

07.09.2021

POL-2021-105614

Pekka Sallinen
Poliisitarkastaja

Eduskunnan lakivaliokunta

Asiantuntijan lausunto valtioneuvoston kirjelmään komission ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi tekoälyn harmonisoiduksi sääntelyksi (Artificial Intelligence Act)

1 Tausta

Eduskunnan lakivaliokunta on pyytänyt 1.9.2021 lähettämällään viestillä Poliisihallitukselta kirjallista asiantuntijalausuntoa valtioneuvoston kirjelmään komission ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi tekoälyn harmonisoiduksi sääntelyksi (Artificial Intelligence Act).

Digitaalisen tiedon määrä on kasvanut ja kasvaa merkittävästi edelleen myös poliisiasioissa. Tiedon analysointia sekä tutkintaa varten poliisilla on tarve kehittää ja ottaa käyttöön uusia tehokkaita tekoälyä hyödyntäviä ratkaisuja. Tekoälyjärjestelmiin sekä niiden käyttöön kohdistuva sääntely tukee osaltaan tekoälyjärjestelmien käyttöön liittyvän luottamuksen kehittymistä. Tekoälyä hyödyntävien ratkaisujen avulla on mahdollista tehostaa poliisin toimintaa ja tukea sisäisen turvallisuuden toteutumista tavoitteiden mukaisesti.

On tarkoituksenmukaista, että ehdotetussa sääntelyssä kiinnitetään huomiota tekoälyn käyttöönoton edellytysten luomisen lisäksi myös muun muassa henkilöiden perusoikeuksien ja -vapauksien sekä erityisesti henkilötietojen korkean tason suojeluun. Ehdotusta voidaan pitää olemassa olevaa lainsäädäntöä tukevana sekä käyttötapausten riskiperustaisuutta arvioivana asetuksena. Korkean riskin tekoälyjärjestelmien käyttötapausten määritelmää tulisi kuitenkin tarkentaa yksiselitteisemmiksi ja poliisitoiminnan tarpeita vastaaviksi.

2 Asiantuntijan huomiot asetusehdotukseen

Valtioneuvoston kirjelmässä sivulla 12 mainittu asetusehdotuksen artiklan 5 esittämä kielto käyttää reaaliaikaista biometrista tunnistamista poliisitoiminnassa viittaa asetusehdotuksen artiklaan 15 liittyvään kieltoon biometriseen etätunnistamiseen julkisissa tiloissa lainvalvontatarkoituksessa, koskien täten poliisin lisäksi myös muita lainvalvontaviranomaisia. Asetusehdotus ei

kuitenkaan kiellä yksityisen turvallisuusalan suorittamaa reaaliaikaista biometristä etätunnistamista.

Lainvalvontaviranomaisilla tulisi kuitenkin olla mahdollisuudet hyödyntää biometriseen tunnistamiseen pohjautuvia tekoälyjärjestelmiä asetusehdotusta laajemmissa käyttötapauksissa. Mikäli asetuksen kanta tiukentuisi (vrt. EDPS:n lausunto), sillä olisi merkittäviä vaikutuksia poliisin toimintaan ja heikentäisi mahdollisuuksia ennalta estää, selvittää sekä paljastaa järjestäytyntä ja vakavaa tai terrorismiin liittyvää rikollisuutta. Asetuksen jatkovalmistelussa tulisi soveltuvin osin rajata kiellettyjen tekoälyjärjestelmien käyttötapauksista pois kansallisen turvallisuuden ylläpitämiseen sisältyvät tarkoitukset.

Viitaten kirjelmän kohtaan ”5.2.3 Vaikutukset viranomaisten toimintaan” korostettakoon, että hyödyntämällä tekoälyratkaisuja mm. biometrisen tunnistamisen käyttötapauksissa, on mahdollista tuottaa poliisille ja muille lainvalvontaviranomaisille merkittävää tukea digitaalisen materiaalin läpikäynnissä ja analysoinnissa. Päätöksen käytännön toimenpiteistä tekee kuitenkin viimekädessä aina virkamies, ei tekoälyjärjestelmä. Tekoälyjärjestelmien hyödyntämistä ja käytön rajaamista tulisi tarkastella laajemmin lainvalvontaviranomaisten prosesseihin liittyen.

