

Luonnos

Hallituksen esitys eduskunnalle hallituksen esitykseksi eräiden tekoälyjärjestelmien valvonnasta annetun lain muuttamiseksi – luvantamismenettely jälkikäteisessä biometrisessä etätunnistamisessa

PERUSTELUT

2.3 Tekoälyjärjestelmien riskiperusteinen sääntely

Suuririskiset tekoälyjärjestelmät. Tietyt tekoälyjärjestelmät luokitellaan asetuksen nojalla suuririskisiksi tekoälyjärjestelmiksi ja niille voidaan asettaa tiukennettuja vaatimuksia. On huomattava, että kaikki järjestelmät eivät ole tekoälyasetuksen soveltamisalan kattamia suuririskisiä tekoälyjärjestelmiä. Tekoälyasetuksen 3 artiklan 1 kohta sisältää tekoälyjärjestelmän määritelmän ja komissio on antanut tekoälyasetuksen 96 artiklan 1 f kohdan nojalla ohjeet tekoälyjärjestelmän määrittelystä (C(2025) 5053 lopullinen).

Asetuksen 6 artiklassa säädetään suuririskisten tekoälyjärjestelmien luokitussäännöistä. Artiklan 1 kohdan nojalla tekoälyjärjestelmä luokitellaan suuririskiseksi, jos tekoälyjärjestelmä on tarkoitettu käytettäväksi tuotteen turvakomponenttina tai tekoälyjärjestelmä on itse tuote, joka kuuluu liitteessä I luetellun unionin yhdenmukaistamislainsäädännön soveltamisalaan ja tekoälyjärjestelmälle on tehtävä kolmannen osapuolen suorittama vaatimustenmukaisuuden arviointi kyseisen tuotteen saattamiseksi markkinoille tai käyttöön ottamiseksi liitteessä I luetellun unionin yhdenmukaistamislainsäädännön mukaisesti.

Artiklan 2 kohdan mukaan myös asetuksen liitteessä III tarkoitettuja tekoälyjärjestelmiä pidetään suuririskisenä.

Asetuksen liitteessä III säädetään suuririskisiksi tekoälyjärjestelmiksi seuraavilla aloilla luetellut tekoälyjärjestelmät: biometriset tunnistimet (1 kohta), kriittinen infrastruktuuri (2 kohta), yleissivistävä ja ammatillinen koulutus (3 kohta), työllistäminen, henkilöstöhallinto ja itsenäisen ammatinharjoittamisen mahdollistaminen (4 kohta), välttämättömien yksityisten palvelujen ja välttämättömien julkisten palvelujen ja etuuksien saatavuus ja käyttö (5 kohta), lainvalvonta (6 kohta), muuttoliikkeen hallinta, turvapaikka-asiat ja rajavalvonta (7 kohta), oikeudenhoito ja demokraattiset prosessit (8 kohta). Olennaista tässä määrittelyssä on järjestelmän käyttötarkoitus. Liitteen III kohdassa 1, 6 ja 7 tarkoitetuilla aloilla edellytetään, että tekoälyjärjestelmien käyttö on sallittua asiaa koskevan unionin tai kansallisen lainsäädännön nojalla.

Artiklan 3 kohdassa säädetään poikkeuksia asetuksen liitteessä III tarkoitettujen tekoälyjärjestelmien luokitteluun suuririskiseksi. Tekoälyjärjestelmää ei ole pidettävä suuririskisenä, jos se ei aiheuta merkittävää vahingon riskiä luonnollisten henkilöiden terveydelle, turvallisuudelle tai perusoikeuksille, mukaan lukien se, että se ei vaikuta olennaisesti päätöksenteon tulokseen. Artiklan 3 kohdan toisessa alakohdassa luetellaan tilanteet, joissa poikkeus soveltuu: tekoälyjärjestelmän tarkoituksena on suorittaa suppea menettelyllinen tehtävä (a), tekoälyjärjestelmän tarkoituksena on parantaa aiemmin suoritettua ihmisen toiminnan tulosta (b), tekoälyjärjestelmän tarkoituksena on havaita päätöksentekotapoja tai poikkeamia aiemmista päätöksentekotavoista, eikä sen tarkoituksena ole korvata aiemmin tehtyä ihmisen tekemää arviota tai vaikuttaa siihen ilman asianmukaista ihmisen suorittamaa arviota (c), tai tekoälyjärjestelmä on tarkoitettu suorittamaan valmistelutehtäviä, joka koskee liitteessä III lueteltujen käyttötapauksien kannalta merkityksellistä arviointia (d). Kuitenkin liitteessä III tarkoitettua tekoälyjärjestelmää on aina pidettävä suuririskisenä, jos tekoälyjärjestelmä suorittaa luonnollisten henkilöiden profilointia.

Tekoälyjärjestelmän luokittelu 6(2) artiklan nojalla suuririskiseksi tekoälyjärjestelmäksi, ei tarkoita sitä, että sen käyttö olisi kielletty. Tekoälyasetus kuitenkin asettaa näille suuririskiksi tekoälyjärjestelmiksi luokitelluille järjestelmille tiettyjä vaatimuksia.

Asetuksen 6 artiklan 5 alakohdan mukaan komissio antaa viimeistään 2 päivänä helmikuuta 2026 ohjeet, jossa täsmennetään tätä suuririskisten tekoälyjärjestelmien luokitussääntöjä koskevan artiklan käytännön täytäntöönpano. Komissio antaa myös kattavan luettelon käytännön esimerkeistä sellaisten tekoälyjärjestelmien käyttötapauksista, jotka ovat suuririskisiä ja muita kuin suuririskisiä.

2.10 Luvanantamismenettely jälkikäteiseen biometriseen etätunnistamiseen

Jälkikäteisen etätunnistamisen näkökulmasta asetuksen keskeiset määritelmät ovat biometrinen tieto (3 artiklan 34 kohta), biometrinen tunnistus (3 artiklan 35 alakohta), biometrinen etätunnistusjärjestelmä (3 artiklan 41 alakohta) ja jälkikäteinen biometrinen etätunnistusjärjestelmä (3 artiklan 43 alakohta).

Komission tulee tekoälyasetuksen 6 artiklan 5 alakohdan nojalla antaa ei-sitovat ohjeet käytännön esimerkeistä korkeariskisistä tekoälyjärjestelmien käyttötapauksista. Komissio julkaisi luonnokset ohjeiksi 19.5.2026 julkista kuulemista varten. Ohjeluonnoksen (kohta 3.1.1.) mukaan biometrisenä datana ei pidetä tietoja, jotka viittaavat kuolleisiin henkilöihin, ruumiisiin, kuolleiden ihmisten jäännöksiin tai niiden jälkiin. Tekoälyjärjestelmät, joiden tarkoituksena on verrata objekteja epäilyyn liikkeiden kartoittamiseksi biometristä dataa hyödyntämättä, ei ole asetuksen liitteen III kohdan 1(a) tarkoittamaa biometristä etätunnistamista (ohjeluonnos kappale 124).

Komission ohjeluonnoksen (3.1.2.1) mukaan artiklan 3 kohdan 41 määritelmä biometrisestä etätunnistamisesta edellyttää, että tietojärjestelmä täyttää kolme vaatimusta: 1) tietojärjestelmän tarkoitus tulee olla biometrinen tunnistaminen, 2) tunnistamisen tulee tapahtua ilman kohteena olevan henkilön aktiivista osallistumista ja tyypillisesti etäältä, ja 3) tietojärjestelmän tulee verrata henkilön biometristä dataa viitetietokannassa olevaan biometriseen dataan. Ohjeluonnoksen mukaan 3 artiklan 35 tarkoittamana biometrisenä tunnistamisena ei tarkoiteta biometrisen datan prosessointia muussa kuin henkilön tunnistamistarkoituksessa. Esimerkiksi lisätietojen kerääminen tai rikosten välisten yhteyksien muodostaminen biometristen näytteiden avulla ei ole biometristä tunnistamista (kappale 132). Henkilön paikantamista ei myöskään komission ohjeluonnoksessa pidetä biometrisenä tunnistamisena, jos siinä ei käytetä biometrisiä tietoja tai biometrisiä tietoja ei verrata olemassa olevaan biometrisiä tietoja sisältävään viitetietokantaan (kappale 134).

Asetuksen 26 artiklan 10 kohdan mukaan rikoksesta epäillyn tai tuomitun henkilön kohdennettua etsintää koskevan tutkinnan yhteydessä suuririskisen tekoälyjärjestelmän, joka on tarkoitettu käytettäväksi jälkikäteiseen biometriseen etätunnistukseen, käyttöönottajalla on pyydettävä oikeusviranomaiselta tai hallintoviranomaiselta, jonka päätös on sitova ja johon sovelletaan tuomioistuINVALVONTAA, lupaa kyseisen järjestelmän käyttöön etukäteen tai ilman aiheutonta viivytystä ja viimeistään 48 tunnin kuluessa kyseisen järjestelmän käyttöön, paitsi jos sitä käytetään mahdollisen epäillyn alustavaan tunnistamiseen rikokseen suoraan liittyvien objektiivisten ja todennettavissa olevien tosiseikkojen perusteella, sanotun kuitenkin rajoittamatta direktiivin (EU) 2016/680 [rikosasioden tietosuojadirektiivin] soveltamista. Kukin käyttö on rajoitettava siihen, mikä on ehdottoman välttämätöntä kyseessä olevan rikoksen tutkintaa varten. On huomattava, että vaatimus hakea etukätes lupaa ei siis koske kaikkia liitteen III kohdan 1(a) tarkoittamia biometrisiä etätunnistusjärjestelmiä. Lupamenettely on rajattu koskemaan vain rikoksesta epäillyn tai tuomitun tutkinnassa tapahtuvaa kohdennettua etsintää.

Lisäksi 26 artiklan 10 kohdassa on todettu, että velvoite hakea lupaa jälkikäteiseen biometriseen tunnistamiseen ei koske tilannetta, jossa on kyse epäillyn alustavasta tunnistamisesta. Alustavaa tunnistamista ei ole asetuksessa määritelty. Alustavalla tunnistamisella voidaan katsoa

Luonnos

tarkoitettavan tilanteita, joissa tarkoituksena on tunnistaa yksi tai useampi mahdollinen epäilty viitetietokannasta, jotta voidaan selvittää heidän henkilöllisyytensä tai todeta, onko viitetietokannassa vastaavaa biometristä profiilia. Tällöin ei välttämättä tunnisteta epäillyn henkilöllisyyttä. Alustavaa tunnistamista olisi esimerkiksi epäillyn biometristen tietojen vertailu poliisin tiedossa olevien henkilöiden biometrisistä tunnisteista. Tarkoituksena voi olla esimerkiksi selvittää epäillyn todennäköinen henkilöllisyys tai selvittää onko henkilöstä aiemmin tehty biometrinen profiili olemassa. Tällainen tilanne voi olla kyseessä esimerkiksi, kun poliisi poimii mahdollisten epäilyjen kasvokuvat valvontakameran kuvista ja vertaa niitä aiemmin muilta rikospaikoilta kerättyihin biometrisiin jälkiin selvittääkseen onko sama henkilö mukana useammassa rikoksessa. Samoin alustavasta tunnistamisesta on kyse esimerkiksi, jos valvontakameran kuvaa hyödynnetään ja verrataan kuvia poliisin tietokantoihin mahdollisten epäiltyjen löytämiseksi. Alustavasta tunnistamisesta olisi kyse myös tilanteessa, jossa viranomainen etsii lentokentän videovalvonnasta kohdennetusti henkilöä sosiaalisesta mediasta kerätyn kuvan perusteella. Tekoälyjärjestelmän käyttö alustavaan tunnistamiseen ei edellytä tekoälyasetuksen mukaista ennakkolupaa.

