

EUROOPPALAINEN ALGORITMISEN SYRJINNÄN ARVIOINTIMENETELMÄ



Yhteistyössä

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

Louise Hooper

Ylja Remmits

Ioanna Papageorgiou

Euroopan unionin
yhteisrahoittama



EUROOPAN UNIONI

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

Euroopan neuvoston
yhteisrahoittama ja toteuttama

EUROOPPALAINEN ALGORITMISEN SYRJINNÄN ARVIOINTIMENETELMÄ

Louise Hooper

Ylja Remmits

Ioanna Papageorgiou

Yhteistyössä

Interfederal Centre for Equal Opportunities (Unia), Belgia

Yhdenvertaisuusvaltuutettu (YVV), Suomi

Commission for Citizenship and Gender Equality (CIG), Portugali

Tämä julkaisu on laadittu Euroopan unionin ja Euroopan neuvoston taloudellisella tuella. Julkaisun 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 luonteeseen, 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 (Anti-discrimination and Inclusion Department) tekoälykoordinaattorille, F-67075 Strasbourg Cedex, sähköposti: anti-discrimination@coe.int

Kansi ja ulkoasu: Euroopan neuvoston julkaisuista ja visuaalisesta ilmeestä vastaava osasto (Publications and Visual Identity Division)
Englanninkielisen julkaisun taitto: Luminess
Suomenkielisen julkaisun taitto: Vida Design, Pori
Käännös: ALM Translations
Käännöksen oikeudellinen tarkastus: Rebekka Nurmala
Kuvat: Shutterstock, Unsplash ja Better Images of AI

Sisällys

LYHENTEET	7
TERMINOLOGIA	8
KIITOKSET	11
TIIVISTELMÄ	12
JOHDANTO	14
Uuden oikeudellisen kehyksen tärkeimmät elementit	15
Tekoälyasetuksen mukaiset riskiluokat	20
Miten riskiluokkia sovelletaan arviointimenetelmässä?	21
Kielletyt syrjintäperusteet	22
ARVIOINTIMENETELMÄN KÄYTTÖ	24
Vaihe 1	24
Vaihe 2	25
Vaihe 3	25
Vaihe 4	25
VAIHE 1 – TEKÖÄLY- TAI ALGORITMIJÄRJESTELMIEN TUNNISTAMINEN	27
Algoritmijärjestelmien ja tekoälyn tunnistaminen	28
1.1. Alustava tiedonkeruu	29
1.2. Tarkempi asiakirjatutkimus	36
1.3. Algoritmijärjestelmien tai suuririskisten tekoälyjärjestelmien tunnistaminen	40
1.4. Tapauksen käsittelyn jatkaminen	43
VAIHE 2 – TIEDONKERUU TEKÖÄLY- TAI ALGORITMIJÄRJESTELMÄSTÄ SYRJINNÄN TUNNISTAMISEKSI	46
2.1. Algoritmijärjestelmät	49
2.2. Suuririskisistä tekoälyjärjestelmistä saatavilla olevat lisätiedot	61
VAIHE 3 – VASTAANOTETTUIJEN TIETOJEN ARVIOINTIMENETELMÄ	79
Johdatus käsitteisiin	81
Vaiheen 3 käyttö	89
3.1. Mitä tunnettuja tai epäiltyjä syrjinnän riskejä on?	90
3.2. Sisältyykö syötteisiin tai datajoukkoihin tunnettuja syrjintäperusteita tai sijaismuuttujia?	94
3.3. Perusoikeuksiin kohdistuvien riskien arviointi (riskinarvioinnit, HRIA, FRIA ja DPIA)	97
3.4. Mitä algoritmijärjestelmän on tarkoitus tehdä ja miten se tekee sen?	103
3.5. Koulutus-, testaus- ja validointidata	109
3.6. Testaus ja arviointi	115
3.7. Arviointi siitä, onko näyttö riittävää tukemaan tekoäly- tai algoritmijärjestelmään liittyvää <i>prima facie</i> -syrjintätapausta	128
3.8. Voiko vastaaja osoittaa, ettei erilainen kohtelu ole syrjivää?	132
VAIHE 4 – OIKEUSSUOJAKEINOT	138
4.1. Kaikkien algoritmijärjestelmien oikeussuojakeinot	140
4.2. Lisää oikeussuojakeinoja suuririskisille tekoälyjärjestelmille	146
4.3. Tilanteet, joissa järjestelmä tai käytötapausta aiheuttaa riskin perusoikeuksille, mutta sitä ei ole luokiteltu suuririskiseksi tai kielletyksi	149
LÄHTEET	153
Kirjallisuus	153
Lainsäädäntö	160
Juridiikka/oikeuskäytäntö	162

LIITE A – MALLIPOHJA REKISTERÖIDYN PYYNNÖLLE SAADA PÄÄSY TIETOIHIN (DSAR)	167
LIITE B – MALLIPOHJA SELITYKSEN PYYTÄMISEEN TEKÖÄLYASETUKSEN 86 ARTIKLAN MUKAISESTI	170
LIITE C – ESIMERKKEJÄ ALGORITMIEN JA TEKÖÄLYN KÄYTÖSTÄ	172
LIITE D – ESIMERKKEJÄ ALGORITMISESTA SYRJINNÄSTÄ TAI SYRJINNÄN RISKEISTÄ	174
LIITE E – SIJAISMUUTTUJAT	176
LIITE F – LUETTELO TEKÖÄLY- JA ALGORITMIREKISTEREISTÄ EUROOPASSA	179
LIITE G – SYRJIMÄTTÖMYYS DIREKTIIVIT, KIELLETYT SYRJINTÄPERUSTEET JA SOVELTAMISALA	181
LIITE H – MUUT MAHDOLLISET ASIAANKUULUVAT ASETUKSET JA OHJEET	183
LIITE I – SUURIRISKISET TEKÖÄLYYN LIITTYVÄT KÄYTÄNNÖT	186
LIITE J – KIELLETYT TEKÖÄLYYN LIITTYVÄT KÄYTÄNNÖT	188
LIITE K – VAIHEEN 3 MALLILOMAKE	207

Lyhenteet

ADR	Vaihtoehtoinen riidanratkaisu
ADM	Automaattinen päätöksenteko
AI	Tekoäly
EUT	Euroopan unionin tuomioistuin
CSO	Kansalaisjärjestö
DPA	Tietosuojaviranomainen
DPIA	Tietosuojaa koskeva vaikutustenarviointi
DSAR	Rekisteröidyn pyyntö saada pääsy tietoihin
EB	Yhdenvertaisuuselin
EDPB	Euroopan tietosuojaneuvosto
FRIA	Perusoikeusvaikutusten arviointi
GDPR	Yleinen tietosuoja-asetus
HRIA	Ihmisoikeusvaikutusten arviointi
LED	Direktiivi lainvalvontatarkoituksessa käsiteltyjen henkilötietojen suojasta
MSA	Markkinavalvontaviranomainen
RBI	Biometrinen etätunnistus

Terminologia

Tässä arviointimenetelmässä käytetään seuraavia asiaankuuluvia terminologiavalintoja tai käytetyillä termeillä on alla esitetyt merkitykset.

Tekoälyjärjestelmä: ”konepohjainen järjestelmä, joka on suunniteltu toimimaan käyttöönoton jälkeen vaihtelevilla autonomian tasoilla ja jossa voi ilmetä mukautuvuutta käyttöönoton jälkeen ja joka päättelee vastaanottamastaan syötteestä eksplisiittisiä tai implisiittisiä tavoitteita varten, miten tuottaa tuotoksia, kuten ennusteita, sisältöä, suosituksia tai päätöksiä, jotka voivat vaikuttaa fyysisiin tai virtuaalisiin ympäristöihin” (tekoälyasetus, 3 artiklan 1 kohta).

Algoritmijärjestelmä: Tässä arviointimenetelmässä käytetty termi, joka kattaa sekä tekoälyjärjestelmät että muut järjestelmät, mukaan lukien automaattisen päätöksenteon (ADM) järjestelmät. Termi sisältää myös tekoälyjärjestelmät, joita ei käytetä päätöksentekoprosesseissa.

Automaattisen päätöksenteon (ADM) järjestelmä: Termi kattaa monenlaisia automaattisia järjestelmiä, joita käytetään päätöksenteon yhteydessä tai tarkoituksiin. Ne voivat olla tekoälypohjaisia, mutta ne voivat pohjautua myös muihin teknologioihin, kuten yksinkertaisiin ”jos A, niin B”-sääntöihin. Ne vaihtelevat täysin automaattisista järjestelmistä, joihin ei liity lainkaan ihmisen tekemiä syötteitä, osittain automaattisiin järjestelmiin tai päätöksenteon tukijärjestelmiin, joihin sisältyy sekä koneen että ihmisen tekemiä syötteitä ja joita käytetään hyvin laajasti.

Tapauksen käsittelijä: yhdenvertaisuuselimen henkilö, joka suorittaa arvioinnin missä tahansa tämän arviointimenetelmän vaiheessa osana syrjintätapausten tutkintatyötä.¹

Kantelija(t): Henkilö tai henkilöryhmä, joka väittää kokevansa tai kokee (laitonta) syrjintää. Jotta termit olisivat yhdenmukaisia yleisen tietosuoja-asetuksen ja tekoälyasetuksen sanamuotojen kanssa, termit ”rekisteröity” ja ”henkilöt, joihin vaikutukset kohdistuvat” vastaavat termiä ”kantelija”, kun viitataan näiden asetusten sovellettaviin säännöksiin.

Sekaannusmatriisi: Taulukko, jota käytetään algoritmijärjestelmän suorituskyvyn arviointiin vertaamalla sen ennusteita todellisiin reaali maailman tuloksiin. Sekaannusmatriisitaulukon riveille merkitään todelliset reaali maailman tulokset, kun taas sarakkeille merkitään järjestelmän ennusteet. Taulukosta voi tarkistaa, kuinka moni ennusteista oli oikein tai väärin.

Asiantuntija: Erityisosaamista tai teknistä asiantuntemusta omaava henkilö, jota yhdenvertaisuuselin on konsultoinut tai joka tukee tapauksen käsittelijää minkä

1. Vaikka tämä arviointimenetelmä on ensisijaisesti suunnattu yhdenvertaisuuselimille, se voi olla hyödyllinen myös kansallisille ihmisoikeusinstituutioille (NHRI), oikeusasiamieslaitoksille tai muille sidosryhmille. Kun kansalliset ihmisoikeusinstituutiot ja oikeusasiamiehet käyttävät tätä arviointimenetelmää, termi ”tapauksen käsittelijä” voi viitata myös näiden instituutioiden tapauksia käsitteleviin työntekijöihin.

tahansa tämän arviointimenetelmän vaiheen aikana. Asiantuntija tarjoaa asiantuntevaa tukea, mutta ei ole pääasiallinen tapauksen käsittelijä.

Suuririskinen tekoälyjärjestelmä: Termillä viitataan tekoälyjärjestelmään, joka on määritelty tyhjentävästi tekoälyasetuksen 6 artiklassa. Myös termiä ”suuririskinen tekoäly” saatetaan käyttää.

Syöttötiedot: Kaikki algoritmijärjestelmälle syötetyt tiedot, signaalit ja raakadata, joiden perusteella järjestelmä tuottaa tuotoksensa. Esimerkiksi tekoälypohjainen syöpien seulontasovellus, jonka tarkoituksena on havaita epäilyttäviä luomia, voi käyttää syöttötietoina ikää, sukupuolta ja luomen kuvaa. Suurten kielimallien (LLM) järjestelmissä, kuten ChatGPT:ssä, syöte sisältää keskustelutyypin vuorovaikutuksen tekstin ja mahdollisesti myös aiempien vuorovaikutusten tekstit.

Markkinavalvontaviranomainen: kansallinen viranomainen tai kansalliset viranomaiset, jotka vastaavat asetuksen (EU) 2019/1020 (markkinavalvonta ja tuotteiden vaatimustenmukaisuus) mukaisista toimista ja tarvittavien toimenpiteiden toteuttamisesta.

Syrjimättömyys: termiä ”syrjimättömyys” käytetään termin ”yhdenvertaisuus” tai siihen liittyvien termien sijaan.

Syrjimättömyysdirektiivit: termillä viitataan liitteessä G lueteltuihin EU:n direktiiveihin.

Ilmoitettu laitos: Vaatimustenmukaisuuden arviointilaitos, joka tekee kolmannen osapuolen vaatimustenmukaisuusarvioita, mukaan lukien testejä, sertifiointeja ja tarkastuksia. Ilmoitettu laitos voi esimerkiksi arvioida suuririskisten tekoälyjärjestelmien vaatimustenmukaisuuden EU:n tekoälyasetuksessa säädettyjen vaatimustenmukaisuuden arviointimenettelyjen mukaisesti.

Ei-suuririskinen tekoälyjärjestelmä: Tekoälyjärjestelmä, joka ei sisällä tekoälyasetuksen suuririskisten tekoälyjärjestelmien tyhjentävään määritelmään. On kuitenkin huomioitava tämän tarkoittavan vain sitä, että näitä järjestelmiä ei luokitella tekoälyasetuksen mukaan suuririskisiksi järjestelmiksi. Se ei tarkoita, että nämä tekoälyjärjestelmät olisivat riskittömiä.

Tuotostiedot: Algoritmijärjestelmän tulokset syöttötietojen käsittelyn jälkeen. Esimerkiksi yksilön ennakoitu ominaisuus, pisteytys, suositus, päätös tai sisältö, kuten kuvat, video tai teksti.

Tarjoaja/käyttöönottaja: Näitä termejä käytetään tekoälyasetuksen 3 artiklan määritelmän mukaisesti. Vaikka nämä termit on määritelty tekoälyjärjestelmien kontekstissa, niitä voidaan soveltaa vastaavasti myös muihin kuin tekoälyjärjestelmiin.

Ehdot täyttävä ADM: tässä arviointimenetelmässä ehdot täyttävällä ADM:llä tarkoitetaan automaattisen päätöksenteon järjestelmien alaluokkaa, joka täyttää yleisen tietosuoja-asetuksen 22 artiklan mukaiset ”pelkästään” automaattista päätöksentekoa käyttävien järjestelmien kriteerit (asetus (EU) 2016/679). Tällaisiin järjestelmiin sovelletaan tiukempia avoimuus- ja tiedonantovelvoitteita yleisen tietosuoja-asetuksen mukaisesti.

Vastaaja: organisaatio tai yksikkö, jota yhdenvertaisuuselin tutkii laittoman syrjinnän vuoksi valituksen, viran puolesta tehtävän (*ex officio*) menettelyn tai markkinavalvontaviranomaisen tekemän ilmoituksen johdosta. Yleisen tietosuoja-asetuksen ja tekoälyasetuksen konteksteissa vastaajiin voidaan viitata termeillä ”rekisterinpitäjä” ja tekoälyn ”tarjoajat” tai ”käyttöönottajat” kyseisten asetusten määritelmien mukaisesti.

Katso EU:n tekoälyasetukseen liittyvä termistö [EU:n tekoälyasetuksen 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 kansalaisuutta ja tasa-arvoa käsittelevän komission (Commission for Citizenship and Gender Equality, CIG) kanssa.

Raportin ovat laatineet Louise Hooper (kansainvälinen konsultti, Euroopan neuvosto), Ylja Remmits ja Ioanna Papageorgiou (Algorithm Audit / kansainväliset konsultit, Euroopan neuvosto). Euroopan neuvosto haluaa kiittää hankkeeseen osallistuneita instituutioita ja Euroopan komissiota jatkuvasta sitoutumisesta raportin laatimisprosessin ajan sekä erityisesti seuraavia henkilöitä: Nele Roekens, Sophie Vincent, Thelma Raes ja Laetitia Parmentier (Unia, Belgia), Tiina Valonen ja Ville Rantala (YVV, Suomi), Carla Peixe, Lúcia Pestana ja Alexandra Andrade (CIG, Portugali), Massimiliano Santini (Euroopan komission uudistus- ja investointityöryhmä, pääsihteeristö) sekä Menno Ettema, Sara Haapalainen, Ayca Dibekoğlu ja Delfine Gaillard (Euroopan neuvoston osallisuutta ja syrjinnän torjuntaa käsittelevä osasto).

Erityiskiitokset Raphaële Xenidisille, Kris Shrishakille, Brent Mittelstadtille, Chris Russellille, Ydo Bergstralle ja Jurriaan Parielle osallistumisesta raportin tarkistukseen sekä Laurens Naudtsille ja Plixavra Vogiatzogloulle asiantuntijapanoksesta. Raportissa hyödynnettiin myös Brysselissä 15. huhtikuuta 2026 järjestettyyn monikansalliseen seminaariin ja työpajaan osallistuneiden yhdenvertaisuuselinten ja kansalaisjärjestöjen kansallisten asiantuntijoiden panosta. Heidän näkemyksensä rikastuttivat näiden suuntaviivojen analyttisiä ja toiminnallisia osia.



YHDENVERTAISUUSVALTUUTETTU
NON-DISCRIMINATION OMBUDSMAN



COMISSÃO PARA A CIDADANIA
E A IGUALDADE DE GÉNERO

Tiivistelmä

Algoritmijärjestelmät voivat sekä vahvistaa että luoda syrjintää, koska ne on usein suunniteltu erottamaan yksilöitä toisistaan. Ne voivat esimerkiksi luokitella henkilöitä, asettaa heitä paremmuusjärjestykseen tai kohdistaa heihin erilaisia toimia. Yhdessä historiallisten eriarvoisuuksien ja algoritmijärjestelmien dataan, sääntöihin ja suunnitteluvalintoihin sisältyvien inhimillisten vinoumien kanssa järjestelmien syrjivät kuviot voivat toistua ja laajentua, ellei niitä tunnisteta ja niiden riskejä lievennetä ennakoivasti.

Tämä arviointimenetelmä antaa vaiheittaiset ohjeet yhdenvertaisuuselimille ja muille ihmisoikeusjärjestöille Euroopassa tekoälyyn (AI) tai algoritmijärjestelmiin liittyvien syrjintätapausten arviointiin. Se on tarkoitettu näiden elinten tapausten käsittelijöille, neuvonantajille ja asianajajille, kun tutkitaan syrjintävaihteita, joihin liittyy tai joihin epäillään liittyvän tekoälyä tai automaattista päätöksentekoa (ADM). Tavoitteena on, että arviointimenetelmä toimisi huomiotavien ongelmien ja hyödynnettävien lähteiden viiteluettelona arvioinnin joka vaiheessa. Arviointimenetelmä on jaettu neljään iteratiiviseen vaiheeseen:

Vaihe 1: tekoälyyn tai algoritmeihin liittyvien tapausten tunnistaminen

Vaihe 2: tiedonkeruu tekoäly- tai algoritmijärjestelmästä syrjinnän tunnistamiseksi

Vaihe 3: vastaanotettujen tietojen arviointimenetelmä

Vaihe 4: oikeussuojakeinot.

Nämä vaiheet perustuvat tekoälyä koskevaan eurooppalaiseen sääntelykehykseen, erityisesti EU:n tekoälyasetukseen, ja syrjinnän vastaiseen lainsäädäntöön. Vaiheissa viitataan tarvittaessa myös muuhun lainsäädäntöön, kuten tietosuojaan, esimerkiksi tapauksiin ja oikeuskäytäntöön. Eri vaiheissa suuririskiset tekoälyjärjestelmät ja muut järjestelmät erotetaan toisistaan EU:n tekoälyasetuksen mukaisesti. Tekoälyasetuksen 77 artiklan mukaan erityisesti perusoikeuksia suojelevilla viranomaisilla on valtuudet pyytää ja saada käyttöönsä suuririskisten tekoälyjärjestelmien tekninen dokumentaatio ja data sekä testata tällaisia järjestelmiä, ja näitä keinoja käsitellään arviointimenetelmän vaiheissa.

Arviointimenetelmässä ei keskitytä kansalliseen lainsäädäntöön, ja joissakin maissa kansallinen lainsäädäntö voi tarjota tehokkaampia tutkintavaltuuksia tai täytäntöönpanokelpoisia keinoja algoritmiseen syrjintään liittyvien tietojen saamiseen. Tapausten käsittelijöiden on suositeltavaa huomioida nämä seikat käyttäessään tätä työkalua.

Neljän vaiheen soveltamisen tueksi arviointimenetelmä sisältää laajan luettelon liitteitä, jotka tarjoavat esimerkkejä tietojen pyytämisestä, tukevat algoritmisen syrjinnän riskien ymmärtämistä esimerkiksi tekoälyjärjestelmätyypin tai järjestelmän soveltamisalan mukaan ja auttavat tietojen arvioinnissa esimerkiksi tarjoamalla tarkistuslistan / täytettävän lomakkeen vaihetta 3 varten.

Jotta tämän arviointimenetelmän käyttö olisi helpompaa, on hyödyllistä ymmärtää tekoälyn ja algoritmisten vinoumien ja syrjinnän sekä niihin liittyvän terminologian

perusteet, ja työkalu tarjoaa myös termiluettelon käytön tueksi. Muut hankkeen ”Upholding Equality and Non-Discrimination by Equality Bodies regarding the Use of Artificial Intelligence in Public Administrations” osana laaditut julkaisut täydentävät tätä arviointimenetelmää ja voivat auttaa perusymmärryksen muodostamisessa.

- ▶ Oikeussuoja algoritmista syrjintää vastaan Euroopassa: nykyiset puitteet ja jäljellä olevat puutteet, joulukuu 2025 (saatavilla englannin lisäksi myös ranskaksi, hollanniksi, portugaliksi, suomeksi ja ruotsiksi).
- ▶ Tekoälyä ja algoritmiperusteista syrjintää koskevat eurooppalaiset suuntaviivat yhdenvertaisuuselimille ja muille kansallisille ihmisoikeustoimijoille, joulukuu 2025 (saatavilla englannin lisäksi myös ranskaksi, hollanniksi, portugaliksi, suomeksi ja ruotsiksi).

Johdanto

Uudet tekoälyä koskevat sääntelykehykset, kuten EU:n tekoälyasetus,² EU:n yhdenvertaisuuselinten normeja koskevat direktiivit (jäljempänä ”direktiivit yhdenvertaisuuselimistä koskevista normeista”)³ ja tekoälyä ja ihmisoikeuksia, demokratiaa ja oikeusvaltioperiaatetta koskeva Euroopan neuvoston puiteyleissopimus (jäljempänä ”Euroopan neuvoston tekoälyä koskeva puiteyleissopimus”), tarjoavat yhdenvertaisuuselimille ja ihmisoikeusjärjestöille uusia työkaluja ja valtuuksia algoritmisen syrjinnän tutkintaan.

Näihin työkaluihin liittyy tiettyjä rajoituksia ja haasteita. Esimerkiksi kaikkia syrjiviä algoritmijärjestelmiä ei välttämättä luokitella tekoälyksi EU:n tekoälyasetuksen mukaan.⁴ Lisäksi monet tekoälyyn ja syrjintään liittyvät lainsäädännön osa-alueet ovat vielä epäselviä. Tämä on myös monille lukijoille ja tapausten käsittelijöille uusi ja suhteellisen monimutkainen oikeudenala.

Näistä haasteista huolimatta tämä nelivaiheinen arviointimenetelmä pyrkii tarjoamaan rakenteen ja tukea algoritmijärjestelmän mahdollisesti tekemän tai sen avulla tehdyn päätöksen tai kohtelun syrjivien vaikutusten systemaattiseen analysointiin. Lukijoiden ei tule pitää arviointimenetelmän kaikkia vaiheita pakollisina tehtävinä. Sen sijaan vaiheet tarjoavat viitteellisiä ohjeita, jotka sisältävät erilaisia työkaluja järjestelmien tunnistamiseen, todisteiden keräämiseen ja arviointiin sekä tarvittavien toimien päättämiseen. Kun arviointimenetelmän vaiheita noudatetaan ja tarvittaessa haetaan (teknistä) asiantuntija-apua, käytettävissä on välineitä, joilla voidaan osoittaa syrjintäoletta ja hakea oikeussuojakeinoja, jos algoritmista syrjintää esiintyy.

Yhdenvertaisuuselinten on suhtauduttava tekoälyyn ja automaattiseen päätöksentekoon liittyviin syrjintäväitteisiin samalla tavalla kuin mihin tahansa muuhun syrjintätapaukseen, mutta myös tunnistettava, että algoritmijärjestelmien toiminnan avoimuuden puute tai epävarmuus on tarvittaessa huomioitava syrjinnän riskien arvioinnissa ja *prima facie* -tapauksen osoituksessa. Tämä johtuu siitä, että ymmärretään

-
2. Euroopan parlamentin ja neuvoston asetus (EU) 2024/1689, annettu 13 päivänä kesäkuuta 2024, tekoälyä koskevista yhdenmukaistetuista säännöistä ja asetusten (EY) N:o 300/2008, (EU) N:o 167/2013, (EU) N:o 168/2013, (EU) 2018/858, (EU) 2018/1139 ja (EU) 2019/2144 sekä direktiivien 2014/90/EU, (EU) 2016/797 ja (EU) 2020/1828 muuttamisesta (tekoälysäädös).
 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.
 4. Tiettyt esimerkit algoritmista syrjinnästä perustuvat yksinkertaisiin sääntöpohjaisiin järjestelmiin, joita ei luokitella tekoälyksi. Esimerkkejä tästä ovat alankomaalaiset syrjivien algoritmien tapaukset lastenhoidon tukia koskevassa skandaalissa (Amnesty International, 2021) ja Alankomaiden koulutuksen toimeenpanoviraston käyttämässä petosriskien pisteytysmallissa (Rechtbank Overijssel, 2024).

paremmin tekoälyjärjestelmiä valmistavien yritysten, niiden käyttöönottajien sekä henkilöiden, joihin järjestelmiä käytetään, välinen vallan ja tiedon epätasapaino.⁵ Näissä olosuhteissa todistustaakka voi siirtyä vastaajalle, jonka on osoitettava, että algoritmijärjestelmä ei ole syrjinyt henkilöä tai vaikuttanut syrjintään laittomalla tavalla. Avoimuutta on lisättävä, jotta voidaan tehostaa niiden henkilöiden oikeus-suojaa, joihin järjestelmien vaikutukset kohdistuvat.

Euroopan parlamentti hyväksyi tekoälyä koskevan digitaalialan koontiasetuksen,⁶ jolla pyritään selkeyttämään ja yksinkertaistamaan tiettyjä tekoälyä koskevia sääntöjä. Näihin muutoksiin viitataan tarvittaessa.

Uuden oikeudellisen kehyksen tärkeimmät elementit

Direktiivit yhdenvertaisuuseliimiä koskevista normeista

Yhdenvertaisuuselinten normeja koskevissa direktiiveissä, jotka oli saatettava osaksi kansallista lainsäädäntöä 19. kesäkuuta 2026 mennessä (direktiivit yhdenvertaisuus-eliimiä koskevista normeista, 24 artikla), kuvataan yhdenvertaisuuselinten toimintaa koskevat vähimmäisvaatimukset niiden tehokkuuden parantamiseksi ja riippumattomuuden takaamiseksi. Näitä valtuuksia on tulkittava rinnakkain EU:n syrjimättömyysdirektiiveissä säädettyjen olemassa olevien valtuuksien kanssa.

Direktiivin 2024/1500 johdanto-osan kappaleessa 21 ja direktiivin 2024/1499 johdanto-osan kappaleessa 22 todetaan taloudellisten resurssien kohdentamisesta seuraavaa:

On tärkeää kiinnittää huomiota automatisoitujen järjestelmien, kuten tekoälyn, käytön tarjoamiin mahdollisuuksiin ja riskeihin. Tasa-arvoelimillä olisi erityisesti oltava käytettävissään sopivat henkilöstö- ja tekniset resurssit. Kyseisten resurssien olisi etenkin mahdollistettava se, että tasa-arvoelimet sekä käyttävät automatisoituja järjestelmiä työssään että arvioivat kyseisten järjestelmien syrjimättömyysääntöjen mukaisuutta. Jos tasa-arvoelin on osa elintä, jolla on useita tehtäviä, sen tasa-arvotehtävän hoitamiseen tarvittavat resurssit olisi varmistettava.⁷

5. Tätä käsitellään tarkemmin alakohdassa 3.8.

6. Euroopan parlamentin ja neuvoston asetus (EU) 2026/1744, annettu 8 päivänä heinäkuuta 2026, asetusten (EU) 2024/1689, (EU) 2018/1139 ja (EU) 2023/1230 muuttamisesta tekoälyä koskevien yhdenmukaistettujen sääntöjen täytäntöönpanon yksinkertaistamiseksi (tekoälyä koskeva digitaalialan koontiasetus). Saatavilla osoitteessa <https://eur-lex.europa.eu/eli/reg/2026/1744/oj/eng> (viitattu 24. heinäkuuta 2026).

7. Lisäksi tekoälyä koskevan puiteyleissopimuksen 26 artikla edellyttää, että yhdenvertaisuuselimet ovat tehokkaita, puolueettomia ja riippumattomia ja että niillä on tarvittavat valtuudet, asiantuntemus ja resurssit.

EU:n tekoälyasetus, 77 artikla: perusoikeuksia suojelevien viranomaisten valtuudet ja yhteistyö markkinavalvontaviranomaisten kanssa

Yhdenvertaisuuselimille ja kansallisille ihmisoikeusinstituutioille annetaan uusia valtuuksia, jotta ne voivat vastata tekoälyasetuksen 77 artiklan⁸ mukaisiin suuririskisiä tekoälyjärjestelmiä koskeviin vaatimuksiin ja hoitaa tehtävänsä.⁹ Tekoälyä koskevassa digitaalialan koontiasetuksessa selvennetään, että nämä valtuudet eivät rajoita elinten olemassa olevia valtuuksia ja riippumattomuutta.¹⁰

Perusoikeuksia suojelevien viranomaisten luettelo oli määrä ilmoittaa komissiolle ja muille jäsenvaltioille 2. marraskuuta 2024 mennessä, ja jäsenvaltioiden ”on pidettävä [viranomaisten] luettelo ajan tasalla”.¹¹ Komissio tunnustaa, että ”77 artiklan mukaisten elinten” luetteloa päivitetään jatkuvasti tekoälyasetuksen täytäntöönpanon ollessa kesken.¹² Täten luetteloon voidaan myöhemmin lisätä yhdenvertaisuuselimet, joita jäsenvaltiot eivät ilmoittaneet ensimmäiseen määräaikaan mennessä. Luettelosta voidaan myös poistaa yhdenvertaisuuselimä.

Asianmukaisilla viranomaisilla on 77 artiklan 1 kohdan mukaan valtuudet pyytää ja saada käyttöönsä tekoälyasetuksen nojalla luotu tai ylläpidetty dokumentaatio ymmärrettävällä kielellä ja saavutettavassa muodossa, kun dokumentaation käyttö on tarpeen, jotta viranomaiset voisivat suorittaa tehokkaasti tehtävänsä omalla lainkäyttöalueellaan. Tämän tulisi tarkoittaa, että pyyntöjä voidaan esittää muiden kansallisten toimivaltaisten viranomaisten, mukaan lukien markkinavalvontaviranomaisten ja ilmoitettujen laitosten, sekä tarjoajien, käyttöönottajien tai muiden tekoälyjärjestelmän elinkaaren toimijoiden luomasta tai ylläpitämästä dokumentaatiosta. Tekoälyä koskevassa digitaalialan koontiasetuksessa selvennetään, että tietoon ja dokumentaatioon tutustumista koskevat pyynnöt olisi esitettävä toimivaltaiselle markkinavalvontaviranomaiselle, jonka ”on tarvittaessa ja ilman aiheetonta viivytystä myönnettävä... pääsy tällaiseen tietoon tai dokumentaatioon, myös pyytämällä

8. Tekoälyasetuksen 77 artiklan 1 kohta, mukaan lukien koontiasetuksen muutokset: ”Kansallisilla viranomaisilla tai elimillä, jotka valvovat perusoikeuksien, mukaan lukien oikeus syrjimättömyyteen, suojelua koskevan unionin oikeuden mukaisten velvoitteiden noudattamista tai panevat niitä täytäntöön, on oltava valtuudet esittää pyyntö saada ja saada käyttöönsä sellainen mikä tahansa luotu tai ylläpidetty tieto tai dokumentaatio asiaankuulavalta markkinavalvontaviranomaiselta tämän asetuksen nojalla ymmärrettävällä kielellä ja koneluettavassa muodossa sähköisesti, kun tiedon tai dokumentaation käyttö on tarpeen, jotta ne voisivat hoitaa tehokkaasti toimeksiantonsa omalla lainkäyttöalueellaan. Tällä artiklalla ei rajoiteta asianomaisten kansallisten viranomaisten tai elinten toimeksiantojen piiriin kuuluvaa toimivaltaa, tehtäviä, valtuuksia ja riippumattomuutta.”

9. Monet yhdenvertaisuuselimet sisältyvät 77 artiklan määritelmään, mutta eivät kaikki. Termiä ”77 artiklan mukainen viranomainen” käytetään tässä asiakirjassa tarkoittamaan yhdenvertaisuuselimä ja kansallisia ihmisoikeusinstituutioita, jotka vastaavat tekoälyasetuksen 77 artiklan määritelmää.

10. Euroopan parlamentin ja neuvoston asetukset (EU) 2026/1744, annettu 8 päivänä heinäkuuta 2026, asetusten (EU) 2024/1689, (EU) 2018/1139 ja (EU) 2023/1230 muuttamisesta tekoälyä koskevien yhdenmukaistettujen sääntöjen täytäntöönpanon yksinkertaistamiseksi (tekoälyä koskeva digitaalialan koontiasetus). Saatavilla osoitteessa <https://eur-lex.europa.eu/eli/reg/2026/1744/oj/eng>, (viitattu 24. heinäkuuta 2026).

11. Tekoälyasetus, 77 artiklan 2 kohta.

12. <https://digital-strategy.ec.europa.eu/en/policies/fundamental-rights-protection-authorities-ai-act>, viitattu 5. kesäkuuta 2026.

tällaista tietoa tai dokumentaatiota tarjoajalta tai käyttöönottajalta”¹³, ja että viranomaisten tai elinten ”on tehtävä tiivistä yhteistyötä ja annettava toisilleen keskinäistä apua, joka on tarpeen niiden toimeksiantojen hoitamiseksi”.¹⁴ Tähän yhteistyöhön ja avunantoon on sisällyttävä tiedonvälitys, kun se on tarpeellista tekoälyasetuksen ja muun unionin lainsäädännön, mukaan lukien syrjimättömyysdirektiivien (katso liite G), tehokasta valvontaa tai täytäntöönpanoa varten.

Jos dokumentaatio ei riitä sen selvittämiseen, onko perusoikeuksia suojaavan unionin oikeuden mukaisia velvoitteita rikottu, yhdenvertaisuuselin voi esittää markkina-
valvontaviranomaiselle perustellun pyynnön järjestää suuririskisen tekoälyjärjestelmän testaus teknisin keinoin (EU:n tekoälyasetus, 77 artiklan 3 kohta; [katso vaihe 4](#)).

Kaikkea saatua dataa tai dokumentaatiota on käsiteltävä 78 artiklan mukaisten luottamuksellisuusvaatimusten mukaisesti. 78 artiklan 2 kohdan mukaan 77 artiklan mukaisen viranomaisen on pyydettävä ainoastaan dataa, joka on ehdottoman välttämätöntä tekoälyjärjestelmien aiheuttaman riskin arvioimiseksi ja valtuuksien käyttämiseksi tämän asetuksen ja unionin lainsäädännön mukaisesti. Tekoälyasetuksen mukaan tehtyjen pyyntöjen tulee siksi olla selkeitä ja rajattuja, jotta niiden hylkäykset voidaan välttää.

Kun tietoja pyydetään ja hankitaan, yhdenvertaisuuselimen on varmistettava, että käytössä ovat riittävät ja tehokkaat kyberturvallisuustoimenpiteet saatujen tietojen ja datan turvallisuuden ja luottamuksellisuuden suojaamiseksi. Yhdenvertaisuuselimen on poistettava tällaiset tiedot sovellettavan unionin tai kansallisen lainsäädännön mukaisesti heti, kun niitä ei enää tarvita siihen tarkoitukseen, jota varten ne hankittiin.

Vastaavasti Euroopan neuvoston antamissa ohjeissa, kuten tekoälyä koskevassa puiteyleissopimuksessa ja [yhdenvertaisuutta ja tekoälyä koskevassa suosituksessa CM/Rec\(2026\)1](#), kuvataan toimenpiteitä, joilla jäsenvaltiot ja muut sidosryhmät voivat edistää yhdenvertaisuutta sekä ehkäistä ja torjua syrjintää kaikissa tekoälyjärjestelmien elinkaaren vaiheissa.

Luottamuksellisuus

Tekoälyasetuksen 78 artiklan 1 kohdassa on esitetty luottamuksellisuusvaatimukset, joiden mukaan Euroopan komission, markkina-
valvontaviranomaisten ja ilmoitettujen laitosten (70 artikla) sekä muiden tekoälyasetuksen soveltamiseen osallistuvien luonnollisten ja oikeushenkilöiden on varmistettava saamiensa tietojen ja datan luottamuksellisuus siten, että suojellaan erityisesti seuraavia:

- Teollis- ja tekijänoikeuksia ja luonnollisen henkilön tai oikeushenkilön luottamuksellisia liiketoimintatietoja tai liikesalaisuuksia, lähdekoodi mukaan lukien

13. Euroopan parlamentin ja neuvoston asetukset (EU) 2026/1744, annettu 8 päivänä heinäkuuta 2026, asetusten (EU) 2024/1689, (EU) 2018/1139 ja (EU) 2023/1230 muuttamisesta tekoälyä koskevien yhdenmukaistettujen sääntöjen täytäntöönpanon yksinkertaistamiseksi (tekoälyä koskeva digitaalialan koontiasetus). Saatavilla osoitteessa <https://eur-lex.europa.eu/eli/reg/2026/1744/oj/eng>, (viitattu 24. heinäkuuta 2026).

14. Ibid.

(direktiivi (EU) 2016/943, 5 artikla). Yhdenvertaisuuselinten kannalta merkityksellisessä direktiivin 2016/943 5 artiklassa säädetään poikkeuksesta, joka koskee väärinkäytöksen taikka väärän tai laittoman toiminnan paljastamista, edellyttäen, että vastaaja (yhdenvertaisuuselin tai mahdollisesti markkina-valvontaviranomainen) toimii tarkoituksenaan suojata yleistä etua (5 artiklan b alakohta) tai unionin oikeudessa tai kansallisessa laissa tunnustettua oikeutettua etua (5 artiklan d alakohta). Perusoikeuksien suojeleminen ja syrjinnän ehkäiseminen tai siihen puuttuminen sisältyvät molemmat, ainakin oletettavasti, tähän poikkeukseen.

- ▶ Asetuksen tehokasta täytäntöönpanoa, etenkin tarkastuksia, tutkimuksia ja auditointeja varten.
- ▶ Yleisiä ja kansallisia turvallisuusetuja.
- ▶ Rikosoikeudellisten tai hallinnollisten menettelyjen toteuttamista.
- ▶ Unionin tai kansallisen lainsäädännön nojalla turvallisuusluokiteltuja tietoja.

Tällä hetkellä on epäselvää, miten nämä voivat vaikuttaa yhdenvertaisuuselinten mahdollisuuksiin saada tietoja asianmukaisilta osapuolilta. Jos tietojen luovuttamisesta kieltäydytään luottamuksellisuuteen vedoten, yhdenvertaisuuselimellä voi kuitenkin olla mahdollisuus kääntyä EU:n tekoälyasetuksen mukaisen toimivaltaisen viranomaisen tai yleisen tietosuojasetuksen mukaisen tietosuojaviranomaisen puoleen. Jos liikesalaisuudet mainitaan salassapitoperusteena, toimivaltaisen valvontaviranomaisen tai tuomioistuimen on todennäköisesti punnittava kyseessä olevia oikeuksia ja etuja sen määrittämiseksi, mitä tietoja on annettava (katso *CK v. Dun & Bradstreet Austria GmbH* ja *Magistrat der Stadt Wien* (2025), kuvattu [vaiheessa 2.1](#)).

Eri sektoreiden välinen yhteistyö

Jotta uusi oikeudellinen kehys olisi mahdollisimman tehokas, on myös pyydettävä, kehitettävä, vahvistettava ja virallistettava yhteistyötä asiaankuuluvien markkina-valvontaviranomaisten, tietosuojaviranomaisten ja muiden 77 artiklan mukaisten viranomaisten kanssa, jos tällaista yhteistyötä ei vielä tehdä. Tämä yhteistyövaatimus on määrätty 77 artiklan 1 kohdan b alakohdan muutoksessa, joka on kuvattu tekoälyä koskevassa digitaalialan koontiasetuksessa.¹⁵ Tätä vaatimusta varten voi olla tarpeen tai hyödyllistä kehittää eri viranomaisten välisiä yhteistyökäytäntöjä.¹⁶ Esimerkkejä ja hyviä käytäntöjä on jäljempänä tekstiruudussa. Uusien yhdenvertaisuuselinten normeja koskevien direktiivien mukaan jäsenvaltioiden on tarjottava kansallinen kehys, jonka avulla yhdenvertaisuuselimet voivat toteuttaa tutkintatoimenpiteitä, ja siinä on myös säädettävä mekanismeista, joiden avulla yhdenvertaisuuselimet

15. Euroopan parlamentin ja neuvoston asetus (EU) 2026/1744, annettu 8 päivänä heinäkuuta 2026, asetusten (EU) 2024/1689, (EU) 2018/1139 ja (EU) 2023/1230 muuttamisesta tekoälyä koskevien yhdenmukaistettujen sääntöjen täytäntöönpanon yksinkertaistamiseksi (tekoälyä koskeva digitaalialan koontiasetus). Saatavilla osoitteessa <https://eur-lex.europa.eu/eli/reg/2026/1744/oj/eng>, (viitattu 24. heinäkuuta 2026).

16. Katso myös Euroopan neuvoston tekoälyä koskevan puiteyleissopimuksen (2024) 26 artikla, jonka mukaan ”tehokasta yhteistyötä [instituutioiden] välillä” on helpotettava, ja yhdenvertaisuuselinten normeja koskevien direktiivien 14 artikla, jossa edellytetään asianmukaisia yhteistyömekanismeja.

voivat tehdä yhteistyötä asianomaisten viranomaisten kanssa kyseistä tarkoitusta varten (direktiivit yhdenvertaisuuselimistä koskevista normeista, 8 artikla).

Tässä suhteessa keskeisessä roolissa ovat yhdenvertaisuuselinten ja niiden jäsenvaltioiden hallitusten väliset neuvottelut, joilla varmistetaan selkeä oikeusperusta tiedonvälitykselle erilaisten 77 artiklan mukaisten elinten, mukaan lukien yhdenvertaisuuselinten ja tietosuojaviranomaisten, sekä markkinavalvontaviranomaisten ja 77 artiklan mukaisten elinten välillä tekoälyasetuksen 73 artiklan 7 kohdan ja 79 artiklan 2 kohdan mukaisen yhteistyön mukaisesti (Autoriteit Persoonsgegevens 2024, 37 kohta). Tällaisten oikeusperustojen olemassaolo on edellytys tietojen jakamista koskevien kahden- ja monenvälisen yhteistyösopimusten solmimiselle. Tällaisten sopimusten tulee olla laaja-alaisia, jotta ne kattavat 77 artiklan mukaisten elinten ja markkinavalvontaviranomaisten toimeksiannon ja mahdollistavat tarvittaessa ylimääräisten tapauskohtaisten kahdenvälisen sopimusten tekemisen (Autoriteit Persoonsgegevens 2024, 37 kohta).

Esimerkkejä ja hyviä käytäntöjä

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 tiedeminstisteriö (Department of Science, Technology and Innovation, 2024).

Norjassa yhdenvertaisuuselin on tehnyt yhteistyötä tietosuojaviranomaisen kanssa osana tekoälyn sääntelyn testiympäristöä (Norwegian Data Protection Authority, 2023).

Ranskassa Defender of Rights -yhdenvertaisuuselimen ja CNIL-tietosuojaviranomaisen (Commission Nationale de l'Informatique et des Libertés) välistä yhteistyötä helpottavat useat mekanismit: osapuolet ovat laatineet yhteisymmärryspöytäkirjana tehdyn sopimuksen, ja Defender of Rights toimii myös CNIL:n hallituksen neuvonantajana. Tämän rakenteellisen yhteyden ansiosta Defender of Rightsille ilmoitetaan kaikista CNIL:n hallituksen kokousten vastaanottamista tapauksista (Euroopan neuvosto, 2025b).

Yhdistyneessä kuningaskunnassa tietosuojaviranomaisen (Information Commissioner's Office) ja yhdenvertaisuutta ja ihmisoikeuksia käsittelevän komission (Equality and Human Rights Commission) välisessä yhteisymmärryspöytäkirjassa on määritelty tiedonjaon ja yhteistyön periaatteet, tiedonjaon oikeusperustat, tiedonhallintaan ja -käsittelyyn liittyvät käytännön yksityiskohdat sekä kunkin elimen roolit, tehtävät ja valtuudet. Katso: yhteisymmärryspöytäkirja

Tekoälyasetuksen mukaiset riskiluokat

EU:n tekoälyasetuksen sääntelykehyksen mukaan tekoälyjärjestelmät voidaan luokitella sen perusteella, millaisen riskitason ne oletettavasti aiheuttavat perusoikeuksille, terveydelle ja turvallisuudelle (tekoälyasetus, 1 artikla). Tämä lähestymistapa vastaa ajatusta, että kaikkien tekoälyjärjestelmien riskit eivät ole samantasoisia: tietyt järjestelmät aiheuttavat riskejä, joita ei voida hyväksyä, ja ne on kiellettävä kokonaan, toiset aiheuttavat merkittäviä riskejä, jotka vaativat tiukkaa valvontaa, kun taas toisten ei katsota tarvitsevan tekoälyyn liittyvää sääntelyä lainkaan.

Riskiluokka määrittää sovellettavat velvoitteet – ne vaihtelevat ehdottomasta kiellosta kattaviin teknisiin vaatimuksiin ja tavanomaisiin avoimuusvelvoitteisiin. Yhdenvertaisuuselimille tällä riskiperusteisella rakenteella on suora merkitys: se määrittää, mitä tietoja ja dokumentaatiota tulee olla olemassa, ja vaikuttaa tekoälyasetuksen mukaisiin käytettävissä oleviin oikeussuojakeinoihin.

Kielletyt tekoälykäytännöt

EU:n tekoälyasetus kieltää tietyt tekoälyyn liittyvät käytännöt, jotka aiheuttavat kohtuuttomia riskejä perusoikeuksille, turvallisuudelle tai demokraattisille arvoille (tekoälyasetus, 5 artikla). Näitä ovat esimerkiksi seuraavat:

- ▶ tarkoituksellisesti manipuloivat tekniikat, jotka vääristävät olennaisesti henkilön käyttäytymistä, mukaan lukien ilman suostumusta tuotettu seksuaalinen tai intiimi sisältö tai lasten hyväksikäyttöä sisältävä materiaali
- ▶ haavoittuvuuksien hyödyntäminen
- ▶ sosiaaliset pisteytysjärjestelmät
- ▶ luonnollisten henkilöiden riskinarvioinnit, jotta voidaan arvioida tai ennustaa profiloinnin perusteella sen riskiä, että luonnollinen henkilö syyllistyy rikokseen
- ▶ reaaliaikainen biometrinen etätunnistus julkisissa tiloissa (rajoitettuja poikkeuksia lukuun ottamatta)
- ▶ tunteentunnistus työpaikka-/koulutusympäristöissä
- ▶ biometrinen luokittelu, jossa luonnolliset henkilöt luokitellaan kielletyn syrjintäperusteen perusteella
- ▶ kasvokuvien kohdentamaton haravointi.

Katso myös [liite J – Kielletyt tekoälyyn liittyvät käytännöt](#).

Suuririskiset tekoälyjärjestelmät

Suuririskisiin tekoälyjärjestelmiin kuuluvat käyttötapaukset, joiden katsotaan aiheuttavan merkittäviä riskejä terveydelle, turvallisuudelle tai perusoikeuksille, sekä tekoälyasetuksen liitteen III (6 artikla) mukaisilla aloilla käytettävät järjestelmät. Näihin kuuluvat järjestelmät, joita käytetään esimerkiksi seuraaviin:

- ▶ biometriikka
- ▶ kriittisen infrastruktuurin hallinta
- ▶ yleissivistävä ja ammatillinen koulutus

- työllistäminen ja henkilöstöhallinto
- välttämättömien palvelujen ja etuuksien saatavuus ja käyttö
- lainvalvonta
- muuttoliikkeen hallinta, turvapaikka-asiat ja rajavalvonta
- oikeudenhoito.

Huomautus: liitteessä III tarkoitettua tekoälyjärjestelmää pidetään aina suuririskisenä, jos tekoälyjärjestelmä profiloi luonnollisia henkilöitä.

Katso myös [liite I – Suuririskiset tekoälyyn liittyvät käytännöt](#).

Jos tekoälyjärjestelmällä on tarkoitus tehdä jotakin seuraavista, järjestelmää ei pidetä suuririskisenä (6 artiklan 3 kohta):

- suppea menettelyllinen tehtävä
- parantaa aiemmin suoritettun ihmisen toiminnan tulosta
- havaita päätöksentekotapoja tai poikkeamia aiemmista päätöksentekotavoista
- valmistelutehtävä, joka koskee käyttötapausten kannalta merkityksellistä arviointia.

Suuririskisiin tekoälyjärjestelmiin sovelletaan tekoälyasetuksen mukaisesti laajoja dokumentointivaatimuksia, avoimuusveloitteita ja riskinhallintamenettelyjä.

Yleiskäyttöinen tekoäly (GPAI)

Suuririskisten ja kiellettyjen käytäntöjen luokat kattavat tietyt käyttötapaukset, ja luokittelu perustuu järjestelmien nimenomaiseen tarkoitukseen. Sitä vastoin yleiskäyttöiset tekoälymallit, kuten suuriin kielimalleihin (LLM) perustuvat järjestelmät, pystyvät suorittamaan monenlaisia erillisiä tehtäviä, ja ne voidaan integroida erilaisiin ketjun loppupään järjestelmiin tai sovelluksiin (tekoälyasetus, 3 artiklan 63 kohta). Yleiskäyttöisellä tekoälyllä ei nimensä mukaisesti ole tiettyä tarkoitusta. Yleiskäyttöinen tekoälymalli voi kuitenkin toimia perustana käyttösovelluksille, joilla on tiettyjä tarkoituksia ja jotka voivat kuulua suuririskisten järjestelmien luokkaan.

Yleiskäyttöisen tekoälyn velvoitteiden mukaan laadittu dokumentaatio ei todennäköisesti ole yhdenvertaisuuselinten saatavilla tekoälyasetuksen mukaan, koska käyttöoikeudet rajoittuvat suuririskisten tekoälyjärjestelmien käyttösovelluksiin (tekoälyasetus, 77 artikla). Yhdenvertaisuuselimet voivat vedota olemassa oleviin valtuuksiinsa ja kansalliseen lainsäädäntöön, mutta useimmissa tapauksissa on erittäin todennäköistä, että tietojen saantiin tarvitaan tuomioistuimen määräys. Yleiskäyttöiset tekoälymallit kuuluvat tässä arviointimenetelmässä yleisesti algoritmijärjestelmien luokkaan.

Miten riskiluokkia sovelletaan arviointimenetelmässä?

Kuten edellä on kuvattu, EU:n tekoälyasetus tarjoaa uusia valtuuksia saada tietoja suuririskisistä järjestelmistä. Arviointimenetelmä on siksi jäsennelty ensisijaisesti suuririskisten tekoälyjärjestelmien ja muiden algoritmijärjestelmien välisten erojen mukaisesti. Ei-suuririskisten tekoälyjärjestelmien tapauksissa yhdenvertaisuuselinten

odotetaan toimivan muihin algoritmijärjestelmiin sovellettavan tietokehyksen mukaan. Arviointimenetelmän vaihe 1 auttaa tapausten käsittelijöitä ymmärtämään, millainen järjestelmä on kyseessä.

Tekoälyasetus asettaa ylimääräisiä sääntelyvaatimuksia toimijoille, jotka osallistuvat suuririskisten tekoälyjärjestelmien kehittämiseen, jakeluun ja käyttöönottoon. Kun kyseessä ovat tällaiset järjestelmät, tämä tarjoaa merkittäviä ja asiaankuuluvia tietoja riskinhallintatoimenpiteistä, käytetystä datasta ja käytössä olevista datanhallintakäytännöistä, keskeiset rakenteelliset valinnat, datavalinnat ja järjestelmän käyttötarkoitukset selittävän teknisen dokumentaation sekä tietoa testauksesta, valvonnasta ja tunnistetuista syrjintäriskeistä. Tämä dokumentaatio on tärkeä resurssi yhdenvertaisuuselimille, jotka pyrkivät tunnistamaan tai arvioimaan mahdollisia algoritmiseen syrjintään liittyviä tapauksia.

Tällaisia tietoja ei ole saatavilla kaikissa tai edes useimmissa tapauksissa. Nämä vaatimukset auttavat kuitenkin yhdenvertaisuuselimiä tunnistamaan ja tulkitsemaan tekoälyyn ja muihin algoritmijärjestelmiin liittyvää näyttöä myös silloin, kun tällaisia muodollisia vaatimuksia ei ole. Tämä johtuu siitä, että ne toimivat viitteellisinä vaiheina syrjintäriskien tunnistamisessa, lieventämisessä tai poistamisessa, ja dokumentaatio on usein osa vakiomallista ohjelmistoa / teknistä kehitystä.

Arviointimenetelmässä pyritään erottamaan toisistaan tapaukset, joissa yhdenvertaisuuselimelle on EU:n tekoälyasetuksen 77 artiklan nojalla annettu valtuudet pyytää ja tarkastella suuririskisten järjestelmien tekoälyasetuksen mukaan luotua tai ylläpidettyä dokumentaatiota, ja tapaukset, joissa tällaisia valtuuksia ei ole.

On tärkeää muistaa, että kansalliset oikeudelliset kehykset tarjoavat usein yhdenvertaisuuselimille tiedonkeruu- tai tutkintavaltuuksia. Yhdenvertaisuuselimillä, jotka eivät ole 77 artiklan mukaisia viranomaisia, ei ole tekoälyasetuksen mukaista suoraa oikeusperustaa saada suuririskisten tekoälyjärjestelmien sovellettavaa dokumentaatiota, mutta ne voivat silti hyödyntää näitä kansallisen ja muun unionin lainsäädännön mukaisia valtuuksia.

Kielletyt syrjintäperusteet

Kielletyt syrjintäperusteet mainitaan tämän arviointimenetelmän eri osissa. Ne ovat ominaisuuksia, jotka on kielletty Euroopan ihmisoikeussopimuksen (”ihmisoikeussopimus”) ja EU:n direktiivien perusteella.

Euroopan ihmisoikeustuomioistuin on laatinut [Euroopan ihmisoikeussopimuksen 14 artiklaa ja kahdennentoista pöytäkirjan 1 artiklaa käsittelevän oppaan](#) (Guide on Article 14 of the European Convention on Human Rights and on Article 1 of Protocol No. 12 to the Convention).

Taulukko 1. Unionin lainsäädännön mukaiset kielletyt syrjäntäperusteet

Merkintä X taulukossa tarkoittaa, että ominaisuus sisältyy kyseiseen sopimukseen tai direktiiviin. Tyhjä solu tarkoittaa, että ominaisuus ei sisälly sopimukseen tai direktiiviin.

	Euroopan ihmis-oikeussopimuksen 14 artikla	Euroopan unionin perusoikeuskirja	EU:n syrjimättömyys-direktiivit
Sukupuoli	X	X	X (2004/113/EY, 2000/78/EY, 2006/54/EY, 2023/970/EU, 2010/41/EU)
Rotu ¹⁷	X	X	X (2000/43/EY)
Ihonväri	X	X	
Kieli	X	X	
Uskonto	X	X (tai vakaumus)	X (2000/78/EY)
Poliittinen tai muu mielipide	X	X	X (2000/78/EY)
Kansallinen tai yhteiskunnallinen alkuperä	X	X (etninen tai yhteiskunnallinen alkuperä)	
Kansalliseen vähemmistöön kuuluminen	X	X	
Varallisuus	X	X	
Syntyperä	X	X	
Muu asema	X		
Vammaisuus	Muu asema	X	X (2000/78/EY)
Ikä	Muu asema	X	X (2000/78/EY)
Sukupuolinen suuntautuminen	Muu asema	X	X (2000/78/EY)
Kansalaisuus	Muu asema	X (perus-sopimusten soveltamisalalla)	
Geneettiset ominaisuudet	Muu asema	X	
Siviilisäät	Muu asema		
Maahanmuuttaja-tai pakolaisasema	Muu asema		

17 Koska kaikki ihmiset kuuluvat samaan lajiin, Euroopan neuvoston ministerikomitea hylkää teorial, jotka perustuvat eri "rotujen" olemassaoloon. Termiä "rotu" käytetään kuitenkin tässä asiakirjassa sen varmistamiseksi, etteivät henkilöt, joita yleisesti ja virheellisesti pidetään "toiseen rotuun kuuluvina", jää lainsäädännön tarjoaman suojan ja politiikan täytäntöönpanon ulkopuolelle.



Arviointimenetelmän käyttö

Arviointimenetelmässä käytetään nelivaiheista lähestymistapaa (katso myös alta kuva 1).

Vaihe 1: tekoölyyn tai algoritmeihin liittyvien tapausten tunnistaminen

Vaihe 2: tiedonkeruu tekoöly- tai algoritmijärjestelmästä syrjinnän tunnistamiseksi

Vaihe 3: vastaanotettujen tietojen arviointimenetelmä

Vaihe 4: oikeussuojakeinot

Arviointimenetelmässä erotellaan tarvittaessa tapausten eri lähteet toisistaan:

- A. valitus (yksilön tai ryhmän tekemä)
- B. viran puolesta (*ex officio*) tehtävä tutkinta
- C. markkinaoikeuden viranomaisen antamat tiedot.

Huomautus: vaiheet esitetään peräkkäin arviointimenetelmän rakenteellisen selkeyden vuoksi. Ne eivät ole käytännössä selkeästi peräkkäisiä, vaan usein sirkulaarisia ja iteratiivisia.

Vaihe 1

Ensimmäinen ilmoitus tai tieto syrjintätapauksesta, johon algoritmijärjestelmien voidaan havaita liittyvän.

Keskeiset kysymykset:

- Onko tapauksessa kyse tekoölyasetuksen mukaisesta suuririskisestä tekoölyjärjestelmästä?
- Onko tapauksessa kyse algoritmijärjestelmästä?

Vaihe 2

Seuraava vaihe on etsiä tietoa tunnistetusta järjestelmästä. Tämä voi tukea syrjinnän myöhempää tunnistamista. Vaiheessa 2 esitetään ne asiaankuuluvat tiedot, asiakirjat ja muut todisteet, jotka voivat olla yhdenvertaisuuselinten ja niiden mahdollisten lähteiden saatavilla tai käytettävissä.

Huomautus: Tässä vaiheessa tunnistetut tiedot analysoidaan tarkemmin vaiheessa 3. Näin ollen vaiheita 2 ja 3 tulisi tarkastella yhdessä. Vastaavasti oikeussuojakeinoja tapauksiin, joissa tietoa puuttuu mutta niiden hankkimiseen on lain mukaan valtuudet, käsitellään vaiheessa 4.

Keskeinen kysymys:

- Mitä tietoja on saatavilla ja kuinka ne voidaan saada?

Vaihe 3

Asiaankuuluvan näytön täydellinen analyysi tehdään käyttämällä apuna ehdotettuja kysymyksiä. Nämä kysymykset eivät ole tyhjentäviä.

Sitten kyseiseen näyttöön sovelletaan syrjimättömyyslainsäädännön oikeudellista kehystä.

Keskeiset kysymykset:

- Voidaanko osoittaa syrjinnän *prima facie* -tapaus?
- Onko todennäköistä, että vastaaja pystyy täyttämään todistustaakan?
- Kun kaikki todisteet huomioidaan, onko laiton syrjintä näytetty toteen?

Vaihe 4

Harkitse ja käytä käytettävissä olevia oikeussuojakeinoja.

Keskeinen kysymys:

- Mitä oikeussuojakeinoja on haettava tai käytettävä?

Kaikissa vaiheissa tapauksen käsittelijän on huomioitava seuraavat seikat.

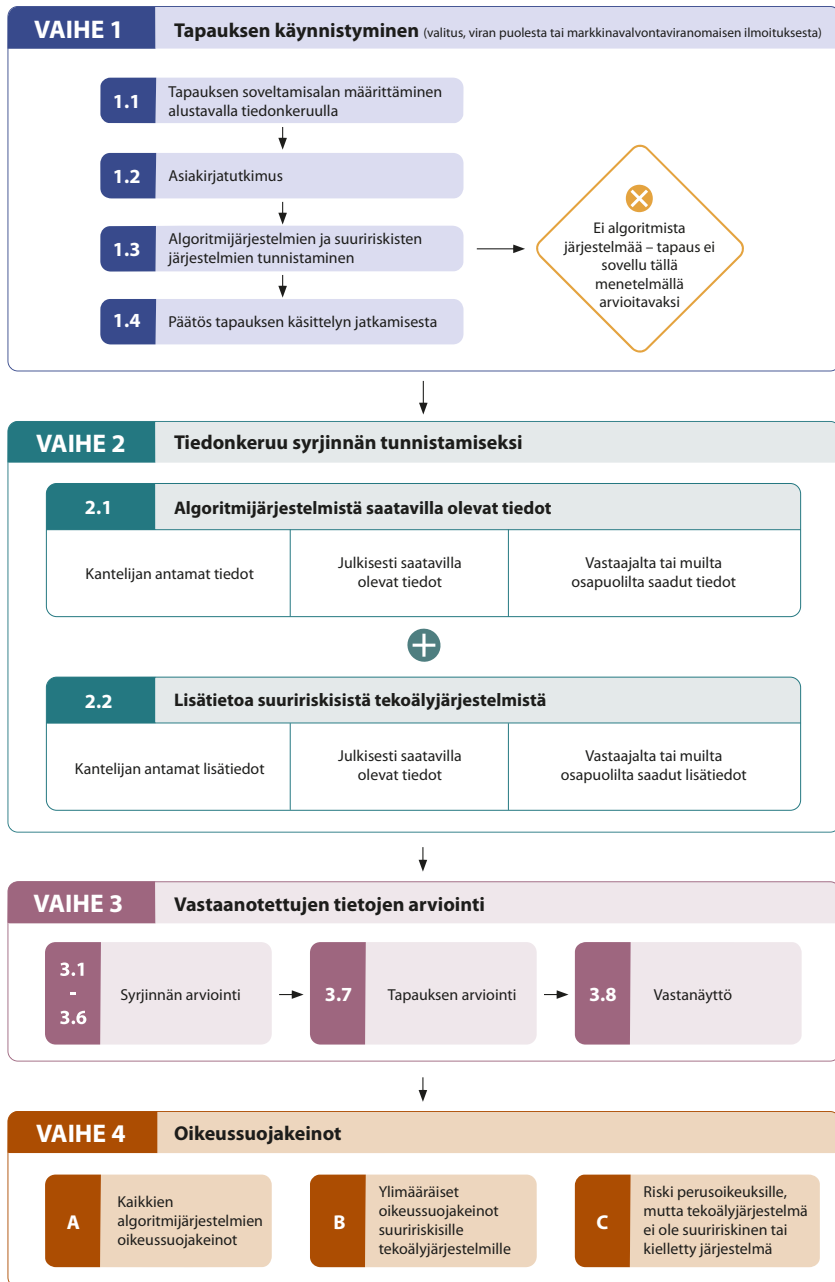
- Jos syrjintää ei voida perustellusti osoittaa, tapauksen käsittely on lopetettava.
- Jos kyseessä ei ole algoritmijärjestelmä, tapauksen käsittely tämän arviointimenetelmän mukaan on lopetettava. Tällöin tapausta tulee käsitellä yhdenvertaisuuselimen tavanomaisen syrjintäprosessin mukaisesti.

Asiantuntijoiden käyttö

Asiantuntija-avun hakeminen voi olla tarpeen tietyissä tämän arviointimenettelyn osissa, kuten silloin, kun tarvitaan data- tai tietojenkäsittelytieteen asiantuntemusta mallin tai datan tekniseen arviointiin. Arviointimenetelmässä kuvataan, minkä tyyppisiin kysymyksiin asiantuntijaa voidaan pyytää vastaamaan ja milloin tätä tulisi harkita. Tekoälyä koskevassa digitaalialan koontiasetuksessa kuvattujen 77 artiklan

muutosten¹⁸ mukaan yhdenvertaisuuselimet voivat mahdollisesti hakea apua markkinavalvontaviranomaisilta, muilta viranomaisilta tai asiantuntevilta elimiltä 77 artiklan 1 kohdan b alakohdan keskinäistä apua koskevan säännöksen nojalla.

Kuva 1. Arviointimenetelmän vaiheet 1–4



18. Katso edeltä kohta "EU:n tekoälyasetus, 77 artikla: perusoikeuksia suojelevien viranomaisten valtuudet".



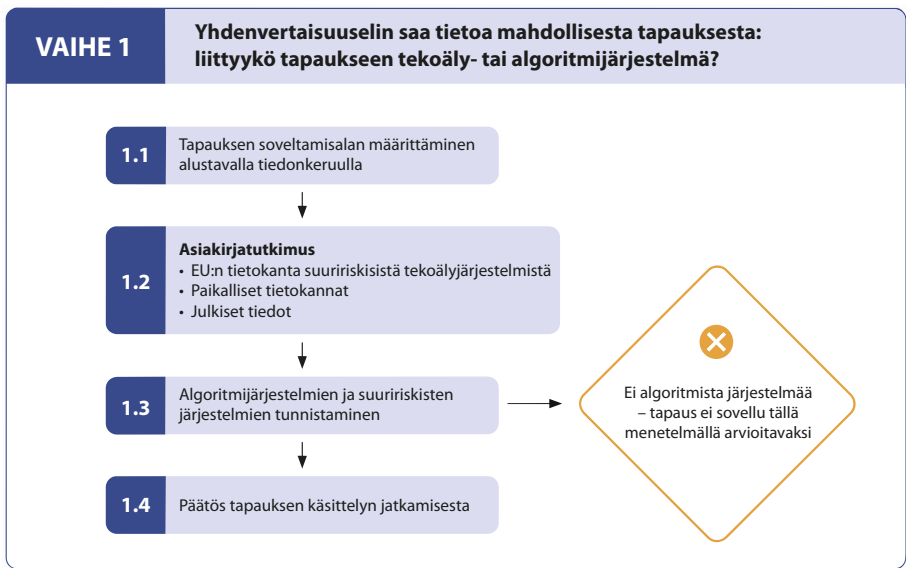
Vaihe 1

Tekoäly- tai algoritmijärjestelmien tunnistaminen

Tämän ensimmäisen vaiheen tarkoituksena on ainoastaan ymmärtää, onko kyseessä automaattisen päätöksenteon järjestelmä tai (suuririskinen) tekoälyjärjestelmä, ja määrittää, onko tietoa riittävästi vaiheeseen 2 siirtymistä varten. Tässä vaiheessa ei tehdä yksityiskohtaista tutkimusta.

Vaihe 1 koostuu seuraavista alivaiheista.

Kuva 2. Vaihe 1 – Liittyykö tapaukseen tekoäly- tai algoritmijärjestelmä?



Huomautus: vaiheet esitetään peräkkäin tämän käytännön rakenteellisen selkeyden vuoksi. Alivaiheet eivät ole käytännössä selkeästi peräkkäisiä vaan usein sirkulaarisia ja iteratiivisia.

Tekoälyyn ja automaattiseen päätöksentekoon liittyvien tapausten tunnistaminen vaihtelee sen mukaan, mikä tapauksen lähde oli:

- A. valitus (yksilön tai ryhmän tekemä)
- B. viran puolesta (*ex officio*) tehtävä tutkinta
- C. markkinaevalvontaviranomaisen antamat tiedot.

Algoritmijärjestelmien ja tekoälyn tunnistaminen

Algoritmijärjestelmät voivat yksinkertaisimmillaan olla esimerkiksi ihmisten määritelmien sääntöjen rajallisen joukon automatisointia. Yleisesti ottaen algoritmijärjestelmiä (mukaan lukien tekoälyä) on vaikea tunnistaa. Määritelmät ovat muuttuneet vuosien varrella tai niitä tulkitaan eri tavoin.

EU:n tekoälyasetuksen 3 artiklan 1 kohdan teknisen määritelmän mukaan

tekoälyjärjestelmä tarkoittaa konepohjaista järjestelmää, joka on suunniteltu toimimaan käyttöönoton jälkeen vaihtelevilla autonomian tasoilla ja jossa voi ilmetä mukautuvuutta käyttöönoton jälkeen ja joka päättää vastaanottamastaan syötteestä eksplisiittisiä tai implisiittisiä tavoitteita varten, miten tuottaa tuotteita, kuten ennusteita, sisältöä, suosituksia tai päätöksiä, jotka voivat vaikuttaa fyysisiin tai virtuaalisiin ympäristöihin.¹⁹

19. Tätä täydentävät Euroopan komission tiedonannon C(2025) 5053 suuntaviivat, jotka koskevat asetuksen (EU) 2024/1689 (tekoälyasetus) mukaista tekoälyjärjestelmän määritelmää (Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689).

Silloinkin, kun määritelmistä ollaan yksimielisiä, organisaatiot eivät usein tunnista algoritmijärjestelmiä tai viittaavat niihin eri termeillä.

Algoritmijärjestelmän mahdollisen käytön arvioinnin tulee sen vuoksi kattaa useita eri termejä.

Kaikki seuraavat termit voivat viitata algoritmijärjestelmien käyttöön:

- ▶ automaatio, konepohjainen, tietokonepohjainen ja algoritmipohjainen
- ▶ profilointi tai profiilien luonti
- ▶ automaattinen päätöksenteko tai päätöksenteon tukijärjestelmät
- ▶ järjestelmä tai tietokone, joka tekee päätöksiä tai analysoi/vertaa/suosittelee/käsittelee henkilön tietoja
- ▶ järjestelmä, tietokone tai kamera, joka näkee/kuuntelee/ymmärtää jotakin
- ▶ maininta pisteyttämisestä, todennäköisyydestä, uskottavuudesta tai tulevan käyttäytymisen arvioinnista
- ▶ automaattinen riskinarviointi ja automaattinen tunnistus
- ▶ mikä tahansa maininta tilastoista
- ▶ mikä tahansa maininta koneoppimisesta.

Seuraavat sanat saattavat viitata tekoälyn käyttöön:

- ▶ koneoppiminen ja syväoppiminen
- ▶ mallin/koneen/tietokoneen koulutus
- ▶ datasta opitut kuviot
- ▶ suuriin kielimalleihin (LLM) perustuva
- ▶ ennakoivat mallit.

Esimerkki: ”Palveluntarjoajamme laskee näiden tietojen perusteella matemaattis-tilastollisilla menetelmillä todennäköisyysarvoja, joita käytetään maksuhäiriöriskin arviointiin ja osoitteen vahvistamiseen.”

1.1. Alustava tiedonkeruu

A. Valitus

Kun tapauksen lähteenä on valitus, on olemassa alkupiste, jossa valitus on tehty. Tässä vaiheessa voidaan kerätä alustavia tietoja siitä, onko kyseessä algoritmi- tai tekoälyjärjestelmä. Tämä alustava tiedonkeruu on kevyttä, jotta se olisi mahdollisimman yhdenmukaista yhdenvertaisuuselinten olemassa olevien valitusten vastaanotto-prosessien kanssa.

1.1.1. Soveltamisalan ja toimivallan alustava määrittäminen

- ▶ Valituksen lähde: puhelu, verkkolomake, posti tai jokin muu.
- ▶ Kantelijan nimi ja yhteystiedot.
- ▶ Lyhyt raportti ongelmasta.

- ▶ Mikä organisaatio on vastaaja (organisaatio, jota valitus koskee)?
 - Julkinen vai yksityinen taho?
- ▶ Toimivallan arviointi.
 - Kielletyt syrjintäperusteet?
 - Sektori?
- ▶ Haettu oikeussuojakeino / tapauksen tarkoitus.
 - Neuvojen antaminen?
 - Asian vieminen oikeuteen?
 - Toimenpiteen suositteleminen?

Kuuluuko tämä tapaus yhdenvertaisuuselimen toimivaltaan? Onko valitus jo tehty toiselle elimelle/taholle tai onko jokin muu taho jo osallisena tapauksessa?

1.1.2. Lisätietojen kerääminen valituksesta

Kantelijalla voi olla lisätietoja käytettävissään. Tämä osio sisältää esimerkkikysymyksiä, joita voidaan esittää kantelijalle joko verkkolomakkeen tai (puhelin)keskustelun kautta, jotta voidaan selvittää, onko kyseessä algoritmi- tai tekoälyjärjestelmä.

Tekoälyasetuksessa ja yleisessä tietosuojajärjestelmässä on asetettu avoimuusvelvoitteita koskien tietoja, joita yksilöille – rekisteröidyille tai henkilöille, joihin vaikutukset kohdistuvat – on annettava algoritmi- tai tekoälyjärjestelmien käytöstä. Katso alla olevista tekstilaatikoista asiaankuuluvat säännökset. Sovellettavat tiedot voidaan antaa yksilöille henkilökohtaisen viestinnän tai sopimusten kautta. Ne sisältyvät yleensä tietosuojailmoituksiin tai käyttöehtoihin, tai niistä tiedotetaan muutoin julkisesti organisaation verkkosivustolla tai alustoilla (katso kohta [1.2.3 Vastaajan verkkosivusto ja ulkoinen viestintä](#)).

Siksi pyytämällä asianomaisia toimittamaan jo tässä vaiheessa kaikki heillä mahdollisesti olevat asiaankuuluvat asiakirjat sekä minimaalisella julkisten tietojen tarkastelulla voidaan tukea seuraavaa vaihetta (katso kohta [1.2 Tarkempi asiakirjatutkimus](#)).

Huomaus: nämä säännökset eivät kata kaikkia tapauksia, joissa käytetään tekoäly- tai algoritmijärjestelmiä, ja siksi tiedon puute voi yksinkertaisesti tarkoittaa tarvetta lisätiedusteluihin.

Tekoälyasetuksen useiden eri kohtien mukaan henkilöille on ilmoitettava tekoälyn käytöstä.

- ▶ Ennen suuririskisen tekoälyjärjestelmän käyttöä työpaikalla työntekijöiden edustajille ja asianomaisille työntekijöille on ilmoitettava, että heihin sovelletaan suuririskistä tekoälyjärjestelmää (tekoälyasetus, 26 artiklan 7 kohta).
- ▶ Sellaisten suuririskisten tekoälyjärjestelmien käyttöönottajien, jotka tekevät tai auttavat tekemään luonnollisiin henkilöihin liittyviä päätöksiä, on ilmoitettava luonnollisille henkilöille, että heihin sovelletaan suuririskistä tekoälyjärjestelmää (tekoälyasetus, 26 artiklan 11 kohta). Näiden tietojen on sisällettävä järjestelmän käyttötarkoitus ja sen tekemien päätösten tyytit. Käyttöönottajien

on myös ilmoitettava luonnollisille henkilöille heidän oikeudestaan saada selitys tämän asetuksen mukaisesti (tekoälyasetus, johdanto-osan kappale 93).

- ▶ Asianomaisille luonnollisille henkilöille on ilmoitettava, että he ovat vuorovaikutuksessa (esimerkiksi chattibottien tai ääniyhdistyksen kautta) tekoälyjärjestelmän kanssa (tekoälyasetus, 50 artiklan 1 kohta). Tämä voidaan tehdä selkeiden ilmoitusten tai ponnahdusikkunoiden avulla esimerkiksi seuraavasti: "Hei, olen chattibotti." / "Hei, keskustele nyt tekoälyavustajan kanssa." / "Olen X, tukea tarjoava tekoälyavustaja."
- ▶ Vastaavasti tunteentunnistusjärjestelmän (tekoälyjärjestelmä, jonka tarkoituksena on esimerkiksi tunnistaa asiakkaiden vihaisuus tai tyytyväisyys kasvojen tai äänen avulla) tai biometrisen luokitusjärjestelmän (tekoälyjärjestelmä, jonka tarkoituksena on esimerkiksi tunnistaa henkilön sukupuoli hiusten tai kasvonmuodon perusteella) käyttöönottajien on ilmoitettava järjestelmän toiminnasta niille luonnollisille henkilöille, jotka altistuvat järjestelmälle (tekoälyasetus, 50 artiklan 3 kohta).