Komission tekoälyn asetusehdotuksen ja kansallisen sääntelyn tavoitteet sekä vaatimukset tulisi yhdenmukaistaa. Esimerkiksi pakkokeinolain (806/2011) uudistuksen myötä poliisin tavoitteena on saada mahdollisuus käyttää rikoksesta epäiltyjen henkilöiden biometrisiä tietoja (esimerkiksi kasvokuva) reaaliaikaisesti suunnitelmallisen tarkkailun ja teknisen katselun yhteydessä, mutta asetusehdotuksen artiklan kohta 5 rajaa merkittävästi tätä mahdollisuutta. Nykyisin Tulli, toisin kuin poliisi, voi suorittaa reaaliaikaista kasvojentunnistusta teknisen valvonnan yhteydessä. Poliisin osalta ole-massa oleva kansallinen lainsäädäntö on vielä tiukempi kuin esitetty asetus-teksti.

Passi- ja henkilökorttiasioissa biometrisellä henkilöllisyyden todentamisella sekä laittomien kaksoishenkilöllisyyksien torjunnalla on suuri merkitys myös yhteiskunnallisesti. Tulevaisuutta ajatellen on tärkeää varmistaa, etteivät tällaiset käyttötavat kuvasta kuvaan verrattaessa jatkossakaan muutu kielletyiksi. Esitetyt muotoilut eivät siihen viittaa, joskaan esimerkiksi juuri kaksoishenkilöllisyyksien estämistä biometrisen vertailun avulla ei erikseen ole asetusehdotuksessa käsitelty. Biometrinen algoritmi ei asiakirjoja myönnettäessä missään oloissa tee päätöksiä, vaan toimii vain virkamiehen apuna. Virkamies tekee kokonaisvaltaisen tunnistuksen perusteella aina lopullisen päätöksen.

2.1 Reaaliaikaisen kasvokuvavertailun tarve teknisen valvonnan yhteydessä Schengen-alueen ulko- ja sisärajoilla

Reaaliaikaisessa kasvokuvavertailussa henkilö pyritään yksilöimään kuvavirrasta koneellisesti massasta kasvoja kuvarekisterisisältöön vertailemalla. Kasvojen tunnistukseen käytettävää teknologiaa olisi tarpeellista hyödyntää poliisilain (872/2011) 4 luvun 1 §:n teknisen valvonnan yhteydessä keskeisillä Schengen-alueen ulko- ja sisärajanylityspaikoilla, kuten satamissa ja

lentokentillä, jotka on tunnistettu liikkuvan rikollisuuden kipupisteiksi. Näissä kohteissa myös valvonnan tarve on suuri. Teknisellä laitteistolla helpotettaisiin lainmukaisesti rikoksesta epäiltyjen tunnistamista, kuten maahantulo-kiellon rikkojia sekä viranomaisten rikoksesta etsintäkuuluttamia henkilöitä. Esimerkiksi vuonna 2019 pelkästään Helsingin poliisilaitos käsitteli 228 maahantulokiellon rikkomisasiaa, joista puoleen liittyi myös muu rikosnimike.

Kokonaisuutta voidaan verrata poliisimiehen tai rajavartijan toimintaan, jossa poliisi kuva kädessä odottaa esimerkiksi laivalistalta löytynyttä maahantulo-kiellossa olevaa henkilöä. Kuvavirrasta tapahtuvan reaaliaikaisen tunnistamisen avulla virkamiehen on vain helpompi kohdentaa toimenpiteensä oikeaan henkilöön, jolloin muiden henkilöiden oikeuksia loukataan mahdollisimman vähän. Kaikissa tapauksissa järjestelmän käyttö olisi tilapäistä ja tiettyyn ennalta yksilöitävissä olevaan rikostapaukseen liittyvää. Yleisesti ottaen voidaanakin kysyä, onko perusoikeuksien kunnioittamisen kannalta parempi, että kymmenen poliisia tekee saman työn kuin tekoäly. Erikseen todettakoon, ettei jokaista Suomeen saapuvaa matkustajalaivaa vastassa ole aina edes viranomaisia.

Esimerkiksi vuoden 2016 Berliinin joulutorin iskun tavoin poliisilla voi olla tarve tunnistaa terroristiseen tekoon syylistynyt henkilö myös Schengen-alueen sisärajalta. Vastaava tilanne olisi voinut olla Suomessa elokuussa 2017, jos Turun terrori-iskun tekijä olisi onnistunut pakenemaan paikalta ja hän olisi yrittänyt paeta Turun sataman kautta ulkomaille.

