org/wp-content/uploads/2024/01/Minimal-Guidelines-on-Improving-Complaints-Data-Collection-by-Equality-Bodies-1.pdf>, viitattu 11. marraskuuta 2025.

311. Equinet (2025), Embedding equality safeguards into technical standards for the EU AIA and empowering equality defenders: Equinet's participation in the project "Equality by Design, Deliberation and Oversight", saatavilla osoitteessa <https://equineteurope.org/latest-developments-in-ai-equality/>, viitattu 11. marraskuuta 2025.

OSA II



6. Direktiivit yhdenvertaisuuselimiiä koskevista normeista

6.1. Yleinen tausta

Toukokuun 7. päivänä 2024 annettiin kaksi uutta direktiiviä, joiden tarkoituksena on taata yhdenvertaisuuselinten tehokkuus ja riippumattomuus ja siten vahvistaa ”yhdenvertaisen kohtelun periaatteen soveltamista”.³¹² Ne ovat jatkoa Equinetin,³¹³ Euroopan rasismien ja suvaitsemattomuuden vastaisen komission (ECRI)³¹⁴ ja Euroopan komission standardointityölle.³¹⁵

Niissä vahvistetaan yhdenmukaiset vähimmäisvaatimukset:

312. Direktiivit yhdenvertaisuuselimiiä koskevista normeista, 1 artikla.

313. Equinet (2016), *Developing Standards for Equality Bodies: An Equinet Working Paper*.

314. Euroopan rasismien ja suvaitsemattomuuden vastaisen komission ECRI:n yleissuositus n:o 2 (tarkastettu): *Equality Bodies to Combat Racism and Intolerance at National Level*, joulukuu 2017.

315. Komission suositus (EU) 2018/951, annettu 22 päivänä kesäkuuta 2018, tasa-arvoelimiä koskevista normeista.

- direktiivi 2024/1500 koskee naisten ja miesten yhdenvertaista kohtelua ja yhtäläisiä mahdollisuuksia työssä ja ammatissa
- direktiivi 2024/1499 koskee henkilöiden rodusta tai etnisestä alkuperästä riippumatonta yhdenvertaista kohtelua, uskonnosta tai vakaumuksesta, vammaisuudesta, iästä tai seksuaalisesta suuntautumisesta riippumatonta yhdenvertaista kohtelua työssä ja ammatissa sekä naisten ja miesten yhdenvertaista kohtelua sosiaaliturvaa koskevissa asioissa ja tavaroiden ja palvelujen saatavuudessa ja tarjonnassa.

Direktiivit yhdenvertaisuuselimiiä koskevista normeista³¹⁶ voivat auttaa yhdenvertaisuuselimiiä ehkäisemään ja paljastamaan tekoälyjärjestelmiin liittyvää syrjintää, ja niiden johdanto-osissa mainitaan nimenomaisesti tekoäly ja automatisoidut järjestelmät:

On tärkeää kiinnittää huomiota automatisoitujen järjestelmien, kuten tekoälyn, käytön tarjoamiin mahdollisuuksiin ja riskeihin. Yhdenvertaisuuselimillä olisi erityisesti oltava käytettävissään sopivat henkilöstö- ja tekniset resurssit. Kyseisten resurssien olisi etenkin mahdollistettava se, että yhdenvertaisuuselimet sekä käyttävät automatisoituja järjestelmiä työssään että arvioivat kyseisten järjestelmien syrjimättömyysääntöjen mukaisuutta. Jos yhdenvertaisuuselin on osa elintä, jolla on useita tehtäviä, sen tasa-arvottehtävän hoitamiseen tarvittavat resurssit olisi varmistettava.³¹⁷

Direktiivit yhdenvertaisuuselimiiä koskevista normeista on saatettava osaksi kansallista lainsäädäntöä kesäkuuhun 2026 mennessä.

6.2. Toimivaltuuksien ja resursoinnin muutokset

6.2.1. Toimivallan laajuuden laajentaminen

Yhdenvertaisuuselimien normeja koskevilla direktiiveillä laajennetaan yhdenvertaisuuselinten toimivaltuuksia. Erityisesti niiden valtioiden, jotka eivät vielä ole näin tehneet, olisi laajennettava yhdenvertaisuuselinten toimivaltaa sukupuolten välisen tasa-arvon periaatteen toteutumiseen sosiaaliturvaa koskevissa kysymyksissä liittyvän direktiivin (79/7/ETY) ja työllisyyttä koskevan puitedirektiivin (2000/78/EY) kattamiin perusteisiin ja elämäntilanteisiin ja annettava niille enemmän toimivaltaa uskonnon tai vakaumuksen, iän, vammaisuuden ja seksuaalisen suuntautumisen perusteiden kattamiseksi työllisyyden alalla sekä biologisen ja sosiaalisen sukupuolen perusteiden kattamiseksi sosiaaliturvan alalla.³¹⁸ Tämä on tärkeää, koska sosiaaliturvan parissa käytettyjen automaattisen päätöksenteon (ADM) järjestelmien

316. Equinet (2024) ja Euroopan neuvoston kehittämä kaikille avoin verkkokurssi tarjoavat kattavan yleiskatsauksen asetuksesta.

317. Direktiivi 2024/1500, johdanto-osan 21 kohta ja direktiivi 2024/1499, johdanto-osan 22 kohta.

318. Direktiivi 2024/1499, 1 artiklan 2 kohta. Käytännössä monien yhdenvertaisuuselinten toiminta-alue ulottuu jo EU:n syrjintälainsäädännön vähimmäisvaatimuksia laajemmalle. Ks. Equinet 2024: 24.

on usein todettu olevan vinoutuneita naisia kohtaan, kuten Itävallassa, Ranskassa ja Ruotsissa on havaittu.³¹⁹

On tärkeää huomata, että direktiivien soveltamisala rajoittuu edelleen EU:n syrjimättömyyslainsäädännön kattamiin perusteisiin ja elämänalueisiin.³²⁰ Yhdenvertaisuuselimien normeja koskevat direktiivit asettavat kuitenkin vähimmäisvaatimukset, ja kansallisella tasolla yhdenvertaisuuselinten toimivalta saattaa olla laajempi.

Lisäksi kyseisissä direktiiveissä viitataan nimenomaisesti intersektionaaliseen syrjintään mitä tulee yhdenvertaisuuselinten edistäviin ja ehkäiseviin toimiin. Direktiiveissä säädetään, että tässä yhteydessä yhdenvertaisuuselimet "voivat ottaa huomioon epäedulliset erityistilanteet, jotka perustuvat intersektionaaliseen syrjintään".³²¹ Direktiivien johdanto-osissa sanotaan myös, että "[o]n tärkeää, että tasa-arvoelimet yhdenvertaisen kohtelun edistämiseksi, syrjinnän ehkäisemiseksi, syrjintää koskevien tietojen keräämisessä ja tämän direktiivin mukaisessa uhrien auttamisessa kiinnittävät erityistä huomiota intersektionaaliseen syrjintään".³²²

Koska tekoälyjärjestelmät ja erityisesti ennustava analytiikka todennäköisesti synnyttävät intersektionaalisen syrjinnän eri muotoja, on erityisen tärkeää, että yhdenvertaisuuselimet hyödyntävät näitä uusia valtuuksiaan aloittaen työnsä edistävistä ja ehkäisevistä toimista (Xenidis 2020).

6.2.2. Velvollisuus tarjota riittäviä resursseja

Direktiivin 4 artiklan mukaan valtioiden on "varmistettava, että kullakin tasa-arvoelimellä on käytettävissään tarvittavat henkilöstö-, tekniset ja taloudelliset resurssit, jotta se voi hoitaa kaikki tehtävänsä ja käyttää kaikkia toimivaltuuksiaan tuloksellisesti". Edellä mainituissa johdanto-osissa resurssikysymys yhdistetään nimenomaisesti tekoäly- ja ADM-järjestelmien ongelmiin,³²³ joiden käsittely saattaa edellyttää uusia ja ylimääräisiä teknisiä ja henkilöstöresursseja.

Mitä tämä tarkoittaa käytännössä?

Henkilöstöresurssit

Yhdenvertaisuuselimillä on oltava "pätevä[ä] henkilöstö[ä] ..., jotta ne voivat suorittaa kaikki tehtävänsä tehokkaasti",³²⁴ "palkata riittävästi ihmisiä, joilla on erilaisia ja toisiaan täydentäviä taitoja, jotta ne voivat suorittaa kaikki tehtävänsä tehokkaasti

319. Allhutter D. et al. (2020), "Algorithmic profiling of job seekers in Austria: How austerity politics are made effective", *Frontiers in Big Data*, 3, saatavilla osoitteessa <https://doi.org/10.3389/fdata.2020.00005>, viitattu 11. marraskuuta 2025; Romain et al. (2023); Amnesty International (2024), "Sweden: Authorities must discontinue discriminatory AI systems used by welfare agency", saatavilla osoitteessa www.amnesty.org/en/latest/news/2024/11/sweden-authorities-must-discontinue-discriminatory-ai-systems-used-by-welfare-agency/, viitattu 11. marraskuuta 2025.

320. Direktiivit 2024/1499 ja 2024/1500, johdanto-osan 15 kohta.

321. Direktiivit 2024/1499 ja 2024/1500, 5 artiklan 2 kohta.

322. Direktiivi 2024/1499, johdanto-osan 16 kohta; direktiivi 2024/1500 johdanto-osan 15 kohta, ks. myös direktiivi (EU) 2023/970 (samapalkkaisuus), johdanto-osan 15 kohta.

323. Direktiivi 2024/1499, johdanto-osan 22 kohta ja direktiivi 2024/1500, johdanto-osan 21 kohta.

324. Direktiivi 2024/1499, johdanto-osan 21 kohta ja direktiivi 2024/1500, johdanto-osan 20 kohta.

ja tuloksellisesti” ja ”tarjota kilpailukykyistä palkkaa ja työolot”.³²⁵ Tekoälyn ja ADM-järjestelmien ongelmien käsittelyn yhteydessä tämä edellyttää seuraavia toimia:

- ▶ Teknologia-asiantuntijoita, mukaan lukien datatutkijoita, tulee palkata ja heille tulee tarjota kilpailukykyistä palkkaa yhdenvertaisuuselinten sisäisen teknisen asiantuntijuuden rakentamiseksi. Vaihtoehtoisesti voidaan varmistaa (palkkaamalla tai täydennyskouluttamalla), että yhdenvertaisuuselimillä on sisäiset valmiudet valita ulkopuolisia teknisiä asiantuntijoita, esimerkiksi markkinaevalvontaviranomaisten tai muiden 77 artiklan mukaisten elimien tutkijoita tai asiantuntijoita, ja tehdä yhteistyötä heidän kanssaan.
- ▶ On varmistettava (palkkaamalla tai täydennyskouluttamalla), että riittävä määrä yhdenvertaisuuselinten oikeudellisia ja poliittisia asiantuntijoita tuntee ADM-/tekoälyjärjestelmien toiminnan (vähintään niiden tekniset perustoiminnot) sekä tekoäly- ja ADM-järjestelmiin liittyvän lainsäädännön, erityisesti tekoälyasetuksen.
- ▶ Valitusten käsittelystä vastaavaa henkilöstöä tulee kouluttaa sen suhteen, miten ADM-/tekoälyjärjestelmän mahdollinen käyttö voidaan havaita yhdenvertaisuuselimille tehtävissä valituksissa, ja valituksien tutkimiseen ja mahdollisten jatkokysymysten esittämiseen tulee palkata riittävästi henkilöstöä.

Alankomaalainen ihmisoikeusinstituutti Netherlands Institute for Human Rights suoritti menestyksekkäästi oma-aloitteisen tutkimuksen liittyen mahdolliseen rakenteelliseen syrjintään, joka koski lastenhoitoetusjärjestelmän toimintaa, ja se aikoo ottaa käyttöön puitteet teknologiaan perustuvien tietotapausten käsittelyä varten. Kun otetaan huomioon tällaiseen tapaukseen tarvittavien resurssien määrä, instituutti katsoo, että ihanteellisessa tapauksessa tämä käsittely tulisi hoitaa kouluttamalla instituution sisäisiä lakimiehiä ja palkkaamalla datatieteilijöitä (Ilieva 2024: 73).

Monet koulutukseen ja täydennyskoulutukseen liittyvistä suosituksista ovat Euroopan neuvoston puiteyleissopimuksen 20 artiklan mukaisia. Kyseinen artikla koskee ”kaikkien väestöryhmien riittävää digitaalista lukutaitoa ja digitaitoja, myös erityisiä ammatillisia taitoja niille, jotka vastaavat tekoälyjärjestelmien aiheuttamien riskien tunnistamisesta, arvioinnista, ehkäisemisestä ja lieventämisestä”.