Kohdennettu etsintä on kyseessä silloin kun rikostutkinnassa on edetty tilanteeseen, jossa mahdollisten epäiltyjen joukkoa on rajoitettu ja henkilöllä on tutkinnassa epäillyn asema tai hänet on tuomittu rikoksesta. Tavoitteena on tällöin epäillyn tai rikoksesta tuomitun sijainnin paikantaminen.

Ennakkolupaa vaativana biometrisenä jälkikäteisenä etätunnistamisena ei myöskään pidetä muita käyttötarkoituksia, kuten kadonneen henkilön hakua tai uhrien paikantamista. Näissä ei ole kyse rikoksesta epäillyn tai tuomitun kohdennetusta etsinnästä.

Lainvalvontaviranomaiset käyttävät tekoälyjärjestelmiä rikospaikan analysointiin ja suuren tietomäärän analysointiin tapahtumien kulun tutkimiseksi. Tällöin rikospaikalta kerätään paljon erilaista materiaalia, mukaan lukien valvontakameroiden materiaalia. Tavoitteena on kerätä tutkintanäkökulmia siihen mitä on tapahtunut analysoimalla henkilöitä ja objekteja. Henkilöitä ei verrata biometrisiin tietokantoihin. Tällöin on kyse alustavaa tunnistamista edeltävästä työvaiheesta ja huolimatta siitä, että mukana olisi biometristen tunnisteiden vertailua suljetusta tiedostojoukosta, kyseessä ei olisi biometrinen etätunnistaminen. Sama koskee tilanteita, joissa kyse on henkilöiden esiintymisen etsimisestä biometristen ominaisuuksien perusteella ilman, että muodostetaan tunnistamisen mahdollistavia biometrisiä malleja. Biometristä etätunnistamista ei myöskään ole se, jos lainvalvontaviranomaiset käyttävät tekoälyjärjestelmää, joka ryhmittelee rikospaikalla näkyvät henkilöt ikäryhmiin manuaalisen arvioinnin tukemiseksi.

Kansallisesti henkilöstä tulee rikoksesta epäilty vasta kun esitutkinta on käynnistetty. Näin ollen ennen esitutkinnan käynnistämistä tehty poliisin toimivaltaan kuuluvat toimenpiteet kuten hahmon etsintä turvakameroiden tallenteista luonnollisen henkilön liikkeiden seuraamiseksi ja paikantamiseksi taikka tuntemattoman potentiaalisen epäillyn tunnistamiseksi rikokseen liittyvien seikkojen perusteella eivät edellyttäisi asetuksen nojalla päätöstä oikeusviranomaiselta tai hallintoviranomaiselta. Tekoälyjärjestelmän käyttö rikosten ennalta estämiseen ei myöskään olisi tämän artiklan soveltamisalaan kuuluva toimenpide.

26 artiklan 10 kohdan toisessa alakohdassa säädetään siitä, että jos ensimmäisen alakohdan nojalla haettu lupa hylätään, kyseiseen lupaan linkitetyn jälkikäteisen biometrisen etätunnistusjärjestelmän käyttö on lopetettava välittömästi ja sen suuririskisen tekoälyjärjestelmän käyttöön liittyvät henkilötiedot, jota varten lupaa haettiin, on poistettava.

26 artiklan 10 kohdan kolmannessa alakohdassa säädetään siitä, ettei tällaista suuririskistä tekoälyjärjestelmää, joka on tarkoitettu käytettäväksi jälkikäteiseen biometriseen

Luonnos

etätunnistukseen, saa missään tapauksessa käyttää lainvalvontatarkoituksiin kohdentamattomalla tavalla ilman minkäänlaista yhteyttä tiettyyn rikokseen, rikosoikeudelliseen menettelyyn, todelliseen ja välittömään tai todelliseen ja ennakoitavissa olevaan rikoksen uhkaan tai tietyn kadonneen henkilön etsimiseen. On varmistettava, että päätöstä, jolla on yksittäiseen henkilöön kohdistuvia kielteisiä oikeusvaikutuksia, ei saa tehdä pelkästään tällaisen jälkikäteisen biometrisen etätunnistusjärjestelmän tuotosten perusteella. Kohta ei rajoita yleisen tietosuojasetuksen 9 artiklan ja rikosasioiden tietosuojadirektiivin 10 artiklan soveltamista biometrinen tietojen käsittelyn osalta.

26 artiklan 10 kohdan viidennessä alakohdassa säädetään siitä, että käyttötarkoituksesta tai käyttöönottajasta riippumatta tällaisten suuririskisten tekoälyjärjestelmien kaikenlainen käyttö on dokumentoitava asianomaiseen poliisitiedostoon ja asetettava pyynnöstä asianomaisen markkinavalvontaviranomaisen ja kansallisen tietosuojaviranomaisen saataville, lukuun ottamatta lainvalvontaan liittyvien arkaluonteisten operatiivisten tietojen luovuttamista. Alakohta ei rajoita valvontaviranomaisille rikosasioiden tietosuojadirektiivin nojalla annettuja valtuuksia. 26 artiklan 10 kohdan kuudennen alakohdan mukaan käyttöönottajien on toimitettava asianomaisille markkinavalvonta- ja kansallisille tietosuojaviranomaisille vuosittain raportit jälkikäteisten biometrinen etätunnistusjärjestelmien käytöstä, lukuun ottamatta lainvalvontaan liittyvien arkaluonteisten operatiivisten tietojen luovuttamista. Raportit voidaan koota yhteen siten, että ne kattavat useamman kuin yhden käyttökerran.

26 artiklan 10 kohdan seitsemännen alakohdan mukaan jäsenvaltiot voivat unionin oikeuden mukaisesti ottaa käyttöön jälkikäteisten biometrinen etätunnistusjärjestelmien käyttöä koskevaa rajoittavampaa lainsäädäntöä.

Komission odotetaan antavan ohjeet asetuksen 96 artiklan nojalla myös biometristä jälkikäteistä etätunnistamista koskevan sääntelyn soveltamisesta.

3.1.12 Jälkikäteinen biometrinen etätunnistaminen

Asetuksen nojalla kansallisesti tulee säätää jälkikäteistä biometristä etätunnistamista koskevasta luvanantamismenettelystä. Asetuksen nojalla määräytyy se, milloin jälkikäteisessä biometrisessä tunnistamisessa käytetty tekoälyjärjestelmä luokitellaan suuririskiseksi (artikla 6(2) ja liite III) ja milloin sitä ei luokitella suurirriskiseksi (artikla 6(3)). Artiklassa 26(10) puolestaan säädetään milloin suurirriskiseksi luokitellun biometristä jälkikäteistä etätunnista koskevan tekoälyjärjestelmän käyttö edellyttää kansallisesti säädettävää luvanantamismenettelyä. Viranomaisten toimivallasta kerätä biometrisiä tunnistamistietoja ja käyttää jälkikäteistä biometristä etätunnistamista asetuksen asettamissa puitteissa ei säädetä asetuksessa. Asetus nimenomaisesti rajaa lupaa edellyttävän menettelyn ulkopuolelle mahdollisen epäillyn alustavan tunnistamisen. Toisin sanoen esimerkiksi tunnistamattoman epäillyn liikkeiden seuranta ja yhdistäminen tiettyyn paikkaan tai ajoneuvoon ei vielä ole rikoksesta epäillyn tai tuomitun asetuksessa tarkoitettua kohdennettua etsintää eikä siten jälkikäteistä biometristä etätunnistamista eikä vaadi tekoälyasetuksen tarkoitamaan ennakkolupaa. Myöskään kadonneiden tai uhrien jälkikäteisessä tunnistamisessa ja paikantamisessa ei olisi kyse viranomaislupaa vaativasta toimesta. Tekoälyjärjestelmän käyttö rikosten ennalta estämiseen ei myöskään olisi asetuksen mukaista luvanvaraista rikoksesta epäillyn tai tuomitun biometristä jälkikäteistä etätunnistamista.

Tätä nykyä asetuksen tarkoittama jälkikäteinen biometrinen etätunnistaminen on käytössä poliisissa, eli lainsäädäntö mahdollistaa ja sallii jälkikäteisen biometrinen etätunnistamisen käytön ja poliisilla on siihen tekninen mahdollisuus sekä soveltuva teknologia. Poliisi saa jälkikäteisessä biometrisessä etätunnistamisessa käytettävää aineistoa oman teknisen valvontansa järjestelmistä tai esitutkinnassa todisteena kerätyistä yritysten, yhteisöjen tai yksityisten

Luonnos

kameratallenteista. Lisäksi Tullilla on tekninen mahdollisuus sekä soveltuva teknologia ja lainsäädäntö jälkikäteiseen biometriseen etätunnistamiseen. Myös Rajavartiolaitoksella on voimassa lainsäädäntö jälkikäteiseen biometriseen etätunnistamiseen.

Poliisin toimivaltuudesta tekniseen valvontaan säädetään poliisilaissa (872/2011, 4 luvun 1 §). Teknisellä valvonnalla tarkoitetaan jatkuvaa tai toistuvaa ajoneuvoihin, ajoneuvojen kuljettajiin, jalankulkijoihin tai yleisöön kohdistuvaa teknisellä laitteella tapahtuvaa katselua tai kuuntelua sekä äänen tai kuvan automaattista tallentamista. Poliisi saa siitä ennalta ilmoitettuaan suorittaa yleisellä paikalla tai yleisellä tiellä teknistä valvontaa yleisen järjestyksen ja turvallisuuden ylläpitämiseksi, rikosten ennalta estämiseksi, rikoksesta epäillyn tunnistamiseksi sekä erityisten valvontakohteiden vartioimiseksi. Lisäksi poliisilla on oikeus poliisilain 4 luvun 2 §:n 1 momentin nojalla saada viranomaiselta ja julkista tehtävää hoitamaan asetetulta yhteisöltä poliisille kuuluvan tehtävän suorittamiseksi tarpeelliset tiedot ja asiakirjat maksutta ja salassapitovelvollisuuden estämättä, jollei sellaisen tiedon tai asiakirjan antamista poliisille tai tietojen käyttöä todistena ole laissa nimenomaisesti kielletty tai rajoitettu. Poliisilain 4 luvun 3 § puolestaan antaa poliisille oikeuden saada yksityiseltä yhteisöltä tai henkilöltä rikoksen estämiseksi tai selvittämiseksi tarvittavia tietoja. Poliisi voi siis teknisen valvonnan ja tiedonsaantioikeutensa nojalla saada myös biometrisiä tunnisteita kuten kasvokuvia käytettäväksi jälkikäteisessä biometrisessä etätunnistamisessa rikoksesta epäillyn tai tuomitun henkilön kohdennettua etsintää varten.

Lisäksi poliisin toimivaltuuksista hankkia rikosten selvittämiseksi tarvittavaa tietoa säädetään pakkokeinolaissa (806/2011) ja esitutkintalaissa (805/2011).