Edellä mainitussa kokonaisuudessa virkamies ei automaattisesti reagoisi koneen antamiin tuloksiin, vaan varmistaisi ensin laitteiston näytöltä saadun tuloksen vastaavan etsittyä henkilöä. Kasvojentunnistusohjelmistojen on tutkitusti todettu merkittävästi tehostavan virkamiehen tekemää oikeellista tunnistamista, niin kasvojentunnistuskoulutuksen saaneiden kuin normaalien käyttäjien osalta. Järjestelmän käyttö vähentää virkamiehen tekemiä turhia tarkastuksia ja kohdistaa ne suuremmalla todennäköisyydellä oikeisiin henkilöihin.

Alkuvuodesta 2019 PTR-yhteistyössä toteutetun järjestelmän testauksen yhteydessä ohjelmisto antoi yhden virheellisen ilmoituksen kerran noin 8000 matkustajan joukosta. Testiin osallistuneista noin kymmenestä virkamiehestä järjestelmä antoi samana aikana satoja positiivisia tuloksia. Testihenkilöt myös vaihtoivat pukeutumistyyliään testin aikana.

2.2 Reaaliaikaisen kasvokuvavertailun tarve salaisten pakkokeinojen ja tiedonhankintakeinojen käytön yhteydessä

Poliisi ei voi kohdistaa kohdehenkilöihinsä reaaliaikaista kasvokuvavertailua pakkokeinolain 10 L 12 §:n suunnitelmallisen tarkkailun tai 20 §:n teknisen katselun yhteydessä. Pakkokeinolain 10 L 2 §:n mukaisesti salaisista pakkokeinoista suunnitelmallista tarkkailua ja teknistä katselua saa käyttää vain, jos niillä voidaan olettaa olevan erittäin tärkeä merkitys rikoksen selvittämi-

selle. Lainsäädännön puutteet ovat kriittisiä. Käytännössä poliisi ei voi hyödyntää nykyaikaista tekniikkaa eikä myöskään tietosuojavaltuutetun mielestä tämä ole mahdollista.¹

Poliisi voisi käyttää salaisia pakkokeinoja kuvavirrasta tunnistamisen yhteydessä esimerkiksi seuraavissa tositapahtumiin pohjautuvissa käyttötapauksissa:

1. Poliisi epäilee ulkomaalaiseen järjestäytyneeseen rikollisuuteen kuuluvia henkilöitä suunnittelevan törkeää ryöstöä Suomessa kultasepänliikkeisiin. Poliisi on kohdistanut henkilöihin suunnitelmallista tarkkailua ja todennut heidän tiedustelleen iltaisin kultasepänliikkeitä sekä mahdollisia pakoreittejä niiden ympäristössä. Henkilöt ovat palanneet Schengen-alueella sijaitsevaan kotimaahansa. Koska henkilöt matkustavat aina väärin henkilöllisyyksien turvin, käyttää poliisi suunnitelmallisessa tarkkailussa epäiltyjen tekijöiden löytämiseksi satamien teknisen valvonnan välineistöön kytkettyä henkilöiden automaattista kuvavirrasta tunnistamista. Tunnistamisen avulla on välttämätöntä löytää tekijät silloin, kun he saapuvat maahan toteuttamaan valmistelomaansa törkeää ryöstöä.

2. Mies vainoaa entistä aviopuolisoaan ja on luvannut naiselle tappavansa tämän. Mies on määrätty kärkeäoikeuden toimesta lähestymiskieltoon, jota mies on kuitenkin rikkonut toistuvasti. Miehen uhkaukset ja yhteydenotot ovat yltyneet, minkä johdosta poliisi asentaa naisen asunnon läheisyyteen teknisen katselun suojaamaan naista. Teknisen katselun yhteydessä on välttämätöntä tunnistaa kuvavirrasta epäilty tekijä, jotta poliisi ehtii ajoissa estämään miehen teot.

3. Lähi-idästä kotoisin olevat miehet vierailevat moskeijalla poliisin tarkkaillessa heitä. Vierailun jälkeen miehet siirtyvät toiseen kaupunkiin, jossa he hautaavat kerrostalon lähimetsään konepistoolin maastokätköön. Poliisi ryhtyy suorittamaan alueella teknistä katselua, jonka yhteydessä on välttämätöntä tunnistaa reaaliaikaisesti suunnitelmallisen tarkkailun piirissä olevat rikokseen liittyvät henkilöt.

4. Nuori henkilö haaveilee aiempien koulusurmaajien innoittamana toteuttavansa joukkosurman. Henkilö on poliisin tekemän uhka-arvion perusteella todettu potentiaalisesti joukkosurman tekijäksi. Henkilön haaveena on toteuttaa joukkosurma elokuvateatterissa lasten näytöksessä kahlitsemalla hätäuloskäytävät ja ampumalla lapsia teatterin etuosasta hyvässä valaistuksessa. Henkilö on käynyt harjoittelemassa ampumista ampumaradalla.