Tekniset resurssit

Teknisiä resursseja voidaan pitää resursoinnin ”kolmantena osa-alueena” yhdenvertaisuuselinten henkilöstön ja rahoituksen lisäksi (Equinet 2024). Tämä kattaa toimitilat, infrastruktuurin ja riittävät resurssit tietotekniikkatarpeiden täyttämiseksi, mukaan lukien tiedonkeruujärjestelmät ja verkkokonsultointivälineet.³²⁶ Tekoäly- ja ADM-järjestelmien osalta seuraavat toimenpiteet saattavat olla tarpeen:

- ▶ Varmistaa, että valituksia käsittelevä tietotekniikkajärjestelmä antaa henkilöstölle mahdollisuuden helposti merkitä ja havaita valitukset, joiden suhteen epäillään, että tekoäly- ja ADM-järjestelmiä on saatettu käyttää. Eri valitusten välillä pitäisi olla havaittavissa kuvioita, jotka saattavat viitata tekoäly- ja ADM-järjestelmien

325. Equinet (2023), Measuring Standards for Equality Bodies: Indicators for Self-Assessment, Resources-kappale, kohdat 2.2.1.1 ja 2.2.1.2.

326. Equinet (2023), Measuring Standards for Equality Bodies: Indicators for Self-Assessment.

käyttöön. Tämä auttaisi ratkaisemaan yhden tekoäly- ja ADM-järjestelmistä johtuvan syrjinnän tunnistamisen käytännön esteen, jonka Unia on todennut: "valitusten käsittelyyn liittyvä työmäärä tarkoittaa, että tekniseen järjestelmään jätettyjen valitusten perusteella ei ole aina helppo havaita, että samaa organisaatiota koskevia valituksia on tullut useita. Teknisessä järjestelmässä on parannettavaa myös siinä, että vaikka järjestelmässä on kenttä, johon voidaan kirjata, onko tapaukseen liittynyt tekoäly- tai ADM-järjestelmä, tämä kenttä on piilotettu syvälle lomakkeisiin, jotka käyttäjien on täytettävä valituksen tekemistä varten, joten ne jäävät helposti huomaamatta." (Xenidis 2025)

- ▶ Asianmukaisesti suojattu IT-infrastruktuuri, jotta data-analyyssejä voidaan tehdä tekoäly- ja ADM-järjestelmien tutkimisen yhteydessä. Kun otetaan huomioon valitusten arkaluonteisuus ja ihmisten henkilötiedot, yhdysvaltalaisen teknologiayritysten tarjoamien pilvipalvelujen käyttöä ei voida pitää turvallisena IT-infrastruktuurina.³²⁷

Tarvittavien resurssien määrän osalta Equinet korostaa, että "yhdenvertaisuuselimet voivat itse parhaiten määritellä, mitä resursseja tarvitaan 'kunkin tehtävän tehokkaaseen hoitamiseen kohtuullisessa ajassa', perustuen niiden arvioon ratkaistavista ongelmista sekä toteuttavista toimista ja toimenpiteistä" (Equinet, 2024). Välineitä koskevia keskusteluja voidaan käydä myös kollektiivisella tasolla esimerkiksi Equinetin kautta, koska sillä on foorumi tällaisille keskusteluille monivuotisen standardihankkeen kautta. Hankkeeseen sisältyy vuosittaisia tapaamisia, joissa asianomaiset jäsenet keskustelevat kaikista yhdenvertaisuuselinten resursseihin, riippumattomuuteen ja valtuuksiin liittyvistä näkökohdista.

Direktiiveissä, jotka käsittävät yhdenvertaisuuselimiä koskevia normeja, todetaan, että yhdenvertaisuuselimet voivat käyttää tekoäly- ja ADM-työkaluja toimeksiantonsa hoitamiseen. Vaikka yhdenvertaisuuselimet voivat näin tehostaa toimintaansa (esimerkiksi havaitsemalla eri valitusten välisiä kuvioita), nämä välineet on hankittava, arvioitava ja otettava käyttöön huolella ja niiden käyttöohjeita noudattaen.

327. Katso Yhdysvaltojen Cloud Act- ja Foreign Surveillance Intelligence Act -lait. Tutustu myös viimeaikaiseen raportointiin, jonka mukaan Microsoft on saattanut sulkea kansainvälisen rikostuomioistuimen pääsyyttäjän sähköpostitilin reaktiona Yhdysvaltojen presidentin Trumpin asetukseen. Molly Quell (2025), *Trump's sanctions on ICC prosecutor have halted tribunal's work*, saatavilla osoitteessa <https://apnews.com/article/icc-trump-sanctions-karim-khan-court-a4b4c02751ab84c09718b1b95cbd5db3>, viitattu 11. marraskuuta 2025.

6.2.3. Yhdenvertaisuuselinten rooli niiden toimeksiannon ja resursoinnin osalta ADM- ja tekoälyjärjestelmien kontekstissa

Elinten toimeksiannon ja erityisesti intersektionaalisen syrjinnän käsitteen osalta

- ▶ Hyödyntää viittauksia intersektionaalisuuteen, jotta tutkimuksissa ja viestinnässä voidaan puuttua ADM- ja tekoälyjärjestelmiin mahdollisesti sisältyvään, usein intersektionaaliseen syrjintään.
- ▶ Edistää yhdenvertaisuuselinten toimeksiannon laajentamista kattamaan muutkin kuin EU:n syrjinnän vastaisen lainsäädännön mukaiset perusteet.
- ▶ Edistää intersektionaalisuuden laajempaa soveltamista, sillä tällä hetkellä direktiiveissä ”intersektionaalinen työ” rajataan ehkäisy- ja edistämistoimiin.

Resursoinnin osalta

- ▶ Arvioida tekoäly-/ADM-järjestelmien käsittelyyn tarvittavia teknisiä ja henkilöstöresursseja.
- ▶ Edistää tekniseen ja henkilöstöön liittyvää lisäresurssointia myös osana yhdenvertaisuuselinten normeja koskevien direktiivien kansallisen lainsäädännön saattamisen kontekstissa.
- ▶ Tunnistaa, millaiset tekniset välineet ovat hyödyllisiä, ja tehdä kansainvälistä yhteistyötä niiden hankkimiseksi tai kehittämiseksi. Esimerkiksi valituksia käsittelevien ohjelmistojen kontekstissa on priorisoitava avoimen lähdekoodin ohjelmistoja, joita eri yhdenvertaisuuselimet voivat käyttää ja joita voidaan tarvittaessa muokata tiettyjen tarpeiden mukaan. Toinen esimerkki voisi olla sellaisten tutkimusvälineiden kehittäminen, joita useat yhdenvertaisuuselimet voivat käyttää, sen sijaan, että kukin kehittäisi saman välineen alusta asti.³²⁸

6.3. Valtuuksien muutokset

Yhdenvertaisuuselinten normeja koskevissa direktiiveissä asetetaan yhdenmukaiset vähimmäisstandardit sille, millaisia valtuuksia yhdenvertaisuuselimillä on, ja annetaan niille uusia välineitä algoritmisen syrjinnän torjumiseksi kahdella rintamalla:

- ▶ syrjinnän ehkäisyä ja yhdenvertaisen kohtelun edistämistä koskevat valtuudet
- ▶ tutkintaa ja korvausten hakemista koskevat valtuudet.

Osiassa 6.3 tarkastellaan, mitä direktiivien säännökset tarkoittavat tekoäly- ja ADM-järjestelmien kontekstissa.

Yhdenvertaisuuselinten normeja koskevien direktiivien säädetyt valtuudet liittyvät Euroopan neuvoston puiteyleissopimuksessa asetettuihin velvoitteisiin ottaa käyttöön

328. Samankaltaisia aloitteita voidaan havaita esimerkiksi tietosuojan alalla. Katso EDPB:n verkkosivustojen tarkastustyökalu, saatavilla osoitteessa www.edpb.europa.eu/our-work-tools/our-documents/support-pool-experts-projects/edpb-website-auditing-tool_en, viitattu 11. marraskuuta 2025.

tai pitää voimassa oikeussuojakeinoja,³²⁹ suojatoimia³³⁰ ja valvontamekanismeja.³³¹ Näihin velvollisuuksiin sisältyvät ”nykyisten kehitysvalmiuksien jatkuva seuranta ja auditointi, julkiset kuulemiset ja sitouttaminen, riskien ja vaikutusten hallintakehykset ja ihmisoikeusvaikutusten arviointikehykset, tekniset standardit, koulutus ja tietoisuuden lisäämisohjelmat”.³³²

6.3.1. Yhdenvertaisen kohtelun edistäminen ja syrjinnän ehkäiseminen

Yhdenvertaisuuselimien normeja koskevien direktiivien mainittu yhdenvertaisuuselinten toimivalta ”edistää tasa-arvoista kohtelua” edellyttää, että ”jäsenvaltiot mahdollistavat yhdenvertaisuuselinten siirtymisen reaktiivisesta, korjaavasta lähestymistavasta ennakoivaan, ennaltaehkäisevään ja edistävään lähestymistapaan” (Equinet, 2024). Tämä muutos on kriittinen automaattisen päätöksenteon ja tekoälyjärjestelmien yhteydessä, sillä tietoisuuden ja tiedon puute ovat kaksi haastetta, jotka liittyvät syrjinnän ehkäisemiseen ja sovitteluun.

Tietoisuuden lisääminen

Yhdenvertaisuuselimien normeja koskevien direktiivien 5 artiklan 1 kohdassa säädetään yhdenvertaisuuselinten uudesta yleisestä valtuudesta lisätä tietoisuutta. Tekoäly- ja ADM-järjestelmien kontekstissa tämä tarkoittaa tietoisuuden lisäämistä tekoäly- ja ADM-järjestelmien aiheuttamista syrjintäriskeistä, olemassa olevista syrjimättömyysoikeuksista sekä mahdollisista muutoksenhaku- ja oikeussuojakeinoista, kuten yhdenvertaisuuselinten olemassaolosta. Tietoisuuden lisäämistöimien tulisi olla helposti saatavilla,³³³ ja erityistä huomiota on kiinnitettävä haavoittuvassa asemassa oleviin henkilöihin, joihin tekoäly- ja ADM-järjestelmien vaikutukset usein kohdistuvat. Tämä tietoisuuden lisääminen liittyy markkinavalvontaviranomaisten vaatimuksiin kiinnittää erityistä huomiota tekoälyjärjestelmiin, jotka aiheuttavat riskin haavoittuvassa asemassa oleville ryhmille, ja ilmoittaa yhdenvertaisuuselimille, jos perusoikeuksiin kohdistuva riski havaitaan.³³⁴

329. Euroopan neuvoston puiteyleissopimus, 14 artikla.

330. Euroopan neuvoston puiteyleissopimus, 15 artikla.

331. Euroopan neuvoston puiteyleissopimus, 9 artikla.

332. Euroopan neuvosto (2024), tekoälyä ja ihmisoikeuksia, demokratiaa ja oikeusvaltioperiaatetta koskeva puiteyleissopimus, selitysmuistio, kohta 63.

333. Direktiivit yhdenvertaisuuselimistä koskevista normeista, 12 artikla.

334. Tekoälyasetus, 79 artiklan 2 kohta.

Ennakoiva ehkäisy

Yhdenvertaisuuselimien normeja koskevien direktiivien 5 artiklan 2 kohta tuo toisen muutoksen yhdenvertaisuusdirektiiveihin³³⁵ nähden, sillä siinä annetaan yhdenvertaisuuselimille valtuudet toimia ennakoivasti syrjinnän ehkäisemisessä. Tällaisiin toimiin kuuluvat muun muassa ”positiivisten toimien ja sukupuolten tasa-arvon valtavirtaistamisen edistäminen julkisten ja yksityisten yhteisöjen keskuudessa, asianmukaisen koulutuksen, neuvonnan ja tuen tarjoaminen niille, julkiseen keskusteluun osallistuminen, yhteydenpito asiaankuuluvien sidosryhmien, myös työmarkkinaosapuolten, kanssa ja hyvien käytäntöjen vaihdon edistäminen.”³³⁶

Yhdessä yhdenvertaisuuselimien normeja koskevien direktiivien 4 artiklan kanssa tulkittuna tämä tarkoittaa, että yhdenvertaisuuselimillä tulee olla riittävät resurssit tällaisten toimien toteuttamiseen.

Kuuleminen

Yhdenvertaisuuselimien normeja koskevien direktiivien 15 artiklassa edellytetään, että jäsenvaltiot kuulevat yhdenvertaisuuselimia lainsäädännöstä, politiikasta, menettelyistä ja ohjelmista, jotka liittyvät yhdenvertaisuusdirektiiveistä johtuviin oikeuksiin ja velvollisuuksiin. Tätä artiklaa voidaan tulkita suppeasti siten, että se rajoittuu yhdenvertaisuuslainsäädäntöön ja -politiikkaan. Johdanto-osan kappaleissa esitetyn kuulemisen tarkoituksena on kuitenkin antaa yhdenvertaisuuselimille mahdollisuus osallistua ”yhdenvertaisuuden valtavirtaistami[seen]”³³⁷ Yhdenvertaisuuselinten on näin ollen osallistuttava digitaalisia palveluita koskevaan lainsäädäntöön ja politiikkaan, mukaan lukien tekoälyasetuksen täytäntöönpanoon tai tekoäly- ja ADM-järjestelmien erityiskäyttöä koskevaan kansalliseen lainsäädäntöön.