Yleinen tietosuoja-asetus (GDPR)

- ▶ Myös yleinen tietosuoja-asetus sisältää avoimuusvaatimuksia (GDPR, 5 artiklan 1 kohdan a alakohta, 13 artikla, 14 artikla), joiden mukaan rekisteröidylle on ilmoitettava algoritmijärjestelmien käytöstä, mukaan lukien tiedot rekisterinpitäjän identiteetistä, käsittelyn tarkoituksista sekä automaattisen päätöksenteon ja profiloinnin käytöstä (katso [vaihe 2.1.1 Kantelijan antamat tiedot](#)).

Nämä tiedot voivat sisältyä käyttöehtoihin tai tietosuojailmoitukseen tai -selostukseen. Tekoälyasetuksen osalta tekoälyvirasto julkaisi ohjeet tekoälylain mukaisista avoimuusvelvoitteista heinäkuussa 2026.²⁰

Kysymyksiä, joita kantelijalle voi esittää ja/tai jotka on huomioitava asiakirjatutkimuksessa

Huomautus: Kantelija ei välttämättä tiedä, mitä tietoja hänellä on tai ovatko ne tärkeitä tapauksessa. Siksi on hyödyllistä yksinkertaisesti kysyä aluksi seuraavat kysymykset: "Mitä verkkosivustoja/sovelluksia käytit?" ja "Saitko mitään asiakirjoja?"

Asiaankuuluvia asiakirjoja voivat olla muun muassa kantelijan lähettämä hakemus, vastaajana toimivan organisaation lähettämät kirjeet, sähköpostit, laskut, suostumuslomakkeet ja tietosuojailmoitukset, kantelijan ja vastaajan väliset sopimukset, mukaan lukien niiden liitteet ja päivitykset, jotka toimitetaan paperikopioina, sähköpostitse tai sovelluksen tai portaalin ilmoitusten kautta. Jos saatavilla on asiaankuuluvaa dokumentaatiota, se on kerättävä ja siihen on tutustuttava kohdassa [1.2 Tarkempi asiakirjatutkimus](#), jotta voidaan vastata seuraaviin kysymyksiin tai osaan niistä.

- ▶ Kerrottiinko kantelijalle, että tekoälyjärjestelmää käytettiin tai käytetään parhaillaan?

20. Katso lisätietoja: [Guidelines on transparency obligations for providers and deployers of AI systems | Shaping Europe's digital future](#).

- Jos tapaus koskee työpaikkaa: onko kantelija ottanut yhteyttä työntekijöiden edustajiin tai ammattiliittoon?
- Jos on: mitä tietoja tällöin saatiin?
- ▶ Kerrottiinko kantelijalle, että automaattista tietojenkäsittelyä käytettiin?²¹
- ▶ Kysyttiinkö kantelijalta lupaa tiettyjen tietojen käsittelyyn tai pyydettiinkö häneltä vahvistusta tietosuojaselosteen tai -ilmoituksen lukemisesta?
 - Jos kyllä: voidaanko pyydetyn luvan teksti tai tietosuojaseloste tai -ilmoitus jakaa?
 - Jos ei: mainittiinko muutoin esimerkiksi lauseita ”näin käsittelemme tietojasi” tai ”tietojasi voidaan käyttää seuraaviin tarkoituksiin”?
- ▶ Mainittiinko automaatiota tai itsenäisesti tehtäviä suorittavaa tai päätöksentekoon syötteitä antavaa tietokonejärjestelmää? Esimerkiksi seuraavien kaltaisiin lauseisiin ja sanavalintoihin on kiinnitettävä huomiota.
 - Järjestelmä tai tietokone, joka tekee päätöksiä tai analysoi/vertaa/suosittelee/ käsittelee henkilön tietoja.
 - Järjestelmä, tietokone tai kamera, joka ”näkee”/”kuuntelee”/”ymmärtää” jotakin.
 - Maininta pisteyttämisestä, todennäköisyydestä, uskottavuudesta tai tulevan käyttäytymisen arvioinnista.
 - Tietokonejärjestelmän käyttö prosessin tukena. Tämä voi sisältää tuotenimen. Esimerkki: ”Käytämme Clippyä/Frankia/Mayaa tietojesi käsittelyyn ja työemme tukemiseen”.
- ▶ Sisältääkö kantelijan ja vastaajan välinen sopimus viittauksia automaatioon, algoritmisiin prosesseihin, erityisesti nimettyihin järjestelmiin, tilastoihin, suorituskykymittareihin, luokituksiin tai pisteytykseen (kuten automaattiseen deaktivointiin tai luotettavuuspisteisiin)?
 - Jos kyllä: voidaanko sopimus tai asiaankuuluvat sopimuslausekkeet jakaa?
- ▶ Missä vuorovaikutus tai viestintä (vastaajana toimivan) organisaation kanssa tapahtui?
- ▶ Kasvokkain tai puhelimitse tapahtuvissa vuorovaikutustilanteissa:
 - Jos kyseessä oli tapaaminen kasvokkain, käyttikö henkilö tietokonetta päätöksenteon tai johtopäätösten tekemisessä?
- ▶ Tietokoneen tai älypuhelimien kautta tapahtuvissa vuorovaikutustilanteissa:
 - Liittyikö tapaukseen verkossa täytetty lomake?
 - Kuinka kauan vuorovaikutuksen jälkeen saatiin tulos tai päätös (välittömästi, muutamassa minuutissa tai tunnissa, muutamassa päivässä vai tätä pidemmässä ajassa)?
 - Pyydettiinkö henkilötietojen käsittelyyn lupaa esimerkiksi pyytämällä henkilötietoja tai tietosuoja koskevan ruudun rastittamista?

21. Kun henkilötietoja käytetään täysin automaattiseen päätöksentekoon, käyttäjille on ilmoitettava heihin liittyvästä automaattisen päätöksenteon käytöstä (yleinen tietosuoja-asetus, 13 artiklan 2 kohdan f alakohta).

- Pyydettiinkö vuorovaikutuksessa järjestelmän kanssa tietoja mistään kielletystä syrjintäperusteesta (katso kohta [Kielletyt syrjintäperusteet](#))?

1.1.3. Julkisten tietojen nopea tarkistus

EU:n tietokanta suuririskisistä tekoälyjärjestelmistä

2. elokuuta 2026 alkaen EU:n tietokannan suuririskisistä järjestelmistä²² odotetaan olevan käytettävissä suuririskisille järjestelmille ennen niiden markkinoille saattamista tai käyttöönottoa. Tekoälyä koskevan digitaalialan koontiasetuksen mukaan ennen 2. joulukuuta 2027 käyttöön otetut erilliset suuririskiset tekoälyjärjestelmät ja ennen 2. elokuuta 2028 käyttöön otetut tuotteiden osina toimivat suuririskiset tekoälyjärjestelmät edellyttävät rekisteröintiä vain, jos niihin tehdään ”merkittäviä muutoksia”.²³ Tietokannan julkiset osat ovat kaikkien saatavilla.

Nopea haku tietokannasta – tapaukseen sovellettavilla avainsanoilla, kuten vastaajana toimivan organisaation nimellä, järjestelmän nimellä tai kyseisellä sektorilla – voi olla hyödyllinen lähtöpiste, jos valitustapaus liittyy koulutukseen, työllisyyteen, julkiseen hallintoon, pankkiyhteisöön tai vakuutusyhtiöön, oikeudenkäyttöön ja vaaleihin tai jos tapaukseen sisältyy esimerkiksi henkilöiden tunnistamiseen, kasvon- tai äänen-tunnistukseen, tunteentunnistukseen tai aikomusten tai riskien ennustamiseen liittyvää automaatiota.

- Jos vastaaja liittyy tietokannan mukaan mihin tahansa valituksen kannalta merkitykselliseen käyttötapaukseen, on suhteellisen varmaa, että tapaukseen sisältyy (suuririskinen) tekoälyjärjestelmä.²⁴ Siirry [vaiheeseen 1.3](#).

Huomautus: Rekisteröintivelvollisuuksiin sovelletaan tiettyjä poikkeuksia. On myös mahdollista, ettei tarjoaja tai käyttöönottaja ole noudattanut sääntelyyn liittyviä velvoitteitaan. Lisätietoja tietokannassa saatavilla olevista tiedoista on [vaiheessa 2.2.2 Julkisesti saatavilla olevat tiedot](#).

Käyttötapausluettelon vertailu

- [Liite C](#) sisältää luettelon algoritmijärjestelmien ja tekoälyn yleisistä käyttötavoista eri sektoreilla. Vaikuttaako jokin näistä esimerkeistä merkitykselliseltä valitukseen liittyvän tilanteen, tapauksen tai prosessin kannalta? Katso myös tekoälytietokannat ja käyttötapaukset [liitteestä F](#).

22. Vaikka tätä tietokantaa ei vielä ole eikä ole varmaa, millaisia sen suunnittelu ja käyttöliittymä tulevat olemaan, tietokanta on sisällytetty tähän, koska sen odotetaan olevan erittäin tärkeä tiedonlähde tulevaisuudessa.

23. Euroopan parlamentin ja neuvoston asetus (EU) 2026/1744, annettu 8 päivänä heinäkuuta 2026, asetusten (EU) 2024/1689, (EU) 2018/1139 ja (EU) 2023/1230 muuttamisesta tekoälyä koskevien yhdenmukaistettujen sääntöjen täytäntöönpanon yksinkertaistamiseksi (tekoälyä koskeva digitaalialan koontiasetus). Saatavilla osoitteessa <https://eur-lex.europa.eu/eli/reg/2026/1744/oj/eng> (viitattu 24. heinäkuuta 2026). Muissa tapauksissa, joissa suuririskinen järjestelmä on tarkoitettu viranomaiskäyttöön, asetuksen vaatimusten noudattamisen edellyttämät toimenpiteet on toteutettava elokuuhun 2030 mennessä (tekoälyasetus, 111 artiklan 2 kohta).

24. Huomaa, että kyseessä voi olla (suuririskinen) tekoälyjärjestelmä, vaikka järjestelmää ei olisi kirjattu tietokantaan, sillä poikkeuksiakin on.

Yleinen internethaku

- ▶ Valitukseen liittyvään tilanteeseen, tapaukseen tai prosessiin liittyvästä inno-vaatiosta/automaatiosta tai vastaajana toimivasta organisaatiosta voi tehdä internethaun.
 - Esimerkki: ”Käyttääkö [kansallisuuden] poliisi tekoälyä?”
 - Esimerkiksi Suomen tapauksessa tämä antaa luettelon hakutuloksista, jotka sisältävät seuraavan tuloksen: [poliisin biometristen tietojen keruun valtuuksien laajentamista koskeva artikkeli Finland plans major expansion of police biometric data collection powers – ID Tech](#).
 - Esimerkki: ”Käytetäänkö tekoälyä rekrytinnissa [maassa]?”
 - Esimerkiksi Belgian tapauksessa tämä antaa seuraavan tuloksen, joka viittaa siihen, että kolmasosa belgialaisista yrityksistä käyttää tekoälyä rekrytointiprosesseissa: [www.aneews.com.tr/europe/2023/07/19/in-belgium-one-third-of-companies-use-artificial-intelligence-in-their-recruitment-processes](#).
 - Varmista, että saadut tulokset ovat aitoja hakutuloksia eivätkä tekoälyllä tuotettuja.

Huomautus: tietyt käytännöt ovat kiellettyjä tekoälyasetuksen 5 artiklan mukaan. Katso luettelo [liitteestä J](#) – kielletyt tekoälyyn liittyvät käytännöt.

Nämä vaiheet ovat vain viitteellisiä. Jos näihin kysymyksiin annettujen vastausten perusteella on todennäköistä, että tekoäly- tai algoritmijärjestelmää käytettiin, siirry [vaiheeseen 1.3](#).

Jos järjestelmän käytöstä ei saada varmuutta tietojen avulla, harkitse (julkisten) lisätietojen keräämistä asiakirjatutkimusta koskevassa [vaiheessa 1.2](#).

B. Viran puolesta (*ex officio*)

Joillakin yhdenvertaisuuselimillä on valtuudet aloittaa tutkimuksia viran puolesta (*ex officio*) tai yleisen valitusoikeuden (*actio popularis*) perusteella (kansallisen lainsäädännön mukaan).

Tässä vaiheessa oletetaan, ettei tapaukseen liity yksilön tai yksilöistä koostuvan ryhmän tekemää kantelua. Tutkimuksen myöhemmissä vaiheissa yhdenvertaisuuselin voi päättää ottaa tutkimukseen mukaan suoraan asianomaisia henkilöitä.

Tässä arviointimenetelmässä oletetaan, että käsiteltävä ala (sektori, sektorin sisäinen toiminta-alue ja mahdollisesti tietyt organisaatiot) on jo määritetty. Tämä voi tarkoittaa esimerkiksi vakuutusyhtiöiden käyttämiä hinnoittelualgoritmeja tai sosiaaliturvan/etuuksien petosriskien pisteytystä.

Kerättävät tiedot

- ▶ Käsiteltävä tilanne, tapaus tai prosessi ja saatavilla olevat julkiset tiedot.

- ▶ Yhdenvertaisuuselimen tai muun asiaankuuluvan tahon (ratkaisemattomat) valitukset. Nämä voivat olla valituksia, jotka eivät olleet erillään riittävän vahvoja, tai tapauksia, joissa kantelija on peruuttanut valituksensa.
- ▶ Osoitus tekoäly- tai algoritmijärjestelmien osallisuudesta, jos saatavilla; katso edeltä kohta [Algoritmijärjestelmien ja tekoälyn tunnistaminen](#).
- ▶ Tiedot organisaatiosta, joka olisi tämän viran puolesta (*ex officio*) tehtävän tutkinnan kohteena, jos se aloitettaisiin virallisesti (jäljempänä ”vastaaja”), tai sektorikohtaisen tarkastelun tapauksessa luettelo organisaatioista, jotka edustavat tarkasteltavana olevaa sektoria.²⁵

Vertailu olemassa olevien tapausten luetteloon

- ▶ **Liite C** sisältää luettelon algoritmijärjestelmien ja tekoälyn yleisistä käyttötavoista eri sektoreilla. Vaikuttaako jokin näistä esimerkeistä merkitykselliseltä mahdolliseen tutkintaan liittyvän tilanteen, tapauksen tai prosessin kannalta?

Kun tapauksen käsittely aloitetaan viran puolesta (*ex officio*), voi olla jo selvää, että kyseessä on tekoälyjärjestelmä. Vaiheet 1.2 ja 1.3 eivät ole tässä tilanteessa tarpeellisia: siirry [vaiheeseen 1.4](#).

C. Markkinavalvontaviranomaisen tekemä ilmoitus

Yhdenvertaisuuselimen odotetaan saavan markkinavalvontaviranomaiselta tietoja tekoälyjärjestelmistä, jotka aiheuttavat syrjintäriskin, erityisesti seuraavissa tapauksissa.

- ▶ **Vakavat vaaratilanteet (tekoälyasetus, 73 artiklan 7 kohta)**
 - Jos tarjoaja ilmoittaa markkinavalvontaviranomaiselle vakavasta vaaratilanteesta,²⁶ markkinavalvontaviranomaisen on ilmoitettava asiasta 77 artiklan mukaisille viranomaisille, tarvittaessa myös yhdenvertaisuuselimelle. Komission kuuleminen raportointimenettelyjä koskevista erityisohjeista ja vaaratilanteita koskevien ilmoitusten mallista päättyi 7. marraskuuta 2025.²⁷
- ▶ **Riskin aiheuttavat tuotteet (tekoälyasetus, 79 artikla, yhdessä asetuksen (EU) 2019/1020 3 artiklan 19 kohdan kanssa)**
 - Jos markkinavalvontaviranomaisella on riittävä syy uskoa, että tekoälyjärjestelmä voidaan luokitella tuotteeksi, joka aiheuttaa riskin oikeudelle syrjimättömyyteen, sillä on velvollisuus ilmoittaa asiasta asiaankuuluville

25. Jos yhdenvertaisuuselin esimerkiksi aloittaa viran puolesta (*ex officio*) tehtävän tutkinnan vakuutusyhtiöiden käyttämistä hinnoittelualgoritmeista, tässä vaiheessa käytäntöä voidaan käyttää edustavaa luetteloa vakuutusyhtiöistä tietyn vastaajan sijaan.

26. Vakavalla vaaratilanteella tarkoitetaan tekoälyjärjestelmän vaaratilannetta tai toimintahäiriötä, joka johtaa suoraan tai välillisesti johonkin seuraavista:
 (a) henkilön kuolema tai vakava vahinko henkilön terveydelle
 (b) vakava tai peruuttamaton häiriö kriittisen infrastruktuurin hallinnassa ja toiminnassa
 (c) perusoikeuksien suojaamiseen tarkoitettujen unionin oikeuden mukaisten velvoitteiden rikkominen
 (d) vakava vahinko omaisuudelle tai ympäristölle (tekoälyasetus, 3 artiklan 49 kohta).

27. Katso lisätietoja: [AI Act: Commission issues draft guidance and reporting template on serious AI incidents, and seeks stakeholders' feedback](#).

77 artiklan mukaisille viranomaisille, mukaan lukien yhdenvertaisuuselimelle, ja tehdä yhteistyötä niiden kanssa.

Nämä tiedot voivat sisältää seuraavia.

- ▶ Organisaatio: julkinen tai yksityinen taho.
- ▶ Tekoälyjärjestelmä: järjestelmän ja suuririskisen käyttötapauksen luokituksen tunnistaminen (tekoälyasetuksen liite I tai liite III, mukaan lukien kohdealue ja käyttötapaus).
- ▶ Organisaation rooli (käyttönottaja, tarjoaja tai muu).
- ▶ Kun ilmoitus perustuu tekoälyasetuksen 73 artiklaan (vakava vaaratilanne):
 - vaaratilanteen tai toimintahäiriön olosuhteet
 - tapahtuneen tai epäillyn vahingon tyyppi
 - tekoälyjärjestelmän ja vaaratilanteen välinen suhde (miten tekoäly aiheutti vaaratilanteen tai vaikutti siihen)
 - kaikki saatavilla olevat tiedot tarjoajan suorittamasta vaaratilannetta koskevan tutkimuksen riskinarvioinnista sekä ehdotetuista tai toteutetuista korjaavista toimenpiteistä.
- ▶ Kun ilmoitus perustuu tekoälyasetuksen 79 artiklaan (riski):
 - syy, jonka vuoksi tekoälyjärjestelmän katsotaan aiheuttavan riskin perusoikeuksille
 - (valinnainen; jos saatavilla) asiaankuuluvat tiedot jo tehdyistä arvioinneista
 - (valinnainen; jos saatavilla) ehdotetut tai toteutetut korjaavat toimenpiteet.
- ▶ Tapauksissa, joissa on kyse lainvalvonnan, muuttoliikkeen, turvapaikka-asioiden ja rajavallvonnan aloilla käytetystä suuririskisestä tekoälyjärjestelmästä (liitteen III kohdat 1, 6 ja 7), markkinaviranomainen voi tarkastella tekoälyjärjestelmää koskevia tietoja sellaisina kuin ne on tallennettu EU:n suuririskisten tekoälyjärjestelmien tietokantaan.

Kun yhdenvertaisuuselin saa ilmoituksen markkinaviranomaiselta, voidaan olla varmoja, että tapaukseen liittyy suuririskinen tekoälyjärjestelmä. Vaiheet 1.2 ja 1.3 eivät ole tässä tapauksessa tarpeellisia: siirry [vaiheeseen 1.4](#).

1.2. Tarkempi asiakirjatutkimus

Jos asiakirjatutkimusta voidaan tehdä enemmän, on olemassa useita lähteitä, joista voidaan tarkistaa, odotetaanko tapaukseen liittyvän automaattista päätöksentekoa tai tekoälyä. Tässä kohdassa kerrotaan näistä lähteistä ja tiedoista, joita voidaan etsiä.

Tässä kohdassa mainitut vaiheet vaihtelevat asiakirjatutkimuksen syvyyden ja käytetyn ajan mukaan:

- ▲ osoittaa priorisoitavat vaiheet.
- ▼ osoittaa lisävaiheita perusteellisempaan asiakirjatutkimukseen.

Esimerkiksi EU:n tietokannasta (jäljempänä) pitäisi olla suhteellisen helppoa tehdä hakuja, kun tietokanta on käytettävissä ja vastaaja on rekisteröitynyt tietokantaan. Tämä antaa nopean vastauksen kysymykseen ”käytetäänkö tekoälyjärjestelmää?” Jos käyttöönottajaa ei ole rekisteröity tietokantaan, tarvitaan lisätutkimuksia.

Tätä kohtaa ei sovelleta tapauksiin, joissa lähde on ”C. Markkinavalvontaviranomaisen tekemä ilmoitus”. Tässä tapauksessa markkinavalvontaviranomainen on jo todennut, että kyseessä on suuririskinen tekoälyjärjestelmä, joten tässä kohdassa esitetty asiakirjatutkimus on tarpeetonta.

1.2.1. EU:n tietokanta suuririskisistä tekoälyjärjestelmistä

Vastaajaa tai mitä tahansa muuta tunnettua käyttöönottajaa tai tarjoajaa voidaan hakea tietokannasta.

Onko vastaaja listattu käyttöönottajaksi tietokannan osassa C?²⁸

- ▲ Onko vastaaja valituksen kannalta merkityksellisen käyttötapauksen käyttöönottaja? Mikä organisaatio on tarjoaja?

Tietokannassa olevat, alustavaa tunnistamista varten tarvittavat tiedot:

- ▶ tarjoajan ja valtuutetun edustajan yhteystiedot
- ▶ käyttöönottajan nimi ja yhteystiedot (vain viranomaiset, unionin toimielimet, elimet, toimistot tai virastot tai niiden puolesta toimivat henkilöt)
- ▶ tekoälyjärjestelmän tarjoajan EU:n tietokantaan syöttämä URL-osoite.

Onko vastaaja merkitty tarjoajaksi tietokannan osassa A tai B?

- ▲ Onko vastaaja valituksen kannalta merkityksellisen suuririskisen käyttötapauksen tarjoaja?
- ▲ Onko vastaaja sellaisen käyttötapauksen tarjoaja, joka on tarkoitettu käytettäväksi suuririskisellä kohdealueella mutta kuuluu itsearviointiin mukaan tekoälyasetuksen 6 artiklan 3 kohdassa kuvattuun poikkeukseen? Kansalliset toimivaltaiset viranomaiset voivat pyytää tätä arviointia.

Tietokannassa olevat, alustavaa tunnistamista varten tarvittavat tiedot:

- ▶ tarjoajan ja valtuutetun edustajan yhteystiedot
- ▶ tuotenimi tai muu viite, joka mahdollistaa tekoälyjärjestelmän tunnistamisen ja jäljittämisen (tämä voi olla hyödyllistä esimerkiksi silloin, kun suuririskistä järjestelmää käytetään osana toista järjestelmää)
- ▶ käyttötarkoitus.

28. Huomaa, että vain viranomaisten on rekisteröidyttävä käyttöönottajiksi. Muilla organisaatioilla ei ole vastaavaa velvoitetta.

Jos järjestelmä löytyy tästä tietokannasta, käytössä on tekoälyjärjestelmä. Siirry [vaiheeseen 1.3](#) ja/tai [1.4](#).

Jos järjestelmää ei löydy, etsi tietokannasta vastaajaa vastaavia organisaatioita:

- ▼ Onko tietokannassa lueteltu samankaltaisia organisaatioita tarjoajina tai käyttöönottajina valituksen kannalta merkityksellisessä käyttötapauksessa? Esimerkiksi muut samankaltaiset vakuutusyhtiöt, jotka käyttävät tekoälyjärjestelmiä hinnoitteluun, jos tapauksessa on kyse (epä)reilusta hinnoittelusta, tai muut saman maan julkisyhteisöt, jotka käyttävät tekoälyjärjestelmiä etuuksien arviointiin, jos tapauksessa on kyse etuuksien epäamisestä.

49 artiklan 4 kohdan mukaan lainvalvonnan, muuttoliikkeen, turvapaikka-asioiden ja rajavalvonnan aloilla käytettyjen suuririskisten tekoälyjärjestelmien rekisteröinnin on tapahduttava 71 artiklassa tarkoitetun EU:n tietokannan suojattuun ei-julkiseen osaan, ja siihen on sisällyttävä tarvittaessa ainoastaan 49 artiklan 4 kohdassa kuvatut tiedot. Pääsyä näihin tietokannan osiin on rajoitettu. Lisätietoja tietokannan ei-julkisesta osasta ja lainvalvonnan alan avoimuutta koskevista näkökohdista on vaiheen 2.2.2 kohdassa [Tiedonsaantia koskevat rajoitukset](#) ja vaiheen 2.2.4 lainvalvonnan alaa koskevassa tekstiruudussa.

1.2.2. Muut (suuririskisten) tekoälyjärjestelmien ja algoritmijärjestelmien tietokannat ja luettelot

Jotkut organisaatiot ja paikallishallinnot ylläpitävät paikallisia tietokantoja, rekistereitä tai luetteloita käytetyistä tekoälyjärjestelmistä. Näiden tietokantojen luettelo on [liitteessä F](#). Kaikkia näitä tietokantoja ei voida soveltaa kaikissa tapauksissa. Valitse vain ne, jotka ovat olennaisia käsiteltävässä kansallisessa kontekstissa.

Hae vastaajaa tietokannasta:

- ▲ Onko algoritmijärjestelmä tai tekoäly merkitty valituksen kattaman tilanteen, tapauksen tai prosessin kannalta merkityksellisen vastaajan käyttämäksi tai kehittämäksi?

Hae vastaajaa vastaavia organisaatioita:

- ▼ Onko algoritmijärjestelmä tai tekoäly merkitty valituksen kattaman tilanteen, tapauksen tai prosessin kannalta merkityksellisen vastaavan organisaation käyttämäksi tai kehittämäksi, jos tämä valitus olisi koskenut tätä vastaavaa organisaatiota?

Vertaa olemassa olevien käyttötapausten luetteloon:

- ▼ [Liitteessä C](#) on luettelo algoritmijärjestelmien ja tekoälyn yleisistä käyttötavoista eri aloilla.

Vaikuttaako jokin näistä käyttötapauksista merkitykselliseltä valitukseen liittyvän tilanteen, tapauksen tai prosessin kannalta?

1.2.3. Vastaajan verkkosivusto ja ulkoinen viestintä

Tietosuojailmoitus/-seloste

Etsi sanamuotoja, jotka viittaavat algoritmijärjestelmien käyttöön. Jäljempänä on esimerkkejä näistä.

- ▲ Tarkoitukset, jotka viittaavat automaatioon, profiilien luomiseen tai tilastollisiin menetelmiin. Katso kohta [Algoritmijärjestelmien ja tekoälyn tunnistaminen](#) sekä kysymykset, jotka on kuvattu kohdassa 1.1.2 Kysymyksiä, joita kantelijalle voi esittää ja/tai jotka on huomioitava asiakirjatutkimuksessa.
- ▲ Kolmannet osapuolet, jotka saavat henkilötietoja (vastaanottajat tai vastaanottajaluokat). Katso, onko merkkejä kolmansien osapuolten, kuten luottopisteytysrytysten tai luottotietolaitosten, osallisuudesta tapaukseen. Jos on, tämä voi viitata profilointiin tai automaattiseen päätöksentekoon.
- ▼ Rekisterinpitäjän yhteystiedot: onko rekisterinpitäjä tunnettu tekoälyratkaisujen tai automaation käyttäjä käsiteltävällä sektorilla? Jos tekoäly- tai algoritmijärjestelmä on olemassa, rekisterinpitäjä on tyypillisesti järjestelmän käyttöönottaja ja tämän arviointimenetelmän mukainen vastaaja.

Muut viestintätyypit

Onko viestinnässä mainittu algoritmijärjestelmää, joka voi olla merkityksellinen tässä tapauksessa?

- ▼ Etsi vastaajan verkkosivustolta artikkeleita tekoälyn, innovaatioiden ja automaation käyttöönotosta tai katso vastaajan verkkosivustolla/alustalla olevat usein kysytyt kysymykset. Helpoin tapa etsiä tiettyä verkkosivustoa on lisätä hakupyyntöön komento "site: [vastaajan verkkosivusto]". Esimerkki: innovatio, tekoäly site: bigbank.com.
- ▼ Katso, onko organisaatiolla datatieteeseen, tekoälyyn tai koneoppimiseen liittyviä teknisiä työpaikkailmoituksia. Onko viestinnässä mainittu algoritmijärjestelmää, joka voi olla merkityksellinen tässä tapauksessa? Esimerkiksi pankin "vanheman datatieteilijän" työpaikkailmoitus sisältää seuraavat tiedot: Rahanpesun ja terrorismin rahoituksen estäminen on tärkeää sekä yhteiskunnallemme että organisaatiollemme ... Vastuualueet sisältävät nykyisen sääntöpohjaisen tapahtumien seurantarjestelmäme (TM) optimoinnin ja myöhemmin edistyneempien analytiikkamenetelmien, kuten koneoppimisen, käyttöönoton TM-malleissamme. Katso työpaikkailmoitus [senior data scientist transaction monitoring – Rabobank](#).

Tarvittaessa: tarkista asiaankuuluvien suuririskisten tekoälyjärjestelmien käyttötapusten käyttöönottajien verkkosivustot ja viestintä.

Jos EU:n tietokannassa suuririskisistä tekoälyjärjestelmistä on kolmannen osapuolen käyttöönottajien listaamia tapaukseen liittyviä käyttötapauksia, tutustu tarjoajan verkkosivustoon.

- ▼ Onko vastaaja merkitty verkkosivustolla ”organisaatioksi, jonka kanssa teemme yhteistyötä” tai ”organisaatioksi, johon asiakkaamme luottavat”?
- ▼ Mainitaanko vastaajaa millään muulla tavalla tarjoajan verkkosivustolla? Tämä tieto voi löytyä helpoiten internetistä hakukoneen kautta. Esimerkkihaku: [vastaaja] site: [tarjoaja].com.

1.2.4. Tarkempi julkisten tietojen tarkastelu

Osa tässä mainituista vaiheista on jo mainittu vaiheessa 1.1. Tietojen täydellisyyden vuoksi ne toistetaan tässä.

Yleinen internethaku

- ▼ Katso internethaku vaiheesta 1.1.3.
- ▼ Tarkenna [vaiheessa 1.1.3](#) tehtyä hakua tarkistamalla erityisesti, ovatko kansalaisjärjestöt tai kansalliset tai kansainväliset elimet tai organisaatiot raportoineet vastaajan tai vastaavien organisaatioiden tekoäly- tai algoritmijärjestelmien käytöstä valitusta vastaavassa tilanteessa, tapauksessa tai prosessissa. Sovellettavia kansalaisjärjestöjä ovat esimerkiksi Amnesty, AlgorithmWatch ja kansalliset kansalaisyhteiskunnan organisaatiot. Esimerkiksi Alankomaissa tietosuojaviranomainen laatii tekoäly- ja algoritmiriskiraportin kahdesti vuodessa. Alankomaiden kansallista kontekstia koskeva haku voisi olla esimerkiksi ”[valitukseen liittyvä sektori] Autoriteit Persoonsgegevens tekoäly- ja algoritmiriskiraportti”.
- ▼ Valinnainen: tarkenna hakua ja sisällytä siihen kansallisia ja kansainvälisiä tekoälystrategioita.
- ▼ Muita asiaankuuluvia resursseja voivat olla esimerkiksi taloudellisen yhteistyön ja kehityksen järjestön (OECD) tekoälyyn liittyviä vaaratilanteita ja vaaroja seuraava [AI Incidents and Hazards Monitor](#) ja [tekoälytapauksien tietokanta AI Incident Database](#) tai Euroopan neuvoston raportit, kuten syrjintää, tekoälyä ja algoritmista päätöksentekoa koskeva raportti Discrimination, artificial intelligence and algorithmic decision making (Zuiderveen Borgesius, 2018).

1.3. Algoritmijärjestelmien tai suuririskisten tekoälyjärjestelmien tunnistaminen

Vaiheissa 1.1 ja 1.2 kerättyjen tietojen perusteella voidaan kohtuullisesti määrittää, käytetäänkö tapauksessa algoritmijärjestelmää tai suuririskistä tekoälyjärjestelmää ja kuinka varma tämä määrittys on.

Muistutus: tässä arviointimenetelmässä vain suuririskiset tekoälyjärjestelmät ja algoritmijärjestelmät erotetaan toisistaan. Algoritmijärjestelmiin kuuluvat ei-suuririskiset tekoälyjärjestelmät ja automaattisen päätöksenteon järjestelmät. Tekoälyasetus asettaa suuririskisille tekoälyjärjestelmille kattavia avoimuus- ja dokumentaatiovelvoitteita, mikä tarkoittaa, että niitä koskevissa tapauksissa saatavilla odotetaan olevan lisädokumentaatiota. Jos tekoälyjärjestelmä ei ole suuririskinen, saatavilla olevat tiedot ja noudatettavat vaiheet ovat samat kuin yksinkertaisemmilla algoritmijärjestelmillä, ja siksi ne yhdistetään yhdeksi luokaksi.

Järjestelmän tyyppi

- **Suuririskinen tekoälyjärjestelmä**
- **Algoritmijärjestelmä**

Varmuus

- **Suhteellinen varmuus**
- **Mahdollinen**

Huomautus: tekoäly- tai algoritmijärjestelmien käytön varmistaminen on tässä vaiheessa hankala ja monimutkainen arviointitehtävä, koska saatavilla olevaa tietoa on rajallisesti. Alla lueteltujen johtopäätösten varmuusarviot ovat vain suuntaa-antavia ehdotuksia.

EU:n tietokanta suuririskistä tekoälyjärjestelmistä

Onko järjestelmä rekisteröity EU:n tietokantaan?

- KYLLÄ, osaan A tai C: Tässä tapauksessa on tunnistettu suuririskinen tekoälyjärjestelmä. On **suhteellisen varmaa**, että tässä tapauksessa on käytetty **suuririskistä tekoälyjärjestelmää**.
- KYLLÄ, osaan B:²⁹ Kyseessä on tekoälyjärjestelmä, mutta suuririskisten järjestelmien edellyttämää dokumentaatiota ei odoteta olevan saatavilla. On **suhteellisen varmaa**, että tässä tapauksessa on käytetty **algoritmijärjestelmää**.
- EI, mutta on olemassa samankaltaisia organisaatioita (kuten toinen pankki), jotka ovat maininneet osassa A tai C tapauksen kannalta merkityksellisiä järjestelmiä (kuten luottopisteytysjärjestelmiä). Siksi voi olla kohtuullista olettaa, että vastaaja on käyttänyt samankaltaista suuririskistä järjestelmää. Tässä arviointimenetelmän vaiheessa oletetaan, että on **suhteellisen varmaa**, että tässä tapauksessa on käytetty **algoritmijärjestelmää**. Tässä tapauksessa on **mahdollisesti** käytetty **suuririskistä tekoälyjärjestelmää**.

Vastaajan antamat tiedot (joko kantelijalle, julkisissa asiakirjoissa tai pyynnöstä annetut)

- Vastaaja ilmoitti automaation, algoritmien tai tekoälyn käytöstä tapauksen kannalta merkityksellisiin tarkoituksiin joko suoraan kantelijalle tai tietosuojailmoituksessa/-selosteessa. On **suhteellisen varmaa**, että tässä tapauksessa on käytetty **algoritmijärjestelmää**.
- Vastaaja ilmoitti automaation, algoritmien tai tekoälyn käytöstä suuririskisten tekoälyjärjestelmien luokkien (katso liite I) kannalta merkityksellisiin tarkoituksiin joko suoraan kantelijalle tai tietosuojailmoituksessa/-selosteessa. On **suhteellisen varmaa**, että tässä tapauksessa on käytetty **algoritmijärjestelmää** ja **mahdollisesti suuririskistä tekoälyjärjestelmää**.
- Vastaaja on rekisteröinyt algoritmi- tai tekoälyjärjestelmän julkiseen tietokantaan (katso liite F) tapauksen kannalta merkityksellisiin tarkoituksiin. On **suhteellisen varmaa**, että tässä tapauksessa on käytetty **algoritmijärjestelmää**.

29. Tekoälyasetuksen 6 artiklan 3 kohdan mukaan tekoälyjärjestelmää ei pidetä suuririskisenä.

- Vastaaja on julkisesti ilmoittanut blogikirjoituksissa, lehdistötiedotteissa tai muissa lähteissä käyttävänsä algoritmijärjestelmiä tai tekoälyä tapauksen kannalta merkityksellisiin tarkoituksiin. Huomaa, että viittaukset algoritmijärjestelmien käyttöön voivat olla epämää räisiä tai vältteleviä (katso [vaiheesta 1.1](#) mahdollisia käytettyjä ilmaisia). On **suhteellisen varmaa**, että tässä tapauksessa on käytetty **algoritmijärjestelmää**.

Muut tiedot

- Arvostetut tahot, kuten kansalaisjärjestöt ja luotettavat mediaorganisaatiot, ovat ilmoittaneet vastaajan käyttäneen algoritmijärjestelmiä tai tekoälyä tapauksen kannalta merkityksellisiin tarkoituksiin. Organisaation vahvistusta tästä ei löydy. On **suhteellisen varmaa**, että tässä tapauksessa on käytetty **algoritmijärjestelmää**.
- Muut osapuolet ovat ilmoittaneet vastaajan käyttäneen algoritmijärjestelmiä tai tekoälyä tapauksen kannalta merkityksellisiin tarkoituksiin. Vastaajan vahvistusta tästä ei löydy. Tässä tapauksessa on **mahdollisesti** käytetty **algoritmijärjestelmää**.
- Tekoäly- ja algoritmijärjestelmiä käytetään usein tapauksen kannalta merkityksellisiin tarkoituksiin, kuten [liitteessä C](#) kuvattuihin käyttötarkoituksiin. Tässä tapauksessa on **mahdollisesti** käytetty **algoritmijärjestelmää**.
- Samankaltaisten organisaatioiden on raportoitu käyttävän algoritmijärjestelmiä tapauksen kannalta merkityksellisiin tarkoituksiin. Tässä tapauksessa on **mahdollisesti** käytetty **algoritmijärjestelmää**.
- Tapauksessa on asiayhteyteen liittyviä vihjeitä, jotka viittaavat siihen, että algoritmijärjestelmää on saatettu käyttää. Tätä voidaan epäillä esimerkiksi päätöksenteon nopeuden vuoksi, kun monimutkaiset prosessit tai harkintaa vaativat päätökset käsitellään välittömästi tai muutamassa minuutissa. Tässä tapauksessa on **mahdollisesti** käytetty **algoritmijärjestelmää**.
- Tapauksessa on asiayhteyteen liittyviä vihjeitä, jotka viittaavat siihen, että algoritmijärjestelmää on saatettu käyttää. Tätä voidaan epäillä esimerkiksi päätöksenteon nopeuden vuoksi, kun monimutkaiset prosessit tai harkintaa vaativat päätökset käsitellään välittömästi tai muutamassa minuutissa, ja tekoäly- tai algoritmijärjestelmiä käytetään usein tapauksen kannalta merkityksellisiin tarkoituksiin, kuten [liitteessä C](#) kuvattuihin käyttötarkoituksiin, tai samankaltaisten organisaatioiden on raportoitu käyttävän algoritmijärjestelmiä tapauksen kannalta merkityksellisiin tarkoituksiin. On **suhteellisen varmaa**, että tässä tapauksessa on käytetty **algoritmijärjestelmää**.

1.4. Tapauksen käsittelyn jatkaminen

Vaiheet 1.1.–1.3. kattavat arvioinnin, jolla määritetään, onko todennäköistä, että tapaukseen liittyy algoritmijärjestelmä. Jotta voidaan päättää, jatketaanko tapauksen käsittelyä, on tehtävä lisäarviointi perustellun syrjintätapauksen todennäköisyydestä. Tätä on arvioitava yhdenvertaisuuselimen olemassa olevien kriteerien perusteella. Matalampi varmuuskynnys voi olla tarpeen ennen tapauksen käsittelyn jatkamis-päätöstä, kun kyseessä on mahdollisesti algoritmijärjestelmä.

Manjang v. Uber Eats UK Ltd ja muut (2021)

Tämä rotuun perustuvaa syrjintää koskeva kanne nostettiin häirinnän, uhriksi joutumisen ja välillisen syrjinnän perusteella kasvontunnistusteknologian käyt-tönoton jälkeen. Kantajana ollut kuljettaja sai Uber Eatsilta (vastaaja) sähköpostin, jossa hänelle ilmoitettiin alustan pysyvästä käyttöoikeuden keskeytyksestä sillä perusteella, että hän oli jakanut tilinsä Uber Eats -kuljetuskumppaninsa kanssa eikä ollut läpäissyt kasvontunnistustarkistusta. Kantaja totesi vastauksessaan, että algoritmi vaikutti rasistiselta, ja pyysi ongelman ratkaisua, koska algoritmi ei pystynyt tunnistamaan ja vahvistamaan hänen valokuviaan. Kantaja uskoi, että näiden ongelmien vuoksi alusta todennäköisesti pyysi häntä ottamaan itsestään valokuvia useita kertoja päivässä. Uber Eats kiisti syrjintäväitteen ja vaati asian kumoamista varhaisessa vaiheessa, koska yhtiön mukaan se perustui ”asiavirheisiin”. Yhtiö antoi sitten tietoja perusteistaan teknologian toimintaan pohjautuvan väittämän kiistämiseen, ja vastauksena tähän kantaja muutti kan-nettaan. Tuomioistuimien kieltäytyi hylkäämästä muutettua kannetta ja totesi, että kantajan esittäessä kanteensa ei ollut selvää, miksi hänen tilinsä oli deaktivoitu. Muutamaa kuukautta myöhemmin oikeudenkäynnin aikana vastaaja totesi, että kantajalle annetut perustelut automaattisesta päätöksenteosta olivat virheelliset ja että tapauksessa oli käytetty ihmisen tekemää tarkastusta. Kantaja ei luopunut kanteestaan, ja tuomioistuimien totesi, että syy kantajan valokuvien hylkäämiseen ja hänen tilinsä deaktivointiin oli epäselvä. Lopulta asiaan liittyvistä korvauksista sovittiin tuomioistuimen ulkopuolisessa riidanratkaisussa.

Tämä on esimerkki yhdenvertaisuuselimen rahoittamasta ja tukemasta tapauk-sesta, tässä tapauksessa kyseessä oli Yhdistyneen kuningaskunnan Equality and Human Rights Commission.

Taulukko 2. Suuririskisen tekoälyjärjestelmän tai algoritmijärjestelmän käytön varmuus ja syrjinnän todennäköisyys

	Matala syrjinnän todennäköisyys	Keskitasoinen syrjinnän todennäköisyys	Korkea syrjinnän todennäköisyys
Suhteellisen varmasti suuririskinen tekoälyjärjestelmä	Korkean prioriteetin tapaus, jossa harkittava (sisäisen) algoritmijärjestelmien asiantuntijan osallistumista	Korkean prioriteetin tapaus, jossa harkittava (sisäisen) algoritmijärjestelmien asiantuntijan osallistumista	Korkean prioriteetin tapaus, jossa harkittava (sisäisen) algoritmijärjestelmien asiantuntijan osallistumista
Suhteellisen varmasti algoritmijärjestelmä, mahdollisesti suuririskinen tekoälyjärjestelmä	Keskitason prioriteetin tapaus, jossa harkittava (sisäisen) algoritmijärjestelmien asiantuntijan osallistumista	Korkean prioriteetin tapaus, jossa harkittava (sisäisen) algoritmijärjestelmien asiantuntijan osallistumista	Korkean prioriteetin tapaus, jossa harkittava (sisäisen) algoritmijärjestelmien asiantuntijan osallistumista
Suhteellisen varmasti algoritmijärjestelmä	Matalan prioriteetin tapaus, jossa harkittava (sisäisen) algoritmijärjestelmien asiantuntijan osallistumista, jos tapauksen käsitte- lyä jatketaan	Keskitason prioriteetin tapaus, jossa harkittava (sisäisen) algoritmijärjestelmien asiantuntijan osallistumista	Korkean prioriteetin tapaus, jossa harkittava (sisäisen) algoritmijärjestelmien asiantuntijan osallistumista
Mahdollisesti algoritmijärjestelmä	Käytä olemassa olevia menetelmiä tämän arviointi- menetelmän sijaan	Tämän arviointi- menetelmän mukaan matalan prioriteetin tapaus, jossa syrjinnän todennäköisyys on keskitasoinen mutta tekoälyjärjestelmän käytön todennäköisyys on pieni; käytä ole- massa olevia mene- telmiä tämän arviointi- menetelmän sijaan	Keskitason pri- oriteetin tapaus, jossa harkittava (sisäisen) algo- ritmijärjestelmien asiantuntijan osallistumista

Epäilty virheellinen tekoälyasetuksen mukainen luokittelu

Virheellinen luokittelu ei-suuririskiseksi järjestelmäksi

On mahdollista, että tekoälyjärjestelmien tarjoajat liitteessä III kuvatuilla alueilla välttävät suuririskisten tekoälyjärjestelmien velvoitteet määrittelemällä järjestelmän itsearvioinnissa jollakin seuraavista tavoista.

- Ei tekoälyjärjestelmä. Tässä tapauksessa tekoälyasetusta ei sovellettaisi järjestelmään.

- ▶ Ei suuririskinen järjestelmä poikkeusten vuoksi (tekoälyasetus, 6 artiklan 3 kohta). Tässä tapauksessa järjestelmä on silti rekisteröitävä EU:n tietokannan B-osioon. Kyseisen tarjoajan on dokumentoitava arvionsa, jonka mukaan järjestelmä ei ole suuririskinen, ennen järjestelmän saattamista markkinoille tai käyttöönottoa sekä rekisteröitävä kyseinen järjestelmä EU:n tietokannan B-osioon (tekoälyasetus, 49 artiklan 2 kohta). Arvioinnilla ei ole julkaisuvelvoitetta, mutta tarjoajan on toimitettava arviointiin liittyvä dokumentaatio pyynnöstä kansallisille toimivaltaisille viranomaisille (markkinaviranomainen tai ilmoittamisesta vastaava elin).
- ▶ Ei suuririskinen järjestelmä, koska sen tarkoitus ei sisälly tekoälyasetuksen liitteen III käyttötapauksen sanamuotoon (tekoälyasetus, 6 artiklan 3 kohta).

Jos yhdenvertaisuuselin epäilee, että järjestelmä on virheellisesti arvioitu suuririskisten tekoälyjärjestelmien määritelmän ulkopuolelle, sen tulee ilmoittaa asiasta asiaankuuluvalla markkinavalvontaviranomaiselle riippumatta siitä, voidaanko syrjintätapaus osoittaa (katso vaiheesta 4 markkinavalvontaviranomaisten menettelytavat, kun tarjoaja on luokitellut tekoälyjärjestelmän ei-suuririskiseksi, sekä vaihe 4.3).

Tässä arviointimenetelmässä järjestelmää on käsiteltävä algoritmijärjestelmänä, koska tietoja, joiden odotetaan olevan saatavilla suuririskisistä tekoälyjärjestelmistä, ei todennäköisesti ole tässä tapauksessa käytettävissä.

Kysyttäviä kysymyksiä

- ▶ Kattavatko liitteen III käyttötapaukset järjestelmän?
- ▶ Onko järjestelmä todennäköisesti tekoälyjärjestelmä?
Katso kohta [Algoritmijärjestelmien ja tekoälyn tunnistaminen](#).
- ▶ Sisältyykö se käytännön esimerkkien luetteloon? (Katso [liite C](#) ja/tai komission laatima luettelo, kun se on saatavilla (6 artiklan 4 kohta)).
- ▶ Katso tietokannan osio B. Järjestelmän tarjoajalla on velvoite rekisteröidä sekä itsensä että järjestelmä tietokantaan 49 artiklan mukaisesti.

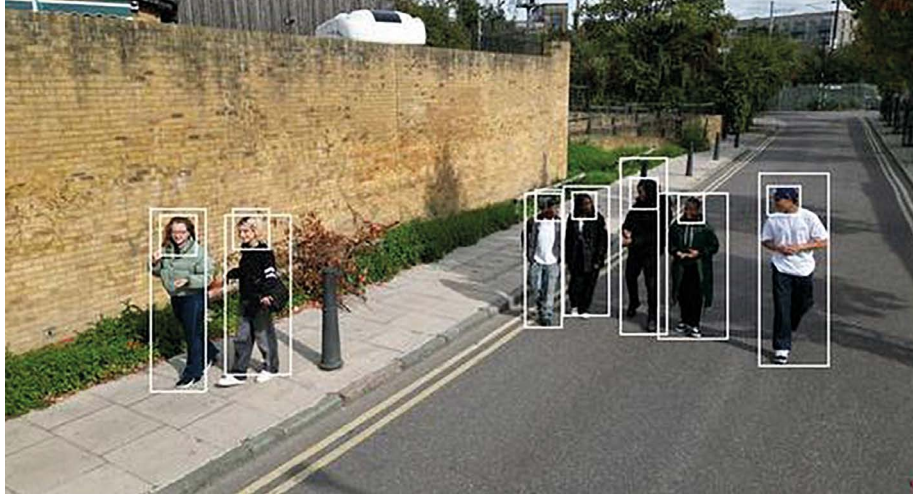
Epäilty kielletty järjestelmä

Tietyt käytännöt ovat kiellettyjä tekoälyasetuksen nojalla (katso [liite J – Kielletyt tekoälyyn liittyvät käytännöt](#)).

Tapaukset, joissa yhdenvertaisuuselin kohtaa kielletyn järjestelmän tai käytännön:

- ▶ Koska nämä käytännöt ovat kiellettyjä, käyttö itsessään rikkoo EU:n lainsäädäntöä. Asianmukaiselle markkinavalvontaviranomaiselle on ilmoitettava asiasta välittömästi riippumatta siitä, voidaanko syrjintätapausta osoittaa.
- ▶ Lisäksi, kun yhdenvertaisuuselin toteaa, että tähän luetteloon tällä hetkellä sisällymätön käytäntö loukkaa perusoikeuksia, sen on koottava asianmukainen näyttö käytännöstä ja toimitettava raportit jäsenvaltion toimivaltaisille viranomaisille ja komissiolle (katso [vaihe 4.3](#)).

Kiellettyihin käytäntöihin liittyvät tapaukset voivat myös sisältää suuririskisiä järjestelmiä ja/tai aiheuttaa syrjintää, ja yhdenvertaisuuselimen on päätettävä, tarvitaanko syrjintään liittyviä lisätoimia.



Vaihe 2

Tiedonkeruu tekoäly- tai algoritmijärjestelmästä syrjinnän tunnistamiseksi

Vaiheessa 2 tunnistetaan saatavilla tai käytettävissä olevat tiedot, jotka liittyvät sekä järjestelmään että syrjinnän osoittamisen todennäköisyyteen. Siinä annetaan myös ohjeita mahdollisista lähteistä ja tiedonkeruusta.

Vaihe 2 koostuu seuraavista alivaiheista.

Kuva 3. Vaihe 2 – Tiedonkeruu syrjinnän tunnistamiseksi

VAIHE 2		Tiedonkeruu tekoäly- tai algoritmijärjestelmästä syrjinnän tunnistamiseksi	
2.1		Algoritmijärjestelmistä saatavilla olevat tiedot	
2.1.1 Kantelijan antamat tiedot ▶ Haastattelut ▶ Kantelijalta saadut asiakirjat ▶ Rekisteröidyn pyyntö saada pääsy tietoihin (DSAR)	2.1.2 Julkisesti saatavilla olevat tiedot ▶ Vastaajan ulkoinen viestintä ▶ Olemassa oleva oikeuskäytäntö ▶ Muut lähteet	2.1.3 Vastaajalta tai muilta osapuolilta saadut tiedot ▶ Vastaajalta pyydetty tiedot – Tietosuoja koskeva vaikutustenarviointi (DPIA) – Ihmisoikeus- tai perusoikeusvaikutusten arviointi (HRIA/FRIA) – Yhdenvertaisuus- ja sukupuolivaikutusten arviointi – Tekoälyasetuksen mukainen dokumentaatio ▶ Tilasto- tai kyselytiedot ▶ Muut tuoteturvallisuus-asiakirjat	

2.2 Lisätietoa suuririskisistä tekoälyjärjestelmistä			
2.2.1 Kantelijan antamat lisätiedot ► 86 artiklaan perustuva pyyntö: oikeus selitykseen	2.2.2 Julkisesti saatavilla olevat tiedot ► Tekoälyasetuksen suuririskisten tekoälyjärjestelmien tietokanta	2.2.3 Vastaajalta tai muilta osapuolilta saadut lisätiedot ► Tekoälyasetuksen mukainen dokumentaatio ► FRIA ► DPIA	2.2.4 Markkinavalvontaviranomaiselta saatu ilmoitus tai viran puolesta (<i>ex officio</i>) tehtävä tutkinta

Vaikka yhdenvertaisuuselin ei olisi 77 artiklan mukainen viranomainen ja/tai järjestelmää ei olisi tunnistettu suuririskiseksi, vaihetta 2.2 (esimerkiksi yhdenvertaisuusvaikutusten arviointia ja tilasto- tai kyselytietoja) voidaan silti käyttää viitekehyksenä, jonka avulla yhdenvertaisuuselin voi pyytää vastaavia tietoja käyttöönottajalta tai tarjoajalta tutkinta- tai tiedonkeruuvaltuuksiensa puitteissa ja arvioida [vaiheessa 3](#) annettuja vastauksia tai niiden puutetta. On kuitenkin huomattava, ettei vastaajilla ole tekoälyasetuksen mukaan velvoitetta toimittaa tällaisia asiakirjoja näissä tilanteissa (velvoite saattaa kuitenkin olla olemassa muun lainsäädännön, kuten tuoteturvallisuus- tai kuluttajansuojalainsäädännön, nojalla).

Vaiheessa 2 kerätty näyttö analysoidaan vaiheessa 3. Käytännössä nämä vaiheet suoritetaan yleensä yhdessä.

Vaiheeseen 2 mennessä on tietyllä varmuudella tunnistettu, että tarkasteltavaan tapaukseen liittyy algoritmi- tai tekoälyjärjestelmä, ja se on mahdollisesti luokiteltu suuririskiseksi tekoälyjärjestelmäksi.³⁰ Seuraava vaihe on etsiä tietoa tunnistetusta järjestelmästä. Tämä voi tukea syrjinnän myöhempää tunnistamista [vaiheessa 3](#).

Lähteet luokitellaan kolmeen eri luokkaan.

1. Tiedot, jotka kantelija voi antaa yhdenvertaisuuselimelle. Tällaiset tiedot voivat olla kantelijoiden saatavilla tai käytettävissä kyseiseen prosessiin liittyvän henkilökohtaisen kokemuksen, vastaajan kanssa tapahtuneen viestinnän ja ensisijaisesti yleisen tietosuojaa-asetuksen ja tekoälyasetuksen mukaisen tiedonsaantioikeuden kautta.
2. Muita tietoja voi olla julkisesti saatavilla.
3. Tiedot, joita yhdenvertaisuuselin voi pyytää vastaajalta kansalliseen tai unionin lainsäädäntöön perustuvien tutkinta- ja tiedonkeruuvaltuuksiensa nojalla, mukaan lukien EU:n tekoälyasetuksen mukaiset valtuudet.

On muistettava, että tietoja voidaan jakaa tai pyytää myös oikeudenkäyntiä edeltävän viestinnän tai oikeudenkäyntimenettelyn aikana.

³⁰ Jos tekoäly- tai algoritmijärjestelmän tunnistaminen ei ole mahdollista, on lopetettava tämän käytännön käyttö ja jatkettava sen sijaan tavallisilla menettelytaivoilla.

Huomautus: vaiheen 2 ei ole tarkoitus olla tyhjentävä; saatavilla voi olla myös muuntyyppisiä tietoja tai tiedonlähteitä. Kansalliset oikeudelliset kehykset, mukaan lukien tiedonvälityksen vapautta koskeva lainsäädäntö tai asiakirjojen avoimuutta koskevat säännöt, voivat antaa yhdenvertaisuuselimille arviointimenetelmässä kuvattuja valtuuksia kattavampia tiedonkeruu- tai tutkintavaltuuksia. Tiedonsaantia voidaan tukea myös yhdenvertaisuuselinten normeja koskevien direktiivien uusilla selvitysvaltuuksilla (katso johdanto ja [vaihe 4](#)).

Tiedonhankinnan yleisiä esteitä

Tiedonhankintastrategioihin, kuten tiedonvälityksen vapautta koskeviin pyyntöihin, voi liittyä haasteita ja rajoituksia. Argumentit voivat koskea erityisesti luottamuksellisuutta ja operatiivisia vaatimuksia. Esimerkiksi Ranskassa kansalaisjärjestöjen esittämä tiedonvälityksen vapautta koskeva pyyntö saada selvyyttä perhe-etuksien myöntämisestä vastaavan sosiaaliviraston (CNAF) käyttämästä riskipisteytysjärjestelmästä johti siihen, että vain aiempien mallien (eli ei sillä hetkellä käytetyn mallin) lähdekoodi ja käytettyjen muuttujien luettelot julkaistiin rajoitetusti (Euroopan neuvosto, 2025a; *La Quadrature du Net* ja *muut v. Premier ministre and Ministère de la Culture* 2024; katso myös Big Brother Watch, 2025).

Asiassa *Kelly v. National University of Ireland* (C-104/10) kantaja väitti kokeneensa sukupuoleen perustuvaa syrjintää tapauksessa, jossa häneltä evättiin pääsy ammatilliseen koulutusohjelmaan, ja pyysi oppilaitokselta tietoja muiden hakijoiden pätevyydestä. Euroopan unionin tuomioistuim (EUT) totesi, että unionin johdettu lainsäädäntö ei anna tällaista yksilöllistä tiedonsaantioikeutta. EUT:n mukaan kansallisten tuomioistuinten on kuitenkin päätettävä, onko näiden tietojen julkistaminen tässä tapauksessa tarpeen sovellettavan lainsäädännön eli direktiivin 97/80/EY tavoitteiden toteutumiseksi.

EUT voi tulevaisuudessa vastaavasti tulkita syrjimättömyysdirektiivien asiaankuuluvia säännöksiä varmistaakseen tehokkaan oikeusturvan syrjintää vastaan tavalla, joka helpottaa kantajien tiedonsaantia jo *prima facie* -tapausta edeltävässä vaiheessa (Farkas ja O'Farrell, 2015).

Voi olla hyödyllistä ylläpitää helposti hallittavaa käytettyjen lähteiden luetteloa, josta voidaan hakea tietoja. Tämä voi auttaa tunnistamaan syrjintään liittyviä kuvioita ja säästää tapausten käsittelijöiden arvokasta aikaa. Kirjallisuuskatsausten otsikot voivat olla esimerkiksi seuraavanlaisia:

- ▶ lähde (mukaan lukien linkki)
- ▶ avainsanat (esimerkiksi sijaismuuttujaan liittyvä syrjintä tai vinoumien lieventäminen)
- ▶ yhteenveto
- ▶ merkityksellisyys (esimerkiksi kasvontunnistusjärjestelmän havaittu syrjintä).

2.1. Algoritmijärjestelmät

2.1.1. Kantelijan antamat tiedot

Kantelijalla on usein tietoja, jotka ovat erittäin merkityksellisiä mahdollisen syrjinnän tunnistamisessa. Tällaiset tiedot voivat olla kantelijoiden saatavilla tai käytettävissä kyseiseen prosessiin liittyvän henkilökohtaisen kokemuksen, vastaajan kanssa tapahtuneen viestinnän ja ensisijaisesti yleisen tietosuoja-asetuksen mukaisen tiedonsaantioikeuden kautta (katso alta tekstiruutu).

Kun tapausta käsitellään osana viran puolesta (*ex officio*) tehtävää tutkintaa tai markkinavalvontaviranomaisen tekemän ilmoituksen vuoksi, tapauksessa ei ole varsinaista kantelijaa. Tiedonkeruussa on huomioitava seuraavat seikat.

- ▶ Tapaukseen voidaan ottaa mukaan muiden/vanhempien/ratkaisemattomien valitusten kantelijoita. Voidaan myös selvittää, onko valitus jo tehty toiselle elimelle/taholle.
- ▶ Tarvittaessa voidaan ehdottaa yleisen tietosuoja-asetuksen mukaisen tiedonsaantioikeuden kollektiivista käyttöä suuririskisissä tapauksissa.³¹

Yleisen tietosuoja-asetuksen avoimuusvelvoitteet ja tietoja koskevat oikeudet

GDPR sisältää *ex ante*-avoimuusvelvoitteet ja *ex post*-tiedonsaantioikeudet, joiden avulla rekisteröidyt voivat saada tietoa henkilötietojensa oikeudenmukaisesta käytöstä.

Ex ante

- ▶ Yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan ja johdanto-osan kappaleen 60 mukaan rekisteröidyn henkilötietoja on käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi ja rekisteröidylle on ilmoitettava tällaisesta käsittelystä ja sen tarkoituksista. Rekisterinpitäjän on toimitettava rekisteröidylle lisätiedot, jotka ovat tarpeen asianmukaisen ja

31. Vaikka yleinen tietosuoja-asetus, tekoälyasetus ja direktiivi lainvalvontatarkoituksessa käsiteltävien henkilötietojen suojasta tarjoavat rajoitettuja mahdollisuuksia kollektiiviseen edustukseen, tutkijat ovat väittäneet, että yksilöiden oikeuksien kollektiivinen käyttö voi silti olla hyödyllistä (Mahieu, Asghari ja van Eeten, 2018). Useat henkilöt voivat esimerkiksi lähettää tiedonsaantipyyntöjä, ja tämän tuloksena saadut tiedot voidaan sitten jakaa luotettavalle välittäjälle datalahjoituksina. Tällaiset kollektiiviset toimet yksilöiden kautta voivat auttaa luomaan laajemman tietopohjan tiettyjen toimijoiden tai sektoreiden tiedonkäytöstä. Vastaavasti rekisteröityjen tai henkilöiden, joihin vaikutukset kohdistuvat, kollektiivinen – mutta yksilöllinen – yleisen tietosuoja-asetuksen 15 ja 22 artiklan mukaisen tiedonsaantioikeuden tai tekoälyasetuksen 86 artiklan mukaisen oikeuden saada selitys käyttö voi tarjota keinoja kattavampien tietojen saamiseksi tekoälyjärjestelmien toiminnasta. Tekoälyä koskevan digitaalialan koontiasetuksen ehdotettujen muutosten, jotka koskevat yleisessä tietosuoja-asetuksessa kuvattua oikeutta saada pääsy tietoihin, myötä tiedonsaantipyyntöjen tehokkuus sekä yksilöllisillä että kollektiivisilla avoimuutta koskevilla keinoilla voi kuitenkin heikentyä merkittävästi. Katso lisätietoja jäljempää kohdasta [Rekisteröidyn pyynnön saada pääsy tietoihin \(DSAR\) tekeminen ja vastauksen saaminen yleisen tietosuoja-asetuksen 15 artiklan mukaisesti](#).

läpinäkyvän käsittelyn varmistamiseksi, ottaen huomioon henkilötietojen käsittelyn erityiset olosuhteet ja asiayhteys.

- Yleisen tietosuoja-asetuksen 13 ja 14 artiklan mukaan rekisteröidylle on annettava tiedot rekisterinpitäjän identiteetistä ja yhteystiedoista, henkilötietojen käsittelyn tarkoituksista sekä käsittelyn oikeusperusteesta, kyseessä olevista henkilötietoryhmistä, kun tietoja saadaan kolmansilta osapuolilta tai yleisesti saatavilla olevista lähteistä, sekä automaattisen päätöksenteon, muun muassa profiloinnin, olemassaolosta.³²

Nämä *ex ante* -tiedot ovat tyypillisesti luonteeltaan yleisempiä ja sisältyvät usein tietosuojailmoituksiin tai -selosteisiin.

Ehdot täyttävä ADM

- Yleisen tietosuoja-asetuksen 13 artiklan 2 kohdan f alakohdan ja 14 artiklan 2 kohdan g alakohdan mukaan rekisteröidyille on nimenomaisesti ilmoitettava yleisen tietosuoja-asetuksen 22 artiklassa kuvatun pelkästään automaattisen päätöksenteon, kuten profiloinnin, olemassaolosta sekä ainakin näissä tapauksissa merkityksellisistä tietojen käsittelyyn liittyvästä logiikasta samoin kuin kyseisen käsittelyn merkittävyys ja mahdolliset seuraukset rekisteröidylle.

Pelkästään automaattinen päätöksenteko on sallittua yleisen tietosuoja-asetuksen 22 artiklan 2 kohdan mukaan vain, jos päätös

- on välttämätön rekisteröidyn ja rekisterinpitäjän välisen sopimuksen tekemistä tai täytäntöönpanoa varten
- on hyväksytty rekisterinpitäjään sovellettavassa unionin oikeudessa tai jäsenvaltion lainsäädännössä
- perustuu rekisteröidyn nimenomaiseen suostumukseen. Tämän perusteella yhdenvertaisuuselinten tulisi myös voida tutustua sopimuksen asiaankuuluviin kohtiin, käsittelyn tai suostumuksen oikeuttavaan lainsäädäntöön sekä siihen, mihin suostumus tarkalleen ottaen on annettu esimerkiksi allekirjoitetussa kirjallisessa ilmoituksessa, sähköisellä lomakkeella tai sähköpostiviestissä.

Ex post

- Yleisen tietosuoja-asetuksen 15 artiklan mukaan rekisteröidyillä on oikeus pyytää pääsyä henkilötietoihinsa, mukaan lukien tietoja kyseessä olevista henkilötietoryhmistä, käsittelyn tarkoituksista, vastaanottajista tai vastaanottajaryhmistä, joille henkilötietoja on luovutettu tai on tarkoitus luovuttaa, sekä automaattisen päätöksenteon, kuten profiloinnin, olemassaolosta.

Ehdot täyttävä ADM

- Yleisen tietosuoja-asetuksen 15 artiklan h alakohdan mukaan, jos tapauksessa on kyse pelkästään automaattisesta päätöksenteosta, muun muassa 22 artiklassa tarkoitettusta profiloinnista, rekisteröidyillä on myös oikeus pyytää

32. Konsensus siitä, että tämä koskee myös muita kuin ehdot täyttäviä ADM-järjestelmiä, koska molempien artikloiden ja asetuksen 2016/679 johdanto-osan kappaleen 60 mukaan rekisterinpitäjien on ilmoitettava rekisteröidylle käsittelyn tarkoituksista, vaikuttaa voimistuvan (Barros Vale ja Zanfir-Fortuna, 2022: 16).

näissä tapauksissa merkitykselliset tiedot käsittelyyn liittyvästä logiikasta samoin kuin kyseisen käsittelyn merkittävyydestä ja mahdollisista seurauksista rekisteröidylle.

Euroopan tietosuojaneuvosto kannustaa rekisterinpitäjiä ”hyvän käytäntönä” antamaan merkityksellistä tietoa käytetystä logiikasta ja selittämään automaattisen päätöksenteon ja profiloinnin merkityksen ja mahdolliset seuraukset myös silloin, kun ADM-järjestelmä ei täytä ehtoja (Barros Vale ja Zanfir-Fortuna, 2022: 16).

Huomautus: kansallisilla lainkäyttöalueilla voi olla asiakirjojen jakamista koskevia lisäoikeuksia. Esimerkiksi Ruotsissa henkilöllä, joka hakee työpaikkaa, ylennystä tai harjoittelumahdollisuutta mutta ei tule valituksi, on oikeus pyytää ja saada työnantajalta kirjallista tietoa valitun henkilön koulutuksesta, työkokemuksesta ja muista pätevyyksistä, jotta pätevyysiä voidaan vertailla (Ruotsin syrjintälainsäädäntö, pykälä 4).

Jos yleinen tietosuoja-asetus ei kata kyseessä olevaa maata, on sovellettava kansallisen lainsäädännön säännöksiä.

Keskeisiä tapauksia: SCHUFA Holding (2023) ja CK v. Dun & Bradstreet Austria GmbH ja Magistrat der Stadt Wien (2025)

(Hakasulkeissa olevat numerot viittaavat päätöksen kohtiin.)

Automaattisen järjestelmän mahdollinen käyttö ja rekisteröidylle annettavat tiedot ovat aiheuttaneet ongelmia yleisen tietosuoja-asetuksen yhteydessä, kun tiettyjä säännöksiä sovelletaan ”pelkästään automaattiseen käsittelyyn, kuten profilointiin” (22 artikla). Jotta 22 artiklaa voidaan soveltaa, kolmen ehdon on täytyttävä.

- ▶ Tapauksessa tulee olla ”päätös” (katso johdanto-osan kappale 71, joka osoittaa tämän laajan soveltamisalan ja sisältää esimerkkejä verkossa tehtävän luottihakemuksen automaattisesta hylkäämisestä ja sähköisen rekrytoinnin käytännöistä ilman ihmisen osallistumista).
- ▶ Päätöksen on perustuttava ”pelkästään automaattiseen käsittelyyn” (kuten profilointiin).
- ▶ Tällä pelkästään automaattiseen käsittelyyn perustuvalla päätöksellä tulee olla rekisteröityä ”koskevia oikeusvaikutuksia”, tai sen tulee ”vaikuttaa häneen vastaavalla tavalla merkittävästi”.

Kun nämä ehdot täyttyvät, automaattista päätöksentekojärjestelmää käyttävien organisaatioiden on kyettävä antamaan rekisteröidylle ”merkitykselliset selitykset... tehdyn päätöksen pääkohdista”. Tämä sanamuoto vastaa tekoälyasetuksen 86 artiklan mukaista oikeutta selitykseen.

SCHUFA Holding

Asiassa C-634/21 SCHUFA Holding (pisteyttäminen) Euroopan unionin tuomioistuimien käsitteli tapausta, jossa yksityinen yhtiö tarjosi luottokelpoisuusarvioiteja sopimuskumppaneilleen, kuten pankeille. Luottokelpoisuuspäätöksiä varten henkilöiden ominaisuuksia vertailtiin ryhmään, joka muodostui muista vastaavaisista ominaispiirteistä omaavista ja tietyllä tavalla toimineista henkilöistä. Sitten

tehtiin matemaattisten ja tilastollisten menetelmien avulla pisteytys, joka koski henkilön lainan takaisinmaksun kaltaisen tulevan toiminnan todennäköisyyttä tämän henkilön tiettyjen ominaispiirteiden perusteella [14].

Pankki (kolmas osapuoli) ei suostunut myöntämään lainaa kantajalle (OQ) SCHUFA:n pankille toimittamien kielteisten tietojen vuoksi. OQ pyysi SCHUFA:a toimittamaan tietoja tallennetuista henkilötiedoista ja poistamaan niistä hänen mielestään virheelliset tiedot [15].

Vastauksena tähän pyyntöön SCHUFA antoi OQ:lle tiedoksi hänen pistemääränsä tason ja selitti pääpiirteittäin, miten pistemäärä lasketaan. Yritys kieltäytyi kuitenkin liikesalaisuuteen vedoten paljastamasta laskennassa huomioon otettuja tekijöitä ja niiden painotusta. Lopuksi SCHUFA totesi, että sen toiminta rajoittui tietojen toimittamiseen pankille, ja että pankki teki varsinaisen päätöksen. Käytännössä yhtiö siis väitti, ettei pistemäärä ollut ”pätös” [16].

Vastauksena kolmeen esitettyyn kysymykseen tuomioistuimien totesi seuraavaa.

- ▶ Päätös: päätöksen käsite on riittävän laaja, jotta siihen voi sisältyä henkilön luottokelpoisuuden laskennan tulos, joka perustuu todennäköisyysarvoon, joka koskee tämän henkilön kykyä täyttää maksusitoumukset tulevaisuudessa [47].
- ▶ ”Pelkästään automaattiseen käsittelyyn, kuten profilointiin” perustuva: oli riidatonta, että SCHUFA:n toiminta vastasi profiloinnin määritelmää, joten ehto täyttyi.
- ▶ Henkilöä ”koskevia oikeusvaikutuksia” tai vaikuttaa henkilöön ”vastaavalla tavalla merkittävästi”: Liian alhaisesta todennäköisyysarvosta seuraa miltei kaikissa tapauksissa, että pankki kieltäytyy myöntämästä henkilölle haettua lainaa. Koska arvo toimi kolmannen osapuolen toiminnan ”keskeisenä perustana”, myös tämä ehto täyttyi [48].

Tämän vuoksi tuomioistuimien totesi, että ”olosuhteissa, joissa luottotietopalveluja tarjoavan yrityksen määrittämä ja pankille tiedoksi annettu todennäköisyysarvo vaikuttaa olennaisesti luoton myöntämiseen, tämän arvon määrittämisestä on pidettävä itsessään päätöksenä, jolla on rekisteröityä ’koskevia oikeusvaikutuksia tai joka vaikuttaa häneen vastaavalla tavalla merkittävästi’ yleisen tietosuoja-asetuksen 22 artiklan 1 kohdassa tarkoitetulla tavalla”.

Tuomioistuimien toisti myös tarpeen seuraaviin:

- ▶ profiloinnin aiheuttamien syrjintäriskien ehkäisy
- ▶ asianmukaisten matemaattisten tai tilastollisten menetelmien käyttö profiloinnissa
- ▶ sellaisten teknisten ja organisatoristen toimenpiteiden toteuttaminen, jotka soveltuvat erityisesti varmistamaan, että henkilötietojen virheellisyyteen johtavat tekijät korjataan ja virheriski minimoidaan
- ▶ tietojen turvaaminen.

Merkittävää on, että tuomioistuimien totesi myös, etteivät jäsenvaltiot voi antaa yleisen tietosuoja-asetuksen nojalla säännöstöä, jossa sallitaan profilointi 5 artiklassa (henkilötietojen käsittelyä koskevat periaatteet) ja 6 artiklassa (käsittelyn lainmukaisuus) asetettujen vaatimusten vastaisesti, tai sivuuttaa unionin tuomioistuimen

vaatimuksia varsinkaan vahvistamalla lopullisesti, mikä on kyseessä olevien oikeuksien ja intressien punninnan tulos [70].

Dun & Bradstreet

Selitysten on oltava sellaisia, että rekisteröity voi ymmärtää päätöksen ja tarvittaessa riitauttaa sen sekä käyttää tietoja koskevia oikeuksiaan. Näitä vaatimuksia ei voida täyttää pelkästään algoritmin kaltaisen monimutkaisen matemaattisen kaavan ilmoittamisella eikä automaattisen päätöksenteon kaikkien vaiheiden yksityiskohtaisella kuvauksella, koska kumpikaan näistä ei ole riittävän tiivis ja ymmärrettävä selitys [58–59].

”Merkityksellisissä tiedoissa automaattiseen päätöksentekoon liittyvästä logiikasta” on kuvattava menettely ja sovellettavat periaatteet siten, että rekisteröity voi ymmärtää, mitä hänen henkilötietojaan on käytetty ja millä tavoin kyseisessä automaattisessa päätöksenteossa. Automaattisen päätöksenteon yhteydessä toteutettavien toimien monimutkaisuus ei voi vapauttaa rekisterinpitäjää selitysvastuusta [61].

Luottoihin liittyvän profiloinnin kontekstissa EUT totesi, että tuomioistuin voisi katsoa riittävän läpinäkyväksi ja ymmärrettäväksi muun muassa sen, että rekisteröidylle ilmoitetaan, missä määrin huomioon otettujen henkilötietojen muuttuminen olisi johtanut erilaiseen lopputulokseen [62]. Tämä ei välttämättä koske kaikkia algoritmijärjestelmiä.

Jos rekisterinpitäjä katsoo, että näitä tietoja ei voida toimittaa paljastamatta kolmannen osapuolen tietoja tai liikesalaisuuksia, rekisterinpitäjän on toimitettava väitetyt suojatut tiedot toimivaltaiselle valvontaviranomaiselle tai tuomioistuimelle, jonka on punnittava kyseessä olevia oikeuksia ja intressejä määrittääkseen asetuksen 15 artiklan mukaisen rekisteröidyn tiedonsaantioikeuden laajuuden.

Nämä kaksi tapausta tarjoavat ohjeita lähestymistavasta, jota EUT voi käyttää harkitessaan, missä määrin ja missä muodossa tietoja on annettava saataville yleisen tietosuojasetuksen nojalla. Tämä voi vastaavasti koskea myös tekoälyasetuksessa kuvattuja selityksiä.

Asianomaisen henkilön haastattelu

Kantelijoilla, jotka tekevät valituksen syrjinnästä yhden tai useamman kielletyn syrjintäperusteen perusteella, on usein merkityksellistä tietoa ominaisuuksista, joita he ovat antaneet vastaajalle joko äskettäin tai aiemmin. Lisäksi voi olla hyödyllistä kerätä muita tietoja henkilön kiellettyihin syrjintäperusteisiin kuuluvista ominaisuuksista ja tilanteista, joissa tietoja näistä ominaisuuksista on saatettu antaa vastaajalle. Muista huomioida myös omat tietosuojavelvoitteesi. Esimerkiksi seuraavanlaisia kysymyksiä voidaan kysyä.