Poliisin toimivaltuuksiensa puitteissa hankkimien henkilötietojen (ml. biometristen tietojen) käsittelystä säädetään poliisin henkilötietolaissa ja erityisesti sen 2 luvussa. Kun kyse on tutkintaja valvontatehtävästä poliisi saa käsitellä 2 luvun 5 §:ssä tarkoitetuista henkilöistä 4 §:ssä tarkoitettujen henkilön perustietojen lisäksi 6 §:n 2 alakohdan nojalla myös muun muassa tuntomerkkitietoja henkilöllisyyden toteamiseksi, mukaan lukien sormen-, käden- ja jalanjäljet, käsiala-, ääni- ja hajunäyte, DNA-tunniste, kasvokuva ja muut biometriset tiedot. Lain 7 § määrittelee tarkemmin missä tilanteissa poliisi saa käsitellä rikosten ennalta estämiseen tai paljastamiseen liittyviä henkilötietoja ja noiden edellytysten täytyessä poliisi saa 8 §:n nojalla käsitellä myös tuntomerkkitietoja henkilöllisyyden toteamiseksi, mukaan lukien ääninäyte, kasvokuva ja muut biometriset tiedot

Edellä mainittujen toimivaltuuksien avulla poliisi voi tunnistaa tuntemattomia tekijöitä, saada tietoa muista rikoksista, joita epäilty henkilö on tehnyt, ja selvittää, onko rikokseen osallistunut muita henkilöitä. Lisäksi saattaa ilmetä tietoa, joka voi toimia perustana mahdolliselle motiivikuvaukselle tai henkilön vapauttamiselle epäilyistä. Poliisi voi toimivaltuuksiensa puitteissa käyttää muun muassa tekniikkaa automaattiseen kasvojen kuvien, sormenjälkien ja tuntomerkkitietojen vertaamiseen eri rekistereihin, jotka sisältävät biometrisiä tietoja. Vertailu suoritetaan osana rikostutkintaa, muun muassa henkilöllisyyden selvittämiseksi tai henkilösuorituksen valitsemiseksi biometristen tietojen avulla. Lisäksi voidaan verrata tekoälyjärjestelmän avulla tekijän ääninauhoituksia epäillyn ääninäytteeseen.

Tullin toimivaltuudesta tekniseen valvontaan säädetään tullilaissa (304/2016, 28 §). Tullin toimivaltuuksista hankkia rikosten selvittämiseksi tarvittavaa tietoa säädetään niin ikään pakkokeinolaissa ja esitutkintalaissa. Toimivaltuuksilla hankittujen henkilötietojen (ml. biometristen tietojen) käsittelystä säädetään Tullin henkilötietolaissa. Mainitun lain 14 §:n 2 momentin mukaan Tullilla on oikeus käsitellä myös automaattisessa kasvojentunnistuksessa vertaamalla teknisessä valvonnassa saatuja henkilötietoja 8 ja 10 §:n perusteella tallennettuihin henkilötietoihin

Luonnos

rikosten ennalta estämiseen, selvittämiseen, paljastamiseen tai syyteharkintaan saattamiseen liittyvään toimenpiteeseen taikka pakkokeinon käyttöön liittyvää toimenpidettä varten.

Rajavartiolaityksellä ei ole tällä hetkellä käytössä jälkikäteisen biometrisen etätunnistamisen teknologioita, mutta Rajavartiolaityksen oma toimialakohtainen lainsäädäntö sisältää toimivaltuussäännökset kyseisen teknologian käyttöön. Nykyisellään rajavartiolaity (578/2025) antaa rajavartiioviranomaiselle toimivaltuudet biometrisen etätunnistamisen käyttöön. Rajavartiolaityksen toimivaltuudesta tekniseen valvontaan säädetään rajavartiolaityn 29 §:ssä. Teknisessä valvonnassa kertyvän kuvan ja äänen käyttäminen esimerkiksi jälkikäteiseen biometriseen etätunnistamiseen on mahdollistettu rajavartiolaityn 31 §:ssä, jossa säädetään Rajavartiolaityksen oikeudesta käyttää rajanylityspaikalla teknisessä valvonnassa kertyvää kuvaa ja ääntä henkilöiden automaattiseen tunnistamiseen pykälässä mainitulla käyttöalalla. Rajavartiolaityksen oikeudesta hankkia ja saada rikosten estämiseksi, paljastamiseksi ja selvittämiseksi tarvittavaa tietoa säädetään esitutkintalaissa, pakkokeinolaissa, rikostorjunnasta Rajavartiolaityksessä annetussa laissa (108/2018) ja henkilötietojen käsittelystä Rajavartiolaityksessä annetussa laissa (639/2019). Henkilötietojen käsittelystä säädetään Rajavartiolaityksen henkilötietolaissa.

Nykyinen laki henkilötietojen käsittelystä poliisitoimissa sallii 2 luvun 15 §:n mukaisesti erityisiin henkilötietoryhmiin kuuluvien tietojen, kuten biometristen tietojen käytön silloin, kun se on käsittelytarkoituksen kannalta välttämätöntä. Sekä Tullin Rajavartiolaityksen henkilötietolaikoihin sisältyy vastaavat säännökset (4 §). Jälkikäteisessä biometrisessä etätunnistamisessa välttämättömyyden perustana on poliisin tarve selvittää asianosaisen henkilön liikkeet rikoksen tekoajankohtana tai sen jälkeen. Vastaavasti poliisilla voi olla tarve saada tieto tai varmuus epäillyn henkilöllisyydestä löytämällä hänestä parempilaatuinen kuva tallennemassasta. Sanottu koskee myös Tullia ja Rajavartiolaitysta. Harvoissa käyttötapauksissa poliisi voi esimerkiksi tietää tuntemattoman tekijän olleen tiettyssä paikassa tai kulkeneen tiettyä reittiä useasti, jolloin ristiin vertaamalla pyritään löytämään oikea henkilö tallennemassasta.

Rikosasioiden tietosuojalain 6 §:n tarpeellisuusvaatimuksen mukaisesti käsiteltävien henkilötietojen on oltava käsittelyn tarkoituksen kannalta asianmukaisia ja tarpeellisia eivätkä ne saa olla liian laajoja niihin tarkoituksiin, joita varten niitä käsitellään. Lisäksi poliisin henkilötietolain 1 luvun 2 §:n mukaisesti henkilötietojen käsittelyssä on noudatettava suhteellisuus- ja tarkoitussidonnaisuusperiaatetta, jolloin biometristä etätunnistamista ei ole voitu käyttää minkä tahansa rikoksen tai rikkomuksen selvittämiseen. Siksi Poliisihallitus on linjannut, että mm. kasvojen tunnistukseen käytettävää KASTU-järjestelmää saa käyttää vain vankeusuhkaisten tekojen selvittämiseen.

Lähtökohtaisesti kameravalvonnan tuottamat tiedot ovat aina henkilötietoja, jos henkilö on niistä kuvan tai äänen perusteella tunnistettavissa joko suoraan tai välillisesti. Tekoälyn avulla järjestelmistä pyritään tekemään vielä entisestään proaktiivisempaa, jolloin tapahtumiin reagointi olisi nopeampaa. Etenkin rikostapauksissa, joissa poliisi kerää toimivaltuuksiensa nojalla materiaalia omista järjestelmistään ja ulkopuolisilta kameravalvojilta, työn keskeinen tarkoitus on rikoksesta epäillyn henkilön tunnistaminen sekä sen kautta rikosvastuun toteuttaminen. Jälkikäteinen biometrinen etätunnistaminen on erittäin tehokas työkalu. Sen avulla voidaan tehostaa resurssien käyttöä manuaaliseen analysointiin verrattuna ja parantaa analyysin laatua ja minimoida tietojen leviäminen ja siten myös yksityisyyden suojan puuttuminen.

Rikosasioiden tietosuojalain 20 §:ssä säädetään, että rekisterinpitäjän on ennen henkilötietojen käsittelyn aloittamista arvioitava suunniteltujen käsittelytoimien vaikutukset henkilötietojen suojaan. Lisäksi lain 21 §:ssä säädetään, että rekisterinpitäjän on kuultava tietosuojavaltuutettua, jos tietojen käsittely erityisesti uusien tekniikoiden, mekanismien tai menettelyjen

käyttämisen johdosta aiheuttaa merkittävän riskin rekisteröityjen oikeuksien kannalta. Jälkikäteisen biometrisen etätunnistamisen ja KASTU-järjestelmän osalta näin on jo poliisissa tehty.

Jälkikäteinen biometrinen etätunnistaminen kohdistuu pääsääntöisesti poliisin teknisen valvonnan tavoin suureen joukkoon ihmisiä. Erityistä siinä on tietyn tai tiettyjen henkilöiden liikkeiden selvittäminen ja tunnistamistarkoitus datamassasta. Tunnistaminen perustuu henkilön kasvokuvasta järjestelmän avulla luotuun biometriseen malliin, jolle lähdekuvan avulla etsitään vastavuuksia tallennemassasta. Lähdekuvan avulla esiin seulotut ehdokkaat ovat aina suuntaa antavia, eikä vertailutulos olisi koskaan henkilöllisyyden täydellä varmuudella osoittava tunnistus. Lopullisen päätöksen tuloksesta ja jatkotoimenpiteistä tekee aina virkamies eli luonnollinen henkilö.

3.2.7 Luvanantamismenettely jälkikäteiseen biometriseen etätunnistamiseen

Tekoälyasetuksen 26 artiklassa säädetään suuririskisten tekoälyjärjestelmien käyttöönottajien velvollisuuksista. Artiklan 10 kohdassa edellytetään, että rikoksesta epäillyn tai tuomitun henkilön kohdennettua etsintää koskevan tutkinnan yhteydessä suuririskisen tekoälyjärjestelmän, joka on tarkoitettu käytettäväksi jälkikäteiseen biometriseen etätunnistukseen, käyttöönottajana on pyydettävä oikeus- tai hallintoviranomaiselta ennakkolupa. Luvanantamismenettelyn toteuttaminen edellyttää, että menettelystä säädetään kansallisesti.

Tekoälyasetus ei säädä kansallisten toimivaltaisten viranomaisten toimivaltuuksista käyttäen jälkikäteistä biometristä etätunnistamista. Toimivaltuuksista säädetään kansallisesti. Poliisi ja muut toimivaltaiset lainvalvontaviranomaiset voivat siten edelleen hyödyntää biometrisiä etätunnistusjärjestelmiä niille säädettyjen toimivaltuuksien puitteissa. Tekoälyasetus edellyttää kuitenkin, että jälkikäteisen biometrisen etätunnistamisen käyttö rikoksesta epäillyn tai tuomitun henkilön kohdennettua etsintää koskevan tutkinnan yhteydessä suuririskistä tekoälyjärjestelmää käyttäen on mahdollista vain oikeus- tai hallintoviranomaisen antaman luvan jälkeen. Lupaa ei tarvita, jos kyse on rikoksesta epäillyn alustavan tunnistamista tai kyse on muutoin tekoälyasetuksen ennakkolupamenettelyn soveltamisalan ulkopuolelle jäävästä jälkikäteisestä biometrisestä etätunnistamisesta. Luvanantamismenettely tuo uuden ennakkovalvonnan tason jälkikäteisen biometrisen etätunnistamisen käyttöön asetuksen kattamissa tilanteissa. Tekoälyasetuksen ei katsota vaikuttavan poliisin tai muiden lainvalvontaviranomaisten toimivaltuuksiin vaan edellyttää ainoastaan tietyissä asetuksessa säädetyissä tilanteissa ennakkoluvan hankkimista.

Tekoälyasetuksen mukaan ennakkoluvan antava viranomainen voi olla oikeusviranomainen tai hallintoviranomainen, jonka päätös on sitova ja johon sovelletaan tuomioistuINVALVONTAA. Esi-tyksessä luvanantaminen säädettäisiin hallintoviranomaisen tehtäväksi, joka olisi Poliisihallitukseen perustettava ennakkolupatoiminto. Ennakkolupatoiminto toimisi riippumattomana ja operatiivisesta toiminnasta erillään olevana hallinnollisena elimenä. TuomioistuINVALVONTA toteutettaisiin jälkikäteisenä tuomioistuinKONTROLLINA. Tällainen malli vastaisi rakenteeltaan useita voimassa olevia salaisia pakkokeinoja koskevia oikeusturvajärjestelyjä, joissa etukäteinen tuomioistuinKONTROLLI ei kaikilta osin ole mahdollista tai tarkoituksenmukaista, mutta joissa koh- teelle taataan myöhemmin mahdollisuus saada toimenpiteen laillisuus riippumattoman tuomio- istuimen arvioitavaksi.