Tämä säännös on myös Euroopan neuvoston puiteyleissopimuksen 19 artiklan mukainen. Siinä määrätään, että ”tekoälyjärjestelmiin liittyv[istä] tärke[istä] kysymyks[istä]” on järjestettävä julkisia ja eri sidosryhmien välisiä kuulemisia.

335. Tässä raportissa ”yhdenvertaisuusdirektiiveillä” tarkoitetaan seuraavia EU:n lainsäädännön keskeisiä direktiivejä: Neuvoston direktiivi 2000/43/EY, annettu 29 päivänä kesäkuuta 2000, rodusta tai etnisestä alkuperästä riippumattoman yhdenvertaisen kohtelun periaatteen täytäntöönpanosta (direktiivi 2000/43/EY); neuvoston direktiivi 2000/78/EY, annettu 27 päivänä marraskuuta 2000, yhdenvertaista kohtelua työssä ja ammatissa koskevista yleisistä puitteista (direktiivi 2000/78/EY); Euroopan parlamentin ja neuvoston direktiivi 2006/54/EY, annettu 5 päivänä heinäkuuta 2006, miesten ja naisten yhtäläisten mahdollisuuksien ja yhdenvertaisen kohtelun periaatteen täytäntöönpanosta työhön ja ammattiin liittyvissä asioissa (uudelleenlaadittu toisinto) (direktiivi 2006/54/EY); neuvoston direktiivi 2004/113/EY, annettu 13 päivänä joulukuuta 2004, miesten ja naisten yhdenvertaisen kohtelun periaatteen täytäntöönpanosta tavaroiden ja palvelujen saatavuuden ja tarjonnan alalla (direktiivi 2004/113/EY); Euroopan parlamentin ja neuvoston direktiivi 2010/41/EU, annettu 7 päivänä heinäkuuta 2010, miesten ja naisten tasa-arvoisen kohtelun periaatteen soveltamisesta itsenäisiin ammatinharjoittajiin sekä neuvoston direktiivin 86/613/ETY kumoamisesta (direktiivi 2010/41/EU); Euroopan parlamentin ja neuvoston direktiivi (EU) 2023/970, annettu 10 päivänä toukokuuta 2023, miesten ja naisten samapalkkaisuuden periaatteen soveltamisen lujittamisesta palkkauksen läpinäkyvyyden ja täytäntöönpanomekanismien avulla (direktiivi 2023/970/EU); neuvoston direktiivi 79/7/ETY, annettu 19 päivänä joulukuuta 1978, miesten ja naisten tasa-arvoisen kohtelun periaatteen asteittaisesta toteuttamisesta sosiaaliturvaa koskevissa kysymyksissä (direktiivi 79/7/ETY).

336. Direktiivit yhdenvertaisuuselimia koskevista normeista, 5 artiklan 2 kohta.

337. Samankaltaista säännöksen analyysia varten katso Equinet (2024).

Tiedonkeruu, pääsy yhdenvertaisuustietoihin ja raporttien laatiminen

Yhdenvertaisuuselimien normeja koskevien direktiivien 16 artiklassa annetaan yhdenvertaisuuselimille valtuudet kerätä tietoja (painottaen niiden erittelyä),³³⁸ tehdä selvityksiä,³³⁹ saada pääsy muiden keräämiin tilastoihin³⁴⁰ ja antaa suosituksia kerätävistä yhdenvertaisuustiedoista.³⁴¹ Tämä valtuus on nimenomaisesti sidottu yhdenvertaisuuselinten raportointivelvoitteisiin, joihin kuuluvat raportit ”yhdenvertaisen kohtelun ja syrjinnän tilasta jäsenvaltiossa”.³⁴² Johdanto-osan kappaleissa annetaan myös tarkempia tietoja tiedonkeruun tarkoituksista. Tällaisia ovat esimerkiksi toimet, joilla voidaan ”arvioida syrjintää määrällisesti”, ”arvioida yhdenvertaisuutta koskevan lainsäädännön täytäntöönpanoa” ja ”edistää näyttöön perustuvaa päätöksentekoa”.

Näitä valtuuksia voidaan soveltaa tekoäly-/ADM-järjestelmien alalla erityisesti siksi, että voitaisiin ymmärtää paremmin, missä vaiheessa tekoäly-/ADM-järjestelmien käyttöönotto on virastoissa.

Tietosuojalainsäädäntöä ei tule pitää esteenä yhdenvertaisuustietojen keräämiselle (EU:n perusoikeusvirasto, 2021). Yleisen tietosuoja-asetuksen 9 artiklan 2 kohdan a, g ja j alakohdassa sallitaan henkilötietojen erityisryhmien kerääminen ja käsittely tietyin edellytyksin esimerkiksi tilasto- tai tutkimustarkoituksiin. Euroopan komission syrjimättömyyttä, yhdenvertaisuutta ja moninaisuutta käsittelevän korkean tason ryhmän yhdenvertaisuustietoja käsittelevä alaryhmä on hyväksynyt erilaisia suuntaviivoja ja julkaissut ohjeita yhdenvertaisuustietojen keräämisestä ja käytöstä. Maaliskuussa 2025 alaryhmä julkaisi yhdenvertaisuustietojen keräämistä ja käyttöä koskeva asiakirjan ”Collecting and using equality data in full compliance with EU General Data Protection Regulation and national data protection rules”, jossa tuodaan esille useiden Euroopan unionin jäsenvaltioiden parhaita käytäntöjä sekä perusoikeusviraston ja alaryhmän jäsenten jakamia kokemuksia (yhdenvertaisuustietoja käsittelevä alaryhmä, 2025; katso myös Ilieva, 2024).

6.3.2. Yhdenvertaisuuselinten rooli yhdenvertaisen kohtelun edistämisessä ja syrjinnän ehkäisemisessä

Tietoisuuden lisääminen

- ▶ Lisätä tietoisuutta asianosaisten uusista oikeuksista: osana tietoisuuden lisäämiseen liittyviä valtuuksiaan yhdenvertaisuuselinten on lisättävä tietoisuutta asianosaisten tekoälyjärjestelmiin liittyvistä oikeuksista, kuten oikeudesta tehdä valitus ja oikeudesta saada selvitys, tekoälyasetuksen ja EU:n tietosuoja-lainsäädännön mukaisesti.

338. Direktiivit yhdenvertaisuuselimää koskevista normeista, 16 artiklan 1 kohta.

339. Direktiivit yhdenvertaisuuselimää koskevista normeista, 16 artiklan 2 kohta.

340. Direktiivit yhdenvertaisuuselimää koskevista normeista, 16 artiklan 3 kohta.

341. Direktiivit yhdenvertaisuuselimää koskevista normeista, 16 artiklan 4 kohta.

342. Direktiivit yhdenvertaisuuselimää koskevista normeista, 17 artiklan c kohta.

- ▶ Lisätä tietoisuutta perusoikeuksiin kohdistuvista riskeistä hyödyntämällä olemassa olevaa tekoälyjärjestelmiä koskevaa näyttöä kansallisella ja Euroopan tasolla.
- ▶ Toiminta median ja toimittajien kanssa uusien tutkimusten ja näitä asioita koskevan raportoinnin lisäämiseksi.
- ▶ Yhteistyö olemassa olevien aloitteiden kanssa tietoisuuden lisäämiseksi: yleisölle suunnattu tietoisuuden lisääminen voi tarkoittaa sellaisiin paikkoihin menoa, joissa yleisö jo on. Esimerkiksi meneillään olevassa eurooppalaisessa AlgoLit-hankkeessa,³⁴³ joka käsittelee algoritmista sovittelua, pyritään tekemään yhteistyötä sovittelijoiden ja sosiaalityöntekijöiden kanssa tietoisuuden lisäämiseksi tekoäly- ja ADM-järjestelmiin liittyvistä kysymyksistä julkisella sektorilla. Yhdenvertaisuuselimet voivat harkita yhteistyötä tällaisten hankkeiden kanssa varmistaakseen, että syrjäintäriskejä käsitellään riittävästi tällaisissa ohjelmissa, ja edistääkseen yhdenvertaisuuselinten roolia syrjimättömyysoikeuksien käytössä. Tämä on erityisen tärkeää, koska tekoälyn haasteisiin liittyvässä koulutuksessa käytetään usein pikemminkin ”etiikkaan perustuvaa” lähestymistapaa perusoikeuksiin pohjautuvan sijaan (Xenidis, 2025).
- ▶ Seurata tekoälyjärjestelmien tarjoajien ja käyttöönottajien strategioita, mukaan lukien tekoäly-/ADM-järjestelmien tarjoajien ja käyttöönottajien ”riskien vähentämiseen” liittyviä strategioita (Xenidis, 2025) ja ”etiikkapesua” (Equinet, 2025) (esimerkiksi suuririskisten järjestelmien järjestelyn ulkopuolelle jättäytyminen tai 5 artiklan mukaisten kiellettyjen järjestelmien määritelmien kierto).

Ennakoiva ehkäisy

- ▶ Tarjota koulutusta tekoäly-/ADM-järjestelmien yksityisille ja julkisille käyttöönottajille (mukaan lukien julkishallinnon virastoille) sekä lainsäädäntö- ja tuomiovallan insituutioille. Esimerkiksi Euroopan neuvosto tarjoaa erilaisten kansallisten kontekstien tekoälyä ja syrjinnän torjumista käsittelevän kurssin yhteistyössä yhdenvertaisuuselinten (kuten Suomen yhdenvertaisuusvaltuutetun, Ranskan Défenseur des droits -viraston, Portugalin Comissão para a Cidadania e a Igualdade de Género -komission ja Belgian Unian) kanssa.
- ▶ Edistää osallisuutta ja yhdenvertaisuutta luonnontieteiden, matematiikan, tekniikan ja teknologian aloilla (STEM-tieteet).

Tiedonkeruu, pääsy yhdenvertaisuustietoihin ja raporttien laatiminen

- ▶ Tunnistaa tekoäly-/ADM-järjestelmiin liittyvä syrjintä ja tekoälyasetuksen täytäntöönpano julkisen raportoinnin prioriteeteiksi.
- ▶ Laatia raportteja, jotka perustuvat kansallisiin katsauksiin tekoäly-/ADM-järjestelmien käytöstä tietyllä alalla, keskittyen erityisesti aloihin, joita pidetään tekoälyasetuksen liitteen III mukaisesti suuririskisinä. Näissä asiakirjakatsauksissa voidaan hyödyntää tietoja, jotka ovat saatavilla EU:n tietokannassa, mutta niissä voidaan myös mennä pidemmälle ja analysoida järjestelmiä, joita ei pidetä suuririskisinä tai jotka eivät ole julkisessa tietokannassa (kuten lainvalvonnan tai muuttoliikkeen ja rajavalvonnan hallinnan järjestelmät), jotta voidaan

343. FARI (2025), ”ALGO-LIT (Erasmus+ -hanke)”, saatavilla osoitteessa www.fari.brussels/research-and-innovation/project/algo-lit, viitattu 11. marraskuuta 2025.

osoittaa, että myös muihin kuin suuririskisiin tekoälyjärjestelmiin on kiinnitettävä huomiota. Tällaisia raportteja voidaan laatia myös useiden eri maiden välisenä yhteistyönä yleisten kuvioiden ja trendien tunnistamiseksi.

- Toteuttaa kyselytutkimuksia tekoälyä ja ADM-järjestelmiä koskevista yleisön käsityksistä ja syrjintäriskien ymmärtämisestä. Ihannetapauksessa tämä tehtäisiin useissa eri maissa, jotta tilanteita ja vastauksia voitaisiin vertailla. Ruotsissa hallitus antoi yhdenvertaisuusvaltuutetulle toimeksiannon parantaa tietämystä syrjinnän riskeistä, joita liittyy tekoälyn ja muun automaattisen päätöksenteon käyttöön ammatillisissa konteksteissa (Ruotsin työministeriö, hallituksen päätös 07/06/2022, A2022/00877), ja työn tuloksista julkaistiin raportti marraskuussa 2023. Raportissa arvioitiin työnantajien tietämyksen tasoa tekoälyn käytöstä ja kävi ilmi, etteivät työnantajat olleet tietoisia siitä, että he käyttivät jo tekoälyä ja muuta automaattista päätöksentekoa.³⁴⁴
- Tehdä tiivistä yhteistyötä tilastovirastojen kanssa sen varmistamiseksi, että eriteltyjä tietoja kerätään ja niitä voidaan käyttää tekoäly-/ADM-järjestelmien vinoumien tekniseen analysointiin.