- Milloin olit ensimmäisen kerran ja myöhemmin yhteydessä tähän organisaatioon/viranomaiseen? Jos organisaatioon/viranomaiseen on otettu yhteyttä jo ennen valitukseen liittyvää tapahtumaa, tietoja kiellettyihin syrjintäperusteisiin kuuluvista ominaisuuksista on saatettu antaa tuolloin.

- Pyydettiinkö sinua täyttämään lomakkeita?
- Jos pyydettiin, mitä lomakkeita sinua pyydettiin täyttämään?
- Tarkastele [kiellettyjen syrjintäperusteiden](#) luetteloa. Pyydetiinkö sinua antamaan tietoja tai rastittamaan ruutuja, jotka liittyivät johonkin näistä ominaisuuksista?
- Tarkastele yleisten sijaismuuttujien luetteloa, joka on kuvattu [liitteessä E](#). Pyydetiinkö sinua antamaan näihin ominaisuuksiin liittyviä tietoja?

Kantelijalta saadut asiakirjat

Merkityksellisiä tietoja voi olla kantelijan saatavilla tai käytettävissä olevissa asiakirjoissa. Näitä voivat olla esimerkiksi seuraavat:

- kantelijan toimittamat asiakirjat (hakemuslomakkeet, viestintä, pyyntö saada pääsy tietoihin tai muut pyynnöt)
- vastaajan kantelijalle antamat asiakirjat (vastaajan ja kantelijan väliset sopimukset liitteineen, tietojen käsittelyä koskevat tiedot tai tietosuojailmoitukset sekä sisäinen viestintä, mukaan lukien sopimuksia koskevat päivitykset).

Rekisteröidyn pyynnön saada pääsy tietoihin (DSAR) tekeminen ja vastauksen saaminen yleisen tietosuoja-asetuksen 15 artiklan mukaisesti

Rekisteröidyillä on oikeus pyytää rekisterinpitäjältä (yleensä järjestelmän käyttöönottajalta) pääsyä henkilötietoihinsa yleisen tietosuoja-asetuksen 15 artiklan nojalla. Asianmukaisesti käsitellyt DSAR-pyyntöjen vastaukset voivat sisältää tietoja (katso lisätietoja [vaiheesta 3](#)), jotka ovat erittäin merkityksellisiä nimenomaan kyseisen henkilön tapauksessa, mukaan lukien seuraavia:

- käsiteltävät henkilötietoluokat ja näiden tietojen digitaaliset kopiot
- käsittelyn tarkoitukset
- henkilötietojen vastaanottajat tai vastaanottajaryhmät
- automaattisen päätöksenteon ja/tai profiloinnin käyttö ja merkityksellisiä tietoja siihen liittyvästä logikasta sekä tällaisen käsittelyn merkityksestä ja suunnitelluista seurauksista rekisteröidylle.

Jos kantelija ei ole vielä tehnyt DSAR-pyyntöä, on suositeltavaa kannustaa häntä tekemään se ennen valituksen tai tutkimuksen jatkamista. Vaikka DSAR-pyyntöjen tekemiselle ei ole virallisia vaatimuksia, on suositeltavaa tehdä pyyntö kirjallisesti ja säilyttää siihen liittyvät tiedot (kopiot kaikista sähköposteista tai kirjeistä, postilla tai muuten toimitetut asiakirjat sekä kuvakaappaus, jos käytetään verkkolomaketta, portaalia tai asiakaspalvelukanavaa). Katso malli [liitteestä A](#).

DSAR-pyyntöihin liittyvien yleisen tietosuoja-asetuksen velvoitteiden noudattamatta jättäminen on yleistä. Siksi monissa tapauksissa pyyntöön ei vastata, vastaus saadaan viiveellä tai pyynnön tekemisen jälkeen annetaan riittämättömiä tai epätäydellisiä tietoja. Rekisteröityjen oikeuksiaan käyttävien kantelijoiden tulisi olla varautuneita mahdolliseen jatkoviestintään, kuten muistutusten ja lisäselvityspyyntöjen lähettämiseen organisaatiolle. Jos tapaukseen liittyy korkeita riskejä, voidaan harkita yhteistyötä asiaankuuluvan kansallisen tietosuojaviranomaisen kanssa (katso kohta [Eri sektoreiden välinen yhteistyö](#)).

Tekoälyä koskeva digitaalialan koontiasetus tuo muutoksia rekisteröidyn oikeuteen saada tietoja yleisen tietosuoja-asetuksen nojalla. Ehdotettua muutosta yleisen tietosuoja-asetuksen 12 artiklan 5 kohtaan³³ on kritisoitu (Skiotyte ja Sadauskaitė, 2026). Jos muutos hyväksytään, se antaisi rekisterinpitäjille mahdollisuuden kieltäytyä DSAR-pyyntöistä tai periä niistä maksuja, jos pyyntöjen katsotaan olevan kohtuuttomia tai niillä tavoitellaan muita kuin tietosuojaan liittyviä tarkoituksia. Tämän ei pitäisi vaikuttaa hyväksyttäviin, rekisteröityjen tietoihin liittyvien oikeuksien käyttämistä koskeviin pyyntöihin.

2.1.2. Julkisesti saatavilla olevat tiedot

Vastaajan ulkoinen viestintä

Vastaaja voi antaa asiaankuuluvia tietoja verkkosivustollaan tai alustallaan, kuten usein kysytyissä kysymyksissä, käyttöehdoissa tai tietosuojailmoituksissa, sovellettavien yleisen tietosuoja-asetuksen avoimuusvelvoitteiden mukaisesti (katso edeltä yleisen tietosuoja-asetuksen avoimuusvelvoitteita ja tietoja koskevia oikeuksia käsittelevä tekstiruutu).

Huomiota on kiinnitettävä erityisesti järjestelmän tarkoitukseen, tietojenkäsittelyn tarkoituksiin, käsiteltävien tietojen tyyppeihin, mukaan lukien viittaukset arkaluonteisiin tietoihin – joita kutsutaan myös henkilötietojen erityisryhmiksi – ja kaikkiin (ehdot täyttäviin) ADM-järjestelmiin tai profilointiin, niiden logiikkaan ja seurauksiin liittyviin tietoihin. Nämä saattavat viitata algoritmien tai kiellettyjen syrjintäperusteiden käyttöön (katso lisätietoja [vaiheista 3.2 ja 3.3](#)).

Joissakin maissa (kuten Suomessa) julkishallinnolla on tiedotusvelvoitteita, joiden perusteella ADM-järjestelmien käyttöä koskevat tiedot on julkaistava kyseisten tahojen verkkosivustoilla ja niistä on ilmoitettava päätöksenteon yhteydessä. Systemaattisia kansallisia tai kansainvälisiä luetteloita ei kuitenkaan juurikaan ole, vaikka paikallisia aloitteita tekoäly- ja ADM-sovellusten tietokantojen luomisesta on tehty (esimerkiksi Belgiassa ja Suomessa). Tämän vuoksi yhdenvertaisuuselimillä on haasteita toteuttaa algoritmiseen syrjintään liittyvien tapausten tutkimista, valvomista, tunnistamista ja haastamista sekä uhrien tukemista koskevaa toimeksiantoaan (Euroopan neuvosto, 2025a).

Olemassa oleva oikeuskäytäntö

On tutustuttava oikeuskäytäntöön, joka koskee joko samankaltaisia tekoäly- tai algoritmijärjestelmiä tai automaattisen päätöksenteon prosesseja. Tämä voi sisältää kansallisen, eurooppalaisen (mukaan lukien Euroopan ihmisoikeustuomioistuimen ja Euroopan unionin tuomioistuimen) ja ulkomaisen oikeuskäytännön, koska algoritmijärjestelmät

33. Johdanto-osan kappale 35, 3 artikla, ehdotus, Euroopan parlamentin ja neuvoston asetus asetusten (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 ja direktiivien 2002/58/EY, (EU) 2022/2555 ja (EU) 2022/2557 muuttamisesta digitaalisen lainsäädäntökehyksen yksinkertaistamiseksi sekä asetusten (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868 ja direktiivin (EU) 2019/1024 kumoamisesta (digitaalialan koontiasetus). Saatavilla osoitteessa: [EUR-Lex - 52025PC0837](#).

ja -alustat toimivat usein samankaltaisen logiikan ja toistuvien kuvioden mukaisesti eri maissa.

Koska EU:n tekoälyn ja algoritmien sääntelyä koskeva oikeuskäytäntö on vielä varhaisessa vaiheessa, voidaan harkita myös yleiseen tietosuoja-asetukseen liittyvän oikeuskäytännön tarkastelua erityisesti automaattiseen päätöksentekoon liittyvissä tapauksissa, sillä tämä voi tarjota käsittelyä tukevia suuntaviivoja. Seuraavien tietojen tarkastelua voidaan harkita.

- ▶ Tietokannat, kuten [EUR-Lexin EU:n oikeuskäytäntöä koskeva tietokanta](#) tai [Euroopan unionin perusoikeusviraston oikeudellinen tietokanta](#), jotka sisältävät EUT:n tai tuomioistuinten käsittelemiä tapauksia. Hakuja voi tehdä käyttämällä avainsanoja, kuten ”tekoäly”, ”automaattinen päätöksenteko”, ”profilointi” ja ”luottopisteytys”. Näiden avulla voidaan tarkastella olemassa olevia tuomioita tai seurata vireillä olevia kansallisten tuomioistuinten EUT:lle tekemiä ennakkoratkaisupyyntöjä, jotka liittyvät tekoälyasetuksen tai yleisen tietosuoja-asetuksen olennaisiin näkökohtiin.
- ▶ Kun tarvitaan erityisesti tekoäly- tai algoritmijärjestelmiin liittyviä tietokantoja, voidaan tutustua myös [oikeuskäytäntöä koskevaan Tech Litigation -tietokantaan](#). Se sisältää tietoja automaattisia järjestelmiä vastaan nostetuista kanteista, kuten kansallisten ja kansainvälisten tuomioistuinten sekä tietosuojaviranomaisten antamia tuomioita, päätöksiä ja lausuntoja. Lisäksi [Ethical Tech Initiative -hankkeen DAIL- eli Database of AI Litigation -tietokantaan](#) on kerätty tekoäly- ja algoritmijärjestelmiin liittyviä yhdysvaltalaisia oikeudenkäyntitietoja. Se voi tarjota arvokasta tietoa tietänyttyypisten teknologioiden algoritmiseen syrjintään, systeemiin puutteisiin ja syrjintäriskeihin liittyvistä uusista oikeudenkäyntitrendeistä. Tietokanta sisältää myös tietoja yhdysvaltalaisista yrityksistä, jotka toimivat Euroopan unionissa joko vastaavien tekoälyjärjestelmien tarjoajina tai rekisterinpitäjinä (kuten Clearview AI).
- ▶ Jotkut kansalaisjärjestöt ovat alkaneet koota tietokantoja, jotka keskittyvät nimenomaan algoritmiseen syrjintään liittyviin tapauksiin ([Algorithm Watchin ilmoituslomake](#)). Näistä tietokannoista on enemmän hyötyä, jos yhdenvertaisuuselimet osallistuvat niihin raporttimalla omien oikeudenkäyntiensä tai tutkimustensa tuloksista. Tämä on tehtävä noudattaen tietosuojan ja oikeudenkäyntiä varten laaditun aineiston suojan periaatteita.
- ▶ [GDPR Enforcement Tracker -työkalun luettelo yleisen tietosuoja-asetuksen perusteella annetuista sakoista](#) ja [Euroopan tietosuojaneuvoston sakkoja käsittelevä sivusto](#): Yleiskatsaus EU:n tietosuojaviranomaisten yleisen tietosuoja-asetuksen nojalla määräämistä sakoista ja seuraamuksista. Tämä luettelo sisältää tiedot tapaukseen liittyvästä maasta, viranomaisesta, päivämäärästä, sakkojen määrästä, rekisterinpitäjästä/käsittelijästä, sektorista ja tapauksen tyypistä.
- ▶ [Automaattista päätöksentekoa koskeva Automated Decision-Making Under the GDPR -raportti](#): Future of Privacy Forumin raportti: oikeuskäytäntökokoelma automaattisesta päätöksenteosta yleisen tietosuoja-asetuksen nojalla huhtikuuhun 2022 mennessä.
- ▶ Kansalliset oikeuskäytäntötietokannat.

Muut lähteet

Monet erilaiset tietolähteet voivat olla hyödyllisiä algoritmisen syrjinnän tunnistamisessa, tutkimisessa tai osoittamisessa.

- ▶ Euroopan rasismien ja suvaitsemattomuuden vastaisen komission (ECRI) seitsemänneen seurantajakson maakohtaiset raportit, joissa huomioidaan myös tekoäly.
- ▶ Kansalaisjärjestöjen raportit, jotka käsittelevät joko samankaltaisia tekoäly- tai algoritmijärjestelmiä tai samankaltaisia päätöksentekoprosesseja.
- ▶ YK:n valvontaelinten, kuten naisten syrjinnän poistamista käsittelevän komitean (CEDAW), rotusyrjinnän poistamista käsittelevän komitean (CERD), lapsen oikeuksien komitean, kidutuksen vastaisen komitean (CAT), erityisraporttien, maailman terveysjärjestön (WHO) ja taloudellisten, sosiaalisten ja sivistyksellisten oikeuksien komitean, tekemät havainnot.
- ▶ Muiden kansainvälisten elinten, kuten Euroopan turvallisuus- ja yhteistyöjärjestön (Etyj) demokraattisten instituutioiden ja ihmisoikeuksien toimiston (OSCE) ja taloudellisen yhteistyön ja kehityksen järjestön (OECD), tekemät havainnot. Tässä suhteessa OECD:n tekoälyyn liittyvien vaaratilanteiden ja vaarojen rekisteri ([OECD AI Incidents Monitor, näyttöön perustuva tietokanta tekoälyjärjestelmien luotettavuudesta – OECD.AI](#)) voi olla erityisen merkityksellinen.
- ▶ Kansallisten erikoistuneiden elinten, kuten oikeusasiamiehien, yhdenvertaisuuselinten ja kansalaisjärjestöjen, tekemät havainnot.
- ▶ Hallinnolliset rekisterit, kuten kansalliset ja paikalliset väestötietorekisterit.
- ▶ Valitustiedot, kuten poliisilta, syyttäjiltä sekä oikeudenkäyntiasiakirjoista ja -rekistereistä saadut tilastot.
- ▶ Akateeminen ja ad hoc -tutkimus, mukaan lukien EU:n tutkimuslaitosten, kuten Euroopan unionin perusoikeusviraston (FRA) ja Euroopan tasa-arvoinstituutin (EIGE), tekemät havainnot. Myös haku kohdealueen perusteella [MIT AI Risk Repository](#) -arkistosta voi olla hyödyllistä.
- ▶ Oikeuskäytäntöä, politiikkaa ja käytäntöjä koskevien tietojen vertailu eri jäsenvaltioiden välillä ("eurooppalainen konsensus" -tiedot).

2.1.3. Vastaajalta tai muilta osapuolilta saadut tiedot

Kansallisen tai unionin lainsäädännön mukaisia valtuuksia käyttäen pyydetty tiedot

Yhdenvertaisuuselimet voivat pyytää tietoja vastaajilta ja muilta osapuolilta, esimerkiksi järjestelmän käyttöönottajalta tai tarjoajalta (jos tämä on eri organisaatio kuin vastaaja), käyttämällä tutkinta- ja tiedonkeruuvaltuuksiaan asiaankuuluvan lainsäädännön, kuten yhdenvertaisuuselinten normeja koskevien direktiivien täytäntöönpanevien lakien,³⁴ tiedonvälityksen vapautta koskevan lainsäädännön ja kansainvälisten

34. Yhdenvertaisuuselinten normeja koskevien direktiivien 16 artiklan mukaan jäsenvaltioiden on varmistettava, että yhdenvertaisuuselimet voivat toteuttaa syrjintää koskevia riippumattomia selvityksiä (16 artiklan 2 kohta). Lisäksi on varmistettava, että yhdenvertaisuuselimillä on pääsy oikeuksia ja velvollisuuksia koskeviin tilastoihin, jos yhdenvertaisuuselimet katsovat tällaiset tilastot tarpeelliseksi voidakseen laatia kokonaisarvioinnin syrjintätilanteesta kyseisessä jäsenvaltiossa sekä tässä direktiivissä tarkoitetut kertomukset (16 artiklan 3 kohta).

välineiden, kuten Euroopan neuvoston tekoälyä koskevan puiteyleissopimuksen³⁵, nojalla tai tekemällä yhteistyötä kansallisten tietosuojaviranomaisten kanssa.

Tietoja voidaan jakaa myös tutkinnan, oikeudenkäyntiä edeltävän viestinnän tai oikeudenkäyntimenettelyn aikana.

Selvitykset: direkttiivit yhdenvertaisuuselimä koskevistä normeista (8 artikla)

Direktiivien 2024/1499 ja 2024/1500 8 artikla voi vahvistaa yhdenvertaisuuselinten oikeutta saada tietoa. Tämä perustuu erityisesti seuraaviin:

- ▶ Yhdenvertaisuuselinten normeja koskevien direkttiivien 8 artiklan 1 kohdan mukaan jäsenvaltioiden on varmistettava, että yhdenvertaisuuselimillä on valtuudet tehdä selvityksiä siitä, onko direktiiveissä säädettyä yhdenvertaisen kohtelun periaatetta rikottu.
- ▶ Yhdenvertaisuuselinten normeja koskevien direkttiivien 8 artiklan 2 kohdan mukaan jäsenvaltioiden on tarjottava selvityksen tekoa varten kehys, jonka avulla yhdenvertaisuuselimet voivat toteuttaa tutkintatoimenpiteitä. Kyseisellä kehyksellä on erityisesti annettava yhdenvertaisuuselimille
 - tehokkaat oikeudet saada pääsy tietoihin ja asiakirjoihin, jotka ovat tarpeen sen toteamiseksi, onko syrjintää tapahtunut
 - asianmukaiset mekanismit, joiden avulla yhdenvertaisuuselimet voivat tehdä yhteistyötä asianomaisten julkisten elinten kanssa kyseistä tarkoitusta varten.

On tärkeää huomata, että 8 artiklan 3 kohdan mukaan jäsenvaltiot voivat myös antaa nämä valtuudet toiselle toimivaltaiselle elimelle. Tämä voi olla esimerkiksi markkinavalvontaviranomainen. Tällaisessa tapauksessa markkinavalvontaviranomainen voi käyttää 8 artiklan 1 ja 2 kohdan mukaisia valtuuksia. Kun tällainen toimivaltainen elin on saanut selvityksensä päätökseen, sen on annettava yhdenvertaisuuselimelle pyynnöstä tietoja selvityksen tuloksista.

Jos markkinavalvontaviranomaiselle on annettu nämä valtuudet, on tärkeää huomata, että tekoälyasetuksen mukaan tämä edellyttää yhteistyötä yhdenvertaisuuselimen kanssa (79 artiklan 2 kohta).

- ▶ Selvitykset voivat olla erityisen merkityksellisiä ei-suuririskisiä järjestelmiä koskevissa tapauksissa, joissa on osoittautunut vaikeaksi saada asiakirjatodisteita tai joissa epäillään tietyn ihmisryhmän syrjintää, mutta yksittäistapauksissa ei ole riittävästi todisteita.

35. Euroopan neuvoston tekoälyä koskevan puiteyleissopimuksen (2024) mukaan kunkin osapuolen on otettava käyttöön tai pidettävä voimassa toimenpiteet sen varmistamiseksi, että käytössä ovat riittävät avoimuus- ja valvontavaatimukset (8 artikla), sekä varmistettava vastuuvollisuus ja vastuu ihmisoikeuksiin kohdistuvista haitallisista vaikutuksista (9 artikla). 14 artikla erityisesti edellyttää, että kukin osapuoli varmistaa esteettömien ja tehokkaiden oikeussuojakeinojen saatavuuden, mukaan lukien toimenpiteet, joilla varmistetaan, että asiaankuuluvat tiedot merkittävästi ihmisoikeuksiin vaikuttavista tekoälyjärjestelmistä ja niiden merkityksellisestä käytöstä dokumentoidaan ja toimitetaan elimille, joilla on valtuudet tutustua kyseisiin tietoihin, ja tarvittaessa asetetaan soveltuvin osin asianomaisten henkilöiden saataville, jotta asianomaiset henkilöt voivat riitauttaa päätökset ja tehdä valituksen toimivaltaisille viranomaisille.

Huomautus: selvityksiä ei voida aloittaa eikä jatkaa, jos samaan tapaukseen liittyvä oikeudenkäyntimenettely on vireillä. Selvityksiin sovelletaan todennäköisesti kansallista lainsäädäntöä.

Tietosuoja koskeva vaikutustenarviointi (DPIA)

Yleisen tietosuoja-asetuksen 35 artiklan 1 kohdan mukaan rekisterinpitäjän on ennen käsittelyä toteutettava tietosuoja koskeva vaikutustenarviointi (DPIA), jos henkilötietojen käsittely aiheuttaa todennäköisesti käsittelyn luonteen, laajuuden, asiayhteyden ja tarkoitusten perusteella luonnollisen henkilön oikeuksien ja vapauksien kannalta korkean riskin. Tämän vuoksi DPIA-arvioinnit ovat erittäin merkityksellisiä tapauksissa, joissa on kyse automaattisesta päätöksenteosta ja profiloinnista algoritmijärjestelmien avulla (yleinen tietosuoja-asetus, 35 artiklan 3 kohta). Lukuun ottamatta suppeaa joukkoa suuririskisten tekoälyjärjestelmien käyttöönottajia, joilla on tekoälyasetuksen mukainen tietojen julkaisuvelvoite (katso myös DPIA jäljempää vaiheesta 2.2.3), yleisessä tietosuoja-asetuksessa tai tekoälyasetuksessa ei ole lakisääteistä vaatimusta, jonka mukaan käyttöönottajien olisi julkaistava DPIA-arviointi tai toimitettava se yhdenvertaisuuselimelle. Vaikutustenarviointien hallinta jää siis tietosuojaviranomaisten tekemien aloitteiden vastuulle – yhteistyö tietosuojaviranomaisten kanssa voi olla tässä suhteessa merkityksellistä. Tämän ei tule estää yhdenvertaisuuselintä tekemästä tällaisia pyyntöjä. Osa organisaatioista voi suostua toimittamaan DPIA-arvioinnin, jos se on saatavilla – joko yleisen tietosuoja-asetuksen 35 artiklan 3 kohdan nojalla tai vapaaehtoisesti – tai jopa julkaista siitä yhteenvedon. DPIA-arviointia voidaan pyytää myös oikeudenkäyntiä edeltävän viestinnän tai oikeudenkäyntimenettelyn aikana.

Ihmisoikeus- tai perusoikeusvaikutusten arviointi (HRIA/FRIA)

Tekoälyasetuksessa säädetään nimenomaisesti velvoitteesta suorittaa minkä tahansa tyyppinen perusoikeusvaikutusten arviointi (FRIA) vain tietyille suuririskisten tekoälyjärjestelmien käyttöönottajille ja tarjoajille (katso myös perusoikeusvaikutusten arviointi jäljempää vaiheesta 2.2.3). Muille algoritmi- tai tekoälyjärjestelmille tällaista velvoitetta ei tekoälyasetuksen nojalla ole. Tämä ei kuitenkaan estä tarjoajia ottamasta tällaisia välineitä käyttöön vapaaehtoisesti (European Center for Not-for-Profit Law ja Tanskan ihmisoikeusinstituutti, 2025; FRA, 2025) EU:n ja kansallisen tason perusoikeuksien kunnioittamista ja suojelemista koskevan yleisen velvoitteensa perusteella ja keinona parantaa tekoälyyn liittyvien toimijoiden vastuullisuutta tässä suhteessa (Mantelero, 2024).

Ihmisoikeusvaikutusten arviointi (HRIA) on yleisnimitys prosessille ja työkaluille, joilla tunnistetaan, arvioidaan ja käsitellään tuotteiden tai toimien mahdollisia ja todellisia ihmisoikeuksiin kohdistuvia haitallisia vaikutuksia, ja arviointi voidaan toteuttaa useissa eri muodoissa. Euroopan neuvoston kehittämä HUDERIA-menetelmä ja siihen liittyvä malli tarjoavat yhden tavan ihmisoikeusriskien arviointiin (Euroopan neuvosto, 2025c, 2026).

Vastaavasti kehittäjät ovat saattaneet tehdä HRIA- tai FRIA-arvioinnin vapaaehtoisesti ei-suuririskisille tekoälyjärjestelmille – esimerkiksi kehittäjän oman

huoellisuusvelvoitteen tai ihmisoikeussitoumuksen noudattamisen vuoksi tai erilaisten kehysten, kuten YK:n yrityksiä ja ihmisoikeuksia koskevien ohjaavien periaatteiden, perusteella. Kansallinen tai alueellinen lainsäädäntö, politiikka tai käytäntö voi myös edellyttää perus- tai ihmisoikeusvaikutusten arviointien tekemistä ja julkaisua.

Kaikissa näissä tapauksissa yhdenvertaisuuselimet voivat pyytää tällaisten arviointien jakamista osana tiedonkeruuta koskevia valtuuksiaan.

Yhdenvertaisuus- ja sukupuolivaikutusten arviointi

Jos tällaisia arviointeja edellytetään kansallisessa lainsäädännössä, yhdenvertaisuuselimet voivat pyytää niitä. Niiden tekemiseen tai jakamiseen ei kuitenkaan välttämättä ole lakisääteistä vaatimusta.

Tekoälyasetuksen mukainen dokumentaatio

Vaikka järjestelmää ei luokiteltaisi suuririskiseksi, yhdenvertaisuuselimet voivat silti pyytää vastaavia tietoja käyttöönottajalta tai tarjoajalta tutkinta- tai tiedonkeruuvaltuuksiensa puitteissa. Vaikka vastaajilla ei ole oikeudellista velvoitetta laatia ja/tai toimittaa tällaisia asiakirjoja ei-suuririskisten järjestelmien tai muiden kuin tekoälyjärjestelmien tapauksissa, yhdenvertaisuuselimet voivat jäsentää pyyntönsä tekoälyasetuksen tarjoaman kehyksen mukaan ja arvioida vastaajan reaktiota – tai sen puutetta – vastaavasti vaiheissa 3 ja 4.

Tutkimus- ja tilastotiedot

Yhdenvertaisuuselimet voivat toteuttaa erilaisia selvityksiä, kuten otantatutkimuksia, joilla pyritään kartoittamaan syrjintää kohdanneiden ryhmien kokemuksia, tai mielipidetutkimuksia, joilla mitataan ennakkoluulojen esiintyvyyttä, tai saada pääsyn tällaisiin selvityksiin (direktiivit yhdenvertaisuuselimistä koskevista normeista, 16 artikla). Yhdenvertaisuuselimet voivat myös hyödyntää asiaankuuluvia virallisia tilastolähteitä, kuten kansallisten tilastokeskusten EU:n syrjimättömyysdirektiivien puitteissa kokoamia lähteitä, sekä väestönlaskennan ja muiden tärkeiden lähteiden, kuten työvoimatutkimuksen (LFS) ja tulojen ja elinolojen aihealuetta koskevan otantatutkimuksen (SILC), kautta kerättyjä tietoja.

Direktiivit yhdenvertaisuuselimistä koskevista normeista

- ▶ Direktiivien 2024/1499 ja 2024/1500 16 artiklan 2 kohdan mukaan yhdenvertaisuuselimet voivat toteuttaa syrjintää koskevia riippumattomia selvityksiä.
- ▶ Direktiivien 2024/1499 ja 2024/1500 16 artiklan 3 kohdan mukaan jäsenvaltioiden on varmistettava, että yhdenvertaisuuselimillä on pääsy EU:n syrjinnän vastaisten direktiiveistä johtuvia oikeuksia ja velvollisuuksia koskeviin tilastoihin kansallisen lainsäädännön mukaisesti, jos yhdenvertaisuuselimet katsovat tällaiset tilastot tarpeelliseksi voidakseen laatia kokonaisarviointin syrjintätilanteesta kyseisessä jäsenvaltiossa.

Muut tuoteturvallisuuslainsäädännön mukaiset asiakirjat

Kun yritys myy kuluttajalle muita kuin suuririskisiä tuotteita, tapaukseen voidaan soveltaa yleisen tuoteturvallisuusasetuksen³⁶ (GPSR) ja markkinavalvonnasta annetun asetuksen³⁷ mukaisia velvoitteita. Nämä sisältävät esimerkiksi tekoälyasetusta vastaavia velvoitteita ja dokumentointivaatimuksia. Tämä ei sisälly tämän arviointimenetelmän soveltamisalaan, koska valtuudet kuuluvat markkinavalvontaviranomaiselle. Nämä asetukset mainitaan kuitenkin, koska yleistä tuoteturvallisuusasetusta pidetään ei-suuririskisten tekoälyjärjestelmien turvaverkkona (tekoälyasetus, johdanto-osan kappale 166), ja tämän asetuksen vaatimukset voivat johtaa siihen, että sovellettava dokumentaatio on saatavilla joko suoraan yksilölle tai yhdessä markkinavalvontaviranomaisen kanssa toimivan yhdenvertaisuuselimen kautta. Tämän asetuksen kattamien valmistajien on esimerkiksi varmistettava, että tuotteeseen liitetään selkeät ohjeet ja turvallisuustiedot (9 artiklan 7 kohta), ja laadittava tekniset asiakirjat ja suoritettava riskianalyysit, jotka on asetettava markkinavalvontaviranomaisen saataville (9 artiklan 2 ja 3 kohta ja 15 artikla).

2.2. Suuririskisistä tekoälyjärjestelmistä saatavilla olevat lisätiedot

2.2.1. Kantelijan käytettävissä olevat lisätiedot

Selityspyynnön tekeminen ja vastauksen saaminen
tekoälyasetuksen 86 artiklan mukaisesti

Tätä oikeutta voidaan käyttää DSAR-pyynnön lisäksi (katso kohta [Rekisteröidyn pyynnön saada pääsy tietoihin \(DSAR\) tekeminen ja vastauksen saaminen yleisen tietosuoja-asetuksen 15 artiklan mukaisesti](#)). Jos päätöksellä, joka on tehty suuririskisen tekoälyjärjestelmän tuotoksen perusteella, on henkilöön merkittävä ja haitallinen vaikutus, henkilöllä on oikeus saada tietoa tekoälyjärjestelmän roolista päätöksentekoprosessissa sekä tehdyn päätöksen pääkohdista. Näiden selitysten tulee olla selkeitä ja merkityksellisiä. Asianmukaisesti käsitellyillä vastauksilla voidaan saada tärkeitä tietoja esimerkiksi syöttötiedoista ja päätökseen vaikuttaneista kriteereistä (katso lisätietoja [vaiheesta 3](#)), ja näitä voidaan sitten käyttää *prima facie*-syrijintätapauksen tunnistamiseen. Jos kantelija ei ole vielä tehnyt tällaista pyyntöä, on suositeltavaa kannustaa häntä tekemään se ennen valituksen tai tutkimuksen jatkamista. Katso malli [liitteestä B](#).

Tämä oikeus on voimassa vain siltä osin kuin oikeudesta ei ole toisin säädetty unionin lainsäädännössä. Jos algoritmijärjestelmä on esimerkiksi täysin automaattinen järjestelmä, joka käsittelee asianomaisen henkilön henkilötietoja, voi olla, että oikeus selitykseen saadaan yleisen tietosuoja-asetuksen 13–15 artiklojen nojalla (asetus (EU) 2016/679). Jos vastaaja hylkää tällä perusteella tehdyn selityspyynnön, seuraava vaihe on tehdä jatkopyyntö yleisen tietosuoja-asetuksen (muun sovellettavan unionin lainsäädännön) nojalla (ellei sitä ole jo tehty). Katso malli [liitteestä A](#).

36. Asetus (EU) 2023/988.

37. Asetus (EU) 2019/1020.

2.2.2. Julkisesti saatavilla olevat tiedot

EU:n tietokanta

Katso myös kohta 1.2.1 EU:n tietokanta.

Vaiheessa 1 tehtiin alustava tietojen tarkistus EU:n tietokannasta. Jos vastaaja sisältyy tietokantaan, tässä vaiheessa tulisi olla jo tunnistettu, onko vastaaja merkitty

- ▶ tarjoajaksi tietokannan A- tai B-osioon:
 - sellaisen suuririskisen käyttötapauksen tarjoajaksi, joka on kantelijan tapauksen kannalta merkityksellinen
 - sellaisen käyttötapauksen tarjoajaksi, joka on tarkoitettu käytettäväksi suuririskisellä kohdealueella mutta kuuluu tekoälyasetuksen 6 artiklan 3 kohdassa kuvattuun poikkeukseen
- ▶ käyttöönottajaksi tietokannan C-osioon
 - sellaisen käyttötapauksen käyttöönottajaksi, joka on valitustapauksen kannalta merkityksellinen; mikä organisaatio on tarjoaja?

Alla on lueteltu tietokannan tärkeimmät tarkasteltavat tiedot (tekoälyasetus, liite VIII).

A jakso: suuririskiset tekoälyjärjestelmät

- ▶ Tarjoajan ja valtuutetun edustajan yhteystiedot.
- ▶ Tuotenimi ja muut viitetiedot, joiden avulla tekoälyjärjestelmä voidaan tunnistaa ja jäljittää (tämä voi olla hyödyllistä esimerkiksi silloin, kun suuririskistä järjestelmää käytetään osana toista järjestelmää).
- ▶ Käyttötarkoitus.
- ▶ Yleisluontoinen kuvaus järjestelmän käyttämistä tiedoista (data ja syöttötiedot) ja sen toimintalogiikasta (ei koske lainvalvonnan, muuttoliikkeen hallinnan, turvapaikka-asioiden ja rajavalvonnan aloilla käytettyjä järjestelmiä).
- ▶ Tekoälyjärjestelmän tila (onko järjestelmä esimerkiksi vielä markkinoilla).
- ▶ Ilmoitetun laitoksen antaman todistuksen tyyppi, numero ja viimeinen voimassaolopäivä sekä tarvittaessa kyseisen ilmoitetun laitoksen nimi tai tunnusnumero ja skannattu jäljennös todistuksesta (ei koske lainvalvonnan, muuttoliikkeen hallinnan, turvapaikka-asioiden ja rajavalvonnan aloilla käytettyjä järjestelmiä).
- ▶ Kaikki jäsenvaltiot, joissa tekoälyjärjestelmä on saatettu markkinoille, otettu käyttöön tai asetettu saataville unionissa (hyödyllistä yhteistyössä muiden viranomaisten kanssa).
- ▶ Kopio EU-vaatimustenmukaisuusvakuutuksesta (tekoälyasetus, 47 artikla).
- ▶ Sähköiset käyttöohjeet (ei koske lainvalvonnan, muuttoliikkeen hallinnan, turvapaikka-asioiden ja rajavalvonnan aloilla käytettyjä järjestelmiä).

B jakso: tekoälyjärjestelmä, jonka tarjoaja on määritellyt ei-suuririskiseksi

- ▶ Tarjoajan ja valtuutetun edustajan yhteystiedot.
- ▶ Tuotenimi ja muut viitetiedot, joiden avulla tekoälyjärjestelmä voidaan tunnistaa ja jäljittää.
- ▶ Käyttötarkoitus.

- Tämän asetuksen 6 artiklan 3 kohdan mukainen edellytys tai sen mukaiset edellytykset, joiden perusteella tekoälyjärjestelmän ei katsota olevan suuririskinen (ei koske lainvalvonnan, muuttoliikkeen hallinnan, turvapaikka-asioiden ja rajavalvonnan aloilla käytettyjä järjestelmiä).
- Tekoälyjärjestelmän tila (onko se esimerkiksi vielä markkinoilla).
- Kaikki jäsenvaltiot, joissa tekoälyjärjestelmä on saatettu markkinoille, otettu käyttöön tai asetettu saataville unionissa.

C jakso: suuririskisten järjestelmien käyttöönottajat (tekoälyasetus, 49 artiklan 3 kohta)

- Käyttöönottajän nimi ja yhteystiedot (vain viranomaiset, unionin toimielimet, elimet, toimistot tai virastot tai niiden puolesta toimivat henkilöt)
- Tekoälyjärjestelmän tarjoajan järjestelmästä EU:n tietokantaan kirjaamien tietojen URL-osoite.
- Yhteenveto perusoikeusvaikutusten arvioinnista (FRIA) (ei koske lainvalvonnan, muuttoliikkeen hallinnan, turvapaikka-asioiden ja rajavalvonnan aloilla käytettyjä järjestelmiä).
- Yhteenveto tietosuojaa koskevasta vaikutustenarvioinnista (DPIA).

Kaikkia suuririskisiä tekoälyjärjestelmiä ei ole lueteltu EU:n tietokannan julkisessa osassa.

Alla oleva taulukko näyttää, missä käyttötapauksissa tiedot on annettava tietokannassa.

Taulukko 3. EU:n ja kansallisen tason suuririskisten järjestelmien tietokannassa saatavilla olevat tiedot

Julkinen osa (49 artiklan 1–3 kohta) (lukuun ottamatta yksityisiä käyttöönottajia, elleivät ne toimi julkisyhteisön puolesta)	Ei-julkinen osa (49 artiklan 4 kohta)	Kansallinen täytäntöönpano/rekisteri (49 artiklan 5 kohta)
Kaikki alla kuvatut tiedot ovat pakollisia ja sisältyvät tietokannan julkiseen osaan.	Vain rajoitetut tiedot ovat pakollisia, ja ne sisältyvät tietokannan suojattuun, ei-julkiseen osaan.	Rekisteröinti-vaatimuksia sovelletaan vain kansallisella tasolla.
Yleissivistävä ja ammatillinen koulutus	Lainvalvonta	Kriittinen infrastruktuuri
Työllistäminen, henkilöstöhallinto ja itsenäisen ammatinharjoittamisen mahdollistaminen	Muuttoliikkeen hallinta, turvapaikka-asiat ja rajavalvonta	
Välttämättömien palvelujen ja etuuksien saatavuus ja käyttö	Testattavana olevat suuririskiset tekoälyjärjestelmät	
Oikeudenhoito ja demokraattiset prosessit	Lainvalvonnan, muuttoliikkeen hallinnan, turvapaikka-asioiden ja rajavalvonnan aloilla käytetyt biometriset tiedot	

Tiedonsaantia koskevat rajoitukset

Tekoälyasetuksen 49 artiklan 4 kohdan d alakohdan mukaan lainvalvonnan, muutto-liikkeen hallinnan, turvapaikka-asioden ja rajavaltion aloilla (liitteen III kohdat 1, 6 ja 7) käytettyjä suuririskisiä tekoälyjärjestelmiä koskevat tiedot, sellaisina kuin ne on tallennettu EU:n tietokantaan, rekisteröidään tietokannan ei-julkiseen osaan, johon ainoastaan Euroopan komissiolla ja sovellettavilla markkinavalvontaviranomaisilla on pääsy. Näissä tarkoituksissa ainoastaan tietosuojaviranomainen tai Euroopan tietosuojavaltuutettu (EDPS, komission puolesta) ovat asiaankuuluvia markkinavalvontaviranomaisia (74 artiklan 8 ja 9 kohta), joilla on pääsy tietokannan tietoihin.

Tämä ei tarkoita, etteikö aineisto, johon nämä tiedot perustuvat, voi olla saatavilla. Se tarkoittaa kuitenkin, että pääsy dokumentaatioon edellyttää enemmän perusteluja, ja pääsyä koskevat pyynnöt saatetaan hylätä. Artiklan 77 mukaisilla yhdenvertaisuuselimillä on valtuudet pyytää ja saada käyttöönsä tämän asetuksen nojalla luotu tai ylläpidetty dokumentaatio (katso jäljempää vaihe 2.2.3). Tällaisen pyynnön tulee olla riittävän hyvin perusteltu sen osoittamiseksi, että pyyntö on tarpeen yhdenvertaisuuselimen tehtävän tehokkaaseen toteuttamiseen sen omalla lainkäyttöalueella.

Asetuksessa todetaan myös selkeästi, että ”markkinavalvontatoimet eivät saa millään tavoin vaikuttaa oikeusviranomaisten riippumattomuuteen tai muutoin vaikuttaa niiden toimiin niiden toimiessa oikeudellisessa ominaisuudessaan” (74 artiklan 8 kohta). Tämä tarkoittaa, että 74 artiklan 8 kohdan mukaisia rajoituksia ei sovelleta asiaankuuluviin tietoihin, jotka on asetettava yhdenvertaisuuselimen tai yksilön saataville oikeudenkäyntimenettelyjen kautta. Arkaluonteisen aineiston saatavuuteen, jopa näiden menettelyjen kautta, sovelletaan todennäköisesti muita luottamuksellisuusvaatimuksia sekä yleisiä ja kansallisia turvallisuusasetuksia (katso kohta [Luottamuksellisuus](#)).

Jos yhdenvertaisuuselinten, markkinavalvontaviranomaisten ja muiden 77 artiklan mukaisten elinten väliselle tietojen jakamiselle luodaan oikeusperustat (katso kohta [Eri sektoreiden välinen yhteistyö](#)), yhdenvertaisuuselimet voivat saada pääsyn markkinavalvontaviranomaisten 71 artiklan 4 kohdan ja 49 artiklan 4 kohdan nojalla saamiin tietoihin (Euroopan neuvosto, 2025b).

2.2.3. Vastaajalta tai muilta osapuolilta saadut lisätiedot

Tekoälyasetuksen dokumentointi- ja ilmoitusvelvoitteet

Katso myös [EU:n tekoälyasetus](#), 77 artikla: perusoikeuksia suojelevien viranomaisten valtuudet.

Tekoälyasetuksessa kuvattujen velvoitteiden mukaan suuririskisten tekoälyjärjestelmien tarjoajien ja käyttöönottajien tulee luoda ja ylläpitää erityyppistä dokumentaatiota järjestelmän koko elinkaaren ajan. Artiklan 77 mukaisilla yhdenvertaisuuselimillä on valtuudet pyytää ja saada käyttöönsä tekoälyasetuksen nojalla luotu tai ylläpidetty dokumentaatio ymmärrettävällä kielellä ja saavutettavassa

muodossa, jotta yhdenvertaisuuselimet voivat suorittaa tehokkaasti tehtävänsä omalla lainkäyttöalueellaan.³⁸ (EU:n tekoälyasetus, 77 artikla)

Tämä dokumentaatio on lueteltu alla olevassa taulukossa, joka sisältää teknisen dokumentaation eri tyypit.

On suositeltavaa pyytää kaikkia näitä tietoja, koska nämä asiakirjat yhdessä tarjoavat selkeän kuvan järjestelmän käytöstä, suunnittelusta, datasta ja riskeistä.

Vaiheessa 3 selitetään yksityiskohtaisesti, mitä nämä tiedot voivat osoittaa ja miten niitä voidaan hyödyntää.

Dokumentaation rakenne perustuu todennäköisesti alan viime vuosina kehittämiin yleisiin ja toimialakohtaisiin dokumentointistandardeihin. Tämä sisältää liitteen IV viittaukset ”datalomakkeisiin” ja ”mallikortteihin”. On hyödyllistä, jos yhdenvertaisuuselimet ovat tietoisia näistä kahdesta dokumentaatiotyypistä (Mittelstadt, 2024). Tämän tyyppisen dokumentaation vaadittua rakennetta ja sisältöä sitovat teknisen sekakomitean 21 (JTC-21) standardit (katso jäljempää kohta [Yhdenmukaistetut standardit](#)).

Katso myös kohta [Eri sektoreiden välinen yhteistyö](#).

Seuraavassa kuvataan luettelo vaatimuksista, jotka tekoälyasetuksen mukaisten suuririskisten tekoälyjärjestelmien on täytettävä. Vaikka kaikki vaatimukset eivät nimenomaisesti vaadi dokumentointia, on turvallista olettaa, että näistä vaatimuksista on olemassa ainakin sisäistä dokumentaatiota.

38. Yhdenvertaisuuselimillä, jotka eivät kuulu 77 artiklan soveltamisalaan, ei ole tekoälyasetuksen nojalla lisäoikeusperustaa saada pääsyä suuririskisten tekoälyjärjestelmien asianmukaiseen dokumentaatioon, vaan niiden on turvauduttava olemassa oleviin valtuuksiinsa. On edelleen kyseenalaista, pystyvätkö yhdenvertaisuuselimet saamaan riittävästi tietoa suuririskisten tekoälyjärjestelmien toiminnasta voidakseen hoitaa tehtävänsä tehokkaasti.

Taulukko 4. EU:n tekoälyasetuksen mukaiset suuririskisten tekoälyjärjestelmien vaatimukset

Vaatus (artikla)	Velvoitteen kuvaus	Rooli
Riskinhallinta-järjestelmä (9 artikla)	Riskinhallintajärjestelmä, joka tunnistaa ja analysoi kohtuudella ennakoitavissa olevia riskejä, joita suuririskinen tekoäly-järjestelmä voi aiheuttaa liittyen terveyteen, turvallisuuteen tai perusoikeuksiin, kun suuririskistä tekoälyjärjestelmää käytetään käyttötarkoituksensa mukaisesti.	Tarjoaja
Data ja datanhallinta (10 artikla)	Koulutus-, validointi- ja testausdata-joukkoihin on sovellettava datanhallinta- ja hallinnointikäytäntöjä. Käytäntöihin kuuluvat suunnitteluvallinnat, datan keruuprosessit ja alkuperä, asiaankuuluvat tietojenkäsittelytoimet, oletusten muotoilu, vinoumien selvittäminen ja asianmukaiset toimenpiteet vinoumien ehkäisemiseksi.	Tarjoaja
Suuririskisten tekoälyjärjestelmien tekninen dokumentaatio (11 artikla, liite IV)	Tekoälyjärjestelmän yleinen kuvaus sekä tiettyjen tietojen ja prosessien yksityiskohtainen kuvaus. Tarkempi kuvaus on jäljempänä olevassa taulukossa.	Tarjoaja
Tietojen säilyttäminen (12 artikla)	Järjestelmien on tallennettava tapahtumat, jotka ovat merkityksellisiä terveyteen, turvallisuuteen tai perusoikeuksiin kohdistuvien riskien tunnistamiselle ja markkinoille saattamisen jälkeisen seurannan helpottamiselle. Tämä sisältää käyttöjakson, viitetietokannan, syöttötietojen ja tulosten tarkastamiseen osallistuneiden luonnollisten henkilöiden tunnistetietojen kirjaamisen.	Tarjoaja
Käyttöohjeet (13 artikla) ja ihmisen suorittama valvonta (14 artikla)	Järjestelmien toiminnan tulee olla riittävän avointa. Tämä sisältää järjestelmän ominaisuudet, valmiudet ja rajoitukset sekä sen käyttötarkoituksen ja suorituskykymitarit. Lisäksi on huomioitava järjestelmän toiminnan edellyttämä ihmisen suorittama valvonta ja resurssit.	Tarjoaja käyttöönottajalle

Vaatus (artikla)	Velvoitteen kuvaus	Rooli
Laadunhallinta-järjestelmä (17 artikla)	Käytäntöjen, menettelytapojen ja ohjeiden dokumentointi, mukaan lukien strategia säännösten noudattamista varten, suunnittelu- ja laadunvalvontatekniikat sekä tarkastukset ennen järjestelmän kehitystä, sen aikana ja sen jälkeen. Sisältää myös tekniset eritelvät ja datanhallintajärjestelmät. Lisäksi dokumentaatio menettelyistä, jotka liittyvät vakavasta vaaratilanteesta ilmoittamiseen, viranomaisten kanssa käytävään viestintään, tietojen säilyttämiseen, resurssien hallintaan ja vastuuvollisuuskehykseen.	Tarjoaja
Automaattisesti tuotetut lokitiedot (19 artikla)	Tarjoajien on säilytettävä automaattisesti tuotettuja lokitietoja vähintään kuusi kuukautta. Rahoituslaitosten on säilytettävä lokitietoja osana asiakirjoja, jotka säilytetään asiaankuuluvan rahoituspalvelulainsäädännön nojalla.	Tarjoaja
Automaattisesti tuotetut lokitiedot (26 artikla)	Käyttönottajien on säilytettävä automaattisesti tuotettuja lokitietoja vähintään kuusi kuukautta. Rahoituslaitosten on säilytettävä lokitietoja osana asiakirjoja, jotka säilytetään asiaankuuluvan rahoituspalvelulainsäädännön nojalla.	Käyttönottaja
Perusoikeusvaikutusten arviointi (27 artikla)	Vaikka poikkeuksia sovelletaan, suuririskisten tekoälyjärjestelmien käyttönottajien on tehtävä arviointi järjestelmän käytön mahdollisista perusoikeusvaikutuksista. Tämä sisältää kuvauksen prosesseista, joissa suuririskistä tekoälyjärjestelmää käytetään käyttötarkoituksensa mukaisesti, ajanjaksosta, jonka kuluessa järjestelmää on tarkoitus käyttää, ja kuinka usein, niiden luonnollisten henkilöiden luokista, joihin järjestelmän käyttö vaikuttaa, erityisistä haitan riskeistä, ihmisen suorittamien valvontatoimenpiteiden toteuttamisesta ja toimenpiteistä, jotka on toteutettava kyseisten riskien toteutuessa.	Käyttönottaja

Vaatusmus (artikla)	Velvoitteen kuvaus	Rooli
EU-vaatimusten-mukaisuus-vakuutus (47 artikla, liite V)	Tarjoajan on laadittava kirjallinen (koneluettava) allekirjoitettu EU-vaatimustenmukaisuusvakuutus kul-lekin tekoälyjärjestelmälle ja pidettävä se kansallisten toimivaltaisten viranomaisten saatavilla kymmenen vuotta sen jälkeen, kun suuririskinen tekoälyjärjestelmä on saatettu markkinoille tai otettu käyttöön. EU-vaatimustenmukaisuusvakuutuksessa on ilmoitettava, että kyseinen suuriris-kinen tekoälyjärjestelmä täyttää teko-älyasetuksen 2 jaksossa vahvistetut vaatimukset.	Tarjoaja
CE-merkintä (48 artikla)	Järjestelmiin sovelletaan asetuksen (EY) N:o 765/2008 30 artiklassa kuvattuja yleisiä periaatteita, ja niissä on käytettävä CE-merkintää.	Tarjoaja
Markkinoille saattamisen jälkeisen seurannan tiedot (72 artikla)	Tarjoajien on perustettava markkinoille saattamisen jälkeinen seurantajärjes-telmä, joka kerää, dokumentoi ja analy-soi asiaankuuluvia tietoja järjestelmän suorituskyvystä vaatimustenmukaisuuden arvioinnin mahdollistamiseksi.	Tarjoaja
Vakavista vaaratilanteista ilmoittaminen (73 artikla)	Tarjoajien on ilmoitettava vakavista vaara-tilanteista niiden jäsenvaltioiden markkina-valvontaviranomaisille, joissa kyseinen vaaratilanne tapahtui.	Tarjoaja markkina-valvontaviran-omaiselle. Markkinavalvonta-viranomainen voi ottaa yhden-vertaisuus-elimen mukaan tapaukseen.

Tarjoajilta tekoälyasetuksen 11 artiklan ja liitteen IV mukaan vaadittu tekninen dokumentaatio voi olla hyödyllinen resurssi yhdenvertaisuuselimille.

Siinä tarkastellaan teknistä dokumentaatiota tarkemmin ja ohjataan yhdenvertaisuus-elimiä tietoihin, jotka voivat olla merkityksellisiä tämän arviointimenetelmän sovel-tamisen kannalta.

Taulukko 5. 11 artiklan ja liitteen IV mukaiset teknisen dokumentaation tyypit
Taulukko on luvalla muokattu Mittelstadtin (2024) julkaisusta.

Dokumentaation tyyppi	Selitys
1. Tekoäly-järjestelmän yleinen kuvaus	Tämä sisältää seuraavat: – käyttötarkoitus – vuorovaikutus järjestelmän kanssa – järjestelmän versio, joka kuvastaa sen suhdetta aiempiin versioihin – järjestelmän käyttö laitteiden tai ohjelmistojen kanssa, jotka eivät ole osa itse tekoälyjärjestelmää, tai tuotteet, joiden osa tekojärjestelmä on – kuvaus laitteistosta, jossa tekoälyjärjestelmää on tarkoitus käyttää – käyttöliittymän peruskuvaus ja ohjeet käyttöönottajalle.
2. Järjestelmän rakenne-spesifikaatiot	Tämä sisältää seuraavat: – järjestelmän kehittämisessä käytetyt menetelmät ja vaiheet – järjestelmän rakennespesifikaatiot, tekoälyjärjestelmän ja algoritmien yleinen logiikka; keskeiset rakenteelliset valinnat, mukaan lukien periaatteet ja tehdyt oletukset ja se, mihin nähden järjestelmä on suunniteltu optimoitumaan – valittujen parametrien merkitys – kuvaus järjestelmän odotetusta tuotoksesta ja tuotoksen laadusta – päätökset mahdollisista teknisistä ratkaisuja koskevista kompromisseista, joita on tehty vaatimusten noudattamiseksi.
3. Järjestelmä-arkkitehtuuri	Selitys, miten ohjelmistokomponentit rakentuvat suhteessa toisiinsa tai ovat vuorovaikutuksessa ja miten ne osallistuvat järjestelmän toimintaan, sekä tekoälyjärjestelmän kehittämiseen, kouluttamiseen, testaamiseen ja validointiin käytetyt laskentaresurssit.
4. Dataa koskevat vaatimukset	Dataa koskevat vaatimukset sisältävät datalomakkeet, joissa kuvataan koulutusmenetelmät ja -tekniikat sekä käytetyt koulutusdatajoukot, mukaan lukien yleinen kuvaus näistä datajoukoista, tiedot niiden alkuperästä, laajuudesta ja pääpiirteistä, datan hankinnasta ja valinnasta, merkintämenettelyistä sekä datan puhdistusmenetelmästä.
5. Ihmisen suorittama valvonta	14 artiklan mukaisesti tarvittavien ihmisen suorittamien valvonta-toimenpiteiden arviointi, mukaan lukien niiden teknisten toimenpiteiden arviointi, jotka ovat tarpeen, jotta käyttöönottajien on helpompi tulkita tekoälyjärjestelmien tuloksia.

Dokumentaation tyyppi	Selitys
6. Suorituskyky-mittarit	Käytetyt validointi- ja testausmenettelyt, mukaan lukien tiedot käytetystä validointi- ja testausdatasta ja sen tärkeimmistä ominaisuuksista; mittarit, joita käytetään mittaamaan tarkkuutta, vakautta ja vaatimusten noudattamista sekä mahdollisia syrjiviä vaikutuksia. Sisältää lisäksi kaikki testilokit ja testiraportit, myös ennalta määriteltujen muutosten osalta.
7. Valmiudet	Yksityiskohtaiset tiedot tekoälyjärjestelmän seurannasta, toiminnasta ja valvonnasta ja erityisesti sen suorituskykyyn liittyvistä valmiuksista ja rajoituksista. Tämä sisältää tiettyjä henkilöryhmiä koskevat tarkkuusasteet.
8. Riskinhallinta	Riskinhallintajärjestelmä 9 artiklan kuvauksen mukaisesti.
9. Markkinoille saattamisen jälkeinen seuranta	Yksityiskohtainen kuvaus käytössä olevasta järjestelmästä, jolla arvioidaan tekoälyjärjestelmän suorituskykyä markkinoille saattamisen jälkeisessä vaiheessa 72 artiklan mukaisesti.
10. Muu unionin lainsäädäntö	Sovelletut yhdenmukaistetut standardit ja kopio EU-vaatimustenmukaisuusvakuutuksesta (47 artikla).

Yhdenmukaistetut standardit

Yhdenmukaistetut standardit ovat eurooppalaisten standardointiorganisaatioiden (CEN/CENELEC) parhaillaan laatimia teknisiä standardeja, joiden noudattaminen tarjoaa suuririskisten tekoälyjärjestelmien tarjoajille tekoälyasetusta koskevan ”vaatimustenmukaisuusolettaman”. Käytännössä tämä todennäköisesti kattaa laajan kirjon erilaisia tietoja, kuten tiedot, joita tarvitaan tekoälyjärjestelmän toiminnan, ominaisuuksien, valmiuksien, vahvuuksien, rajoitusten ja suorituskyvyn ymmärtämisen tukemiseksi lakitekstin mukaisesti (Soler Garrido et al., 2024).

Seuraavia kehitteillä olevia standardeja on pidetty erityisen tärkeinä yhdenvertaisuus-elinten saatavilla olevan teknisen dokumentaation vaatimusten määrittämisen kannalta.³⁹

- **JT021036** ”Artificial intelligence – Concepts, measures and requirements for managing bias in AI systems”: Tämän standardin tarkoituksena on määritellä tekoälyjärjestelmien vinoumien arviointia ja hallintaa koskevat käsitteet, toimet ja vaatimukset. Tämä sisältää tekoälyn tarjoajan ja käyttöönottajän tahattomat vinoumat tekoälyjärjestelmän spesifikaatioiden mukaisesti tekoälyasetuksen kontekstissa.

39. Luettelon ja kuvauksen kaikista kehitteillä olevista standardeista löydät CEN:n/CENELECin työohjelmasta ”CEN/CLC/JTC 21 Work Programme”, joka on saatavilla sivulla [CEN - CEN/CLC/JTC 21](#), viitattu 25. kesäkuuta 2026. Myös muut standardit, kuten aiemmat kansainväliset standardointityöt (kuten ISO-/IEC-standardit), voivat olla merkityksellisiä käsiteltäessä tekoälyjärjestelmien vinoumia ja avoimuutta. Kansainväliset standardit eivät yleensä ole maksuttomia, ja niihin sovelletaan immateriaalioikeuksien suojaa, minkä vuoksi yhdenvertaisuuselinten voi olla haastavaa saada pääsy niihin.

- **JT021008** "AI trustworthiness framework", osat 1 (lokikirjanpito), 2 (tarkkuus ja vakaus) ja 3 (avoimuus ja ihmisen suorittama valvonta): tämän standardin tarkoituksena on määritellä terminologia, käsitteet, vaatimukset ja ohjeet lokikirjanpidolle, tarkkuudelle, vakaudelle, avoimuudelle ja ihmisen suorittamalle valvonalle.
- **JT021024** "AI risk management": Tämän standardin tarkoituksena on määritellä vaatimukset ja antaa ohjeita tekoälyjärjestelmien riskinhallintaan koko tekoälyjärjestelmän elinkaaren ajalle. Tässä asiakirjassa tarjoajilta edellytetään objektiivisten kriteerien asettamista riskien hyväksyttävyydelle, mutta siinä ei määritellä hyväksyttäviä riskitasoja.

Näissä standardeissa ei todennäköisesti määritellä kynnysarvoja tai selitetä, miksi ihmisten tai ihmisryhmien erilainen kohtelu katsotaan laittomaksi syrjinnäksi. Mittelstadin (2024) mukaan yhdenvertaisuuselinten tulisi olla tietoisia siitä, että standardit asettavat vinoumien mittausta ja lieventämistä koskevia odotuksia, mutta ne eivät määritä, ovatko vinoumat laittomia tai epäeettisiä.

Standardit, vaatimustenmukaisuuden arvioinnit ja sertifikaatit

Yhdenmukaistettujen standardien vaatimuksia noudattavien suuririskisten järjestelmien oletetaan olevan tekoälyasetuksen 2 jakson (suuririskisiä tekoälyjärjestelmiä koskevat vaatimukset) vaatimusten mukaisia. On kuitenkin tärkeää huomata, että avoimuus- tai muiden velvoitteiden noudattaminen ei tarkoita, että tekoälyjärjestelmän tai sen tuotoksen käyttö olisi laillista asetuksen tai muun lainsäädännön nojalla, eikä sen tulisi rajoittaa muita unionin tai kansallisessa lainsäädännössä tekoälyjärjestelmien käyttöönottajille asetettuja avoimuusvelvoitteita (johdanto-osan kappale 137). Tarjoajien on lueteltava tekoälyjärjestelmään sovellettavat yhdenmukaistetut standardit. Jos yhdenmukaistettuja standardeja ei ole käytetty, tarjoajien on selitettävä, miten tekoälyasetuksen (tekoälyasetus, III luvun 2 jakso) vaatimukset on täytetty muutoin, esimerkiksi käyttämällä muita asiaankuuluvia standardeja ja teknisiä eritelmiä. Tämän avulla yhdenvertaisuuselinten tulisi voida määrittää, milloin asianmukaista vinoumia, luotettavuutta tai yhdenmukaistettua riskinhallintaa koskevaa standardia on noudatettu.

Vaatimustenmukaisuusolettaman vaikutus

Vaatimustenmukaisuusolettama ei estä syrjinnän tai muiden ihmisoikeusriskien tutkimista tai niihin liittyvien toimien toteuttamista. Ensinnäkin tekoälyasetuksessa itsessään tunnustetaan, että asetuksen mukainen tekoälyjärjestelmä voi yhä aiheuttaa riskin, ja 82 artiklassa säädetään menettelystä tällaisissa tilanteissa. Vastaavasti yleisen tuoteturvallisuusasetuksen (EU) 2023/988 7 artiklan 3 kohdan (jota voidaan soveltaa ei-suuririskisiin tekoälyjärjestelmiin) mukaan asetuksessa säädetty yleisen turvallisuusvaatimuksen vaatimustenmukaisuusolettama ei estä markkinavalvontaviranomaista toteuttamasta kaikkia asetuksen mukaisia asianmukaisia toimenpiteitä, jos on näyttöä siitä, että tuote on vaarallinen olettamasta huolimatta.

Huomio: jos talouden toimija esittää testiraportteja tai todistuksia, jotka osoittavat tuotteen olevan unionin yhdenmukaistamislainsäädännön vaatimusten mukainen, markkinavalvonnasta annetun asetuksen (EU) 2019/1020 mukaan

markkinavalvontaviranomaisten on otettava kyseiset testiraportit ja todistukset asianmukaisesti huomioon.

Perusoikeusvaikutusten arviointi

Vaatus perusoikeusvaikutusten arvioinnin (FRIA) tekemisestä koskee vain tiettyjä suuririskisten tekoälyjärjestelmien käyttöönottajia tekoälyasetuksen 27 artiklan ja liitteen III 5 kohdan b ja c alakohtien mukaisesti. Tämä sisältää seuraavat:

- a. suuririskisten tekoälyjärjestelmien käyttöönottajat, jotka ovat julkisoikeudellisia laitoksia tai julkisia palveluja tarjoavia yksityisiä tahoja
- b. sellaisten suuririskisten tekoälyjärjestelmien käyttöönottajat, jotka on tarkoitettu käytettäväksi luonnollisten henkilöiden luottokelpoisuuden arviointiin tai heidän luottopisteytyksensä määrittämiseen (lukuun ottamatta tekoälyjärjestelmiä, jotka on tarkoitettu käytettäväksi talouspetosten havaitsemiseen) tai luonnollisia henkilöitä koskevaan riskinarviointiin ja hinnoitteluun sairaus- ja henkivakuutusten tapauksessa.

Tekoälyä koskevassa digitaalialan koontiasetuksessa tunnustetaan, että FRIA- ja DPIA-arviointien välillä on yhtymäkohtia. Näin ollen voi olla tarpeen pyytää DPIA-arviointia, jos siihen on ristiviitattu eikä sitä ole sisällytetty FRIA-arviointiin.⁴⁰

FRIA-arvioinnin jälkeen käyttöönottajalla on tekoälyasetuksen 27 artiklan 3 ja 5 kohdan mukaan ilmoitettava toimivaltaiselle markkinavalvontaviranomaiselle arvioinnin tuloksista täytetyllä (standardoidulla) mallilla. Lisäksi käyttöönottajalla on toimitettava yhteenveto FRIA-arvioinnin havainnoista osana rekisteröintiprosessiaan EU:n tietokantaan, jos sillä on rekisteröintivelvoite tekoälyasetuksen 49 artiklan 3 kohdan mukaisesti. Tätä velvoitetta ei sovelleta toisen luokan (luotto- ja vakuutusalan) käyttöönotajiin. Yhdenvertaisuuselinten odotetaan siksi löytävän EU-tietokannan C-osiosta yhteenveto liitteen VIII mukaisesti vain ensimmäiseen luokkaan kuuluvien julkisyhteisöjen tai yksityisten tahojen suorittamista pakollisista FRIA-arvioinneista.

Huomautus: Molempien velvoitteiden soveltaminen on rajoitettua, jos viranomaiset ottavat käyttöön suuririskisiä tekoälyjärjestelmiä lainvalvonnan, muuttoliikkeen, turvapaikka-asioiden ja rajavalvonnan aloilla. Tekoälyasetuksen 49 artiklan 4 kohdan mukaan FRIA-arvioinnin havaintojen yhteenvetoa ei toimiteta tällöin EU:n tietokantaan lainkaan – ei edes sen suojattuun, ei-julkiseen osaan. Lisäksi tekoälyasetuksen 27 artiklan 3 kohdan nojalla tällaiset käyttöönottajat voidaan poikkeustapauksissa – kuten yleisen turvallisuuden vuoksi – vapauttaa velvollisuudesta ilmoittaa markkinavalvontaviranomaisille FRIA-arvioinnin tuloksista tekoälyasetuksen 46 artiklan 1 kohdassa kuvatun vaatimustenmukaisuuden arviointimenettelystä poikkeamisen jälkeen (katso myös alta lainvalvonnan alaa käsittelevä tekstiruutu). Yhdenvertaisuuselinten mahdollisuudet saada tietoja tällaisissa tapauksissa ovat siis tekoälyasetuksen nojalla rajalliset.

40. Euroopan parlamentin ja neuvoston asetus (EU) 2026/1744, annettu 8 päivänä heinäkuuta 2026, asetusten (EU) 2024/1689, (EU) 2018/1139 ja (EU) 2023/1230 muuttamisesta tekoälyä koskevien yhdenmukaistettujen sääntöjen täytäntöönpanon yksinkertaistamiseksi (tekoälyä koskeva digitaalialan koontiasetus). Saatavilla osoitteessa <https://eur-lex.europa.eu/eli/reg/2026/1744/oj/eng> (viitattu 24. heinäkuuta 2026).

Muiden luokkien suuririskisten tekoälyjärjestelmien käyttöönottajat – esimerkiksi rekrytointiyritys, joka käyttää tekoälyä työnhakijoiden seulontaan tai valintaan – eivät ole laillisesti velvollisia tekemään FRIA-arviointeja. Tämä ei kuitenkaan välttämättä tarkoita, etteikö tällaisissa tapauksissa tehtäisi FRIA-arviointeja. Tiedyt organisaatiot saattavat tehdä niitä kansallisen lainsäädännön nojalla, YK:n yrityksiä ja ihmisoikeuksia koskevien ohjaavien periaatteiden kaltaisten puitteiden mukaisesti tai omien huolellisuusvelvoitteidensa tai ihmisoikeussitoumustensa vuoksi. Näissä tapauksissa yhdenvertaisuuselimet voivat pyytää tällaisten arviointien jakamista osana tiedonkeruuta koskevia valtuuksiaan.

Suuririskisten tekoälyjärjestelmien tarjoajiin ei sovelleta vaatimusta suorittaa tekoälyasetuksen 27 artiklassa tarkoitettua tietäntyyppistä perusoikeusvaikutusten arviointia. Perusoikeuksiin kohdistuvien mahdollisten tai todellisten haitallisten vaikutusten tunnistamiseen, arviointiin ja käsittelyyn käytettävä, ihmisoikeusvaikutusten arvioinnin (HRIA) puitteisiin pohjautuva FRIA on kuitenkin yleisenä työkaluna osa vaatimustenmukaisuuden arviointia ja tarjoajan riskin- ja laadunhallintajärjestelmää koskevaa velvoitetta tekoälyasetuksen 9 artiklan 2 kohdan, 17 artiklan 1 kohdan g alakohdan ja 43 artiklan mukaisesti (Mantelero, 2024). Tämäntyyppinen vaikutustenarviointi noudattaa tyypillisesti standardeihin perustuvaa lähestymistapaa, ja yhdenvertaisuuselimet voivat pyytää sitä vastaavasti yhdessä muun tekoälyasetuksen nojalla ylläpidettävän dokumentaation kanssa käyttäessään tekoälyasetuksen 77 artiklan mukaisia valtuuksiaan (katso edeltä kohta 2.1.3).

EU:n tekoälyasetuksen mukaisten lakisääteisten vaatimusten lisäksi kansallinen tai alueellinen lainsäädäntö, politiikka tai käytäntö voi edellyttää ihmis- tai perusoikeusvaikutusten arviointien tekemistä ja joissakin tapauksissa niiden julkistamista. Näissä tapauksissa yhdenvertaisuuselimet voivat pyytää tällaisten arviointien jakamista osana tiedonkeruuta koskevia valtuuksiaan.

Tietosuoja koskeva vaikutustenarviointi (DPIA)

Yleisen tietosuoja-asetuksen 35 artiklan 1 kohdan mukaan rekisterinpitäjän on ennen käsittelyä toteutettava tietosuoja koskeva vaikutustenarviointi (DPIA), jos henkilötietojen käsittely aiheuttaa todennäköisesti käsittelyn luonteen, laajuuden, asiayhteyden ja tarkoitusten perusteella luonnollisen henkilön oikeuksien ja vapauksien kannalta korkean riskin. DPIA-arvioinnit ovat siis määritelmänsä mukaisesti erittäin merkityksellisiä tapauksissa, joissa on kyse suuririskisistä tekoälyjärjestelmistä, joihin liittyy henkilötietojen käsittelyä, automaattista päätöksentekoa ja profilointia (vertaa yleisen tietosuoja-asetuksen 35 artiklan 3 kohtaan).

DPIA-arviointien yhteenvetojen lisäämistä EU:n tietokantaan (C-osioon) kuitenkin edellytetään vain tietyltä kapealta suuririskisten tekoälyjärjestelmien käyttöönottajien ryhmältä, jonka on rekisteröitävä tekoälyn käyttö EU:n tietokantaan 49 artiklan 3 kohdan mukaisesti. Tämä sisältää käyttöönottajat, jotka ovat viranomaisia, unionin toimielimiä, elimiä, toimistoja tai virastoja tai niiden puolesta toimivia henkilöitä. Muilla käyttöönottajilla ja suuririskisillä tekoälyjärjestelmillä ei ole suoraa lakisääteistä vaatimusta yleisen tietosuoja-asetuksen tai tekoälyasetuksen nojalla julkaista tai toimittaa DPIA-arviointia yhdenvertaisuuselimelle. Vaikutustenarviointien hallinta jää siis tietosuojaviranomaisten tekemien aloitteiden vastuulle – yhteistyö

tietosuojaviranomaisten kanssa voi olla tässä suhteessa merkityksellistä. Tämän ei tule estää yhdenvertaisuuselinä tekemästä tällaisia pyyntöjä osana kansallisen lainsäädännön mukaisia tiedonkeruuvaltuuksiaan. Osa organisaatioista voi suostua toimittamaan DPIA-arvioinnin, jos se on saatavilla, tai jopa julkaista siitä yhteenvedon. DPIA-arviointia voidaan pyytää myös oikeudenkäyntiä edeltävän viestinnän tai oikeudenkäyntimenettelyn aikana.

Digitaalialan koontiasetuksen ehdotuksessa⁴¹ edellytetään, että Euroopan tietosuojaneuvosto laatii yhdenmukaiset, EU:n laajuiset luettelot käsittelytoimista, jotka edellyttävät tai eivät edellytä DPIA-arviointia, sekä yhteisen menetelmän ja mallin,⁴² joiden odotetaan korvaavan nykyisen hajanaisen kansallisten luetteloiden järjestelmän ja yhdenmukaistavan nämä luettelot EU:n tasolla.

2.2.4. Markkinaevalvontaviranomaiselta saatu ilmoitus tai viran puolesta (*ex officio*) tehtävä tutkinta

Yhdenvertaisuuselin voi odottaa saavansa markkinaevalvontaviranomaiselta tietoja tekoälyjärjestelmistä, jotka aiheuttavat riskin oikeuksille syrjimättömyyteen tai liittyvät näitä oikeuksia loukkaaviin vakaviin vaaratilanteisiin. Katso lisätietoja odotettavissa olevista tietotyypeistä kohdasta 1.1 C: *Markkinaevalvontaviranomaisen tekemä ilmoitus*.

Yhdenvertaisuuselimet voivat saada tekoälyyn liittyvän dokumentaation myös markkinaevalvontaviranomaisilta, jos markkinaevalvontaviranomainen on jo saanut sen tarjoajalta. Tällöin yhdenvertaisuuselin voisi saada pääsyn dokumentaatioon nopeammin. Vastaajat eivät voi estää markkinaevalvontaviranomaisia jakamasta dokumentaatiota yhdenvertaisuuselimille liikesalaisuuden suojan nojalla etenkin silloin, kun yhdenvertaisuuselimet pyytävät dokumentaatiota markkinaevalvontaviranomaisen kautta (Euroopan neuvosto, 2025b). Vastaava käytännön esimerkki tästä on tapauksen *CK v. Dun & Bradstreet Austria GmbH ja Magistrat der Stadt Wien* 76 kohdassa.

Kun tapausta käsitellään osana viran puolesta (*ex officio*) tehtävää tutkintaa tai markkinaevalvontaviranomaisen ilmoituksen perusteella, on harkittava seuraavia toimia:

- ▶ yhdenvertaisuuselimen tutkinnalle välttämättömien asiakirjojen pyytäminen markkinaevalvontaviranomaiselta
- ▶ asiantuntijakeskustelun tai työpajan järjestäminen asianmukaisten järjestöjen tai muiden organisaatioiden kanssa, jotta keskustelujen kautta voidaan saada merkityksellisiä tietoja
- ▶ tietoisuuden lisääminen ja kuulemisten järjestäminen asianomaisten henkilöiden tai ryhmien tunnistamiseksi esimerkiksi kyselytutkimusten tai muiden osallistavien tiedonkeruuprosessien avulla.

41. 3 artikla, ehdotus Euroopan parlamentin ja neuvoston asetukseksi asetusten (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 ja direktiivien 2002/58/EY, (EU) 2022/2555 ja (EU) 2022/2557 muuttamisesta digitaalisen lainsäädäntökehyksen yksinkertaistamiseksi sekä asetusten (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868 ja direktiivin (EU) 2019/1024 kumoamisesta (digitaalialan koontiasetus), *EUR-Lex - 52025PC0837 - EN - EUR-Lex*, viitattu 25. kesäkuuta 2026.

42. Euroopan tietosuojaneuvosto järjesti toukokuussa 2026 kuulemisen DPIA-mallista, joka on saatavilla osoitteessa www.edpb.europa.eu/our-work-tools/documents/public-consultations/2026/edpb-dpia-template_en.

Lainvalvonnan ala

Tiedonkeruumahdollisuudet lainvalvonnan alalla ovat rajallisemmat, mikä vaikeuttaa tekoäly- tai algoritmijärjestelmien käytön ja siitä johtuvan syrjinnän tunnistamista.⁴³

Tekoälyasetus

- Tekoälyasetuksen 49 artiklan 4 kohdan mukaan suuririskisten tekoälyjärjestelmien osalta lainvalvonnan, muuttoliikkeen, turvapaikka-asioiden ja rajavalvonnan aloilla rekisteröinnin on tapahduttava 71 artiklassa tarkoitetun EU:n tietokannan suojattuun ei-julkiseen osaan, ja siihen on sisällyttävä tarvittaessa ainoastaan rajalliset tiedot, jotka eivät sisällä esimerkiksi tietoja syöttödatasta tai toimintalogiikasta. Tähän tietokannan ei-julkiseen osaan on pääsy 74 artiklan 8 kohdassa tarkoitetuilla markkinavalvontaviranomaisilla siltä osin kuin näitä järjestelmiä käytetään lainvalvontatarkoituksessa ja rajaturvallisuudessa, eikä yhdenvertaisuuselimillä ole periaatteessa pääsyä tähän tietokannan osaan. Lisätietoja on kohdassa [2.2.2 Tiedonsaantia koskevat rajoitukset](#).
- Tekoälyasetuksen 27 artiklan 1 kohdan mukaisesti lainvalvontaviranomaisten on viranomaisina tehtävä perusoikeusvaikutusten arviointi (FRIA) ennen suuririskisen tekoälyjärjestelmän käyttöönottoa. Tähän sovelletaan kuitenkin kahta poikkeusta. Ensinnäkin tekoälyasetuksen 49 artiklan 4 kohdan c alakohdan mukaan FRIA- tai DPIA-arvioinnin havaintojen yhteenvetoa ei toimiteta tällaisten käyttöönottajien tapauksessa EU:n tietokantaan lainkaan – ei edes sen suojattuun, ei-julkiseen osaan. Toiseksi markkinavalvontaviranomainen voi poikkeustapauksissa, mukaan lukien yleisen turvallisuuden vuoksi, antaa tällaisille toimijoille luvan tiettyjen suuririskisten tekoälyjärjestelmien markkinoille saattamiseen tai käyttöönottoon noudattamatta vaatimustenmukaisuuden arviointimenettelyjä tai ”kiireellisessä” tilanteessa ilman lupaa lainkaan (tekoälyasetus, 46 artiklan 1 ja 2 kohta). Tämä sisältää tekoälyasetuksen 27 artiklan 3 kohdan nojalla myös vapautuksen velvollisuudesta ilmoittaa markkinavalvontaviranomaiselle FRIA-arvioinnin tuloksista.

Huomio: Tekoälyasetuksen 27 ja 46 artiklassa ei säädetä poikkeuksista, joiden mukaan FRIA-arviointia ei tarvitsisi suorittaa lainkaan, ja 46 artiklan 1 kohdan mukaan ”lupa on voimassa rajallisen ajanjakson, kun tarvittavia vaatimustenmukaisuuden arviointimenettelyjä suoritetaan”. 46 artiklan 2 kohdan mukaan kiireellisissä tapauksissa lupaa on pyydettävä ”ilman aiheutonta viivytystä tekoälyjärjestelmän käytön aikana tai sen jälkeen”.

Jos lupa myöhemmin evätään, on tärkeää huomata, että

- suuririskisen järjestelmän käyttö on lopetettava välittömästi
- kaikki tällaisen käytön tulokset ja tuotokset on välittömästi hävitettävä.

Mahdollisia keinoja, joilla yhdenvertaisuuselimet voivat saada sekä DPIA- että FRIA-arviointeihin liittyviä tietoja, käsitellään jäljempänä.

43. Yleisen tietosuoja-asetuksen ja LED-direktiivin algoritmisia tietoja koskevien oikeuksien vertailu: katso González Fuster (2020).

Direktiivi lainvalvontatarkoituksessa käsiteltujen henkilötietojen suojasta

Lisäksi lainvalvontatarkoituksessa käsiteltujen henkilötietojen suojasta annetussa direktiivissä (LED)⁴⁴ säädetään useista poikkeuksista ja mahdollisista rajoituksista yksilöiden tiedonsaantioikeuksiin kansallisten täytäntöönpanotoimenpiteiden kautta, jos se on tarpeen, jotta vältetään tuottamasta haittaa rikosten ennalta estämiselle, paljastamiselle, tutkimiselle tai rikoksiin liittyville syytetoimille taikka rikosoikeudellisten seuraamusten täytäntöönpanolle tai jotta voidaan suojella yleistä tai kansallista turvallisuutta (LED-direktiivi, 13 artiklan 3 kohta ja 15 artikla).

Käytännöt siis vaihtelevat jäsenvaltioiden välillä sen suhteen, minkä tyyppisiä tietoja on annettava ja miten niihin voi saada pääsyn. Tämän vuoksi viittaus kansalliseen lainsäädäntöön on tällä alalla välttämätön.

Automaattinen päätöksenteko

- ▶ LED-direktiivin 11 artikla kieltää tietyt automaattisen käsittelyn muodot, kuten profiloinnin, jollei sitä ole nimenomaisesti sallittu rekisterinpitäjään sovellettavassa unionin oikeudessa tai jäsenvaltion lainsäädännössä, jossa on otettu huomioon rekisteröidyn oikeuksia ja vapauksia koskevat asianmukaiset suojatoimet. Suojalta vaadittu vähimmäistaso sisältää oikeuden vaatia, että käsittelyyn osallistuu rekisterinpitäjän puolesta ihminen. Lainvalvonnan suorittamaa automaattista käsittelyä koskevia kansallisia kehyksiä on tarkasteltava sen selvittämiseksi, mitä tietoja automaattisesta käsittelystä tulisi olla saatavilla. Eri jäsenvaltioiden täytäntöönpanotoimenpiteet: Katso Vogiatzoglou ja Marquiene, 2022. Katso myös johdanto-osan kappale 38.
- ▶ LED-direktiivin 13 ja 14 artiklassa ei nimenomaisesti määrätä automaattisen päätöksenteon, kuten profiloinnin, käyttöön liittyvistä tiedonantovelvoitteista.

Tietojen luovuttaminen

- ▶ LED-direktiivin 13 artiklan 1 kohdan mukaan rekisterinpitäjän on asetettava rekisteröidyn saataville ainakin tiedot rekisterinpitäjän henkilöllisyydestä ja yhteystiedoista, rekisteröidyn oikeudesta pyytää rekisterinpitäjältä pääsy häntä itseään koskeviin henkilötietoihin ja henkilötietojen käsittelyn tarkoituksista.

Kyseiset tiedot eivät koske tiettyä rekisteröityä vaan tiettyä käsittelymenettelyä ja kaikkia rekisteröityjä, joihin ne mahdollisesti vaikuttavat. Ne ovat yleensä saatavilla toimivaltaisen viranomaisen verkkosivustolla. On raportoitu, että lainvalvontaviranomaisia hallinnoivan yksikön, kansallisen poliisilaitoksen tai toimivaltaisen ministeriön verkkosivustolta ei ole aina helppoa tai mahdollista löytää asiaankuuluvia tietoja (Vogiatzoglou ja Marquiene, 2022).

- ▶ LED-direktiivin 13 artiklan 2 kohta laajentaa annettavia tietoja, sillä sen mukaan rekisterinpitäjän on annettava erityistapauksissa rekisteröidylle myös tiedot käsittelyn oikeusperusteesta, mahdollisista henkilötietojen vastaanottajista tai vastaanottajaryhmistä ja tarvittaessa lisätietoja varsinkin, jos henkilötiedot

44. Viittauksia LED-direktiiviin tietolähteiden osalta ei pidetä tyhjentävinä; muutkin vapauden, turvallisuuden ja oikeuden laajemman alan välineet, kuten neuvoston päätös SIS II, VIS ja Eurodac, voivat sisältää oleellisia ja menettelyllisiä sääntöjä rekisteröityjen oikeuksista, kuten tiedonsaantioikeudesta ja oikeudesta saada pääsy tietoihin.

kerätään rekisteröidyn tietämättä. 13 artiklan 3 kohdan mukaan jäsenvaltiot voivat hyväksyä lainsäädäntötoimenpiteitä, joilla tätä ilmoitusta viivytetään tai rajoitetaan tai ilmoitus jätetään kokonaan tekemättä, jos tällainen toimenpide on välttämätön ja oikeasuhteinen demokraattisessa yhteiskunnassa.

Jos tällaiset tiedot ovat riittävän tarkkoja, ne voidaan tarjota verkkosivustolla vaadittujen vähimmäistietojen ohella.

Oikeus saada pääsy tietoihin

- ▶ LED-direktiivin 14 artiklan nojalla rekisteröidyillä on oikeus saada enemmän tietoja henkilötietojen käsittelytoimista kuin yleisesti julkisesti saatavilla olevissa tiedoissa on. Tämä sisältää esimerkiksi käsittelyn tarkoituksen, käsittelyn kohteena olevat henkilötietoryhmät, vastaanottajat tai vastaanottajaryhmät, joille henkilötietoja on luovutettu, sekä käsiteltävät henkilötiedot ja tietojen alkuperästä käytettävissä olevat tiedot.

Toisin kuin yleisessä tietosuoja-asetuksessa, tässä artiklassa ei nimenomaisesti säädetä oikeudesta saada tietoa automaattisen päätöksenteon olemassaolosta ja logiikasta eikä rekisteröidylle aiheutuvista mahdollisista seurauksista. Lainvalvontaviranomaiset voivat kuitenkin olla kansallisen lainsäädännön nojalla velvollisia antamaan tietoja henkilöiden profiloinnista.

- ▶ LED-direktiivin johdanto-osan kappaleen 43 mukaan annettujen tietojen ei tarvitse sisältää käsiteltyjen tietojen varsinaista kopiota, kuten esimerkiksi yleisessä tietosuoja-asetuksessa on määrätty, vaan täydellinen yhteenveto riittää. Vastauksen sisältö – jos pääsy tietoihin ei evätä muodollisin perustein – supistuu usein standardoituihin, lyhyisiin vastauksiin, jotka eivät sisällä olennaisia tietoja mutta ovat silti muodoltaan vaatimusten mukaisia (Erdogan, 2024).
- ▶ LED-direktiivin 15 artiklan mukaan jäsenvaltiot voivat hyväksyä lainsäädäntötoimenpiteitä, joilla rajoitetaan kokonaan tai osittain rekisteröidyn oikeutta saada pääsy tietoihin siltä osin ja niin pitkäksi aikaa kuin osittainen tai täydellinen rajoittaminen on välttämätön ja oikeasuhteinen toimenpide demokraattisessa yhteiskunnassa, jotta voidaan esimerkiksi suojata yleistä tai kansallista turvallisuutta tai välttää virallisten tai laillisten tiedustelujen, tutkimusten tai menettelyjen estämistä.

Pyyntö saada pääsy tietoihin

- ▶ LED-direktiivin 14 artiklassa ja 17 artiklan 3 kohdassa on kuvattu kaksi menettelytapaa, joilla oikeutta saada pääsy tietoihin voidaan käyttää. Ensimmäinen on LED-direktiivin 14 artiklan mukainen ”suora” pääsy tietoihin, jossa yksilöt voivat ottaa suoraan yhteyttä rekisterinpitäjänä toimivaan lainvalvontaviranomaiseen ja kysyä henkilötiedoistaan. Toinen on poikkeusmenettely eli ”epäsuora” pääsy tietoihin, jossa oikeutta saada pääsy tietoihin käyttää välittäjänä toimiva kansallinen tietosuojaviranomainen.

Kansallisia lakeja, jotka panevat täytäntöön epäsuoran pääsyn tietoihin, kuten Belgiassa, jossa epäsuora pääsy tietoihin on oletusarvoinen, on kritisoitu niiden rakenteellisista ja menettelyllisistä puutteista (Dimitrova ja De Hert, 2024), sillä

ne rajoittavat tietojenkäsittelytoimien tehokasta valvontaa ja asiaankuuluvien tietojen välittämistä asianomaisille rekisteröidyille.

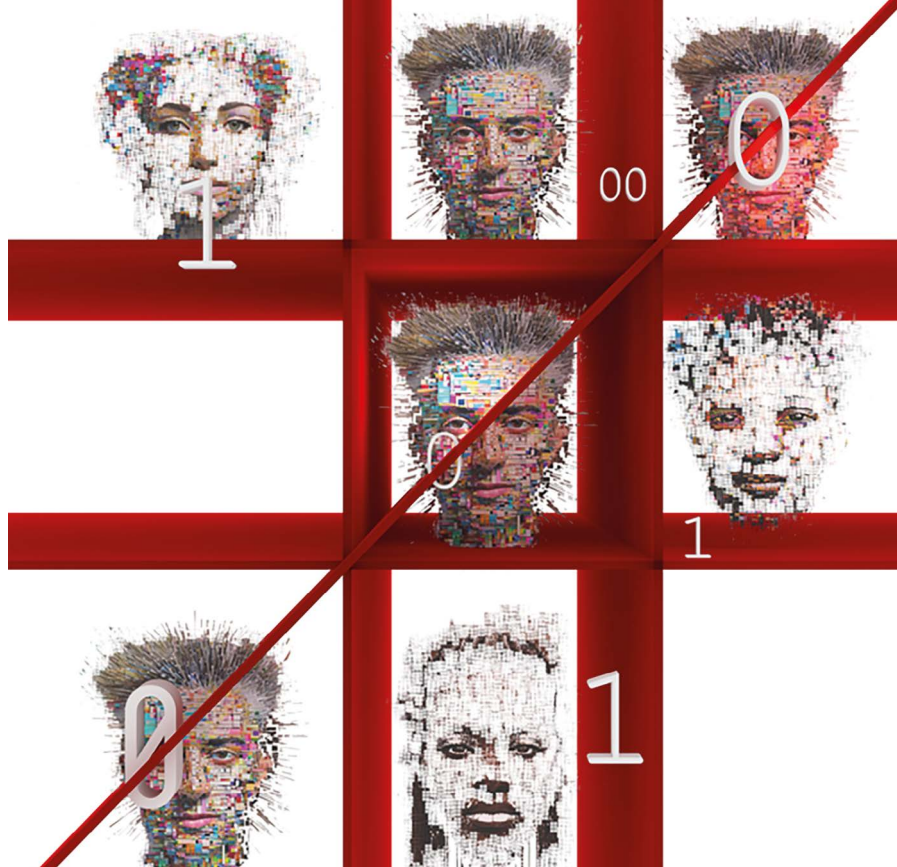
Huomautus: Jos toimivaltainen viranomainen kerää tietoja lainvalvontatarkoituksiin, ne kuuluvat LED-direktiivin soveltamisalaan. Tällaisia ovat esimerkiksi tiedot henkilön aiemmasta rikoshistoriasta. Jos tiedot on haravoitu toisesta julkisesta lähteestä tai kerätty muihin kuin lainvalvontatarkoituksiin (kuten siviilisäädyn, työllisyyden tai koulutustilanteen selvittämiseksi), ne kuuluvat yleisen tietosuoja-asetuksen soveltamisalaan. Tietyissä lainvalvonnan käyttämissä tekoälyjärjestelmissä voidaan käyttää molempia syöttötietojen tyyppejä, ja siksi on huolellisesti määritettävä, kuuluvatko sovellettavat tietoihin liittyvät oikeudet yleisen tietosuoja-asetuksen vai LED-direktiivin soveltamisalaan. Tilanteesta tulee entistä monimutkaisempi, kun yksityiset yritykset osallistuvat ohjelmistokehitykseen tai asiaankuuluvan datan käsittelyyn tai hallintaan (katso Erdogan, 2023). Epävarmoissa tapauksissa on suositeltavaa konsultoida lakiasiantuntijaa.

Seloste käsittelytoimista

- ▶ LED-direktiivin 24 artiklan mukaan rekisterinpitäjien on ylläpidettävä selostetta kaikista sen vastuulle kuuluvista käsittelytoimista. Tämä sisältää esimerkiksi käsittelyn tarkoitukset, henkilötietojen vastaanottajien ryhmät, joille henkilötietoja on luovutettu tai luovutetaan, ja tarvittaessa profiloinnin käytön. Ne on asetettava tietosuojaviranomaisten saataville pyynnöstä (katso yhteistyömahdollisuudet tietosuojaviranomaisten kanssa kohdasta [Eri sektoreiden välinen yhteistyö](#)).

Tietosuoja koskeva vaikutustenarviointi (DPIA)

Lainvalvonnan kontekstissa LED-direktiivin 27 artikla edellyttää tietosuoja koskevaa vaikutustenarviointia (DPIA), jos käsittely etenkin uutta teknologiaa käytettäessä todennäköisesti aiheuttaa luonnollisen henkilön oikeuksien ja vapauksien kannalta korkean riskin. DPIA-arviointia koskevat velvoitteet vaihtelevat jäsenvaltioissa kansallisten täytäntöönpanotoimenpiteiden mukaan. 29 artiklan mukainen tietosuojatyöryhmä suositteli, että kansalliset lainsäätäjät velvoittaisivat rekisterinpitäjät suorittamaan DPIA-arvioinnin automaattisten päätösten yhteydessä. Kuten FRIA-arvioinneissa, lainvalvontaviranomaisten ei kuitenkaan tarvitse toimittaa näistä arvioinneista yhteenvetoa EU:n tietokantaan (tekoälyasetus, 49 artiklan 4 kohdan c alakohta).



Vaihe 3

Vastaanotettujen tietojen arviointimenetelmä

Vaiheessa 3 esitellään tekoälyjärjestelmien aiheuttaman syrjinnän tyypit riippumatta siitä, käytetäänkö järjestelmiä automaattiseen päätöksentekoon vai päätöksenteon tukena.

Käsitteiden johdannossa esitellään syrjinnän tyypit ja niiden soveltaminen tekoälykontekstiin. Yhdenvertaisuuselimille uusia käsitteitä voivat olla sijaismuuttujaan liittyvä syrjintä ja erilaiset muuttujat. Siinä esitellään myös syrjintäolettaman tai *prima facie* -tapauksen tunnistaminen ja osoittaminen.

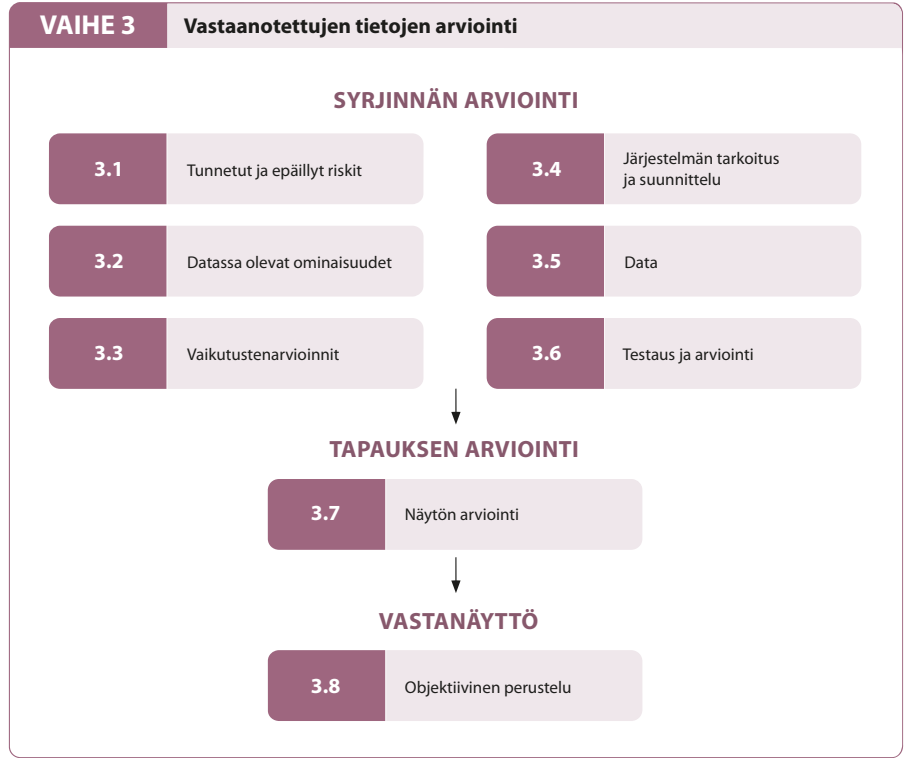
Vaiheen 3 operatiivinen osa on suunniteltu auttamaan tapausten käsittelijöitä arvioimaan vaiheessa 2 saatuja tietoja, ja liitteessä K olevaa mallilomaketta voidaan käyttää rinnakkain tässä vaiheessa tietojen kirjaamiseen. Vaiheissa 3.2–3.6 tapauksen käsittelijälle annetaan lyhyt selitys käsiteltävistä tiedoista, pohdittavia kysymyksiä, mahdollisia tietolähteitä, jotka voivat auttaa näihin kysymyksiin vastaamisessa, sekä esimerkkejä syrjinnän tai syrjivien käytäntöjen indikaattoreista.

Vaiheessa 3.7 kootaan kaikki nämä havainnot yhteen ja annetaan ohjeet sen arvioimiseksi, onko syrjäntäolettama perusteltu, ja ennen kaikkea siitä, mitä on tehtävä, jos saatavilla olevat todisteet ovat riittämättömiä tai avoimuus on puutteellista.

Vaiheessa 3.8 annetaan ohjeita sen arvioimiseksi, kuinka todennäköisesti vastaaja pystyy kumoamaan syrjäntäolettaman tai esittämään perusteluita syrjinnälle.

Ei ole tarkoitus olettaa, että tapausten käsittelijöillä olisi valmiudet vastata kaikkiin kysymyksiin tai pääsy kaikkiin asiakirjoihin tai todisteisiin. Sen sijaan tavoitteena on, että tämä vaihe auttaa tapausten käsittelijöitä hyödyntämään saatavilla olevia tietoja parhaalla mahdollisella tavalla ja ymmärtämään niiden merkityksen.

Kuva 4. Vaihe 3 – Vastaanotettujen tietojen arviointi



Vaiheessa 2 olisi tullut aloittaa asiaankuuluvien asiakirjojen ja muiden todisteiden kerääminen. Vaiheessa 3 näiden todisteiden avulla arvioidaan, voidaanko syrjäntäolettama tai *prima facie*-tapaus osoittaa ja onko todennäköistä, että vastaaja pystyy kumoamaan syrjäntäolettaman tai esittämään tapaukseen liittyviä perusteluita.

Tekninen asiantuntemus voi olla hyödyllistä monissa vaiheen 3 alivaiheissa. Konsultoitavilla asiantuntijoilla tulisi olla kattava ymmärrys tilastotieteestä, data-tieteestä ja tekoälystä. Algoritmi-järjestelmien kehittämisen kannalta keskeisiä käsitteitä, kuten koulutusdataa, pohjatotuustunnisteita, tuotoksia ja syötteitä, ei selitetä tässä arviointimenetelmässä tarkemmin, vaan niiden oletetaan olevan tilastotieteen, datatieteen ja tekoälyn alojen perustietoa. Kun etsitään teknisiä asiantuntijoita, on

varmistettava, että asiantuntija ymmärtää sekä datatieteen että syrjimättömyyden periaatteet.

Joissakin tapauksissa jäsenvaltion markkina- ja valvontaviranomaisilla tai muilla virastoilla voi olla tarvittava tekninen asiantuntemus, jota yhdenvertaisuuselimet voivat hyödyntää (katso kohta [Eri sektoreiden välinen yhteistyö](#)).

Lisäksi joskus sektorikohtainen asiantuntemus voi auttaa ymmärtämään historiallisten ja olemassa olevien eriarvoisuuksien kuvioita alalla, jolla järjestelmää sovelletaan. Sektorikohtaista asiantuntemusta käytettäessä voi olla hyödyllistä konsultoida asiantuntijoita, joilla on taustaa yhteiskuntatieteistä ja empiirisestä tutkimuksesta, sillä tämä tausta auttaa yhdistämään sektorikohtaisen asiantuntemuksen tekniseen asiantuntemukseen. Jos tämä ei ole mahdollista, yhdenvertaisuuselimen voi olla tarpeen tehdä lisätutkimuksia historiallisesta ja muusta eriarvoisuudesta arvioidakseen, onko se vaikuttanut järjestelmään. Tämä voi esimerkiksi sisältää tiettyihin yhteisöihin kohdistuvan liiallisen poliisitoiminnan tai sukupuolten väliset tuloderot.

Asiantuntijoiden ottamista mukaan tapaukseen suositellaan tarvittaessa kussakin alivaiheessa.

Huomio: kuten arviointimenetelmässä aiemmin todettiin, uutta yhteistyön ja keskinäisen avunannon vaatimusta koskeva 77 artiklan 1 kohdan b alakohta voi johtaa siihen, että markkina- ja valvontaviranomainen tai muu asetuksen mukainen viranomainen tai elin voi tarjota tarvittavaa asiantuntemusta.

Huomio: jos saatavilla ei ole riittävästi tietoa, yhtä seuraavista on tarkasteltava:

- ▶ avoimuuden puutteen vaikutus todistustaakkaan (katso avoimuus [vaiheesta 3.7](#))
- ▶ järjestelmän arvioinnin ja testauksen pyytäminen markkina- ja valvontaviranomaiselta (katso [vaihe 4.2.1](#)).

Tämän arviointimenetelmän käytössä odotetaan kohtuullista syrjintälainsäädännön tuntemusta, mutta peruskäsitteet toistetaan tämän vaiheen alussa, jotta niiden yhteys algoritmijärjestelmiin voidaan havainnollistaa paremmin.

Johdatus käsitteisiin

Syrjinnän tyypit

Välitön syrjintä

Henkilöä kohdellaan epäsuotuisammin kuin muita vastaavassa tilanteessa olevia kohdellaan tai kohdeltaisiin, ja syynä tähän on henkilön ominaisuus, joka sisältyy kiellettyihin syrjintäperusteisiin (ja ainoastaan ikää/vammaisuutta ja todellista työhön liittyvää vaatimusta koskevissa EU-tapauksissa tälle ei ole perustetta).

Esimerkki välittömästä algoritmisesta syrjinnästä

Suomessa rahoituslaitos eväsi eräältä lainaa hakeneelta mieheltä lainan. Päätös pohjautui lainan luottotappioriskin arvioinnissa käytettyyn pisteytysjärjestelmään, joka otti pisteytyksessä huomioon esimerkiksi asuinpaikan, sukupuolen, iän ja äidinkielen. Tutkinnassa todettiin, että mies olisi saanut lainan, jos hän olisi ollut nainen tai hänen äidinkielenä olisi ollut ruotsi. Lisäksi miehen takaisinmaksun laiminlyönnin todennäköisyydestä ei tehty yksilöllistä riskinarviointia, vaan häneltä yksinkertaisesti evättiin laina hänen sukupuoleensa ja äidinkieleensä liittyvien tilastollisten oletusten perusteella. Yhdenvertaisuus- ja tasa-arvolautakunta totesi vuonna 2018 yhdenvertaisuusvaltuutetun tutkintapyyntöä jälkeen, että kyseessä oli välittömän syrjinnän tapaus.

Lisämateriaaleja

- ▶ Luottokelpoisuuden arviointimenettely, toimivalta, välitön moniperusteinen syrjintä, sukupuoli, kieli, ikä, asuinpaikka, taloudelliset syyt, uhkasakko, Suomen yhdenvertaisuus- ja tasa-arvolautakunta (2018)
-

Välillinen syrjintä

Näennäisesti neutraali sääntö, peruste tai käytäntö, joka asettaa suojattuun ryhmään kuuluvat henkilöt epäedullisempaan asemaan verrattuna muihin samankaltaisessa tilanteessa oleviin henkilöihin, ellei

- ▶ sääntö, peruste tai käytäntö ole objektiivisesti perusteltu oikeutetulla tarkoituksella
- ▶ keino kyseisen tarkoituksen saavuttamiseksi ole asianmukainen ja välttämätön.

Vielä ei ole velvoittavaa päätöstä siitä, ovatko jotkut tai kaikki automaattiset päätöksentekoprosessit sääntöjä, perusteita tai käytäntöjä, mutta joidenkin toimijoiden keskuudessa on vahva näkemys siitä, että algoritmeja käyttävät automaattiset päätöksentekoprosessit ovat lähes varmasti sääntöjä, perusteita tai käytäntöjä välillisen syrjinnän tapausten konteksteissa (Allen ja Masters, 2019).

Esimerkki välillisestä algoritmisesta syrjinnästä (Deliveroon tapaus)

Deliveroon algoritmisen, työvuorojen jakamiseen tarkoitetun ”omatoimisen varausjärjestelmän” todettiin olevan välillisesti syrjivä, varsinkin vakaumuksen (osallistuminen työtaistelutoimiin, kuten lakkoihin) ja vammaisuuden perusteella. Käyttämällä osallistumis- ja luotettavuustilastoja, jotka olivat näennäisesti neutraaleja kriteerejä, järjestelmä käytännössä asetti epäedulliseen asemaan kuljettajat, jotka pidättäytyivät työstä oikeutetuista syistä, kuten lakkojen, sairauden tai hoitovastuiden vuoksi, laskemalla heidän pisteitään ja rajoittamalla siten heidän mahdollisuuksiaan saada töitä tulevaisuudessa.

Käytettyjen tilastojen ”sokeus” eli järjestelmän kyvyttömyys ottaa huomioon kiellettyihin syrjintäperusteisiin kuuluvia kuljettajien poissaolosyitä johti siihen,

että erilaisia tilanteita käsiteltiin kaikkia samalla tavalla, mikä puolestaan vaikutti suhteettomasti suojattuihin ryhmiin.

Lisämateriaaleja

- *Filcams Cgil Bologna ym. v. Deliveroo Italia S.R. (2020)*
 - *Purificato (2021)*
-

Moniperusteinen syrjintä

Syrjintää voi tapahtua useamman kuin yhden syrjintäperusteen perusteella. Henkilö voi esimerkiksi joutua syrjinnän kohteeksi rodun, sukupuolen ja vammaisuuden perusteella. Useampaan kuin yhteen syrjintäperusteeseen liittyvää syrjintää kuvailaan useilla eri termeillä. Esimerkkejä käytetyistä termeistä ovat ”moniperusteinen syrjintä”, ”kumulatiivinen syrjintä”, ”yhdistetty syrjintä”, ”yhdistelmäsyryjintä” ja ”intersektionaalinen syrjintä” (Fredman, 2016). Näiden termien merkitykset poikkeavat toisistaan hieman. Tämän arviointimenetelmän kannalta on tärkeää tunnistaa, että syrjinnän perusteet voivat olla monitahoisia (Xenidis, 2021).

Intersektionaalinen syrjintä

”Pohjimmiltaan ... intersektionaalisuus on tapa käsitellä identiteettiä ja sen suhdetta valtaan” (Crenshaw, 2015).

Intersektionaalinen syrjintä eroaa muista moniperusteisen syrjinnän muodoista siinä, että se ei ole pelkästään yhteen syrjintäperusteeseen pohjautuvien syrjintätapausten yhteenlaskettu summa, vaan siinä huomioidaan erilaisten henkilökohtaisten ominaisuuksien, joita ei voida erottaa toisistaan, päällekkäisyys. Sosiaaliset, taloudelliset, kulttuuriset ja institutionaaliset rakenteet lomittuvat toisiinsa ja muodostavat monimutkaisen järjestelmän, joka luo (ja ylläpitää) eriarvoisuutta (Crenshaw, 1991). Esimerkiksi sosiaaliset luokat, kuten ikä ja sukupuoli, voivat olla päällekkäisiä ja luoda etuja tai haittoja olosuhteista riippuen. Eriarvoisuus voi muuttua olosuhteiden ja tosiasioiden mukaan, ja joskus se riippuu myös ajasta ja paikasta. Esimerkiksi nainen, jolla ei ole maahanmuuttajataustaa, voi olla ”vähemmän” tasa-arvoisessa asemassa kuin mies, mutta maahanmuuttajataustaiseen naiseen verrattuna hänen asemansa on parempi. Yhteiskunnallinen eriarvoisuus voi myös muokata valtasuhteita. Nämä toisiinsa kytkeytyvät eriarvoisuusrakenteet heijastuvat algoritmijärjestelmien suunnittelussa, kehittämisessä ja testaamisessa käytettyyn tosielämän dataan. Lisäksi tekoälyjärjestelmien kehittämisessä käytetyt koneoppimismenetelmät saattavat löytää toisiinsa vaikuttavia kuvioita, joita ei tunneta tai jotka eivät ole ilmeisiä vakio-mallisten data-analyyysien perusteella. Tällä tavoin algoritmijärjestelmät voivat johtaa intersektionaaliseen syrjintään (Xenidis, 2021). Vaikka EUT hylkäsi intersektionaalista syrjintää koskevan hakemuksen Parrisin tapauksessa (C-443/17), jotkut kommentaattorit ovat ehdottaneet, että tätä asiaa olisi tarkasteltava uudelleen, kun otetaan huomioon erityisesti ilmiön lisääntyvä tunnistus unionin oikeudessa, kuten miesten ja naisten samapalkkaisuuden periaatteen soveltamisen lujittamisesta annetussa direktiivissä (EU) 2023/970 ja naisiin kohdistuvan väkivallan ja perheväkivallan torjumisesta annetussa direktiivissä (EU) 2024/1385 (Howard, 2024).

Sijaismuuttujaan liittyvä syrjintä

Kun syrjintä perustuu sijaismuuttujiksi kutsuttuihin ominaisuuksiin, jotka eivät itsessään liity mihinkään kiellettyyn syrjintäperusteeseen (katso [kielletty syrjintäperusteet](#)), mutta korreloivat kielletyn syrjintäperusteen kanssa, tätä kutsutaan sijaismuuttujaan liittyväksi syrjinnäksi. Vaikka unionin lainsäädännössä ei nimenomaisesti tunnisteta sijaismuuttujaan liittyvää syrjintää tai viitata siihen, se on kuitenkin teoreettinen käsite, joka auttaa ymmärtämään, miten algoritmista syrjintää voi syntyä.

- ▶ Sijaismuuttujaan liittyvä syrjintä voi olla välitöntä syrjintää, jos valittujen – neutraalien – ominaisuuksien ja nimenomaisesti kiellettyjen syrjintäperusteiden välillä on erottamaton yhteys (raskauteen ja sukupuoleen liittyvä esimerkki: *Dekker v. Stichting Vormingscentrum voor Jong Volwassenen (VJV-Centrum) Plus*, 1990; *Dita Danosa v. LKB Lizings SIA*, 2010; *Andersen v. Region Syddanmark*, 2010; *VL v. Szpital Kliniczny im. dra J. Babińskiego SPZOZ v. Krakowie*, 2021).
- ▶ Vaihtoehtoisesti sijaismuuttujaan liittyvä syrjintä voi olla välillistä syrjintää, jos sääntö, peruste tai käytäntö, mukaan lukien sijaismuuttuja, vaikuttaa suhteettomalla tavalla henkilöihin, joilla on kiellettyihin syrjintäperusteisiin kuuluvia ominaisuuksia (katso käytännön selitys tästä asiasta *Jyske Finans v. Ligebehandlingsnævnet*, 2017 (C-668/15)).

Keskeinen tapaus: *Dekker v. Stichting Vormingscentrum* (1990)

Työnantajan todettiin loukanneen välittömästi miesten ja naisten tasa-arvoisen kohtelun periaatteen toteuttamisesta mahdollisuuksissa työhön, ammatilliseen koulutukseen ja uralla etenemiseen sekä työoloissa annetussa direktiivissä (neuvoston direktiivi 76/207/ETY) esitettyä tasa-arvoisen kohtelun periaatetta, koska työnantaja kieltäytyi tekemästä työsopimusta sellaisen naispuolisen hakijan kanssa, jonka se oli katsonut soveltuvaksi tekemään kyseistä työtä, ja kieltäytymisen perusteena olivat sellaiset raskaana olevan naisen työhön ottamisesta mahdollisesti aiheutuvat, työnantajan kannalta haitalliset seuraukset, jotka johtuvat viranomaisten antamista työkyvyttömyyttä koskevista säännöistä, joissa ei tehdä eroa sen mukaan, johtuuko työtehtävien hoitamisen estyminen raskaudesta ja synnytyksestä vai sairaudesta. Tuomioistuimien totesi, että kyse oli sukupuoleen perustuvasta välittömästä syrjinnästä, koska raskaus voidaan esittää työhön ottamisesta kieltäytymisen syyksi ainoastaan naisten kohdalla.

Sijaismuuttujat

Syrjimättömyyslainsäädännön kontekstissa ”sijaismuuttujilla” viitataan ominaisuuksiin tai niiden yhdistelmiin, joita ei itsessään ole sisällytetty kiellettyjen syrjintäperusteiden luokkaan asianmukaisessa oikeudellisessa kehyksessä, mutta jotka korreloivat näiden perusteiden kanssa siten, että niiden käyttö voi johtaa laittomaan syrjintään. Yksi esimerkki tästä on postinumero. Postinumero ei itsessään ole syrjivä, mutta se voi toimia kielletyn syrjintäperusteen, kuten etnisen alkuperän, sijaismuuttujana, jos tietyllä alueella esimerkiksi asuu paljon maahanmuuttajia tai tietyn etnisen alkuperän omaavia henkilöitä.

Sijaismuuttajat voidaan tunnistaa yliedustuksesta: jos tietyn kielletyn syrjintäperusteen omaavat henkilöt ovat yliedustettuina ryhmässä, tämän ryhmän tunnisteet ovat todennäköisesti sijaismuuttajia. Näin ollen yllä olevassa esimerkissä postinumero voidaan tunnistaa sijaismuuttajaksi, koska eri alkuperiä omaavat henkilöt ovat yliedustettuina tietyillä alueilla.

Kun sijaismuuttujaa käytetään algoritmijärjestelmän syötteenä, syrjintä on mahdollista. On huomattava, että sijaismuuttujan tyyppin mukaan sijaismuuttujien käyttö voi viitata sekä välittömään että välilliseen syrjintään (Weerts et al., 2024). Tiettyjen ominaisuuksien tiedetään aiheutta koskevien tutkimusten ja asiaankuuluvan oikeuskäytännön perusteella olevan kiellettyjen syrjintäperusteiden sijaismuuttajia. Sijaismuuttajia voidaan tunnistaa myös ymmärtämällä ja analysoimalla algoritmijärjestelmän käyttökontekstia ottaen huomioon olemassa olevat historialliset eriarvoisuudet ja väestötiedot.

Katso lisätietoja ja esimerkkejä erityyppisistä sijaismuuttajista [liitteestä E](#).

[Chezin tapauksessa \(C-83/14\)](#) määrättiin kollektiivinen toimenpide (sähkömittareiden sijoittaminen romanien asuinalueelle kuudesta seitsemään metrin korkeudelle muiden alueiden alle kahden metrin korkeuden sijaan) asuinalueelle, jonka asukkaat olivat pääasiassa mutta eivät yksinomaan romanitaustaisia. Jos käy ilmi, että kyseinen toimenpide on otettu käyttöön ja/tai pidetty voimassa suurimmalle osalle kyseisen kaupunginosan asukkaista yhteiseen etniseen alkuperään liittyvistä syistä, toimenpide merkitsee välitöntä tai välillistä syrjintää, joka kohdistuu myös muihin kuin romanitaustaisiin alueen asukkaisiin. Kansallisen tuomioistuimen tehtävänä oli arvioida asia ottamalla huomioon kaikki sen kannalta merkitykselliset seikat ja direktiivin 2000/43 8 artiklan 1 kohdassa tarkoitetut todistustaakan kääntämistä koskevat säännöt.

Esimerkki algoritmeista: korkeakoulujen opintoavustuksen tarkastus

Tämä esimerkki auttaa selittämään, kuinka sijaismuuttajat toimivat. Tässä tapauksessa ominaisuudet ”vanhempien lähellä asuminen” ja ”ammattillisen koulutuksen suorittaminen” toimivat ominaisuuden ”muu kuin eurooppalainen maahanmuuttajatausta” sijaismuuttujina.

Alankomaiden koulutuksen toimeenpanovirasto (Dienst Uitvoering Onderwijs eli DUO) pyrkii tarkistusten avulla varmistamaan, että opintoavustukset on myönnetty asianmukaisesti. Tätä prosessia kutsutaan korkeakoulujen opintoavustuksen tarkastukseksi (hollanniksi tästä käytettiin lyhennettä CUB). Syntyi epäily, että nykyään lopetettu CUB-prosessi syrji maahanmuuttajataustaisia opiskelijoita. Tämä epäily perustui opiskelijoiden tekemiin valituksiin tapauksissa, joissa opiskelijoiden väitettiin saaneen avustuksia väärin perustein. Opiskelijoita edustaneet asianajajat huomasivat, että heidän asiakkaansa olivat ylivoimaisesti maahanmuuttajataustaisia. Tutkinnassa paljastui, että prosessissa käytettiin petosriskin pisteytysjärjestelmää avustusten (laittoman) käytön tutkinnan priorisointiin.

Algorithm Audit analysoi algoritmijärjestelmää ja CUB-prosessin eri vaiheiden käsitte-lyeroja sekä tutki, voidaanko järjestelmään syötettyjä tietoja pitää sijaismuuttujina.⁴⁵ Järjestelmän havaittiin käyttävän kolmea syötettä: opiskelijan ikää, koulutustasoa ja etäisyyttä opiskelijan ja hänen vanhempiansa osoitteiden välillä. Kansalaisuutta, maahanmuuttotustausta tai muita rotuun tai etniseen alkuperään liittyviä tietoja ei käytetty petosten pisteytysjärjestelmässä.

Algorithm Auditin tärkeimmät havainnot olivat seuraavat:

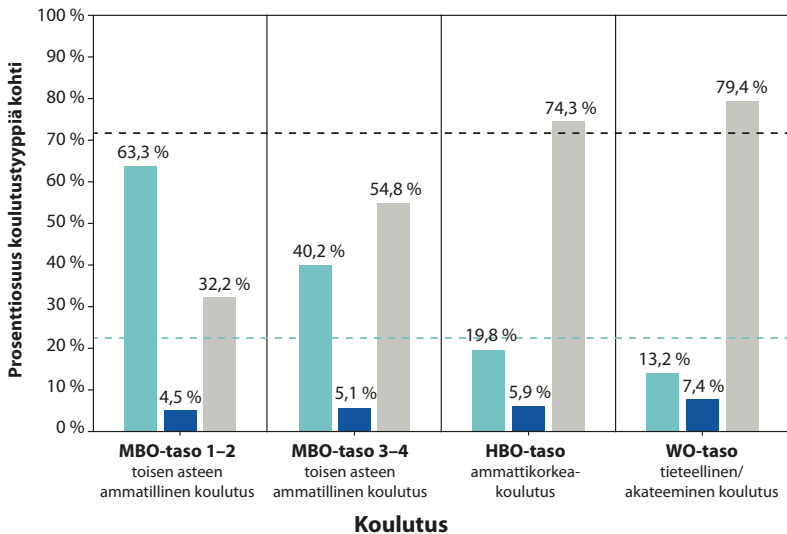
- ▶ CUB-prosessi johti kaiken kaikkiaan muun kuin eurooppalaisen maahanmuuttajataustan omaavien opiskelijoiden eriarvoiseen kohteluun.
- ▶ Riskiprofiileissa määritettiin korkeammat riskipisteet maahanmuuttajataustaisille opiskelijoille: muun kuin eurooppalaisen taustan omaavilla maahanmuuttajaopiskelijoilla oli kaksi kertaa suurempi todennäköisyys joutua suuririskiseen luokkaan kuin alankomaalaistaustaisilla opiskelijoilla.
- ▶ Opiskelijoiden manuaalinen lisävalinta kontrolliryhmään vahvisti yliedustusta sen vähentämisen sijaan. Muun kuin eurooppalaisen maahanmuuttajataustan omaavat opiskelijat joutuivat alankomaalaistaustaisia opiskelijoita 6,2 kertaa todennäköisemmin tarkastukseen, johon sisältyi invasiivinen kotikäynti.

Alankomaalainen tuomioistuin totesi, ettei tällä käytännöllä ollut objektiivisia perusteita, ja sen katsottiin aiheuttavan välillistä syrjintää (Rechtbank Overijssel, 2024).

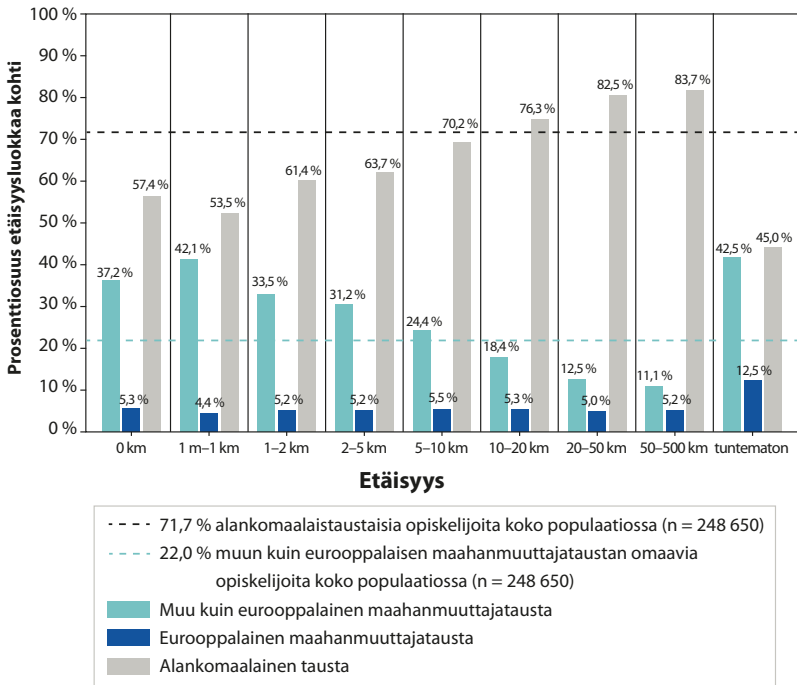
Yksityiskohtaiset analyysit osoittivat, että riskipisteytysjärjestelmä antoi korkeammat riskipisteet alempien koulutusasteiden (ammatillinen koulutus) sekä lähempänä vanhempiaan asuville opiskelijoille. Molempien muuttujien osoitettiin korreloivan (voimakkaasti) maahanmuuttajataustan kanssa, eli ne toimivat maahanmuuttajataustan sijaismuuttujina (katso alla olevat kaaviot).

45. Algorithm Audit sai täydet käyttöoikeudet sekä algoritmiin että DUO:n sisäisiin tietoihin. Yleisen tietosuojasetuksen vuoksi DUO ei kerää tai käsittele tietoja opiskelijoiden alkuperästä CUB-prosessin tarkoituksia varten. Näitä analyysejä varten DUO ja Algorithm Audit tekivät yhteistyötä Alankomaiden kansallisen tilastoviraston (Netherlands Statistics tai CBS) kanssa. CBS toimitti syntymä- ja alkuperämaita koskevat yhdistetyt tilastotiedot Algorithm Auditin määrittelemien populaatioiden perusteella kullekin prosessivaiheelle (riskiluokka, valinta kontrolliin, tulosten kontrolli, valitusmenettely ja valituksen tulos) ja syötemuuttujille (koulutus, ikä ja etäisyys vanhempaan/vanhempiin).

Kaavio 1: (Muun kuin) eurooppalaisen maahanmuuttajataustan ja alankomaalaisen taustan omaavien, opintoavustusta saavien populaatioiden jakauma koulutustyyppin mukaan – 2014 (n = 248 650)



Kaavio 2: (Muun kuin) eurooppalaisen maahanmuuttajataustan ja alankomaalaisen taustan omaavien, opintoavustusta saavien populaatioiden jakauma osoitteiden välisten etäisyyksien mukaan – 2014 (n = 248 650)



Kaavion lähde: Algorithm Audit
 Täydellinen selitys: katso Algorithm Audit, 2024a ja 2024b.

Verrokkit

Verrokilla viitataan tässä henkilöön, joka on samankaltaisessa tilanteessa kuin kantelija, mutta jolla ei ole syrjinnän perusteeksi oletettua, kiellettyihin syrjintäperusteisiin kuuluvaa ominaisuutta.

Huomio: On mahdollista, että kahden ihmisryhmän voidaan katsoa olevan vastavassa tilanteessa yhden valituksen yhteydessä mutta ei toisen. Siksi on aina tärkeää arvioida verrokkeja riidanalaisen toimen tavoitteiden kannalta (Euroopan neuvosto ja Euroopan unionin perusoikeusvirasto, 2018: 44–49).

Asianmukaisen verrokin valinta on tärkeää algoritmijärjestelmien näyttöä arvioitaessa ja erityisesti silloin, kun arvioidaan järjestelmän tarkoitusta, koulutus-, testaus- ja validointitoimenpiteitä sekä varsinaista testausta ja arviointeja. Erityisesti voi olla tarpeen arvioida, käytettiinkö kiellettyihin syrjintäperusteisiin kuuluvien ominaisuuksien tietoja algoritmijärjestelmän kouluttamiseen ja millaisia valintoja järjestelmää testattaessa on tehty. Tätä käsitellään tarkemmin kohdissa 3.3, 3.5 ja 3.6.

Syrjintäolettan osoittaminen

EU:n syrjimättömyysdirektiivien mukaan, kun henkilö, joka katsoo kärsineensä vääryyttä sen vuoksi, että häneen ei ole sovellettu yhdenvertaisen kohtelun periaatetta, esittää tuomioistuimessa tai muussa toimivaltaisessa viranomaisessa tosiseikkoja, joiden perusteella voidaan olettaa tapahtuneen välitöntä tai välillistä syrjintää, vastaajan on näytettävä toteen, että yhdenvertaisen kohtelun periaatetta ei ole rikottu.⁴⁶ Katso myös [vaihe 3.8](#).

Tämä tarkoittaa, että kantelijan on esitettävä riittävästi näyttöä, jotta syrjintäolettan voidaan osoittaa.

Tämän jälkeen todistustaakka siirtyy vastaajalle. Käytännössä kansallisilla tuomioistuimilla on harkintavaltaa sen määrittämisessä, milloin kantelijan esittämä näyttö riittää siirtämään todistustaakan vastaajalle.⁴⁷

Näyttö voi sisältää tilastotietoja,⁴⁸ kirjallisia asiakirjoja – jos niissä on syrjintään liittyvää sisältöä tai ne liittyvät kantajan tapaukseen – sekä asiaankuuluvista lähteistä saatuja raportteja ja analyyskejä (katso [vaiheessa 2](#) kerätyt tiedot), tilannetestausta (katso [vaihe 3.6](#)), arkipäätteitä, todistajanlausuntoja ja aihetodisteista tehtyjä päätelmiä. EUT on korostanut, että on tärkeää ”ottaa huomioon kaikki riidanalaiseen käytäntöön liittyvät olosuhteet” (C-83/14 CHEZ, 80–84 kohta). Näin ollen sekä tilastollisia että kvalitatiivisia tietoja voidaan käyttää syrjintäolettan osoittamiseen, ja on perusteltua väittää, että tosiasiaa molempia tulisi hyödyntää.

46. Direktiivi 2000/78/EY, 10 artikla, direktiivi 2006/54/EY, 19 artikla, direktiivi 2000/43/EY, 8 artikla.

47. Käytännössä tämä vaihtelee usein välillisen ja välittömän syrjinnän tapausten välillä. Lisätietoja: katso Farkas ja O’Farrell (2015).

48. Lisätietoja tilastoista todistusaineistona on jäljempänä kohdassa ”[Tilastotietojen lähestymistapa](#)”.

Mitä ”yhdenvertaisuustiedot” ovat?

Tässä arviointimenetelmässä viitataan sekä kvantitatiivisiin (mukaan lukien tilastolisiin) että kvalitatiivisiin tietoihin termillä ”yhdenvertaisuustiedot”. Tämä perustuu seuraavaan yhdenvertaisuustietoja koskeissa ohjeissa (Euroopan komissio, 2021) annettuun määritelmään:

mikä tahansa tieto, joka on hyödyllinen yhdenvertaisuuden tilan kuvaamisen ja analysoinnin kannalta. Tiedot voivat olla luonteeltaan kvantitatiivisia tai kvalitatiivisia. Ne voivat sisältää yhdistettyjä tietoja, jotka kuvastavat eriarvoisuutta tai sen syitä tai vaikutuksia yhteiskunnissa. Joskus yhdenvertaisuustietojen tuottamiseen voidaan käyttää tietoja, jotka on kerätty ensisijaisesti muuhun kuin yhdenvertaisuustarkoitukseen. (Euroopan komissio, 2021: 8)

Yhdenvertaisuustietoja käytetään muun muassa luotettavan näytön esittämiseen hallinnollisissa tai oikeudellisissa syrjintätapauksissa välilliseen tai välittömään syrjintään viittaavien tietojen avulla sekä vaikuttamisen ja tietoisuuden lisäämisen tukemiseen yhdenvertaisuuden ja syrjimättömyyden alalla (Euroopan komissio, 2021: 9).

Lisämateriaaleja

- ▶ ”Handbook on identifying and using equality data in legal casework” (Ilieva, 2024)
- ▶ ”Strategic litigation handbook” (Equinet, 2017)
- ▶ ”Handbook: artificial intelligence, judicial decision-making and fundamental rights” (JuLIA Project, 2024).

Vaiheen 3 käyttö

Seuraavissa kohdissa esitetään ohjeistavia kysymyksiä, jotka voivat auttaa yhdenvertaisuuselimiä määrittämään, onko kyseessä *prima facie*-syrjintätapaus. Tavoitteena on osoittaa, mistä vaiheessa 2 kerätyistä tiedoista voidaan löytää sovellettavaa näyttöä, mitä näytöstä kannattaa etsiä ja miten näyttöä voidaan käyttää syrjinnän osoittamiseen.

Jokaisessa tämän osan kohdassa noudatetaan seuraavaa perusrakennetta.

- ▶ Selitys siitä, mitä yhdenvertaisuuselimen on arvioitava.
- ▶ Kysymyksiä, joita kannattaa pohtia tietoja arvioitaessa.
- ▶ Mahdollisia tiedonlähteitä.
- ▶ Syrjinnän indikaattorit.

Kohdissa 3.7 ja 3.8 esitetään sitten viitekehys, jolla voidaan arvioida, riittääkö kerätty näyttö tukemaan tekoäly- tai algoritmijärjestelmään liittyvän syrjinnän *prima facie*-tapausta (3.7 [Näytön riittävyyden arviointi](#)) ja kuinka todennäköisesti vastaaja pystyy kumoamaan syrjintäolettan tai esittämään perustelut mahdolliselle syrjinnälle (3.8 [Voiko vastaaja osoittaa, ettei erilainen kohtelu ole syrjivää?](#)). Tämä auttaa

määrittämään, onko vastaajaa vastaan ryhdyttävä toimenpiteisiin. Näiden tehtävien prosessissa ja näytön tutkimisessa on väistämättä jonkin verran päällekkäisyyksiä.

On erittäin epätodennäköistä, että yhdenvertaisuuselin voi saada pääsyn kaikkiin tietoihin tai vastata kaikkiin kysymyksiin tässä vaiheessa. Sen sijaan kysymykset on tarkoitettu antamaan ohjeita siitä, minkä tyyppisiä tietoja voi olla saatavilla ja miten niitä voidaan arvioida sekä erikseen että kollektiivisesti.

Liitteessä K on mallilomake, jota voidaan käyttää tietojen kirjaamisen apuna ja mukauttaa yhdenvertaisuuselimen tarpeiden mukaan.

Lisämateriaaleja

Osa vaiheen 3 käsitteistä voi olla uusia tai tuntemattomia. Alla mainitut resurssit auttavat selittämään näitä tarkemmin.

- ▶ Wachter, Mittelstadt ja Russell, 2020, Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI. *Computer Law & Security Review*, Vol. 41, heinäkuu 2021.
- ▶ Mittelstadt, 2024, How to use the Artificial Intelligence Act to investigate bias and discrimination: A guide for equality bodies, *Equinet*.

3.1. Mitä tunnettuja tai epäiltyjä syrjinnän riskejä on?

Algoritmi järjestelmien käyttöön tietyissä konteksteissa voi liittyä syrjivien käytäntöjen luontainen riski. Kun algoritmista syrjintää on aiemmin osoitettu tapahtuneen vastaavanlaisessa käyttötapauksessa vastaavalla sektorilla, tämä voi viitata laajempaan syrjintäriskiin, joka koskee myös arvioitavana olevaa tapausta. Jos esimerkiksi on osoitettu, että poliisitoiminnassa käytetty kasvontunnistus on syrjivää, on todennäköistä, että myös muihin tarkoituksiin käytetty kasvontunnistus on syrjivää.

3.1.1. Onko tekoälyasetuksessa nimenomaisesti mainittu syrjintäriskien vuoksi algoritmijärjestelmän tyyppi tai kohdeala, jolla sitä sovelletaan?

Tekoälyasetuksessa viitataan sekä sektoreihin että niiden sisäisiin käyttötapauksiin.

Kun algoritmijärjestelmiä käytetään sektoreilla, joilla esiintyy historiallista eriarvoisuutta ja/tai joilla syrjintää on osoitettu esiintyvän usein, tämän tulisi lisätä epäilyksiä syrjinnästä. Algoritmi järjestelmät perustuvat tosielämän dataan. Olemassa olevat eriarvoisuudet ja inhimilliset vinoumat heijastuvat datassa, ja siksi niitä voi usein esiintyä ja ne voivat voimistua algoritmijärjestelmässä.

Historiatietoihin perustuva datan vinouma: esimerkki algoritmeista: Amazonin rekrytointityökalu

Amazon kehitti tekoälypohjaisen rekrytointityökalun, joka oli koulutettu aiemmillä, pääasiassa miespuolista hakijakuntaa edustavilla ansioluetteloilla. Tämän seurauksena järjestelmä oppi, että miespuoliset hakijat olivat suosittavia. Vaikka järjestelmä ei nimenomaisesti käyttänyt sukupuolta syötteenä, se hyödynsi naispuolisuuteen liittyviä sijaismuuttujia – kuten sanaa ”naisten” (esimerkiksi ”naisten shakkijoukkueen kapteeni”) tai naisten korkeakoulujen tutkintoja – ja alensi järjestelmällisesti naishakijoiden hakemusten pisteitä (Dastin, 2018).

Monet tekoälyasetuksen suuririskisistä käyttötapauksista luokiteltiin EU:ssa suuririskiksi nimenomaan syrjintäriskin vuoksi. Tekoälyasetuksen johdanto-osan kappaleissa 54 ja 56–60 mainitaan nimenomaisesti syrjintään, historiallisten syrjinnän muotojen jatkumiseen ja tiettyihin haavoittuvuuksiin liittyvät riskit. Vaikka järjestelmä ei olisi teknologisesti monimutkainen ja/tai tekoälypohjainen, (sääntöpohjaisten) algoritmijärjestelmien käyttöön näissä käyttötapauksissa liittyy samanlainen syrjintäriski. [Liitteessä I](#) on kuvattu suuririskisten tekoälyjärjestelmien käyttöaloja ja -tapauksia.

Käyttötapaus, johon on nimenomaisesti viitattu tekoälyasetuksessa, vaatii lisätarkastelua. Lisäksi näissä tapauksissa voi olla käytettävissä sekä kvalitatiivisia että kvantitatiivisia yhdenvertaisuustietoja, joita voidaan usein löytää oikeuskäytännöstä ja akateemisista, kansalaisjärjestöjen tai hallituksen raporteista. Katso myös kohta [2.1.2 Olemassa oleva oikeuskäytäntö](#) ja muut lähteet.

Huomio: jos järjestelmä on suuririskinen tekoälyjärjestelmä, joka on kirjattu EU:n tietokantaan, mukaan lukien tietokannan B-osa,⁴⁹ siihen nimenomaan viitataan tekoälyasetuksessa ja se voi täten aiheuttaa korkean syrjintäriskin.

Pohdittavia kysymyksiä

- ▶ Sisältääkö algoritmijärjestelmä sellaisen ”tyypin” teknologiaa, jonka tiedetään aiheuttavan syrjintäriskin, kuten profilointia (6 artiklan 3 kohta ja johdanto-osan kappale 53), ennakoivaa riskianalytiikkaa (johdanto-osan kappale 42) tai biometriikkaa ja tunteiden tunnistamista (liitteen III 1 kohta, johdanto-osan kappaleet 44 ja 54)?
- ▶ Liittyikö päätös tai koettu kohtelu johonkin seuraavista sektoreista?
 - Yleissivistävä ja ammatillinen koulutus (liitteen III 3 kohta, johdanto-osan kappale 56).
 - Työllistäminen, henkilöstöhallinto ja itsenäisen ammatinharjoittamisen mahdollistaminen (liitteen III 4 kohta, johdanto-osan kappale 57).

49. Jos järjestelmä on EU:n tietokannan B-osiossa, tarjoaja on itse arvioinut sen olevan suuririskisellä alalla käytettävä järjestelmä, mutta sen ei katsota aiheuttavan riskiä rajoitettujen poikkeusten perusteella (katso tekoälyasetus, 6 artiklan 3 kohta). Vaikka tekoälyasetuksen edellyttämää dokumentaatiota ei todennäköisesti ole saatavilla, tätä järjestelmää sovelletaan kohdealueella, johon tekoälyasetuksessa nimenomaisesti viitataan sen syrjintäriskien vuoksi.

- Välttämättömien yksityisten palvelujen ja välttämättömien julkisten palvelujen ja etuuskien (sosiaalihuolto) saatavuus ja käyttö (liitteen III 5 kohdan a alakohta).
 - Luottopisteytyksen määrittäminen (liitteen III 5 kohdan b alakohta, johdanto-osan kappale 58).
 - Sairaus- ja henkivakuutukset (liitteen III 5 kohdan c alakohta, johdanto-osan kappale 58).
 - Terveystietopalvelujen saatavuus ja käyttö (liitteen III 5 kohdan a alakohta, johdanto-osan kappale 58).
 - Lainvalvonta (liitteen III 6 kohta, johdanto-osan kappale 59).
 - Muuttoliikkeen hallinta, turvapaikka-asiat ja rajavalvonta (liitteen III 7 kohta, johdanto-osan kappale 60).
 - Oikeudenhoidon (liitteen III 8 kohdan a alakohta, johdanto-osan kappale 61).
 - Demokraattiset prosessit (liitteen III 8 kohdan b alakohta, johdanto-osan kappale 61).
- Jos tapaus liittyy johonkin edellä mainituista sektoreista, kattaako se käyttötapausten, joka on lueteltu liitteen III asiaankuuluvassa jaksossa (mukaan lukien asiaankuuluvassa johdanto-osan kappaleissa)?

Mahdollisia tiedonlähteitä yleisesti osoitetun syrjintäriskin arviointiin

EU:n tekoälyasetus

- 6 artikla, liite III ja johdanto-osan kappaleet – näissä on kuvattuja suuririskisiä tekoälytyyppejä.
- 5 artikla – tässä on kuvattu kielletyt tekoälykäytännöt. Katso myös johdanto-osan kappaleet 28–45.

Muut

- Komission ohjeet kielletyistä tekoälykäytännöistä: Commission's guidelines on prohibited artificial intelligence (AI) practices, as defined by the AI Act.
- Tulevat ohjeet: Commission guidelines on classification of high-risk AI systems and related requirements.⁵⁰

Syrjintäriskin indikaattorit

Jos jotakin näistä indikaattoreista voidaan soveltaa tapaukseen, se ei itsessään ole todiste syrjinnästä. Nämä indikaattorit voivat kuitenkin viitata järjestelmään, johon liittyy syrjintäriski, seuraavissa tilanteissa:

- jos järjestelmä on A- tai C-osioon sisältyvä suuririskinen tekoälyjärjestelmä
- ei-suuririskinen järjestelmä:

50. Tämän arviointimenetelmän editointihetkellä komissio on julkaissut ohjeiden luonnoksen, jolle pyydetään palautetta: [Commission seeks feedback on the draft guidelines for the classification of high-risk artificial intelligence systems](#).

- jos järjestelmää on tarkoitus käyttää joko sektorilla, jolla on tunnistettu syrjintäriski (liite III tai johdanto-osan kappaleet), ja/tai
- jos kyseessä on teknologiatyyppi, johon liittyy tunnettu syrjintäriski.

Kirjaa tietoihin, onko järjestelmä suuririskinen vai ei, tai onko se tarkoitettu käytettäväksi sektoreilla tai aloilla, joihin liittyy tekoälyasetuksen mukaan syrjintäriski.

Epäilty virheellinen tekoälyasetuksen mukainen luokittelu

Jos yhdenvertaisuuselin epäilee, että järjestelmä on virheellisesti itsearvioitu ei-suuririskiseksi tekoälyjärjestelmäksi tai että sitä ei ole tunnistettu kielletyksi tekoälykäytännöksi (katso epäillyt kielletyt tekoälyjärjestelmät [vaiheesta 1.4](#)), yhdenvertaisuuselimen on ilmoitettava asiasta asiaankuuluvalla markkinavalvontaviranomaiselle riippumatta siitä, voidaanko syrjintätapausta osoittaa (katso myös [vaihe 4](#)).

3.1.2. Ovatko kansalliset tai alueelliset viranomaiset, kansalliset tai kansainväliset kansalaisjärjestöt tai ihmisoikeusjärjestöt havainneet tunnetun syrjintäriskin tällä sektorilla tai tässä teknologiassa?

Oikeusasiamieslaitosten, kansalaisyhteiskunnan ja akateemisten laitosten raportointi sekä olemassa oleva oikeuskäytäntö voivat osoittaa, että tietyn kielletyn syrjintäperusteen tuloksiin liittyy eriarvoisuutta.

Arvioi vaiheessa 2 kerättyjen tietojen avulla, onko tämä järjestelmä tai järjestelmätyyppi jo tunnettu tai epäilty syrjiviä tuloksia tuottava järjestelmä. Kaikki asiaankuuluvat tiedot voivat myös auttaa seuraavissa vaiheissa.

Tässä vaiheessa sektorikohtaisesta asiantuntemuksesta voi olla hyötyä.

Mahdollisia tiedonlähteitä yleisesti osoitetun syrjintäriskin arviointiin

- ▶ Yhdenvertaisuuselimen seuranta, tutkimukset tai selvitykset
- ▶ Kansalaisjärjestöjen ja kansallisten ja kansainvälisten elinten raportit
- ▶ Olemassa oleva oikeuskäytäntö
- ▶ Internethaut
- ▶ Asiantuntijat

Syrjinnän indikaattorit

- ▶ Muut ovat havainneet tai epäilevät syrjintää vastaajan algoritmijärjestelmien tietyssä käyttötapauksessa, jonka senhetkinen tapaus myös kattaa.

- ▶ Muut ovat havainneet tai epäilevät syrjintää algoritmijärjestelmien samankaltaisissa käyttötapauksessa, jonka senhetkinen tapaus myös kattaa, mikä osoittaa mahdollisen syrjivän kuvion olemassaolon.

Kirjaa tietoihin alue, jolla riskin tiedetään esiintyvän, teknologia ja kaikki muut asiaankuuluvat tiedot ja todisteet. Esimerkkejä:

Sektori: lainvalvonta

Teknologia: kasvontunnistus, biometriikka

Tiedonlähteet: kansalaisjärjestön / akateemisen laitoksen tekemä tutkimus, tekoälyasetuksen 5 artikla (kielletyt järjestelmät), 6 artikla (suuririskiset järjestelmät) ja liite III.

Käyttötapaukset, joita on pidettävä suuririskisinä tai kiellettyinä tekoälyasetuksen mukaan

Jos tietyssä algoritmisessa käyttötapauksessa havaittu syrjivien tulosten kuvio on vahva ja johdonmukainen mutta ei sisälly liitteen III luetteloihin, yhdenvertaisuuselinten on harkittava käyttötapauksen ilmoittamista Euroopan komissiolle, jotta se voidaan lisätä 7 artiklan mukaiseen luetteloon (katso [vaihe 4.3.2](#)).

Tilanteet, joissa yhdenvertaisuuselin toteaa tekoälykäytännön olevan perustavanlaatuisesti ristiriidassa unionin perusoikeuskirjassa kuvattujen ihmisarvon, vapauden, yhdenvertaisuuden, demokratian ja oikeusvaltioperiaatteen arvojen sekä perusoikeuksien kunnioittamisen kanssa, mutta käytäntöä ei ole kielletty eikä pidetä suuririskisenä tekoälyasetuksen mukaan (katso [vaihe 4.3.2](#)).

3.2. Sisältyykö syötteisiin tai datajoukkoihin tunnettuja syrjintäperusteita tai sijaismuuttujia?

Algoritmijärjestelmän syöttödata määrittelee tuotoksen ja siten järjestelmän tuloksen. Siksi syrjintää on epäiltävä, jos algoritmijärjestelmä käyttää syötteenä kiellettyä syrjintäperustetta (katso [kielletyt syrjintäperusteet](#)) tai sijaismuuttujaa (katso [sijaismuuttujaan liittyvä syrjintä](#)).

Tässä vaiheessa sektorikohtainen asiantuntemus voi olla hyödyllistä.

Pohdittavia kysymyksiä

- ▶ Käsitelläänkö henkilötietoja, jotka paljastavat kiellettyjä syrjintäperusteita tai niiden sijaismuuttujia?
- ▶ Viitataan asiaankuuluvissa asiakirjoissa kiellettyihin syrjintäperusteisiin tai tunnettuihin sijaismuuttujiin (katso [liite E](#))?
- ▶ Mainitaan kielletyt syrjintäperusteet tai tunnetut sijaismuuttujat suoraan järjestelmän syötteissä (joko koulutuksessa, testauksessa tai käytössä)?

Tämä voidaan muotoilla esimerkiksi seuraavasti: "X:ää, Y:tä ja Z:aa käytetään ennakkointiin/laskentaan".

- ▶ Onko yksi järjestelmän syötteistä tai niiden yhdistelmä todennäköinen sijaismuuttuja kielletylle syrjäntäperusteelle sektorikohtaisen tiedon perusteella? Tähän kysymykseen vastaaminen voi edellyttää kansallisten tilastojen tai sellaisten sektorikohtaisten asiantuntijoiden konsultointia, joilla on tietoa eriarvoisuuden esiintymisestä ja suhteista tietyllä sektorilla. Esimerkkejä:
 - Maissa, joissa terveydenhuoltoon liittyvistä kustannuksista voi saada vero- vähennyksiä, vammaiset henkilöt ovat todennäköisesti yliedustettuina tätä vähennystä hyödyntävien henkilöiden joukossa. Näin ollen tämän vähennyksen käyttö on todennäköinen sijaismuuttuja vammaisuudelle.
 - Monissa maissa maahanmuuttajataustaiset ihmiset ovat aliedustettuina korkeakoulututkimuksen suorittaneiden henkilöiden joukossa, joten koulutustaso on todennäköinen sijaismuuttuja rodulle / etniselle taustalle.
- ▶ Liittyykö jokin mainituista sijaismuuttujista erottamattomasti kiellettyyn syrjäntäperusteeseen? Katso [liite E – Sijaismuuttujat](#).
- ▶ Voidaanko epäilyä siitä, että syöte (tai syötteiden yhdistelmä) on sijaismuuttuja, tukea todisteilla? Onko esimerkiksi saatavilla kansallisen tilastokeskuksen tai akateemisen laitoksen tekemien tutkimusten tilastoja, jotka osoittavat kiellettyihin syrjäntäperusteisiin kuuluvan ominaisuuden omaavien henkilöiden yli- tai aliedustuksen tietyssä syötteiden alaryhmässä? Esimerkkejä:
 - Jos koulutustaso on yksi etnisen alkuperän sijaismuuttujaksi epäillyistä tekijöistä, onko saatavilla tilastoja, jotka osoittavat, että maahanmuuttajataustaiset henkilöt ovat yliedustettuina ammatillisen tutkinnon suorittaneiden joukossa?

Huomio: Tällaisen todistusaineiston kerääminen saattaa vaatia asiantuntijatukea yhteistyökumppaneilta, joilla on kokemusta data-analytiikasta.

- ▶ Onko järjestelmä koulutettu, testattu tai validoitu kiellettyjä syrjäntäperusteita sisältävillä tiedoilla? (Katso [vaihe 3.5](#))

Mahdollisia tiedonlähteitä järjestelmän syötteiden ymmärtämiseen

Kantelija

- ▶ Luettelo kantelijan vastaajalle toimittamista tiedoista.
- ▶ Kantelijalle annetut selitykset, perustelut ja todisteet tapaukseen liittyvästä kohtelusta.

Yleinen tietosuoja-asetus, 13 ja 14 artikla: rekisteröidylle toimitettavat tiedot

- ▶ Rekisteröidylle (kantelijalle) toimitettavat tiedot, kun henkilötietoja kerätään rekisteröidyltä (yleinen tietosuoja-asetus, 13 artikla).
- ▶ Rekisteröidylle toimitettavat henkilötiedot, kun tietoja ei ole saatu rekisteröidyltä (yleinen tietosuoja-asetus, 14 artikla).
- ▶ Automaattiseen päätöksentekoon liittyvä logiikka (13 artiklan 2 kohdan f alakohta ja 14 artiklan 2 kohdan g alakohta).

Yleinen tietosuoja-asetus, DSAR-pyyntöön saatu vastaus

- ▶ Kyseessä olevat henkilötietoryhmät (15 artiklan 1 kohdan b alakohta): rekisterinpitäjän on toimitettava rekisteröidylle kopio käsiteltävistä henkilötiedoista. Tämä voi sisältää kolmansien osapuolten toimittamia tietoja (yleinen tietosuoja-asetus, 14 artikla).
- ▶ Mahdollisesti: päätöksenteossa käytetyt syöttömuuttujat tai parametrit ja niiden muodostus (esimerkiksi tilastotietojen avulla) sekä niiden merkitys kokonaispisteytyksessä (julkisasiamies P. Pikamäen ratkaisuehdotus, asia SCHUFA Holding, 2023, 58 kohta).

EU:n tekoälyasetus, 86 artikla: oikeus selitykseen

- ▶ Syöttödata ja tehdyn päätöksen pääkohdat.

Julkisesti saatavilla olevat tiedot

- ▶ EU:n tietokanta suuririskisistä tekoälyjärjestelmistä: A-osion suuririskiset tekoälyjärjestelmät – kuvaus järjestelmän käyttämistä tiedoista (data ja syötteet) ja toimintalogiikasta.
- ▶ Alustan usein kysytyt kysymykset.
- ▶ Yhtiön julkinen viestintä.

Vastaaja

Tarjoajalta:

EU:n tekoälyasetus, 11 artikla ja liite IV: tekninen dokumentaatio

- ▶ Liitteen IV 2 kohdan b alakohta, tekoälyjärjestelmän ja algoritmien yleinen logiikka, periaatteet ja tehty oletukset, myös niiden henkilöiden tai henkilöryhmien osalta, joihin järjestelmää on tarkoitus käyttää, tärkeimmät luokitusvalinnat, se, mihin nähden järjestelmä on suunniteltu optimoitumaan, ja eri parametrien merkitys sekä kuvaus järjestelmän odotetusta tuotoksesta ja tuotoksen laadusta.
- ▶ Liitteen IV 2 kohdan d alakohta, yleinen kuvaus datajoukoista sekä tiedot niiden alkuperästä, laajuudesta ja pääpiirteistä.

Käyttöönottajalta:

EU:n tekoälyasetus, 27 artikla: perusoikeusvaikutusten arviointi

- ▶ Niiden luonnollisten henkilöiden ja ryhmien luokat, joihin järjestelmän käyttö todennäköisesti vaikuttaa tietyssä käyttöyhteydessä (EU:n tekoälyasetus, 27 artiklan 1 kohdan c alakohta).

Muut

- ▶ Sopimuslausekkeet.
- ▶ Asiakirjatutkimus, olemassa oleva oikeuskäytäntö ja tilastot yli- ja aliedustuksesta kohdealueella.

Syrjinnän indikaattorit

- ▶ Kiellettyjen syrjintäperusteiden suora käyttö järjestelmässä.
- ▶ Kiellettyyn syrjintäperusteeseen erottamattomasti liittyvien sijaismuuttujien käyttö järjestelmässä.
- ▶ Tunnettujen sijaismuuttujien käyttö järjestelmässä.
- ▶ Kiellettyjen syrjintäperusteiden tai sijaismuuttujien käyttö järjestelmän kouluttamisessa, testauksessa tai validoinnissa.

Kaikki edellä mainitut edellyttävät näyttöä siitä, että nämä syötteet johtavat eriarvoiseen kohteluun. Indikaattorit *a* ja *b* viittaavat välittömään syrjintään. Indikaattorit *c* ja *d* viittaavat välilliseen syrjintään.

- ▶ Kirjaa tietoihin kiellettyjen syrjintäperusteiden suora käyttö järjestelmässä. Missä niitä käytetään ja miten?
- ▶ Kirjaa tietoihin kiellettyjen syrjintäperusteiden tai sijaismuuttujien käyttö, jos ne vaikuttavat tai niiden uskotaan vaikuttavan järjestelmän tuloksiin. Tutki järjestelmän teknistä suunnittelua ja (epäiltyjen) sijaismuuttujien vaikutusta järjestelmän tuloksiin. Se, että sijaismuuttujaa käytetään syötteenä, ei itsessään riitä todisteeksi syrjinnästä. Seuraava vaihe on arvioida näyttöä, jotta ymmärretään, johtaako näiden syötteiden käyttö eriarvoiseen kohteluun.⁵¹
- ▶ Jos kyseessä on sijaismuuttuja, liitä tietoihin todisteet tai perustelut siitä, miksi yhdenvertaisuuselin pitää kyseisiä tekijöitä sijaismuuttujina.

3.3. Perusoikeuksiin kohdistuvien riskien arviointi (riskinarvioinnit, HRIA, FRIA ja DPIA)

Suuririskisten tekoälyjärjestelmien tarjoajilla ja käyttöönottajilla on erilaisia velvoitteita tunnistaa ja dokumentoida syrjintäriskejä. Jos algoritmijärjestelmät eivät ole suuririskisiä, tekoälyn tarjoajat ja/tai käyttöönottajat ovat saattaneet tunnistaa ja dokumentoida syrjintäriskit yleisen tietosuoja-asetuksen vaatimusten (erityisesti DPIA-arvioinnit) tai yrityksiä ja ihmisoikeuksia koskevan huolellisuusvelvoitteen (Yhdistyneet kansakunnat, 2011) mukaisesti. Uusia velvoitteita voidaan ottaa käyttöön myös Euroopan neuvoston tekoälyä koskevan puiteyleissopimuksen perusteella.

Syrjintäriskit tunnistetaan yleensä perusoikeusvaikutusten arvioinnissa (FRIA), tietosuoja koskevassa vaikutustenarvioinnissa (DPIA) ja/tai muissa riskinhallintamenetelyissä. Jos nämä prosessit tehdään oikein, niissä tulisi tunnistaa ja kirjata ylös kaikki tekoälyjärjestelmän tai sen avulla tapahtuvan datan käsittelyn aiheuttamat syrjintäriskit sekä kaikki toteutetut lieventävät toimenpiteet ja niiden vaikutukset.

51. Järjestelmän syöte, joka viittaa mahdolliseen kiellettyyn syrjintäperusteeseen tai tunnettuun sijaismuuttujaan mutta ei ole päällekkäinen kielletyn syrjintäperusteen kanssa, ei välttämättä yksinään riitä syrjintäväitteen tueksi. Katso esimerkiksi Tanskan STAR-tapaus. Tässä tapauksessa ennakkointityökalu käytti ennustearvoja "syntyperä" tai "alkuperä". Lautakunta totesi, ettei profiilitökalussa käytetty termi "syntyperä" viitannut etniseen alkuperään. www.retsinformation.dk/eli/accn/W20220951825. Lisätietoja: Equinet, 2022: 23–24.

Teknisessä dokumentaatiossa ja riskinarvioinneissa voidaan mainita vinoumat tai oikeudenmukaisuus eriarvoisuuden tai syrjinnän sijaan.

Tässä vaiheessa sekä teknisestä että sektorikohtaisesta asiantuntemuksesta voi olla hyötyä.

Perusoikeusvaikutusten arviointi: tekoälyasetus

Vaatus tehdä FRIA-arviointi koskee vain tiettyjä suuririskisten tekoälyjärjestelmien käyttöönottajia (katso lisätietoja [vaiheesta 2.2](#)).

FRIA-arvioinnin (ja muiden arviointien) on sisällettävä erilaisia tietoja, jotka tuovat esiin mahdollisia puutteita ja haittoja oikeuksille, kuten syrjimättömyydelle. Tämä sisältää seuraavat:

- ▶ kuvaus käyttöönottajien prosesseista, joissa suuririskistä tekoälyjärjestelmää käytetään tarjoajan käyttötarkoituksen mukaisesti
- ▶ kuvaus ajanjaksosta, jonka kuluessa järjestelmää on tarkoitus käyttää, ja kuinka usein
- ▶ kuvaus ihmisen suorittamien valvontatoimenpiteiden toteuttamisesta
- ▶ niiden luonnollisten henkilöiden ja ryhmien luokat, joihin järjestelmän käyttö todennäköisesti vaikuttaa
- ▶ erityiset sellaisen haitan riskit, joka todennäköisesti kohdistuu henkilön perusoikeuksiin, mukaan lukien syrjimättömyyteen, ottaen huomioon tarjoajan antamat tiedot
- ▶ toimenpiteet, jotka on toteutettava kyseisten riskien toteutuessa, mukaan lukien sisäistä hallintoa ja valitusmekanismeja koskevat järjestelyt.

Jos käyttöönottajalla olisi pitänyt tehdä FRIA-arviointi mutta sitä ei ole tehty tai se ei sisällä asianmukaisia tietoja, katso [vaihe 4](#).

DPIA

DPIA-arvioinnissa⁵² on huomioitava kaikki luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat riskit, jotka johtuvat henkilötietojen käsittelystä, eikä pelkästään tietosuojaan liittyviä riskejä. Tämä sisältää myös syrjintäriskit (29 artiklan mukainen tietosuojatyöryhmä, 2017a). Yhdenvertaisuuselimen voi olla tarpeen tehdä yhteistyötä tietosuojaviranomaisten kanssa.

Pohdittavia kysymyksiä

Tarjoajan ja käyttöönottajien tekemien erilaisten riskinarviointien tietoja tulisi vertailla keskenään, ja niiden mahdolliset eroavaisuudet on huomioitava.

- ▶ Onko tarjoaja tai käyttöönottaja tunnistanut asiaankuuluvia perusoikeusriskejä, joita toinen ei ole havainnut?

52. Euroopan tietosuojaneuvosto järjesti toukokuussa 2026 kuulemisen DPIA-mallista, joka on saatavilla osoitteessa https://www.edpb.europa.eu/public-consultations/template-for-data-protection-impact-assessment_en.

- Jos yksi osapuoli on tehnyt useamman kuin yhden riskinarvioinnin tai useamman kuin yhden tyyppisen riskinarvioinnin, ovatko tunnistetut riskit johdonmukaisia näissä arvioinneissa? Puuttuuko yhdessä arvioinnissa tunnistettuja riskejä toisesta (ellei sille ole hyvää selitystä; jos riski esimerkiksi liittyy vain lapsiin ja sitä käsitellään nimenomaisesti lapsiin kohdistuvien riskien arvioinnissa)?

Kaikki algoritmijärjestelmät, mukaan lukien suuririskiset tekoälyjärjestelmät:

- Onko tarjoaja tai käyttöönottaja tunnistanut syrjintää (tai muuta perusoikeuksiin kohdistuvaa riskiä)?
- Onko tarjoaja ottanut käyttöön riskinhallintaprosessin?
- Miten riskinhallintamenettelyjä ja vaikutustenarviointeja käytettiin datan tai järjestelmän vinoumien tai eriarvoisuuden määrittämiseen? Miten vinouma on määritelty tai rajattu?
- Onko lieventämättömiä riskejä olemassa? Teknisessä dokumentaatiossa mainittuja riskejä voidaan mahdollisuuksien mukaan verrata riskinhallintajärjestelmään.

Huomio: jos syrjintää on tunnistettu ja sen edellyttämiä hallintatoimenpiteitä on toteutettu, tarvitaan lisätutkimuksia (katso vaihe 3.6, [Testaus ja arviointi](#)). Jos järjestelmä on suuririskinen ja yhdenvertaisuuselin on 77 artiklan mukainen viranomainen, yhdenvertaisuuselin voi pyytää pääsyä 9 artiklan mukaiseen riskinarviointidokumentaatioon.

Tapauksissa, joihin liittyy suuririskinen tekoälyjärjestelmä:

- Onko riskinhallintaprosessi 9 artiklan vaatimusten mukainen?

Tapauksissa, joihin liittyy suuririskinen tekoälyjärjestelmä ja käyttöönottajalta edellytetään FRIA-arviointia:

- Onko FRIA tehty oikein? Sen ei tulisi olla vain ruutujen rastittamista.
- Onko käyttöönottaja ottanut riskinarviointia tehdessään mukaan asiaankuuluvia sidosryhmiä? (Johdanto-osan kappaleessa 96 kuvataan tämä mahdollisuus).
- Olisiko tullut kuulla sidosryhmiä, kuten henkilöitä, joihin järjestelmä todennäköisesti vaikuttaa? (Katso jäljempää Bridgesin tapaus).
- Jos kuulemisprosessi on järjestetty, harkitse yhteydenottoa kuultuihin henkilöihin, mutta muista, että heillä saattaa olla salassapitovelvollisuus tai salassapitosopimus.
- Tarkista, että kaikki teknisessä dokumentaatiossa (11 artikla) tunnistetut syrjintäriskit on mainittu riskinhallintajärjestelmän dokumentaatiossa (9 artikla). Jos näin ei ole, voi syntyä syrjintäoletta.

Mahdollisia tiedonlähteitä riskeistä ja riskinarvioinneista

Kanteliija

Yleinen tietosuoja-asetus, 13–15 artikla, rekisteröidylle toimitettavat tiedot

- ▶ Automaattisen päätöksenteon ja/tai profiloinnin olemassaolo (yleinen tietosuoja-asetus, 13–15, 21 ja 22 artikla).
- ▶ Käytetyn automaattisen päätöksenteon logiikka (yleinen tietosuoja-asetus, 13 artiklan 2 kohdan f alakohta, 14 artiklan 2 kohdan g alakohta ja 15 artiklan 1 kohdan h alakohta).

Julkisesti saatavilla olevat tiedot

- ▶ EU:n tietokanta suuririskisistä tekoälyjärjestelmistä: C-osion käyttöönottaja: yhteenveto DPIA- ja FRIA-arvioinneista (ellei kyseessä ole lainvalvonta tai muuttoliikkeen hallinta).

Vastaaja

Tarjoajalta:

EU:n tekoälyasetus, 9 artikla, riskinhallintajärjestelmä

- ▶ Tarjoajien on otettava käyttöön riskinhallintajärjestelmä suuririskisille tekoälyjärjestelmille. Sen tulee olla jatkuva iteratiivinen prosessi, joka sisältää seuraavat:
 - riskien tunnistaminen: niiden tunnettujen ja kohtuudella ennakoitavissa olevien riskien tunnistaminen ja analysointi, joita järjestelmä voi aiheuttaa perusoikeuksille (9 artiklan 2 kohdan a alakohta)
 - riskinhallinta: asianmukaisten ja kohdennettujen riskinhallintatoimenpiteiden hyväksyminen (9 artiklan 2 kohdan d alakohta), mukaan lukien tiedon ja koulutuksen tarjoaminen käyttöönottajille riskien poistamiseksi tai vähentämiseksi (9 artiklan 5 kohdan c alakohta ja 13 artikla)
 - testaus: järjestelmä on testattava tarkoituksenmukaisimpien ja kohdennetuimpien riskinhallintatoimenpiteiden määrittämiseksi (9 artiklan 6 kohta)
 - erityiset henkilöryhmät: riskinhallintajärjestelmää täytäntöön pantaessa on kiinnitettävä huomiota siihen, onko suuririskisellä tekoälyjärjestelmällä todennäköisesti sen käyttötarkoitus huomioon ottaen haitallinen vaikutus alle 18-vuotiaisiin henkilöihin ja tarvittaessa muihin haavoittuvassa asemassa oleviin ryhmiin (9 artiklan 9 kohta).

Riskinhallintaa edellytetään kuitenkin vain riskeille, ”joita voidaan kohtuudella lieventää ja poistaa suuririskisen tekoälyjärjestelmän kehittämisen tai suunnittelun avulla tai asianmukaisten teknisten tietojen antamisella”.

EU:n tekoälyasetus, 10 artikla, data ja datanhallinta (katso vaiheesta 3.6 [koulutus-, testaus- ja validointidata](#))

EU:n tekoälyasetus, 11 artikla ja liite IV, tekninen dokumentaatio

- ▶ Liitteessä IV olevan 2 kohdan g alakohdan mukaan teknisen dokumentaation on sisällettävä tiedot mahdollisista syrjivistä vaikutuksista.

- Liitteen IV 3 kohta: yksityiskohtaiset tiedot tekoälyjärjestelmän seurannasta, toiminnasta ja valvonnasta, erityisesti seuraavien seikkojen osalta: sen suorituskyykyyn liittyvät valmiudet ja rajoitukset, mukaan lukien tarkkuusaste niiden henkilöiden tai henkilöryhmien osalta, joihin järjestelmää on tarkoitus käyttää, sekä odotettu yleinen tarkkuus suhteessa käyttötarkoitukseen; ennakoitavissa olevat tahattomat seuraukset ja riskin lähteet terveyden ja turvallisuuden, perusoikeuksien sekä syrjinnän suhteen ottaen huomioon tekoälyjärjestelmän käyttötarkoitus; tämän asetuksen 14 artiklan mukaisesti tarvittavat ihmisen suoritamat valvontatoimenpiteet, mukaan lukien tekniset toimenpiteet, jotka on otettu käyttöön, jotta käyttöönottajien olisi helpompi tulkita tekoälyjärjestelmien tuloksia; tarvittaessa syöttödataa koskevat spesifikaatiot.

Käyttöönottajalta:

EU:n tekoälyasetus, 13 artikla, avoimuus ja tietojen antaminen käyttöönottajille

- Tarjoajan käyttöönottajalle toimittamat käyttöohjeet (13 artiklan 3 kohta):
 - tunnetut tai ennakoitavissa olevat olosuhteet, jotka liittyvät järjestelmän käyttöön sen käyttötarkoituksen mukaisesti tai kohtuudella ennakoitavissa olevissa väärinkäytön olosuhteissa ja jotka voivat aiheuttaa perusoikeuksiin kohdistuvia riskejä
 - tarvittaessa järjestelmän käyttäytyminen niiden henkilöiden tai henkilöryhmien osalta, joihin järjestelmää on tarkoitus käyttää
 - tarvittaessa syöttötietoja koskevat spesifikaatiot tai muut käytettyjä koulutus-, validointi- ja testausdatajoukkoja koskevat olennaiset tiedot ottaen huomioon suuririskisen tekoälyjärjestelmän käyttötarkoitus.

EU:n tekoälyasetus, 26 artiklan 9 kohta, tietosuoja koskeva vaikutustenarviointi: tehdään tarjoajan antamien tietojen perusteella / yleinen tietosuoja-asetus, 35 artikla, tietosuoja koskeva vaikutustenarviointi (DPIA)

EU:n tekoälyasetus, 27 artiklan 1 kohdan d alakohta, perusoikeusvaikutusten arviointi

- Erityiset sellaisen haitan riskit, joka todennäköisesti kohdistuu henkilön perusoikeuksiin, mukaan lukien syrjimättömyyteen, ottaen huomioon tarjoajan antamat tiedot.

Muut

- Arviointi, joka tehdään Euroopan neuvoston tekoälyjärjestelmistä aiheutuvia ihmisoikeuksiin, demokratiaan ja oikeusvaltioperiaatteeseen kohdistuvia riskejä ja vaikutuksia käsittelevällä menetelmällä (HUDERIA-menetelmä).
 - Jotkut organisaatiot voivat tehdä ja julkaista HRIA-, FRIA- tai DPIA-arvioinnin tai lasten oikeuksia koskevan vaikutustenarvioinnin vapaaehtoisesti. Myös "eettinen" arviointi voi olla olemassa.
 - Muut vastaajan jakamat (riskin)arvioinnit.
 - Tiedonvälityksen vapautta koskevat pyynnöt, jos saatavilla.
-

Keskeinen tapaus: *R (Bridges) v. Chief Constable of South Wales Police, 2020*

(Hakasulkeissa olevat numerot viittaavat tuomion kohtiin.)

Bridgesin tapaus oli Yhdistyneen kuningaskunnan muutoksenhakutuomioistuimen ratkaisema asia, jossa tarkasteltiin, oliko viranomainen loukannut ihmisoikeuksia tai laiminlyönyt velvollisuutensa arvioida yhdenvertaisuusvaikutuksia Yhdistyneen kuningaskunnan yhdenvertaisuuslainsäädännön (Equality Act 2010) nojalla ennen reaaliaikaisen kasvontunnistuksen käyttöönottoa. Julkisen sektorin yhdenvertaisuusvelvoite edellyttää, että viranomainen ottaa asianmukaisesti huomioon tarpeen poistaa syrjintää, häirintää, uhriksi joutumista ja vastaavia toimia, edistää yhtäläisiä mahdollisuuksia ja vaalia hyviä suhteita henkilöiden välillä riippumatta siitä, onko henkilöillä tietty ominaisuus vai ei.

Tuomioistuin totesi seuraavaa:

- ▶ Velvoite on täytettävä ennen käytännön (kasvontunnistuksen käytön) harkintaa ja sen aikana.
- ▶ Velvoitetta on noudatettava asiallisesti, tarkasti ja ennakkoluulottomasti – sen ei tule olla vain ruutujen rastittamista.
- ▶ Velvoitetta ei voida siirtää muille, mikä voi aiheuttaa vaikeuksia käyttöönottajina toimiville viranomaisille, jotka ovat riippuvaisia kolmannen osapuolen tarjoajista, erityisesti jos järjestelmän suorituskyvystä ei ole annettu riittävästi tietoa tai viranomaisella ei ollut riittävästi asiantuntemusta tai kokemusta tiedon tai järjestelmän ymmärtämiseksi [199].

Lisäksi, jos arvioinnin kannalta olennaista materiaalia ei ole saatavilla, on velvoite hankkia tällaista materiaalia – tämä voi edellyttää lisäkonsultaatioita asiaankuuluvien ryhmien kanssa. Lopuksi, jos velvoitetta on käsitelty perusteellisesti niin, että päätöksen mahdollinen vaikutus yhdenvertaisuustavoitteisiin ja niiden edistämiseen on arvioitu asianmukaisesti, päätöksentekijän on päätettävä, kuinka paljon painoarvoa päätöstä ohjaaville tekijöille annetaan.

Kaiken kaikkiaan tuomioistuin totesi, että velvoitteen vaatimusten noudattaminen edellyttää kohtuullisten toimenpiteiden toteuttamista, jotta voidaan kartoittaa tietoja, joita viranomainen ei välttämättä vielä tiedä, ehdotetun päätöksen tai käytännön mahdollisesta vaikutuksesta henkilöihin, joilla on tapauksen kannalta merkityksellisiä ominaisuuksia. Tässä tapauksessa tämä tarkoitti erityisesti rotua ja sukupuolta [181].

Todettiin, ettei pelkkä ihmisen osallistuminen prosessiin todennäköisesti täyttäisi lakisääteistä velvoitetta, koska velvoite koskee nimenomaan prosessia kokonaisuutena, ei vain päätöksen sisältöä.

Lisäksi tuomioistuin totesi, että ihmiset tekevät virheitä [185].

Vastaavia havaintoja voidaan todennäköisesti soveltaa tekoälyasetuksen mukaisiin riskinarvioiteihin.

Syrjinnän indikaattorit

Syrjintäriskiä, joka on tunnistettu mutta jota ei ole lievennetty, valvottu tai perusteltu, on pidettävä vahvana indikaattorina.

- ▶ Suora viittaus syrjintään, vinoumaan tai epäoikeudenmukaisuuteen FRIA-arvioinnissa.
 - ▶ Suora viittaus syrjintään, vinoumaan tai epäoikeudenmukaisuuteen DPIA-arvioinnissa.
 - ▶ Tilanteet, joissa vinouma mainitaan riskinä mutta vinouman merkitystä ja tyyppiä ei ole määritelty tai ne on määritelty virheellisesti dokumentaatioissa.
 - ▶ Tilanteet, joissa tunnistetuille syrjinnän, vinoumien tai epäoikeudenmukaisuuden riskeille ei ole käytössä riskinhallintamenettelyjä tai menettelyt ovat puutteellisia.
 - ▶ Dokumentaatioissa on selvästi mainittu syrjintäriski, jota ei ole lievennetty.
 - ▶ Riittämätön testaus.
 - ▶ Suora viittaus perusoikeuksien loukkaamisen riskiin joko FRIA- tai DPIA-arvioinnissa:
 - jos on olemassa minkäänlainen perusoikeuksien loukkaamisen riski, tarvitaan lisätutkimuksia järjestelmän syrjimättömyyden varmistamiseksi.
 - ▶ Jos FRIA tai DPIA on puutteellinen, pintapuolinen tai epätarkka, tarvitaan lisätutkimuksia.
 - ▶ Asiaankuuluvien sidosryhmien kuulematta jättäminen riskien tunnistamiseksi silloin, kun sidosryhmät olisi selvästi pitänyt huomioida (FRIA-arviointia koskevat huolellisuusvelvoitteet eivät esimerkiksi välttämättä täyty, jos vammaisia henkilöitä koskevien päätösten tekemiseen on suunniteltu järjestelmä ilman, että vammaisia henkilöitä tai heitä edustavia järjestöjä on kuultu ennen käyttöönottoa).
- ▶ Kirjaa tietoihin kaikki tarjoajan tai käyttöönottajän tunnistamat syrjintäriskit ja riskin lieventämiseksi tehdyt toimenpiteet.
 - ▶ Pohdi ja kirjaa tietoihin, havaitaanko riskinarvioinnissa tai DPIA- tai FRIA-arvioinnissa selkeitä puutteita.

3.4. Mitä algoritmijärjestelmän on tarkoitus tehdä ja miten se tekee sen?

Jotta yhdenvertaisuuselimet voivat arvioida, onko algoritmista syrjintää tapahtunut, niiden on ymmärrettävä itse järjestelmää ainakin yleisellä tasolla. Järjestelmän tarkoituksen, rakenteen ja toiminnan ymmärtäminen auttaa arvioimaan seuraavia seikkoja.

- ▶ Mikä järjestelmän tarkoitus on?
 - Liittyykö tarkoitus alueeseen, jolla on historiallisesti esiintynyt syrjintää kiellettyjen syrjintäperusteiden perusteella?

- Soveltuuko käytetty data tarkoitukseen (katso [vaihe 3.5](#))?
- Miten syötteet vaikuttavat tuotoksiin?
 - Vaikuttaako vaiheessa 3.2 tunnistettu syöte tuotokseen ja johtaako se mahdolliseen erilaiseen kohteluun?
- Vaikuttaako algoritmijärjestelmä päätöksentekoprosessiin kokonaisuudessaan vai lopulliseen, kohderyhmään kohdistuvaan vaikutukseen:
 - Miten merkittävä rooli järjestelmällä on? Onko järjestelmä esimerkiksi ainoa päätöksentekijä vai avustaako se päätöksentekijöitä?
 - Onko algoritmijärjestelmä kokonainen järjestelmä vai osa suurempaa järjestelmää, johon voi liittyä muita algoritmijärjestelmiä?

Käyttötarkoitusta ja suunnittelua koskevissa tiedoissa on yleisesti ottaen tarkasteltava, vaikuttavatko suunnitteluvalinnat sopivilta järjestelmän käyttötarkoitukseen ja todelliseen käyttöön. Tässä vaiheessa sekä teknisestä että sektorikohtaisesta asiantuntemuksesta on hyötyä.

Yhdenvertaisuuselinten käytettävissä olevien tietojen tulisi viime kädessä auttaa yhdenvertaisuuselimiä ymmärtämään, mitä tekoälyjärjestelmä tekee ja miten se toimii, antamalla merkityksellistä tietoa käytetystä logiikasta, käsittelyn merkityksestä ja odotetuista seurauksista yksilölle sekä siitä, miksi suunnitteluun ja dataan liittyvät valinnat on tehty. Kun algoritmijärjestelmän ymmärretään olevan ehdot täyttävä ADM tai merkitykselliseen päätöksentekoon käytettävä suuririskinen tekoälyjärjestelmä, tällaisten tietojen saatavuus on välttämätöntä. Jos järjestelmän toiminnan ymmärtäminen ei kuitenkaan ole mahdollista dokumentaation perusteella, tapaukseen voi liittyä avoimuuden puutetta koskevia ongelmia (katso jäljempää vaiheesta 3.7. kohta Avoimuus).

Järjestelmän suunnittelu voi myös olla erityisen merkityksellistä myöhemmin, kun tarkastellaan tapoja, joilla vastaaja voi pyrkiä kumoamaan syrjintäolettan tai perustelemaan tehtyjä päätöksiä.

Pohdittavia kysymyksiä

Tarkoitus ja käyttö

- Miten algoritmijärjestelmää on tarkoitus käyttää?
 - Mikä käyttötarkoitus on?
 - Miten järjestelmää käytetään käytännössä?
 - Tapauksissa, joissa järjestelmän tarjoaa toimittaja: käyttääkö käyttöönottaja järjestelmää toimittajan tarkoittamalla tavalla?
- Kenelle järjestelmä on suunniteltu?
 - Mitä suunnitteluvalintoja (katso alta tekstiruutu) tehtiin niiden henkilöiden tai henkilöryhmien osalta, joihin järjestelmän käytön on tarkoitus kohdistua?
- Onko tehty oletuksia henkilöistä tai henkilöryhmistä, joihin järjestelmän käytön on tarkoitus kohdistua? Järjestelmän voidaan esimerkiksi odottaa olevan vain aikuisten käytössä, tai järjestelmän voidaan olettaa olevan käytössä tietyllä

sektorilla tai kohdistuvan tiettyyn populaatioon. Ovatko nämä oletukset järkeviä ja perusteltuja?

- ▶ Miten järjestelmä vaikuttaa ihmisten kohteluun?
- ▶ Tapauksissa, joissa ihminen on vastuussa henkilöiden kohteluun vaikuttavien valintojen tekemisestä (ihminen mukana prosessissa):
 - Onko päätöksentekijöille annettu ohjeita tai käytäntöjä, jotka auttavat heitä ymmärtämään, miten tekoälyjärjestelmää käytetään tai miten tuotoksia tulkitaan?
 - Onko asiaankuuluvalla henkilöllä tarvittava pätevyys, koulutus ja valtuudet kumota tekoälyjärjestelmän tekemä päätös?
 - Onko asiaankuuluva henkilö koulutettu ymmärtämään ja tulkitsemaan järjestelmän tuotoksia ja tunnistamaan, missä voi esiintyä vinoumia ja missä tarvitaan ihmisen väliintuloa?

Huomautus: pelkkä ihmisen osallistuminen prosessiin ei tarkoita, etteikö järjestelmä vaikuttaisi henkilöiden kohteluun, koska järjestelmän tuotokset vaikuttavat prosessissa mukana olevaan ihmiseen enemmän tai vähemmän.

Järjestelmän toimintaperiaate

- ▶ Mihin nähden järjestelmä on suunniteltu optimoitumaan?
 - Oliko se suunniteltu optimoitumaan johonkin muuhun (hieman erilaiseen) tarkoitukseen kuin sen käyttötarkoitukseen? Oliko se esimerkiksi optimoitu virheiden ennustamiseen, mutta nyt sitä käytetään petosten ennakointiin?
- ▶ Käyttääkö järjestelmä ryhmän ominaisuuksia tuottaakseen yksilöä koskevia tuotoksia (profilointi)?
- ▶ Miten järjestelmä käsittelee poikkeamat?
 - Miten järjestelmä käsittelee poikkeamat odotetusta käyttäytymisestä (esimerkiksi virheet tai epätavallinen toiminta)?
 - Kohdellaanko kaikkia poikkeamia samalla tavalla riippumatta niiden taustalla olevista syistä?
- ▶ Suunniteltiinko järjestelmä oikeudenmukaiseksi ja yhdenvertaiseksi?
 - Huomioitiinko suunnittelussa oikeudenmukaisuus tai syrjimättömyys?
 - Onko kontekstisidonnainen oikeudenmukaisuuden käsite määritelty tarkasti?
 - Mitä toimenpiteitä tehtiin oikeudenmukaisuuden ja yhdenvertaisuuden edistämiseksi suunnittelussa?

Tuotosten vaikutus

- ▶ Miten (ennalta koulutetun) mallin tai algoritmin valinta tehtiin?
 - Onko tämä menettely dokumentoitu ja järjestelmän käyttöönottajien saatavilla?
- ▶ Mitkä kriteerit vaikuttavat järjestelmän tuotoksiin?

- Käsitelläänkö tai käytetäänkö datassa olevia kiellettyjä syrjintäperusteita ja/tai sijaismuuttujia automaattisen päätöksenteon tai profiloinnin perustana (kuten profiilin luomiseen tarvittavina syötteinä tai profiilissa olevissa tiedoissa)?
- Onko saatavilla mittareita tietyn syötteen painokertoimista / vaikutuksesta tuotokseen?
- ▶ Mille kriteereille annetaan eniten painoarvoa järjestelmässä tai päätöksessä?
 - Voiko vastaaja väittää, että kielletyillä syrjintäperusteilla ja/tai sijaismuuttujilla on merkityksellinen vaikutus tuotokseen?
- ▶ Mikä on useiden sijaismuuttujien, kuten postinumeron ja koulutuksen kaltaisten tekijöiden, kumulatiivinen vaikutus yhdessä?
- ▶ Ovatko käytetyt tai eniten painoarvoa saaneet tiedot mielivaltaisia tai epäolennaisia käyttötarkoitukseen nähden?

Mahdollisia tiedonlähteitä järjestelmän tarkoituksen, suunnittelun ja toiminnan ymmärtämiseen

Kanteliija

Yleinen tietosuoja-asetus, 13–15 artikla, rekisteröidylle toimitettavat tiedot

- ▶ Automaattisen päätöksenteon ja/tai profiloinnin olemassaolo (yleinen tietosuoja-asetus, 13–15, 21 ja 22 artikla).
- ▶ Käytetyn automaattisen päätöksenteon logiikka (yleinen tietosuoja-asetus, 13 artiklan 2 kohdan f alakohta, 14 artiklan 2 kohdan g alakohta ja 15 artiklan 1 kohdan h alakohta).

Yleinen tietosuoja-asetus, 15 artiklan 3 kohta: DSAR

- ▶ DSAR-pyyntöön vastauksena annettavien tietojen laajuus, luonne ja yksityiskohtaisuuden taso voivat vaihdella. Jos kyseessä on ehdot täyttävä ADM, tietoihin on sisällytettävä seuraavat, mutta nämä tiedot (tai osa niistä) voidaan antaa myös muiden algoritmijärjestelmien tapauksissa:
 - Päätöksenteossa käytetyt syöttömuuttujat tai parametrit ja niiden muodostus (esimerkiksi tilastotietojen avulla) sekä niiden merkitys kokonaispisteytyksessä (julkisasiamies P. Pikamäen ratkaisuehdotus, asia SCHUFA Holding, 2023, 58 kohta).
 - Syöttömuuttujan vaikutus pisteytykseen, selitys siitä, miksi rekisteröidylle annettiin tietty pisteytys, luettelo mahdollisista profiililuokista ja vaihtoehtoisista skenaarioista.
 - Käytetty laskentaperiaate: yksityiskohtaiset selitykset pistemäärän laskentamenetelmästä, rekisteröidyn kohdistaminen arviointitulokseen ja profiililuokkien luettelo (Barros Vale ja Zanfir-Fortuna, 2022).
 - Automaattisen päätöksenteon ja/tai profiloinnin käyttö ja merkityksellisiä tietoja siihen liittyvästä logiikasta sekä tällaisen käsittelyn merkityksestä ja suunnitelluista seurauksista rekisteröidylle (15 artiklan 1 kohdan h alakohta).

EU:n tekoälyasetus, 86 artikla: oikeus selitykseen

- ▶ Tekoälyjärjestelmän rooli päätöksentekoprosessissa. Esimerkkejä: "Tekoälyjärjestelmää [tekoälyjärjestelmän nimi/kuvaus] käytettiin [tekoälyjärjestelmän tarkan toiminnon, esimerkiksi datan analysoinnin, kriteerien arvioinnin tai tunteiden tunnistamiseen tarkoitetun puheanalyysin, kuvaus]. Tekoälyjärjestelmä edisti päätöksentekoprosessia [esimerkiksi analysoimalla tietoja ja arvioimalla asiaankuuluvia parametreja]".
- ▶ Käsittelyn logiikka: "Järjestelmä analysoi syöttötiedot käyttämällä [algoritmien tai mallien, kuten päätöspuiden, kuvaus] suorittaakseen [tavoitteen, kuten riskinarvioinnin, kuvaus]".
- ▶ Tuotos: "Tämän analyysin perusteella tekoälyjärjestelmä tuotti seuraavan tuotoksen, joka sisällytettiin lopulliseen päätökseen: [tuotoksen, kuten pisteytyksen tai luokituksen, kuvaus]".
- ▶ Päätöksen vaikutus asianomaiseen henkilöön: "Päätöksellä on seuraavat mahdolliset vaikutukset sinuun: [vaikutus luottokelpoisuuteen, tiettyjen palveluiden saatavuuteen, talouteen jne.]. Nämä vaikutukset ovat merkityksellisiä, koska ne voivat vaikuttaa merkittävästi mahdollisuuteesi [seurausten, kuten ohjelmiin osallistumisen tai rahoitustarjousten saamisen, selitys]".
- ▶ Kriteerien painotus: "Keskeisimmät päätökseen vaikuttavat kriteerit painotettiin seuraavasti: [lyhyt selitys kunkin kriteerin tärkeydestä]".

Vastaaja

Tarjoajalta

EU:n tekoälyasetus, suuririskisiä tekoälyjärjestelmiä koskevan liitteen VIII A jakson 5 ja 6 kohta

- ▶ Kuvaus tekoälyjärjestelmän käyttötarkoituksesta, yleisluontoinen ja lyhyt kuvaus järjestelmän käyttämisestä tiedoista (data ja syöttötiedot) ja sen toimintalogiikasta.
- ▶ Jos kyseessä on lainvalvonta / muuttoliikkeen hallinta, tietokannassa voi olla asiaankuuluvan markkinavalvontaviranomaisen käytettävissä olevia lisätietoja.

EU:n tekoälyasetus, 11 artikla ja liite IV, tekninen dokumentaatio

- ▶ 1 kohdan a alakohdan mukainen käyttötarkoitus.
- ▶ 1 kohdan d alakohdan mukainen kuvaus kaikista muodoista, joissa tekoälyjärjestelmä saatetaan markkinoille tai otetaan käyttöön (kuten laitteistoon sisällytetyt ohjelmistopakettit, ladattavat versiot tai sovellusrajapinnat (API)).
- ▶ 1 kohdan h alakohdan mukainen käyttöönottajalle tarjottu käyttöliittymän peruskuvaus.
- ▶ 2 kohdan b alakohdan mukaiset järjestelmän rakennespesifikaatiot ja yleinen logiikka. Katso edeltä kohta [3.2 Sisältyykö syötteisiin tai datajoukkoihin tunnettuja syrjintäperusteita tai sijaismuuttujia?](#)

Käyttöönottajalta

13 artikla, avoimuus ja tietojen antaminen käyttöönottajille

- ▶ Tarjoajan on annettava (13 artiklan 2 kohdan mukaiset) käyttöohjeet käyttöönottajalle.
- ▶ 13 artiklan 3 kohdan b alakohdan iv luetelmakohdan mukaisesti tarvittaessa suuririskisen tekoälyjärjestelmän tekniset valmiudet ja ominaisuudet, jotta voidaan antaa tietoja, jotka ovat merkityksellisiä sen tuotoksen selittämiseksi, ja 3 kohdan b alakohdan v luetelmakohdan mukaisesti järjestelmän käyttäytyminen niiden henkilöiden tai henkilöryhmien osalta, joihin järjestelmää on tarkoitus käyttää.
- ▶ 13 artiklan 3 kohdan c alakohdan mukaisesti suuririskisen tekoälyjärjestelmän ja sen suorituskyvyn muutokset, jotka tarjoaja on määritellyt ennalta ensimmäisen vaatimustenmukaisuuden arvioinnin yhteydessä, jos sellaisia on.

Muut

- ▶ Asiakirjatutkimus
- ▶ Sopimuslausekkeet
- ▶ Alustan usein kysytyt kysymykset
- ▶ Yhtiön julkinen viestintä

Syrjinnän indikaattorit

Vahvat indikaattorit

Nämä indikaattorit *yhdessä* voivat tukea *prima facie* -tapausta.

- ▶ Epäilyillä kriteereillä (kuten [vaiheessa 3.2](#) on tunnistettu) on merkittävä vaikutus järjestelmän tuotokseen.
 - Kun kielletyllä syrjintäperusteella tai siihen erottamattomasti liittyvällä sijaismuuttujalla on merkittävä vaikutus järjestelmän tuotokseen, tämä on selvä osoitus välittömästä syrjinnästä.
 - Kun (epäilyillä) sijaismuuttujalla on merkittävä vaikutus järjestelmän tuotokseen, se on osoitus välillisestä syrjinnästä.
- ▶ Järjestelmän tuotos (ainakin osittain) määrittää yksilöiden kohtelun.

Muut indikaattorit

- ▶ Käyttötarkoituksen, oletusten ja/tai suunnitteluvaihtoehtojen epäilyllään heijastavan tai vahvistavan historiallisen eriarvoisuuden, mikä johtaa eriarvoiseen kohteluun.
- ▶ Suunnitteluvaihtoehdot suosivat yhtä ihmisryhmää toisen kustannuksella.
- ▶ Järjestelmä on optimoitu historiallisesti etuoikeutetussa asemassa oleville ryhmille.
- ▶ Järjestelmää ei käytetä siihen tarkoitukseen, johon se on kehitetty/tarjottu.

- ▶ Kirjaa tietoihin järjestelmän tarkoitus ja optimointi.
- ▶ Kirjaa tietoihin sijaismuuttujat ja kielletyt syrjintäperusteet, jotka vaikuttavat järjestelmän tuotoksiin ja mittarit niiden painokertoimista / vaikutuksesta tuotokseen, jos ne ovat saatavilla

3.5. Koulutus-, testaus- ja validointidata

Dataa käytetään algoritmijärjestelmien kehittämiseen ja testaamiseen. Jopa manuaalisesti suunnitellut sääntöpohjaiset algoritmijärjestelmät validoidaan dataa käyttäen. Data edustaa todellisuutta aina epätäydellisesti. Vinoumat ja olemassa olevat eriarvoisuudet heijastuvat datassa. Datan vinoumien ja eriarvoisuuksien arviointi voi auttaa osoittamaan, että tuloksena oleva järjestelmä johtaa syrjiviin tuloksiin. On huomattava, että datan vinoumien ymmärtäminen ei itsessään osoita eriarvoista kohtelua. Yhdessä muiden täydentävien analyysilähteiden kanssa se kuitenkin edistää *prima facie* -tapauksen osoittamista, ja sitä voidaan käyttää lisätestauspyyntöjen perustelemiseen.

Kun tilastollisia yhdenvertaisuustietoja on saatavilla, tämä osio on lisäksi merkityksellinen näiden tilastojen laskennassa käytettyjen tietojen validiteetin ja luotettavuuden arvioinnissa. Tällaisissa tapauksissa tämä osio on luettava yhdessä [kohdan 3.6](#) kanssa.

Datasta tulee yleisesti ottaen selvittää, mitä tietoa vastaaja on antanut järjestelmän kouluttamisesta ja testaamisesta. Tästä voidaan pystyä tunnistamaan keskeisiä syrjintäongelmia esimerkiksi tapauksissa, joissa datajoukkoon ei ole sisällytetty naisia tai koulutustiedot on saatu kaupungista, mutta järjestelmää käytetään maaseudulla.

Muissa tapauksissa saatetaan tarvita teknistä ja sektorikohtaista asiantuntemusta sen selvittämiseksi, onko järjestelmä koulutettu ja testattu edustavilla, asiaankuuluvilla, tarkoilla ja asianmukaisesti mitatuilla ja yleistettävillä datajoukoilla.

Huomioitavia keskeisiä seikkoja ovat esimerkiksi erilaiset vinoumat. Nämä vinoumat eivät ole toisistaan riippumattomia, vaan yksi vinouma vaikuttaa toiseen.

- ▶ Onko todennäköistä, että data sisältää historiallisia vinoumia? Kaikilla kohdealueilla, joilla esiintyy historiallista tai olemassa olevaa eriarvoisuutta, tämä eriarvoisuus heijastuu datassa, ellei sitä korjata erittäin huolellisesti. Esimerkkejä tästä ovat tummaihoisten henkilöiden yhteisöihin aiemmin kohdistunut liiallinen poliisitoiminta ja lapsista ja muista hoitovelvollisuuksista johtuvat työttömyysjaksot, jotka voivat vaikuttaa sukupuolten tasa-arvoon.
- ▶ Sisältääkö data edustavuusvinoumia? Vastaako kohderyhmä esimerkiksi todellista käyttöryhmää? Esimerkiksi Lissabonia edustava data ei välttämättä edusta Portoa. Helsinkiä 30 vuotta sitten edustanut data ei välttämättä vastaa nykyistä väestöä. Lisäongelmia voi aiheuttaa se, keitä datassa on edustettuina ja missä määrin. Esimerkiksi terveystiedoissa naiset voivat olla aliedustettuina ja/tai raskaana olevat naiset voivat olla yliedustettuina. Mikä tahansa näistä voi vääristää tietoja ja vaikuttaa tuloksiin. Lisäksi on kiinnitettävä huomiota siihen, miten vähemmistöt ovat edustettuina datassa. Jos esimerkiksi tiettyjä aksentteja ei ole sisällytetty puheentunnistusjärjestelmään, järjestelmä toimii näiden aksenttien tapauksissa heikommin. Jos hijabia käyttäviä henkilöitä ei ole sisällytetty kasvotunnistusdataan, on mahdollista, ettei hijabia käyttäviä henkilöitä tunnisteta asianmukaisesti.
- ▶ Sisältääkö data valintaharhoja? Näin voi käydä silloin, kun tietoja on vain tietystä datan alaryhmästä. Esimerkki tästä on lainojen hyväksymisjärjestelmä, joka sisältää tietoja vain aiemmin lainan saaneiden henkilöiden ryhmän luottotappioista. Poliisin partiointitiedot sisältävät dataa vain alueista, joilla poliisi on partioinut.

Petostiedot saattavat sisältää vain ryhmän, joiden mahdollisia petoksia on aiemmin tutkittu. Rekrytointitiedoissa on vähemmän dataa hakijoista, joiden ansioluetteloita ei koskaan valittu työnhakuprosessin jatkotoimiin. Tämä voi vääristää dataa varsinkin tilanteissa, joissa kiellettyihin syrjintäperusteisiin kuuluvan ominaisuuden omaavat henkilöt ovat historiallisesti olleet yli- tai aliedustettuina.

- Sisältääkö data mittausharjoja? Tämä tarkoittaa tilannetta, jossa tunnisteet (mittaus) eivät vastaa käsitteitä, joita niiden on tarkoitus mitata. Jos esimerkiksi halutaan mitata sosiaalietuuksiin liittyviä petoksia mutta päätetään, että kaikki virheellisesti myönnetty etuudet ovat merkityksellisiä, tuloksena on, että mukaan sisällytetään sekä viattomat virheet että tahalliset petokset. Tällä voi puolestaan olla erilaisia vaikutuksia tiettyihin ryhmiin, kuten henkilöihin, joilla on heikko lukutaito tai alhainen koulutustaso tai jotka eivät puhu kyseisen maan kieltä äidinkielenään. Toinen mittausharhan muoto on tilanne, jossa inhimilliset vinoumat (tai inhimillinen syrjintä) vaikuttavat merkittyihin tunnisteisiin, joita sitten pidetään pohjatotuuksina. Kaikissa tilanteissa, joissa pohjatotuustunnisteet perustuvat ihmisten tekemiin, harvintavallan alaisiin arvioihin, on olemassa riski, että inhimilliset vinoumat johtavat mittausharhoihin. Esimerkkejä tästä ovat opettajien arvioinnit, rekrytointitiedot tai petostutkinnat.

Pohdittavia kysymyksiä

Tarkastele alla olevia kysymyksiä ja huomioi mahdolliset vinoumat ja eriarvoisuus. Kaikki alla olevat kysymykset ovat subjektiivisia, monitahoisia ja kontekstisidonnaisia. Näihin vastaaminen edellyttää hyvää ymmärrystä käsiteltävästä sektorista ja sen olemassa olevista eriarvoisuuksista sekä käytetyistä järjestelmistä ja teknologiasta. Tämän arvioinnin tulos antaa lähinnä suuntaa jatkoarvioinnille, tai sitä voidaan käyttää *prima facie* -tapauksen osoittamiseen.

On huomioitava, että manuaalisesti suunniteltujen algoritmijärjestelmien tapauksissa koulutusdataa ei ole. Joissakin tekoälyjärjestelmissä koulutusdata ei sisällä merkittyjä tunnisteita. Tällaisissa tapauksissa odotetaan kuitenkin olevan testausdataa, joka sisältää jonkinlaisia merkittyjä tunnisteita sen testaamiseksi, tuottaako malli asianmukaisia tai hyväksyttäviä tuotoksia.

Koulutus-, testaus- ja validointidata

- Miten koulutus-, testaus- ja validointidata valittiin?
- Mitä koulutus-/testaus-/validointidataa kerättiin?
- Mitkä tämän datan lähteet ovat?
- Mihin tarkoitukseen data alun perin kerättiin? Voiko datan käytöstä eri konteksteissa aiheutua ongelmia? Jos data esimerkiksi kerättiin terveydentilan arviointia varten, aiheuttaako sen uudelleenkäyttö vakuutustarkoituksiin mahdollisia mittausharhaan liittyviä ongelmia?
- Mitä menetelmiä datan keräämiseen käytettiin?
 - Vaikuttavatko nämä menetelmät hyväksyttäviltä siinä mielessä, että ne tuottavat kohtuullisen luotettavaa ja asianmukaista dataa algoritmijärjestelmän käyttötarkoituksen kannalta?

- Varmistettiin menetelmillä, että data oli edustavaa ja asianmukaisesti mitattua? Voidaanko kohtuudella odottaa, että data voidaan yleistää kohdealueelle ja kontekstiin, jossa algoritmijärjestelmiä nyt sovelletaan?
- Kerättiin (tai merkittiin) lisätietoja käytettäväksi koulutus-/testaus-/validointidatana? Käytettiinkö datan keräyksessä satunnaisotoksia?
- ▶ Jos datajoukko on peräisin kolmannelta osapuolelta, miten se on hankittu? Tarkistettiin kolmannen osapuolen toimittama data?
- ▶ Onko olemassa historiallisia eriarvoisuuksia, jotka todennäköisesti heijastuvat datassa (katso aiempi vinoumia käsittelevä osio)? Tässä on huomioitava myös kumulatiivinen/intersektionaalinen syrjintä.
- ▶ Ovatko vähemmistöt riittävästi edustettuina datassa? Tämä on erityisen olennaista algoritmijärjestelmille, joita käytetään aloilla, joilla kulttuuri, tausta ja fyysinen ulkonäkö voivat vaikuttaa tuotoksiin.

Tunnisteet

- ▶ Kuinka luotettavia tunnisteet ovat?
- ▶ Vastaavatko tunnisteet järjestelmien tarkoitusta? Toisin sanoen, mittaavatko tunnisteet sitä, mitä järjestelmän on tarkoitus ennustaa?
- ▶ Voidaanko oikeellisuutta arvioida objektiivisesti? Onko tämä määritetty?
- ▶ Tapauksissa, joissa tunnisteiden merkintään liittyy ihmisen harkintaa, voivatko inhimilliset vinoumat vääristää tunnisteita? Onko syitä epäillä syrjintää?

Olemassa olevat lieventävät toimenpiteet

- ▶ Miten datan laatua arvioitiin?
 - Mitä toimenpiteitä, kuten datan täydentämistä tai poistamista, tehtiin havaittujen laatuongelmien korjaamiseksi?
- ▶ Mitä toimenpiteitä tehtiin sen varmistamiseksi, että data oli edustavaa, asianmukaista, tarkasti mitattua ja yleistettävää?
- ▶ Miten datajoukossa mahdollisesti esiintyviä vinoumia ja eriarvoisuutta lievennettiin?
 - Toteutettiinkö vinoumia lieventäviä⁵³ toimenpiteitä?
 - Minkä vinoumien vuoksi nämä toimenpiteet toteutettiin? Onko olemassa tunnistettuja vinoumia, joita lieventäviä toimenpiteitä ei ole toteutettu?
 - Mitä tekniikoita käytettiin?
 - Onko käytettävissä tietoa näiden vinoumien lieventämistoimenpiteiden tehokkuudesta?

53. Vinoumien lieventämistoimenpiteet voivat olla mitä tahansa toimenpiteitä, joilla pyritään ehkäisemään datan tai järjestelmän vinoumia. Näitä voivat olla satunnaisotanta, lisädatan kerääminen edustavuuden parantamiseksi, tarkat tapausten arviointikäytännöt, kahden käsittelijän periaatteen mukainen tarkastelu tapausten arvioinnissa, datan uudelleenpainotus ja monet muut toimenpiteet.

Mahdollisia tiedonlähteitä käytetyn datan arviointiin

Kanteliija

EU:n tekoälyasetus, 86 artikla: oikeus selitykseen

Yleinen tietosuoja-asetus, 13–15 artikla, rekisteröidylle toimitettavat tiedot

Julkisesti saatavilla olevat tiedot

EU:n tietokanta suuririskisistä tekoälyjärjestelmistä

- ▶ A-osio, suuririskiset tekoälyjärjestelmät – järjestelmän käyttämät tiedot, kuten data ja syötteet.
- ▶ C-osio, käyttöönottaja – DPIA- ja FRIA-arviointien yhteenvedo (ellei niitä käytetä lainvalvonnan tai muuttoliikkeen hallinnan aloilla).

Vastaaja

Tarjoajalta:

EU:n tekoälyasetus, liitteen IV 2 kohdan d alakohta, tekninen dokumentaatio

- ▶ ”Tarvittaessa dataa koskevat vaatimukset sellaisten datalomakkeiden muodossa, joissa kuvataan koulutusmenetelmät ja -tekniikat sekä käytetyt koulutusdatajoukot, mukaan lukien yleinen kuvaus näistä datajoukoista, tiedot niiden alkuperästä, laajuudesta ja pääpiirteistä; se, kuinka data on hankittu ja valittu; merkintämenettelyt (esim. ohjattua oppimista varten), datan puhdistusmenetelmät (esim. poikkeamien havaitseminen).”

EU:n tekoälyasetus, 10 artikla, data ja datanhallinta

- ▶ Tarjoajien on otettava käyttöön asianmukaiset käytännöt siinä määrin, että datajoukot ovat ”käyttötarkoitukseen nähden merkityksellisiä, riittävän edustavia ja niin suurelta osin kuin mahdollista virheettömiä ja täydellisiä. Niillä on oltava asianmukaiset tilastolliset ominaisuudet, tarvittaessa myös niiden henkilöiden tai henkilöryhmien osalta, joihin liittyy suuririskistä tekoälyjärjestelmää on tarkoitus käyttää. Kyseiset datajoukkojen ominaisuudet voidaan saavuttaa yksittäisten datajoukkojen tai niiden yhdistelmän tasolla.”

Tämä kattaa vähintään seuraavat:

- ▶ asiaankuuluvat suunnitteluvalinnat
- ▶ datan keruuprosessit ja käyttö (10 artiklan 2 kohdan b, e ja g alakohdat)
- ▶ asiaankuuluvat tietojenkäsittelytoimet, kuten huomautusten ja tunnisteiden lisääminen (10 artiklan 2 kohdan c alakohta)
- ▶ oletusten muotoilu erityisesti niiden tietojen osalta, joita datan on tarkoitus mitata ja edustaa (10 artiklan 2 kohdan d alakohta)
- ▶ vinoumia on nimenomaisesti tarkasteltava, ja lisäksi on toteutettava ”asianmukaiset toimenpiteet... havaittujen mahdollisten vinoutumien havaitsemiseksi, ehkäisemiseksi ja lieventämiseksi” (10 artiklan 2 kohdan g alakohta) datajoukoissa, jos ne ”todennäköisesti vaikuttavat... kielteisesti perusoikeuksiin tai johtavat unionin oikeudessa kiellettyyn syrjintään” (10 artiklan 2 kohdan f alakohta).

EU:n tekoälyasetus, 17 artiklan 1 kohdan f alakohta, laadunhallinta

- Kirjallisten käytäntöjen, menettelyiden ja ohjeiden on sisällytettävä seuraavat: "datanhallintajärjestelmät ja -menettelyt, mukaan lukien datanhankinta, datankeruu, datan analysointi, tunnistamisen lisääminen, datan tallentaminen, datan suodattaminen, datanlouhinta, datan yhdistäminen, datan säilyttäminen ja kaikki muut dataan liittyvät toimet, jotka suoritetaan ennen suuririskisten tekoälyjärjestelmien markkinoille saattamista tai käyttöönottoa ja näitä toimia varten".

Käyttöönottajalta:

EU:n tekoälyasetus, 13 artiklan b alakohdan vi luetelmakohta, käyttöohjeet

- Tarjoajan on toimitettava "tarvittaessa syöttötietoja koskevat spesifikaatiot tai muut käytettyjä koulutus-, validointi- ja testausdatajoukkoja koskevat olennaiset tiedot ottaen huomioon suuririskisen tekoälyjärjestelmän käytötarkoitus" (tarjoajan käyttöönottajalle toimittamissa tiedoissa).

EU:n tekoälyasetus, 26 artiklan 4 kohta

- Siltä osin kuin käyttöönottaja valvoo syöttötietoja, käyttöönottajan on varmistettava, että syöttötiedot ovat merkityksellisiä ja riittävän edustavia suuririskisen tekoälyjärjestelmän käyttötarkoituksen kannalta.

Muut

- Dokumentaatioaloitteet
- Datajoukkojen datalomakkeet.
- Mallikortit mallien raportointia varten.
- Sovelletut datanhallinta- ja laatustandardit – jos vastaaja mainitsee standardien käytön, nämä standardit voivat auttaa ymmärtämään, mihin vastaaja on sitoutunut.
- Jos kyseessä on lainvalvonta / muuttoliikkeen hallinta, tietokannassa voi olla asiaankuuluvan markkinavalvontaviranomaisen käytettävissä olevia lisätietoja.

Syrjinnän indikaattorit

Alla mainitut indikaattorit osoittavat dataan liittyviä ongelmia, jotka voivat osaltaan vahvistaa *prima facie* -tapauksia osoittamalla yleisesti, että käytössä oleva data on epäluotettavaa tai sisältää vinoumia. Nämä indikaattorit voivat myös kannustaa pyytämään lisätästä. Tämä luettelo ei todennäköisesti kata kaikkia indikaattoreita. Yllä kuvatuista kohdista voi seurata muitakin huomioitavia seikkoja, joita ei ole tässä lueteltu.

- Yleiset dataongelmat:
 - ei edustavaa (maantieteellisellä alueella tai sektorilla)
 - virheellisesti hankittua (uudelleenkäytettyä)
 - ei ajantasaista
 - valintaharhoja esiinty

- mittausharhoja esiintyy siinä mielessä, etteivät tunnisteet vastaa ennakoitavia käsitteitä tai ovat yleisesti epäluotettavia.
- ▶ Syrjintään liittyvien datan laatuongelmien indikaattorit:
 - data ei edusta kaikkia asianosaisia
 - suuri todennäköisyys, että data heijastaa historiallista tai jatkuvaa eriarvoisuutta
 - valintaharha johtaa todennäköisesti kiellettyihin syrjintäperusteisiin kuuluvia ominaisuuksia omaavien ryhmien yli- tai aliedustukseen
 - mittausharha vaikuttaa todennäköisesti ryhmiin, joilla on kiellettyihin syrjintäperusteisiin kuuluvia ominaisuuksia
 - datan hankinnassa tai luomisessa tai tunnisteiden lisäämisessä on viitteitä syrjinnästä.
- ▶ Dataa koskevia päätöksiä ei ole dokumentoitu riittävästi.
- ▶ Lieventäviä toimenpiteitä ei ole tehty tai niiden tehokkuutta ei voida osoittaa.

Indikaattorit siitä, ettei tekoälyasetuksen suuririskisiä järjestelmiä koskevia vaatimuksia ole noudatettu

Vaikka tekoälyasetuksen vaatimusten noudattamatta jättäminen ei ole tämän arviointimenetelmän keskiössä, kaikki viitteet siitä, ettei tekoälyasetuksen vaatimuksia täytetä, voivat johtaa korjaaviin toimenpiteisiin (katso [vaihe 4](#)).

- ▶ Tarjoaja ei voi osoittaa, että käytössä olevilla käytännöillä varmistetaan datajoukkojen noudattavan seuraavia vaatimuksia: Ne ovat ”käyttötarkoitukseen nähden merkityksellisiä, riittävän edustavia ja niin suurelta osin kuin mahdollista virheettömiä ja täydellisiä. Niillä on oltava asianmukaiset tilastolliset ominaisuudet, tarvittaessa myös niiden henkilöiden tai henkilöryhmien osalta, joihin liittyen suuririskistä tekoälyjärjestelmää on tarkoitus käyttää. Kyseiset datajoukkojen ominaisuudet voidaan saavuttaa yksittäisten datajoukkojen tai niiden yhdistelmän tasolla.” Vaihtoehtoisesti tarjoaja ei pysty antamaan tästä todisteita.
- ▶ Tarjoaja ei ole tehnyt vinoumatestejä tai testannut kaikkia sovellettavia vinoumia.
- ▶ Tarjoaja ei ole toteuttanut tehokkaita toimenpiteitä havaittujen tai epäiltyjen vinoumien ehkäisemiseksi ja lieventämiseksi.

- ▶ Kirjaa tietoihin kaikki yleiset dataongelmat, datan laatuun liittyvät ongelmat, riittämättömään dokumentointiin liittyvät ongelmat ja mahdolliset lieventäviin toimenpiteisiin liittyvät huolenaiheet.
- ▶ Kirjaa tietoihin kaikki eriarvoisuuteen ja syrjintään liittyvät dataongelmat, lieventäviin toimenpiteisiin liittyvät huolenaiheet ja – jos saatavilla – perustelut sille, miten nämä voivat johtaa eriarvoiseen kohteluun käsiteltävässä tapauksessa.
- ▶ Kirjaa tietoihin kaikki viitteet siitä, ettei dataan sovellettavia tekoälyasetuksen säännöksiä noudateta.

3.6. Testaus ja arviointi

Testauksen ja arvioinnin tulokset voivat antaa arvokasta tietoa sen arvioimiseksi, onko syrjintää esiintynyt. Keskeinen kysymys on, tuottaako algoritmijärjestelmä eriarvoisia tuloksia erilaisille henkilöryhmille. Yksi tapa osoittaa tämä on järjestelmän tuotosten tilastointi.

Kun tilastollisia yhdenvertaisuustietoja on saatavilla, näiden tietojen validiteetti ja luotettavuus on arvioitava (katso jäljempää). Tämän vuoksi on tärkeää tarkastella näiden tilastojen laskennassa käytettyjen tietojen validiteettia ja luotettavuutta. Siksi tämä osio on luettava yhdessä [kohdan 3.5](#) kanssa.

Tässä vaiheessa teknisestä ja sektorikohtaisesta asiantuntemuksesta voi olla hyötyä.

Eri ryhmien, joilla on erilaisia kiellettyihin syrjintäperusteisiin kuuluvia ominaisuuksia, tulosten testaamiseksi tarvitaan tietoa näistä kielletyistä syrjintäperusteista. Jos halutaan esimerkiksi testata, tuottaako järjestelmä erilaisia tuotoksia miehille ja naisille, on tiedettävä, ketkä testattavassa datassa ovat miehiä ja ketkä naisia. Näitä tietoja ei välttämättä ole aina saatavilla. Tässä tapauksessa testauksessa on keskityttävä käytettävissä oleviin ominaisuuksiin, mukaan lukien sellaisiin, jotka kuuluvat tai saattavat liittyä kiellettyihin syrjintäperusteisiin. Tämä tarkoittaa esimerkiksi tilanteita, joissa etnistä alkuperää koskevia tietoja ei välttämättä ole saatavilla, mutta kansalaisuutta koskevia tietoja on, tai kasvokuvia koskevia tapauksia, joissa ei ole saatavilla rotua koskevia tietoja, mutta kasvokuvista saatuja ihonväriä koskevia tietoja voidaan käyttää.

(Lisä)tilastotietojen hankkiminen

Kun tilastotietoja ei ole saatavilla tai ne eivät riitä algoritmisen syrjinnän arviointiin, on olemassa vaihtoehtoja, jotka voivat auttaa hankkimaan (lisä)tilastotietoja.

Markkina- ja valvontaviranomaisen suorittama arviointi ja testaus

Jos yhdenvertaisuuselin ei pysty selvittämään, onko unionin oikeuden mukaisia oikeuksia loukattu, tekoälyasetuksen 77 artiklan 3 kohdan mukaan yhdenvertaisuuselin "voi esittää markkina- ja valvontaviranomaiselle perustellun pyynnön järjestää suuririskisen tekoälyjärjestelmän testaus teknisin keinoin". Yhdenvertaisuuselimen tulisi olla tiiviisti mukana testauksessa.

Johdanto-osan kappaleessa 157 tehdään selväksi, että 77 artiklan mukaista menettelyä on sovellettava perusoikeuksille riskin aiheuttaviin suuririskisiin tekoälyjärjestelmiin, markkinoille saatettuihin kiellettyihin järjestelmiin (6 artikla), kiellettyjen käytäntöjen vastaisesti käyttöön otettuihin tai käytettyihin järjestelmiin (5 artikla) sekä suuririskisiin ja ei-suuririskisiin tekoälyjärjestelmiin, jotka on asetettu saataville asetuksessa säädettyjen avoimuusvaatimusten vastaisesti ja joihin liittyy riski (6 artiklan 4 kohta ja 50 artikla).

Yhdenvertaisuuselimen suorittama tai kolmansien osapuolten kanssa yhteistyössä tehty testaus

Yhdenvertaisuuselimet voivat laatia omia yhdenvertaisuustietojaan tehdessään valvonta- ja muita tehtäviään syrjintää ja/tai yhdenvertaisuuselimiä koskevien direktiivien ja asetusten nojalla tai muutoin. Näitä tietoja on kuitenkin käytettävä varoen, koska on olemassa riski, ettei niitä pidetä riippumattomina oikeudenkäyntimenettelyissä. Tällä hetkellä on epäselvää, miten tekoälyasetuksen 78 artiklan luottamuksellisuutta koskevat velvollisuudet vaikuttavat yhteen tarkoitukseen hankittujen tietojen käyttöön siviilioikeudenkäynneissä (verrattuna asetuksessa nimenomaisesti mainittuihin rikosoikeudellisiin ja hallinnollisiin menettelyihin).

On pohdittava, onko näyttö, johon tapauksessa on tarkoitus vedota, hankittu seuraavasti:

1. yhdenvertaisuuselimen riippumattoman ja puolueettoman kiistanratkaisuroolin tai valvonta- ja tiedonkäsittelyroolin tuloksena
2. oikeudenkäyntitarkoitusta varten.

Jos tiedot laadittiin ensimmäisen vaihtoehdon tuloksena, niiden riippumattomuus saatetaan kyseenalaistaa. Equinet on todennut seuraavaa:

Kun yhdenvertaisuuselin käyttää oikeudenkäyntimenettelyissä omia tietojaan, tuomioistuimella voi teoriassa olla vaikeuksia pitää tällaisia tietoja ulkoisina ja riippumattomina. Lisäksi tapauksissa, joita yhdenvertaisuuselin ratkaisee (osittain) omien yhdenvertaisuustietojensa perusteella, asian osapuolet ja muut tarkkailijat saattavat kyseenalaistaa tällaisen käytännön ainakin kahdesta eri syystä: onko elin puolueeton kiistanratkaisuelin, jos se tunnistaa ja käyttää ennakoivasti väitettyä uhria suosivaa näyttöä[?], ja onko tällainen näyttö uskottavaa, jos elin itse on tuottanut tiedot, kun elimen on määritelmänsä mukaan tarkoitus edistää yhdenvertaisuutta / tukea uhreja[?]. Tällaiset mahdolliset (koetut) oikeudenmukaiseen oikeudenkäyntiin / oikeuskeinojen tasapuolisuuteen liittyvät ongelmat saattavat vaikuttaa yhdenvertaisuuselimen yleiseen uskottavuuteen yhteiskunnassa, mukaan lukien sen raportointiroolissa. (Ilieva, 2024)

Algoritmijärjestelmän tilastolliset analyysit

Tapauksissa, joissa algoritmijärjestelmä ja asiaankuuluvat tiedot ovat yhdenvertaisuuselimen käytettävissä, yhdenvertaisuuselin voi tehdä oman tilastollisen arviointinsa. Sekä oikeudenmukaisuusmittareita että niiden täytäntöönpanomenetelmiä on hyödynnetty useissa avoimen lähdekoodin oikeudenmukaisuusvälineissä. Näitä välineitä voidaan käyttää algoritmijärjestelmien tai niiden datajoukkojen suorituskykypuutteiden mittaamiseen. Yleisiä esimerkkejä ovat IBM AI Fairness 360 ja Microsoft Fairlearn, mutta saatavilla on monia muitakin. Ei ole olemassa yhtä tiettyä suositeltavaa välinettä, koska niillä kaikilla on omat hyötynsä ja puutensa (Mittelstadt, 2024).

Tilannetestaus

Myös tilannetestausta voidaan käyttää syrjintään liittyvän näytön hankintaan. Tilannetestaus tarkoittaa kokeellista menetelmää, jossa testattavien parien ainoa eroavaisuus on kielletty syrjintäperuste. Näin voidaan testata kohtelun mahdollisia eroja.

Joissakin konteksteissa, kuten algoritmisessa rekrytinnissa, varteenotettava vaihtoehto on kerätä tilastotietoja tietystä algoritmijärjestelmästä (syrijintää koskevan) tilannetestausten avulla. Useissa maissa, kuten Yhdistyneessä kuningaskunnassa, Alankomaissa, Ranskassa, Tanskassa, Suomessa ja Ruotsissa, tilannetestaus on hyväksytty päteväksi todistemuodoksi (Euroopan komissio, 2019). Laajamittainen tilannetestaus voi myös tuottaa tilastotietoa, ja sitä on sovellettu monissa eri yhteyksissä, kuten työllisyyden, asumisen ja muunlaisten hyödykkeiden ja palveluiden saatavuudessa. Testien tuloksia pidetään hyväksyttävänä todisteina useissa EU-maissa. Luotettavien tulosten varmistamiseksi yhdenvertaisuuselimen voi olla tarpeen tehdä testauksessa yhteistyötä asiantuntijatahojen kanssa (Makkonen, 2016).

Yhteistyö tilastolaitosten kanssa / yleisten tilastojen käyttö

Yleisiä tilastoja voidaan käyttää osoittamaan, että sijaismuuttajien käyttö johtaa erilaiseen kohteluun. Esimerkki tästä on Alankomaiden korkeakoulujen opintoavustuksen tarkastuksia koskeva tapaus:

- ▶ Algoritmi käytti koulutustasoa opiskelijoiden erottamiseen toisistaan.
- ▶ Alankomaiden kansallisen tilastoviraston (CBS) yleisten tilastojen mukaan alimmilla koulutustasoilla olivat yliedustettuina opiskelijat, joilla oli muu kuin länsimainen maahanmuuttajatausta: näitä opiskelijoita oli noin kaksi kertaa odotettua enemmän muihin opiskelijoihin verrattuna ([StatLine – Mbo; studenten, niveau, leerweg, migratie 2005/06–2021/22](#))
- ▶ Kun näitä tietoja käytettiin ilman yksittäisten opiskelijoiden taustatietojen tarkastelua, koulutustaan käyttäminen algoritmijärjestelmissä johti opiskelijoiden eriarvoiseen kohteluun.

Tuomioistuinten lähestymistapa tilastotietoihin

Tilastotietojen tarpeellisuus

Tilastot eivät itsessään välttämättä paljasta syrjintää tai syrjiviä käytäntöjä (*Hugh Jordan v. Yhdistynyt kuningaskunta*, hakemusno 24746/94, Euroopan ihmisoikeustuomioistuin).⁵⁴ Ne kuuluvat merkityksellisiin todisteisiin, joita voidaan käyttää välillisen tai välittömän syrjinnän *prima facie*-tapauksen osoittamiseen tai kumoamiseen. Tuomioistuimet voivat yleensä olla taipuvaisempia hyväksymään kantelijoiden esittämiä tilastollisia todisteita välittömän syrjinnän *prima facie*-tapauksen osoittamiseksi kuin tukeutumaan vastaajien esittämiin tällaisiin todisteisiin sen kumoamiseksi, mikä heijastaa osapuolten välistä tiedon epätasapainoa ja kantelijoiden kohtaamia tunnettuja vaikeuksia saada syrjintäväitteitä tukevia todisteita (Makkonen, 2007). Kansallisen tuomioistuimen tehtävänä on

54. Tilastot osoittivat eron eri uskontokuntiin kuuluvien surmattujen määrien välillä mutta eivät sitä, olivatko surmat laittomia tai johtuivatko ne turvallisuusjoukkojen jäsenten liiallisesta voimankäytöstä (kohta 154).

arvioida, ovatko saatavilla olevat tilastot ”päteviä” ja voidaanko ne ottaa huomioon tapauksessa (katso Enderby, asia C-127/92, 16 kohta).

Tilastotiedot ja välitön syrjintä

Välittömän syrjinnän tapauksessa tilastot voivat paljastaa syrjivän kuvion olemassaolon ja siten tarjota näyttöä välittömästä syrjinnästä yksittäisen valituksen tapauksessa. Tilastollisen näytön käyttöä ei kuitenkaan yleensä vaadita välittömän syrjinnän *prima facie* -tapauksen osoittamiseksi.

Tilastotiedot ja välillinen syrjintä

Tilastotiedot ovat erityisen hyödyllisiä välillisen syrjinnän tapauksissa, joissa kantelija voi tilastojen avulla osoittaa, että näennäisesti neutraalin käytännön tai säännön soveltamisella on suhteeton vaikutus tiettyyn henkilöryhmään verrattuna muihin vastaavassa tilanteessa oleviin (FRA, 2018: 242).

Kun kantelija pystyi erityisesti osoittamaan, että kiistattomat viralliset tilastot perustivat *prima facie* -näytön siitä, että tietty sääntö,

vaikka se olikin laadittu neutraalilla tavalla, vaikutti tosiasiaissa selvästi suurempaan osaan naisia kuin miehiä, vastaajahallituksen asiana oli näyttää tämän johtuvan objektiivisista seikoista, jotka eivät liittyneet sukupuoleen perustuvaan syrjintään (*Hoogendijk v. Alankomaat*, 2005).

Tiukkaa kynnysarvoa ei ole asetettu, mutta yleensä on saavutettava merkittävä arvo, jotta voidaan osoittaa erilainen vaikutus. Käytännössä tämä yleensä tarkoittaa huomattavasti suurempaa määrää (Ingrid Rinner-Kühn, 1989), huomattavasti pienempää prosenttiosuutta (Helga Nimz, 1991, ja Maria Kowalska, 1990) tai merkittävää erotusta (M.A. De Weerd, 1994), vaikka tilastotietojen toimittaminen välillisen syrjinnän osoittamiseksi ei olekaan muodollinen vaatimus (katso *DH ym. v. Tšekin tasavalta*, 2007, 188 kohta). Tarkkoja tilastotietoja ei kuitenkaan vaadita. Tämä koskee erityisesti tapauksia, joissa syrjintävaihtamisen tehneellä osapuolella ei ole pääsyä näihin tilastoihin tai pääsy näihin tilastoihin on vaikeaa (*Minoo Schuch-Ghannadan*, 2019).

Muun datan ja näytön käyttö

Näyttö muiden käytännöistä tai uskomuksista samaan suojattuun ryhmään kuuluvia henkilöitä kohtaan voi olla riittävää. Esimerkiksi käytäntöä, jossa lapset asetettiin eri luokkiin heidän riittämättömän kroatian kielitaitonsa perusteella, sovellettiin vain romanioppilaisiin, mikä johti oletettavaan erilaisesta kohtelusta, vaikka tilastot eivät osoittaneet syrjintää. Euroopan ihmisoikeustuomioistuin on todennut, että välillinen syrjintä voidaan näyttää toteen ilman tilastollista näyttöä (*Oršuš ym. v. Kroatia*, 2010).

Algoritmijärjestelmiä koskevissa tapauksissa muutkin tosiseikat ja todisteet voivat riittää *prima facie* -syrjinnän osoittamiseen. Esimerkiksi Deliveroon tapauksessa tuomioistuin ei edellyttänyt laajoja tilastollisia testejä tai monimutkaista data-analyysiä. Sen sijaan järjestelmän suunnittelu itsessään – sellaisena kuin se oli perustasolla rekonstruoitu saatavilla olevien tietojen, kuten sopimuslausekkeiden, alustan usein

kysyttyjen kysymysten, vastaajan ulkoisen ja sisäisen viestinnän sekä asianomaisten henkilöiden todistusten, perusteella – yhdistettynä sen ennakoitavissa olevien vaikutusten arviointiin riitti osoittamaan suhteettoman haitan ja osoittamaan *prima facie* -syrjintätapauksen.

Tilastollisten yhdenvertaisuustietojen arviointi vastaajan kannalta

Yhdenvertaista kohtelua koskevan lainsäädännön tarkoituksia varten tilastotietojen on oltava sekä päteviä että luotettavia.

Validiteetti- ja luotettavuustestejä on sovellettava kaikissa konteksteissa. Seuraava kolmivaiheinen prosessi voi auttaa tässä.

- ▶ Onko tarjoajan tai käyttöönottajän testauksessa ja arvioinnissa käyttämä lähestymistapa perustunut pätevään ja luotettavaan tilastotietoon tai onko se tuottanut sellaista?
- ▶ Onko vastaajan väitteitä kyseenalaistava tilastollinen näyttö sekä pätevää että luotettavaa?
- ▶ Onko tilastollinen vastanäyttö pätevää ja luotettavaa?

Jotta tilastotietoja voidaan pitää ”pätevinä”, seuraavien kriteerien on täyttyttävä:

- ▶ Ne vaikuttavat yleisesti ottaen merkityksellisiltä.
- ▶ Ne kattavat riittävästi yksilöitä.
- ▶ Ne kuvaavat ilmiöitä, jotka eivät ole sattumanvaraisia tai lyhytaikaisia.
- ▶ Ne ovat kokonaisuutena ”merkityksellisiä ja riittäviä”.

Tilastotietojen luotettavuus viittaa käytetyn mittauksen/testin stabiliteettiin tai johdonmukaisuuteen. Esimerkiksi syrjintää koskeva mittaus on luotettava siinä määrin kuin mittausmenetelmä tuottaa samat tulokset toistetuissa tutkimuksissa. Jos esimerkiksi mitataan vuosittain ilmoitettujen yhdenvertaisuutta koskevien tapausten määrää, mutta toimivaltaisten (yhdenvertaisuus)elinten määrä muuttuu ajan myötä, tällä on negatiivinen vaikutus mittarin luotettavuuteen ja myös sen vertailukelpoisuuteen ajan kuluessa. Mikään mittaus ei ole täysin luotettava, vaan luotettavuus on aina suhteellisuuskysymys.⁵⁵

Yhdenvertaisuusmittareiden valinta

Datatieteessä on tunnistettu useita mittareita, joilla mitataan erilaisia käsityksiä siitä, mikä on oikeudenmukaista. Näitä mittareita ei ole ohjattu syrjimättömyyslainsäädännöllä, eikä päällekkäisyys datatieteen ja tekoälyn alan oikeudenmukaisuuden mittareiden ja yhdenvertaisuuden käsitteiden välillä ole aina selvä (Weerts et al., 2023). Valitettavasti on matemaattisesti mahdotonta luoda järjestelmää, joka olisi oikeudenmukainen kaikkien teknisten mittareiden mukaan.

55. Katso Euroopan komissio, 2021: 20; Enderby, 1993, 17 kohta; Seymour-Smith, 1999, 62 kohta. Syrjimättömyystapauksissa sovellettavien tilastojen yleiset vaatimukset: katso *Enderby v. Frenchay Health Authority and Secretary of State for Health*, 17 kohta.

Siksi on välttämätöntä määrittää, mitä erilainen kohtelu ja epäedullinen asema (syrjinnän olennaisena osana) tarkoittavat käsiteltävän tapauksen yhteydessä, ja valita mittarit, jotka vastaavat käsiteltävää tapausta parhaiten. On huomattava, että pelkkä sellaisen oikeudenmukaisuusmittarin esittäminen, joka osoittaa järjestelmän olevan ”oikeudenmukainen” kyseisellä mittarilla, ei tarkoita, että järjestelmä johtaa yhdenvertaiseen kohteluun. Jos epäoikeudenmukaisuutta esiintyy, on tärkeää pohtia, miksi päätös käyttää kyseisiä yhdenvertaisuusmittareita tehtiin ja mitä toimenpiteitä on tehty syntyneen eriarvoisuuden korjaamiseksi.

Demografinen pariteetti mittaa, onko tietyn ennusteen todennäköisyys sama kahdelle eri ryhmälle. Tämä mittari on merkityksellisin silloin, kun yksi tuotos on kyseessä olevien henkilöiden kannalta epäedullinen muihin tuotoksiin verrattuna. Tämä heijastaa eriarvoisen kohtelun käsitettä parhaiten esimerkiksi tilanteissa, joissa tavoitteena on ennakoida petoksia (kun yhtä ryhmää epäillään petoksesta useammin kuin toista) tai rekrytoida työntekijöitä (kun yksi ryhmä valitaan haastatteluun useammin kuin toinen). Monissa tapauksissa demografinen pariteetti on asianmukainen mittari, ellei ole pakottavia syitä turvautua toiseen mittariin. On huomioitava, että demografiseen pariteettiin voidaan joskus viitata myös termeillä riippumattomuus, ryhmätason oikeudenmukaisuus, tilastollinen pariteetti, erilainen vaikutus, yhtäläinen valintaprosentti tai yhtäläinen hyväksymisprosentti.

Muut asiaankuuluvat mittarit perustuvat järjestelmän virheisiin ja testaavat, aiheuttavatko järjestelmät yhdelle ryhmälle enemmän virheitä kuin toiselle. Tämän tyyppinen mittari on merkityksellisin silloin, kun haitta johtuu ylivoimaisesti järjestelmien virheistä tuotosten sijaan. Esimerkkejä, joissa virhepohjaiset mittarit ovat merkityksellisimpiä, ovat kasvontunnistus ja diagnostinen testaus lääketieteessä. Katso alla olevasta taulukosta 6 yleiskatsaus mahdollisesti merkityksellisistä mittareista.

On epätodennäköistä, että yleispätevä lähestymistapa testaukseen on riittävä. Sen sijaan on olennaista tarkastella sekä käytettyjä tilastollisia malleja että niiden rajoituksia ja ympäröiviä olosuhteita, kuten päätöksenteosta vastaavaa organisaatiota ja käytettyjä prosesseja (Barocas et al., 2023). ”Numerot” sellaisinaan ilman kontekstia eivät ole riittävän merkityksellisiä ollakseen päteviä tai luotettavia.

Vaikka demografinen pariteetti valittaisiin ensisijaiseksi mittariksi, on suositeltavaa harkita lisäksi mittaria, joka ottaa huomioon virheet. Tarjoajilla on vaatimus asettaa ”odotettu yleinen tarkkuus” tiettyjen henkilöryhmien osalta (tekoälyasetus, liitteen IV 3 kohta).

Yhdenvertaisuustilastot voidaan esittää suhdelukuina tai erillisinä ryhmien välisinä mittareina. Jäljempänä on muutamia esimerkkejä.

- ▶ Demografisen pariteetin tilastot rekrytointiympäristössä voidaan ilmaista seuraavasti: 25 % miespuolisista hakijoista ja 15 % naispuolisista hakijoista kutsutaan haastatteluun automaattisen ansioluetteloon perustuvan valinnan jälkeen. Tämä voidaan ilmaista myös suhdelukuna: $0,15/0,25 = 0,6$.
- ▶ Syöpäseulonnan yhtäläiset mahdollisuudet voidaan ilmaista seuraavasti: Seulontatyökalulla havaitaan 75 % miehistä, joilla on syöpä, ja 65 % naisista, joilla on syöpä. Tämä voidaan ilmaista myös suhdelukuna: $0,65/0,75 = 0,87$.

Taulukko 6. Oikeudenmukaisuusmittareiden kuvaus

(mukautettu luvalla lähteestä Mittelstadt, 2023)

Mittari	Kuvaus	Milloin sovelletaan	Esimerkki
Demografinen pariteetti	Eri ryhmillä tulisi olla samankaltainen positiivisten tuotosten aste. Demografiseen pariteettiin voidaan joskus viitata myös termeillä riippumattomuus, ryhmätason oikeudenmukaisuus, tilastollinen pariteetti, erilainen vaikutus, yhtäläinen valintaprosentti tai yhtäläinen hyväksymisprosentti.	– Tilanteissa, joissa tuotos itsessään (virheiden sijaan) aiheuttaa haittaa. – Tilanteissa, joissa historiallisen datan odotetaan olevan puolueellista. – Tilanteissa, joissa ei ole luotettavia tunnistuksia (ei hyväksytyjä pohjatotuuksia).	Rekrytointi, lainojen myöntäminen, petosten havaitseminen ja koulutuksen saatavuus.
Yhtäläiset mahdollisuudet	Eri ryhmillä tulisi olla samankaltainen väärien negatiivisten aste. Tähän voidaan viitata myös termillä väärien negatiivisten virhesuhteen tasapaino.	– Tilanteissa, joissa merkittävä haitta johtuu vääristä negatiivisista tuloksista. – Lisäksi luotettavia tunnistuksia (hyväksytyjä pohjatotuuksia) on olemassa.	Sairauksien seulonta.
Ennustava pariteetti	Väärien positiivisten prosenttiosuuden kaikista positiivisista tulisi olla samankaltainen eri ryhmillä. Tähän voidaan viitata myös termeillä tuotostestaus ja positiivisen ennustearvon pariteetti.	– Tilanteissa, joissa merkittävä haitta johtuu vääristä positiivisista tuloksista. – Lisäksi luotettavia tunnistuksia (hyväksytyjä pohjatotuuksia) on olemassa.	Poliisin suorittama kasvontunnistus tutkinnan kohteena olevan henkilön tunnistamiseksi.
Väärien positiivisten osuuden tasapaino	Eri ryhmillä tulisi olla samankaltainen väärien positiivisten aste. Tähän voidaan viitata myös termillä ennusteen yhdenvertaisuus.	– Tilanteissa, joissa merkittävä haitta johtuu vääristä positiivisista tuloksista. – Lisäksi luotettavia tunnistuksia (hyväksytyjä pohjatotuuksia) on olemassa.	Poliisin suorittama kasvontunnistus tutkinnan kohteena olevan henkilön tunnistamiseksi.
Tasapainotetut todennäköisyydet	Oikeiden ja väärien positiivisten osuuksien tulisi olla samankaltaiset eri ryhmillä. Tähän voidaan myös viitata termeillä ehdollinen menettelyn tarkkuuden yhdenvertaisuus ja toisenlainen väärinkohtelu.	– Tilanteissa, joissa sekä väärien positiivisten että väärien negatiivisten aiheuttamat haitat on huomioitava. – Lisäksi luotettavia tunnistuksia (hyväksytyjä pohjatotuuksia) on olemassa.	Sairauden hoito riskialttiilla leikkauksella.

Vastaajan antamien tilastojen arviointi

Yhdenvertaisuuselinten tulisi huomioida vähintään kolme seikkaa tilastollisten yhdenvertaisuusmittareiden validiteetin arvioinneissa.

1. Yleisesti ottaen mittarin laskennassa käytetyn datan laatu ja vinoumat (katso [vaihe 3.5](#)).
2. Mittarin suunnittelu ja vertailuryhmien valinta.

Kun tarkastellaan tapaa, jolla järjestelmän tarjoaja on tunnistanut ja mitannut suorituskypuutteita, yhdenvertaisuuselinten on kiinnitettävä erityistä huomiota siihen, miten mittauspäätös on tehty ja mitä henkilöryhmiä vertaillaan toisiinsa. Tämä on tärkeä päätös syrjimättömyyslainsäädännön kontekstissa, jossa muita heikommassa asemassa olevien ryhmien ja vertailuryhmien asianmukaisten määrittely on usein avainasemassa. (Mittelstadt, 2024). Ryhmien valinta voi (tarkoituksella) peittää tosielämän eriarvoisia tuotoksia.

Yhdenvertaisuuselimiä kehoitetaan pohtimaan seuraavia seikkoja:

- ▶ millaisia sovellettavia muita heikommassa asemassa olevia ryhmiä ja vertailuryhmiä tapauksessa voitaisiin harkita, ennen kuin tarkastellaan vastaajan tilastoja
- ▶ onko vastaaja valinnut ja määritellyt nämä samat ryhmät, ja jos ei ole, yhdenvertaisuuselimen on arvioitava, mitä tietoja vastaajan valinnoissa on saatu lisää tai menetetty
- ▶ mitä intersektionaalisia ryhmiä tapaukseen liittyy, koska keskittyminen pelkästään yhden ominaisuuden omaaviin ryhmiin piilottaa intersektionaaliset eriarvoisuudet
- ▶ millaisia selityksiä vastaaja on antanut ja erityisesti tietoja siitä, missä määrin huomioon otettujen henkilötietojen variaatiot olisivat johtaneet erilaisiin tuloksiin, jotta voidaan ymmärtää vastaajan valitsemia vertailuryhmiä
- ▶ mahdollisten lisätilastotietojen hankinta tapauksissa, joissa vastaaja ei ole raportoinut asiaankuuluvia oikeudenmukaisuusmittareita tai on määritellyt ryhmät, joihin vaikutuksia kohdistuu, liian kapeasti (katso edeltä tekstiruutu (Lisä)tilastotietojen hankkiminen) (Mittelstadt, 2024).

Tilastolliset yhdenvertaisuusmittarit ovat usein osa laajempia suorituskypyraportteja, jotka sisältävät erilaisia testituloksia. Nämä mittaavat järjestelmän suorituskypyn eri osa-alueita, kuten tarkkuutta (kuinka usein järjestelmä tekee oikean ennusteen) ja vakautta (sietokyky virheitä, odottamatonta käyttäytymistä ja tosielämän muutoksia (vaeltelu) vastaan). Yhdenvertaisuuselinten on tärkeää ymmärtää järjestelmän suorituskypyy yleisesti, sillä se on erittäin merkityksellinen algoritmisen syrjinnän arvioinnissa. Tämä koskee erityisesti tilanteita, joissa pohditaan mahdollista objektiivista perustelua (katso [vaihe 3.8](#)), kun keskeisiin kysymyksiin sisältyy järjestelmän sopivuuden tai asianmukaisuuden ja tarpeellisuuden selvittäminen.

3. Mittarien merkitys käsiteltävälle järjestelmälle käytännössä.

Mittarien tulisi edustaa käsiteltävää algoritmijärjestelmää. Käytetyt testit ovat saattaneet vanhentua tai järjestelmään liittyvät prosessit muuttua (esimerkki tästä on järjestelmä, johon sovelletaan hallituksen politiikkaa, mutta tämä politiikka on muuttunut).

On huomioitava, että käytettyjen mittareiden tulee edustaa järjestelmää sen jälkeen, kun mahdollisia lieventäviä toimenpiteitä vinoumien vähentämiseksi tai syrjinnän ehkäisemiseksi on tehty. Jos nämä toimenpiteet ovat manuaalisia, yhdenvertaisuuselinten on varmistettava, että tilastot vastaavat manuaalisen toimenpiteen jälkeistä tulosta.

Jos suuririskiselle tekoälyjärjestelmälle on arvioinnin jälkeen myönnetty vaatimustenmukaisuustodistus, sen oletetaan täyttävän tekoälyasetuksen 10 artiklan 4 kohdan mukaiset tietovaatimukset, joiden mukaan niissä "on otettava käyttötarkoituksen edellyttämässä laajuudessa huomioon ne ominaisuudet tai osatekijät, jotka ovat ominaisia sille maantieteelliselle, viitekehystenä olevalle, käyttäytymiseen liittyvälle tai toiminnalliselle ympäristölle, jossa suuririskistä tekoälyjärjestelmää on tarkoitus käyttää".

On todennäköistä, että nämä näkökohdat ohjaavat validiteetin testausta käytännössä (katso lisätietoja tilastotiedoista vaiheesta 3.6), mutta on tärkeää huomata, että tämä oletamus voidaan kumota. Yhdenvertaisuuselinten voi erityisesti olla tarpeen harkita, täyttävätkö käytetyt tiedot todella tekoälyjärjestelmän käyttötarkoituksen mukaiset vaatimukset. Jos järjestelmää käytetään muuhun kuin sen käyttötarkoitukseen, tätä oletamaa ei sovelleta.

Pohdittavia kysymyksiä

Yleinen suorituskypyttestaus

- ▶ Mitä suorituskypyn osa-alueita on testattu?
- ▶ Miten ja minne järjestelmän suorituskypyä eri henkilöiden ja henkilöryhmien tapauksissa koskevat tiedot on tallennettu?
 - Päivitetäänkö näitä tietoja järjestelmän elinkaaren aikana? Jos päivitetään, niin miten?
- ▶ Mitä mahdollisia vaikutuksia henkilöihin ja henkilöryhmiin on otettu huomioon suorituskypyttestausta tehtäessä?
- ▶ Valittiinko testauksen keskiöön jokin haitan muoto (kuten väärät positiiviset tai väärät negatiiviset)?
- ▶ Mitä mittareita suorituskypyttestauksessa käytettiin?
- ▶ Onko suorituskypyttestauksen avulla tuotettu sekaannusmatriiseja?
- ▶ Miten testitulokset validoitiin?
- ▶ Ovatko suorituskypyttestauksessa käytetyt tiedot riittävän edustavia, asiaan kuuluvia ja tarkasti ja asianmukaisesti mitattuja (katso [vaihe 3.5](#))?
- ▶ Täyttääkö vastaajan suorituskypyttestaus validiteetti- ja luotettavuusvaatimukset?

Tilastolliset yhdenvertaisuustiedot

- ▶ Minkä tyyppisiä tilastollisia yhdenvertaisuustietoja, oikeudenmukaisuusmittareita tai vinoumatestejä käytettiin?

- Vastaavatko vastaajan valitsevat mittarit yhdenvertaista kohtelua kyseisessä kontekstissa? (Yleensä demografinen pariteetti, ellei muille mittareille ole selkeitä perusteita. Katso edeltä taulukko 6).
- Jos tapauksessa käytettiin virhepohjaisia mittareita, otettiinko huomioon samat haitan muodot kuin tavallisessa suorituskkytestauksessa? (Jos tavallisessa suorituskkytestauksessa käytettiin esimerkiksi väärin positiivisiin keskittyvää mittaria, tehtiinkö sama yhdenvertaisuustestauksessa?) Kun testataan yhdenvertaisuutta suorituskvyn perusteella, loogisesti ajatellen myös tässä yhdenvertaisuustestissä tulisi käyttää parhaiten soveltuvaa suorituskymittaria. Soveltumattoman mittarin valinta voi viitata laiminlyöntiin yhdenvertaisuustestauksessa.
- Millä perusteella tai oikeutuksella nämä on valittu?
- Harkittiinko ja/tai hylättiinkö muita vaihtoehtoja? Jos harkittiin/hylättiin, miksi?
- Oliko käytettyjen, erilaisia kiellettyjä syrjintäperusteita kattavien testien kirjo riittävän laaja, jotta testeillä pystyttiin havaitsemaan erityyppisiä mahdollisia syrjinnän muotoja tai eri (intersektionaalisii) ryhmiin kohdistuvia vaikutuksia?
- Onko kullekin testille valittu asiaankuuluvat ”vertailuryhmät”? Sisältyvätkö nämä näkökohdat järjestelmän tekniseen dokumentaatioon?
- Käytettiinkö (jonkin tyyppisiä) oikeudenmukaisuuden valvontaa tai vinoumien poistamista koskevia menetelmiä?
 - Millä perusteella tai oikeutuksella nämä on valittu?
 - Harkittiinko ja/tai hylättiinkö muita vaihtoehtoja? Jos harkittiin/hylättiin, miksi?
 - Sisältyvätkö nämä näkökohdat järjestelmän tekniseen dokumentaatioon?
- Mitä hyötyjä ja haittoja oikeudenmukaisuuden valvonnasta tai vinoumien poistamisesta aiheutui?
 - Mihin henkilöryhmiin tämä vaikutti / tulee vaikuttamaan?
 - Tutkittiinko muiden ryhmien yhdenvertaiseen kohteluun kohdistuvia toissijaisia vaikutuksia?
- Miten testitulokset validoitiin?
- Ovatko tilastojen laskennassa käytetyt tiedot riittävän edustavia, asiaankuuluvia ja tarkasti ja asianmukaisesti mitattuja (katso [vaihe 3.5](#))?
- Täyttävätkö vastaajan tilastotiedot validiteetti- ja luotettavuusvaatimukset?

Mahdollisia tiedonlähteitä tilastollisten yhdenvertaisuustietojen arviointiin

Kantelija

Yleinen tietosuoja-asetus, 15 artiklan 1 kohdan h alakohta, merkitykselliset tiedot käsittelyyn liittyvästä logiikasta

Vastaaja

Tarjoajalta

EU:n tekoälyasetus, 10 artikla, data ja datanhallinta

EU:n tekoälyasetus, 11 artikla, tekninen dokumentaatio (liitteen IV 2 kohdan g alakohta ja 3 kohta):

- ▶ ”käytetyt validointi- ja testausmenettelyt, mukaan lukien tiedot käytetystä validointi- ja testausdatasta ja sen tärkeimmistä ominaisuuksista; mittarit, joita käytetään mittaamaan tarkkuutta, vakautta ja muiden III luvun 2 jaksossa vahvistettujen asiaankuuluvien vaatimusten noudattamista sekä mahdollisia syrjiviä vaikutuksia; testilokit ja kaikki vastuuhenkilöiden päiväämät ja allekirjoittamat testiraportit, myös f alakohdassa tarkoitettujen ennalta määriteltujen muutosten osalta”.

EU:n tekoälyasetus, 11 artikla, lokit

Muut tiedot, joita vastaajalta voidaan pyytää:

- ▶ pääsy järjestelmään
 - ▶ esimerkkejä (synteettisistä) datajoukoista
 - ▶ kaikki järjestelmän suorituskykyä tai luotettavuutta koskevat raportit, mukaan lukien virhematriisit
 - ▶ tiedot suoritettujen testauksen tyypistä ja menetelmästä, mukaan lukien mahdollisesti sovelletut (yhdenmukaistetut) standardit
 - ▶ kaikki raportit suoritetuista vinouma- ja oikeudenmukaisuustesteistä
 - ▶ vapaaehtoinen HRIA-, FRIA- tai DPIA-arviointi tai eettisiä ohjeita tai lasten oikeuksia koskeva vaikutustenarviointi
 - ▶ vastaajan jakamat muut (riskin)arviointit
 - ▶ tiedonvälityksen vapautta koskevat pyynnöt.
-

Syrjinnän indikaattorit

- ▶ Kiellettyihin syrjintäperusteisiin kuuluvia ominaisuuksia omaavien henkilöryhmien tuotoksissa on puutteita tai virheitä sellaisten parhaiten sovellettavien mittareiden mukaan, jotka edustavat yhdenvertaista kohtelua kyseisessä tapauksessa.
- ▶ Parhaiten sovellettavat mittarit, jotka edustavat yhdenvertaista kohtelua kyseisessä tapauksessa, eivät ole saatavilla, tai on käytetty epäasianmukaisia mittareita.
- ▶ Kiellettyihin syrjintäperusteisiin kuuluvia ominaisuuksia omaavien henkilöryhmien tuotoksissa on puutteita tai virheitä muiden (ei sen mittarin, joka parhaiten edustaa yhdenvertaista kohtelua kyseisessä tapauksessa) mittareiden mukaan.
- ▶ Kaikkia ryhmiä, joihin vaikutukset kohdistuvat, ei ole huomioitu, tai nämä ryhmät on määritetty liian suppeasti ilman, että intersektionaalinen syrjintä on huomioitu.
- ▶ Oikeat ryhmät tunnistettiin ja asianmukaisia mittareita sovellettiin, mutta johtopäätökset eivät ole pitäviä esimerkiksi dataongelmien vuoksi.
- ▶ Vain yhden testatun mittarin tuloksista on raportoitu useiden oikeudenmukaisuusmittareiden (kuten täsmällisyyden, saannin ja virheprosenttien⁵⁶) tulosten sijaan. Useiden eri mittareiden testaaminen voi olla tarpeen erilaisten suorituskykypuutteiden selvittämiseksi.

Syrjinnän kumulatiiviset indikaattorit

Kaikki aiemmin mainitut indikaattorit voivat toimia kumulatiivisesti. Seuraavassa on muutamia esimerkkejä tästä.

- ▶ Tarjoaja/käyttöönottaja on tunnistanut syrjintärisikin (katso [vaihe 3.3](#)), mutta testaus ei ole kattanut kaikkia henkilöitä ja/tai ryhmiä, joihin se voi kohdistua – tämä koskee erityisesti sijaismuuttujia ja kumulatiivista/intersektionaalista syrjintää. Esimerkki tästä on tapaus, jossa on testattu sukupuoleen perustuvaa syrjintää mutta ei rotuun tai etniseen alkuperään perustuvaa, vaikka rotusyrjinnän riski tunnistettiin.
- ▶ Kolmas osapuoli on tunnistanut syrjinnän (tai sen riskin) (katso [vaihe 3.1](#)), mutta testaus ei ole kattanut kaikkia henkilöitä ja/tai ryhmiä, joihin se voi kohdistua – tämä koskee erityisesti sijaismuuttujia ja kumulatiivista/intersektionaalista syrjintää. Esimerkki tästä on tapaus, jossa on testattu sukupuoleen perustuvaa syrjintää mutta ei rotuun tai etniseen alkuperään perustuvaa syrjintää, vaikka aiemmissa samankaltaisissa tapauksissa henkilöitä on asetettu muita heikompaan asemaan sekä rodun että raskauden perusteella.
- ▶ Syöttökriteerit liittyvät vahvasti kiellettyihin syrjintäperusteisiin tai algoritmeissa käytetään sijaismuuttujia (katso [vaihe 3.3](#)), eikä testauksella selvitetä, täyttyvätkö suojatun ryhmän yhdenvertaisen kohtelun vaatimukset.

56. Data-analyysseissä voidaan käyttää erilaisia mittareita järjestelmän suorituskyvyn eri osa-alueiden kuvaamiseen. Esimerkiksi täsmällisyys keskittyy positiivisten ennusteiden tarkkuuteen (väärin hälytysten välttäminen), kun taas saanti mittaa kykyä havaita kaikki todelliset positiiviset tapaukset (huomaamatta jääneiden tapahtumien välttäminen).

- Kirjaa tietoihin tilastoista ilmenevät tuotosten tai käsittelyn puutteet.
- Kirjaa tietoihin kaikki raportoituihin tilastoihin liittyvät ongelmat (kuten virheellinen mittari tai dataan liittyvät ongelmat).
- Kirjaa tietoihin mahdolliset testauksen puutteet.
- Yhdistä tämän vaiheen tulokset edellisen vaiheen tuloksiin selvittääksesi, voidaanko *prima facie* -syrijintätapaus näiden yhdistettyjen tietojen perusteella osoittaa ja/tai onko vastaaja onnistuneesti kumonnut oletettaman tai perustellut syrjinnän (jos tarkastellaan perusteluja, katso myös järjestelmän tavoitteita koskeva näkökohta kohdasta 3.4).
- Kirjaa tehty johtopäätös tietoihin.

Esimerkki: Smart Check Amsterdam

Tämä malli suunniteltiin seulomaan sosiaaliturvahakemuksia ja tunnistamaan hakemukset, jotka todennäköisimmin sisälsivät merkittäviä virheitä, merkitsemään ne ja lähettämään sitten tapaukset tutkintaosastolle lisätutkimuksia varten. Tavoitteena oli vähentää tutkittaviksi merkittyjen hakemusten määrää.

Riskipisteiden määrittämiseksi tarkasteltiin viittätoista ominaisuutta. Nämä sisälsivät useita erilaisia tekijöitä, kuten tiedon siitä, oliko hakija aiemmin hakenut tai saanut sosiaaliturvaetuuksia, sekä hakijan osoitteiden lukumäärän ja varojen yhteenlaskun summan. Mallissa pyrittiin tarkoituksella välttämään kiellettyjen syrjintäperusteiden ja sijaismuuttujien käyttöä.

Tekijöiden mukaan mallin koulutus sisälsi tietoja 3 400 aiemmasta tutkinnasta. Tämä johti historiallisten vinoumien riskiin. Jos tapauksia käsitelleet henkilöt olivat esimerkiksi historiallisesti tehneet enemmän virheitä tietyn etnisen ryhmän tapauksissa, malli saattoi virheellisesti oppia ennustamaan, että tämä ryhmä syyllistyi petokseen muita useammin.

Amsterdamin viranomaiset käyttivät oikeudenmukaisuuden määritelmää, joka perustui virheellisesti määrättyjen tutkimusten taakan tasaiseen jakautumiseen eri väestöryhmien kesken. Myös käytetty kuulemisprosessi oli kattava. Kaikki sidosryhmät Amsterdamin tietosuojaviranomaisesta ulkopuolisiin konsulttiyrityksiin antoivat hankkeelle hyväksyntänsä. Ainoastaan henkilöitä, joihin vaikutukset suoraan kohdistuisivat (eli sosiaaliturvaetuuksien saajia), edustanut ryhmä ei hyväksynyt hanketta.

Järjestelmä siirtyi kuitenkin testausvaiheeseen. Alkuperäinen malli merkitsi virheellisesti tutkittaviksi kaksi kertaa todennäköisemmin muita kuin alankomaalaisia hakijoita ja lähes kaksi kertaa todennäköisemmin muun kuin länsimaisen taustan omaavia hakijoita. Myös miehet merkittiin virheellisesti tutkittaviksi 14 % todennäköisemmin kuin muut hakijat.

Amsterdamin kaupunki testasi myös tapauksia käsitelleiltä ihmisiltä kerättyjä tietoja. Tässä prosessissa havaittiin, että ihmiset merkitsivät todennäköisemmin virheellisesti tutkittaviksi sekä alankomaalaisia että naisia.

Vinoumien vuoksi tiimi yritti korjata ongelman käyttämällä koulutusdatan uudelleenpainotusta. Tämä tarkoitti sitä, että muun kuin länsimaisen taustan omaaville hakijoille, joiden katsottiin tehneen merkityksellisiä virheitä hakemuksissaan, annettiin vähemmän painoarvoa datassa ja vastaaville länsimaisen taustan omaaville enemmän. Kun mallin uudelleenpainotus oli tehty, alankomaalaiset ja muut hakijat merkittiin yhtä todennäköisesti virheellisesti tutkittaviksi.

Ongelmana datan uudelleenpainottamisessa oli, ettei se voinut taata oikeudenmukaisuutta intersektionaalisissa tapauksissa, vaikka se saattoikin vähentää maahanmuuttajataustaisiin henkilöihin liittyviä oikeudenmukaisuusvaikutuksia.

Järjestelmä otettiin kuitenkin rajoitetusti käyttöön todellisilla hakijoilla. Sen suorituskykyä oli tarkoitus mitata kahdella keskeisellä kriteerillä: i) pystyisikö se käsittelemään hakijoita ilman vinoumia ja ii) pystyisikö se havaitsemaan sosiaaliturvapatokset paremmin ja oikeudenmukaisemmin kuin tapauksia käsittelevät ihmiset.

Sen sijaan, että järjestelmä olisi merkinnyt tutkittaviksi vähemmän hakijoita, se merkitsi niitä enemmän. Se ei myöskään ollut ihmisiä parempi tunnistamaan tapauksia, jotka vaativat lisätarkastelua. Lisäksi uudelleenpainotuksesta huolimatta järjestelmä merkitsi nyt virheellisesti tutkittaviksi sekä alankomaalaisia henkilöitä että naisia. Myös lapsiperheellisiä sosiaaliturvaetuuksien hakijoita merkittiin todennäköisemmin tutkittaviksi.

Lopulta projektia ei jatkettu.

Edellä on yhteenveto artikkelista "Inside Amsterdam's high-stakes experiment to create fair welfare AI", 11. kesäkuuta 2025, MIT Technology Review, Lighthouse Reports ja Trouw EG, Geiger G. ja Braun JC. Lisätietoja: katso Lighthouse Reports, 2025.

3.7. Arviointi siitä, onko näyttö riittävää tukemaan tekoäly- tai algoritmijärjestelmään liittyvää *prima facie*-syrjintätapausta

- ▶ Tarkista kaikki tiedot ja vastaukset vaiheessa 3 esitettyihin kysymyksiin ja pohdi näiden perusteella, onko *prima facie*-syrjintätapausta osoitettu. Käytä syrjinnän indikaattoreita ohjeena.
- ▶ Tässä vaiheessa oletetaan, ettei *prima facie*-tapausta tukeville tosiseikoille ole riittävää selitystä (sellainen voi olla, mutta tällä on merkitystä vasta vastaajan puolustuksen arvioinnissa (katso jäljempää kohta 3.8)).
- ▶ Vastaavasti, jos näyttöön tai järjestelmän avoimuuteen liittyviä puutteita on, tämän ei tule estää tapauksen mahdollista käsittelyä oikeudessa tai jatkamista tässä vaiheessa. On muistettava, että **vaiheessa 1** todettiin, että vaateiden

varhainen poistaminen tiedon epätasapainon vuoksi on todennäköisesti epä-tarkoituksenmukaista: katso kohta [1.4 Manjang v. Uber Eats UK Ltd ym. \(2021\)](#).

Yhtä tai useita seuraavista on ehkä pohdittava.

- ▶ Kuka uhri on ja mitä kiellettyjä syrjintäperusteita on käytetty?
- ▶ Kuka on asianmukainen verrokki? Miksi tämä verrokki on valittu?
- ▶ Onko välillistä tai välitöntä syrjintää tapahtunut?
- ▶ Onko kumulatiivista tai intersektionaalista syrjintää tapahtunut?
- ▶ Onko sijaismuuttujaan liittyvää syrjintää havaittu?
- ▶ Miksi syrjintää on tapahtunut (syy-yhteys)? Voidaan tarkastella esimerkiksi, onko syrjintää tapahtunut järjestelmän tavoitteen, kehityksen tai käytetyn datan tai sen vuoksi, että käyttöönottaja käyttää järjestelmää muuhun kuin sen käyttötarkoitukseen tai käyttää järjestelmää virheellisesti.

Jos kyseessä on välillinen syrjintä, myös seuraavia kysymyksiä on pohdittava:

- ▶ Mikä tapaukseen liittyvä neutraali sääntö, peruste tai käytäntö on?
- ▶ Miten säännön, perusteen tai käytännön vaikutukset ovat merkittävästi muita negatiivisempia suojatulla ryhmällä?
- ▶ Onko kantelija näyttänyt toteen tosiseikkoja, joiden perusteella voidaan tehdä johtopäätöksiä siitä, että häntä on kohdeltu epäsuotuisammin kiellettyjen syrjintäperusteiden vuoksi?
- ▶ Jos erilainen kohtelu ei liity ”suoraan” kiellettyyn syrjintäperusteeseen, onko niiden välinen yhteys muutoin riittävä? Tämä on erityisen tärkeää sijaismuuttujiin liittyvää syrjintää tarkasteltaessa.
- ▶ Mikä oli syrjinnän konteksti? Voisiko vastaaja hyväksyttävästi perustella, että päätös tehtiin muusta syystä kuin kielletyn syrjinnän perusteella?

Onko kaikki olosuhteet huomioon ottaen osoitettu *prima facie* -syrjintätapaus?

Jos on, jatka kohtaan [3.8](#).

Jos ei ole, pohdi seuraavia kysymyksiä.

- ▶ Onko tapahtunut sellaista dokumentointi-, testaus-, valvonta- tai raportointivelvoitteiden noudattamatta jättämistä, joka voisi selittää syrjinnän tai johtaa näytön puutteisiin?
- ▶ Onko käytettävissä oikeudenkäyntiä edeltäviä menettelyitä, joilla näytön puutteet voitaisiin täyttää?
 - Harkitse todisteiden esittämistä koskevien hakemusten tekemistä avoimuuteen ja oikeussuojan saatavuuteen liittyvien näkökohtien perusteella Euroopan ihmisoikeussopimuksen 13 artiklan (oikeus tehokkaaseen oikeussuojakeinoon kansallisen viranomaisen edessä) ja Euroopan unionin perusoikeuskirjan 47 artiklan (oikeus tehokkaiisiin oikeussuojakeinoihin ja puolueettomaan tuomioistuimeen) nojalla.
 - On huomioitava, että tilanteissa, joissa vastaaja pyrkii vetoamaan liikesalaisuuksiin tai kolmansien osapuolten oikeuksiin, luottamuksellisia menettelyjä voi olla saatavilla markkinavalvontaviranomaisen, tietosuojaviranomaisen tai

tuomioistuinten kautta. Olemassa oleva oikeuskäytäntö viittaa siihen, että taipumus vaatia näiden tietojen saataville asettamista on kasvamassa: katso [Dun & Bradstreet](#) (yleisen tietosuoja-asetuksen kontekstissa):

Jos rekisterinpitäjä katsoo, että näitä tietoja ei voida toimittaa paljastamatta kolmannen osapuolen tietoja tai liikesalaisuuksia, rekisterinpitäjän on toimitettava väitetysti suojatut tiedot toimivaltaiselle valvontaviranomaiselle tai tuomioistuimelle, jonka on punnittava kyseessä olevia oikeuksia ja intressejä määrittääkseen asetuksen 15 artiklan mukaisen rekisteröidyn tiedonsaanti-oikeuden laajuuden. (Katso myös kohta [Luottamuksellisuus](#)).

Katso lisätietoja tilastotietojen toimittamisen merkityksestä syrjinnän *prima facie*-tapauksen osoittamisessa [tilastotietoja koskevasta kohdasta 3.6](#).

Avoimuus

Tuomioistuin voi tehdä päätelmiä merkityksellisten tilasto- tai muiden tietojen toimittamatta jättämisestä. Syrjintää koskevia päätelmiä voidaan tehdä myös tapaukseen liittyvistä tosiasioista ja olosuhteista, kuten vastaajan vastauksista kysymyksiin tai asiaankuuluvien käytännesääntöjen noudattamatta jättämisestä. Jos vastaaja ei anna tietoja, tämä voi käytännössä johtaa siihen, että tuomioistuin olettaa syrjinnän tapahtuneen, koska vastaaja ei ole täyttänyt todistustaakkaa (katso tietojen antaminen oikeudellisen velvoitteen vuoksi kohdasta [3.8](#)).

- ▶ Päätelmiä voidaan usein tehdä kyselyn tai oikeudenkäyntiä edeltävän prosessin tai menettelyn aikaisen tiedonannon kautta saaduista epäselvistä, riittämättömistä tai välttelevistä vastauksista.
- ▶ Päätelmiä voidaan tehdä myös siitä, jos taho kieltäytyy vahvistamasta tiedon olemassaoloa tai kiistää sen.

Pohdittavia kysymyksiä

- ▶ Onko vastaaja laiminlyönyt tietojen antamista niin, että se on johtanut avoimuuden puutteeseen? Vastattiinko esimerkiksi asianmukaisesti yleisen tietosuoja-asetuksen mukaisiin pyyntöihin, tiedonvälityksen vapautta koskeviin pyyntöihin, oikeudenkäyntiä edeltävään viestintään tai EU:n tekoälyasetuksen nojalla tai muulla tavoin tehtyihin pyyntöihin?
- ▶ Voidaanko käytettävissä olevasta näytöstä tehdä päätelmiä? Esimerkkejä tästä ovat tilastot, tapaukseen liittyvät tosiasiat ja tunnettu syrjintä.
- ▶ Voidaanko näytön puutteesta tehdä päätelmiä? Esimerkkejä tästä ovat tilanteet, joissa ei saada vastauksia kysymyksiin tai ohjeita tai käytännesääntöjä ei noudateta.
- ▶ Kun huomioidaan kaikki tapaukseen liittyvät olosuhteet, antavatko asiaan liittyvät tosiseikat ja olosuhteet, mukaan lukien kysymyksiin tai tietopyyntöihin, kuten DSAR-pyyntöön, vastaamatta jättäminen tai EU:n tekoälyasetuksen 86 artiklan mukaisen selityksen puute, mahdollisuuden syrjintäpäätelmään?

EUT:n esimerkkejä

- ▶ C-109/88, *Handels- og Kontorfunktionærernes Forbund I Danmark v. Danfoss*: ammattiliitto nosti kanteen yrityksen naispuolisten työntekijöiden puolesta, koska he ansaitsivat keskimäärin 7 % vähemmän kuin miespuoliset kollegansa samassa tai vastaavassa työtehtävässä. Tässä tapauksessa EUT totesi, että syrjintäolettaama syntyi palkkajärjestelmän avoimuuden puutteen vuoksi. Todistustaakka siirtyi vastaajalle/työnantajalle, jonka asiana oli osoittaa, ettei sen noudattama palkanmaksukäytäntö ollut syrjivä ja että palkkaerojen syyt olivat objektiivisia.
- ▶ C-415/10 *Galina Meister v. Speech Design Carrier Systems GmbH*: kantaja väitti, että työhönottomenettelyssä esiintyy sukupuoleen, ikään ja etniseen alkupe-
rään perustuvaa syrjintää ja pyysi tuomioistuinta määräämään työnantajan julkistamaan tiedon siitä, oliko prosessin päätteeksi palkattu toinen työnhakija. EUT totesi, että vaikka syrjimättömyysdirektiiveissä ei säädetä oikeudesta saada pääsy tällaisiin tietoihin, vastaajan kieltäytyminen antamasta kantajalle pääsyä minkäänlaisiin tietoihin voi olla yksi niistä tekijöistä, jotka voidaan ottaa huomioon määritettäessä tosiseikkoja, joiden perusteella voidaan olettaa välittömän tai välillisen syrjinnän tapahtuneen.

Esimerkkejä avoimuuden puutteen seurauksista kansallisissa oikeuskäytännöissä

▶ Alankomaiden asia NL24.38560 (2025) (välituomio)

Tuomioistuin päätti omasta aloitteestaan tutkia viisumialgoritmin olemassa-
oloa ja ohjeisti asianomaista ministeriä

- antamaan päätöksenteon kannalta merkityksellisiä tietoja
- tekemään HRIA-arvioinnin

päätöksenteon avoimuuden ja Euroopan ihmisoikeussopimuksen 13 artiklan ja EU:n perusoikeuskirjan 47 artiklan mukaisen tehokasta oikeussuojakeinoa koskevan oikeuden perusteella.

▶ Yhdistyneen kuningaskunnan verotuomioistuimen (Tax Tribunal) (ensimmäinen aste) asia *Elsbury v. The Information Commissioner* (2025) UKFTT 915 (GRC) (2. elokuuta 2025)

Tuomioistuin totesi, että koska HMRC (Yhdistyneen kuningaskunnan His Majesty's Revenue and Customs) ei ole myöntänyt tai kiistänyt pyydettyjen tietojen hallus-
sapitoa, tämä vahvistaa tutkimus- ja kehitystoiminnan verohelpotuksia koskeaan viestintään perustuvaa väitettä siitä, että HMRC:n henkilöstö saattaa käyttää hakemusten käsittelyssä luvatta tekoälyä. Tämä heikentää veronmaksajien luot-
tamusta hakemusten käsittelyyn ja vaikuttaa negatiivisesti yritysten haluun hakea oikeutettuja helpotuksia, mikä estää tutkimus- ja kehitystoiminnan verohelpotusten tavoitteita täyttymästä.

▶ *Filcams Cgil Bologna ym. v. Deliveroo Italia S.R.* (2020):

Bolognan tuomioistuin totesi, ettei yritys ollut täyttänyt todistustaakkaa, koska se ei ollut osoittanut eikä selittänyt algoritmin toimintaa käytännössä

eikä toimittanut näyttöä sen todellisesta toiminnasta. Yritys ei selventänyt, mitä kriteerejä kuljettajien tilastojen määrittämiseen käytettiin, eikä näitä kriteerejä kerrottu alustalla, jossa viitattiin vain yleisesti ”luotettavuuteen” ja ”osallistumiseen” tulevien työmahdollisuuksien indikaattoreina. Lisätietoja tästä tapauksesta: katso [Purificato \(2021\)](#).

3.8. Voiko vastaaja osoittaa, ettei erilainen kohtelu ole syrjivää?

Käytännössä on todennäköisesti tarkasteltava samaa näyttöä ja pohdittava samoja kysymyksiä kuin edellä (3.1–3.8). On kuitenkin mahdollista, että tässä vaiheessa on saatu tarkasteltavaa lisänäyttöä tai vastaajan selitys näytöstä tai järjestelmästä on yksityiskohtaisempi. Tämä edellyttää alkuperäisen aineiston ja aiemmin tehdyn analyysin tarkistamista sen varmistamiseksi, että niitä voidaan yhä soveltaa uusien tietojen valossa.

Kun syrjintää väittävä henkilö on osoittanut *prima facie* -syrjintätapauksen, todistustaakka siirtyy vastaajalle, jonka on osoitettava, ettei erilainen kohtelu ole syrjivää. Tämä voidaan tehdä seuraavin tavoin:

- ▶ Osoitetaan, ettei kohtelu tosiasiallisesti ole erilaista, koska esimerkiksi verrokki on valittu väärin, päätöksen perusteena ei ole ollut kielletty syrjintäperuste tai tapauksen tosiseikat ja olosuhteet poikkeavat verrokista.
- ▶ Todistetaan, ettei kielletyn syrjintäperusteen ja erilaisen kohtelun välillä ollut syy-yhteyttä.
- ▶ Osoitetaan, että erilainen kohtelu voidaan perustella jollakin unionin lainsäädännössä luetelluista poikkeuksista (kuten todellista työhön liittyvää vaatimusta koskevilla tapauksilla), vaikka kyseessä on kielletty syrjintäperuste.
- ▶ Todistetaan, että hyväksytty toimenpide, laki tai käytäntö on asianmukainen ja välttämätön asiaankuuluvan oikeutetun tavoitteen saavuttamiseksi ja etteivät aiheutuneet haitat ole suhteettomia tavoiteltuihin tavoitteisiin nähden (kohtuullinen ja objektiivinen peruste) Euroopan ihmisoikeussopimuksen mukaisesti välillisen ja välittömän syrjinnän osalta sekä EU:n lainsäädännön mukaisesti välillisen syrjinnän tapauksissa.

Jos mitään näistä ei voida näyttää toteen, vastaaja on vastuussa syrjinnästä.

Näin ollen algoritmi- tai tekoälyjärjestelmien konteksteissa vastaajan on annettava asianmukaiset tiedot järjestelmästä, kun *prima facie* -tapaus on osoitettu. Näillä tiedoilla voidaan pyrkiä osoittamaan, että tehdyt valinnat olivat objektiivisuuden ja syrjimättömyyden vaatimusten mukaisia. Katso lisätietoja tilastotietojen toimittamisen merkityksestä todistustaakan kumoamisessa kohdan [3.6 tilastotietoja koskevasta lähestymistavasta](#).

Taulukko 7. Syrjimättömyysdirektiivit ja todistustaakan siirtyminen sekä esimerkkejä EUT:n päättelystä, kun näyttöä ei ole annettu

Direktiivi	Johdanto- osan kappaleet / artiklat	Kielletyt syrjintäperusteet	Soveltamisala	Esimerkkitapaus, joka kuvaa EUT:n päättelyä, kun vastaaja ei ole antanut asianmukaisia tai tarvittavia tietoja ja/tai täyttänyt muita avoimuusvaatimuksia
2000/43/EY (rodusta tai etnisestä alkuperästä riippuma- tonta yhden- vertaista kohtelua koskeva direktiivi)	Johdanto- osan kappaleet 15 ja 21 8 artikla	Rotu ja etninen alkuperä – ei kansalaisuus, eikä rajoita kolman- sien maiden kansalaisten ja kansalaisuudetto- mien henkilöiden oikeudelliseen ase- maan perustuvaa kohtelua	Työllistäminen, ammattillinen koulutus, sosiaaliturva, yleissivistävä koulutus, tavarat ja palvelut, mukaan lukien asuminen	Meister C-415/10: kieltäytyminen tietojen (esimerkiksi rekrytointikriteerien) antamisesta voi johtaa syrjintäpäätelmään
Direktiivi 2000/78/EY	Johdanto- osan kappale 31 10 artikla	Uskonto tai vakau- mus, vammaisuus, ikä, seksuaalinen suuntautuminen	Työllistäminen ja ammatti	Kelly C-104/10: ei oikeutta tietoihin, mutta tietojen antamatta jättäminen voi antaa tuomioistuimille mahdollisuuden päättelmiin
Direktiivi 2006/54/ EY (uudel- leenlaadittu miesten ja naisten yhtä- läisiä mah- dollisuuksia koskeva direktiivi)	Johdanto- osan kappale 30 19 artikla	Sukupuoli (mukaan lukien raskaus ja äitiys)	Työllistäminen ja ammatti (mukaan lukien sosiaalitur- vajärjestelmät)	Danfoss C109/88: jos palkkajärjestelmä ei ole avoin, todistustaakka siirtyy työnantajalle Enderby C-127/92: palkkaerojen perusteluja voidaan pyytää objektiivista perustetta koskevaa testiä varten Kenny C-427/11: verrokkien palkkatietoja voidaan vaatia <i>prima facie</i> -tapauksen kumoamiseksi

Direktiivi	Johdanto- osan kappaleet / artiklat	Kielletyt syrjintäperusteet	Soveltamisala	Esimerkkitapaus, joka kuvaa EUT:n päättelyä, kun vastaaja ei ole antanut asianmukaisia tai tarvittavia tietoja ja/tai täyttänyt muita avoimuusvaatimuksia
Direktiivi 2004/113/EY (direktiivi miesten ja naisten yhdenvertaisen kohtelun periaatteen täytäntöönpanosta tavaroiden ja palvelujen saatavuuden ja tarjonnan alalla)	Johdanto- osan kappale 22 9 artikla	Sukupuoli	Tavarat ja palvelut	Test-Achats C-236/09 Katso myös 5 artiklassa kuvattu sukupuolen käyttäminen vakuutuspalveluja ja niihin liittyviä rahoituspalveluja koskevien maksujen ja etuuksien laskennassa
2010/41/EU (direktiivi miesten ja naisten tasa-arvoisen kohtelun periaatteen soveltamisesta itsenäisiin ammatinharjoittajiin)		Sukupuoli	Yrittäjät ja heidän puolisonsa tai kumppaninsa	(Vireillä oleva asia) Loredas C-531/23: poikkeaminen velvollisuudesta kirjata tosiasiallinen työaika
2023/970/EU, palkkauksen läpinäkyvyyttä koskeva direktiivi (saatettava osaksi kansallista lainsäädäntöä kesäkuuhun 2026 mennessä)	5, 6 ja 8–9 artikla		Työllistäminen	Tarjoaa suoran oikeuden avoimuuteen. II luvussa säädetään oikeudesta palkkauksen läpinäkyvyyteen (5 artikla), palkanmuodostus- ja palkkakehityspolitiikasta (6 artikla), oikeudesta esteettömiin tietoihin (8 ja 9 artikla) sekä palkkaerojen raportoinnista (9 ja 10 artikla).

Onko objektiivinen peruste olemassa?

Jotta voidaan osoittaa, ettei erilainen kohtelu ole syrjivää välillisen syrjinnän tapauksessa⁵⁷, vastaaja voi väittää, että käytännölle on objektiivinen peruste. Tässä osiossa

57. Unionin lainsäädännön mukaan perusteita ei yleensä ole saatavilla välittömän syrjinnän tapauksissa, lukuun ottamatta ikää/vammaisuutta ja todellisia työhön liittyviä vaatimuksia koskevia tapauksia.

korostetaan seikkoja, joiden avulla voidaan arvioida vastaajan esittämiä objektiivisia perusteita.

Erilaisen kohtelun oikeuttamiseksi on osoitettava seuraavat seikat:

- ▶ algoritmijärjestelmällä on oikeutettu tavoite
- ▶ algoritmijärjestelmä soveltuu tai on asianmukainen kyseisen tavoitteen saavuttamiseen
- ▶ algoritmijärjestelmä on välttämätön kyseisen tavoitteen saavuttamiseksi
- ▶ algoritmijärjestelmä on oikeasuhteinen, mikä tarkoittaa, että se on tehokas tavoitteen saavuttamisessa, oikeutetun tavoitteen saavuttamiseksi ei ole muita keinoja, jotka johtaisivat pienempään kohtelueroon, ja oikeutettu tavoite on riittävän tärkeä oikeuttaakseen erilaisen kohtelun.

Esimerkki EUT:n asiasta C-167/97 Seymour-Smith

Tilanteissa, joissa laittoman irtisanomisen korvausvaatimukset olivat mahdollisia vasta kahden työvuoden jälkeen ja tilastojen mukaan tämä syrji välillisesti naisia, välillisesti syrjivästä säännöstä, perusteesta tai käytännöstä vastuussa olevan jäsenvaltion oli osoitettava, että säännös oli perustellun sosiaalipoliittisen tavoitteen mukainen, että siihen ei liity sukupuoleen perustuvaa syrjintää ja että se on voinut kohtuudella arvioida, että valituilla keinoilla edistetään tämän tavoitteen toteuttamista. Kyseisessä tapauksessa tuomioistuin totesi, että ”pelkät yleisluonteiset väitteet työllisyyden edistämiseksi tarkoitetun toimenpiteen soveltuvuudesta eivät riitä, jotta voitaisiin katsoa, että riidanalaisen säännöksen tavoitteeseen ei liity sukupuoleen perustuvaa syrjintää, eikä niiden perusteella voida myöskään kohtuudella arvioida, että valituilla keinoilla voitaisiin edistää tämän tavoitteen toteuttamista” (76–77 kohta). Tuomioistuin totesi myös, että tilastojen osalta voi olla aiheellista ottaa huomioon paitsi säädöksen antamispäivänä käytettävissä olleet tilastotiedot, myös sellaiset myöhemmät tilastotiedot, joiden perusteella voidaan selvittää kyseisen säädöksen vaikutusta miespuolisiin ja naispuolisiin työntekijöihin (49 kohta).

Järjestelmän tavoite

Kohtuullisen ja objektiivisen perusteen esittäminen alkaa oikeutetusta tavoitteesta. Tässä voi olla hyödyllistä huomioida, onko vastaaja maininnut eri tavoitteita eri asiakirjoissa. Katso kohta [3.4 Mitä algoritmijärjestelmän on tarkoitus tehdä ja miten se tekee sen?](#)

Erityyppiset tavoitteet on huomioitava:

- ▶ alemman tason tavoitteet (petosten ennustaminen, opiskelijan tietokoneen ääressä olemisen määrittäminen tai lainan takaisinmaksun laiminlyönnin todennäköisyyden ennustaminen)
- ▶ ylemmän tason tavoitteet (julkisten menojen minimointi koskien sellaisten henkilöiden etuuksia, jotka eivät ole oikeutettuja niihin, verkossa tehtävien kokeiden valvonta tai yleisen maksukyvyttömyysasteen minimointi).

Voi olla tarpeen huomioida myös kansallinen oikeudellinen kehys, jonka nojalla algoritmijärjestelmä otettiin käyttöön. Katso *Glukhin v. Venäjä*, hakemusnro 11519/20 (4. heinäkuuta 2023) (jäljempänä).⁵⁸

Sopivuus tai asianmukaisuus

Vastaajan tulee osoittaa, että algoritmijärjestelmä pystyy saavuttamaan sille määritetyn tavoitteen. Tämä tarkoittaa esimerkiksi, että tilanteissa, joissa tavoitteena on päätöksentekoprosessin tehokkuuden parantaminen, vastaajan tulee osoittaa, että algoritmi on lyhentänyt käsittelyaikaa, vähentänyt tarvittavaa kapasiteettia tai muuten lisännyt tehokkuutta. Ennakoivan järjestelmän tapauksessa sopivuuden osoittaminen voi tarkoittaa järjestelmän ennustustarkkuuden osoittamista. On huomioitava, että sopivuusväittämien tulee vastata järjestelmän tavoitetta. Tässä on otettava huomioon sekä laajemmat että ylemmän tason tavoitteet. Järjestelmä voi olla tapaukseen sopimaton, jos se ei täytä yhtä seuraavista tavoitteista:

- ▶ Alemman tason tavoitteet. Esimerkiksi tilanteet, joissa järjestelmä on suunniteltu optimoitumaan johonkin muuhun kuin sen käyttötarkoitukseen. Esimerkki tästä on järjestelmä, joka on optimoitu virheiden ennustamiseen, mutta jota käytetään petosten ennakointiin.
- ▶ Ylemmän tason tavoitteet. Esimerkiksi tilanteet, joissa tavoitteena on vähentää vilpillisiin etuushakemuksiin käytettäviä menoja, mutta algoritmien tuella tehtävät tarkastukset ovat kalliimpia kuin saavutettu säästö, eli algoritmijärjestelmä ei sovellu kyseiseen tavoitteeseen.

Välttämättömyys

- ▶ Tavoitetta ei voida saavuttaa (yhtä tehokkaasti) ilman algoritmia
 - verrattuna tilanteeseen ennen algoritmia
 - verrattuna muihin kuin algoritmisiin lähestymistapoihin.
- ▶ Tavoitetta ei voida saavuttaa (yhtä tehokkaasti) toisella algoritmijärjestelmällä
 - verrattuna algoritmeihin, jotka käyttävät muita syötteitä (esimerkiksi pois-sulkemalla vahvimmat sijaismuuttajat)
 - verrattuna muihin kehityksessä käytettäviin datajoukkoihin (joissa on vähemmän historiallisia eriarvoisuuksia tai inhimillisiä vinoumia).

Esimerkki Euroopan ihmisoikeustuomioistuimen asiasta *Glukhin v. Venäjä*, hakemusnro 11519/20 (4. heinäkuuta 2023)

Euroopan ihmisoikeustuomioistuin käsitteli tapausta, jossa reaaliaikaista kasvontunnistusteknologiaa (LFR) käytettiin mielenosoittajan löytämiseksi ja paikan-tamiseksi Venäjän metrossa, 8 artiklan (oikeus nauttia yksityis- ja perhe-elämän kunnioitusta) ja 10 artiklan (sananvapaus) perusteella. Tuomioistuin tunnusti nyky-aikaisten tieteellisten tutkinta- ja tunnistustekniikoiden merkityksen (85 kohta) ja

58. Katso myös asiasta *Beghal v. Yhdistynyt kuningaskunta* lisätietoja vaatimuksista, joita kansalliselle lainsäädännölle asetetaan, jotta riitautettua toimenpidettä voidaan pitää lain mukaisena.

huomioi käytettyjen toimenpiteiden oikeusperustan puutteet, koska LFR:n käytön sääntely lainsäädännössä on rajoitettua. Tuomioistuin arvioi myös käytettyjen toimenpiteiden tarpeellisuutta demokraattisessa yhteiskunnassa ottaen erityisesti huomioon niiden mahdollisen lamaannuttavan vaikutuksen sananvapauteen ja kokoontumisvapauteen (10 artikla). Tuomioistuin totesi päätöksessään seuraavaa:

90. Kaikkien edellä mainittujen seikkojen perusteella tuomioistuin katsoo, että erittäin tunkeilevan kasvontunnistusteknologian käyttö, kun kantaja käyttää ihmisoikeussopimuksessa turvattua oikeuttaan sananvapauteen, on ristiriidassa niiden oikeusvaltioperiaatteen mukaisten demokraattisen yhteiskunnan ihanteiden ja arvojen kanssa, joita sopimus on tarkoitettu ylläpitämään ja edistämään. Kantajan henkilötietojen käsittelyä kasvontunnistusteknologian avulla hallinnollista rikkomusta koskevassa oikeudenkäynnissä – ensin kantajan tunnistamiseen Telegramissa julkaistujen valokuvien ja videon perusteella ja sitten hänen paikantamiseensa ja pidättämiseensä hänen matkustaessaan Moskovan metrossa – ei voitu pitää demokraattisessa yhteiskunnassa välttämättömänä.

Suhteellisuus

Kaikissa tapauksissa järjestelmän käytöstä johtuvan syrjinnän, jota vastaaja pyrkii perustelemaan, tulee olla suhteellista tavoiteltuun tavoitteeseen nähden. Yleisesti tämä edellyttää, että tuomioistuin vertaa haitan vakavuutta muihin tässä osiossa käsiteltyihin tekijöihin.

Pohdittavia kysymyksiä

- ▶ Voiko vastaaja todistaa, ettei syrjintää ole tapahtunut?
- ▶ Voiko vastaaja osoittaa, ettei häntä tule kohdella kuin syrjintää olisi tapahtunut?
 - Voiko prosessissa mukana oleva ihminen ratkaista riittävällä tavalla mahdollisen järjestelmään jääneen syrjinnän?
 - On huomioitava, että syrjintä voi johtua inhimillisestä virheestä algoritmi-järjestelmän sijaan.
- ▶ Voisiko vastaaja väittää, että on valittu väärä verrokki?
- ▶ Voiko vastaaja osoittaa, ettei kantelija ole verrokkiin verrattuna samankaltaisessa tai vastaavassa tilanteessa?
- ▶ Onko erilaiselle kohtelulle olemassa kestävä vaihtoehtoista selitystä, joka ei liity syrjintään?
- ▶ Mitä toimia on tehty syrjinnän välttämiseksi (kohtuulliset mukautukset)?
- ▶ Voiko vastaaja tarvittaessa osoittaa, ettei erilainen kohtelu perustu kiellettyyn syrjintäperusteeseen vaan muihin objektiivisiin eroihin?
- ▶ Kattavatko syrjimättömyysdirektiivit nimenomaisesti nämä objektiiviset erot?
- ▶ Onko kyseisellä säännöksellä tai käytännöllä oikeutettu tavoite?
- ▶ Katso uudestaan kohdan 3.4 tiedot siitä, mitä tekoälyjärjestelmän on tarkoitus tehdä ja miten se tekee sen – olivatko valitut keinot sopivia?
- ▶ Ovatko tavoitteen saavuttamiseksi käytetyt keinot sopivia, tarpeellisia ja suhteellisia tavoiteltuun tavoitteeseen nähden?



Vaihe 4

Oikeussuojakeinot

Vaiheessa 4 kuvataan yksityiskohtaisesti yhdenvertaisuuselinten käytettävissä olevat oikeussuojakeinot ja toimintatavat. Valtuudet ja toimeksiannot todennäköisesti vaihtelevat merkittävästi jäsenvaltioittain, joten tässä vaiheessa on tarkoitus tarkastella erityisesti yhdenvertaisuuselinten normeja koskevien direktiivien, jotka on saatettava osaksi kansallista lainsäädäntöä 19. kesäkuuta 2026 mennessä, tekoälyasetuksen, yleisen tietosuoja-asetuksen ja muun asiaankuuluvan unionin lainsäädännön välistä suhdetta.

Yleensä on tarpeen harkita useampaa kuin yhtä oikeussuojakeinoja ongelmasta tai tapauksesta riippuen.

Kohdassa 4.1 käsitellään kaikkien algoritmijärjestelmien oikeussuojakeinoja.

Kohdassa 4.2 on lisää oikeussuojakeinoja suuririskisille järjestelmille.

Kohdassa 4.3 esitetään, mitä yhdenvertaisuuselimen tulisi tehdä tapauksessa, jossa järjestelmä tai käyttötapaus aiheuttaa riskin perusoikeuksille, mutta sitä ei ole luokiteltu tekoälyasetuksen mukaan suuririskiseksi järjestelmäksi, mukaan lukien toimenpiteet, joita markkinavalvontaviranomainen voi tehdä ja jotka edellyttäisivät tai voisivat edellyttää yhdenvertaisuuselimen osallistumista.

Kuva 5. Vaihe 4 – Oikeussuojakeinot

VAIHE 4		Oikeussuojakeinot
4.1	Kaikkien algoritmijärjestelmien oikeussuojakeinot	MAHDOLLISET TOIMENPITEET • Yhdenvertaisuuselinten normeja koskevien direktiivien mukaiset korjausvaltuudet • Alkuvaiheen apu • Valituksen tekeminen markkinavalvontaviranomaiselle • Yleisen tietosuoja-asetuksen oikeussuojakeinot • Vaihtoehtoinen riidanratkaisu • Oikeudenkäynti • Yhdenvertaisuustietojen kerääminen ja raportointi
4.2	Ylimääräiset oikeussuojakeinot suuririskisille tekoälyjärjestelmille	MAHDOLLISET TOIMENPITEET • Markkinavalvontaviranomaisen vastaus vakavaan vaaratilanteeseen • Markkinavalvontaviranomaisen tutkinta tuotteen vakavasta riskistä perusoikeuksille • Virheellinen tekoälyjärjestelmän riskiluokitus • Vaatimustenmukaiset järjestelmät, jotka aiheuttavat riskin perusoikeuksille
4.3	Vakava riski perusoikeuksille, mutta tekoälyjärjestelmä ei ole suuririskinen tai kielletty järjestelmä	MAHDOLLISET TOIMENPITEET • Tekoälyasetuksen muutoksen haku • Lisäykset tekoälyasetuksen liitteeseen III

Syrjimättömyysdirektiivien ja yhdenvertaisuuselinten normeja koskevien direktiivien nojalla yhdenvertaisuuselimille annetaan laajat valtuudet toteuttaa toimia syrjinnän ehkäisemiseksi ja yhdenvertaisen kohtelun edistämiseksi. Näihin valtuuksiin kuuluvat tietoisuuden lisääminen (5 artikla), uhrien auttaminen (6 artikla), vaihtoehtoinen riitojenratkaisu (7 artikla), yhdenvertaisen kohtelun periaatteen rikkomista koskevien selvitysten tekeminen (8 artikla), lausuntojen ja päätösten antaminen, mukaan lukien oikeus tosiseikkojen selvittämiseen (9 artikla), ja toimiminen oikeudenkäynneissä, mukaan lukien oikeus esittää huomioita (10 artikla).

Jos algoritmijärjestelmässä on havaittu syrjintää, näiden valtuuksien käyttöä on harkittava, jotta voidaan varmistaa seuraavat:

- ▶ Vastaaja lopettaa tekoälyjärjestelmän käytön syrjivällä tavalla tai, jos tämä ei ole mahdollista, vastaaja lopettaa tekoälyjärjestelmän käytön kokonaan.
- ▶ Algoritmisesta syrjinnästä tiedotetaan asianmukaisesti asianosaisille ryhmille ja elimille.
- ▶ Yksittäisille uhreille tarjotaan neuvontaa ja apua, mukaan lukien vaihtoehtoiseen riidanratkaisuun (ADR) ja oikeudenkäyntimenettelyihin liittyviä neuvoja.
- ▶ Korjaavia toimenpiteitä, kuten koulutuksen, neuvonnan ja tuen tarjoamista, toteutetaan.
- ▶ Algoritmijärjestelmiin liittyvästä syrjinnästä käydään julkista keskustelua. Lisäksi edistetään positiivista erityiskohtelua ja yhdenvertaisuuden valtavirtaistamista julkisten ja yksityisten toimijoiden keskuudessa.
- ▶ Viestintää käydään asiaankuuluvien sidosryhmien, kuten työmarkkina-osapuolten, kanssa, ja hyvien käytäntöjen vaihtoa edistetään.

Tällaisia toimia toteuttaessaan yhdenvertaisuuselimet voivat huomioida erityiset epäedulliset tilanteet, jotka johtuvat intersektionaalisesta syrjinnästä. Tämä tarkoittaa syrjintää, joka perustuu syrjimättömyysdirektiivien mukaisten kiellettyjen syrjintäperusteiden yhdistelmään.

Yhdenvertaisuuselinten on otettava huomioon kullekin kohderyhmälle soveltuvat viestintävälineet ja -muodot. Yhdenvertaisuuselinten on keskityttävä erityisesti ryhmiin, joiden tiedonsaanti voi olla vaikeaa esimerkiksi epävarman taloudellisen tilanteen, iän, vammaisuuden, lukutaidon, kansalaisuuden tai kotipaikka-aseman tai verkkotyökalujen käytettävyyden puutteen vuoksi.

Keskeiset resurssit

- ▶ "Strategic litigation handbook" (Equinet, 2017)
- ▶ "How to use the Artificial Intelligence Act to investigate AI bias and discrimination: a guide for equality bodies" (Mittelstadt, 2024)

4.1. Kaikkien algoritmijärjestelmien oikeussuojakeinot

Vaiheissa 2 ja 3 kuvatun prosessin olisi pitänyt auttaa tunnistamaan, esiintyykö syrjintää ja mikä syrjinnän syy on voinut olla. Yhdenvertaisuuselinten on käytettävä näissä vaiheissa kerättyjä tietoja korjaavien toimien ehdottamiseen ja kiistanalaisten käytäntöjen, algoritmien tai järjestelmien poistoa tai muokkausta koskevan suunnitelman laatimiseen. Yhdenvertaisuuselin on esimerkiksi saattanut todeta, että oikeudenmukaisuusmittareiden valinta oli käyttötapaukseen nähden sopimaton tai ettei data ollut riittävän edustavaa.

Jos yhdenvertaisuuselin katsoo, että syrjinnän riski tai havaittu syrjintä on laitonta, mutta tilanne voidaan korjata, on harkittava toimia, joilla pyritään seuraaviin:

- ▶ Järjestelmän käytön kieltäminen, kunnes syrjintä on poistettu.
- ▶ Kaikki korjaavat toimenpiteet, jotka on toteutettava.

Jos yhdenvertaisuuselin päättää, että syrjinnän riski on laiton eikä sitä voida korjata, on harkittava toimia, joilla voidaan saavuttaa jokin seuraavista tuloksista:

- ▶ Algoritmijärjestelmän käytön kieltäminen kokonaan.
- ▶ Algoritmijärjestelmän käytön kieltäminen tietyllä sektorilla.
- ▶ Algoritmijärjestelmän käytön kieltäminen tietyyn tarkoitukseen.

Tällaisia toimia voidaan toteuttaa siten, että yhdenvertaisuuselimet käyttävät omia valtuuksiaan lausuntojen, suositusten ja konsultointien antamiseen yhdessä markkina-valvontaviranomaisen kanssa joko yleisen tietosuoja-asetuksen tai tekoälyasetuksen nojalla tai tuomioistuinten kautta.

4.1.1. Yhdenvertaisuuselinten korjausvaltuudet

Yhdenvertaisuuselinten on ensin harkittava kansallisen lainsäädännön mukaisten korjausvaltuuksiensa käyttöä, kuten aiemmin on kuvattu. Nämä voivat sisältää kaikki yhdenvertaisuuselinten normeja koskevien direktiivien virallistettavat korjaavat toimenpiteet, kuten lausunnon tai suosituksen antamisen tai kuulemisen tai testauksen vaatimisen, tai vain osan niistä.

Jos yhdenvertaisuuselinten normeja koskevat direktiivit on saatettu osaksi kansallista lainsäädäntöä, yhdenvertaisuuselimillä tulisi olla korjausvaltuuksia. Näitä valtuuksia on kuvattu esimerkiksi 9 artiklassa (sitovan tai ei-sitovan lausunnon antaminen kansallisen kontekstin mukaan) ja 15 artiklassa (kuulemis- ja suositusvaltuudet).

Yhdenvertaisuuselimillä tulee myös olla valtuudet toimittaa ja dokumentoida arviot tapauksesta, mukaan lukien tosiseikkojen selvittäminen ja perusteltu päätelmä syrjinnän olemassaolosta. Algoritmisen syrjinnän tapauksessa tämä voi tapahtua yhteistyössä markkinavalvontaviranomaisen kanssa.

Sekä ei-sitovien lausuntojen että sitovien päätösten on tarvittaessa sisällettävä toimenpiteitä havaitun yhdenvertaisen kohtelun periaatteen rikkomisen korjaamiseksi ja sen ehkäisemiseksi jatkossa. Yhdenvertaisuuselimet saattavat tarvita asiantuntija-apua tiettyjen toimenpiteiden toteuttamisessa, ja jos tarvittavaa asiantuntemusta ei ole, yhdenvertaisuuselimet voivat halutessaan konsultoida markkinavalvontaviranomaista. Ei-sitovien lausuntojen jatkotoimille, kuten palautevelvoitteelle, ja sitovien päätösten täytäntöönpanolle on otettava käyttöön asianmukaiset mekanismit.

Kuulemisia voidaan käyttää ongelmien olemassaolon tunnistamiseen, järjestelmien asianomaisiin henkilöihin tai yhteisöihin kohdistuvien sosiaalisten ja syrjivien vaikutusten testaamiseen sekä näytön keräämiseen.

Yleisesti suositukset ja kuulemiset voidaan suunnata sen varmistamiseen, ettei ongelmia esiinny tulevaisuudessa, esimerkiksi suosittelemalla seuraavia:

- ▶ tietosuoja ja yhdenvertaisuutta koskevat vaikutustenarvioinnit
- ▶ yhteisön kuuleminen ja yhteisöjohtoinen FRIA-arviointi
- ▶ testiympäristöjen käyttö ja tosielämän olosuhteissa tapahtuva testaus.

Lisämateriaaleja

- ▶ Crowley (2023), "Informing the policy agenda: equality bodies making recommendations"

4.1.2. Alkuvaiheen avun tarjoaminen uhreille

Yhdenvertaisuuselinten normeja koskevien direktiivien 6 artiklassa säädetään, että yhdenvertaisuuselinten on annettava alkuvaiheen apua uhreille tiedottamalla heille seuraavista:

- ▶ Syrjintään ja algoritmijärjestelmiin liittyvä oikeudellinen kehys, mukaan lukien uhrien erityistilanteeseen kohdennettu neuvonta.

- Yhdenvertaisuuselimen tarjoamat palvelut ja niihin liittyvät menettelylliset näkökohdat.
- Käytettävissä olevat oikeussuojakeinot, mukaan lukien mahdollisuus saattaa asia tuomioistuimen käsiteltäväksi, esimerkiksi
 - syrjinnän vastaisen lainsäädännön nojalla
 - tekoälyasetuksen nojalla – katso esimerkiksi oikeus tehdä valitus markkina-
valvontaviranomaiselle (tekoälyasetus, 85 artikla) ja [oikeus selitykseen](#) (teko-
älyasetus, 86 artikla)
 - tietosuojalainsäädännön nojalla – esimerkiksi valituksen tekeminen tietosuoja-
viranomaiselle (yleinen tietosuoja-asetus, 77 artikla) ja rekisteröidyn oikeus
tehdä [pyyntö saada pääsy tietoihin](#) (yleinen tietosuoja-asetus, 15 artikla).⁵⁹
- Sovellettavat luottamuksellisuutta koskevat säännöt ja henkilötietojen suoja (esimerkiksi yhdenvertaisuuselinten tietosuojakäytännöt ja tarvittaessa mah-
dolliset ristiriidat näytön, jonka yhdenvertaisuuselin on saanut hoitaessaan
tiettyä osaa toimeksiannostaan, ja sen, että elin voi toimittaa kyseisen näytön
yksityishenkilön käytettäväksi oikeudessa, välillä).
- Mahdollisuus saada psykologista tai muunlaista tukea muilta elimiltä tai
organisaatioilta.

Yhdenvertaisuuselinten on ilmoitettava kantelijalle kohtuullisessa ajassa, päätetäänkö valituksen käsittely vai onko sitä syytä jatkaa.

Alkuvaiheen avun antamisen jälkeen yksittäisen kantelijan käytettävissä olevat oikeussuojakeinot voivat sisältää seuraavia:

- [Valituksen tekeminen markkina-
valvontaviranomaiselle](#) (tekoälyasetus, 85 artikla).
- [Vaihtoehtoisten riitojenratkaisumenetelmien harkinta](#).
- [Syrjintätapausten vieminen kansallisen tuomioistuimen käsiteltäväksi](#).

Kaikki päätökset parhaasta toimintatavasta on tehtävä yhdessä asianomaisen henkilön tai ryhmän kanssa. Jos yhdenvertaisuuselimellä ei ole valmiuksia, päte-
vyyttä (esim. tietosuojaa koskevien vaatimusten esittämiseen) tai resursseja ajaa
asianomaisen henkilön pyytämää toimenpidettä, asia tulee siirtää toiselle toimi-
valtaiselle oikeudellisia asioita käsittelevälle palveluntarjoajalle.

4.1.3. Oikeushenkilön tai luonnollisen henkilön avustaminen valituksen tekemisessä markkina- valvontaviranomaiselle

Jos vaiheessa 3 tehdyssä tutkinnassa on havaittu tekoälyasetuksen vaatimusten
noudattamiseen liittyviä ongelmia, oikeushenkilöllä tai luonnollisella henkilöllä on
oikeus tehdä valitus markkina-
valvontaviranomaiselle (EU:n tekoälyasetus, 85 artikla).
Tämä tarkoittaa, että oikeus ulottuu oikeushenkilöllisyyden omaaviin tahoihin, kuten

59. Oikeus selitykseen on olemassa sekä yleisen tietosuoja-asetuksen (15 ja 22 artikla) että tekoäly-
asetuksen (86 artiklan) nojalla. [Vaiheessa 2](#) ja liitteissä [A](#) ja [B](#) annetaan lisäselityksiä ja malleja
pyynnön tekemistä varten.

yhtiöihin tai organisaatioihin. Yhdenvertaisuuselin voi auttaa valituksen tekijää vaiheessa 3 tunnistetulla näytöllä.

Tämä oikeus ei rajoita EU:n ja kansallisen lainsäädännön mukaisia olemassa olevia oikeuksia ja oikeussuojakeinoja, vaan täydentää niitä (johdanto-osan kappale 170). Se ei rajoitu suuririskisiin tekoälyjärjestelmiin.

Kaikki tällaiset valitukset otetaan ”huomioon” markkinavalvontatoimien suorittamisessa markkinavalvonnasta ja tuotteiden vaatimustenmukaisuudesta annetun asetuksen (EU) 2019/1020 mukaisesti. Määräajat vahvistetaan todennäköisesti kansallisessa lainsäädännössä (katso asetus (EU) 2019/1020, 11 artikla).

Kaikki tekoälyjärjestelmät, jotka eivät ole suuririskisiä, voivat kuulua yleisen tuoteturvallisuusasetuksen (EU) 2023/988 ja markkinavalvonnasta annetun asetuksen (EU) 2019/1020 soveltamisalaan.

On tärkeää, että tuotteisiin liittyvät tekoälyjärjestelmät, jotka eivät ole tämän asetuksen mukaisesti suuririskisiä ja joiden ei näin ollen tarvitse täyttää suuririskisille tekoälyjärjestelmille vahvistettuja vaatimuksia, ovat kuitenkin turvallisia, kun ne saatetaan markkinoille tai otetaan käyttöön. Tämän tavoitteen saavuttamiseksi Euroopan parlamentin ja neuvoston asetusta (EU) 2023/988 (53) sovellettaisiin turvaverkkona. (Tekoälyasetus, johdanto-osan kappale 166)

Oikeus tehdä valitus ei rajoita muita hallinnollisia tai oikeudellisia oikeussuojakeinoja, ja siksi se on vaihe, joka olisi toteutettava yhdessä kaikkien muiden sovellettavien oikeussuojakeinojen kanssa. Yksinään tämä ei todennäköisesti ole paras oikeussuojakeino yksilölle. Tämä johtuu erityisesti vahingonkorvausta koskevan säännöksen puutteesta. Se on kuitenkin tärkeä rinnakkaistoimenpide, ja koska markkinavalvontaviranomaisella on erittäin laajat valtuudet ja oikeussuojakeinot asetuksen (EU) 2019/1020 nojalla, valituksen tekoa kannattaa harkita asianmukaisessa tapauksessa. Markkinavalvontaviranomaiselle tehdyn valituksen tulisi johtaa tämän viranomaisen suorittamaan jäsennellympään tutkintaan ja laajempiin oikeussuojakeinoihin, jotka voivat vaikuttaa kattavampaan kohderyhmään kuin yksittäinen syrjintäkanne. Markkinavalvontaviranomaisella on laajat valtuudet sekä tekoälyasetuksen että asetuksen (EU) 2019/1020 nojalla, ja se voi tehdä asiakirjatarkastusten lisäksi myös fyysisiä ja laboratoriotarkastuksia (katso kohta 4.2).

Jos valitus hyväksytään, markkinavalvontaviranomainen voi vaatia talouden toimijaa ryhtymään korjaaviin toimenpiteisiin, jos nämä toimenpiteet ovat asianmukaisia ja oikeasuhteisia. Jos korjaavia toimenpiteitä ei tehdä tai ne epäonnistuvat, markkinavalvontaviranomainen voi kieltää tai rajoittaa tuotteen saattamista markkinoille tai vaatia tuotteen poistamista markkinoilta tai palautusmenettelyjä. Jos tuotteet aiheuttavat riskin, jonka vaikutus ulottuu markkinavalvontaviranomaisen oman jäsenvaltion ulkopuolelle, markkinavalvontaviranomaisen on välittömästi ilmoitettava toteutetuista toimenpiteistä Euroopan komissiolle ja muille EU:n jäsenvaltioille. Asetuksessa (EU) 2019/1020 on kuvattu kattavat säännökset koskien rajat ylittävää yhteistyötä valvontaviranomaisten kesken.

4.1.4. Rekisteröidyn oikeussuojakeinot yleisen tietosuoja-asetuksen tai kansallisten tietosuojajärjestelmien nojalla

Yleisen tietosuoja-asetuksen nojalla rekisteröidyllä (luonnollisella henkilöllä) on selityksen saantia koskevan oikeuden lisäksi seuraavat rekisteröidyn oikeudet:

- ▶ Oikeus vastustaa henkilötietojen automaattista käsittelyä (21 artikla).
- ▶ Oikeus vaatia, että rekisterinpitäjä oikaisee ilman aiheutonta viivytystä rekisteröityä koskevat epätarkat ja virheelliset henkilötiedot, ja oikeus saada puutteelliset henkilötiedot täydennettyä muun muassa toimittamalla lisäselvitys (16 artikla).
- ▶ Oikeus saada rekisterinpitäjä poistamaan rekisteröityä koskevat henkilötiedot ilman aiheutonta viivytystä, jos jokin seuraavista perusteista täyttyy (17 artikla):
 - rekisteröity peruuttaa suostumuksen, eikä käsittelyyn ole muuta laillista perustetta
 - rekisteröity vastustaa käsittelyä 21 artiklan 1 kohdan nojalla
 - henkilötietoja on käsitelty lainvastaisesti.

Nämä voivat olla merkityksellisiä silloin, kun algoritmijärjestelmä on johtanut syrjintään. Toteutetut toimenpiteet voivat edellyttää tietosuoja-asiantuntijan tai -viranomaisen osallistumista.

Jos jäsenvaltiot ovat ottaneet käyttöön tietosuojajärjestelmiä yleisen tietosuoja-asetuksen lisäksi tai jos yleistä tietosuoja-asetusta ei sovelleta kyseiseen valtioon, on tärkeää ottaa huomioon mahdolliset kansalliset tietosuojalait.

4.1.5. Vaihtoehtoisen riidanratkaisun tarjoaminen lainsäädännön mukaisesti

Yhdenvertaisuuselinten normeja koskevien direktiivien 7 artiklan mukaan yhdenvertaisuuselinten on voitava tarjota osapuolille mahdollisuus vaihtoehtoiseen riidanratkaisuun. Kyseistä menettelyä voi johtaa yhdenvertaisuuselin itse tai muu toimivaltainen yksikkö kansallisen lainsäädännön ja käytännön mukaisesti, jolloin yhdenvertaisuuselin voi esittää kyseiselle yksikölle huomioita. Tällainen vaihtoehtoinen riidanratkaisu voidaan toteuttaa eri muodoissa, kuten välitys- tai sovittelumenettelynä, kansallisen lainsäädännön ja käytännön mukaisesti. Se, että riitaa ei ole saatu ratkaistua, ei estä osapuolia käyttämästä oikeuttaan saattaa asia tuomioistuimen käsiteltäväksi. Jäsenvaltioiden on varmistettava, että sovellettava vanhentumisaika on riittävän pitkä, esimerkiksi keskeyttämällä vanhentumisajan kuluminen osapuolten osallistuessa vaihtoehtoiseen riidanratkaisumenettelyyn, jotta riidan osapuolille voidaan taata mahdollisuus saattaa asiansa tuomioistuimen käsiteltäväksi.

4.1.6. Syrjimättömyyttä ja ihmisoikeuksia koskevat oikeudenkäynnit

Yhdenvertaisuuselimillä tulee olla oikeus toimia oikeudenkäynneissä siviili- ja hallinto-oikeudellisissa asioissa, mukaan lukien oikeus esittää syrjimättömyysdirektiiveihin liittyviä huomioita tuomioistuimelle kansallisen lainsäädännön ja käytännön mukaisesti. Tämä vaihtelee jäsenvaltioittain.

Yhdenvertaisuuselinten normeja koskevien direktiivien 10 artiklan mukaan yhdenvertaisuuselimen oikeus toimia oikeudenkäynneissä sisältää myös vähintään yhden seuraavista:

- ▶ oikeus panna vireille oikeudenkäyntimenettely yhden tai useamman uhrin puolesta
- ▶ oikeus osallistua oikeudenkäyntimenettelyyn yhden tai useamman uhrin tukena
- ▶ oikeus käynnistää oikeudenkäyntimenettelyjä omissa nimissään yleisen edun puolustamiseksi.

Tämä sisältää myös yhdenvertaisuuselimen 9 artiklan mukaisten sitovien päätösten täytäntöönpanon (katso jäljempää). Kun harkitaan strategisen eli yhteiskunnalliseen muutokseen pyrkivän oikeudenkäyntimenettelyn aloittamista, yhdenvertaisuuselinten on suositeltavaa tutustua asiaa koskevaan Equinetin käsikirjaan ”Strategic litigation handbook” (Equinet, 2017: 17).

Tekoöljyjärjestelmiin voi todennäköisesti liittyä merkittäviä mahdollisuuksia strategiisiin oikeudenkäynteihin, koska sekä teknologia että lainsäädäntö ovat suhteellisen uusia. Strateginen oikeudenkäynti ei välttämättä ole paras lähestymistapa joka tilanteessa. Esimerkiksi tuloksen saaminen voi kestää liian kauan asianomaisen henkilön kannalta, onnistuneen kanteen tekemiseen tarvittavat tiedot voivat puuttua ja testaus- ja neuvotteluprosessien aloittaminen voi olla tehokkaampaa. Näitä ja useita muita tekijöitä on harkittava tapauskohtaisesti.

4.1.7. Tiedonkeruu, pääsy yhdenvertaisuustietoihin ja raportointi

Pääsy yhdenvertaisuustietoihin on tärkeää, kun halutaan osoittaa tekoällyn ja automaattisen päätöksenteon järjestelmien aiheuttama syrjintä. Yhdenvertaisuuselimet voivat hyödyntää näitä uusia valtuuksia ja kerätä tietoja algoritmisen syrjinnän esiintymisestä laajemmin. Tässä arviointimenetelmässä on annettu suosituksia muistiin kirjattavista tiedoista, jotka voivat auttaa yhdenvertaisuuselimä algoritmijärjestelmiin liittyvien yhdenvertaisuustietojen keräämisessä. Kerätyistä tilastoista voi olla hyötyä esimerkiksi silloin, kun tuomioistuimessa osoitetaan *prima facie* -syrjintätapaus. Jos yhdenvertaisuuselin huomaa, että tiettyyn sektoriin tai algoritmijärjestelmän käyttötapaukseen liittyen pyydetään usein apua, voidaan tarvita lisätutkimuksia tai tämän kohteen priorisointia.

Yhdenvertaisuustietojen kerääminen on monissa maissa riittämätöntä esimerkiksi sen vuoksi, että sitä on usein rajoitettu lainsäädännöllä. Yhdenvertaisuuselimet eivät usein pysty käsittelemään arkaluonteisia henkilötietoja vinoumien mittaus- ja lieventämistarkoituksiin yleisen tietosuoja-asetuksen 9 artiklan 2 kohdan g alakohdan ja tekoälyasetuksen 10 artiklan 5 kohdan mukaan. Yhdenvertaisuuselimet voivat kuitenkin suositella tiedonkeruusääntöjen ja -käytäntöjen uudistamista, jotta algoritmista syrjintää koskevaa tietämystä voitaisiin parantaa (katso Euroopan neuvosto, 2025b).

Rakenteellisten ongelmien tunnistaminen ja niistä raportointi vuosittain

Tiedonkeruun tulee auttaa yhdenvertaisuuselinä tunnistamaan algoritmijärjestelmien rakenteellista eriarvoisuutta ja raportoimaan siitä. Jos yhdenvertaisuuselin käyttää tietokantaa tapausten ja annettujen neuvojen tietojen tallentamiseen, siihen tulisi lisätä uusi tapausluokka, jolla yhdenvertaisuuselin voi seurata tekoälyjärjestelmien todistettua tai epäiltyä syrjivää käyttöä. Pidemmällä aikavälillä tätä arviointimenetelmää voidaan käyttää tietokantaan sisällytettävien tarkkojen alojen suunnitteluun, jotta tällaisia tapauksia koskevaa dataa voidaan kerätä ja analysoida.

Inspiraatiota varten arviointimenetelmän vaiheessa 3 on kunkin osion lopussa kuvattu indikaattoreita siitä, minkä tyyppistä tietoa tietokantaan voitaisiin tallentaa, ja [liitteessä K](#) on lomake-ehdotus tietojen kirjaamiseen.

Rakenteellisiin ongelmiin voivat sisältyä esimerkiksi seuraavat:

- ▶ Näyttö tietyntyyppisestä algoritmijärjestelmästä tai -teknologiasta johtuvasta syrjinnästä.
- ▶ Näyttö syrjinnästä, jota aiheutuu algoritmijärjestelmien käytössä tietyillä sektoreilla.
- ▶ Näyttö epäilystä syrjinnästä algoritmijärjestelmän käyttösektorilla tai -tyypissä.
- ▶ Näyttö siitä, että algoritmijärjestelmien käyttöönotto eri sektoreilla vaikuttaa suhteettomasti tiettyihin ryhmiin.
- ▶ Tekoälyjärjestelmät tai käyttötapaukset, joiden tulisi kuulua seuraaviin mutta jotka eivät kuulu niihin tällä hetkellä:
 - kielletty
 - luokiteltu suuririskiseksi
 - yleiskäyttöiset mallit, joihin liittyy systeemisiiä riskejä
 - johonkin näistä luokista sisältyvä järjestelmä, joka kuitenkin aiheuttaa hyväksymättömän syrjintäriskin
- ▶ järjestelmälliset laiminlyönnot tekoälyasetuksen syrjintään liittyvien osien noudattamisessa, kuten riittämätön vinoumien tai oikeudenmukaisuuden testaus ja riittämättömät datankeruukäytännöt.

4.2. Lisää oikeussuojakeinoja suuririskisille tekoälyjärjestelmille

4.2.1. Markkinaevalvontaviranomaisen ja yhdenvertaisuuselimen yhdessä toteuttamat toimet

Tekoälyasetuksen 77 artiklan mukaisten yhdenvertaisuuselimille annettujen valtuuksien lisäksi markkinaevalvontaviranomaisilla on velvollisuus tehdä yhteistyötä yhdenvertaisuuselimen kanssa 77 artiklan mukaisena viranomaisena, kun käsitellään vakavia vaaratilanteita (tekoälyasetus, 73 artikla), kun tekoälyjärjestelmät aiheuttavat riskejä (tekoälyasetus, 79 artikla) ja kun tutkitaan vaatimustenmukaista järjestelmää, joka aiheuttaa riskin perusoikeuksille (tekoälyasetus, 82 artikla). Markkinaevalvontaviranomaisen voi olla tarpeen kuulla yhdenvertaisuuselinä

myös tilanteissa, joissa epäillään, että tarjoaja on virheellisesti luokitellut tekoölyjärjestelmän ei-suuririskiseksi (tekoölyasetus, 80 artikla). Näitä prosesseja käsitellään tarkemmin jäljempänä.

Yhdenvertaisuuselin voi tarvittaessa jakaa järjestelmään liittyvät tiedot ja tämän arviointimenetelmän avulla saadun näytön markkinaevalvontaviranomaiselle vakavasta vaaratilanteesta ilmoittamisen, testauksen suorittamisen, arvioinnin tekemisen tai tekoölyasetuksen tai markkinaevalvonnasta annetun asetuksen mukaisten valtuuksien käyttämistä varten vaatiakseen korjaavia toimenpiteitä tai tuotteen peruuttamista tai poistamista markkinoilta tai muita toimia.

Markkinaevalvontaviranomaisen vastaus ilmoitukseen vakavasta vaaratilanteesta (tekoölyasetus, 73 artikla)

Markkinaevalvontaviranomaisella on asetuksen (EU) 2019/1020 nojalla merkittäviä valtuuksia ja vastuuta, jotka liittyvät vakavien vaaratilanteiden käsittelyyn.

Markkinaevalvontaviranomaisen on ilmoitettava 77 artiklan mukaiselle elimelle, jos tarjoaja ilmoittaa sille vakavasta vaaratilanteesta (tekoölyasetus, 73 artiklan 3 kohta). Vakavalla vaaratilanteella tarkoitetaan vaaratilannetta tai tekoölyjärjestelmän toimintahäiriötä, joka suoraan tai välillisesti johtaa perusoikeuksien suojaamiseen tarkoitettujen unionin oikeuden mukaisten velvoitteiden, mukaan lukien syrjimättömyysoikeuden, rikkomiseen (tekoölyasetus, 3 artiklan 49 kohdan c alakohta). Komissio antaa tähän liittyviä ohjeita aikanaan.

Tällaisissa tapauksissa on pohdittava seuraavia kysymyksiä:

- ▶ Sisälsikö vakava vaaratilanne syrjinnän riskin?
 - Jos sisälsi, tulisiko asianomaisilla olla oikeus oikeussuojakeinoihin?
 - Jos tulisi, pohdi, mikä voisi olla tehokkain oikeussuojakeino (esimerkiksi vaihtoehtoinen riidanratkaisu, oikeudenkäynti tai selvitys).
 - Jos asianomaisilla henkilöillä on oikeus rahalliseen korvaukseen, on varmistettava, ettei valittu oikeussuojakeino estä tätä. On myös muistettava noudattaa kaikkia asiaankuuluvia määräaikoja.
- ▶ Onko tällä todennäköisesti lisä- tai jatkuvia vaikutuksia muille henkilöille? Käyttävätkö esimerkiksi pankit järjestelmää luottokelpoisuuden määrittämiseen?
- ▶ Toimiin on ryhdyttävä välittömästi ongelmaa koskevan tietoisuuden lisäämiseksi (direktiivit yhdenvertaisuuseliimiä koskevista normeista, 5 artikla, tai markkinaevalvontaviranomaisen kautta tuoteturvallisuusasetusten nojalla).
- ▶ On selvittävä, onko tekoölyjärjestelmä vuorovaikutuksessa muiden laitteiden/ohjelmistojen kanssa, ja lisättävä tietoisuutta myös muista järjestelmistä, joihin kohdistuu vastaavia vaikutuksia.

Kirjaa tietoihin ongelmaan liittyvä teknologiatyyppi ja sektori, jotta niitä voidaan käyttää yhdenvertaisuuselimen raportoinnissa ja yhdenvertaisuustietojen analysoinnissa.

Tarvittavat korjaavat toimenpiteet riippuvat havaituista ongelmista. Vaiheessa 3 esitettyjen tietojen, vaiheiden ja lähestymistapojen tulisi kuitenkin auttaa yhdenvertaisuuselintä tunnistamaan mahdolliset oikeussuojakeinot.

Markkinavalvontaviranomaisen tutkinta tekoölyasetuksen 79 artiklan 3 kohdan mukaisesti: tuote aiheuttaa vakavan riskin perusoikeuksille, kuten syrjintäriskin

Jos markkinavalvontaviranomainen (yksin tai yhteistyössä 77 artiklan mukaisen elimen kanssa) toteaa, ettei tekoölyjärjestelmä täytä asetuksessa kuvattuja vaatimuksia, seuraavat toimet on tehtävä ilman aiheetonta viivytystä:

- ▶ asianmukaiset korjaavat toimenpiteet tekoölyjärjestelmän saattamiseksi vaatimusten mukaiseksi
- ▶ tiedottaminen komissiolle ja muille jäsenvaltioille arvioinnin tuloksista ja tarjoajan toteutettavista toimista
- ▶ tekoölyjärjestelmän poistaminen markkinoilta (tekoölyasetus, 79 artiklan 5 kohta)
- ▶ järjestelmän palautusmenettely markkinavalvontaviranomaisen asettamassa ajassa, 15 arkipäivän kuluessa tai unionin lainsäädännön mukaisesti (tämä edellyttää sovellettavan lainsäädännön tarkistamista tässä vaiheessa)
- ▶ markkinavalvontaviranomaisen ilmoitus asiaankuuluvalla ilmoitetulle laitokselle.

Markkinavalvontaviranomaisen menettely, kun tarjoaja ei ole luokitellut tekoölyjärjestelmää suuririskiseksi liitteen III mukaisesti (tekoölyasetus, 6 artiklan 4 kohta ja 80 artikla)

Jos markkinavalvontaviranomaisen on selvitettävä, onko tekoölyjärjestelmä virheellisesti jätetty järjestelyn ulkopuolelle itsearvioinnin perusteella (6 artiklan 4 kohta ja 80 artiklassa kuvattu menettely), arvioinnilla on selvitettävä, onko 6 artiklan 3 kohtaa sovellettava tapaukseen.

Tässä tapauksessa on mahdollista, ettei perusoikeusvaikutusten arviointia ole tehty tai syrjintää huomioitu asianmukaisesti. On selvitettävä, täyttääkö tekoölyjärjestelmä seuraavat edellytykset:

- ▶ tarkoituksena on suorittaa suppea menettelyllinen tehtävä
- ▶ tarkoituksena on parantaa aiemmin suoritettun ihmisen toiminnan tulosta
- ▶ tarkoituksena on havaita päätöksentekotapoja tai poikkeamia aiemmista päätöksentekotavoista
- ▶ tarkoituksena on suorittaa arvioinnin valmistelutehtävä.

On kuitenkin mahdollista, että jopa tällaiset järjestelmät voivat aiheuttaa riskejä perusoikeuksille ja syrjimättömyydelle. Yhdenvertaisuuselimet voivat siirtää järjestelmän markkinavalvontaviranomaisen tutkittavaksi, kun selvitetään, onko tekoölyjärjestelmä luokiteltu väärin, ja jakaa markkinavalvontaviranomaiselle myös näytön, johon tämä epäily perustuu.

Tekoölyasetuksen vaatimusten mukaiset suuririskiset järjestelmät, jotka aiheuttavat riskin ihmisten terveydelle tai turvallisuudelle, perusoikeuksille tai muille yleisen edun suojaan liittyville näkökohdille (tekoölyasetus, 82 artikla)

Markkinavalvontaviranomaisella on valtuuksia, joita sovelletaan tekoölyasetuksen 82 artiklan mukaisiin vaatimustenmukaisiin tekoölyjärjestelmiin, jotka aiheuttavat riskin. Ennen näiden toimien toteuttamista markkinavalvontaviranomaisen on tehtävä

- tekoölyasetuksen 79 artiklan mukainen arviointimenettely
- 77 artiklan mukaisen elimen kuuleminen.

Toimijan on toteutettava ”kaikki asianmukaiset toimenpiteet sen varmistamiseksi, että kyseinen tekoölyjärjestelmä ei markkinoille saatettaessa tai käyttöön otettaessa enää aiheuta kyseistä riskiä”.

Vaikka tekoölyasetuksessa ei tätä nimenomaisesti mainita, yhdenvertaisuuselintä tulisi kuulla ainakin silloin, kun markkinavalvontaviranomainen pyrkii selvittämään, onko perusoikeuksiin ja/tai yhdenvertaisuuteen kohdistuvat riskit poistettu onnistuneesti järjestelmästä.

4.3. Tilanteet, joissa järjestelmä tai käyttötapaus aiheuttaa riskin perusoikeuksille, mutta sitä ei ole luokiteltu suuririskiseksi tai kielletyksi

Tällainen tilanne voi syntyä, jos

- tarjoaja on itse arvioinut algoritmijärjestelmän muuksi kuin tekoölyjärjestelmäksi 3 artiklan määritelmän mukaisesti, ja järjestelmä on tämän vuoksi kokonaan asetuksen soveltamisalan ulkopuolella
- algoritmijärjestelmä, jonka tulisi olla kielletty sen aiheuttaman riskin vuoksi, ei sisälly tekoölyasetuksen 5 artiklan kiellettyjen järjestelmien luetteloon
- algoritmijärjestelmä, joka olisi luokiteltava suuririskiseksi, ei sisälly tekoölyasetuksen liitteeseen III, koska joko kyseistä sektoria tai käyttötapauksia ei ole sisällytetty siihen
- tarjoaja on soveltanut 6 artiklan 3 kohdan mukaista poikkeusta tekoölyjärjestelmään, joka muutoin luokiteltaisiin suuririskiseksi.

Huomio: käyttöönottajilla on velvollisuus valvoa suuririskisiä järjestelmiä ja ilmoittaa markkinavalvontaviranomaiselle tapauksista, joissa on syytä katsoa, että tekoölyjärjestelmän ohjeiden mukainen käyttö voi johtaa siihen, että järjestelmä aiheuttaa vakavan riskin perusoikeuksille (tekoölyasetus, 26 artikla yhdessä 79 artiklan kanssa).

Huomio: Jos tekoölyjärjestelmä on asetuksen (EU) 2019/1020 3 artiklan 19 kohdassa määritelty riskin aiheuttava tuote, markkinavalvontaviranomaisen on arvioitava järjestelmä ja tehtävä yhteistyötä asiaankuuluvien 77 artiklan mukaisten viranomaisten kanssa, jos perusoikeuksiin kohdistuvia riskejä havaitaan. Tällaisten tuotteiden oikeussuojakeinot tekoölyasetuksen nojalla rajoittuvat vaatimustenmukaisiin suuririskisiin järjestelmiin. Vaihtoehtoisia oikeussuojakeinoja voi olla saatavilla markkinavalvonnasta annetun asetuksen ja yleisen tuoteturvallisuuslainsäädännön, sopimus- tai vahingonkorvausoikeuden, syrjimättömyyslainsäädännön tai ihmisoikeuslainsäädännön nojalla.

Asianomaisten yksilöiden tai ryhmien kannalta se, ettei järjestelmää ole luokiteltu suuririskiseksi järjestelmäksi tai kielletyksi, ei kuitenkaan tarkoita, etteikö järjestelmä voi aiheuttaa syrjintää tai johtaa perusoikeuksien loukkaamiseen tai käyttöön tavalla, joka loukkaa perusoikeuksia. Yhdenvertaisuuselimet voivat käyttää kaikkia tavanomaisia syrjintää koskevia oikeussuojakeinoja syrjimättömyysdirektiivien ja kansallisen lainsäädännön mukaisesti.

4.3.1. Tekoälyasetuksen muutoksen haku

Jos yhdenvertaisuuselin toteaa tekoälykäytännön olevan perustavanlaatuisesti ristiriidassa unionin perusoikeuskirjassa kuvattujen ihmisarvon, vapauden, yhdenvertaisuuden, demokratian ja oikeusvaltioperiaatteen arvojen sekä perusoikeuksien kunnioittamisen kanssa, tästä on ilmoitettava sekä markkinavalvontaviranomaiselle että komissiolle, jotta tekoälyasetusta voidaan tarvittaessa muuttaa. Tekoälyasetuksessa on kuvattu menettely, jolla tekoälyasetukseen voidaan tehdä muutoksia erilaisissa tilanteissa.

112 artiklan mukaan komission on arvioitava vuosittain liitteessä III (suuririskiset järjestelmät) ja 5 artiklassa (kielletyt järjestelmät) kuvattujen luetteloiden muuttamisen tarvetta ja esitettävä arviointinsa tulokset Euroopan parlamentille. Siksi on tärkeää, että komissiolle ilmoitetaan tekoälyasetuksessa kuvatun menettelyn mukaisesti sellaisia tekoälyjärjestelmiä koskevista huolenaiheista, jotka tulisi kieltää tai jotka voivat olla suuririskisiä aloilla tai käyttötapauksissa, joita ei ole mainittu liitteessä III.

EU:n tekoälyasetuksen viiden ensimmäisen vuoden aikana (1. elokuuta 2029 saakka ja sen jälkeen automaattisesti pidennettynä, ellei tätä vastusteta) komissiolla on valta antaa delegoituja säädöksiä seuraavissa olosuhteissa.

6 artiklan 6 kohta	On lisättävä uusia ehtoja ei-suuririskisten järjestelmien itsearviointien edellytyksiin tai muutettava tai poistettava niitä.
7 artikla	Liitettä III on muutettava lisäämällä siihen käyttötapauksia (muttei aloja) tai muokkaamalla niitä ja poistamalla järjestelmiä luettelosta.
11 artiklan 3 kohta	Liitteen IV mukaista teknistä dokumentaatiota on muutettava (erityisesti tekniikan kehityksen perusteella).
47 artiklan 5 kohta	Liitteessä V vahvistettua EU-vaatimustenmukaisuusvakuutuksen sisältöä on päivitettävä.

Vaikka komissiolla ei ole valtuuksia antaa delegoituja säädöksiä liitteen III otsikoiden muuttamiseksi, sen on arvioitava viimeistään 2. elokuuta 2028 mennessä, onko tarpeen tehdä muutoksia, joilla laajennetaan liitteessä III olevia nykyisiä alojen otsikoita tai lisätään siihen uusia alojen otsikoita, muutoksia luetteloon tekoälyjärjestelmistä, jotka edellyttävät avoimuutta koskevia lisätoimenpiteitä, tai muutoksia, joilla parannetaan valvonta- ja hallintojärjestelmän tehokkuutta. Komission on sitten toimitettava arviointinsa Euroopan parlamentille ja neuvostolle.

Tekoälytoimisto kehittää menetelmän, jolla näitä kriteereitä voidaan arvioida.

4.3.2. Järjestelmää käytetään suuririskisellä alalla, mutta käyttötapausta ei ole mainittu tekoälyasetuksen liitteessä III

Jos tiettyä käyttötapausta ei ole sisällytetty tekoälyasetuksen liitteeseen III, komissiolla on 7 artiklan mukaan valtuudet antaa delegoituja säädöksiä liitteen III muuttamiseksi lisäämällä siihen suuririskisiä tekoälyjärjestelmiä koskevia käyttötapauksia tai muokkaamalla niitä, jos molemmat seuraavista edellytyksistä täyttyvät:

- ▶ tekoälyjärjestelmiä on tarkoitus käyttää millä tahansa liitteessä III luetelluista aloista
- ▶ tekoälyjärjestelmät 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.

Jos yhdenvertaisuuselin siis toteaa, että nämä kriteerit täyttävä käyttötapaus vaikuttaa kielteisesti perusoikeuksiin, mutta käyttötapausta ei ole mainittu liitteen III luetteloissa, on harkittava käyttötapaksesta ilmoittamista komissiolle, jotta se voidaan lisätä luetteloon tekoälyasetuksen 7 artiklan mukaisesti.

Komission huomioitavat tekijät on esitetty tekoälyasetuksen 7 artiklan 2 kohdassa, ja niitä on käsiteltävä, kun raporttia laaditaan. Ne sisältävät seuraavat:

- ▶ tekoälyjärjestelmän käyttötarkoitus
- ▶ missä määrin tekoälyjärjestelmää on käytetty tai todennäköisesti käytetään
- ▶ tekoälyjärjestelmän käsittelemien ja käyttämien tietojen luonne ja määrä, erityisesti se, käsitelläänkö erityisiä henkilötietoryhmiä
- ▶ missä määrin tekoälyjärjestelmä toimii itsenäisesti, ja missä määrin ihmisen on mahdollista kumota päätös tai suositukset, jotka voisivat aiheuttaa mahdollista haittaa
- ▶ missä määrin tekoälyjärjestelmän käyttö on jo aiheuttanut haittaa terveydelle ja turvallisuudelle, vaikuttanut kielteisesti perusoikeuksiin tai herättänyt merkittävää huolta tällaisen haitan tai kielteisen vaikutuksen todennäköisyydestä, mikä käy ilmi esimerkiksi kansallisille toimivaltaisille viranomaisille toimitetuista raporteista tai dokumentoiduista väitteistä taikka muista asianmukaisista raporteista
- ▶ tällaisen haitan tai tällaisen haitallisen vaikutuksen mahdollinen laajuus, erityisesti sen voimakkuus ja kyky vaikuttaa useisiin henkilöihin tai vaikuttaa suhteettomasti erityiseen henkilöryhmään
- ▶ 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
- ▶ missä määrin on kyse vallan epätasapainosta tai missä määrin henkilöt, joille mahdollisesti aiheutuu haittaa tai kohdistuu kielteinen vaikutus, ovat haavoittuvassa asemassa tekoälyjärjestelmän käyttöönottaajaan nähden, erityisesti aseman, valta-aseman, tietämyksen, taloudellisten tai sosiaalisten olosuhteiden tai iän vuoksi

- ▶ missä määrin tekoälyjärjestelmän avulla tuotettu tulos on helposti korjattavissa tai peruutettavissa, 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
- ▶ tekoälyjärjestelmän käyttöönotosta yksilöille, ryhmille tai koko yhteiskunnalle koituvan hyödyn suuruus ja todennäköisyys, tuoteturvallisuuden mahdolliset parannukset mukaan lukien
- ▶ missä määrin voimassa olevassa unionin oikeudessa säädetään
 - tekoälyjärjestelmän aiheuttamiin riskeihin liittyvistä tehokkaista oikeussuojakeinoista, lukuun ottamatta vahingonkorvausvaateita
 - tehokkaista toimenpiteistä kyseisten riskien ehkäisemiseksi tai vähentämiseksi merkittävästi.

Lähteet

Kirjallisuus

Adams-Prassl J., Binns R. ja Kelly-Lyth A. (2022), "Directly discriminatory algorithms", *The Modern Law Review*, 86(1), s. 144–175. Saatavilla osoitteessa <https://doi.org/10.1111/1468-2230.12759> (viitattu 17. lokakuuta 2025).

Ahmed M. (2020), "UK passport photo checker shows bias against dark-skinned women", BBC News. Saatavilla osoitteessa www.bbc.co.uk/news/technology-54349538 (viitattu 13. lokakuuta 2025).

Allen R. ja Masters D. (2019), "Artificial intelligence: the right to protection from discrimination caused by algorithms, machine learning and automated decision-making", *Journal of the Academy of European Law*. Saatavilla osoitteessa DOI: 10.1007/s12027-019-00582-w (viitattu 19. kesäkuuta 2025).

Allen R. ja Masters D. (2020), "Regulating for an equal AI: a new role for equality bodies" Equinet. Saatavilla osoitteessa https://equineteurope.org/publications/regulating-for-an-equal-ai-a-new-role-for-equality-bodies/?__cf_chl_f_tk=3KwuXAuyY1rQSy6KKjf6WQaiw8Fzq0tVZpxUk2K39Qs-1782916549-1.0.1.1-nTAmM4fODMeHv8UOjuY4hye5_YL66T80oAESRgxoA (viitattu 20. lokakuuta 2025).

Algorithm Audit (2024a), "Preventing prejudice". Saatavilla osoitteessa https://algorithmaudit.eu/algoprudence/cases/aa202401_preventing-prejudice/ (viitattu 11. lokakuuta 2025).

Algorithm Audit (2024b), "Addendum to preventing prejudice". Saatavilla osoitteessa https://algorithmaudit.eu/algoprudence/cases/aa202402_preventing-prejudice_addendum/ (viitattu 1. lokakuuta 2025).

Algorithm Watch (2022), "Automated decision-making systems and discrimination: a guidebook for anti-discrimination counselling". Saatavilla osoitteessa <https://algorithmwatch.org/en/autocheck/> (viitattu 29. syyskuuta 2025).

Amnesty International (2021), "Xenophobic machines: discrimination through unregulated use of algorithms in the Dutch childcare benefits scandal". Saatavilla osoitteessa <https://www.amnesty.org/en/documents/eur35/4686/2021/en/> (viitattu 13. lokakuuta 2025).

29 artiklan mukainen tietosuojatyöryhmä (2017a), "Guidelines on data protection impact assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679". Saatavilla osoitteessa <https://ec.europa.eu/newsroom/article29/items/611236/en> (viitattu 8. marraskuuta 2025).

29 artiklan mukainen tietosuojatyöryhmä (2017b), "Opinion on some key issues of the law enforcement directive (EU 2016/680) – wp258", Euroopan komissio. Saatavilla osoitteessa <https://ec.europa.eu/newsroom/article29/items/610178/en> (viitattu 17. lokakuuta 2025).

29 artiklan mukainen tietosuojatyöryhmä (2018a), "Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679 (WP251rev.01, 17/EN)", Euroopan komissio. Saatavilla osoitteessa <https://ec.europa.eu/newsroom/article29/items/612053/en> (viitattu 10. marraskuuta 2025).

29 artiklan mukainen tietosuojatyöryhmä (2018b), "Guidelines on transparency under Regulation 2016/679 (WP260, 17/EN)", Euroopan komissio. Saatavilla osoitteessa www.edpb.europa.eu/our-work-tools/our-documents/article-29-working-party-guidelines-transparency-under-regulation_en (viitattu 10. marraskuuta 2025).

Autoriteit Persoonsgegevens (2024), Final recommendation on supervision of AI: sector and centrally coordinated. Saatavilla osoitteessa www.autoriteitpersoonsgegevens.nl/en/current/final-recommendation-on-supervision-of-ai-sector-and-centrally-coordinated (viitattu 1. lokakuuta 2025).

Barocas S., Hardt M. ja Narayanan A. (2023), *Fairness and machine learning: limitations and opportunities*, MIT Press, Cambridge, MA.

Barros Vale S. ja Zanfir-Fortuna G. (2022), "Automated decision-making under the GDPR: practical cases from courts and data protection authorities", Future of Privacy Forum. Saatavilla osoitteessa <https://fpf.org/blog/fpf-report-automated-decision-making-under-the-gdpr-a-comprehensive-case-law-analysis/> (viitattu 1. lokakuuta 2025).

Big Brother Watch (2025), "Suspicion by design". Saatavilla osoitteessa <https://bigbrotherwatch.org.uk/campaigns/welfare-data-watch/> (viitattu 10. marraskuuta 2025).

Bird K. A., Castleman B. L. ja Song Y. (2024), "Are algorithms biased in education? Exploring racial bias in predicting community college student success", *Journal of Policy Analysis and Management*, Vol. 44 (2). Saatavilla osoitteessa <https://onlinelibrary.wiley.com/doi/full/10.1002/pam.22569> (viitattu 17. lokakuuta 2025).

Boscarol F. (2022), "Costly birthplace: discriminating insurance practice", Algorithm Watch. Saatavilla osoitteessa <https://algorithmwatch.org/en/discriminating-insurance/> (viitattu 13. lokakuuta 2025).

Ceross A. (2025), *Understanding artificial intelligence: concepts, limitations, and risks*, Equinet. Saatavilla osoitteessa <https://equineteurope.org/publications/understanding-artificial-intelligence-concepts-limitations-and-risks/> (viitattu 1. lokakuuta 2025).

College voor de Rechten van de Mens (2023), "Oordeelnummer 2023-111". Saatavilla osoitteessa <https://oordelen.mensenrechten.nl/oordeel/2023-111#kop> (viitattu 14. lokakuuta 2025).

College voor de Rechten van de Mens (CRM) (2025), "Toetsingskader risicoprofilering". Saatavilla osoitteessa www.mensenrechten.nl/actueel/nieuws/2025/01/28/nieuw-toetsingskader-tegen-discriminatie-door-risicoprofilering (viitattu 29. syyskuuta 2025).

Euroopan neuvosto ja Euroopan unionin perusoikeusvirasto (2018), *Handbook on European non-discrimination law*, 2. painos, Euroopan unionin julkaisuautoimisto. ISBN: 978-92-871-9851-8.

Euroopan neuvosto (2025a), "Legal protection against algorithmic discrimination in Europe: current frameworks and remaining gaps". Saatavilla osoitteessa <https://rm.coe.int/legal-protection-eng-web/48802a38d7> (viitattu 4. kesäkuuta 2026).

Euroopan neuvosto (2025b), "Tekoälyä ja algoritmiperusteista syrjintää koskevat eurooppalaiset suuntaviivat yhdenvertaisuuselimille ja muille kansallisille ihmisoikeustoimijoille". Saatavilla osoitteessa <https://rm.coe.int/policy-guidelines-eng-web/48802a38a5> (viitattu 4. kesäkuuta 2026).

Euroopan neuvosto (2025c), "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)". Saatavilla osoitteessa <https://rm.coe.int/prems-002726-gbr-2006-huderia-texte-web-a4/48802ba7b1> (viitattu 19. kesäkuuta 2025).

Euroopan neuvosto (2026), "Model 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)". Saatavilla osoitteessa <https://rm.coe.int/prems-002726-gbr-2006-huderia-texte-web-a4/48802ba7b1> (viitattu 19. kesäkuuta 2025).

Crenshaw K. (1991), "Mapping the margins: intersectionality, identity politics, and violence against women of color", *Stanford Law Review*, 43(6), s. 1241–1299. Saatavilla osoitteessa www.jstor.org/stable/1229039 (viitattu 1. lokakuuta 2025).

Crenshaw K. (2015), "Why intersectionality can't wait", *The Washington Post*. Saatavilla osoitteessa www.washingtonpost.com/news/in-theory/wp/2015/09/24/why-intersectionality-cant-wait/ (viitattu 1. lokakuuta 2025).

Crowley N. (2023), *Informing the policy agenda: equality bodies making recommendations*, Equinet. Saatavilla osoitteessa <https://equineteurope.org/informing-the-policy-agenda-equality-bodies-making-recommendations/> (viitattu 1. lokakuuta 2025).

Dastin J. (2018), "Amazon scraps secret AI recruiting tool that showed bias against women", *Reuters*. Saatavilla osoitteessa www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G (viitattu 10. marraskuuta 2025).

Dimitrova D. ja De Hert P. (2024), "The LED's right of access to one's data: loopholes on proper access, legality review and data protection authority accountability", *New Journal of European Criminal Law*, 15(1), s. 12–32. Saatavilla osoitteessa <https://doi.org/10.1177/20322844231214484> (viitattu 17. lokakuuta 2025).

Equinet (2017), *Strategic litigation handbook*. Saatavilla osoitteessa <https://equineteurope.org/publications/strategic-litigation-handbook/> (viitattu 29. syyskuuta 2025).

Equinet (2022), *Equality Bodies working on cases without an identifiable victim: Actio popularis*. Saatavilla osoitteessa <https://equineteurope.org/equality-bodies-working-on-cases-without-an-identifiable-victim-actio-popularis/> (viitattu 29. syyskuuta 2025).

Equinet (2025), Webinar series: equality by design, deliberation and oversight. Saatavilla osoitteessa <https://equineteurope.org/>

[webinar-series-equality-by-design-empowering-equality-bodies-and-civil-society-on-the-interface-between-technical-standards-and-legal-requirements/](#) (viitattu 1. lokakuuta 2025).

Erdogan I. (2023), "Transparency in the face of new technologies: information rights under the law enforcement directive", *Jean Monnet Network on EU Law Enforcement Working Paper Series*. Saatavilla osoitteessa <https://jmn-eulen.nl/papers/events-on-ai/> (viitattu 17. lokakuuta 2025).

Erdogan I. (2024), "Diving into the iceberg: establishing transparency in AI for law enforcement", *European Papers*, 9(3), s. 956–977. Saatavilla osoitteessa www.europeanpapers.eu/e-journal/diving-into-iceberg-establishing-transparency-ai-for-law-enforcement (viitattu 17. lokakuuta 2025).

Eticas Foundation (2024), Automating (in)justice? An adversarial audit of riscanvi. Saatavilla osoitteessa <https://www.eticasfoundation.org/automating-injustice-an-adversarial-audit-of-riscanvi/> (viitattu 13. lokakuuta 2025).

European Center for Not-for-Profit Law and Danish Institute for Human Rights (2025), A guide to fundamental rights impact assessments (FRIA). Saatavilla osoitteessa <https://ecnl.org/publications/guide-fundamental-rights-impact-assessments-fria> (viitattu 30. huhtikuuta 2026).

Euroopan komissio (2019), *Equality law review: European network of legal experts in gender equality and non-discrimination*, Euroopan unionin julkaisutoimisto. Saatavilla osoitteessa <https://op.europa.eu/s/AiAN> (viitattu 19. kesäkuuta 2026).

Euroopan komissio (2021), *Guidelines on improving the collection and use of equality data*, Euroopan unionin julkaisutoimisto. Saatavilla osoitteessa <https://data.europa.eu/doi/10.2838/9725> (viitattu 17. lokakuuta 2025).

Euroopan komissio (2025), "Supporting the implementation of the AI ACT with clear guidelines". Saatavilla osoitteessa <https://digital-strategy.ec.europa.eu/en/news/supporting-implementation-ai-act-clear-guidelines> (viitattu 1. toukokuuta 2025).

Euroopan ihmisoikeustuomioistuin (2025), "Guide on Article 14 of the European Convention on Human Rights and on Article 1 of Protocol No. 12 to the Convention". Saatavilla osoitteessa https://ks.echr.coe.int/documents/d/echr-ks/guide_art_14_art_1_protocol_12_eng (viitattu 10. marraskuuta 2025).

Farkas L. ja O'Farrell O. (2015), *Reversing the burden of proof: practical dilemmas at the European and national level*, Euroopan unionin julkaisutoimisto. Saatavilla osoitteessa <https://op.europa.eu/en/publication-detail/-/publication/a763ee82-b93c-4df9-ab8c-626a660c9da8/language-en> (viitattu 10. marraskuuta 2025).

FRA (2018), *Handbook on European non-discrimination law – 2018 edition*. Saatavilla osoitteessa <https://fra.europa.eu/en/publication/2018/handbook-european-non-discrimination-law-2018-edition#> (viitattu 1. heinäkuuta 2026).

FRA (2025), "Assessing high-risk artificial intelligence: fundamental rights risks". Saatavilla osoitteessa [Assessing High-risk Artificial Intelligence: Fundamental Rights Risks – European Union Agency for Fundamental Rights](#) (viitattu 4. kesäkuuta 2026).

Fredman S. (2016), *Intersectional discrimination in EU gender equality and non-discrimination law*, European Equality Law Network, Euroopan unionin julkaisutoimisto. Saatavilla osoitteessa <https://op.europa.eu/en/publication-detail/-/publication/d73a9221-b7c3-40f6-8414-8a48a2157a2f/language-en> (viitattu 17. lokakuuta 2025).

González Fuster G. (2020), "Artificial intelligence and law enforcement. Impact on fundamental rights". Euroopan parlamentti. Saatavilla osoitteessa <https://op.europa.eu/s/AiyD> (viitattu 12. marraskuuta 2025).

Howard E. (2024), "Intersectional discrimination and EU law: time to revisit Parris", *Sage Journals*. Saatavilla osoitteessa <https://journals.sagepub.com/doi/10.1177/13582291241285336> (viitattu 1. toukokuuta 2026).

Ilieva S. (2024), *Handbook on identifying and using equality data in legal casework*, Equinet. Saatavilla osoitteessa <https://equineteurope.org/publications/handbook-on-identifying-and-using-equality-data-in-legal-casework/> (viitattu 29. syyskuuta 2025).

Information Commissioner's Office and Equality and Human Rights Commission (2023), Memorandum of understanding between the Information Commissioner and the Equality and Human Rights Commission. Saatavilla osoitteessa <https://ico.org.uk/about-the-ico/our-information/working-with-other-bodies/> (viitattu 1. lokakuuta 2025).

JuLIA Project (2024), *Handbook: artificial intelligence, judicial decision-making and fundamental rights*, JuLIA 101046631, Euroopan komissio (DG JUST – JUST-2021-JTRA). Saatavilla osoitteessa <https://www.julia-project.eu/resources> (viitattu 1. lokakuuta 2025).

Lighthouse Reports (2025), "How we investigated Amsterdam's attempt to build a 'fair' fraud detection model". Saatavilla osoitteessa www.lighthousereports.com/methodology/amsterdam-fairness/ (viitattu 19. kesäkuuta 2026).

Lighthouse Reports (2024), "How we investigated Sweden's suspicion machine". Saatavilla osoitteessa www.lighthousereports.com/methodology/sweden-ai-methodology/ (viitattu 20. lokakuuta 2025).

Lighthouse Reports (2023), "How we investigated France's mass profiling machine". Saatavilla osoitteessa www.lighthousereports.com/methodology/how-we-investigated-frances-mass-profiling-machine/ (viitattu 19. lokakuuta 2025).

Mahieu R. L., Asghari H. ja van Eeten M. (2018), "Collectively exercising the right of access: individual effort, societal effect", *Internet Policy Review*, 7(3). Saatavilla osoitteessa <https://doi.org/10.14763/2018.3.927> (viitattu 10. marraskuuta 2025).

Makkonen T. (2007), *Measuring discrimination: data collection and EU equality law*, Euroopan unionin julkaisutoimisto. Saatavilla osoitteessa <https://op.europa.eu/en/publication-detail/-/publication/7d20295d-212c-4acb-bd9f-6f67f4c7ce67> (viitattu 10. marraskuuta 2025).

Makkonen T. (2016), *European handbook on equality data: 2016 revision*, Euroopan unionin julkaisutoimisto. Saatavilla osoitteessa https://ec.europa.eu/newsroom/just/document.cfm%3Faction%3Ddisplay%26doc_id%3D43205&ved=2ahUKEwiysrmm-eeQAxiw

AIHHUBOH9MQFnoECBgQAQ&usg=AOvVaw1aG86yvIJ51QDEGbA_FR7L (viitattu 10. marraskuuta 2025).

Mantelero A. (2024), "The fundamental rights impact assessment (FRIA) in the AI Act: roots, legal obligations and key elements for a model template", *Computer Law & Security Review*, 54, s. 106020. Saatavilla osoitteessa www.sciencedirect.com/science/article/pii/S0267364924000864 (viitattu 10. marraskuuta 2025).

Mittelstadt B. (2024), "How to use the Artificial Intelligence Act to investigate AI bias and discrimination: a guide for equality bodies", *Equinet*. Saatavilla osoitteessa <https://equineteurope.org/publications/how-to-use-the-artificial-intelligence-act-to-investigate-ai-bias-and-discrimination-a-guide-for-equality-bodies/> (viitattu 1. lokakuuta 2025).

Mittelstadt B., Wachter S. ja Russell C. (2023), "The unfairness of fair machine learning: levelling down and strict egalitarianism by default". Saatavilla osoitteessa <https://arxiv.org/abs/2302.02404> (viitattu 17. heinäkuuta 2026).

Norwegian Data Protection Authority (2023), "Evaluation of the Norwegian Data Protection Authority's regulatory sandbox for artificial intelligence". Saatavilla osoitteessa <https://www.datatilsynet.no/en/news/aktuelle-nyheter-2023/the-sandbox-has-been-evaluated/> (viitattu 17. lokakuuta 2025).

Parviainen H. (2024), "Challenges of direct discrimination in algorithmic recruitment: insuperable or not?*", *International Journal of Comparative Labour Law and Industrial Relations*, 40, 4. joulukuuta 2024, s. 437–466. Saatavilla osoitteessa <https://doi.org/10.54648/ijcl2024017> (viitattu 17. lokakuuta 2025).

Purificato I. (2021), "Behind the scenes of Deliveroo's algorithm: in the blindness of 'frank' its discriminatory potential", *Italian Labour Law e-Journal*, 14(1), s. 169–194. Saatavilla osoitteessa [doi:10.6092/issn.1561-8048/12990](https://doi.org/10.6092/issn.1561-8048/12990) (viitattu 22. kesäkuuta 2026).

PWC (2024), *Onderzoek misbruik uitwonendenbeurs*. Saatavilla osoitteessa www.tweedekamer.nl/kamerstukken/detail?id=2024D07564&did=2024D07564 (viitattu 12. marraskuuta 2025).

Research Institute – Digital Human Rights Center (2025), "Enlightenment 4.0 – human understanding of AI decision-making: report on the theoretical basis of the right to explanation of individual decision-making under Article 86 AI Act", Federal Ministry of Labour and Social Affairs, Health Care and Consumer Protection Republic of Austria. Saatavilla osoitteessa <https://researchinstitute.at/en/enlightenment-4-0-project-results-published-in-english/>; Website of the Ministry of Social Affairs (viitattu 29. syyskuuta 2025).

Schot E. ja Davidson D. (2025), "Onbetrouwbaar algoritme bestempelt jongeren als toekomstig crimineel, Follow the money". Saatavilla osoitteessa www.ftm.nl/artikelen/algoritme-bestempelt-jongeren-onterecht-als-toekomstig-crimineel?share=UommUbfeHZLpB371b2sHbWwyodKB4uUhl7QNw2Jm6lIWxJmeq7VOeP7i73ixLPA%3D (viitattu 13. lokakuuta 2025).

Skiotytë G. ja Sadauskaitë A. (2026), "A Digital Omnibus: identifying interlinks and possible overlaps between different legal acts in the field of digital legislation to

streamline tech rules”, Euroopan parlamentti, talouden ja kasvun politiikkayksikkö, Brysseli. Saatavilla osoitteessa [https://www.europarl.europa.eu/thinktank/en/document/ECTI_STU\(2026\)772641](https://www.europarl.europa.eu/thinktank/en/document/ECTI_STU(2026)772641) (viitattu 30. huhtikuuta 2026).

Smith E. ja Vogell H. (2022), ”How your shadow credit score could decide whether you get an apartment”, ProPublica. Saatavilla osoitteessa www.propublica.org/article/how-your-shadow-credit-score-could-decide-whether-you-get-an-apartment (viitattu 17. lokakuuta 2025).

Soler Garrido J., De Nigris S., Bassani E., Sanchez I., Tatjana E., Antoine-Alexandre A. ja Boulangé T. (2024), *Harmonised standards for the European AI Act*, yhteinen tutkimuskeskus, Euroopan komissio. Saatavilla osoitteessa <https://publications.jrc.ec.europa.eu/repository/handle/JRC139430> (viitattu 17. lokakuuta 2025).

The Guardian (2021), ”What happened when a ‘wildly irrational’ algorithm made crucial healthcare decisions”. Saatavilla osoitteessa www.theguardian.com/us-news/2021/jul/02/algorithm-crucial-healthcare-decisions (viitattu 17. lokakuuta 2025).

Yhdistyneet kansakunnat (2011), ”Guiding principles on business and human rights: implementing the United Nations’ protect, respect and remedy’ framework”, Yhdistyneet kansakunnat, New York ja Geneve. Saatavilla osoitteessa <https://digitallibrary.un.org/record/720245?v=pdf> (viitattu 1. lokakuuta 2025).

Vogiatzoglou P. ja Marquiene T. (2022), Assessment of the implementation of the Law Enforcement Directive, Euroopan parlamentti. Saatavilla osoitteessa [https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU\(2022\)740209](https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2022)740209) (viitattu 17. lokakuuta 2025).

Wachter S., Mittelstadt B. ja Russell C. (2020), ”Why fairness cannot be automated: bridging the gap between EU non-discrimination law and AI”, *Computer Law & Security Review*, Vol. 41, heinäkuu 2021. Saatavilla osoitteessa <https://www.sciencedirect.com/science/article/abs/pii/S0267364921000406> (viitattu 1. heinäkuuta 2026).

Weerts H., Xenidis R., Tarissan F., Olsen H. P. ja Pechenizkiy M. (2023), ”Algorithmic unfairness through the lens of EU non-discrimination law: or why the law is not a decision tree”, *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency*, s. 805–816.

Weerts H., Kelly-Lyth A., Binns R. ja Adams-Prassl J. (2024), ”Unlawful proxy discrimination: a framework for challenging inherently discriminatory algorithms”, *The 2024 ACM Conference on Fairness, Accountability, and Transparency*, s. 1850–1860. doi:10.1145/3630106.3659010.

Xenidis R. (2021), ”Tuning EU equality law to algorithmic discrimination: three pathways to resilience”, *Maastricht Journal of European and Comparative Law*, 27(6), s. 736–758.

Zuiderveen Borgesius F. (2018), ”Discrimination, artificial intelligence and algorithmic decision making”, demokration pääosasto, Euroopan neuvosto. Saatavilla osoitteessa <https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73> (viitattu 10. marraskuuta 2025).

Lainsäädäntö

Neuvoston päätös 2007/533/YOS, tehty 12 päivänä kesäkuuta 2007, toisen sukupolven Schengenin tietojärjestelmän (SIS II) perustamisesta, toiminnasta ja käytöstä, *Euroopan unionin virallinen lehti*, L 205.

Neuvoston direktiivi 76/207/ETY, annettu 9 päivänä helmikuuta 1976, miesten ja naisten tasa-arvoisen kohtelun periaatteen toteuttamisesta mahdollisuuksissa työhön, ammatilliseen koulutukseen ja uralla etenemiseen sekä työoloissa, *Euroopan yhteisöjen virallinen lehti*, EUVL, L 39, 14. helmikuuta 1976, s. 40–42.

Neuvoston direktiivi 97/80/EY, annettu 15 päivänä joulukuuta 1997, todistustaakasta sukupuoleen perustuvissa syrjintätapauksissa, *Euroopan yhteisöjen virallinen lehti*, EYVL, L 014, 20. tammikuuta 1998, s. 6–8.

Neuvoston direktiivi 2000/43/EY, annettu 29 päivänä kesäkuuta 2000, rodusta tai etnisestä alkuperästä riippumattoman yhdenvertaisen kohtelun periaatteen täytäntöönpanosta, *Euroopan yhteisöjen virallinen lehti*, EYVL, L 180, 19. heinäkuuta 2000, s. 22–26.

Neuvoston direktiivi 2000/78/EY, annettu 27 päivänä marraskuuta 2000, yhdenvertaista kohtelua työssä ja ammatissa koskevista yleisistä puitteista, *Euroopan yhteisöjen virallinen lehti*, EYVL, L 303, 2. joulukuuta 2000, s. 16–22.

Neuvoston direktiivi 2004/113/EY, annettu 13 päivänä joulukuuta 2004, miesten ja naisten yhdenvertaisen kohtelun periaatteen täytäntöönpanosta tavaroiden ja palvelujen saatavuuden ja tarjonnan alalla, *Euroopan unionin virallinen lehti*, EUVL, L 373, 21. joulukuuta 2004, s. 37–43.

Neuvoston direktiivi (EU) 2024/1499, annettu 7 päivänä toukokuuta 2024, normeista tasa-arvoelimmille, jotka toimivat asioissa, jotka koskevat henkilöiden rodusta tai etnisestä alkuperästä riippumatonta yhdenvertaista kohtelua, uskonnosta tai vakauksesta, vammaisuudesta, iästä tai seksuaalisesta suuntautumisesta riippumatonta yhdenvertaista kohtelua työssä ja ammatissa ja naisten ja miesten yhdenvertaista kohtelua sosiaaliturvaa koskevista asioista ja tavaroiden ja palvelujen saatavuuden ja tarjonnan osalta sekä direktiivien 2000/43/EY ja 2004/113/EY muuttamisesta, *Euroopan unionin virallinen lehti*, EUVL, L 2024/1499, 2024/1500, 29. toukokuuta 2024.

Euroopan neuvosto (1950), Euroopan ihmisoikeussopimus, Rooma, 4. marraskuuta 1950, Euroopan neuvoston sopimussarja ETS nro 5.

Euroopan neuvosto (2000), ihmisoikeuksien ja perusvapauksien suojaamiseksi tehdyn yleissopimuksen kahdestoista pöytäkirja, Rooma, 4. marraskuuta 2000, Euroopan neuvoston sopimussarja ETS nro 177.

Euroopan neuvosto (2024), tekoälyä ja ihmisoikeuksia, demokratiaa ja oikeusvaltioperiaatetta koskeva Euroopan neuvoston puiteyleissopimus, Vilna, 5. syyskuuta 2024, Euroopan neuvoston sopimussarja ETS nro 225.

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). *Euroopan unionin virallinen lehti*, EUVL, L 204, 26. heinäkuuta 2006, s. 23–36.

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 (ETA:n kannalta merkityksellinen teksti), EUVL, L 132, 17. toukokuuta 2023, s. 21–44.

Euroopan parlamentin ja neuvoston direktiivi (EU) 2024/1385, annettu 14 päivänä toukokuuta 2024, naisiin kohdistuvan väkivallan ja perheväkivallan torjumisesta, EUVL, L 204/1385, 24. toukokuuta 2024.

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, *Euroopan unionin virallinen lehti*, EUVL, L 204/1500, 29. toukokuuta 2024.

European Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act) C(2025) 5052 final, 29. heinäkuuta 2025.

Euroopan parlamentin ja neuvoston asetetus (EU) 2026/1744, annettu 8 päivänä heinäkuuta 2026, asetusten (EU) 2024/1689, (EU) 2018/1139 ja (EU) 2023/1230 muuttamisesta tekoälyä koskevien yhdenmukaistettujen sääntöjen täytäntöönpanon yksinkertaistamiseksi (tekoälyä koskeva digitaalialan koontiasetus). Saatavilla osoitteessa <https://eur-lex.europa.eu/eli/reg/2026/1744/oj/eng> (viitattu 24. heinäkuuta 2026).

Euroopan parlamentin ja neuvoston asetetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (yleinen tietosuoja-asetus), *Euroopan unionin virallinen lehti*, EUVL, L 119, 4. toukokuuta 2016, s. 1–88.

Ehdotus, Euroopan parlamentin ja neuvoston asetetus asetusten (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 ja direktiivien 2002/58/EY, (EU) 2022/2555 ja (EU) 2022/2557 muuttamisesta digitaalisen lainsäädäntökehiksen yksinkertaistamiseksi sekä asetusten (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868 ja direktiivin (EU) 2019/1024 kumoamisesta (digitaalialan koontiasetus), COM/2025/837 final, [EUR-Lex - 52025PC0837 - EN - EUR-Lex](#).

Euroopan parlamentin ja neuvoston asetetus (EU) 2019/1020, annettu 20 päivänä kesäkuuta 2019, markkinavalvonnasta ja tuotteiden vaatimustenmukaisuudesta, *Euroopan unionin virallinen lehti*, EUVL, L 169, 25. kesäkuuta 2019, s. 1–44.

Euroopan parlamentin ja neuvoston asetetus (EU) 2023/988, annettu 10 päivänä toukokuuta 2023, yleisestä tuoteturvallisuudesta, Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 1025/2012 ja Euroopan parlamentin ja neuvoston direktiivin (EU) 2020/1828 muuttamisesta sekä Euroopan parlamentin ja neuvoston direktiivin 2001/95/EY ja neuvoston direktiivin 87/357/ETY kumoamisesta (ETA:n kannalta merkityksellinen teksti), *Euroopan unionin virallinen lehti*, EUVL, L 135, 23. toukokuuta 2023, s. 1–51.

Euroopan parlamentin ja neuvoston asetus (EU) 2024/1689, annettu 13 päivänä kesäkuuta 2024, tekoälyä koskevista yhdenmukaistetuista säännöistä (tekoälysäädös), *Euroopan unionin virallinen lehti*, EUVL, L 2024/1689, 12. heinäkuuta 2024.

Euroopan parlamentin ja neuvoston asetus (EY) N:o 767/2008, annettu 9 päivänä heinäkuuta 2008, viisumitietojärjestelmästä (VIS) ja lyhytaikaista oleskelua varten myönnettäviä viisumeja koskevasta jäsenvaltioiden välisestä tietojenvaihdosta (VIS-asetus), *Euroopan unionin virallinen lehti*, EUVL, L 218, 13. elokuuta 2008, s. 60–81.

Euroopan parlamentin ja neuvoston asetus (EU) N:o 603/2013, annettu 26 päivänä kesäkuuta 2013, Eurodac-järjestelmän perustamisesta sormenjälkien vertailua varten kolmannen maan kansalaisen tai kansalaisuudettoman henkilön johonkin jäsenvaltioon jättämän kansainvälistä suojelua koskevan hakemuksen käsittelystä vastuussa olevan jäsenvaltion määrittämisperusteiden ja -menettelyjen vahvistamisesta annetun asetuksen (EU) N:o 604/2013 tehokkaaksi soveltamiseksi sekä jäsenvaltioiden lainvalvontaviranomaisten ja Europolin esittämistä, Eurodac-tietoihin lainvalvontatarkoituksessa tehtäviä vertailuja koskevista pyynnöistä sekä vapauden, turvallisuuden ja oikeuden alueen laaja-alaisen tietojärjestelmien operatiivisesta hallinnoinnista vastaavan eurooppalaisen viraston perustamisesta annetun asetuksen (EU) N:o 1077/2011 muuttamisesta (uudelleenlaadittu), *Euroopan unionin virallinen lehti*, EUVL, L 180, 29. kesäkuuta 2013, s. 1–30.

Ruotsin syrjintälaki, 2008: 567.

Juridiikka/oikeuskäytäntö

Andersen v. Region Syddanmark, (2010), unionin tuomioistuin, asia C-499/08. Saatavilla osoitteessa https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2010_346_R_0007_01 (viitattu 1. heinäkuuta 2026)

Luottokelpoisuuden arviointimenettely, toimivalta, välitön moniperusteinen syrjintä, sukupuoli, kieli, ikä, asuinpaikka, taloudelliset syyt, uhkasakko (2018), Suomen yhdenvertaisuus- ja tasa-arvolautakunta, täysistunto (ään.), 216/2017. Saatavilla osoitteessa <https://www.yvtltk.fi/en/decisions/multiple-discrimination-in-the-assessment-of-creditworthiness/> (viitattu 13. lokakuuta 2025).

Association Belge des Consommateurs Test-Achats ASBL ym v. Conseil des ministres (2011), unionin tuomioistuin, asia C-236/09; ECLI:EU:C:2011:100. Saatavilla osoitteessa <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62009CJ0236> (viitattu 12. marraskuuta 2025).

Beghal v. Yhdistynyt kuningaskunta, hakemusnro 4755/16 (22. elokuuta 2016), lisätietoja vaatimuksista, joita kansalliselle lainsäädännölle asetetaan, jotta riitautettua toimenpidettä voidaan pitää lain mukaisena. Saatavilla osoitteessa <https://hudoc.echr.coe.int/eng/?i=001-166724>.

CHEZ Razpredelenie Bulgaria AD v. Komisia za zashtita ot diskriminatsia (2015), unionin tuomioistuin, asia C-83/14; ECLI:EU:C:2015:480. Saatavilla osoitteessa <https://eur-lex.europa.eu/legal-content/NL/ALL/?uri=CELEX:62014CJ0083> (viitattu 10. marraskuuta 2025).

CK v. Dun & Bradstreet Austria GmbH ja Magistrat der Stadt Wien (2025), unionin tuomioistuin, asia C-203/22; ECLI:EU:C:2025:117. Saatavilla osoitteessa <https://curia.europa.eu/juris/liste.jsf?num=C-203/22> (viitattu 7. lokakuuta 2025).

David L. Parris v. Trinity College Dublin ym. (2016), unionin tuomioistuin, asia C-232/09; ECLI:C:2010:674. Saatavilla osoitteessa <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62015CJ0443> (viitattu 1. toukokuuta 2026).

Dekker v. Stichting Vormingscentrum voor Jong Volwassenen (VJV-Centrum) Plus (1990), unionin tuomioistuin, asia C-177/88; ECLI:EU:C:1990:383. Saatavilla osoitteessa <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:61988CJ0177> (viitattu 7. lokakuuta 2025).

D.H. ym. v. Tšekin tasavalta (2007), Euroopan ihmisoikeustuomioistuin, hakemusnro 57325/00. Saatavilla osoitteessa [https://hudoc.echr.coe.int/eng#%22itemid%22\[%22001-72317%22\]](https://hudoc.echr.coe.int/eng#%22itemid%22[%22001-72317%22]) (viitattu 1. lokakuuta 2025).

Dita Danosa v. LKB Līzings SIA (2010), unionin tuomioistuin, asia C-232/09; ECLI:EU:C:2010:674. Saatavilla osoitteessa <https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:62009CJ0232> (viitattu 20. lokakuuta 2025).

Enderby v. Frenchay Health Authority and Secretary of State for Health (1993), unionin tuomioistuin, asia C-127/92; ECLI:EU:C:1993:313. Saatavilla osoitteessa <https://curia.europa.eu/juris/liste.jsf?num=C-127/92> (viitattu 1. lokakuuta 2025).

Filcams Cgil Bologna ym v. (...) S.R.L. (2020), Bolognan tuomioistuin, päätös nro 2949/2019. Saatavilla osoitteessa <https://apps.eurofound.europa.eu/platformeconomydb/italian-court-rules-that-the-deliveroo-algorithm-discriminates-workers-106121>.

Frédéric Hay v. Crédit Agricole mutuel de Charente Maritime et des Deux-Sèvres (2012), unionin tuomioistuin, asia C-267-12; ECLI:EU:C:2013:823. Saatavilla osoitteessa <https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:62012CJ0267> (viitattu 12. marraskuuta 2025).

Galina Meister v. Speech Design Carrier Systems GmbH (2012), unionin tuomioistuin, asia C-415/10; ECLI:EU:C:2012:217. Saatavilla osoitteessa <https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:62010CJ0415> (viitattu 12. marraskuuta 2025).

Glukhin v. Venäjä (2023), Euroopan ihmisoikeustuomioistuin, hakemusnro 11519/20. Saatavilla osoitteessa <https://hudoc.echr.coe.int/eng?i=001-225655> (viitattu 7. lokakuuta 2025).

Handels- og Kontorfunktionærernes Forbund I Danmark v. Dansk Arbejdsgiverforening, Danfossin puolesta (1989), unionin tuomioistuin, asia C109/99; ECLI:EU:C:1989:383. Saatavilla osoitteessa <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:61988CJ0109> (viitattu 12. marraskuuta 2025).

Helga Nimz v. Freie und Hansestadt Hamburg (1991), unionin tuomioistuin, asia C-184/89; ECLI:EU:C:1991:50. Saatavilla osoitteessa <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:61989CJ0184> (viitattu 12. marraskuuta 2025).

Hoogendijk v. Alankomaat (2005), Euroopan ihmisoikeustuomioistuin, hakemusno 58641/00. Saatavilla osoitteessa <https://hudoc.echr.coe.int/eng?i=001-68064> (viitattu 1. lokakuuta 2025).

Inge Nolte v. Landesversicherungsanstalt Hannover (1995), unionin tuomioistuin, asia C-317-93; ECLI:EU:C:1995:438. Saatavilla osoitteessa <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:61993CJ0317> (viitattu 12. marraskuuta 2025).

Ingeniørforeningen i Danmark v. Region Syddanmark (2010), unionin tuomioistuin, asia C-499/08; ECLI:EU:C:2010:600. Saatavilla osoitteessa <https://curia.europa.eu/juris/documents.jsf?critereEcli=ECLI:EU:C:2010:600> (viitattu 1. lokakuuta 2025).

Ingrid Rinner-Kühn v. FWW Spezial-Gebäudereinigung GmbH & Co. KG (1989), unionin tuomioistuin, asia C-171/88; ECLI:EU:C:1989:328. Saatavilla osoitteessa <https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A61988CJ0171> (viitattu 12. marraskuuta 2025).

IX v. Wabe eV ja MH Müller Handels GmbH v MJ (2021), unionin tuomioistuin, asia C-804/18 ja C-341/19; ECLI:EU:C:2021:144. Saatavilla osoitteessa <https://eur-lex.europa.eu/legal-content/nl/TXT/?uri=CELEX:62019CC0341> (viitattu 7. lokakuuta 2025).

James v. Eastleigh Borough Council (1990), House of Lords, 2 AC 751. Saatavilla osoitteessa <https://www.bailii.org/uk/cases/UKHL/1990/6.html> (viitattu 12. marraskuuta 2025).

Jyske Finans v. Ligebehandlingsnævnet (2017), unionin tuomioistuin, C-668/15; ECLI:EU:C:2017:278. Saatavilla osoitteessa <https://curia.europa.eu/juris/liste.jsf?num=C-668/15> (viitattu 10. marraskuuta 2025).

Kelly v. National University of Ireland (University College, Dublin) (2011), unionin tuomioistuin, asia C-104/10; ECLI:EU:C:2011:506. Saatavilla osoitteessa <https://eur-lex.europa.eu/legal-content/nl/TXT/?uri=CELEX:62010CJ0104> (viitattu 10. marraskuuta 2025).

La Quadrature du Net ym v. Premier ministre ja Ministère de La Culture (2024), unionin tuomioistuin, asia C-470/21; ECLI:EU:C:2024:370. Saatavilla osoitteessa <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62021CJ0470> (viitattu 14. marraskuuta 2025).

(Loredas) HJ v. US ja MU (2024), unionin tuomioistuin, asia C-531-23; ECLI:EU:C:2024:1050. Saatavilla osoitteessa <https://eur-lex.europa.eu/legal-content/nl/TXT/?uri=CELEX:62023CJ0531> (viitattu 12. marraskuuta 2025).

M. A. De Weerd, née Roks ym. v. Bestuur van de Bedrijfsvereniging voor de Gezondheid, Geestelijke en Maatschappelijke Belangen and others (1994), unionin tuomioistuin, asia C-343/92; ECLI:EU:C:1994:71. Saatavilla osoitteessa <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:61992CJ0343> (viitattu 12. marraskuuta 2025).

Manjang v. Uber Eats UK Ltd ym. (2021), Employment Tribunal, asia nro 3206212/2021. Saatavilla osoitteessa www.gov.uk/employment-tribunal-decisions/mr-p-e-manjang-v-uber-eats-uk-ltd-and-others-3206212-slash-2021 (viitattu 7. lokakuuta 2025).

Tadao Maruko v. Versorgungsanstalt der deutschen Bühnen (2008), unionin tuomioistuin, C-267/06; ECLI:EU:C:2008:179. Saatavilla osoitteessa <https://curia.europa.eu/juris/liste.jsf?num=C-267/06> (viitattu 12. marraskuuta 2025).

Verli Hariev Belov v. CHEZ Elektro Bulgaria AD ym. (2013), unionin tuomioistuin, asia C-394/11; ECLI:EU:C:2013:48. Saatavilla osoitteessa <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62011CJ0394> (viitattu 17. lokakuuta 2025).

VL v. Szpital Kliniczny im. dra J. Babińskiego Samodzielny Publiczny Zakład Opieki Zdrowotnej w Krakowie (2021), unionin tuomioistuin, asia C-16/19; ECLI:EU:C:2021:64, 48 kohta. Saatavilla osoitteessa <https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:62019CJ0016> (viitattu 7. lokakuuta 2025).

Liite A

Mallipohja rekisteröidyn pyynnölle saada pääsy tietoihin (DSAR)

Huomio: DSAR voidaan laatia joko yleisluontoisesti tai tarkemmin määritellyllä tavalla, ja kummallakin lähestymistavalla on omat hyötynsä ja riskinsä.

Tarkat pyynnot voivat lisätä todennäköisyyttä saada juuri pyydetty tiedot, vähentää jatkoviestinnän tarvetta ja nopeuttaa prosessia. Käytännössä kuitenkin pyynnön kohteena olevat organisaatiot antavat usein yksilöllisen vastauksen vasta jatkopyynnön jälkeen. Tarkemmin määriteltujen pyyntöjen esittäminen varhaisessa vaiheessa voi kuormittaa rekisteröityä, joka ei välttämättä tunne asiaankuuluvia toimenpiteitä tai terminologiaa, mikä lisää tietojen puuttumisen riskiä ja mahdollistaa rekisterinpitäjien rajoittavat tulkinnot.

Nämä pyynnot virallistetaan tekoälyä koskevassa digitaalialan koontiasetuksessa⁶⁰. Sen mukaan rekisteröidyn olisi oltava ”mahdollisimman tarkka” tehdessään DSAR-pyyntöjä, kun taas ”liian laajoja ja eriyttämättömiä pyyntöjä olisi myös pidettävä kohtuuttomina”, mikä viittaa siihen, että yleistason erittelemättömät pyynnot saatetaan hylätä liian laajoina.

Tämä malli on vain esimerkki, ja sitä on mukautettava kyseisen tapauksen mukaan.

[Rekisteröidyn nimi ja osoite]

[valinnainen: rekisteröidyn puhelinnumero ja sähköpostiosoite]

[Pyyntöjen päivämäärä]

[Rekisterinpitäjän tiedot – yrityksen osoite]⁶¹

Rekisteröidyn pyyntö saada pääsy tietoihin yleisen tietosuoja-asetuksen 15 artiklan nojalla

60. Johdanto-osan kappale 35, 3 artikla, ehdotus, Euroopan parlamentin ja neuvoston asetus asetusten (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 ja direktiivien 2002/58/EY, (EU) 2022/2555 ja (EU) 2022/2557 muuttamisesta digitaalisen lainsäädäntökehyksen yksinkertaistamiseksi sekä asetusten (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868 ja direktiivin (EU) 2019/1024 kumoamisesta (digitaalialan koontiasetus)

61. Lähetettävä rekisterinpitäjälle: yhteystiedot löytyvät yleensä organisaation tietosuojakäytännöstä tai verkkosivustolla olevasta oikeudellisesta huomautuksesta. Tekoälyjärjestelmään liittyvissä tapauksissa rekisterinpitäjä on tyypillisesti järjestelmän käyttöönottaja (organisaatio, joka käyttää sitä, eli taho, jonka kanssa rekisteröity on ollut vuorovaikutuksessa käsiteltävän prosessin aikana, kuten pankki, vakuutusyhtiö, yliopisto tai työnantaja). Voittoa tavoittelematon järjestö Datenanfragen.de e.V., joka vastaa verkkosivustosta datarequests.org (saatavilla useilla eri kielillä), ylläpitää myös [yritystietokantaa](#), joka sisältää monien eri yritysten tietosuojapyyntöihin liittyviä yhteystietoja.

Hyvä vastaanottaja

Käytän täten **yleisen tietosuoja-asetuksen (GDPR) 15 artiklan** mukaisia oikeuksiani ja pyydän vahvistusta siitä, käsittelettekö minua koskevia henkilötietoja.

Jos käsittelette henkilötietojani, pyydän teitä toimittamaan minulle seuraavat tiedot yleisen tietosuoja-asetuksen 15 artiklan mukaisesti.

1. Pääsy X tarkoitukseen käytettyihin henkilötietoihini

- ▶ Kopio kaikista minua koskevista henkilötiedoista, joita on käytetty tai käsitelty seuraaviin tarkoituksiin:

[Lisää tähän tapauksen kannalta keskeiset tarkoitukset, kuten pankkitilin avaaminen tai hallinnointi pyynnön tekijän nimissä / matkapuhelinsopimuksen tekeminen, uusiminen tai jatkaminen / kelpoisuuden arviointi tai käsittely [tiettyyn etuuteen] liittyen / työhakemuksen käsittely tai arviointi / verkossa olevien tilien, sovellusten tai digitaalisten tilausten käyttöoikeuksien määrittäminen / kuljetusten tai toimitustilausten varaaminen alustalla jne.]

2. Tiedot muista käsittelytarkoituksista

- ▶ Tiedot muista tarkoituksista, joihin henkilötietojani on käsitelty tai käsitellään edellä mainittujen lisäksi.
- ▶ Kuvaus kyseisistä henkilötietoryhmistä.

3. Tietojen luovuttaminen kolmansille osapuolille

- ▶ Vastaanottajat tai vastaanottajaryhmät, joille henkilötietojani on luovutettu, sekä jaettujen tietojen kopiot ja jakamisen tarkoitus sekä tietojen luovutuspäivämäärä(t)

4. Automaattinen päätöksenteko ja profilointi

- ▶ Tieto siitä, onko henkilötietoihini sovellettu yleisen tietosuoja-asetuksen 22 artiklan 1 ja 4 kohdan mukaista automaattista päätöksentekoa.
- ▶ Jos on, pyydän teitä toimittamaan minulle merkitykselliset tiedot käytetystä logiikasta, mukaan lukien henkilötietoryhmistä, tuloksen saavuttamiseksi käytetyistä menettelyistä ja periaatteista sekä tällaisen käsittelyn mahdollisista seurauksista minulle.

5. Profilointitiedot

- ▶ Tieto siitä, onko henkilötietojani käytetty profilointiin.
- ▶ Jos on, pyydän teitä toimittamaan minulle tiedot tämän profiilin sisällöstä ja siitä, miten se luotiin.

Jos siirrätte henkilötietojani kolmanteen maahan tai kansainväliselle järjestölle, pyydän, että minulle kerrotaan yleisen tietosuoja-asetuksen 46 artiklan mukaisista siirtoa koskevista asianmukaisista suojatoimista.

Pyydän teitä toimittamaan pyytämäni minua koskevat henkilötiedot minulle jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa yleisen tietosuoja-asetuksen 20 artiklan 1 mukaisesti.

Pyyntöni sisältävät nimenomaisesti kaikki muut palvelut ja yritykset, joissa toimitte rekisterinpitäjänä yleisen tietosuoja-asetuksen 4 artiklan 7 kohdan mukaisesti.

Kuten yleisen tietosuoja-asetuksen 12 artiklan 3 kohdassa on kuvattu, teidän on toimitettava pyydetty tiedot minulle ilman aiheetonta viivytystä ja joka tapauksessa kuukauden kuluessa pyynnön vastaanottamisesta. Jos määräaikaan tarvitaan enintään kahden kuukauden pidennystä, pyydän, että minulle ilmoitetaan siitä asianmukaisesti.

Yleisen tietosuoja-asetuksen 15 artiklan 3 kohdan mukaan teidän on vastattava tähän pyyntöön ilman minulle aiheutuvia kustannuksia.

[Henkilöllisyyteni todistamiseksi liitän mukaan kopion passistani/ajokortistani jne.]
tai

[Lisää tähän tunnistetiedot. Tämä sisältää usein esimerkiksi nimen, syntymäajan, osoitteen, sähköpostiosoitteen ja niin edelleen.]

Jos ette vastaa pyyntööni ilmoitetussa ajassa, pidätän oikeuden ryhtyä oikeustoimiin teitä vastaan ja tehdä valituksen toimivaltaiselle valvontaviranomaiselle.

Etukäteen kiittäen.

Ystävällisin terveisin

[Lisää nimi tähän]

Liite B

Mallipohja selityksen pyytämiseen tekoälyasetuksen 86 artiklan mukaisesti

Seuraavaan mallipohjaan on sisällytetty Research Institute – Digital Human Rights Centerin (2025b) laatima versio, joka on julkaistu [Itävallan sosiaaliministeriön verkkosivustolla](#).

[Asiaankuuluvan henkilön nimi ja osoite]
[valinnainen: asianomaisen henkilön puhelinnumero ja sähköpostiosoite]
[Pyynnön päivämäärä]
[Tekoälyjärjestelmien käyttöönottajien tiedot⁶²]

Selityspyyntö tekoälyasetuksen 86 artiklan nojalla

Hyvä vastaanottaja

Viittaan tässä pyynnössä minua koskevaan päätökseen [päätöksen kuvaus, esimerkiksi lainahakemuksen hylkääminen, saatu riskinarviointi tai luottopisteytyksen määräitys], jonka sain [päätöksen vastaanottopäivä].

Päätöksellä [] on minuun kohdistuvia oikeusvaikutuksia, koska [selitä lyhyesti päätöksen vaikutus, esimerkiksi lainahakemuksen hylkääminen, tiettyjen palveluiden käytön epääminen tai vakuutushintojen nousu].

[tai] Päätös vaikuttaa minuun merkittävästi ja haitallisesti, koska [anna syyt haitalle, kuten syrjintä erotteluperusteiden vuoksi tai urheiluvetoonlyöntimainosten kohdistaminen peliriippuvaisiin henkilöihin].

Käytän täten oikeuttani selitykseen asetuksen (EU) 2024/1689 (tekoälyasetus) 86 artiklan mukaisesti ja pyydän selkeää ja merkityksellistä selitystä tekoälyjärjestelmän roolista päätöksentekoprosessissa ja tehdyn päätöksen pääkohdista.

62. Lähetettävä tekoälyjärjestelmän käyttöönottajalle: organisaatiolle, joka sitä käyttää – eli taholle, jonka kanssa rekisteröity on ollut vuorovaikutuksessa kyseisen prosessin aikana, kuten pankille, vakuutusyhtiölle, yliopistolle tai työnantajalle. Jos kyseessä on viranomainen – tai sen puolesta toimiva taho – yhteystiedot löytyvät EU:n tietokannan C-osiosta. Muussa tapauksessa käyttöönottajien yhteystiedot on etsittävä tekoälyjärjestelmän käyttöliittymästä, organisaation tietosuojakäytännöstä tai verkkosivustolla olevasta oikeudellisesta huomautuksesta. Jos käyttöönottajaa ei ole nimenomaisesti mainittu, käytä rekisterinpitäjän yhteystietoja. Tämä taho on tyypillisesti myös järjestelmän käyttöönottaja.

Tätä tarkoitusta varten pyydän seuraavia tietoja.

1. Tekoälyjärjestelmän rooli päätöksentekoprosessissa

- ▶ Missä määrin ja millä tavalla tekoälyjärjestelmää käytettiin päätöksentekoprosessissa?

2. Tehdyn päätöksen pääkohdat

- ▶ Mitkä olivat tärkeimmät syyt, mukaan lukien keskeiset päätökseen vaikuttaneet kriteerit, syöttötiedot ja alustavat päätökset, jotka vaikuttivat tehtyyn päätökseen?
- ▶ Mitä muita vaikutuksia tällä päätöksellä on minulle, ja miten näitä vaikutuksia arvioitiin?
- ▶ Miten päätökseen vaikuttaneita kriteerejä painotettiin ja miksi?

3. Ihmisen suorittama arvio ja perusta [ei pakollinen]

- ▶ Tekikö tekoälyjärjestelmä päätöksen täysin automaattisesti, vai tarkistiko sen ihminen? Jos ihminen tarkisti päätöksen, miten tämä käytännössä tehtiin ja kuka / mikä osasto vastasi tarkistuksesta?
- ▶ [valinnainen: käytä, jos sovellettavissa] Mihin sopimus- tai oikeusperustaan päätös perustuu?

[Henkilöllisyyteni todistamiseksi liitän mukaan kopion passistani/ajokortistani jne.]
tai

[Lisää tähän tunnistetiedot. Tämä sisältää usein esimerkiksi nimen, syntymäajan, osoitteen, sähköpostiosoitteen ja niin edelleen.]

Pyydän virallisesti, että toimitatte minulle pyydetty tiedot [x kuukauden] kuluessa [kirjallisesti] maksutta ja ymmärrettävässä muodossa. Jos on kysyttävää, voitte ottaa minuun yhteyttä [jos kyseessä on paperilähetys, käyttäkää yllä olevia yhteystietoja].

Kiitos jo etukäteen pyyntöni käsittelystä. Odotan innolla pikaista vastausta.

Ystävällisin terveisin

[Asianomaisen nimi]

Liite C

Esimerkkejä algoritmien ja tekoälyn käytöstä

Tämä liite sisältää esimerkkejä siitä, missä algoritmi- ja tekoälyjärjestelmiä yleisesti käytetään. Esimerkit on järjestetty sektorikohtaisesti, jotta algoritmien todennäköinen osallisuus voidaan selvittää helpommin. Tässä luettelossa on hyödynnetty Allenin ja Mastersin (2020) sekä Algorithm Watchin (2022) julkaisuja. Lisätietoja näistä on lähdeluettelossa.

Sektori	Esimerkki
Pankkitoiminta	Luottopisteytys
	Asiakkaiden hyväksymisprosessin automaatio
	Petosten tai rahanpesun havaitseminen
Lasten ja nuorten sosiaalipalvelut	Lapsen tulevien sosiaalipalveluiden tarpeen ennustaminen
Koulutus	Sisäänpääsy
	Opiskelijoiden kohdistaminen automaattisesti kouluihin, yliopistoihin tai ohjelmiin
	Automaattinen valvonta
	Poissaolojen ja koulunkäynnin keskeyttämisen ennustaminen tai havaitseminen
	Oppimisongelmien havaitseminen
Työllistäminen	Työhakemusten tai ansioluetteloiden valinta
	Työttömyys- ja työvoimatoimistojen suorittama työllistymisen todennäköisyyden ennustaminen
	Työtarjousten kohdistaminen työnhakijoille
	Työnhakijoiden ohjaaminen koulutukseen tai valmennukseen
	(Lähtö)haastattelujen analysointi
Terveystenhuolto	Sairauden todennäköisyyden ennustaminen
	Diagnostiikkajärjestelmät
	Lisähoitoa tarvitsevien ikääntyneiden määrän ennustaminen

Sektori	Esimerkki
Asuminen	Mahdollisten vuokralaisten automaattinen tarkistus
	Verkkolomakkeet
	Luottotietojen tarkistus
	Asuntoilmoitukset verkkoalustoilla: mitä mainoksia näytetään kenelle? (Automaattinen kohdistus)
Muuttoliike ja rajavalvonta	Seurantalistalla olevien henkilöiden kasvontunnistus
	Viisumihakemusten hyväksymisen automatisointi
	Automaattinen matkustusasiakirjojen tarkistus
Vakuutusala	Verkkolomakkeet
	Hinnoittelualgoritmit
	Asiakkaiden hyväksymisprosessin automaatio
	Korvaushakemusten automaattinen käsittely
	Petosten havaitseminen
Oikeudelliset prosessit	Avustaminen lakien laatimisessa
Oikeus	Dataan perustuvat seuraamusehdotukset
Poliisitoiminta	Rikosten esiintymisen ennustaminen tietyillä alueilla tai naapurustoissa (maantieteellinen ennakoiva poliisitoiminta)
	Häiriköivän tai väkivaltaisen käyttäytymisen ennustaminen
	Riskinarviointi- tai profilointityökalut, joilla ennakoidaan yksilöiden tulevaa rikosriskiä, mukaan lukien rikosten uusimista, tai yleisemmin "vaarallisten" tai "asianomaisten" henkilöiden tunnistaminen (yksilöiden ennakoiva poliisitoiminta)
	Sen arviointi, kuinka todennäköisesti henkilö on vastuussa tehdystä rikoksesta (yksilöiden ennakoiva poliisitoiminta)
	Kameravalvonta, jolla valvotaan rikollista toimintaa
Sosiaali-turvaetuudet	Verkkolomakkeet
	Petosten tai virheiden ennustaminen
	Etuuksien käsittelyn automaatio
Verot	Petosten tai virheiden ennustaminen

Liite D

Esimerkkejä algoritmisesta syrjinnästä tai syrjinnän riskeistä

Sektori tai teknologia	Algoritmin kuvaus	Syrjivän käytännön kuvaus	Lähde
Pankkitoiminta	Luottokelpoisuuden "pisteytys" tai arviointi	Automaattisen päätöksenteon järjestelmä sisälsi sääntöjä, joiden perusteella se päätti, ettei "40-vuotias nainen" ollut luottokelpoinen.	Algorithm Watch (2022) (s. 6) (vastaa tapausta Suomessa, saatavilla osoitteessa algorithmwatch.org)
Koulutus	Kurssin tai tutkinnon suorittamisen ennustava algoritmi	Aliedustetut vähemmistöryhmät saivat jatkuvasti korkeamman riskiarvion lisäksi matalammat tarkkuuspisteet.	Bird, Castleman ja Song (2024)
Kasvontunnistus-teknologia	Teknologia, joka voi tunnistaa tai kohdistaa kasvokuvia	Eri väestöryhmien, kuten ikään, sukupuoleen ja ihonväriin perustuvien välillä on tarkkuuseroja. Nämä erot voivat johtaa syrjintätapauksiin. Alankomaiden yhdenvertaisuuselin totesi, että organisaatioiden on todistettava, ettei teknologia ole syrjivää, eli todistustaakka on käänteinen.	College voor de Rechten van de Mens (2023)
Terveysterveystuho	Algoritmi, joka kohdistaa potilaille "tarvittavan hoidon"	Mielivaltainen pistejärjestelmä, joka johtaa tuntien erilaiseen kohdentamiseen samankaltaisissa tapauksissa.	The Guardian (2021)
Asuminen	Vuokralaisten seulonta-algoritmit, riskipisteytyksen määrittäminen	Vuokralaisten seulonta sellaisien ominaisuuksien perusteella, joiden ei ole osoitettu liittyvän riskiin.	Smith ja Vogell (2022)
Vakuutusala	Hinnoittelualgoritmi	Välitöntä syrjintää, koska kansalaisuus/kansallisuus vaikutti ajoneuvovakuutuksen hintaan muutoin identtisisissä profileissa.	Boscarol (2022)

Sektori tai teknologia	Algoritmin kuvaus	Syrjivän käytännön kuvaus	Lähde
Muuttoliikkeen hallinta ja rajavalvonta	Matkustus-asiakirjojen tarkistus, kasvontunnistusteknologia	Välitöntä syrjintää, koska teknologia antoi väärän tuloksen useammin tummaihoisten kuin vaaleaihoisten kuville.	Ahmed (2020)
Oikeusjärjestelmä / lasten ja nuorten hyvinvointi	Rikoksen uusimisen riskin arviointi	Tietyt kansallisuudet johtivat korkeampiin riskipisteisiin, mikä lisäsi syytteen nostamisen todennäköisyyttä.	Schot ja Davidson (2025)
Poliisitoiminta/lainvalvonta	Rikoksen uusimisen riskinarviointi	Tekoälyjärjestelmän avoimuudessa, selitettävyydessä ja vakaudessa oli puutteita. Epäjohdonmukaiset ja korkeammat riskipisteet henkilöillä, joilla ei ole ”sosiaalisen vakauden tekijöitä”, enimmäkseen nuoremmilla henkilöillä.	Eticas Foundation (2024)
Sosiaali-turvaetuudet	Virheellisten tai vilpillisten lastenhoitoetus-hakemusten havaitseminen	Etninen profilointi, jossa muiden kuin alankomaalaisten henkilöiden hakemuksille annettiin jatkuvasti korkeammat riskipisteet.	Amnesty International (2021)
Sosiaali-turvaetuudet	Sosiaalitukijärjestelmä, joka pahensi syrjäytymistä	Välillistä syrjintää sellaisen näennäisesti neutraalin perusteen kautta, joka asettaa suojatut ryhmät epäedulliseen asemaan.	Amnesty International (2023)
Sosiaali-turvapetosten havaitseminen	Petosriskin pisteytysjärjestelmää käytettiin sosiaali-turvaetuuksien saajien tunnistamiseen jatkotarkastuksia varten	Malli merkitsi suhteettomasti epäilyttäviksi naiset, maahanmuuttajat, pienituloiset sekä henkilöt, joilla ei ollut korkeakoulutusta.	Lighthouse Reports (2024)
Sosiaali-turvapetosten havaitseminen	Petosriskin pisteytysjärjestelmää käytettiin sosiaali-turvaetuuksien saajien tunnistamiseen jatkotarkastuksia varten (CNAF)	Järjestelmää vastustettiin, koska se aiheutti välittömiä ja välillisiä syrjiviä vaikutuksia naisille, vammaisille ja köyhyydessä asuville henkilöille.	La Quadrature du Net (2024) Lighthouse Reports (2023)

Liite E

Sijaismuuttajat

Datatieteen/-analyysin näkökulmasta sijaismuuttajat korvaavat muita muuttujia. Tämä tarkoittaa esimerkiksi muuttujia, joita ei voida havaita tai mitata suoraan. Sijaismuuttajien avulla saatetaan tehdä johtopäätöksiä tietyistä ominaisuuksista ilman, että kyseisiä ominaisuuksia on kirjattu tietoihin suoraan. Esimerkiksi ”30 vuoden työkokemus” viittaa siihen, että henkilön on oltava vähintään 45 vuoden ikäinen (Algorithm Watch, 2022).

Syrjimättömyyslainsäädännön ja algoritmi-/tekoälyjärjestelmien yhteydessä ”sijaismuuttajat” viittaavat ominaisuuksiin, piirteisiin tai niiden yhdistelmiin, joita ei itsessään ole mainittu nimenomaisesti kiellettyjen syrjintäperusteiden joukossa sovellettavassa lainsäädännössä, mutta jotka korreloivat näiden perusteiden kanssa siten, että niiden käyttö voi johtaa laittomaan syrjintään.

Tässä suhteessa voidaan tunnistaa kaksi erilaista sijaismuuttajien tyyppiä.

- a. Tilastolliset sijaismuuttajat: ominaisuudet (tai niiden yhdistelmät), jotka korreloivat kiellettyjen syrjintäperusteiden kanssa ja joiden käyttö voi asettaa suojattuun ryhmään kuuluvat henkilöt suhteettomasti epäedulliseen asemaan. Tällaiset sijaismuuttajat liittyvät yleensä välilliseen syrjintään. Esimerkiksi useimmissa Euroopan maissa koulutustason ja rodun tai etnisen alkuperän välillä on korrelaatio.
- b. Erottamattomasti syrjintäperusteisiin liittyvät sijaismuuttajat: ominaisuus (tai ominaisuuksien yhdistelmä), joka on erottamattomasti sidoksissa kiellettyyn syrjintäperusteeseen siten, että sen käyttö heijastaa luonnostaan syrjivää käytäntöä. Näihin sijaismuuttajiin liittyy tyypillisesti välitöntä syrjintää. Esimerkiksi raskautta on pidetty erottamattomasti sukupuoleen liittyvänä (katso alta taulukko 8).

Vaikka on edelleen epäselvää, kuinka läheinen vastaavuus sijaismuuttujan ja suojatun ryhmän välillä tulisi olla, jotta kyseessä olisi välitön syrjintä, erottamaton yhteys ei edellytä täyttä (100 %) vastaavuutta (Parviainen, 2024). Adams-Prassl, Binns ja Kelly-Lyth ovat todenneet, että tarvitaan vain riittävä vastaavuus (2023), kun taas Weerts et al. (2024) ovat ehdottaneet, että sijaismuuttujan ja kielletyn syrjintäperusteiden tulisi olla ainakin vahvasti ja mahdollisesti jopa deterministisesti yhteydessä toisiinsa. Weerts et al. huomauttavat myös niin sanotun ”jos näin ei olisi” -kysymyksen tärkeydestä: jos kantaja esimerkiksi asuu maassa, jossa eläkeikä perustuu sukupuoleen, hän voi kohtuudella väittää, että hän olisi saavuttanut eläkeiän, jos hänen sukupuolensa olisi eri. Samoin samaa sukupuolta oleva pari, joka asuu samaa sukupuolta olevien henkilöiden avioliitot kieltävässä maassa, voi väittää, että he olisivat voineet mennä naimisiin, jos heidän seksuaalinen suuntautumisensa olisi erilainen. Vastaavasti nainen voi kohtuudella väittää, ettei hän olisi raskaana, jos hänen sukupuolensa olisi eri, ja musliminainen voi väittää, ettei hän käyttäisi huivia, jos hänen uskontonsa olisi eri.

Se, onko tiettyssä tapauksessa olemassa erottamaton yhteys, edellyttää tapauskohtaista oikeudellista arviointia, jossa kontekstuaalisille kriteereille – tarkkojen tilastollisten kynnysarvojen sijaan – annetaan erityinen painoarvo EUT:n syrjintätapauksissa noudattaman lähestymistavan mukaisesti (katso esimerkiksi IX v. *WABE eV* ja *MH Müller Handels GmbH v. MJ*, 78 kohta, jossa painoarvoa annettiin kyseessä olevien merkkien tyypille). Katso alta taulukosta esimerkkejä erityyppisistä kiellettyjen syrjintäperusteiden sijaismuuttujista.

Taulukko 8: Esimerkkejä tunnetuista sijaismuuttujista (kuten muun muassa CRM, 2025, Weerts et al., 2024, ja Algorithm Watch, 2022, ovat maininneet)

Ominaisuus	Sijaismuuttuja perusteelle	Sijaismuuttujan tyyppi
30 vuoden työkokemus (Algorithm Watch, 2022)	Henkilö on yli 45-vuotias	Erottamattomasti yhteydessä toisiinsa
Raskaus (<i>Dekker v. Stichting voor Jong Volwassenen (VJV-Centrum) Plus</i> , 1990)	Sukupuoli	Erottamattomasti yhteydessä toisiinsa
Siviilisääty (<i>Tadao Maruko v. Versorgungsanstalt der deutschen Bühnen</i> , 2008; <i>Frédéric Hay v Crédit Agricole mutuel de Charente Maritime et des Deux-Sèvres</i> , 2012)	Seksuaalinen suuntautuminen maissa, jotka eivät salli samaa sukupuolta olevien avioliittoa	Erottamattomasti yhteydessä toisiinsa maissa, jotka eivät salli samaa sukupuolta olevien avioliittoa
Sukupuoleen perustuva eläkeikä (<i>James v. Eastleigh Borough Council</i> , 1990, 10 kohta)	Sukupuoli	Erottamattomasti yhteydessä toisiinsa
Kieli tai kielitaitotaso	Rotu	Tilastollinen sijaismuuttuja tai erottamattomasti liittyvä
Lukutaito	Rotu (maasta riippuen tämä voi olla myös iän ja sukupuolen sijaismuuttuja)	Tilastollinen sijaismuuttuja
Koulutustaso	Rotu, etninen alkuperä	Tilastollinen sijaismuuttuja
Postinumero tai naapurusto	Rotu (esimerkiksi eriytetyt naapurustot)	Tilastollinen sijaismuuttuja
Tulot	Rotu, sukupuoli	Tilastollinen sijaismuuttuja

Ominaisuus	Sijaismuuttuja perusteelle	Sijaismuuttujan tyyppi
Kotitalouden henkilöiden tai lähisukulaisten lukumäärä	Rotu (sukupuoli)	Tilastollinen sijaismuuttuja
Syntymäpaikka	Rotu	Tilastollinen sijaismuuttuja
Välttämättömien taloudellisten etuuksien saaminen	Rotu	Tilastollinen sijaismuuttuja
Uskonto	Rotu	Tilastollinen sijaismuuttuja
Nimet, jotka sisältävät tietyn kirjainyhdistelmän tai alkavat sillä tai päättyvät siihen	Rotu	Tilastollinen sijaismuuttuja
Poissaolot töistä / myöhäiset peruutukset / vähentynyt käytettävyys (<i>Filcams Cgil Bologna ym v. Deliveroo Italia S.R.L.</i> , 2020)	Vakaumus (ammattiliiton jäsenyys), sukupuoli-identiteetti tai terveydentila	Tilastollinen sijaismuuttuja
Vaatteet ja päähineet (kuten huivin käyttö) (<i>IX v. WABE ja MH Müller Handels</i> , 2021)	Uskonto ja vakaumus	Tilastollinen sijaismuuttuja (viittaa esimerkiksi poliittisiin, filosofisiin tai uskonnollisiin vakaumuksiin liittyviin merkkeihin) tai erotamattomasti syrjintäperusteeseen liittyvä (viittaa nimenomaisesti esimerkiksi selvästi huomattaviin, merkittäviin merkkeihin)

Liite F

Luettelo tekoäly- ja algoritmirekistereistä Euroopassa

Maan- tieteellinen soveltamisala	Nimi	Soveltamisala	Linkki	Päivityk- sen päivä- määrä
Belgia	BoSA AI Observatory	Luettelo kaikista tunnetuista tekoälysovelluk- sista ja -hank- keista, joita liittovaltion insti- tuutiot ja virastot käyttävät	https://bosa.belgium.be/fr/themes/administration-numerique/cooperation-et-partage-des-connaissances/cooperation-nationale-5	
Suuririskisiä tekoäly- järjestelmiä koskeva EU:n tietokanta – tulossa		Suuririskiset tekoäly- järjestelmät		
Jokainen EU-maa – tulossa		Kriittiseen infra- struktuuriin liittyvät suuri- riskiset tekoäly- järjestelmät		
EU	Selected AI cases in the public sector	Tekoäly julkisella sektorilla	Joint Research Centre Data Catalogue – Selected AI cases in the public sector (JRC129301), Euroopan komissio	31. joului- kuuta 2021
EU	Public Sector Tech Watch	Seurantakeskus, joka on omis- tautunut uusien teknologioiden käytön seuran- taan, analysoin- tiin ja tunnetuksi tekemiseen	https://interoperable-europe.ec.europa.eu/collection/public-sector-tech-watch	

Maan-tieteellinen soveltamisala	Nimi	Soveltamisala	Linkki	Päivityksen päivämäärä
Saksa			Use Case Platform – Applied AI Institute	
Helsinki	Helsingin kaupungin tekoälyjärjestelmät	Tekoäly julkisella sektorilla	Tekoälyrekisteri – Helsingin kaupungin tekoälyrekisteri	Jatkuvat päivitykset
Alankomaat	The Algorithm Register of the Dutch Government	Algoritmi-järjestelmät julkisella sektorilla	The Algorithm Register of the Dutch Government	Jatkuvat päivitykset
Yhdistynyt kuningaskunta	Algorithmic transparency standards recording hub	Yhdistyneen kuningaskunnan hallitus (vapaaehtoinen standardi)	Find out how algorithmic tools are used in public organisations – GOV.UK	Jatkuva
Yhdistynyt kuningaskunta	Non-governmental register: Public Law Project Tracking Automated Government (TAG) Register		TAG Register	Jatkuva

Liite G

Syrjimättömyysdirektiivit, kielletyt syrjintäperusteet ja soveltamisala

Direktiivi	Kielletyt syrjintäperusteet	Soveltamisala	Direktiivit yhdenvertaisuuselimää koskevista normeista
2000/43/EY (rodusta riippumatonta yhdenvertaista kohtelua koskeva direktiivi)	Rotu ja etninen alkuperä – ei kansalaisuus, eikä rajoita kolmansien maiden kansalaisten ja kansalaisuudettomien henkilöiden oikeudelliseen asemaan perustuvaa kohtelua	Työllistäminen, ammatillinen koulutus, sosiaaliturva, yleissivistävä koulutus, tavarat ja palvelut, mukaan lukien asuminen	2024/1499
Direktiivi 2000/78/EY	Uskonto tai vakaumus, vammaisuus, ikä, seksuaalinen suuntautuminen	Työllistäminen ja ammatti	2024/1499
Direktiivi 2004/113/EY (direktiivi miesten ja naisten yhdenvertaisen kohtelun periaatteen täytäntöönpanosta tavaroiden ja palvelujen saatavuuden ja tarjonnan alalla)	Sukupuoli	Tavarat ja palvelut	2024/1499

Direktiivi	Kielletyt syrjintäperusteet	Soveltamisala	Direktiivit yhdenvertaisuuselimä koskevista normeista
Direktiivi 2006/54/EY (uudelleenlaadittu toisinto miesten ja naisten yhtäläisten mahdollisuuksien ja yhdenvertaisen kohtelun periaatteen täytäntöönpanosta työhön ja ammattiin liittyvissä asioissa)	Sukupuoli (mukaan lukien raskaus ja äitiys)	Työllistäminen ja ammatti (mukaan lukien sosiaaliturvajärjestelmät)	2024/1500
2010/41/EU (direktiivi miesten ja naisten tasa-arvoisen kohtelun periaatteen soveltamisesta itsenäisiin ammatinharjoittajiin)	Sukupuoli	Yrittäjät ja heidän puolisonsa tai kumppaninsa	2024/1500
2023/970/EU, palkkauksen läpinäkyvyyttä koskeva direktiivi (saatettava osaksi kansallista lainsäädäntöä kesäkuuhun 2026 mennessä)	Sukupuoli (mukaan lukien raskaus ja vanhemmuus), ja sukupuolen ja minkä tahansa muun syrjintäperusteen yhdistelmä	Työllistäminen	2024/1500 (huomioitava, ettei tämä rajoita itse direktiivissä säädettyjen tarkempien säännösten soveltamista)

Liite H

Muut mahdollisesti asiaankuuluvat asetukset ja ohjeet

Euroopan neuvosto

Syrjimättömyys

Ministerikomitean suositus CM/Rec(2019)1 jäsenvaltioille seksimin ehkäisemisestä ja torjumisesta: <https://search.coe.int/cm?i=090000168093b26a>.

Ministerikomitean suositus CM/Rec(2020)1 jäsenvaltioille algoritmijärjestelmien ihmisoikeusvaikutuksista (hyväksytty Euroopan neuvoston ministerikomiteassa 8. huhtikuuta 2020 ministerien sijaisten 1373. kokouksessa): <https://search.coe.int/cm?i=09000016809e1154>.

Ministerikomitean suositus CM/Rec(2026)1 yhdenvertaisuudesta ja tekoälystä (GEC/ADI-AI, Euroopan neuvoston tasa-arvokomitea ja syrjinnän torjuntaa, monimuotoisuutta ja osallisuutta käsittelevä ohjauskomitea): <https://search.coe.int/cm?i=09125948802acd7f>.

Tutkimukset/raportit

Tekoälyn aiheuttamaa syrjintää koskeva Report on preventing discrimination caused by the use of artificial intelligence – Euroopan neuvoston parlamentaarinen yleiskokous, yhdenvertaisuutta ja syrjimättömyyttä käsittelevä komitea, esittelijä: Christophe Lacroix (Belgia, SOC), 29. syyskuuta 2020: <https://pace.coe.int/en/files/28807>.

Shrishak, Kris ja Pénicaud, Soizic (2025): Oikeussuoja algoritmista syrjintää vastaan Euroopassa: nykyiset puitteet ja jäljellä olevat puutteet (saatavilla englannin lisäksi myös ranskaksi, hollanniksi, portugaliksi, suomeksi ja ruotsiksi). Saatavilla osoitteessa <https://www.coe.int/en/web/inclusion-and-antidiscrimination/upholding-equality-and-non-discrimination-by-equality-bodies-regarding-the-use-of-artificial-intelligence-ai-in-public-administrations1> (viitattu 4. elokuuta 2026).

Syrjintää, tekoälyä ja algoritmista päätöksentekoa koskeva Study on discrimination, artificial intelligence and algorithmic decision making – ECRI, marraskuu 2018: <https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73>.

Tekoälyjärjestelmien vaikutuksia, yhdenvertaisuuden edistämistä ja syrjintäriskejä käsittelevä Study on the impact of artificial intelligence systems, their potential for promoting equality, including gender equality, and the risks they may cause in relation to non-discrimination – GEC/CDADI, elokuu 2023: <https://rm.coe.int/prems-112923-gbr-2530-etude-sur-l-impact-de-ai-web-a5-1-2788-3289-7544/1680ac7936>.

Xenidis, Raphaële (2025): Tekoälyä ja algoritmiperusteista syrjintää koskevat eurooppalaiset suuntaviivat yhdenvertaisuuselimille ja muille kansallisille ihmisoikeustoimijoille (saatavilla englannin lisäksi myös ranskaksi, hollanniksi, portugaliksi, suomeksi ja ruotsiksi), Euroopan neuvosto. Saatavilla osoitteessa <https://www.coe.int/en/web/inclusion-and-antidiscrimination/upholding-equality-and-non-discrimination-by-equality-bodies-regarding-the-use-of-artificial-intelligence-ai-in-public-administrations1> (viitattu 4. elokuuta 2026).

Sukupuoli

Ministerikomitean suositus CM/Rec(2026)2 naisiin ja tyttöihin kohdistuvan teknologian avulla tapahtuvan väkivallan vastuusta: [https://search.coe.int/cm/#{%22CoEIdentifier%22:\[%2209125948802acd83%22\],%22sort%22:\[%22CoEValidationDate%20Descending%22\]}](https://search.coe.int/cm/#{%22CoEIdentifier%22:[%2209125948802acd83%22],%22sort%22:[%22CoEValidationDate%20Descending%22]}).

Oikeus ja täytäntöönpano

Arviointiväline, joka koskee tekoälyn käyttöä oikeusjärjestelmissä ja niiden toimintaympäristössä käsittelevän eurooppalaisen eettisen peruskirjan käyttöönottoa – CEPEJ(2023)16Final: <https://rm.coe.int/cepej-2023-16final-operationalisation-ai-ethical-charter-en/1680adcc9c>.

Eurooppalainen eettinen peruskirja tekoälyn käytöstä oikeusjärjestelmissä ja niiden toimintaympäristössä – CEPEJ(2018)14: <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c>.

Kasvontunnistusta koskevat suuntaviivat, yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä tehdyn yleissopimuksen neuvoa-antava komitea, yleissopimus 108, 28. tammikuuta 2021: <https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3>.

Hyvinvointi ja sosiaalinen turvaverkko

Ministerikomitean Decl(17/03/2021)2 – Declaration by the Committee of Ministers on the risks of computer-assisted or artificial-intelligence-enabled decision making in the field of the social safety net (hyväksytty Euroopan neuvoston ministerikomiteassa 17. maaliskuuta 2021 ministerien sijaisten 1399. kokouksessa) <https://search.coe.int/cm?i=0900001680a1cb98>.

Koulutus

Havinga, Beth, Holmes, Wayne ja Persson Jen (2024), Regulating the use of Artificial Intelligence Systems in Education: Preparatory study on the development of a legal instrument. Saatavilla osoitteessa <https://www.coe.int/en/web/education/-/regulating-the-use-of-artificial-intelligence-systems-in-education>.

Kansainvälisten kansalaisjärjestöjen konferenssin hyväksymä suositus Recommendation on the impact of artificial intelligence (AI) on the education sector – CONF-AG(2023)REC4. Saatavilla osoitteessa <https://rm.coe.int/conf-ag-2023-rec4-draft-recommendation-on-the-impact-of-artificial-int/1680ac8e25>.

Muuttoliike, maahanmuutto ja turvapaikka-asiat

Ministerikomitean suositus CM/Rec(2022)17 jäsenvaltioille siirtolais-, pakolais- ja turvapaikanhakijanaisten ja -tyttöjen oikeuksien suojelemisesta (erityisesti kohdat 5–8 ja 22–25): <https://rm.coe.int/prems-092222-gbr-2573-recommandation-cm-rec-2022-17-a5-bat-web-1-/1680a6ef9a>.

Katso myös: Yhdistyneen kuningaskunnan IT Flows policy brief:
<https://bura.brunel.ac.uk/handle/2438/27982>.

Liite I

Suuririskiset tekoälyyn liittyvät käytännöt

Suuririskinen ala	Käyttötapaus
1. Biometriikka	Biometriset etätunnistusjärjestelmät, ei sisällä todentamista
	Biometrinen luokittelu arkaluonteisten tai suojattujen ominaisuuksien tai ominaispiirteiden mukaisesti kyseisten ominaisuuksien tai ominaispiirteiden päättelyn perusteella
	Tunteiden tunnistaminen
2. Kriittinen infrastruktuuri	Kriittisen infrastruktuurin hallinnan ja käytön turvakomponentit
3. Yleissivistävä ja ammatillinen koulutus	Sisään pääsyn tai hyväksymisen määrittäminen tai yksilöiden osoittaminen tietylle koulutustasolle
	Oppimistulosten arviointi ja/tai oppimisprosessin ohjaaminen yleissivistävässä tai ammatillisessa koulutuksessa
	Sopivan koulutustason arviointi
	Opiskelijoiden kielletyn käyttäytymisen tarkkailu tai havaitseminen kokeiden aikana
4. Työllistäminen, henkilöstöhallinto ja itsenäisen ammatinharjoittamisen mahdollistaminen	Luonnollisten henkilöiden rekrytointi tai valinta, kohdennetut työpaikkailmoitukset tai hakijoiden/työhakemusten arviointi
	Työhön liittyvien sopimussuhteiden päätökset (kuten ylennykset), tehtävien jako sekä suorituksen seuranta tai arviointi
5. Välttämättömien palvelujen saatavuus ja käyttö	Sen arviointi, ovatko luonnolliset henkilöt oikeutettuja julkisen avun etuuksiin ja palveluihin
	Luottokelpoisuuden arviointi tai luottopisteytyksen määrittäminen, lukuun ottamatta talouspetoksia
	Riskinarviointi ja hinnoittelu henki- ja sairausvakuutuksissa
	Hätäpuheluiden arviointi ja/tai luokittelu pelastus- ja ensihoitopalvelujen lähettämiseksi tai tärkeysjärjestyksen määrittämiseksi sekä kiireellistä sairaanhoitoa tarvitsevien potilaiden luokittelu

Suuririskinen ala	Käyttötapaus
6. Lainvalvonta	Rikoksen uhriksi joutumisen riskin arviointi
	Valheenpaljastimet tai vastaavat välineet
	Todistusaineiston luotettavuuden arviointi
	Rikokseen tai rikoksen uusimiseen syyllistymisen riskin tai persoonallisuuspiirteiden tai aiemman rikollisen käyttäytymisen arviointi
	Avustaminen rikosten paljastamisen, tutkimisen tai rikoksiin liittyvien syytetoimien yhteydessä
7. Muuttoliikkeen hallinta, turvapaikka-asiat ja rajavalvonta	Valheenpaljastimet tai vastaavat välineet
	Jäsenvaltion alueelle tulevan henkilön aiheuttaman riskin, mukaan lukien turvallisuusriskin, sääntöjenvastaisen maahanmuuton riskin ja terveysriskin, arviointi
	Turvapaikka-, viisumi- ja oleskelulupahakemusten ja niihin liittyvien valitusten käsittely asemaa hakevien luonnollisten henkilöiden kelpoisuuden tarkastamiseksi
	Luonnollisten henkilöiden havaitseminen, tunnistaminen tai henkilöllisyyden määrittäminen, pois lukien (matkustusasiakirjojen) tarkastaminen
8. Oikeudenhoidon ja demokraattiset prosessit	Oikeusviranomaisen avustaminen lainsäädännön tutkimisessa ja tulkinnassa sekä lainsäädännön soveltamisessa konkreettisiin tosiseikkoihin
	Järjestelmät, joiden tarkoituksena on vaikuttaa äänestyskäyttäytymiseen vaaleissa ja/tai kansanäänestyksissä

Huomio: komissio on julkaissut suuririskisten tekoälyjärjestelmien luokittelua koskevien suuntaviivojen luonnoksen, ja sen kuulemisprosessi jatkuu kesäkuuhun 2026 saakka.⁶³

63. Katso lisätietoja: [Commission seeks feedback on the draft guidelines for the classification of high-risk artificial intelligence systems, Shaping Europe's digital future](#), viitattu 5. kesäkuuta 2026.

Liite J

Kielletyt tekoälyyn liittyvät käytännöt

Taulukko 9. Luettelo tekoälyjärjestelmien käytön kielletyistä käytännöistä

Kielletty käytäntö	Tekoäly-asetuksen artikla	Tekoäly-asetuksen johdanto-osan kappale
Tarkoituksellisesti manipuloivat tai harhaanjohtavat tekniikat, joiden tavoitteena on vääristää henkilön käyttäytymistä heikentäen tuntuvasti tämän kykyä tehdä tietoinen päätös ja saaden tämän tekemään päätöksen, joka kohtuullisella todennäköisyydellä aiheuttaa merkittävää haittaa. Tämä kattaa myös ilman suostumusta tuotetun seksuaalisen ja intiimin sisällön tai lasten seksuaalista hyväksikäyttöä esittävän aineiston (CSAM).	5 artiklan 1 kohdan a, ba ja bb alakohta; 5 artiklan 1a ja 1b kohta	Johdanto-osan kappale 29
Sellaisten haavoittuvuuksien hyödyntäminen, jotka liittyvät henkilön ikään, vammaan tai erityiseen sosiaaliseen tai taloudelliseen tilanteeseen, siten, että tavoitteena tai vaikutuksena on olennaisesti vääristää käyttäytymistä tavalla, joka kohtuullisella todennäköisyydellä aiheuttaa merkittävää haittaa.	5 artiklan 1 kohdan b alakohta	Johdanto-osan kappale 29
Luonnollisten henkilöiden tai henkilöryhmien arviointi tai luokittelu tiettyä ajanjaksona heidän sosiaalisen käyttäytymisensä tai tunnettujen, pääteltyjen tai ennakoitujen henkilökohtaisten ominaisuuksiensa tai luonteenpiirteidensä perusteella siten, että sosiaalinen pisteytys johtaa jompaankumpaan tai molempiin seuraavista: – epäedullinen kohtelu sosiaalisissa yhteyksissä, jotka eivät liity siihen asiayhteyteen, jossa tiedot alun perin tuotettiin tai kerättiin – epäedullinen kohtelu, joka on perusteetonta tai suhteetonta.	5 artiklan 1 kohdan c alakohta	Johdanto-osan kappale 31
Riskinarviointien tekeminen, jotta voidaan arvioida tai ennustaa sen riskiä, että luonnollinen henkilö syyllistyy rikokseen, kun tämä perustuu yksinomaan luonnollisen henkilön profilointiin.	5 artiklan 1 kohdan d alakohta	Johdanto-osan kappale 42

Kielletty käytäntö	Tekoäly-asetuksen artikla	Tekoäly-asetuksen johdanto-osan kappale
Kasvontunnistustietokantojen luominen tai laajentaminen haravoimalla kasvokuvia kohdentamattomasti internetistä tai valvontakamerakuvista.	5 artiklan 1 kohdan e alakohta	Johdanto-osan kappale 43
Tunteiden päätteleminen työpaikalla ja oppilaitoksissa, paitsi jos käyttöä on tarkoitus hyödyntää lääketieteellisiin tai turvallisuuteen liittyviin tarkoituksiin.	5 artiklan 1 kohdan f alakohta	Johdanto-osan kappale 44
Biometriset luokittelujärjestelmät, joissa luonnolliset henkilöt luokitellaan heidän biometristen tietojensa perusteella rodun, poliittisten mielipiteiden, ammattiliiton jäsenyyden, uskonnollisen tai filosofisen vakaumuksen, seksuaalisen käyttäytymisen tai seksuaalisen suuntautumisen perusteella.	5 artiklan 1 kohdan g alakohta	Johdanto-osan kappale 30
Reaaliaikaisten biometristen etätunnistusjärjestelmien käyttö julkisissa tiloissa lainvalvontatarkoituksessa, paitsi jos ja siltä osin kuin se on ehdottoman välttämätöntä lainvalvontatarkoituksiin (poikkeuksia sovelletaan).	5 artiklan 1 kohdan h alakohta	Johdanto-osan kappaleet 32, 33, 38, 39, 40 ja 41

Taulukko 10. Kielletyt tekoälykäytännöt voivat liittyä suuririskisiin tekoälyjärjestelmiin

Suuririskiset tekoälyjärjestelmät (Tekoälyasetuksen liite III, 6 artiklan 2 kohta)	Kielletty käytäntö (Tekoälyasetus, 5 artikla)	Esimerkkejä kielletyistä ja mahdollisesti kielletyistä käytötapauksista ja niiden selitykset
1. Biometriikka 1a) Biometriset etätunnistusjärjestelmät (RBI)	(h) Reaaliaikaisten biometrinen etätunnistusjärjestelmien käyttö julkisissa tiloissa lainvalvontatarkoituksessa, paitsi jos ja siltä osin kuin se on ehdottoman välttämätöntä jonkin seuraavan tavoitteen saavuttamiseksi: – kaappauksen uhrien kohdennettu etsintä – erityisen, merkittävän ja välittömän uhan ehkäiseminen – rikoksesta epäillyn henkilön paikantaminen tai tunnistaminen (liitteen II mukaisesti).	Keskeiset elementit: RBI-järjestelmien käyttö seuraavasti: – ”reaaliaikainen” tunnistus – julkiset tilat – lainvalvontaviranomaisten taholta tai puolesta. Johdanto-osan kappaleen 32 mukaan reaaliaikaisten RBI-järjestelmien käyttö ”synnyttää tunteen jatkuvasta valvonnasta ja estää välillisesti kokoontumisvapauden ja muiden perusoikeuksien käyttämisen”. Esimerkki: poliisi käyttää reaaliaikaista kasvontunnistusta valvontakamerakuvista tutkinnan kohteen tunnistamiseen ja pidättämiseen. Moskovan poliisi (<i>Glukhin v. Venäjä, 2024</i>) käytti valvontakamerakuvia rauhanomaisen mielenosoittajan tunnistamiseen ja paikantamiseen reaaliaikaisen biometrisen tunnistuksen avulla.

Suuririskiset tekoälyjärjestelmät (Tekoälyasetuksen liite III, 6 artiklan 2 kohta)	Kielletty käytäntö (Tekoälyasetus, 5 artikla)	Esimerkkejä kielletyistä ja mahdollisesti kielletyistä käyttötapauksista ja niiden selitykset
1a) Biometriset etätunnistusjärjestelmät (RBI)	(e) Kasvokuvien kohdentamaton haravointi tietokannan luomista tai laajentamista varten	Keskeiset elementit: menetelmä tunnistustietokannan luomiseksi tai laajentamiseksi kohdentamattomalla haravoinnilla itse tehdyn tunnistuksen sijaan. Tämä on kiellettyä, koska kohdentamaton haravointi toimii kuin ”pölynimuri”, sillä siinä kerätään kasvokuvia summittaisesti kohdistamatta niitä tiettyihin henkilöihin, kuten 5 artiklan 1 kohdan e alakohdassa on kuvattu. Johdanto-osan kappaleessa 43 perustelua täydennetään sillä, että tämä käytäntö ”lisää tunnetta joukkovalvonnasta” ja voi johtaa perusoikeuksien loukkauksiin. Esimerkki: rajavalvontaviranomaiset rakentavat kasvontunnistustietokantaa joukkoharavoinnin avulla Rajavalvontaviranomaiset saattavat haravoida kasvokuvia sosiaalisesta mediasta, uutisartikkeleista ja valvontakamerakuvista kohdistamatta niitä tiettyihin yksilöihin. Jos nämä kuvat sitten lisätään biometrisen tunnistuksen tietokantaan, kyseessä on 5 artiklan 1 kohdan e alakohdan mukainen kielletty käytäntö.

Suuririskiset tekoälyjärjestelmät (Tekoälyasetuksen liite III, 6 artiklan 2 kohta)	Kielletty käytäntö (Tekoälyasetus, 5 artikla)	Esimerkkejä kielletyistä ja mahdollisesti kielletyistä käytötapauksista ja niiden selitykset
1b) Biometrinen luokittelu suojattujen ominaisuuksien perusteella (tai niiden päättely)	(g) Biometriset luokittelujärjestelmät, joissa luonnolliset henkilöt luokitellaan rodun, poliittisten mielipiteiden, ammattiliiton jäsenyyden, uskonnollisen tai filosofisen vakaumuksen, seksuaalisen käyttäytymisen tai seksuaalisen suuntautumisen päättelyn perusteella	Keskeiset elementit: nimenomainen tarkoitus, jossa luetellut suojatut ominaisuudet (rotu, poliittiset mielipiteet, ammattiliiton jäsenyys, uskonto, seksuaalinen käyttäytyminen tai seksuaalinen suuntautuminen) päätellään biometrysten tietojen perusteella. Biometristä luokittelua pidetään jo itsessään suuririskisenä, ja 5 artiklan 1 kohdan g alakohdan mukaan biometrysten tietojen käyttö näiden ominaisuuksien päättämiseen on ehdottomasti kiellettyä. Esimerkki: tekoälyjärjestelmä, joka analysoi henkilön sosiaalisen median kuvia ja pääättelee hänen seksuaalisen suuntautumisensa biometrysten tietojen perusteella, jotta hänelle voidaan lähettää kohdennettua mainontaa.

Suuririskiset tekoälyjärjestelmät (Tekoälyasetuksen liite III, 6 artiklan 2 kohta)	Kielletty käytäntö (Tekoälyasetus, 5 artikla)	Esimerkkejä kielletyistä ja mahdollisesti kielletyistä käyttötapauksista ja niiden selitykset
1c) Tunteiden tunnistaminen	(f) Tunteiden tunnistaminen työpaikalla ja oppilaitoksissa (poikkeus: lääketieteelliset ja turvallisuustarkoitukset)	Keskeiset elementit: tunteiden tai aikomusten päättely työpaikan tai oppilaitoksen kontekstissa, jos tapaukseen ei liity lääketieteellisiä tai turvallisuusperusteita. 5 artiklan 1 kohdan f alakohdan mukaan tunteiden tunnistamiseen liittyvän suuririskisen käytännön käyttö näissä konteksteissa on kiellettyä. Myös johdanto-osan kappaleessa 44 korostetaan, että tällaiset järjestelmät voivat johtaa haitalliseen tai epäedulliseen kohteluun, kun otetaan huomioon vallan epätasapaino työelämässä tai koulutuksen alalla. Huomio: fyysisten oloilojen, kuten sen, onko bussikuljettaja väsynyt, tunnistaminen ei tämän mukaan ole kiellettyä. Esimerkki: tekoälyjärjestelmä, joka pääättelee, lähtevätkö työntekijät työpaikaltaan ”tyytyväisinä”, ”vihaisina” vai ”surullisina”. Työnantaja yrittää tunnistaa ravintolansa työntekijöiden tunteita valvontakamerakuvien perusteella.

Suuririskiset tekoälyjärjestelmät (Tekoälyasetuksen liite III, 6 artiklan 2 kohta)	Kielletty käytäntö (Tekoälyasetus, 5 artikla)	Esimerkkejä kielletyistä ja mahdollisesti kielletyistä käytötapauksista ja niiden selitykset
3) Yleissivistävä ja ammatillinen koulutus a) Sisään pääsyn/ hyväksymisen määrittäminen	(a) Manipuloivat tai harhaanjohtavat teknikat, joiden tavoitteena on vääristää henkilön käyttäytymistä heikentäen tuntuvasti tämän kykyä tehdä tietoinen päätös ja aiheuttaa haittaa	Keskeiset elementit: sellaisen manipuloivan tai harhaanjohtavan tekniikan käyttö, joka olennaisesti vääristää (tai kohtuullisen todennäköisesti vääristää) yksilön käyttäytymistä. 5 artiklan 1 kohdan a alakohdassa kielletään teknikat, joiden tavoitteena on vääristää tai jotka olennaisesti vääristävät henkilön käyttäytymistä heikentäen tuntuvasti tämän kykyä tehdä tietoinen päätös, joka aiheuttaa merkittävää haittaa. Huomautus: ei ole välttämätöntä, että tapaukseen liittyy nimenomainen tarkoitus, vaan pelkkä vaikutus riittää. Esimerkki: yliopisto käyttää hakuprosessissa chattibotti, joka esittää jäljellä olevien paikkojen määrän tai tekaistuja viestejä. Tämän artiklan nojalla chattibotti, joka käyttää pimeiksi kaavoiksi kutsuttuja tekniikoita, kuten ilmoitusta "Vain kolme paikkaa jäljellä!", kuuluu kiellettyihin käytäntöihin.

Suuririskiset tekoälyjärjestelmät (Tekoälyasetuksen liite III, 6 artiklan 2 kohta)	Kielletty käytäntö (Tekoälyasetus, 5 artikla)	Esimerkkejä kielletyistä ja mahdollisesti kielletyistä käytötapauksista ja niiden selitykset
3) Yleissivistävä ja ammatillinen koulutus b) Oppimistulosten arviointi ja oppimisprosessin ohjaaminen c) (Asianmukaisen) koulutustason arviointi d) Opiskelijoiden kielletyn käyttäytymisen tarkkailu/havaitseminen	(f) Tunteiden tunnistaminen työpaikalla ja oppilaitoksissa (poikkeus: lääketieteelliset ja turvallisuustarkoitukset)	Keskeinen elementti: opiskelijoiden tunnetilojen tai aikomusten ja niiden oppimisprosessivaikutusten päättely. Tekoälyjärjestelmiä voidaan käyttää opiskelijoiden arviointiin, mutta heidän tunteidensa tai aikomustensa tunnistaminen on kiellettyä. Johdanto-osan kappaleessa 44 korostetaan, että tällaiset järjestelmät voivat johtaa haitalliseen tai epäedulliseen kohteluun, kun otetaan huomioon vallan epätasapaino työelämässä tai koulutuksen alalla. Esimerkki: yliopisto käyttää mukautettua oppimisalustaa, joka ohjaa oppimisprosessia opiskelijoiden verkkokameroitten kautta verkkoluentojen aikana havaittujen tunteiden perusteella.

Suuririskiset tekoälyjärjestelmät (Tekoälyasetuksen liite III, 6 artiklan 2 kohta)	Kielletty käytäntö (Tekoälyasetus, 5 artikla)	Esimerkkejä kielletyistä ja mahdollisesti kielletyistä käytötapauksista ja niiden selitykset
4) Työllistäminen ja henkilöstöhallinto a) Rekrytointi (kohdennettu mainonta) tai valinta (työhakemusten arviointi)	(a) Manipuloivat tai harhaanjohtavat teknikat, joiden tavoitteena on vääristää henkilön käyttäytymistä heikentäen tuntuvasti tämän kykyä tehdä tietoinen päätös ja aiheuttaa haittaa (b) Haavoittuvuuden hyödyntäminen	Keskeiset elementit: sellaisen manipuloivan tai harhaanjohtavan tekniikan käyttö, joka olennaisesti vääristää (tai kohtuullisen todennäköisesti vääristää) yksilön käyttäytymistä 5 artiklan 1 kohdan a alakohdassa kielletään teknikat, joiden tavoitteena on vääristää tai jotka olennaisesti vääristävät henkilön käyttäytymistä heikentäen tuntuvasti tämän kykyä tehdä tietoinen päätös, joka aiheuttaa merkittävää haittaa. Huomautus: ei ole välttämätöntä, että tapaukseen liittyy nimenomainen tarkoitus, vaan pelkkä vaikutus riittää. Esimerkki: tekoälypohjainen rekrytointialusta, jolla käytetään tekaistua kiireellisyyttä ja harhaanjohtavaa manipulointia sopimusten allekirjoittamisen edistämiseen. Jos rekrytointitoimisto käyttää tekoälyjärjestelmää, jossa liioitellut palkat/etuudet tai kiireellisyys haittaavat tietoon perustuvaa päätöksentekoa, kyseessä on tämän artiklan mukaan kielletty käytäntö.

Suuririskiset tekoälyjärjestelmät (Tekoälyasetuksen liite III, 6 artiklan 2 kohta)	Kielletty käytäntö (Tekoälyasetus, 5 artikla)	Esimerkkejä kielletyistä ja mahdollisesti kielletyistä käytötapauksista ja niiden selitykset
4) Työllistäminen ja henkilöstöhallinto b) Työhön liittyvien sopimussuhteiden päätökset, kuten irtisanominen, tai tehtävien jako	(a) Manipuloivat tai harhaanjohtavat teknikat, joiden tavoitteena on vääristää henkilön käyttäytymistä heikentäen tuntuvasti tämän kykyä tehdä tietoinen päätös ja aiheuttaa haittaa (b) Haavoittuvuuden hyödyntäminen	Keskeiset elementit: sellaisen manipuloivan tai harhaanjohtavan tekniikan käyttö, joka olennaisesti vääristää (tai kohtuullisen todennäköisesti vääristää) yksilön käyttäytymistä. 5 artiklan 1 kohdan a alakohdassa kielletään teknikat, joiden tavoitteena on vääristää tai jotka olennaisesti vääristävät henkilön käyttäytymistä heikentäen tuntuvasti tämän kykyä tehdä tietoinen päätös, joka aiheuttaa merkittävää haittaa. Huomautus: ei ole välttämätöntä, että tapaukseen liittyy nimenomainen tarkoitus, vaan pelkkä vaikutus riittää. Esimerkki: logistiikkayritys ottaa käyttöön tekoälyjärjestelmän, joka jakaa kuljetustehtäviä ja seuraa kuljettajien suoritusta. Tällainen järjestelmä voi vääristää kuljettajien käyttäytymistä niin, että he työskentelevät laillisia työaikoja pidempään, mikä voi vaikuttaa terveyteen ja turvallisuuteen ja aiheuttaa merkittävää haittaa. Tällainen järjestelmä kuuluisi täten kiellettyihin käytäntöihin.

Suuririskiset tekoälyjärjestelmät (Tekoälyasetuksen liite III, 6 artiklan 2 kohta)	Kielletty käytäntö (Tekoälyasetus, 5 artikla)	Esimerkkejä kielletyistä ja mahdollisesti kielletyistä käytötapauksista ja niiden selitykset
4) Työllistäminen ja henkilöstöhallinto b) Työhön liittyvien sopimussuhteiden päätökset, kuten irtisanominen, tai tehtävien jako	(f) Tunteiden ja/tai aikomusten tunnistaminen työpaikalla ja oppilaitoksissa	Keskeinen elementti: työntekijöiden tunnetilojen tai aikomusten ja niiden työskentelyvaikeutusten päättely Tekoälyjärjestelmiä voidaan käyttää päätöksenteon apuna. Tunteiden tunnistamiseen perustuva apu on kuitenkin kiellettyä. Johdanto-osan kappaleessa 44 korostetaan, että tällaiset järjestelmät voivat johtaa haitalliseen tai epäedulliseen kohteluun, kun otetaan huomioon vallan epätasapaino työelämässä tai koulutuksen alalla. Esimerkki: tekoälyä työntekijöiden valvontaan käyttävä puhelinalvelukeskus käyttää työntekijöiden tunnetilaa suorituskyvyn arviointiin. Jos tässä esimerkissä tekoälyjärjestelmä päättelisi työntekijän tunnetiloja äänitallenteiden perusteella ja ottaisi tämän huomioon suoritusarvioinnissa, kyseessä olisi kielletty käytäntö.

Suuririskiset tekoälyjärjestelmät (Tekoälyasetuksen liite III, 6 artiklan 2 kohta)	Kielletty käytäntö (Tekoälyasetus, 5 artikla)	Esimerkkejä kielletyistä ja mahdollisesti kielletyistä käytötapauksista ja niiden selitykset
5) Välttämättömien palvelujen ja etuuk-sien saatavuus ja käyttö a) Sen arviointi, ovatko luonnolliset henkilöt oikeutettuja välttämättömiin etuuk-siin ja palveluihin	(c) Sosiaalinen pisteytys, joka johtaa epäsuotuisaan kohteluun – yhteyksissä, jotka eivät liity siihen asiayhteyteen, jossa tiedot alun perin kerättiin ja/tai – kohtelu on perustee-tonta tai suhteetonta	Keskeiset elementit: epäedullinen kohtelu sosiaalisissa yhteyksissä, jotka eivät liity siihen asiayhteyteen, jossa tiedot alun perin tuotettiin tai kerättiin, ja/tai kohtelu on perusteetonta tai suhteetonta. Jos tekoälyjärjestelmää käytetään henkilön kelpoisuuden arviointiin, tietoja ei välttämättä oteta eri kontekstista. Esimerkki: viranomaiset ottavat käyttöön tekoälyjärjestelmän, joka myöntää etuuksia henkilöille käyttäen tietoja, jotka eivät liity tähän asiayhteyteen. Näissä kielletyissä tapauksissa on tärkeää, että tietojen keräyskon-teksti poikkeaa olennaisesti niiden käyttökontekstista.

Suuririskiset tekoälyjärjestelmät (Tekoälyasetuksen liite III, 6 artiklan 2 kohta)	Kielletty käytäntö (Tekoälyasetus, 5 artikla)	Esimerkkejä kielletyistä ja mahdollisesti kielletyistä käytötapauksista ja niiden selitykset
5b) Luottokelpoisuuden arviointi	(c) Sosiaalinen pisteytys, joka johtaa epäsuotuisaan kohteluun – yhteyksissä, jotka eivät liity siihen asiayhteyteen, jossa tiedot alun perin kerättiin ja/tai – kohtelu on perustetonta tai suhteetonta	Keskeiset elementit: epäedullinen kohtelu sosiaalisissa yhteyksissä, jotka eivät liity siihen asiayhteyteen, jossa tiedot alun perin tuotettiin tai kerättiin, ja/tai kohtelu on perustetonta tai suhteetonta. Jos tekoälyjärjestelmää käytetään henkilön luottotietojen arviointiin, tähän voidaan käyttää taloudellista historiaa, mutta ei muita, asiaan liittymättömiä tietoja. Esimerkki: rahoituslaitokset ottavat käyttöön tekoälyjärjestelmän lainojen arviointiin mutta käyttävät siinä myös muita kuin taloudellisia tietokantoja. Jos pankki esimerkiksi analysoi myös sosiaalisen median yhteyksiä tai huomioi henkilön osoitteen päättäessään, tuleeko hakijan laina hyväksyä vai ei, tämä voi olla kielletty käytäntö 5 artiklan 1 kohdan c alakohdan mukaisesti.

Suuririskiset tekoälyjärjestelmät (Tekoälyasetuksen liite III, 6 artiklan 2 kohta)	Kielletty käytäntö (Tekoälyasetus, 5 artikla)	Esimerkkejä kielletyistä ja mahdollisesti kielletyistä käytötapauksista ja niiden selitykset
5c) Sairaus- tai henkivakuutuksen hinnoittelun riskinarviointi	(c) Sosiaalinen pisteytys, joka johtaa epäsuotuisaan kohteluun – yhteyksissä, jotka eivät liity siihen asiayhteyteen, jossa tiedot alun perin kerättiin ja/tai – kohtelu on perusteetonta tai suhteetonta	Keskeiset elementit: epäedullinen kohtelu sosiaalisissa yhteyksissä, jotka eivät liity siihen asiayhteyteen, jossa tiedot alun perin tuotettiin tai kerättiin, ja/tai kohtelu on perusteetonta tai suhteetonta Jos tekoälyjärjestelmää käytetään henkivakuutuksen hinnoitteluun, tähän voidaan käyttää terveydellistä taustaa mutta ei muita, asiaan liittymättömiä tietoja. Esimerkki: vakuutuksenantaja ottaa käyttöön tekoälyjärjestelmän, jossa hinnoittelua arvioidaan asiaan liittymättömästä kontekstista saaduilla tiedoilla. Jos vakuutuksenantaja esimerkiksi analysoi sosiaalisen median yhteyksiä ja käyttäytymistä, tämä voi olla kielletty käytäntö 5 artiklan 1 kohdan c alakohdan mukaisesti.

Suuririskiset tekoälyjärjestelmät (Tekoälyasetuksen liite III, 6 artiklan 2 kohta)	Kielletty käytäntö (Tekoälyasetus, 5 artikla)	Esimerkkejä kielletyistä ja mahdollisesti kielletyistä käyttötapauksista ja niiden selitykset
6) Lainvalvonta a) Rikoksen uhriksi joutumisen riskin arviointi b) Valheenpaljastimet c) Todistusaineiston luotettavuuden arviointi d) Rikokseen tai rikoksen uusimiseen syylistymisen riskin tai persoonallisuuspiirteiden arviointi e) Profilointi rikosten paljastamisen, tutkimisen tai rikoksiin liittyvien syytetoimien yhteydessä	(d) Yksinomaan profilointiin perustuva rikoksen riskin arviointi	Keskeiset elementit: arviointi perustuu persoonallisuuspiirteisiin ja ominaisuuksiin eikä objektiivisiin tosiasioihin. Huomio: jos järjestelmä tukee ihmisen tekemää päätöstä, kyseessä voi olla sovellettava poikkeus. 5 artiklan 1 kohdan d alakohdassa kielletään rikosten riskinarvioinnit, jotka perustuvat yksinomaan persoonallisuuspiirteiden profilointiin ilman objektiivisia, todennettavissa olevia tosiseikkoja, jotka liittyvät rikolliseen toimintaan. Esimerkki: ennakkoiva poliisijärjestelmä, jossa yksilöitä profiloidaan demografisten tietojen perusteella. Jos poliisilaitos esimerkiksi ennustaa rikollisen toiminnan todennäköisyyttä iän, kansallisuuden, naapuruston tai vastaavan tiedon perusteella, kyseessä on 5 artiklan 1 kohdan d alakohdan mukainen kielletty järjestelmä.

Suuririskiset tekoälyjärjestelmät (Tekoälyasetuksen liite III, 6 artiklan 2 kohta)	Kielletty käytäntö (Tekoälyasetus, 5 artikla)	Esimerkkejä kielletyistä ja mahdollisesti kielletyistä käytötapauksista ja niiden selitykset
6) Lainvalvonta e) Profilointi rikosten paljastamisen, tutkimisen tai rikoksiin liittyvien syytetoimien yhteydessä	(h) Reaaliaikaisten biometristen etätunnistusjärjestelmien käyttö julkisissa tiloissa lainvalvontatarkoituksessa, paitsi jos se on välttämätöntä jonkin seuraavan tavoitteen saavuttamiseksi: – kaappauksen uhrin kohdennettu etsintä – erityisen, merkittävän ja välittömän uhan ehkäiseminen – rikoksesta epäillyn henkilön paikantaminen tai tunnistaminen (liitteen II mukaisesti).	Keskeiset elementit: RBI-järjestelmien käyttö seuraavasti: – ”reaaliaikainen” tunnistus – julkiset tilat – lainvalvontaviranomaisten taholta tai puolesta. Johdanto-osan kappaleen 32 mukaan reaaliaikaisten RBI-järjestelmien käyttö ”synnyttää tunteen jatkuvasta valvonnasta ja estää välillisesti kokoontumisvapauden ja muiden perusoikeuksien käyttämisen”. Esimerkki: poliisi käyttää reaaliaikaista kasvontunnistusta valvontakamerakuvista tutkinan kohteen tunnistamiseen ja pidättämiseen. <i>Moskovan poliisi (Glukhin v. Venäjä, 2024) käytti valvontakamerakuvia rauhanomaisen mielenosoittajan tunnistamiseen ja paikantamiseen reaaliaikaisen biometrisen tunnistuksen avulla.</i>

Suuririskiset tekoälyjärjestelmät (Tekoälyasetuksen liite III, 6 artiklan 2 kohta)	Kielletty käytäntö (Tekoälyasetus, 5 artikla)	Esimerkkejä kielletyistä ja mahdollisesti kielletyistä käytötapauksista ja niiden selitykset
7) Muuttoliikkeen hallinta, turvapaikka-asiat ja rajavonta (b) Turvallisuuden, poikkeavuuk-sien tai terveyden riskinarviointi (c) Turvapaikka-/viisumi-/lupahakemusten, kelpoisuuden ja valitusten arviointi	(d) Yksinomaan profilointiin perustuva rikoksen riskin arviointi	Keskeiset elementit: arviointi perustuu persoonallisuuspiirteisiin eikä objektiivisiin tosiasioihin. Huomio: jos järjestelmä tukee ihmisen tekemää päätöstä, tapaukseen voidaan soveltaa poikkeuksia. 5 artiklan 1 kohdan d alakohdassa kielletään rikosten riskinarvioinnit, jotka perustuvat vain persoonallisuuspiirteiden profilointiin ilman objektiivisiä, todennettavissa olevia tosiseikkoja, jotka liittyvät rikolli-seen toimintaan. Esimerkki: rajavontaviranomaiset ottavat käyttöön tekoälyjärjestelmän, jossa yksilöiden riskiprofilointi perustuu demografisiin tietoihin. Jos rajavontaviranomaiset käyt-tävät esimerkiksi kansallisuutta tai uskontoa rikosten riskin ennako-in-tiin, kyseessä voi olla 5 artiklan 1 kohdan d alakohdan mukainen kielletty järjestelmä.

Suuririskiset tekoälyjärjestelmät (Tekoälyasetuksen liite III, 6 artiklan 2 kohta)	Kielletty käytäntö (Tekoälyasetus, 5 artikla)	Esimerkkejä kielletyistä ja mahdollisesti kielletyistä käytötapauksista ja niiden selitykset
7) Muuttoliikkeen hallinta, turvapaikka-asiat ja rajavalvonta (b) Turvallisuuden, poikkeavuuksien tai terveyden riskinarviointi	(h) Reaaliaikaisten biometristen etätunnistujärjestelmien käyttö julkisissa tiloissa lainvalvontatarkoituksessa, paitsi jos se on välttämätöntä jonkin seuraavan tavoitteen saavuttamiseksi: – kaappauksen uhrien kohdennettu etsintä – erityisen, merkittävän ja välittömän uhan ehkäiseminen – rikoksesta epäillyn henkilön paikantaminen tai tunnistaminen (liitteen II mukaisesti).	Keskeiset elementit: RBI-järjestelmien käyttö seuraavasti: – ”reaaliaikainen” tunnistus – julkiset tilat – lainvalvontaviranomaisten taholta tai puolesta. Johdanto-osan kappaleen 32 mukaan reaaliaikaisten RBI-järjestelmien käyttö ”synnyttää tunteen jatkuvasta valvonnasta ja estää välillisesti kokoontumisvapauden ja muiden perusoikeuksien käyttämisen”. Esimerkki: reaaliaikainen kasvontunnistus rajalla saaduista valvontakamerakuvista tutkinnan kohteena olevien henkilöiden tunnistamiseen.

Suuririskiset tekoälyjärjestelmät (Tekoälyasetuksen liite III, 6 artiklan 2 kohta)	Kielletty käytäntö (Tekoälyasetus, 5 artikla)	Esimerkkejä kielletyistä ja mahdollisesti kielletyistä käytötapauksista ja niiden selitykset
7) Muuttoliikkeen hallinta, turvapaikka-asiat ja rajavaltu (d) Luonnollisten henkilöiden havaitseminen, tunnistaminen tai henkilöllisyyden määrittäminen (pois lukien matkustusasiakirjojen tarkastaminen)	(e) Kasvokuvien kohdentamaton haravointi	Keskeiset elementit: menetelmä tunnistustietokannan luomiseksi tai laajentamiseksi kohdentamattomalla haravoinnilla itse tehdyn tunnistuksen sijaan. Tämä on kiellettyä, koska kohdentamaton haravointi toimii kuin ”pölynimuri”, sillä siinä kerätään kasvokuvia summittaisesti kohdistamatta niitä tiettyihin henkilöihin, kuten 5 artiklan 1 kohdan e alakohdassa on kuvattu. Johdanto-osan kappaleessa 43 perustelua täydennetään sillä, että tämä käytäntö ”lisää tunnetta joukkovalvonnasta” ja voi johtaa perusoikeuksien loukkauksiin. Esimerkki: rajavaltaviranomaiset rakentavat kasvontunnistustietokantaa joukkoharavoinnin avulla. Rajavaltaviranomaiset saattavat haravoida kasvokuvia sosiaalisesta mediasta, uutisartikkeleista ja valvontakamerakuvista kohdistamatta niitä tiettyihin yksilöihin. Jos nämä kuvat lisätään biometrisen tunnistuksen tietokantaan, kyseessä on 5 artiklan 1 kohdan e alakohdan mukainen kielletty käytäntö.

Liite K

Vaiheen 3 mallilomake

Tämä lomake on suunniteltu esimerkiksi siitä, miten tapauksen käsittelijä voi osiossa 3 annettuja vaiheita noudattaen kirjata havaintonsa muistiin. Esimerkit ovat kuvitteellisia, ja niiden on tarkoitus antaa käsitys siitä, millaisia tietoja lomakkeelle voidaan kirjata. On odotettavissa, että todelliset kirjatut tiedot ovat huomattavasti yksityiskohtaisempia. Viimeinen sarake on tarkoitettu auttamaan näytön tarkistamisessa, kun vastaajalta on saatu tietoja.

Vaihe		Syrjintäolettava	Vastaajan antamien tietojen jälkeen
3.1. Tunnetut ja epäillyt riskit 3.1.1 Järjestelmän tyyppi	Kirjaa tietoihin, onko järjestelmä suuririskinen vai ei, tai onko se tarkoitettu käytettäväksi sektoreilla tai aloilla, joihin liittyy tekoälyasetuksen mukaisesti syrjintäriski.	Esimerkkejä Sektori: Käyttötapaus:	
3.1.2 Tunnetut syrjintäriskit	Kirjaa tietoihin alue, jolla riskin tiedetään esiintyvän, teknologian tyyppi ja kaikki muut asiaankuuluvat tiedot ja todisteet.	Esimerkkejä Sektori: lainvalvonta Teknologia: reaaliaikainen kasvontunnistus, biometriikka Lähde: kansalaisjärjestön tai akateemisen laitoksen tekemä tutkimus, EU:n tekoälyasetuksen 5 artikla (kielleyt järjestelmät), 6 artikla (suuririskiset järjestelmät) ja liite III.	

Vaihe		Syrjintäoletta	Vastaajan antamien tietojen jälkeen
3.2 Kielletyt syrjintäperusteet ja sijaismuuttajat	Kirjaa tietoihin kiellettyjen syrjintäperusteiden suora käyttö järjestelmässä. Missä niitä käytetään ja miten?	Kielletyt syrjintäperusteet Käyttötapa: esimerkiksi syöttötiedot	
Tutki tarkemmin järjestelmän teknistä suunnittelua ja (epäiltyjen) sijaismuuttajien vaikutusta järjestelmän tuloksiin. Se, että sijaismuuttajaa käytetään syötteenä, ei itsessään riitä todisteeksi syrjinnästä. Seuraava vaihe on arvioida näyttöä, jotta ymmärretään, johtaako näiden syötteiden käyttö eriarvoiseen kohteluun.	Kirjaa tietoihin kiellettyjen syrjintäperusteiden tai sijaismuuttajien käyttö, jos ne vaikuttavat tai niiden epäillään vaikuttavan järjestelmän tuloksiin. Kirjaa myös kunkin sijaismuuttajan tietoihin, miksi yhdenvertaisuuselin pitää niitä sijaismuuttajina.	Esimerkkejä Sijaismuuttajat: esimerkiksi postinumero rodun sijaismuuttajana tai raskaus sukupuolen sijaismuuttajana. Näyttö ja argumentit	
3.3: Riskinarvioinnit, mukaan lukien FRIA	Kirjaa tietoihin kaikki tarjoajan tai käyttöönottajan tunnistamat syrjintäriskit ja riskin lieventämiseksi tehdyt toimenpiteet.	Esimerkkejä Riski: rotuun perustuva syrjintä historiallisen vinouman vuoksi Missä tunnistettu: riskinarviointi Lieventävä toimenpide: vinoumien poistamistekniikka	

Vaihe		Syrjintäolettama	Vastaajan antamien tietojen jälkeen
	Pohdi ja kirjaa tietoihin, havaitaanko riskinarvioinnissa tai DPIA- tai FRIA-arvioinnissa selkeitä puutteita.	Riskinarvioinnissa viitataan syrjintään mutta ei rotuun. DPIA: rotua ei ole huomioitu erityisten henkilötietoryhmien datassa. FRIA: rotuun perustuvaa syrjintää ja Euroopan ihmis-oikeussopimuksen 14 artiklaa ei ole huomioitu.	
	Pohdi ja kirjaa tietoihin, onko prosessissa mukana ihmisiä ja mitä vaikutuksia tällä on. Kuka tämä henkilö on? Onko asiaankuuluvalla henkilöllä tarvittava pätevyys, koulutus ja valtuudet kumota tekoälyjärjestelmän tekemä päätös? Onko asiaankuuluva henkilö koulutettu ymmärtämään ja tulkitsemaan järjestelmän tuotoksia ja tunnistamaan, missä voi esiintyä vinoumia ja missä tarvitaan ihmisen väliintuloa? Onko päätöksen tekijöille annettu ohjeita tai käytäntöjä, jotka auttavat heitä ymmärtämään, miten tekoälyjärjestelmää käytetään tai miten tuotoksia tulkitaan?	Yhteyshenkilö: Rooli: tarkastaa päätökset mutta ei päätökseen johdaneita tietoja. On selvitettävä, riittääkö tämä.	

Vaihe		Syrjintäoletta	Vastaajan antamien tietojen jälkeen
3.4 Järjestelmän tavoite	Kirjaa tietoihin järjestelmän tarkoitus ja optimointi.	Järjestelmän tarkoitus: Mihin nähden suunniteltu optimoitumaan:	
	Kirjaa tietoihin sijaismuuttujat ja kielletyt syrjintäperusteet, jotka vaikuttavat järjestelmän tuotoksiin ja mittarit niiden painokertoimista / vaikutuksesta tuotokseen, jos ne ovat saatavilla.	Järjestelmään vaikuttavat kielletyt syrjintäperusteet: Järjestelmään vaikuttavat sijaismuuttujat: Painokertoimia/ vaikutusta koskevat mittarit:	
3.5 Koulutus-, testaus- ja validointidata	Kirjaa tietoihin kaikki yleiset dataongelmat, mukaan lukien datan laatuun liittyvät ongelmat.	Esimerkiksi datan otos on pieni tai vanha tai liittyy toiseen maantieteelliseen alueeseen.	
	Eriarvoisuuteen ja syrjintään liittyvät dataongelmat.		
	Riittämättömään dokumentaatioon liittyvät ongelmat.		
	Lieventämistoiimiin liittyvät huolenaiheet.		
	Perustelu sille, miten dataan ja lieventämistoiimiin liittyvät ongelmat voivat johtaa eriarvoiseen kohteluun tässä tapauksessa.		
	Kirjaa tietoihin kaikki viitteet siitä, ettei dataan sovellettavia tekoälyasetuksen säännöksiä noudateta.		

Vaihe		Syrjintäolettaama	Vastaajan antamien tietojen jälkeen
3.6 Testaus ja arviointi	Tilastoista ilmenevät tuotosten tai käsittelyn puutteet.		
	Raportoituihin tilastoihin liittyvät ongelmat (kuten virheellinen mittari tai dataan liittyvät ongelmat).		
	Testauksen havaitut puutteet.		
Johtopäätös	Tarkista tiedot ja kirjaa muistiin perusteet, joiden perusteella voidaan osoittaa <i>prima facie</i> -syrjintätapaus tai todeta, ettei tapausta voida osoittaa.		
	Tarkista kaikki vaiheet, jos lisätietoja saadaan, jotta voidaan arvioida, onko vastaaja onnistuneesti kumonnut syrjintäolettaaman tai perustellut syrjintätapauksen.		

Tekoäly muokkaa yhteiskuntiamme ja vaikuttaa perusoikeuksiin ja tasa-arvoon. Nämä järjestelmät voivat vahvistaa ja luoda syrjintää, koska ne ovat usein suunniteltu erottelemaan yksilöitä toisistaan: luokittelemalla, asettamalla järjestykseen tai kohdistamalla huomiota näihin yksilöihin. Historialliset eriarvoisuudet ja vinoumat, jotka ovat juurtuneet algoritmisten järjestelmien dataan, sääntöihin ja suunnitteluvalintoihin, voivat johtaa laajaan ja skaalautuvaan syrjintään, ellei näihin kiinniteta huomiota ja niiden vaikutuksia lievennetä.

Tämä menetelmäjulkaisu tarjoaa vaihteittaiset ohjeet yhdenvertaisuuselinten ja muiden ihmisoikeusjärjestöjen käyttöön Euroopassa tekoälyyn tai algoritmisiin järjestelmiin liittyvien syrjintätapausten arvioimiseksi. Julkaisu on tarkoitettu niiden tahojen tapauksittelijoille, neuvonantajille ja lakihenkilöille, jotka tutkivat syrjintään liittyviä valituksia, joissa on mukana tai joiden epäillään liittyvän tekoälyyn tai automaattiseen päätöksentekoon.

Menetelmä perustuu tekoälyä koskevaan eurooppalaiseen sääntelykehikseen, erityisesti EU:n tekoälyasetukseen ja Euroopan neuvoston puiteyleissopimukseen tekoälystä sekä ihmisoikeuksista, demokratiasta ja oikeusvaltioperiaatteesta, sekä syrjinnän vastaiseen lainsäädäntöön, ja siinä viitataan myös muuhun lainsäädäntöön, kuten tietosuojan ja oikeuskäytäntöön.



YHDENVERTAISUUSVALTUUTETTU
NON-DISCRIMINATION OMBUDSMAN



COMISSÃO PARA A CIDADANIA
E A IGUALDADE DE GÉNERO

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 unionin
yhteisrahoittama



EUROOPAN UNIONI

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

Euroopan neuvoston
yhteisrahoittama ja toteuttama