Poliisi suorittaa mahdollisella tekopaikalla teknistä katselua. Poliisin on ensiarvoisen tärkeää saada tieto reaaliaikaisesti jokaisesta vierailusta ja tunnistaa henkilö sekä mahdolliset rikoskumppanit kuvavirrasta, jotta mahdollinen suunniteltu joukkosurma kyetään estämään ajoissa. Normaalin teknisen katselun keinoin riski siitä, ettei tapahtumaa huomata ajoissa kasvaa merkittävästi, koska tallenteita ei pystytä seuraamaan reaaliaikaisesti kuukausien ajan.

¹ Tietosuojavaltuutetun vastaus Poliisihallituksen vaikutusten arviointiin 17.6.2020 Dnro 4659/81/2020. Sama tarve koskee myös salaisia tiedonhankintakeinoja poliisilain puolella.

Käytännössä kuvavirrasta tunnistamista käytettäisiin yksittäisissä rikostapauksissa, joissa poliisi jo kohdistaa muitakin tiedonhankintakeinoja kohteena olevaan henkilöön. Päätöksen biometristen tietojen käytöstä tekisi tapauskohtaisesti pidättämiseen oikeutettu (POV) virkamies, kun se on välttämätöntä. Järjestelmää käytettäisiin esimerkiksi laivalla matkustavan henkilön tunnistamiseksi silloin, kun tästä on saatu poliisin muun tiedonhankinnan kautta viitteitä. Vastaavasti tunnistamista voitaisiin käyttää esimerkiksi lapsikaappauksen uhrin tai terroristisesta rikoksesta epäillyn henkilön löytämiseksi.

2.2.1 Biometristen tietojen käytön välttämättömyys

Edellä mainittuihin esimerkkeihin viitaten korostettakoon, että biometrinen tunnistaminen on yksittäistapauksissa välttämätöntä, jotta rikosten ennalta estäminen tai rikoksen tekijän kiinnisaaminen olisi ylipäättään mahdollista. Ilman biometriseen tunnistamiseen ja siitä saatavaan hälytykseen pohjautuvaa toimintaa, tapahtuman reagointiin syntyisi kriittisiä viiveitä. Tämä pahimassa tapauksessa voisi johtaa ihmishenkien menetyksiin.

Lisäksi mainittakoon, että kohdehenkilöt pyrkivät välttämään poliisin tarkkailla rikollisen toiminnan jatkamiseksi. Tällaisina keinoina mainittakoon esimerkiksi luopuminen teknisten laitteiden käytöstä, vaatteiden vaihto erilaisiin kesken matkan, hiustyylin muuttaminen paluumatkalla sekä erikseen matkustaminen. Ihmisen on kuitenkin vaikea muuttaa pysyvästi kasvojen biometriä, jonka avulla hänet on edelleen mahdollista seuloa kuvavirrasta.

Muita samassa kuvissa olevia henkilöitä, kuin rekisterisisällön vertailukuvaan sopivia tunnistuksia, ei tallennettaisi biometriseen muotoon taustajärjestelmään. Näin toimien muiden kansalaisten perusoikeuksia ei loukattaisi eikä heidän kasvokuvansa olisi jälkikäteen haettavissa biometrisesti taustajärjestelmästä.

Entisiä kumppaneitaan uhanneiden ja kohdennetun väkivallan riskihenkilöiden suhteen voidaan sanoa, että edes viranomaisten aiempi toimintaan puuttuminen ei ole usein poistanut toimintaa epäillyn päämäärän saavuttamiseksi. Varsinkin joukkosurmaa suunnittelevat henkilöt kokevat pääsevänsä tavoitteisiinsa vasta teon toteutettuaan. Vakavaan henkeä tai terveyttä uhkaavaan tekoon pitää pystyä puuttumaan välittömästi.

3 Kokonaisuuden kustannukset

Edellä mainituissa käyttötapauksissa poliisi voisi osittain hyödyntää PTR-viranomaisten yhteistä kamerajärjestelmää, jonka rekisterinpitäjänä toimii Poliisihallitus. Näin ollen kokonaisuuden investointikustannukset olisivat arviolta 550 000 euroa sekä henkilöstö- ja ylläpistokustannukset vuosittain noin 150 000 euroa.