6.3.3. Oikeussuojan ja oikeussuojakeinojen saatavuus

Yhdenvertaisuuselimien normeja koskevilla direktiiveillä pyritään vastaamaan haasteeseen, joka liittyy yhdenvertaisuuselinten nykyisiin eroihin siinä, miten ne edistävät oikeussuojan saatavuutta, antamalla yhdenvertaisuuselimille nimenomaiset valtuudet tukea uhreja ja helpottaa oikeussuojan saatavuutta. Näihin valtuuksiin sisältyvät uhrien auttaminen,³⁴⁵ vaihtoehtoinen riidanratkaisu,³⁴⁶ selvitysten tekeminen,³⁴⁷ lausuntojen ja päätösten antaminen³⁴⁸ ja oikeus toimia oikeudenkäynneissä.³⁴⁹ Näitä säännöksiä käsitellään tarkemmin tässä osiossa.

Uhrien auttaminen ja valitusten vastaanottaminen

Yhdenvertaisuuselimien normeja koskevien direktiivien 6 artiklassa säädetään, että yhdenvertaisuuselinten ”on annettava uhreille apua tiedottamalla heille aluksi seuraavista seikoista: a) oikeudellinen kehys, mukaan lukien heidän erityistilanteeseensa kohdennettu neuvonta; b) tasa-arvoelimen tarjoamat palvelut ja niihin liittyvät menettelylliset näkökohdat; c) käytettävissä olevat oikeussuojakeinot, mukaan lukien mahdollisuus saattaa asia tuomioistuimen käsiteltäväksi; d) sovellettavat luottamuksellisuutta koskevat säännöt ja henkilötietojen suoja; ja e) mahdollisuus saada psykologista tai muunlaista tukea muilta elimiltä tai organisaatioilta.”

Tekoäly-/ADM-järjestelmien yhteydessä tämä tarkoittaa, että uhreille on kerrottava heidän oikeuksistaan tekoälyasetuksen ja EU:n tietosuojaalainsäädännön mukaisesti.

344. Diskrimineringsombudsmannen (2023), ”AI och risker för diskriminering i arbetslivet”, saatavilla osoitteessa www.do.se/rattsfall-beslut-lagar-stodmaterial/publikationer/2023/ai-och-risker-for-diskriminering-i-arbetslivet [ruotsiksi], viitattu 11. marraskuuta 2025.

345. Direktiivit yhdenvertaisuuselimistä koskevista normeista, 6 artikla.

346. Direktiivit yhdenvertaisuuselimistä koskevista normeista, 7 artikla.

347. Direktiivit yhdenvertaisuuselimistä koskevista normeista, 8 artikla.

348. Direktiivit yhdenvertaisuuselimistä koskevista normeista, 9 artikla.

349. Direktiivit yhdenvertaisuuselimistä koskevista normeista, 10 artikla.

Selvitykset

Yhdenvertaisuuselimien normeja koskevien direktiivien 8 artiklassa annetaan yhdenvertaisuuselimille valtuudet tehdä selvityksiä joko valituksen perusteella tai *suo moto* (omasta aloitteestaan, jos elimet tutkivat yhdenvertaista kohtelua koskevan oikeuden mahdollisia loukkauksia). Kuten ECRI korostaa, ”nämä selvitystoimet ovat tärkeitä muutoksenhakuprosessiin kuuluvassa näytön keräämisessä sekä syrjinnän tai suvaitsemattomuuden osoittamisessa”³⁵⁰ Jälkimmäinen toimintamuoto on erityisen tärkeä silloin, kun tekoäly-/ADM-järjestelmä on vaikeasti ymmärrettävä ja tuntematon.

Yhdenvertaisuuselimien normeja koskevien direktiivien 8 artiklan 2 kohdassa yhdenvertaisuuselimille annetaan tehokkaat oikeudet saada pääsy tietoihin ja asiakirjoihin. Tämä on merkityksellistä tekoälyasetuksen kannalta kahdesta eri syystä:

- ▶ Jos yhdenvertaisuuselimet eivät (vielä) ole [77 artiklan](#) mukaisia elimiä, tätä säännöstä voidaan tutkia elinten keinona saada käyttöön luottamuksellisuus-sääntöjen piiriin kuuluvia tietoja ja asiakirjoja, kuten teknistä dokumentaatiota tai perusoikeusvaikutusten arviointien täydellisiä versioita.
- ▶ Oikeutta saada pääsy tietoihin ja asiakirjoihin haittaa usein se, että ymmärrettävässä muodossa olevaa tietoa on vaikea saada. Koska tekoälyasetuksessa säädetään, että asetuksen nojalla laadittujen tietojen tulee olla helposti saatavilla, yhdenvertaisuuselimet voivat hyödyntää tätä ja keskittyä pyytämään tietoja ja asiakirjoja, jotka on laadittu tekoälyasetuksen nojalla. Näin ne voivat varmistaa, että ne saavat ymmärrettävässä muodossa olevaa ja hyödyllistä tietoa (edellyttäen, että saavutettavuusvaatimusta selvennetään ja noudatetaan).

Yhdenvertaisuuselimien normeja koskevien direktiivien 8 artiklan 3 kohdan mukaan yhdenvertaisuuselimet voivat kansallisen lainsäädännön ja käytännön mukaisesti antaa edellä mainitut valtuudet muulle toimivaltaiselle elimelle. Artikla avaa mahdollisuuden yhteistyöhön muttei syrjäytä yhdenvertaisuuselimä, sillä artiklan sanamuodosta käy ilmi, että toinen elin voi käyttää tätä valtuutta yhdenvertaisuuselimien ”lisäksi” eikä ”sijasta”.³⁵¹ Tätä säännöstä voidaan tutkia keinona kehittää virallista yhteistyötä muiden elinten kanssa.

Lausunnot ja päätökset

Yhdenvertaisuuselimien normeja koskevien direktiivien 9 artiklassa annetaan myös keinoja lisätä julkisen sektorin tekoäly-/ADM-järjestelmiin liittyvää yleistä ymmärrystä ja tuntemusta. Siinä säädetään, että ”[s]ekä ei-sitoviin lausuntoihin että sitoviin päätöksiin on tarvittaessa sisällyttävä erityisiä toimenpiteitä havaittujen yhdenvertaisen kohtelun periaatteen rikkomisten korjaamiseksi ja niiden toistumisen estämiseksi” ja että yhdenvertaisuuselinten on ”julkaistava vähintään tiivistelmä niistä lausunnoista ja päätöksistä, joiden ne katsovat olevan erityisen merkityksellisiä”.

350. ECRI, yleissuositus n:o 2.

351. Samankaltaista säännöksen analyysia varten katso Equinet, s. 84 (2024).

Oikeudenkäynti

Yhdenvertaisuuselimien normeja koskevien direktiivien 10 artiklassa annetaan yhdenvertaisuuselimille ei-siirtokelpoinen valtuus toimia oikeudenkäynneissä. Oikeus sisältää myös ”vähintään yhden seuraavista: a) oikeus panna vireille oikeudenkäyntimenettely yhden tai useamman uhrin puolesta; b) oikeus osallistua oikeudenkäyntimenettelyyn yhden tai useamman uhrin tukena; tai c) oikeus käynnistää oikeudenkäyntimenettelyjä omista nimissään yleisen edun puolustamiseksi”.

Tekoäly- ja ADM-järjestelmiin liittyviä oikeudenkäyntejä on vielä vähän, ja yhdenvertaisuuselinten aloitteita tai tukea tällä alalla tarvitaan.

6.3.4. Yhdenvertaisuuselinten rooli oikeussuojan ja oikeussuojakeinojen saatavuudessa

Uhrien auttaminen ja valitusten vastaanottaminen

- ▶ Varmistaa, että uhrien auttamisesta vastaava yhdenvertaisuuselinten henkilöstö on ajan tasalla tekoälyä koskevista asetuksista, jotta uhreille voidaan tiedottaa asianmukaisesti heidän oikeuksistaan.
- ▶ Koordinoida toimintaa markkinavalvontaviranomaisten (MSA) kanssa sen varmistamiseksi, että uhreja, jotka tekevät valituksia markkinavalvontaviranomaisille, voidaan auttaa tekemään valituksia myös yhdenvertaisuuselimille.

Selvitykset

- ▶ Tehdä *suo moto* -selvityksiä tietyistä tekoäly-/ADM-järjestelmistä.
- ▶ Tutkia yhdenvertaisuuselimien normeja koskevien direktiivien 8 artiklan saattamista osaksi kansallista lainsäädäntöä keinona saada käyttöön tekoälyasetuksen nojalla tuotettuja tietoja.

Lausunnot ja päätökset

- ▶ Ehdottaa lausuntojen ja päätösten yhteydessä toimenpiteitä, joilla pyritään levittämään järjestelmiä koskevaa tietoa. Esimerkiksi Bolognan tuomioistuin antoi 31. joulukuuta 2020 tuomion nro 2949/2020, jossa se määräsi Deliveroon maksamaan 50 000 euron korjaukset kantajalle, ja määräsi sitten tuomion tekstin julkaisemisen kansallisessa sanomalehdessä mahdollisimman suuren näkyvyyden takaamiseksi.³⁵²
- ▶ Julkaista järjestelmällisesti tekoäly-/ADM-järjestelmiä koskevia lausuntoja ja päätöksiä, jotta niiden käyttöä ja riskejä koskevaa tietämystä voidaan jakaa julkisesti.

Oikeudenkäynti

- ▶ Toimia oikeudenkäynneissä tekoäly-/ADM-järjestelmiin liittyvissä asioissa.

352. Fernandez Sánchez S. F. (2021), ”Frank, el algoritmo consciente de Deliveroo. Comentario a la Sentencia del Tribunal de Bolonia 2949/2020, de 31 de diciembre”, *Revista De Trabajo Y Seguridad Social CEF*, s. 179–93, saatavilla osoitteessa <https://doi.org/10.51302/rtss.2021.2374> [espanjaksi], viitattu 11. marraskuuta 2025.



7. Temaattiset painopisteet

Tässä osiossa käsitellään tekoälyn käyttöä viidellä eri aihealueella, jotka perustuvat yhdenvertaisuuselinten ja kansallisten ihmisoikeustoimijoiden yleisimmin käsittelemiin sektoreihin: lainvalvonta, muuttoliikkeen, turvapaikka-asioiden ja rajavalvonnan hallinta, koulutus, työllisyys sekä sosiaaliturva- ja työnvälityspalvelut. Kullakin aihealueella käsitellään esimerkkejä tekoälyn käytöstä ja luetellaan EU:n tekoälyasetuksen sovellettavat artiklat, jotka on otettava huomioon kyseisellä sektorilla.

7.1. Temaattinen painopiste: lainvalvonta ja muuttoliikkeen, turvapaikka-asioiden ja rajavalvonnan hallinta

7.1.1. Tausta

Tekoälyjärjestelmien käyttö lainvalvonnassa ja muuttoliikkeen, turvapaikka-asioiden ja rajavalvonnan hallinnassa

Tekoäly- ja ADM-järjestelmiä käytetään erilaisissa yhteyksissä lainvalvonnan, muuttoliikkeen, turvapaikka-asioiden ja rajavalvonnan aloilla.

Lainvalvonnassa aiemmat tutkimukset ovat tuoneet esille käyttötarkoituksia, jotka vaihtelevat aiempiin rikostietoihin perustuvasta kuvioiden kartoittamisesta ja

laittomien esineiden satelliittikuvista havaitsemisesta aina verkossa tapahtuvan vihapuheen havaitsemiseen,³⁵³ vankien väliaikaista vapautta koskeviin päätöksiin³⁵⁴ tai sukupuoleen perustuvan väkivallan riskien arviointiin.³⁵⁵

Myös kuvantunnistusta ja biometriikkaa käytetään laajalti. Suomessa poliisi voi käyttää kuvantunnistusta muiden kuin biometristen piirteiden, kuten vaatteiden ja autojen rekisterikilpien, tunnistamiseen (Xenidis, 2025). Ranska käytti etäkäyttöistä videovalvontaa Pariisin vuoden 2024 kesäolympialaisten ja paralympialaisten aikana.³⁵⁶ Yhdysvaltalaisen Clearview AI -yrityksen kaupallistaman kasvontunnistussovelluksen, joka perustuu sosiaalisen median kasvokuvien kohdentamattomaan haravoimiseen, on kerrottu olevan useiden lainvalvontaviranomaisten käytössä eri puolilla Eurooppaa (Veld et al., 2020).

Tutkimukset osoittavat kuitenkin, että kasvontunnistusteknologioissa voi esiintyä syrjiviä vinoumia.³⁵⁷ Vaikka tekoäly- ja ADM-järjestelmien ei itsessään ilmoitettaisi olevan vinoutuneita, niiden käyttöä arvostellaan siitä, että ne kohdistuvat suhteettomasti vähemmistöihin ja vähemmistöjen valvontaan sekä käyttävät etnistä profilointia. Näin voi tapahtua, kun tiettyjen sijaintien tai väestöryhmien ylivalvonta luo vahvistavan palautesilmukan työkaluihin ja vahvistaa näiden yhteisöjen massavalvontaa tai riskipisteytystä entisestään. Toinen mahdollinen esimerkki tästä on tilanne, jossa järjestelmiä käytetään eri tavoin henkilön ihonvärin mukaan, eli jos poliisit esimerkiksi tulkitsevat järjestelmän tuloksia eri tavoin epäillyn ihonvärin perusteella.