Esi-tyksen valmistelussa ei ole nähty tarpeelliseksi säätää jälkikäteisen biometrisen etätunnista- misen järjestelmien käytöstä tekoälyasetusta rajoittavammin asetuksen 26 artiklan 10 kohdan salliman kansallisen liikkumavaran mukaisesti.

4 Ehdotukset ja niiden vaikutukset

4.1 Keskeiset ehdotukset

Esityksessä säädettäisiin luvanantamismenettelystä, tilanteessa, jossa poliisi, tulli, tai rajaviranomainen käyttäisi suuririskistä tekoälyjärjestelmää jälkikäteiseen biometriseen etätunnistamiseen rikoksesta epäillyn tai tuomitun kohdennettua etsintää koskevan tutkinnan yhteydessä. Esityksessä käytettäisiin tekoälyasetuksen 26 artiklan 10 kohdan sallimaa kansallista liikkumavaraa siitä, mikä viranomainen on toimivaltainen antamaan luvan tekoälyjärjestelmän käyttöön asetuksen tarkoittamassa jälkikäteisen biometrisen etätunnistamisen tilanteessa. Esityksessä säädettäisiin luvan antavan viranomaisen olevan asetuksen edellyttämä hallintoviranomainen ja tähän tehtävään Poliisihallitukseen perustettaisiin erillinen ennakkolupatoiminto. Esityksessä säädettäisiin lupamenettelyprosessin sisällöstä.

4.2 Pääasialliset vaikutukset

4.2.2 Vaikutukset viranomaisiin

Luvanantamismenettely jälkikäteiseen biometriseen etätunnistamiseen

Luvanantamismenettelyllä ei ole arvioitu olevan vaikutuksia lainvalvontaviranomaisten työhön muutoin kuin luvanantomenettelyn osalta. Luvanantomenettelyn ei arvioida aiheuttavan kohutuotonta viivästystä jälkikäteisessä biometrisessä etätunnistamisessa käytettävän tekoälyjärjestelmän käyttöön, sillä ehdotettu pykälä antaa mahdollisuuden hakea lupaa ennakkolupatoiminnolta kiiretapauksissa myös 48 tunnin puitteissa tekoälyjärjestelmän käytön aloittamisen jälkeen.

Poliisin tämänhetkisen arvion mukaan asetuksen tarkoittamaa, tekoälyjärjestelmää jälkikäteisessä biometrisessä etätunnistamisessa käytetään harvakseltaan. Luvanantomenettelyä tultaisiin alustavien arvioiden mukaan tarvitsemaan noin kymmenessä tapauksessa vuositasolla. Luvanantomenettelyssä on kuitenkin kyse uudesta tehtävästä ja toiminnosta Poliisihallitukselle. Menettelyllä arvioidaan olevan vähäisiä vaikutuksia Poliisihallituksen työmäärään ja lainsäädännön toimeenpano tullaan toteuttamaan valtiontalouden menokehyksen puitteissa. Toimeenpanossa tulee kuitenkin ottaa huomioon Poliisihallitukseen perustettavan ennakkolupatoiminnon perustamiseen ja tietojärjestelmä rakenteisiin tarvittavat muutokset. Ennakkolupatoimintoprosessiin osallistuvien virkahenkilöiden tulee toimia erillään varsinaisesta rikostutkintaa suorittavasta viranomaisesta ja tuoda lupaharkintaan riippumattomuutta sekä ulkopuolista kontrollia. Ennakkolupatoiminnon tehtävänä on arvioida lupahakemuksen laillisuutta, välttämättömyyttä ja suhteellisuutta. Luvanantamismenettelyssä käytettävän tietojärjestelmä ratkaisun tulee mahdollistaa sekä tehokas lupaharkinta että riippumattoman aseman säilyttäminen. Tietojärjestelmä ratkaisu voitaisiin rakentaa luomalla esimerkiksi nykyisin käytössä olevaan Patjaan tai Vitjaan erillinen käyttäjärooli ennakkolupatoiminnolle. Lupahakemukset laadittaisiin Patjassa tai Vitjassa ja ennakkolupatoiminto näkisi vain lupaharkinnan kannalta välttämättömät tiedot, sen käyttöoikeudet olisivat rajatut ennakkolupatoiminnon tehtävien suorittamiseen ja kaikki katselut ja päätökset lokitettaisiin erikseen.

4.2.5 Perus- ja ihmisoikeusvaikutukset

Luvanantamismenettelyllä suuririskisen tekoälyjärjestelmän, kuten tässä yhteydessä jälkikäteisen biometrisen etätunnistuksen toteuttamiseksi käytettävän tekoälyjärjestelmän, käyttöön liittyen on useita perus- ja ihmisoikeusvaikutuksia. Luvanantamismenettelyn vaatimisella voidaan katsoa olevan vaikutuksia erityisesti yksityisyyden ja henkilötietojen suojaan, oikeuteen

Luonnos

oikeudenmukaisesta oikeudenkäynnistä, oikeusvaltioperiaatteeseen ja syrjimättömyyteen. Luvanantamismenettely toimii keskeisenä oikeusturvamekanismina, joka edelleen varmistaa osaltaan sen, että suuririskisen tekoälyjärjestelmän käyttö ei riko perus- ja ihmisoikeuksia. Se voi osaltaan varmistaa, että suuririskisiä järjestelmiä käytetään vastuullisella ja oikeasuhtaisella tavalla ja mahdollistaa suuririskisen tekoälyjärjestelmän käytön valvonnan ja vähentää syrjinnän riskiä.

Perustuslain 21 §:n mukaisen tehokkaan oikeusturvan turvaamiseksi biometrisen jälkikäteisen etätunnistamisen lupajärjestelmä rakennettaisiin salaisia pakkokeinoja ja salaisia tiedonhankintakeinoja koskevaa sääntelyä muistuttavaksi. Tässä mallissa luvan biometrisessä jälkikäteisessä etätunnistamisessa käytettävän tekoälyjärjestelmän käyttämiseen myöntäisi Poliisihallitukseen sijoitettava ennakkolupatoiminto. TuomioistuINVALVONTA toteutuisi jälkikäteisesti.

Järjestelmän keskeisenä oikeusturvaelementtinä olisi velvollisuus ilmoittaa toimenpiteestä sen kohteelle sen jälkeen, kun ilmoittaminen voidaan tehdä vaarantamatta rikoksen selvittämistä, kansallista turvallisuutta tai muuta laissa säädettyä suojattavaa etua. Ilmoituksen saatuaan henkilöllä olisi oikeus saattaa lupapäätös ja siihen perustuneen jälkikäteisessä biometrisessä etätunnistamisessa käytetyn tekoälyjärjestelmän käytön lainmukaisuus käräjäoikeuden tutkittavaksi.

Käräjäoikeus voisi tällöin tutkia ainakin seuraavat kysymykset: oliko laissa säädetty käyttötarkoitus käsillä, täyttyivätkö luvan myöntämisen aineelliset edellytykset, oliko toimenpide välttämätön tavoitellun päämäärän saavuttamiseksi, täyttyikö suhteellisuusvaatimus ottaen huomioon toimenpiteen vaikutukset yksityiselämän suojaan ja henkilötietojen suojaan, oliko lupapäätös muutoinkin lainmukainen, oliko toimenpiteen toteuttaminen pysynyt myönnetyn luvan rajoissa.

Käräjäoikeudelle tulisi antaa toimivalta tutustua kaikkeen lupaharkinnan perusteena olleeseen aineistoon, mukaan lukien salassa pidettävä aineisto.

Tällainen malli soveltuisi tilanteeseen, jossa etukäteinen tuomioistuINVALVONTA ei kaikilta osin ole mahdollista tai tarkoituksenmukaista, mutta joissa kohteelle taataan myöhemmin mahdollisuus saada toimenpiteen laillisuus riippumattoman tuomioistuimen arvioitavaksi.

Perustuslain näkökulmasta kyseessä olisi perustelluin vaihtoehto verrattuna siihen, että luvanantava viranomainen olisi tuomioistuin. Ratkaisu turvaisi perustuslain 21 §:ssä tarkoitetun oikeuden saada oikeuksiaan ja velvollisuuksiaan koskeva asia riippumattoman tuomioistuimen käsiteltäväksi sekä vastaisi Euroopan ihmisoikeussopimuksen ja Euroopan unionin oikeuden edellyttämää tehokasta oikeussuojakeinoja. Samalla se vähentäisi mahdollisia valtiosääntöoikeudellisia ongelmia, joita syntyy, jos yksityiselämän suojaan puuttuvasta toimenpiteestä päättäisi yksinomaan hallintoviranomainen ilman mahdollisuutta tehokkaaseen tuomioistuINVALVONTAAN.

5 Muut toteuttamisvaihtoehdot

5.1. Vaihtoehdot ja niiden vaikutukset

5.1.5 Luvanantamismenettely jälkikäteiseen biometriseen etätunnistamiseen

Esityksessä on päädytty säätämään kansallisesti luvanantamismenettely koskien tekoälyjärjestelmän käyttöä jälkikäteisessä biometrisessä etätunnistamisessa tekoälyasetuksen kattamissa tilanteissa. Ennakkolupa on asetuksen mukaan edellytys sille, että kansalliset toimivaltaiset viranomaiset voivat jatkossakin toteuttaa toimivaltuksiensa puitteissa asetuksen soveltamisalaa kuuluvaa jälkikäteistä biometristä etätunnistamista suuririskisen tekoälyjärjestelmän avulla.

Luonnos

Ennakkoluvasta päättäisi Poliisihallitukseen perustettava erillinen hallintoelin, ennakkolupatoiminto.

Esityksen valmistelussa on harkittu vaihtoehtona sitä, että luvan myöntävä viranomaislainen voisi olla oikeusviranomaisena käräjäoikeus. Ennakkoluvan hakemisen tuomioistuimesta voitaisiin arvioida oleva oikeudellisesti selkeä ratkaisu ja sillä voitaisiin taata lupaa koskevan päätöksen luotettavuudelle ja riippumattomuudelle asetetut vaatimukset. Ennakkolupaa olisi tässä vaihtoehdossa pyydetty esitutkintaviranomaisen pidetykseen oikeutetun virkamiehen toimesta. Vastaava menettely on käytössä muun muassa telepakkokeinojen käsittelyssä tuomioistuimissa. Tässä ratkaisussa tulisi olemaan myös kustannus- ja resurssivaikutuksia oikeuslaitokselle niin henkilöresurssien kuin tietojärjestelmäkehityksen myötä. Merkittävimpänä haasteena pidetään ennakkolupapyyntöjen kiireellisen käsittelyn tarvetta, mikä nähtiin tuomioistuinmenettelyn suhteen haasteelliseksi toteuttaa.

EU-tuomioistuin on viime vuosina antanut useita tuomioita liittyen tietojen luovutuksen sitomiseksi tuomioistuimen ennakoivalvontaan. EU-tuomioistuin on esimerkiksi vuonna 2024 antamassaan tuomiossa C-548/21 tulkinnut rikosasioiden tietosuojadirektiiviä siten, että laite-etsintätyyppisessä pakkokeinossa pääsy esimerkiksi tarkkoihin tietoihin koskien henkilön yksityiselämää ja erityisen arkaluonteisiin tietoihin edellyttää riippumattoman hallintoelimen etukäteisvalvontaa. EUT on käsitellyt tietosuojadirektiivin ja päätöksentekuelimen välistä suhdetta aiemmin myös esimerkiksi ratkaisuihinsa ns. Tele2-asiassa C-203/15 ja C-698/15, Prokuratuur-asiassa C-746/18, ja C-793/19 ja C-794/19 (*Saksan liittotasavalta vastaan SpaceNet AG ja Telekom Deutschland GmbH*). Jälkikäteisessä biometrisessä etätunnistamisessa on pääsääntöisesti kyse julkisista tiloista tai rikospaikalta hankitun biometrisen tiedon vertailusta esitutkintaviranomaisilla jo oleviin biometrisiin viitetietokantoihin. Siten tuomioistuimen ennakkolupamenettelyvaatimuksia ei voi suoraan verrata pakkokeinolain mukaisiin henkilötietojen suojaan kajoaviin laite-etsintäpäätöksiin ja tämän vuoksi jälkikäteisessä biometrisessä etätunnistamisessa käytettävän tekoälyjärjestelmän luvittaminen voidaan säätää Poliisihallitukseen perustettavan erillisen hallintoelimen päätettäväksi.

Hallituksen esityksessä eduskunnalle laiksi pakkokeinolain 8 luvun muuttamisesta (HE 70/2025 vp) on arvioitu kattavasti tilannetta, että syyttäjä toimisi vahvistavana viranomaisena. Esityksessä oli kyse Euroopan unionin tuomioistuimen 4.10.2024 antamasta tuomiosta asiassa C-548/21 CG v. Bezirkshauptmannschaft Landeck, joka liittyi toimivaltaisen viranomaisen mahdollisuuteen saada pääsy matkapuhelimen sisältämiin tietoihin rikosten torjuntaa, tutkintaa, selvittämistä ja syyteharkintaa varten. Kyseisessä esityksessä esille tuodut seikat ovat syyttäjän soveltuvuuden osalta myös tämän selvityksen pohjana. Euroopan unionin tuomioistuimen oikeuskäytännön osalta ei ole selvää, miltä osin riippumattomalle hallinnolliselle viranomaiselle asetetut vaatimukset suhtautuvat syyttäjään. Tässä vaihtoehdossa syyttäjällä, joka voisi ottaa asian päätettäväkseen, tarkoitettaisiin sellaista syyttäjää, jonka tehtävänä ei olisi myöhemmin nostaa rikoksesta syyte ja ajaa sitä oikeudenkäynnistä rikosasioissa annetun lain 1 luvun 2 §:n mukaisesti.

Syyttäjän valitsemista päätöksen tekemiseksi oikeusviranomaiseksi puoltaisi menettelyn mahdollinen joustavuus ja joutuisuus sekä jossain määrin mahdollinen kustannustehokkuus verrattuna asian käsittelemiseen tuomioistuimissa. Keskeisimpänä riskinä vaihtoehdon osalta nähtiin kuitenkin se, että ennakkolupamenettely ei ole kansallisesti vakiintunut syyttäjän tehtäviin. Huolta aiheutti myös resurssivaikutukset sekä uuden tehtävän sopiminen syyttäjän toimenkuvaan.

5.2 Muiden jäsenvaltioiden lainsäädäntö

Komissio ehdotti tekoälyasetukseen muutoksia 19.11.2025 (KOM(2025) 836 lopullinen). Neuvoston puheenjohtaja ja Euroopan parlamentti saavuttivat yhteisymmärryksen tekoälyasetuksen muutoksista 6.5.2026. Yhteisymmärryksen mukaan tekoälyasetuksen jälkikäteistä biometristä etätunnistamista koskevien määräysten voimaantulo siirtyy ja ne tulevat voimaan vasta 2.12.2027. Monet jäsenmaista eivät siten ole vielä säätäneet tekoälyasetuksen edellyttämästä ennakkolupamenettelystä jälkikäteisessä biometrisessä etätunnistamisessa käytettävän tekoälyjärjestelmän käyttöön. Ruotsissa on suunnitteilla osoittaa luvanantaminen syyttäjälle, joka on oikeusviranomainen (DS. 2025:32). Tsekin tasavallassa luvanantava viranomainen on tuomioistuin. Tanskan opt-out järjestelyn nojalla tekoälyasetuksen 26 artiklaa ei sovelleta Tanskassa. Sloveniassa ei käytetä jälkikäteistä biometristä etätunnistamista. Liettuaissa, Unkarissa, Itävallassa, Irlannissa ja Kreikassa, Espanjassa tekoälysäädöksen toimeenpano ennakkolupaviranomaisen osalta tehdään myöhemmin.

7 Säännöskohtaiset perustelut

7.2 Laki jälkikäteisessä biometrisessä etätunnistamisessa käytettävän tekoälyjärjestelmän käytön luvanantamismenettelystä

Esityksessä ehdotetaan säädettäväksi laki jälkikäteisessä biometrisessä etätunnistamisessa käytettävän tekoälyjärjestelmän käytön luvanantamismenettelystä. Laissa säädettäisiin tekoälyasetuksen 26 artiklan 10 alakohdan edellyttämästä luvanantamismenettelystä. Esityksessä on päädytty ehdottamaan erillistä lakia, jotta sääntely kattaisi poliisin lisäksi myös tullin ja rajavartiolaitoksen. Vaihtoehtoisesti sama sääntely olisi tullut sijoittaa jokaista eri viranomaista koskevaan toimialakohtaiseen lainsäädäntöön. Erillinen luvanantamismenettelyä koskeva laki koskee yleisen järjestyksen ja turvallisuuden ylläpitämistä ja kuuluu siten valtioneuvoston ohjesäännön 15 §:n nojalla sisäministeriön toimialaan.

Laissa säädettäisiin suuririskisen tekoälyjärjestelmän, tässä yhteydessä tekoälyavusteisen jälkikäteisen biometrisen etätunnistamisen, käytön vaatimasta lupamenettelystä. Esityksen yleisperusteluissa todetuin osin lupavaatimus koskisi kansallisen toimivaltuussääntelyn perusteella tehtävää jälkikäteistä biometristä etätunnistamista. Ehdotettavan säännöksen taustalla on tekoälyasetuksen 26 artiklan 10 kohta, jonka mukaan rikoksesta epäillyn tai tuomitun henkilön kohdennettua etsintää koskevan tutkinnan yhteydessä suuririskisen tekoälyjärjestelmän, joka on tarkoitettu käytettäväksi jälkikäteiseen biometriseen etätunnistukseen, käyttöönottoajan on pyydyttävä oikeusviranomaiselta tai hallintoviranomaiselta, jonka päätös on sitova ja johon sovelletaan tuomioistuINVALVONTAA, lupaa kyseisen järjestelmän käyttöön etukäteen tai ilman aiheetonta viivytystä ja viimeistään 48 tunnin kuluessa kyseisen järjestelmän käyttöön, paitsi jos sitä käytetään mahdollisen epäillyn alustavaan tunnistamiseen rikokseen suoraan liittyvien objektiivisten ja todennettavissa olevien tosiseikkojen perusteella. Asetuksen artiklassa todetaan, että käyttö on rajoitettava siihen, mikä on ehdottoman välttämätöntä kyseessä olevan rikoksen tutkintaa varten eikä tällaista suuririskistä tekoälyjärjestelmää, joka on tarkoitettu käytettäväksi jälkikäteiseen biometriseen etätunnistukseen, saa missään tapauksessa käyttää lainvalvontatarkoituksiin kohdentamattomalla tavalla ilman minkäänlaista yhteyttä tiettyyn rikokseen, rikosoikeudelliseen menettelyyn, todelliseen ja välittömään tai todelliseen ja ennakoitavissa olevaan rikoksen uhkaan tai tietyn kadonneen henkilön etsimiseen.

1 §. Soveltamisala. Pykälässä säädettäisiin lain soveltamisalasta. Tekoälyasetuksen 3 artiklan määritelmät ovat perustana, kun arvioidaan, onko kyse asetuksen tarkoittamasta jälkikäteisessä biometrisessä etätunnistamisessa käytettävästä tekoälyjärjestelmästä. Asetuksen 3 artiklan 35 alakohdan mukaan biometrisellä tunnistamisella tarkoitetaan ihmisen fyysisten, fysiologisten,

käyttäytymiseen liittyvien tai psykologisten ominaisuuksien automaattista tunnistamista luonnollisen henkilön henkilöllisyyden toteamiseksi vertaamalla kyseisen henkilön biometrisiä tietoja tietokantaan tallennettuihin toisten yksilöiden biometrisiin tietoihin. Asetuksen 3 artiklan 41 alakohdan mukaan biometrisellä etätunnistusjärjestelmällä tarkoitetaan tekoälyjärjestelmää, jonka avulla luonnolliset henkilöt voidaan tunnistaa ilman heidän aktiivista osallistumistaan. Tyypillisesti etäältä, vertaamalla henkilön biometrisiä tietoja viitetietokantaan sisältyviin biometrisiin tietoihin. Asetuksen 3 artiklan 43 alakohdan mukaan jälkikäteisellä biometrisellä tunnistamisella tarkoitetaan muuta kuin reaaliaikaista biometristä etätunnistusjärjestelmää. Edellä mainittujen asetuksen määritelmät sisältävät kaksi ratkaisevaa elementtiä: Jälkikäteinen biometrinen etätunnistaminen edellyttää biometrinen tunnistamisen vertailua tietokantaan tallennettuihin biometrisiin tietoihin luonnollisen henkilön tunnistamiseksi. Tunnistukseen käytettävän tekoälyjärjestelmän tulee olla perustettu henkilöiden tunnistamiseen. Muu käyttötarkoitus kuten henkilöiden havaitseminen, ryhmittymisen tunnistaminen, seuranta tai paikantaminen käyttämättä biometrinen tunnistamisen tietokantaa ei ole tekoälyasetuksen tarkoittamaa jälkikäteistä biometristä etätunnistamista, jossa tarkoituksena olisi rikoksesta epäillyn tai tuomitun tunnistaminen.

Asetuksen liitteessä III kohdassa 1(a) luokitellaan jälkikäteinen biometrinen etätunnistusjärjestelmä korkean riskin tekoälyjärjestelmäksi ja siten tekoälyasetuksen asettamien velvoitteiden alaiseksi. Tekoälyasetuksen 6 artiklan 3 alakohta sisältää kuitenkin poikkeuksen liitteessä III säädettyyn luokitteluun. Liitteessä III luokiteltua tekoälyjärjestelmää ei kuitenkaan katsota korkean riskin tekoälyjärjestelmäksi, jos se ei aiheuta merkittävää vahingon riskiä luonnollisten henkilöiden terveydelle, turvallisuudelle tai perusoikeuksille, mukaan lukien se, että se ei vaikuta olennaisesti päätöksenteon sisältöön. Tällaisen tilanteen katsotaan olevan käsillä 6 artiklan 3d alakohdan mukaan, jos tekoälyjärjestelmä on tarkoitettu suorittamaan valmistelutehtäviä, joka koskee liitteessä III lueteltujen käyttötapauksien kannalta merkityksellistä arviota. Näin ollen jälkikäteinen biometrinen etätunnistusjärjestelmä ei ole liitteessä III tarkoitettu suuririskinen tekoälyjärjestelmä, jos sen käyttö on rajoitettu suorittamaan valmistelutehtäviä. Asetuksen 6 artiklan 5 alakohdan mukaan komission tulee antaa kattava luettelo käytännön esimerkeistä sellaisten tekoälyjärjestelmien käyttötapauksista, jotka ovat suuririskisiä ja muita kuin suuririskisiä.

Siltä osin, kun kyse on tekoälyasetuksen tarkoittaman suuririskisen tekoälyjärjestelmän käytöstä jälkikäteisessä biometrisessä etätunnistamisessa, asetuksen 26 artiklassa säädetään näiden suuririskisten tekoälyjärjestelmien käyttöönottajien velvollisuuksista. Artiklan 10 kohdassa edellytetään, että rikoksesta epäillyn tai tuomitun henkilön kohdennettua etsintää koskevan tutkinnan yhteydessä suuririskisen tekoälyjärjestelmän, joka on tarkoitettu käytettäväksi jälkikäteiseen biometriseen etätunnistukseen, käyttöönottajalla on pyydettävä oikeus- tai hallintoviranomaiselta ennakkolupa. Lupaa ei tarvitse hakea, jos suuririskistä tekoälyjärjestelmää käytetään mahdollisen epäillyn alustavaan tunnistamiseen rikokseen suoraan liittyvien objektiivisten ja todennettavissa olevien tosiseikkojen perusteella. Komissio antaa lisäksi tarkentavia ohjeita asetuksen tarkoittamista käyttötapauksista.

Poliisi saa jälkikäteisessä biometrisessä etätunnistamisessa käytettävää aineistoa oman teknisen valvontansa järjestelmistä tai esitutkinnassa todisteena kerätyistä yritysten, yhteisöjen tai yksityisten kameratallenteista. Poliisin toimivaltuudesta tekniseen valvontaan säädetään poliisilaissa (4 luvun 1 §) ja poliisin toimivaltuuksista hankkia rikosten selvittämiseksi tarvittavaa tietoa säädetään pakkokeinolaissa (806/2011) ja esitutkintalaissa (805/2011). Lisäksi toimivaltuuksilla hankittujen henkilötietojen (ml. biometrinen tietojen) käsittelystä säädetään poliisin henkilötietolaissa (616/2019). Lisäksi poliisin toimivaltuuksista hankkia rikosten estämiseksi ja paljastamiseksi sekä vaaran torjumiseksi tarvittavaa tietoa säädetään poliisilaissa (872/2011) 4 ja 5 luvussa.

Pykälässä tarkoitettulla luvanantamismenettelyn alaisella jälkikäteisellä biometrisellä etätunnistamisella tarkoitettaisiin tunnistamisen kohteena olevan henkilön biometrisen tunnisteiden kuten kasvokuvasta tehdyn biometrisen mallin vertaamista biometriseen tietokantaan kuten esimerkiksi valvontakameratallennemateriaaliin muussa kuin alustavassa tunnistamistarkoituksessa. Pykälässä todettaisiin, ettei ennakkolupaa tarvittaisi asetuksen 26 artiklan 10 kohdan mukaisesti silloin, kun jälkikäteistä biometristä etätunnistamista käytetään mahdollisen epäillyn alustavaan tunnistamiseen rikokseen suoraan liittyvien objektiivisten ja todennettavissa olevien tosiseikkojen perusteella. Silloin, kun kyse on epäillyn alustavaan tunnistamiseen liittyvästä poikkeuksesta jälkikäteiseksi biometriseksi etätunnistamiseksi kyse olisi tilanteesta, jossa henkilön kasvokuvasta tehtyä biometristä mallia verrataan poliisin tuntomerkkirekisterissä tai vastaavassa paikassa olevaan kasvokuvien tietokantaan.

Pykälässä säädettäisiin, että poliisin, tullin tai Rajavartiolaitoksen pidättämiseen oikeutetun virkamiehen olisi haettava tekoälyasetuksessa tarkoitetuissa jälkikäteisen biometrisen etätunnistamisen tilanteissa lupaa suuririskisen tekoälyjärjestelmän käyttöön Poliisihallitukseen perustetavalta ennakkolupatoiminnolta. Pykälässä ei säädetä niistä biometrisen etätunnistamisen tilanteista, joita asetuksen soveltamisala ei kata. Nämä tilanteet jäävät olemassa olevan muun lain säädännön varaan.

2 §. Ennakkolupatoiminto. Pykälässä säädetään ennakkolupatoiminnon perustamisesta Poliisihallituksen yhteyteen. Kyseessä olisi tekoälyasetuksen tarkoittamasta uudesta hallintoviranomaisesta. Ennakkolupatoiminnon tehtävänä tämän lain nojalla olisi käsitellä tekoälyasetuksen soveltamisalaan kuuluvien jälkikäteisessä biometrisessä etätunnistamisessa käytettävänä suuririskisen tekoälyjärjestelmän käyttöä koskevat lupahakemukset. Ennakkolupatoiminnolle voitaisiin säätää myös muita tehtäviä.

Pykälän 1 momentin mukaisesti ennakkolupatoiminto toimisi Poliisihallituksen yhteydessä, mutta riippumattomana ja erillisenä ja itsenäisenä toimintona muusta poliisitoiminnasta. Pykälän 1 momentin 2 virkkeen mukaan ennakkolupatoiminto toimisi tehtävässään riippumattomasti ja puolueettomasti. Momentin 3 virkkeen mukaan poliisin hallinnosta annetun lain (110/1992) 4 §:n 4 momenttia ei sovellettaisi ennakkolupatoiminnon toimintaan. Mainitussa säännöksessä on kyse poliisiylijohtajan mahdollisuudesta ottaa yksittäistapauksessa ratkaistavakseen hallinnon sisäisen asian, joka on säädetty muun poliisin henkilöstöön kuuluvan virkamiehen ratkaistavaksi. Säännöksellä korostetaan ennakkotarkastustoiminnon riippumatonta asemaa. Ennakkolupatoiminto ei osallistuisi poliisin operatiiviseen toimintaan, kuten rikostutkinnan suorittamiseen. Pykälän 2 momentin 1 virkkeessä säädettäisiin ennakkolupatoiminnon tehtävästä, joka olisi lain 1 §:ssä tarkoitettujen ennakkolupahakemusten käsittely ja ratkaiseminen.

Pykälän 3 momentissa säädettäisiin tarkennuksista ennakkolupatoiminnon riippumattomuuteen ja puolueettomuuteen. Ennakkolupatoiminto perustettaisiin Poliisihallituksen yhteyteen, mikä jo itsessään varmistaisi, ettei se olisi mukana poliisin operatiivisessa työssä. Poliisihallitus ei toimi esitutkintaviranomaisena, kuten poliisilaitokset ja Keskusrikospoliisi, jolloin kiinteää yhteyttä myöskään poliisin operatiiviseen toimintaa ei olisi. Ehdotetun 3 momentin ensimmäisessä virkkeessä kuitenkin varmistettaisiin, ettei ennakkotarkastustoiminnon henkilöstöllä olisi yhteyksiä rikosten esitutkintaan. Momentin 2 virkkeessä säädettäisiin lisäksi ennakkolupatoiminnon henkilöstön kelpoisuusvaatimuksesta. Koska on tärkeää, että ennakkolupahakemukset arvioitaisiin ja tutkittaisiin huolella, ottaen huomioon biometristen tietojen ja suuririskisten tekoälyjärjestelmien perus- ja ihmisoikeuksien suojaamisen kannalta. Ennakkolupatoiminnon henkilöstöllä tulisi olla tehtävään soveltuva korkeakoulututkinto ja tehtävän edellyttämä riittävä oikeudellinen asiantuntemus. Tehtävässä voisi siten toimia oikeustieteen maisterin lisäksi esimerkiksi riittävän tietosuojasääntelyn osaamisen omaava poliisimies tai rikostorjunnan osaaja.

3 §. *Jälkikäteisessä biometrisessä etätunnistamisessa käytettävän tekoälyjärjestelmän käytöstä päättäminen.* Pykälässä säädettäisiin ennakkolupamenettelystä mukaan lukien tekoälyasetuksen mukaiset kiiretilanteet.

Pykälän 1 momentissa säädettäisiin ennakkolupatoiminnon tehtäväksi päättää luvan antamisesta jälkikäteisessä biometrisessä etätunnistamisessa käytettäväksi tarkoitettun tekoälyjärjestelmän käyttöön tekoälyasetuksen 26 artiklan 10 kohdassa tarkoitettua rikoksesta epäillyn tai tuomitun henkilön kohdennetussa etsinnässä tutkinnan yhteydessä poliisin, Tullin tai Rajavartiolaitoksen pidättämiseen oikeutetun virkamiehen hakemuksesta. Ennakkolupatoiminnon on arvioitava, onko kyse tekoälyasetuksen mukaisesta tilanteesta ja täyttyykö siinä tekoälyasetuksen edellytys siitä, että 26 artiklan 10 kohdan soveltamisalaan kuuluvissa jälkikäteisessä biometrisessä etätunnistamisessa käytettäväksi tarkoitettun tekoälyjärjestelmän kukin käyttö on rajoitettava siihen, mikä on ehdottoman välttämätöntä kyseessä olevan rikoksen tutkintaa varten.

Pykälän 2 momentissa säädettäisiin tekoälyasetuksen mukaisesti poliisin, Tullin tai Rajavartiolaitoksen pidättämiseen oikeutetun virkamiehen toimivallasta päättää 1 momentissa tarkoitettua suuririskisen tekoälyjärjestelmän käytöstä siihen asti, kunnes ennakkolupatoiminto on ratkaissut luvan myöntämistä koskevan hakemuksen.

Pykälän 3 momentissa säädettäisiin tekoälyasetuksen mukaisesti poliisin, Tullin tai Rajavartiolaitoksen pidättämiseen oikeutetun virkamiehen velvollisuudesta saattaa ennakkolupahakemus ennakkolupatoiminnon ratkaistavaksi etukäteen tai ilman aiheutonta viivytystä ja viimeistään 48 tunnin kuluttua jälkikäteisessä biometrisessä etätunnistamisessa käytettäväksi tarkoitettun tekoälyjärjestelmän käytön aloittamisesta, kun kyse on tekoälyasetuksen 26 artiklan 10 kohdassa tarkoitettua rikoksesta epäillyn tai tuomitun henkilön kohdennetusta etsinnästä tutkinnan yhteydessä.

Pykälän 4 momentissa säädettäisiin selkeyden vuoksi siitä, että muissa kuin tekoälyasetuksen soveltamisalaan kuuluvissa jälkikäteisen biometrisen etätunnistamisen tilanteissa poliisin, Tullin ja Rajavartiolaitoksen pidättämiseen oikeutettu virkamies voi päättää sen jälkikäteisen biometrisen etätunnistamisen käytöstä ja myös suuririskistä tekoälyjärjestelmää käyttäen. Tekoälyasetuksen 26 artikla 10 kohdan soveltamisala kattaa ainoastaan jälkikäteiseen biometriseen etätunnistamiseen käytettäväksi tarkoitettun suuririskisen tekoälyjärjestelmän käytön rikoksesta epäillyn tai tuomitun henkilön kohdennettua etsintää koskevan tutkinnan yhteydessä. Tältäkin osin asetus jättää soveltamisalan ulkopuolelle tilanteet, joissa jälkikäteisessä biometrisessä etätunnistamisessa käytetään suuririskistä tekoälyjärjestelmää mahdollisen epäillyn alustavaan tunnistamiseen rikokseen suoraan liittyvien objektiivisten ja todennettavissa olevien tosiseikkojen perusteella. Lisäksi komissio antaa tekoälyasetuksen nojalla erilliset oikeudellisesti sitomattomat ohjeet käyttötapauksista, joihin muun ohella tekoälyasetuksen 26 artiklan 10 kohta soveltuu.

4 §. *Menettely ennakkolupatoiminnossa.* Pykälän 1 momentissa säädetään, että laissa tarkoitettu lupahakemus on otettava viipymättä ennakkolupatoiminnossa käsittelyyn ja asia on käsiteltävä kiireellisesti. Rikoksesta epäillyn ja tuomitun kohdennettu etsintä on syytä suorittaa mahdollisimman ripeästi rikosvastuun toteuttamiseksi ja sen vuoksi lupakäsittelyn tulee sujua kiireellisesti. Asian käsittely tulee suorittaa kirjallisesti, sillä pykälän 2 momentin mukaisesti asia voidaan ratkaista kuulematta kohdennetun etsinnän kohteena olevaa rikoksesta epäiltyä tai tuomitua. Etsinnän kohteena olevan henkilön olinpaikka ei menettelyn tässä vaiheessa ole useinkaan tiedossa. Jos henkilön olinpaikka on tiedossa, niin biometrisessä etätunnistamisessa on kyse rikostutkinnan operatiivisesta vaiheesta, jossa jälkikäteisen biometrisen etätunnistamisen käytön paljastaminen sen kohteena olevalle todennäköisesti voisi vaarantaa tutkintaa. Pykälän 3 momentissa säädettäisiin, että ennakkolupatoiminnon päätös ei olisi oikeudenkäynnistä

hallintoasioissa annetussa laissa (808/2019) tarkoitettu valituskelpoinen hallintopäätös. Jäljempänä lain 9 §:ssä säädetäisiin sen henkilön, johon jälkikäteinen biometrisen etätunnistaminen on kohdennettu, oikeudesta saattaa lupapäätös tuomioistuimen tutkittavaksi.

5 §. Hakemuksen ja päätöksen sisältö. Pykälän 1 momentissa säädetäisiin siitä, mitä jälkikäteisessä biometrisessä etätunnistamisessa käytettävän tekoälyjärjestelmän käyttöä koskevassa hakemuksessa ja luvassa on mainittava. Pykälän 2 momentissa säädetäisiin poliisin, Tullin ja Rajavartiolaitoksen oikeudesta luovuttaa salassapitosäännösten estämättä luovuttaa ennakkolupatoiminnolle sen tehtävien hoitamiseksi välttämättömät asiakirjat, tiedot ja muun aineiston. Asian käsittelyssä on kiinnitettävä erityistä huomiota salassapitovelvollisuuden toteutumiseen ja siihen, että asiakirjoihin ja tietojärjestelmiin sisältyvien tietojen suoja turvataan tarvittavin menettelytavoin ja tietoturvasääntelyin.

6 §. Luvan voimassaoloaika. Pykälässä säädetäisiin jälkikäteisessä biometrisessä etätunnistamisessa käytettävän tekoälyjärjestelmän käyttöä koskevan luvan voimassaoloajasta. Lupa tulisi antaa luvan antopäivästä tai hakemuksessa mainitusta epäillyn rikoksen tapahtuma-ajankohdasta alkaen enintään kuudeksi kuukaudeksi kerrallaan. Riittävän pitkä luvan voimassaoloaika edistää rikostutkinnan edetessä jälkikäteisen biometrisen etätunnistamisen käytön luvassa määritellyissä tilanteissa. Lisäksi säädetäisiin mahdollisuudesta jatkaa luvan voimassaoloa kuusi kuukautta kerrallaan poliisin, Tullin tai Rajavartiolaitoksen pidättämiseen oikeutetun virkamiehen hakemuksesta, mikäli edellytykset luvan antamiselle on luvan voimassaolon päättyessä edelleen voimassa.

7 §. Lupahakemuksen hylkääminen. Pykälässä säädetäisiin tekoälyasetuksen mukaisesti tilanteesta, jossa ennakkolupatoiminto hylkäisi lupahakemuksen. Tällöin tulee soveltaa tekoälyasetuksen 26 artiklan 10 kohdan toisen kappaleen mukaista välitöntä lopettamis- ja poistovelvollisuutta.

8 §. Lupapäätöksestä ilmoittaminen. Pykälän 1 momentissa säädetäisiin siitä, että poiketen siitä, mitä viranomaisten toiminnan julkisuudesta annetun lain (621/1999) 11 §:ssä säädetään, henkilöllä, jonka oikeutta tai velvollisuutta asia koskee, ei ole oikeutta saada tietoa tässä laissa tarkoitettua lupapäätöksestä ennen kuin hänet on tavoitettu. Tämä johtuu toisaalta tavoitteesta toisaalta turvata rikosmenettelyä ja toisaalta siitä, että usein rikoksesta epäillyn tai tuomitun, joka on rikostutkinnassa kohdennetun etsinnän kohteena, olinpaikka on tuntematon. Pykälän 2 momentissa säädetäisiin oikeusturvan toteuttamiseksi, että kun tässä laissa tarkoitettua lupapäätöksen kohde on tavoitettu, lupapäätöksen kohteelle on ilmoitettava viivytyksestä lupapäätöksestä, jollei antamatta jättäminen ole välttämätöntä valtion turvallisuuden varmistamiseksi taikka hengen, terveyden, yksityisyyden tai salassa pidettävien taktisten ja teknisten menetelmien suojaamiseksi eikä ilmoittaminen enää vaaranna rikoksen selvittämistä tai rikosten estämistä.

9 §. Lupapäätöksen saattaminen tuomioistuimen tutkittavaksi. Pykälässä säädetäisiin tekoälyasetuksen 26 artiklan 10 kohdan vaatimusten mukaisesti siitä, että ennakkoluvan antaneen hallintoviranomaisen päätöksen tuomioistuinvalvonnasta. Pykälän 1 momentin mukaan se, jonka kohdennettuun etsintään on annettu lupa käyttää jälkikäteisessä biometrisessä etätunnistamisessa käytettäväksi tarkoitettua tekoälyjärjestelmää, on oikeus saattaa asia tuomioistuimen tutkittavaksi. Asianosaisen vaatimuksesta Helsingin käräjäoikeuden on todettava, ovatko jälkikäteisen biometrisen etätunnistamisen edellytykset tekoälyjärjestelmää käyttäen olleet olemassa. Vaatimus on tehtävä 30 päivän kuluessa siitä, jolloin vaatimuksen esittäjä on saanut tiedon häntä koskevasta biometrisestä jälkikäteisestä etätunnistamisesta tekoälyjärjestelmää käyttäen tekoälyasetuksen 26 artiklan 10 kohdan tarkoittamassa lupapäätöksestä. Pykälän 2 momentissa säädetäisiin, että vaatimuksen käsittelyyn sovelletaan, mitä pakkokeinolain 3 luvun 1

§:n 1 momentissa ja 3 §:ssä säädetään vangitsemisvaatimuksen käsittelemisestä. Lisäksi momentissa säädettäisiin oikeudesta tulla kuulluksi ja mahdollisuudesta ratkaista asia ilman istun- tokäsittelyä. Pykälän 3 momentissa säädettäisiin valitusoikeudesta tuomioistuimen päätökseen.

10 §. Voimaantulo. Pykälässä säädettäisiin lain voimaantulosta.

12.8. Luvanantamismenettely jälkikäteiseen biometriseen etätunnistamiseen

Esityksessä ehdotetussa laissa jälkikäteisessä biometrisessä etätunnistamisessa käytettävän tekoälyjärjestelmän käytön luvanantamismenettelystä säädettäisiin, että Poliisihallituksen yhtey- teen perustettava uusi hallintoviranomainen, ennakkolupatoiminto, arvioisi 26 artiklan 10 koh- dan säätämää poikkeusta lukuun ottamatta jälkikäteisen biometrisen etätunnistusjärjestelmän käytön edellytysten täyttymistä tekoälyasetuksen soveltamisalaan kuuluvissa tilanteissa suh- teessa perusoikeuksien toteutumiseen. Ennakkolupatoiminnon on arvioitava, onko kyse teko- älyasetuksen mukaisesta tilanteesta ja täyttyykö siinä tekoälyasetuksen edellytys siitä, että 26 artiklan 10 kohdan soveltamisalaan kuuluvissa jälkikäteisessä biometrisessä etätunnistamisessa käytettäväksi tarkoitetun tekoälyjärjestelmän kukin käyttö on rajoitettava siihen, mikä on eh- dottoman välttämätöntä kyseessä olevan rikoksen tutkintaa varten. Esityksessä ehdotetusti hal- lintoviranomaisen etukäteisvalvonta, tässä yhteydessä tekoälyasetuksen tarkoittama luvananto- menettely, kattaisi vain tekoälyasetuksen soveltamisalaan kuuluvat tilanteet.

Ehdotetut säännökset täyttävät perustuslain 2 §:n 3 momentissa säädetyn julkisen vallan käytön lainmukaisuuden vaatimuksen. Jälkikäteinen biometrinen etätunnistaminen on poliisille ja eräille muille lainvalvontaviranomaisille jo nykyisin sallittua voimassa olevan, tämän esityksen nykytilan kuvauksessa kuvatus, lainsäädännön nojalla, ja esityksessä ehdotettu hallintoviran- omaisen lupamenettely tarkentaa ja selkeyttää sääntelyä yksilön oikeusturvan vahvistamiseksi. Luvanantomenettelyä koskevat säännökset ovat riittävän tarkkarajaisia, perusteltuja ja suhteel- lisuusperiaatteen mukaisia. Esitykseen sisällytetty jälkikäteisen biometrisen etätunnistamisen kohteen oikeus saattaa lupapäätös tuomioistuimen tutkittavaksi turvaa perustuslain 21 §:n edel- lyttämällä tavalla yksilön oikeuden saada asia käsitellyksi toimivaltaisessa tuomioistuimessa ilman aiheutonta viivytystä ja oikeuden saada päätös, joka koskee hänen oikeuksiaan tai velvol- lisuuksiaan, perustelluksi. Tuomioistuinkontrolli muodostaa keskeisen oikeusturvaa varmista- van elementin, ja osaltaan myös takaa sääntelyn hyväksyttävyyden perusoikeusjärjestelmän kannalta.

Esityksessä ehdotetun seurauksena Poliisihallituksen yhteyteen perustettava hallintoviranomai- nen, ennakkolupatoiminto, arvioisi asetuksen tarkoittaman 26 artikla 10 kohdassa tarkoitetun jälkikäteisessä biometrisessä etätunnistamisessa käytettävän suuririskisen tekoälyjärjestelmän käytön edellytysten täyttymistä suhteessa perusoikeuksien toteutumiseen jo etukäteisesti. Li- säksi henkilöllä olisi oikeus saattaa lupapäätös tuomioistuimen tutkittavaksi. Käytettävissä olisi myös ennakkolupatoiminnon jälkikäteisvalvonta perustelluissa kiiretilanteissa. Hallintoviran- omaisen etukäteisvalvonnalla ja tuomioistuimen jälkikäteisvalvonnalla varmistettaisiin oikeu- denmukainen tasapaino yhtäältä rikollisuuden torjunnan yhteydessä suoritettavan tutkinnan tar- peisiin liittyvien julkisten intressien ja toisaalta yksityiselämän kunnioittamista ja henkilötieto- jen suojaa koskevien perusoikeuksien välillä.

12.9 Ahvenanmaan asema ja suhde itsehallintoon

Luvanantamismenettely jälkikäteiseen biometriseen etätunnistamiseen

Itsehallintolain 18 §:n 6 kohdan mukaan maakunnalla on lainsäädäntövalta yleistä järjestystä ja turvallisuutta koskevissa asioissa, mutta itsehallintolain 27 §:n 34 kohdan mukaan valtakunnalla

Luonnos

on lainsäädäntövalta asioissa, jotka koskevat valtion turvallisuutta. Poliisihallinnosta Ahvenanmaan maakunnassa annetun tasavallan presidentin asetuksen (56/2020) mukaan poliisitoimesta maakunnassa huolehtivat sekä maakunta että valtakunta. Maakunnan poliisi vastaa yleisen järjestyksen ja turvallisuuden ylläpitämisestä, kun taas valtakunnan poliisi vastaa valtion turvallisuudesta sekä hoitaa suojelupoliisille ja keskusrikospoliisille kuuluvat tehtävät. Poliisihallitus johtaa viimeksi mainittua valtion turvallisuutta koskevaa poliisitoimintaa maakunnan poliisin osallistuessa näihin tehtäviin.

Ahvenanmaalla toimii oma poliisilaitos, joka toimii maakuntahallituksen alaisuudessa.

Rajavartiolaitosta koskevat asiat kuuluvat itsehallintolain 27 §:n 1 momentin 34 kohdan mukaisesti valtakunnan lainsäädäntövaltaan. Lisäksi eräitä maakunnan lainsäädäntövaltaan kuuluva asioita on siirretty Rajavartiolaitoksen tehtävistä Ahvenanmaalla annetulla tasavallan presidentin asetuksella (255/2024) Rajavartiolaitoksen hoidettavaksi.

Laki

Laki jälkikäteisessä biometrisessä etätunnistamisessa käytettävän tekoälyjärjestelmän käytön luvanantamismenettelystä

Eduskunnan päätöksen mukaisesti säädetään:

1 §

Luvan hakeminen jälkikäteisessä biometrisessä etätunnistamisessa käytettävän tekoälyjärjestelmän käyttöön rikoksesta epäillyn tai tuomitun kohdennetussa etsinnässä

Poliisin, Tullin tai Rajavartiolaitoksen pidättämiseen oikeutetun virkamiehen on haettava 2 §:ssä tarkoitetulta ennakkolupatoiminnolta lupa jälkikäteiseen biometriseen etätunnistamiseen käytettäväksi tarkoitetun tekoälyjärjestelmän käyttöön, kun kyse on Euroopan parlamentin ja neuvoston asetuksen (EU) 2024/1689 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), jäljempänä *tekoälyasetus*, 26 artiklan 10 kohdassa tarkoitetusta rikoksesta epäillyn tai tuomitun henkilön kohdennetusta etsinnästä tutkinnan yhteydessä.

2 §

Ennakkolupatoiminto

Poliisihallituksen yhteydessä toimii ennakkolupatoiminto. Ennakkolupatoiminto toimii tehtävässään riippumattomasti ja puolueettomasti. Ennakkolupatoiminnon toimintaan ei sovelleta poliisin hallinnosta annetun lain (110/1992) 4 §:n 4 momenttia.

Ennakkolupatoiminnon tehtävänä on tämän lain 1 §:n mukaisten poliisin, Tullin ja Rajavartiolaitoksen pidättämiseen oikeutetun virkamiehen tekemien lupahakemusten käsittely ja ratkaiseminen.

Ennakkolupatoiminnon henkilöstön on toimittava ilman kytköksiä rikosten esitutkintaan. Ennakkolupatoiminnon henkilöstöllä tulee olla tehtävään soveltuva korkeakoulututkinto, riittävä oikeudellinen asiantuntemus, hyvä perehtyneisyys henkilötietojen suojaa koskeviin asioihin ja muu tehtävän hoidon edellyttämä pätevyys

3 §

Jälkikäteisessä biometrisessä etätunnistamisessa käytettävän tekoälyjärjestelmän käytöstä päättäminen

Ennakkolupatoiminto päättää luvan antamisesta jälkikäteisessä biometrisessä etätunnistamisessa käytettäväksi tarkoitetun tekoälyjärjestelmän käyttöön tekoälyasetuksen 26 artiklan 10 kohdassa tarkoitetusta rikoksesta epäillyn tai tuomitun henkilön kohdennetussa etsinnässä tutkinnan yhteydessä poliisin, Tullin tai Rajavartiolaitoksen pidättämiseen oikeutetun virkamiehen hakemuksesta.

Luonnos

Jos asia ei siedä viivytystä, pidättämiseen oikeutettu virkamies voi päättää käytöstä siihen asti, kunnes ennakkolupatoiminto on ratkaissut luvan myöntämistä koskevan hakemuksen.

Asia on saatettava ennakkolupatoiminnon ratkaistavaksi etukäteen tai ilman aiheetonta viivytystä ja viimeistään 48 tunnin kuluttua jälkikäteisessä biometrisessä etätunnistamisessa käytettäväksi tarkoitetun tekoälyjärjestelmän käytön aloittamisesta, kun kyse on tekoälyasetuksen 26 artiklan 10 kohdassa tarkoitetusta rikoksesta epäillyn tai tuomitun henkilön kohdennetusta etsinnästä tutkinnan yhteydessä.

Poliisin, Tullin ja Rajavartiolaitoksen pidättämiseen oikeutettu virkamies voi päättää jälkikäteisessä biometrisessä etätunnistamisessa käytettävän tekoälyjärjestelmän käytöstä muissa kuin tekoälyasetuksen 26 artiklan 10 kohdan tarkoittamissa tilanteissa.

3 §

Menettely ennakkolupatoiminnossa

Jälkikäteisessä biometrisessä etätunnistamisessa käytettäväksi tarkoitetun tekoälyjärjestelmän käyttöä tekoälyasetuksen 26 artiklan 10 kohdassa tarkoitetussa rikoksesta epäillyn tai tuomitun henkilön kohdennetussa etsinnässä tutkinnan yhteydessä koskeva hakemus on otettava viipymättä ennakkolupatoiminnossa käsiteltäväksi. Asia on ratkaistava kiireellisesti. Käsittely tapahtuu kirjallisesti.

Asia voidaan ratkaista kuulematta kohdennetun etsinnän kohteena olevaa rikoksesta epäiltyä tai tuomittua.

Ennakkolupatoiminnon päätös ei ole oikeudenkäynnistä hallintoasioissa annetussa laissa (808/2019) tarkoitettu valituskelpoinen hallintopäätös

4 §

Hakemuksen ja päätöksen sisältö

Jälkikäteisessä biometrisessä etätunnistamisessa käytettävän tekoälyjärjestelmän käyttöä koskevassa hakemuksessa ja luvassa on mainittava:

- 1) epäilty rikos, sen epäilty teko aika ja -paikka taikka tuomittu rikos;
- 2) tutkinnassa olevan kohdennetun etsinnän kohteena oleva rikoksesta epäilty tai rikoksesta tuomittu;
- 3) tosiseikat, joiden nojalla jälkikäteisessä biometrisessä etätunnistamisessa käytettäväksi tarkoitetun tekoälyjärjestelmän käyttö on ehdottoman välttämätöntä kyseessä olevassa kohdennetussa etsinnässä;
- 4) paikka tai alue, josta kerättyä aineistoa saa käyttää jälkikäteisessä biometrisessä etätunnistamisessa käytettäväksi tarkoitetussa tekoälyjärjestelmässä rikoksesta epäillyn tai tuomitun kohdennettua etsintää koskevan tutkinnan yhteydessä;
- 5) jälkikäteisessä biometrisessä etätunnistamisessa käytettäväksi tarkoitetun tekoälyjärjestelmän käyttöä johtava ja valvova poliisin, Tullin tai Rajavartiolaitoksen pidättämiseen oikeutettu virkamies;
- 6) mahdolliset jälkikäteisessä biometrisessä etätunnistamisessa käytettäväksi tarkoitetun tekoälyjärjestelmän käyttöä koskevat rajoitukset ja ehdot.

Poliisi, Tulli ja Rajavartiolaitos saavat salassapitosäännösten estämättä luovuttaa ennakkolupatoiminnolle sen tehtävien hoitamiseksi välttämättömät asiakirjat, tiedot ja muun aineiston. Asian käsittelyssä on kiinnitettävä erityistä huomiota salassapitovelvollisuuden toteutumiseen ja siihen, että asiakirjoihin ja tietojärjestelmiin sisältyvien tietojen suoja turvataan tarvittavin menettelytavoin ja tietoturvallisuusjärjestelyin.

5 §

Luonnos

Luvan voimassaoloaika

Lupa voidaan antaa luvan antopäivästä tai hakemuksessa mainitusta epäillyn rikoksen tapahtuma-ajankohdasta alkaen enintään kuudeksi kuukaudeksi kerrallaan. Ennakkolupatoiminto voi jatkaa luvan voimassaoloa kuusi kuukautta kerrallaan poliisin, Tullin tai Rajavartiolaitoksen pidättämiseen oikeutetun virkamiehen hakemuksesta, mikäli edellytykset luvan antamiselle on luvan voimassaolon päättyessä edelleen voimassa.

6 §

Lupahakemuksen hylkääminen

Ennakkolupatoiminnon hylätessä lupahakemuksen sovelletaan asetuksen 26 artiklan 10 kohdan toisen kappaleen mukaista välitöntä lopettamis- ja poistovelvollisuutta.

7 §

Lupapäätöksestä ilmoittaminen

Poiketen siitä, mitä viranomaisten toiminnan julkisuudesta annetun lain (621/1999) 11 §:ssä säädetään, henkilöllä, jonka oikeutta tai velvollisuutta asia koskee, ei ole oikeutta saada tietoa tässä laissa tarkoitetusta lupapäätöksestä ennen kuin hänet on tavoitettu.

Kun tässä laissa tarkoitetun lupapäätöksen kohde on tavoitettu, lupapäätöksen kohteelle on ilmoitettava viivytyksestä lupapäätöksestä, jollei antamatta jättäminen ole välttämätöntä valtion turvallisuuden varmistamiseksi taikka hengen, terveyden, yksityisyyden tai salassa pidettävien taktisten ja teknisten menetelmien suojaamiseksi eikä ilmoittaminen enää vaaranna rikoksen selvittämistä tai rikosten estämistä.

8 §

Lupapäätöksen saattaminen tuomioistuimen tutkittavaksi

Sen vaatimuksesta, jonka kohdennettuun etsintään on annettu lupa käyttää jälkikäteisessä biometrisessä etätunnistamisessa käytettäväksi tarkoitettua tekoälyjärjestelmää, Helsingin käräjäoikeuden on todettava, ovatko jälkikäteisen biometrisen etätunnistamisen edellytykset tekoälyjärjestelmää käyttäen olleet olemassa. Vaatimus on tehtävä 30 päivän kuluessa siitä, jolloin vaatimuksen esittäjä on saanut tiedon häntä koskevasta biometrisestä jälkikäteisestä etätunnistamisesta tekoälyjärjestelmää käyttäen tekoälyasetuksen 26 artiklan 10 kohdan tarkoittamassa lupapäätöksestä.

Vaatimuksen käsittelemiseen sovelletaan, mitä pakkokeinolain 3 luvun 1 §:n 1 momentissa ja 3 §:ssä säädetään vangitsemisvaatimuksen käsittelemisestä. Vaatimuksen esittäjälle ja pidättämiseen oikeutetulle virkamiehelle on varattava tilaisuus tulla kuulluksi. Asia voidaan ratkaista kansliassa ilman istunkäsittelyä, jos tuomioistuin harkitsee sen soveliaaksi.

Tässä pykälässä tarkoitettua asiaa koskevasta tuomioistuimen päätöksestä saa valittaa.

8 §

Voimaantulo

Tämä laki tulee voimaan päivänä kuuta 20 .