Tekoäly- ja ADM-järjestelmiä käytetään myös erilaisilla muuttoliikkeen, turvapaikkaasioiden ja rajavalvonnan hallinnan aloilla (Dumbrava 2025, Jones et al., 2023, ja McGregor, 2023). Vuonna 2023 AFAR-hankkeeseen (Algorithmic Fairness for Asylum Seekers and Refugees) kuuluvassa raportissa kartoitettiin tekoälyteknologian käyttöä muuttoliike- ja turvapaikka-asioissa Euroopassa ja tunnistettiin seuraavat käyttötavat: tulevan maahanmuuton ja pakkomuuton ennustaminen; riskinarvioinnit ja luokittelu; viisumien, matkustuslupien ja kansalaisuushakemusten käsittely; asiakirjojen todentaminen henkilöllisyyden vahvistamista ja petosten havaitsemista varten;

353. Katso Euroopan unionin perusoikeusvirasto (2022), *Bias in Algorithms: Artificial Intelligence and Discrimination*, Luxemburg: Euroopan unionin julkaisutoimisto, s. 28–49.

354. García T. et al. (2025), "Spanish prisons use a 30-year-old algorithm to decide on temporary releases", *Civio*, saatavilla osoitteessa <https://civio.es/justicia/2025/03/12/spanish-prisons-use-a-30-year-old-algorithm-to-decide-on-temporary-releases/>, viitattu 11. marraskuuta 2025.

355. Public Sector Tech Watch (2025), "Viogen 5.0: discovering Spain's risk assessment system of gender-based violence", saatavilla osoitteessa <https://interoperable-europe.ec.europa.eu/collection/public-sector-tech-watch/viogen-50-discovering-spains-risk-assessment-system-gender-based-violence>, viitattu 11. marraskuuta 2025.

356. Ministère de l'Intérieur (2025), *Expérimentation, en temps réel, de caméras « augmentées »*, saatavilla osoitteessa www.interieur.gouv.fr/actualites/actualites-du-ministere/experimentation-en-temps-reel-de-cameras-augmentees, viitattu 11. marraskuuta 2025.

357. CSO Liberty arvosteli Etelä-Walesin poliisin käyttämää kasvontunnistussovellusta esimerkiksi sukupuoleen ja/tai etniseen alkuperään perustuvasta syrjinnästä, koska positiivisten tulosten suhde oli suurempi naisten ja/tai tummaihoisten ja etnisiin vähemmistöihin kuuluvien henkilöiden kasvojen kohdalla. Katso Englannin ja Walesin muutoksenhakutuomioistuimen päätös asiassa *R (Bridges) v. Chief Constable of South Wales Police* ([2020] EWCA Civ 1058), jossa korostettiin, että Etelä-Walesin poliisin "yhdenvertaisuusvaikutusten arviointi oli ilmeisen puutteellinen ja perustui oikeuserehdykseen (koska siinä ei tunnistettu välillisen syrjinnän riskiä)" ja että sen "myöhempi lähestymistapa automaattisen kasvontunnistuksen käyttöön liittyvän välillisen syrjinnän arviointiin on virheellinen". Katso Xenidis, 2025.

puheentunnistus (turvapaikanhakijoiden alkuperämaan selvittämiseksi tai kielitaidon arvioimiseksi kansalaisuushakemuksissa); sähköinen valvonta (kuten jalkapannat); sosiaaliturvaetuuksien jakaminen; yhteensovittamistyökalut (esimerkiksi vastaanottokeskusten kohdistuksissa); ja matkapuhelintietojen poiminta henkilöllisyyden ja kertomusten vahvistamista varten (Ozkul, 2023).

Tällainen käyttö aiheuttaa riskejä perusoikeuksille. Nämä riskit johtuvat osittain välineisiin mahdollisesti sisältyvistä epätarkkuuksista, vinoumista ja stereotypioista, vaikutuksista oikeudenmukaisuuteen ja oikeudenmukaiseen menettelyyn sekä yksityisyyteen ja tietosuojaan liittyvistä kysymyksistä (Dumbrava, 2025, ja McGregor, 2023). Vuonna 2020 Foxgloven ja Joint Council for the Welfare of Immigrants -järjestön tekemän riitautuksen jälkeen Yhdistyneen kuningaskunnan sisäministeriö lopetti datavirtojen käsittelyyn tarkoitetun algoritmin käytön viisumihakemuksissa. Tämä algoritmi antoi ”punaisen” liikennevalon riskipisteytyksen tiettyjen kansallisuuksien hakijoille (BBC, 2020). Equinetin tapaustutkimuksessa, joka koski ADM-järjestelmän käyttöä Yhdistyneessä kuningaskunnassa pysyvän oleskelustatuksen määrittämiseen ja Yhdistyneessä kuningaskunnassa Brexitin jälkeen asuvien EU:n, Euroopan talousalueen (ETA) ja Sveitsin kansalaisten sekä heidän perheidensä aseman laillistamiseen, tuotiin esille useita järjestelmään liittyviä huolenaiheita. Tällaisia olivat esimerkiksi järjestelmän läpinäkyvättömyys, epävarmuus ihmisten harkintavallasta ja tiettyjen tietokantojen tarkastuksien puute, jotka johtivat naisiin kohdistuviin haitallisiin vaikutuksiin (Allen ja Masters, 2020). Huhtikuussa 2024 Kreikan tietosuojaviranomainen määräsi maahanmuutosta ja turvapaikanhausta vastaavalle ministeriölle 175 000 euron sakon, koska se oli rikkonut yleistä tietosuoja-asetusta kehittäessään ja käyttäessään Centaur- ja Hyperion-ohjelmia turvapaikanhakijoiden vastaanotto- ja majoituskeskuksissa. Centaur oli osittain automaattinen valvontajärjestelmä, jonka tarkoituksena oli ennakoida ja merkitä ”uhkia” muun muassa valvontakameroiden ja droonien avulla, kun taas Hyperion oli maahantulon ja maasta poistumisen valvontajärjestelmä (Kreikan tietosuojaviranomainen, 2024).

Erilaisia vapautuksia

Yksi tekoälyasetuksen ominaispiirre on, että se myöntää lainvalvonnassa ja muutto-liikkeen, turvapaikka-asioden ja rajavalvonnan hallinnassa käytettävälle tekoälyjärjestelmille monenlaisia vapautuksia velvoitteista. Esimerkiksi tietyissä käyttö-tarkoituksissa kiellettyjä tekoälyjärjestelmiä pidetään suuririskisinä vain lainvalvonnan yhteydessä. Yksi esimerkki tästä on biometristä luokittelua koskeva kieltö.³⁵⁸ Lisäksi niitä koskevat muita suuririskisiä tekoälyjärjestelmiä lievemmat rekisteröinti- ja tiedos-tusvelvoitteet (katso [49 artikla](#)), mikä aiheuttaa jatkuvasti kysymyksiä avoimuudesta.

Lainvalvontaan keskittyvien yhdenvertaisuuselinten ryhmien on kiinnitettävä erityistä huomiota seuraaviin tekoälyasetuksen säännöksiin.

358. Tekoälyasetus, 5 artiklan 1 kohdan g alakohta ja liitteessä III olevan 1 kohdan b alakohta.

7.1.2. Kielletyt tekoälyjärjestelmät

5 artikla: kielletyt tekoälyjärjestelmät

- ▶ 5 artiklan 1 kohdan c alakohdan mukaiset luokittelu- ja arviointijärjestelmien sosiaaliset pisteytykset. Arviointia ja luokittelua voi tapahtua esimerkiksi vankiloissa tai pakolaisleireillä videovalvontakuvien perusteella. Tällaisia käytäntöjä voidaan tietyissä olosuhteissa pitää sosiaalisena pisteytyksenä.
- ▶ 5 artiklan 1 kohdan d alakohdan mukainen luonnollisen henkilön rikokseen syyllistymisen riskin arviointi. Tämä kattaa osan ennakkoivasta poliisitoiminnasta.
- ▶ 5 artiklan 1 kohdan e alakohdan mukainen kasvotunnistustietokantojen luonti tai laajennus haravoinnilla.
- ▶ 5 artiklan 1 kohdan h alakohdan mukainen biometrinen etätunnistusjärjestelmien käyttö lainvalvontatarkoituksiin.

Useat kiellot eivät koske lainvalvonnassa tapahtuvaa käyttöä, jota kuitenkin pidetään liitteen III mukaisesti suuririskisenä:

- ▶ 5 artiklan 1 kohdan g alakohta: biometristä luokittelua koskeva kiello ei koske lainvalvontakäyttöä, jota kuitenkin pidetään liitteessä III olevan 1 kohdan b alakohdan mukaisesti suuririskisenä.
- ▶ 5 artiklan 1 kohdan f alakohta koskee tunteiden päättelyä, mutta kielloa ei sovelleta lainvalvontaan tai muuttoliikkeen ja rajavalvonnan hallintaan. Sitä pidetään kuitenkin liitteessä III olevan 1 kohdan c alakohdan mukaan suuririskisenä. Tunteiden päättelyä voidaan käyttää esimerkiksi osana valheenpaljastimia epäiltyjen kuulusteluissa.

7.1.3. Liitteen III mukaiset suuririskiset tekoälyjärjestelmät

- ▶ Biometriikkaa koskeva liitteessä III oleva 1 kohta:
 - biometriset etätunnistusjärjestelmät, elleivät kyseessä ole järjestelmät, joiden ainoana ”tarkoituksena on vahvistaa, että tietty luonnollinen henkilö on se henkilö, joka hän väittää olevansa”³⁵⁹
 - biometrinen luokittelu arkaluonteisten tai suojattujen ominaisuuksien tai ominaispiirteiden mukaisesti kyseisten ominaisuuksien tai ominaispiirteiden päättelyn perusteella³⁶⁰
 - tunteiden tunnistaminen.³⁶¹
- ▶ Liitteessä III olevan 1 kohdan 6 alakohta, joka koskee käyttöä ”lainvalvontaviranomaisten toimesta tai niiden puolesta tai unionin toimielinten, elinten, toimistojen tai virastojen toimesta lainvalvontaviranomaisten tueksi tai niiden puolesta”. Tällaisia käyttötarkoituksia ovat seuraavat:
 - Tilanteet, joissa arvioidaan ”luonnollisen henkilön riskiä joutua rikoksen uhriksi”. Yksi tällainen esimerkki voi olla edellä mainittu VioGen-järjestelmä, jota käytetään Espanjassa sukupuoleen perustuvan väkivallan yhteydessä.³⁶²

359. Tekoälyasetus, liitteessä III olevan 1 kohdan a alakohta.

360. Tekoälyasetus, liitteessä III olevan 1 kohdan b alakohta.

361. Tekoälyasetus, liitteessä III olevan 1 kohdan c alakohta.

362. Tekoälyasetus, liitteessä III olevan 6 kohdan a alakohta.

- "Valheenpaljastim[et] ja vastaav[at] väline[et]".³⁶³
- "Tekoälyjärjestelmät, joita on tarkoitus käyttää... todistusaineiston luotettavuuden arvioinnissa rikostutkinnassa tai rikosoikeudellisissa menettelyissä".³⁶⁴
- Tekoälyjärjestelmät, joita on tarkoitus käyttää rikokseen tai rikoksen uusi-miseen syyllistymisen riskin arvioinnissa "muutenkin kuin luonnollisten henkilöiden profiloinnin perusteella" (muistutus: pelkästään profilointiin perustuvat riskinarvioinnit on kielletty 5 artiklan 1 kohdan d alakohdan mukaan) tai "luonnollisten henkilöiden tai ryhmien persoonallisuuspiirteiden ja persoonallisuusominaisuuksien tai aiemman rikollisen käyttäytymisen arvioinnissa".³⁶⁵
- "Tekoälyjärjestelmät, joita on tarkoitus käyttää... luonnollisten henkilöiden profiloinnissa rikosten paljastamisen, tutkimisen tai rikoksiin liittyvien syyte-toimien yhteydessä".³⁶⁶
- ▶ Muuttoliikkeen hallintaa, turvapaikka-asioita ja rajavalvontaa koskeva liitteessä III olevan 1 kohdan 7 alakohta:
 - "Valheenpaljastim[et] ja vastaav[at] väline[et]".³⁶⁷
 - "Tekoälyjärjestelmät, joita on tarkoitus käyttää... arvioitaessa luonnollisen henkilön, joka aikoo tulla tai on tullut jäsenvaltion alueelle, aiheuttamaa riskiä, mukaan lukien turvallisuusriski, sääntöjenvastaisen maahanmuuton riski ja terveysriski".³⁶⁸
 - "Tekoälyjärjestelmät, joita on tarkoitus käyttää... turvapaikka-, viisumi- ja oleskelulupahakemusten ja niihin liittyvien valitusten käsittelyssä asemaa hakevien luonnollisten henkilöiden kelpoisuuden tarkastamiseksi, mukaan lukien todistusaineiston luotettavuuden arviointi".³⁶⁹
 - "Tekoälyjärjestelmät, joita on tarkoitus käyttää... luonnollisten henkilöiden havaitsemiseen, tunnistamiseen tai henkilöllisyyden määrittämiseen..., pois lukien matkustusasiakirjojen tarkastaminen".³⁷⁰

Muistutus: kaikki nämä käyttötarkoitukset ovat sallittuja, "jos niiden käyttö on sallit-tua asiaa koskevan unionin tai kansallisen lainsäädännön nojalla". Jos käyttö loukkaa ihmisoikeuksia ja/tai on syrjivää, on tutkittava, ovatko toteutetut toimenpiteet oikeasuhteisia ja tarpeellisia demokraattisessa yhteiskunnassa. Euroopan ihmis-oikeustuomioistuin on aiemmin todennut, että uusien teknologioiden käyttöä poliisi-toiminnassa ei voida pitää välttämättömänä demokraattisessa yhteiskunnassa, kun

363. Tekoälyasetus, liitteessä III olevan 6 kohdan b alakohta.

364. Tekoälyasetus, liitteessä III olevan 6 kohdan c alakohta.

365. Tekoälyasetus, liitteessä III olevan 6 kohdan d alakohta.

366. Tekoälyasetus, liitteessä III olevan 6 kohdan e alakohta.

367. Tekoälyasetus, liitteessä III olevan 7 kohdan a alakohta.

368. Tekoälyasetus, liitteessä III olevan 7 kohdan b alakohta.

369. Tekoälyasetus, liitteessä III olevan 7 kohdan c alakohta.

370. Tekoälyasetus, liitteessä III olevan 7 kohdan d alakohta.

on kyse DNA-profiloinnista³⁷¹ ja reaaliaikaisesta kasvontunnistuksesta³⁷². Tuomioistuin totesi asiassa *S. ja Marper* seuraavaa:

Yleissopimuksen 8 artiklan tarjoama suoja heikkenisi kohtuuttomasti, jos nykyaikaisten tieteellisten tekniikoiden käyttö rikosoikeusjärjestelmässä sallittaisiin hinnalla millä hyvänsä ja ilman, että tällaisten tekniikoiden laajamittaisesta käytöstä mahdollisesti saatavat hyödyt tasapainotettaisiin huolellisesti tärkeiden yksityisyyteen liittyvien etujen kanssa... Tuomioistuin katsoo, että valtioilla, jotka pyrkivät toimimaan edelläkävijöinä uusien teknologioiden kehittämisessä, on erityinen vastuu oikean tasapainon löytämisestä tässä suhteessa.

Joidenkin tekoälyjärjestelmien osalta on mahdollista, että tarjoajat voivat itse jättäytyä pois suuririskisten järjestelmien järjestelystä 6 artiklan 3 kohdan mukaisesti. Esimerkkinä voidaan mainita turvapaikkahakemusten käsittelyyn käytetyt tekoälykäännöstyökalut. Tätä välinettä saatetaan pitää arvioinnin ”valmistelutehtävä[nä]”, jolloin se jäisi suuririskisten tekoälyjärjestelmien määritelmän ulkopuolelle. Koska nämä työkalut toimivat tietyillä kielillä muita heikommin,³⁷³ niillä on todennäköisesti syrjiviä vaikutuksia tiettyjä kieliä puhuviin henkilöihin.

7.1.4. Rekisteröintivelvoitteet ja EU:n tekoälyasetuksen tietokanta

Lainvalvonnan ja muuttoliikkeen, turvapaikka-asioiden ja rajavalvonnan hallinnan aloilla käytettyihin suuririskisiin tekoälyjärjestelmiin sovelletaan tekoälyasetuksen mukaan lievempiä rekisteröintivelvoitteita. Niiden käyttö rekisteröidään nimenomaan EU:n tietokannan ei-julkiseen osioon, eikä FRIA-arviointien yhteenvetoja rekisteröidä tietokantaan.

On suositeltavaa, että yhdenvertaisuuselimet ja kansalliset ihmisoikeustoimijat priorisoivat mekanismien luomisen tällaisten käyttötapojen jatkuvaa seurantaa varten [77 artiklan](#) mukaisten valtuuksien avulla (tarvittaessa) tai yhteistyönä markkina-valvontaviranomaisten kanssa.

7.2. Temaattinen painopiste: koulutus

7.2.1. Tausta

Tekoäly- ja ADM-järjestelmiä voidaan käyttää koulutuksen eri aloilla, kuten sisäänpääsyssä (katso Ranskassa käytetty Parcousup-järjestelmä, jolla hakijat asetetaan paremmuusjärjestykseen ja kysyntä ja tarjonta sovitetaan yhteen korkeakoulutuksessa)³⁷⁴

371. *S. ja Marper v. Yhdistynyt kuningaskunta*, tuomio nro 30562/04 ja nro 30566/04 (2008), katso <https://hudoc.echr.coe.int/fre?i=001-90051>, viitattu 11. marraskuuta 2025.

372. *Glukhin v. Venäjä*, tuomio nro 11519/20 (2023), katso <https://hudoc.echr.coe.int/eng?i=001-225655>, viitattu 11. marraskuuta 2025.

373. Bhuiyan J. (2023), ”Lost in AI translation: growing reliance on language apps jeopardizes some asylum applications”, *The Guardian*, saatavilla osoitteessa www.theguardian.com/us-news/2023/sep/07/asylum-seekers-ai-translation-apps, viitattu 11. marraskuuta 2025.

374. AI Law Hub (2020), *French Parcoursup decision*, saatavilla osoitteessa <https://ai-lawhub.com/2020/04/16/french-parcoursup-decision/>, viitattu 11. marraskuuta 2025.

tai oppimistulosten arvioinnissa (esimerkiksi vuonna 2020 Yhdistyneen kuningaskunnan yleissivistävän koulutuksen päättökokeissa)³⁷⁵, hallinnollisissa tarkoituksissa, luokkaopetuksessa ja opiskelijoiden seurannassa. Erityisopetusta tarvitsevia oppilaita varten kehitetään yhä enemmän teknologioita, ja lisäksi luodaan hallintojärjestelmiä, joiden tarkoituksena on havaita esimerkiksi itsemurhariskejä tai terroristisympatiaa. Vuonna 2023 Alankomaiden ihmisoikeusinstituutti totesi, ettei alankomaalainen yliopisto syrjinyt opiskelijaa etnisen alkuperän perusteella käyttämällä huijausten estoon tarkoitettua ohjelmistoa.³⁷⁶ Opiskelija väitti, että ohjelmisto oli syrjivä, koska kasvontunnistus toimi teknisten rajoitusten vuoksi tummaihoisilla opiskelijoilla muita heikommin.

Koulutusympäristöissä käytetään myös muita teknologioita. Ranskassa tietosuojaviranomainen vastusti kasvontunnistuskokeilua kahden ylemmän perusasteen oppilaitoksen sisäänkäynneillä sillä perusteella, että kasvontunnistuksen käyttö ei ollut tietosuojalainsäädännön kannalta oikeasuhteista eikä välttämätöntä.³⁷⁷ Ruotsissa kouluissa käytetyn kasvontunnistuksen todettiin rikkovan tietosuojaa koskevia oikeuksia ja laajempia oikeuksia yksityisyyteen ja henkilökohtaiseen koskemattomuuteen.³⁷⁸ Vastaavasti vaatimus biometristen tietojen antamisesta tunnistamista ja lounasmaksuja varten todettiin laittomaksi Puolassa, koska toimille ei ollut oikeusperustaa.³⁷⁹

7.2.2. Kielletyt käyttötarkoitukset

Seuraavat kielletyt käyttötarkoitukset ovat erityisen merkityksellisiä koulutuksen kannalta:

- ▶ 5 artiklan 1 kohdan a ja b alakohtien mukaiset harhaanjohtavat tekniikat
- ▶ 5 artiklan 1 kohdan c alakohdan mukainen sosiaalinen pisteytys
- ▶ 5 artiklan 1 kohdan f alakohdan mukaan kielletty tunteiden päättely koulutuslaitoksissa
- ▶ 5 artiklan 1 kohdan g alakohdan mukaan kielletyt biometriset luokittelujärjestelmät, "joissa luonnolliset henkilöt luokitellaan heidän biometristen tietojensa perusteella rodun, poliittisten mielipiteiden, ammattiliiton jäsenyyden,

375. Office for Statistics Regulation Authority (2021), *Ensuring statistical models command public confidence: Learning lessons from the approach to developing models for awarding grades in the UK in 2020*, saatavilla osoitteessa <https://osr.statisticsauthority.gov.uk/publication/ensuring-statistical-models-command-public-confidence/>, viitattu 11. marraskuuta 2025

376. Racism and Technology Center (2023), "Judgement of the Dutch Institute for Human Rights shows how difficult it is to legally prove algorithmic discrimination", saatavilla osoitteessa <https://racismandtechnology.center/2023/10/17/judgement-of-the-dutch-institute-for-human-rights-shows-how-difficult-it-is-to-legally-prove-algorithmic-discrimination/>, viitattu 11. marraskuuta 2025.

377. CNIL (2022), "Expérimentation de la reconnaissance faciale dans deux lycées: la CNIL précise sa position", saatavilla osoitteessa www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position, viitattu 11. marraskuuta 2025.

378. KamR Stockholm, asia nro 5888-20, saatavilla osoitteessa https://gdprhub.eu/index.php?title=KamR_Sweden_-_Case_No._5888-20#, viitattu 11. marraskuuta 2025.

379. EDPB (5. maaliskuuta 2020), "Fine for processing student's fingerprints imposed on a school". Katso https://edpb.europa.eu/news/national-news/2020/fine-processing-students-fingerprints-imposed-school_en, viitattu 11. marraskuuta 2025.

uskonnollisen tai filosofisen vakaumuksen, seksuaalisen käyttäytymisen tai seksuaalisen suuntautumisen perusteella”.

7.2.3. Suuririskiset tekoälyjärjestelmät

- ▶ Biometriikkaa koskeva liitteessä III oleva 1 kohta ja erityisesti seuraavat:
 - liitteessä III olevan 1 kohdan a alakohdan mukaiset biometriset etätunnistusjärjestelmät³⁸⁰
 - liitteessä III olevan 1 kohdan b alakohdan mukainen biometrinen luokittelu arkaluonteisten tai suojattujen ominaisuuksien tai ominaispiirteiden mukaisesti kyseisten ominaisuuksien tai ominaispiirteiden päättelyn perusteella (ja tämä on laajempi luokitus kuin 5 artiklan 1 kohdan g alakohdan mukaan kielletyt käytännöt).
- ▶ Yleissivistävää ja ammatillista koulutusta koskeva liitteessä III oleva 3 kohta, joka kattaa seuraavat:
 - ”Tekoälyjärjestelmät, jotka on tarkoitettu käytettäväksi määrittäessä luonnollisten henkilöiden pääsyä tai hyväksymistä yleissivistäviin ja ammatillisiin oppilaitoksiin kaikilla tasoilla tai osoitettaessa luonnollisia henkilöitä niihin”.
 - ”Tekoälyjärjestelmät, jotka on tarkoitettu käytettäväksi arvioitaessa oppimistuloksia”.
 - ”Tekoälyjärjestelmät, jotka on tarkoitettu käytettäväksi sen asianmukaisen koulutustason arviointiin, jonka henkilö saa tai johon hän voi päästä”.
 - ”Tekoälyjärjestelmät, jotka on tarkoitettu käytettäväksi opiskelijoiden tarkkailuun ja kielletyn käyttäytymisen havaitsemiseen kokeiden aikana”.

7.2.4. Avoimuusvaatimukset

- ▶ Avoimuusvaatimuksia koskeva 50 artikla on erityisen merkityksellinen koulutus-kontekstin kannalta, koska generatiivista tekoälyä ja koulutusteknologioita käytetään yhä useammin luokahuoneessa suorassa vuorovaikutuksessa oppilaiden kanssa.

7.2.5. Rekisteröintivaatimukset

Koulutuksen alalla tarjoajien ja käyttöönnottajien on rekisteröitävä suuririskiset tekoälyjärjestelmät tietokannan julkiseen osioon. Rekisteröityihin tietoihin sisältyvät käyttöönnottajien tekemien FRIA-arviointien yhteenvedot.

7.3. Temaattinen painopiste: työllisyys

7.3.1. Tausta

Tekoäly- ja ADM-järjestelmiä voidaan käyttää rekrytointi- ja työllisyysprosessien eri vaiheissa aina työpaikkailmoitusten kirjoittamisesta ja niiden lukijoiden kohdentamisesta itse rekrytointiprosessiin (esimerkiksi ansioluetteloiden käsittelyyn,

³⁸⁰. Tekoälyasetus, liitteessä III oleva 1 kohta.

haastattelujen tekemiseen tai hakijoiden ja työpaikkojen yhteensovittamiseen) tai johtamiseen ja työsuorituksen arviointiin.³⁸¹ Vuonna 2024 Fortune 500 -yrityksistä 98,4 prosenttia käytti tekoälyä tai datapohjaisia järjestelmiä palkkausvaiheessa.³⁸²

Usein työnantajat käyttävät tekoälyjärjestelmiä ihmisten valvonnassa. Tätä väitettä on tarkasteltava huolella, sillä ihmisten valvonnan on täytettävä tietyt edellytykset ollakseen tehokasta, eikä se koskaan ole yksin riittävä perusoikeuksien suoja.³⁸³

7.3.2. Kielletyt käytännöt

- ▶ 5 artiklan 1 kohdan f alakohdan mukainen tunteiden päättely työpaikalla, jota voi tapahtua esimerkiksi rekrytointiprosessin aikana tai työntekijöiden tunteiden valvonnassa.
- ▶ 5 artiklan 1 kohdan g alakohdan mukainen biometrinen luokittelu, jossa "luonnolliset henkilöt luokitellaan heidän biometristen tietojensa perusteella rodun, poliittisten mielipiteiden, ammattiliiton jäsenyyden, uskonnollisen tai filosofisen vakaumuksen, seksuaalisen käyttäytymisen tai seksuaalisen suuntautumisen perusteella". Rekrytoijat tai työnantajat saattavat olla kiinnostuneita tällaisista tiedoista.

7.3.3. Suuririskiset käytännöt

- ▶ Biometriikkaa koskeva liitteessä III oleva 1 kohta ja erityisesti seuraavat:
 - liitteessä III olevan 1 kohdan a alakohdan mukaiset biometriset etätunnistusjärjestelmät
 - liitteessä III olevan 1 kohdan b alakohdan mukainen biometrinen luokittelu arkaluonteisten tai suojattujen ominaisuuksien tai ominaispiirteiden mukaisesti kyseisten ominaisuuksien tai ominaispiirteiden päättelyn perusteella (ja tämä on laajempi luokitus kuin 5 artiklan 1 kohdan g alakohdan mukaan kielletyt käytännöt).
- ▶ Liitteessä III olevan 4 kohdan mukaiset työllistämisen, henkilöstöhallinnon ja itsenäisen ammatinharjoittamisen mahdollistamisen alat. Tämä kattaa seuraavat järjestelmät:
 - "Tekoälyjärjestelmät, jotka on tarkoitettu käytettäväksi luonnollisten henkilöiden rekrytoinnissa tai valinnassa, erityisesti kohdennettujen työpaikka-ilmoitusten esittämiseen, työhakemusten analysointiin ja suodattamiseen sekä hakijoiden arviointiin".³⁸⁴
 - "Tekoälyjärjestelmät, jotka on tarkoitettu käytettäväksi työsuhteen ehtoja, uralla etenemistä ja työhön liittyvien sopimussuhteiden päättämistä koskevien

381. Simons J. (2020), "Machine learning: case studies, Institute for the Future of Work", saatavilla osoitteessa www.ifow.org/publications/2020/2/24/machine-learning-case-studies, viitattu 11. marraskuuta 2025.

382. Jobscan (2024), "2024 Applicant Tracking System (ATS) usage report: key shifts and strategies for job seekers", saatavilla osoitteessa www.jobscan.co/blog/fortune-500-use-applicant-tracking-systems, viitattu 11. marraskuuta 2025.

383. Green B. (2022), "The flaws of policies requiring human oversight of government algorithms", *Computer Law & Security Review*, 45, artikkeli 105681, saatavilla osoitteessa <https://doi.org/10.1016/j.clsr.2022.105681>, viitattu 11. marraskuuta 2025.

384. Tekoälyasetus, liitteessä III olevan 4 kohdan a alakohta.

päätösten tekemiseen, tehtävien jakamiseen yksilöllisen käytöksen tai persoonallisuuspiirteiden tai henkilön ominaisuuksien perusteella tai tällaisissa suhteissa olevien henkilöiden suorituksen ja käyttäytymisen seurantaan ja arviointiin”.

On todennäköistä, etteivät tarjoajat pidä kaikkia näillä alueilla käytettyjä järjestelmiä suuririskisinä 6 artiklan 3 kohdan mukaan. Esimerkiksi ansioluetteloiden ja motivaatiokirjeiden arviointiin käytettävää tekoälyjärjestelmää saatetaan pitää arvioinnin ”valmistelutehtävä[nä]”.

7.3.4. Avoimuusvaatimukset

- 50 artikla avoimuusvaatimuksista on erityisen merkityksellinen työllisyyden kontekstissa ja varsinkin rekrytointivaiheessa, sillä tekoälytyökaluja käytetään yhä enemmän palkkausprosessissa.

7.3.5. Rekisteröinti- ja tiedotusvelvollisuudet

Tekoälyasetuksen 26 artiklan 7 kohdassa säädetään työnantajina toimivien käyttöönottajien tiedotusvelvollisuudesta. Ennen kuin ne ottavat käyttöön tai käyttävät työpaikalla suuririskistä tekoälyjärjestelmää, niiden ”on ilmoitettava työntekijöiden edustajille ja asianomaisille työntekijöille, että heihin sovelletaan suuririskistä tekoälyjärjestelmää”³⁸⁵.

Työllistämiseen, henkilöstöhallintoon ja itsenäisen ammatinharjoittamisen mahdollistamiseen liittyvien tekoälyjärjestelmien tarjoajien (liitteessä III oleva 4 kohta) on rekisteröitävä järjestelmänsä EU:n tietokantaan. Tämä velvoite ei kuitenkaan koske käyttöönottajia, jotka ovat yksityisiä tahoja. Käyttöönottajilla ei myöskään ole velvollisuutta tehdä perusoikeusvaikutusten arviointia. Tämä velvoitteiden puuttuminen saattaa johtaa käytössä olevien järjestelmien ja niiden vaikutusten näkyvyyden puutteeseen esimerkiksi suuryrityksissä.

7.4. Temaattinen painopiste: sosiaaliturva- ja työnvälityspalvelut

7.4.1. Tausta

Lukuisat virastot käyttävät tekoäly- ja ADM-järjestelmiä sosiaaliturva- ja työnvälityspalvelujen alalla esimerkiksi tukikelpoisuuden määrittämiseen, sosiaaliturvaetuuksien laskemiseen, valvonnan kohdentamiseen petosten ja virheiden havaitsemisessa sekä tuensaajien resurssien jakamiseen. Tekoälyjärjestelmiä tarjotaan tapauksia käsitteleville ja työnhakijoita tukeville työntekijöille, ja tekoälyyn perustuvia chatti-botteja käytetään yhä useammin vuorovaikutuksessa edunsaajien kanssa. Ranskan työvoimatoimisto France Travail on kehittänyt useita tekoälyjärjestelmiä osana Intelligence Emploi -ohjelmaansa, mukaan lukien MatchFT-chattibotin, jolla lähetetään työtarjouksia potentiaalisille työnhakijoille ja varmistetaan heidän kiinnostuksensa ja kelpoisuutensa, sekä ChatFT-chattibotin, jota tapauksia käsittelevät työntekijät

³⁸⁵. Tekoälyasetus, 26 artiklan 7 kohta.

voivat käyttää tietojen hakemiseen viraston tietokannoista (info.gouv.fr, 2025). FARI-instituutin (AI for the Common Good Institute) ja Brysselin julkisen työvoimatoimiston Actirisin yhteistyönä toteuttamassa IA-NAVIGATE-hankkeessa kartoitettiin Brysselin työnhakijoita tukevien ammattilaisten tekoälytyökalujen käyttöä ja todettiin, että noin 60 prosenttia oli jo käyttänyt tekoälytyökaluja työssään. Useimmiten työkaluja käytettiin raporttien kirjoittamiseen, työpajojen suunnitteluun, ansioluetteloiden muokkaamiseen ja työhaastatteluihin valmistautumiseen. Tutkimuksessa kävi myös ilmi, että yli 80 prosenttia vastaajista ei ollut saanut tekoälytyökalujen käyttöä koskevia ohjeita työnantajiltaan (Xenidis, 2025).

Osa näistä järjestelmistä on jo todettu syrjiviksi. Esimerkiksi Alankomaissa havaittiin, että petosten ennustamiseen käytetty järjestelmä oli syrjinyt tuensaajia etnisen alkuperän ja kansalaisuuden perusteella.³⁸⁶ Itävallassa työvoimatoimisto kehitti AMS-algoritmin, jonka avulla työllistymismahdollisuuksia voitiin ennustaa ja tukiresursseja jakaa työnhakijoille. Prototyypin osoitettiin syrjivän naisia (erityisesti yksinhuoltajajäitejä) ja maahanmuuttajataustaisia työnhakijoita.³⁸⁷ Puolassa työvoimatoimiston käyttämästä järjestelmästä luovuttiin lopulta, koska sitä pidettiin perustuslain vastaisena.³⁸⁸ ADM- ja tekoälyjärjestelmiä käytetään tai käytettiin myös sosiaaliturvan tuensaajien valvontaan useissa eri maissa, kuten Ranskassa, Alankomaissa, Tanskassa ja Belgiassa – syrjivin lopputuloksin.³⁸⁹

Kansalaisjärjestöt ovat vieneet Ranskan korkeimman hallinto-oikeuden (Conseil d'État) käsiteltäväksi tapauksen, joka koskee Ranskan sosiaaliviraston riskipisteytysjärjestelmän käyttöä mahdollisten petosten ja virheiden ennustamiseen ja kohdennettuun valvontaan.³⁹⁰ Kansalaisjärjestöt ovat tuoneet esille muun muassa sukupuoleen, perhetilanteeseen, ikään ja vammaisuuteen perustuvaa syrjintää. Asianosaiset pyysivät Conseil d'État'ta esittämään Euroopan unionin tuomioistuimelle

386. De Rechtspraak (13. helmikuuta 2019) "SyRI legislation in breach of European Convention on Human Rights", *De Rechtspraak*, saatavilla osoitteessa www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Rechtbanken/Rechtbank-Den-Haag/Nieuws/Paginas/SyRI-legislation-in-breach-of-European-Convention-on-Human-Rights.aspx, viitattu 11. marraskuuta 2025. SyRI-järjestelmän katsottiin myös loukanneen kohtuuttomasti loppukäyttäjien oikeutta yksityisyyteen, koska se käsitteli eri valtion virastoilta saatuja henkilötietoja.

387. Allhutter D et al. (2020) "Algorithmic profiling of job seekers in Austria: How austerity politics are made effective", *Frontiers in Big Data*, 3, saatavilla osoitteessa <https://doi.org/10.3389/fdata.2020.00005>, viitattu 11. marraskuuta 2025.

388. Szymielewicz K. et al. (2015), "Profiling the unemployed in Poland: social and political implications of algorithmic decision making", Fundacja Panoptykon, 2015, saatavilla osoitteessa <https://en.panoptykon.org/profiling-unemployed-poland-report>, viitattu 11. marraskuuta 2025.

389. Romain et al. (2023); Mehrotra D. et al. (2023), "Inside the suspicion machine", *WIRED*, saatavilla osoitteessa www.wired.com/story/welfare-state-algorithms/, viitattu 11. marraskuuta 2025; Geiger G. (2023), "How Denmark's welfare state became a surveillance nightmare", *WIRED*, 7. maaliskuuta, saatavilla osoitteessa www.wired.com/story/algorithms-welfare-state-politics/, viitattu 11. marraskuuta 2025; Amnesty International (2024), "Denmark: AI-powered welfare system fuels mass surveillance and risks discriminating against marginalized groups – report", saatavilla osoitteessa www.amnesty.org/en/latest/news/2024/11/denmark-ai-powered-welfare-system-fuels-mass-surveillance-and-risks-discriminating-against-marginalized-groups-report/, viitattu 11. marraskuuta 2025; Degreve E. (2020), "The use of secret algorithms to combat social fraud in Belgium", *European Review of Digital Administration & Law* 1–2: 167–78.

390. Amnesty International (2024), *France: CNAF State Council Complaint*, saatavilla osoitteessa www.amnesty.org/fr/documents/eur21/8795/2024/en/, viitattu 11. marraskuuta 2025.

kysymyksiä, jotka koskivat muun muassa algoritmista syrjintää.³⁹¹ Kysymys välillisestä syrjinnästä ja tosiasiallisesta yhdenvertaisuudesta on erityisen merkityksellinen sosiaaliturvajärjestelmissä.³⁹²

Toinen keskeinen asia on arvioida, mitkä järjestelmät kuuluvat tekoälyasetuksen mukaisen tekoälyjärjestelmän määritelmän piiriin, sillä monet sosiaaliturvan järjestelmät ovat vielä teknisesti suhteellisen yksinkertaisia, vaikka ne aiheuttavatkin merkittävän riskin perusoikeuksille.

7.4.2. Kielletyt tekoälyjärjestelmät

- ▶ 5 artiklan 1 kohdan c alakohdan sosiaalista pisteytystä koskeva säännös on ratkaisevan tärkeä sosiaaliturva- ja työnvälityspalvelujen alalla, jolla on käytössä monia järjestelmiä esimerkiksi tuensaajien valvontaa tai ohjaamista varten (katso aiempi).
- ▶ 5 artiklan 1 kohdan f alakohdan mukainen tunteiden päättely työpaikalla. Tällaista voi tapahtua esimerkiksi rekrytointiprosessin aikana.

7.4.3. Suuririskiset tekoälyjärjestelmät

Liitteessä III oleva 5 kohta koskee välttämättömien yksityisten ja julkisten palvelujen ja etuuksien saatavuutta ja käyttöä ja kattaa ”tekoälyjärjestelmät, jotka on tarkoitettu käytettäväksi viranomaisten toimesta tai viranomaisten puolesta sen arviointiin, ovatko luonnolliset henkilöt oikeutettuja välttämättömiin julkisen avun etuuksiin ja palveluihin, kuten terveydenhuollon palveluihin, sekä tällaisten etuuksien ja palvelujen myöntämiseen, vähentämiseen, peruuttamiseen tai takaisin perimiseen”.³⁹³

Virastot käyttävät laskentajärjestelmiä ja usein sääntöpohjaisia järjestelmiä edunsaajien etuuksien laskemiseen. Tässä yhteydessä on kyse siitä, mitkä laskentajärjestelmät kuuluvat tekoälyasetuksen tekoälyjärjestelmien määritelmän piiriin.

Tekoälyasetuksen 6 artiklan mukaan tarjoajat voivat tietyin ehdoin jättäytyä suuririskisten järjestelmien järjestelyn ulkopuolelle. Joitakin näistä ehdoista sovelletaan todennäköisesti hyvinvointi- ja sosiaaliturvajärjestelmiin. Esimerkkejä tästä ovat luonnollisen kielen käsittelyn (NLP) käyttö työnhakijoiden sähköpostiviestien

391. Kysymys on seuraava: ”Jos käsiteltävien henkilötietojen rekisterinpitäjä on julkinen sosiaalishallinto, jolle on uskottu julkisen palvelun tehtävä, ja tietojen käsittelyn tarkoituksena on laatia julkisen palvelun käyttäjien riskipisteytys, jota hallinto käyttää kohdennettuun valvontaan, eikä henkilötietojen käsittely aiheuta tällöin välillistä syrjintää neuvoston direktiivin 2000/43/EY, annettu 29 päivänä kesäkuuta 2000, ja neuvoston direktiivin 79/7/ETY, annettu 19 päivänä joulukuuta 1978, tarkoituksen mukaisesti, kun niitä tulkitaan perusoikeuskirjan 20 ja 21 artiklan mukaan, ottaen huomioon, että tämä käsittely on johtanut alle 30-vuotiaiden, opiskelijoiden, pienituloisten, työvoimaan kuulumattomien, yksinhuoltajien (joista 95 % on naisia) tai sosiaalitutkia saavien henkilöiden tarkastusten määrän merkittävään lisääntymiseen?” (Amnesty Internationalin englanninkielisen käännöksen käännös). Amnesty International (2024), *France: CNAF State Council Complaint*, kohta 71, saatavilla osoitteessa www.amnesty.org/fr/documents/eur21/8795/2024/en/, viitattu 11. marraskuuta 2025.

392. Wachter S., Mittelstadt B., Russell C. (2020), ”Bias preservation in machine learning: the legality of fairness metrics under EU non-discrimination law”, *West Virginia Law Review*, 123(3), 735.

393. Tekoälyasetus, liitteessä III olevan 5 kohdan a alakohda.

sisällön analysointiin,³⁹⁴ mitä saatetaan pitää ”valmistelutehtävä[nä]”, tai optisen merkintunnistuksen (OCR) käyttö hakemusten rajaamisessa, kääntämisessä ja siivoamisessa,³⁹⁵ mitä saatetaan pitää ”suppea[na] menettelylli[senä] tehtävä[nä]”. Kuten muualla näissä suuntaviivoissa kuitenkin todetaan, nämä määritelmät ovat edelleen epämääräisiä, ja oikeuskäytännön puuttuessa niitä on tarkkailtava tarkasti.

7.4.4. Rekisteröintivelvoitteet

Sosiaaliturvan alalla tarjoajien ja käyttöönottajien on rekisteröitävä suuririskiset tekoälyjärjestelmät tietokannan julkiseen osioon. Rekisteröityihin tietoihin sisältyvät käyttöönottajien tekemien FRIA-arviointien yhteenvedot.

394. Euroopan unionin perusoikeusvirasto (2020), *Getting the Future Right: Artificial Intelligence and fundamental rights*, Luxemburg: Euroopan unionin julkaisutoimisto, s. 32.

395. Ibid., s. 33.

Lähdeviitteet

Allen R. and Masters D. (2020), *Regulating for an equal AI: A new role for equality bodies: Meeting the new challenges to equality and non-discrimination from increased digitisation and the use of Artificial Intelligence*, Equinet.

BBC (2020), "Home Office drops 'racist' algorithm from visa decisions", BBC, available at: www.bbc.com/news/technology-53650758, accessed 7 November 2025.

Direction générale des Entreprises (2025), Les autorités compétentes pour la mise en œuvre du règlement européen sur l'intelligence artificielle [Competent authorities for the implementation of the Artificial Intelligence Act], Ministère de l'Économie, des Finances et de la Souveraineté industrielle, available at www.entreprises.gouv.fr/priorites-et-actions/transition-numerique/soutenir-le-developpement-de-lia-au-service-de-0, accessed 7 November 2025.

Dumbrava C. (2025), "Briefing: Artificial intelligence in asylum procedures in the EU", European Parliamentary Research Service, available at [www.europarl.europa.eu/RegData/etudes/BRIE/2025/775861/EPRS_BRI\(2025\)775861_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775861/EPRS_BRI(2025)775861_EN.pdf), accessed 7 November 2025.

Equinet (2024), *Understanding the new EU Directives on standards for equality bodies: legal digest on standards for equality bodies*, available at <https://equineteurope.org/publications/understanding-the-new-eu-directives-on-standards-for-equality-bodies-legal-digest-on-standards-for-equality-bodies/>, accessed 11 November 2025.

Equinet (2025), *How to use the Artificial Intelligence Act to investigate AI bias and discrimination: A guide for equality bodies*, European Network of Equality Bodies, available at <https://equineteurope.org/publications/how-to-use-the-artificial-intelligence-act-to-investigate-ai-bias-and-discrimination-a-guide-for-equality-bodies/>, accessed 10 November 2025.

European Union Agency for Fundamental Rights (2021), Equality in the EU: 20 years on from the initial implementation of the Equality Directives, available at: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2021-opinion-equality-directives-01-2021_en_0.pdf, accessed 7 November 2025.

Hellenic Data Protection Authority (2024), Ministry of Migration and Asylum receives administrative fine and GDPR compliance order following an own-initiative investigation by the Hellenic Data Protection Authority, available at: www.dpa.gr/en/enimerwtiko/press-releases/ministry-migration-and-asylum-receives-administrative-fine-and-gdpr, accessed 7 November 2025.

Ilieva M. (2024), *Handbook on identifying and using equality data in legal casework*, Equinet, available at: <https://equineteurope.org/publications/handbook-on-identifying-and-using-equality-data-in-legal-casework/>, accessed 7 November 2025.

info.gouv.fr (2025), France Travail : comment ça marche? [How does France Travail work?], available at: www.info.gouv.fr/actualite/france-travail-comment-ca-marche, accessed 7 November 2025.

Jones C., Lanneau R., Maccanico Y. (2023), Europe's techno borders, EuroMed Rights and Statewatch, available at www.statewatch.org/publications/reports-and-books/europe-s-techno-borders/, accessed 7 November 2025.

McGregor L. (2023), *Digital border governance: a human rights based approach*, University of Essex and the OHCHR, available at www.ohchr.org/en/documents/tools-and-resources/digital-border-governance-human-rights-based-approach, accessed 7 November 2025.

Ozkul D. (2023), Automating immigration and asylum: the uses of new technologies in migration and asylum governance in Europe, Oxford: Refugee Studies Centre, University of Oxford, available at www.rsc.ox.ac.uk/publications/automating-immigration-and-asylum-the-uses-of-new-technologies-in-migration-and-asylum-governance-in-europe, accessed 7 November 2025.

Romain M. et al. (2023), "Is data neutral? How an algorithm decides which French households to audit for welfare fraud", *Le Monde*, available at www.lemonde.fr/en/les-decodeurs/visuel/2023/12/05/how-an-algorithm-decides-which-french-households-to-audit-for-benefit-fraud_6313254_8.html, accessed 11 November 2025.

Subgroup on Equality Data of the European Commission's High Level Group on Non-discrimination, Equality and Diversity (2025), Collecting and using equality data in full compliance with EU General Data Protection Regulation and national data protection rules, Publications Office of the European Union, available at: https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combating-discrimination/equality-data-collection_en, accessed 7 November 2025.

Veld S. (in 't) et al. (2020), Letter to Andrea Jelinek, Chair of the European Data Protection Board on the possible use of the Clearview AI application by law enforcement authorities in the EU, available at www.edpb.europa.eu/sites/default/files/files/file1/edpb_letter_out_2020-0052_facialrecognition.pdf, accessed 7 November 2025.

Xenidis R. (2020), Tuning EU equality law to algorithmic discrimination: Three pathways to resilience, *Maastricht Journal of European and Comparative Law*, available at: <https://journals.sagepub.com/doi/10.1177/1023263X20982173>, accessed 7 November 2025.

Xenidis R. (2025), "Legal protection against algorithmic discrimination in Europe: Current frameworks and remaining gaps", Council of Europe, Strasbourg.

Julkishallinnot ympäri Eurooppaa käyttävät tekoälyä ja/tai automatisoituja päätöksentekojärjestelmiä (ADM) monilla politiikan aloilla, kuten maahanmuutto, sosiaaliturva, oikeus, koulutus, työllisyys, verotus, lainvalvonta ja terveydenhuolto. Tällaisia järjestelmiä käytetään myös yksityisen sektorin kriittisillä aloilla, kuten pankki- ja vakuutusallalla. Vaikka tekoäly- ja ADM-järjestelmät aiheuttavat merkittäviä syrjintäriskejä, näiden riskien tunnistaminen ja lieventäminen on edelleen haasteellista. Siksi yhdenvertaisuuselinten ja muiden kansallisten ihmisoikeustoimijoiden rooli on keskeinen, kun edistetään tekoäly- ja ADM-järjestelmien perusoikeuksien mukaista käyttöä erityisesti julkisella sektorilla. Ohjeiden tarkoituksena on antaa tasa-arvoelimille ja muille kansallisille ihmisoikeustoimijoille, erityisesti Euroopan unionissa, valmiudet torjua syrjintää tekoäly- ja ADM-järjestelmissä. Niissä päivitetään tasa-arvo- ja yhdenvertaisuuselinten vastuut muuttuvassa sääntely-ympäristössä – mukaan lukien Euroopan unionin tekoälyasetus ja Euroopan neuvoston puiteyleissopimus tekoälystä ja ihmisoikeuksista, demokratiasta ja oikeusvaltioperiaatteesta – annetaan suosituksia ja esimerkkejä uusien säännösten soveltamisesta ja tarjotaan apua ja neuvoja kansallisille sidosryhmille, kuten ihmisoikeuksia, tasa-arvoa ja syrjimättömyyttä koskevien päätösten tekijöille ja valvontaviranomaisille.



YHDENVERTAISUUSVALTUUTETTU
NON-DISCRIMINATION OMBUDSMAN



COMISSÃO PARA A CIDADANIA
E A IGUALDADE DE GÉNERO

PREMS 163925

FIN

Euroopan unionin jäsenvaltiot ovat päättäneet yhdistää osaamisensa, voimavaransa ja kohtalonsa. Yhdessä he ovat luoneet vakauden, demokratian ja kestävän kehityksen alueen, jossa pidetään yllä kulttuurista monimuotoisuutta, suvaitsevaisuutta ja yksilön vapauksia. Euroopan unioni on sitoutunut jakamaan saavutuksensa ja arvonsa muiden maiden ja kansojen kanssa.

www.europa.eu

Euroopan neuvosto on maanosansa johtava ihmisoikeusjärjestö. Sillä on 46 jäsenvaltiota, mukaan lukien kaikki Euroopan unionin jäsenet. Kaikki Euroopan neuvoston jäsenvaltiot ovat allekirjoittaneet ihmisoikeuksien, demokratian ja oikeusvaltion suojaamiseksi tehdyn Euroopan ihmisoikeussopimuksen. Euroopan ihmisoikeustuomioistuin valvoo ihmisoikeussopimuksen täytäntöönpanoa jäsenvaltioissa.

www.coe.int



EUROOPAN UNIONI

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE