Translations proofread by EDPB Members.

This language version has not yet been proofread.

Ohjeet 05/2022 kasvojentunnistusteknologian käytöstä lainvalvonnan alalla

Versio 2.0

Annettu 26. huhtikuuta 2023

Aiemmat versiot

Versio 1.0	12. toukokuuta 2022	Ohjeiden hyväksyminen julkista kuulemista varten
Versio 2.0	26. huhtikuuta 2023	Ohjeiden hyväksyminen julkisen kuulemisen jälkeen

Sisällysluettelo

TIIVISTELMÄ

Yhä useammat lainvalvontaviranomaiset käyttävät tai aikovat käyttää kasvojentunnistusteknologiaa. Sitä voidaan käyttää henkilöllisyyden **todentamiseen** tai henkilön **tunnistamiseen** ja videoihin (esim. valvontakamerat) tai valokuviin. Sitä voidaan käyttää useisiin eri tarkoituksiin, kuten poliisin tarkkailulistoilla olevien henkilöiden etsimiseen tai henkilön liikkumisen seuraamiseen julkisissa tiloissa.

Kasvojentunnistusteknologia perustuu **biometristen tietojen** käsittelyyn ja kattaa siten erityisiä henkilötietoryhmiä koskevan käsittelyn. Kasvojentunnistusteknologiassa käytetään usein **tekoälyn** tai koneoppimisen komponentteja. Vaikka tämä mahdollistaa laajamittaisen tietojenkäsittelyn, siihen liittyy myös syrjinnän ja virheellisten tulosten riski. Kasvojentunnistusteknologiaa voidaan käyttää valvotuissa yksi-yhteen-tilanteissa mutta myös suuriin väkijoukkoihin ja merkittäviin liikennekeskuksiin.

Kasvojentunnistusteknologia on **arkaluonteinen väline lainvalvontaviranomaisille.** Lainvalvontaviranomaiset ovat täytäntöönpanoviranomaisia, ja niillä on suvereenit toimivaltuudet. Käytettäessä kasvojentunnistusteknologiaa puututaan usein perusoikeuksiin, myös muihin kuin henkilötietojen suojaa koskevaan oikeuteen, ja saatetaan vaikuttaa yhteiskunnalliseen ja demokraattiseen poliittiseen vakauteen.

Henkilötietojen suojaamiseksi lainvalvonnan yhteydessä vaatimukset, joista säädetään **lainvalvontatarkoituksessa käsiteltyjen henkilötietojen suojasta annetussa direktiivissä**, jäljempänä ’lainvalvontadirektiivi’, on täytettävä. Lainvalvontadirektiivissä säädetään kasvojentunnistusteknologian käyttöön liittyvästä kehyksestä, erityisesti direktiivin 3 artiklan 13 kohdassa (termi 'biometriset tiedot’), 4 artiklassa (henkilötietojen käsittelyä koskevat periaatteet), 8 artiklassa (käsittelyn lainmukaisuus), 10 artiklassa (erityisiä henkilötietoryhmiä koskeva käsittely) ja 11 artiklassa (automatisoidut yksittäispäätökset).

Kasvojentunnistusteknologian käyttö voi vaikuttaa myös useisiin muihin perusoikeuksiin. Näin ollen **Euroopan unionin perusoikeuskirja**, jäljempänä ’perusoikeuskirja’, erityisesti sen 8 artiklan mukainen oikeus henkilötietojen suojaan mutta myös sen 7 artiklassa vahvistettu oikeus yksityisyyteen, on olennaisen tärkeä tulkittaessa lainvalvontadirektiiviä.

Lainsäädäntötoimenpiteet, jotka toimivat henkilötietojen käsittelyn oikeusperustana, puuttuvat suoraan perusoikeuskirjan 7 ja 8 artiklassa taattuihin oikeuksiin. Biometristen tietojen käsittely kaikissa tilanteissa puuttuu niihin itsessään vakavasti. Tämä ei riipu tuloksesta, esimerkiksi positiivisen osuman löytymisestä. Perusoikeuksien ja -vapauksien käyttämistä voidaan rajoittaa ainoastaan lailla ja kyseisten oikeuksien ja vapauksien olennaista sisältöä noudattaen.

Oikeusperustan on oltava sanamuodoltaan **riittävän selkeä**, jotta kansalaiset saavat riittävän käsityksen siitä, millä edellytyksillä ja missä tilanteissa viranomaisilla on valtuudet turvautua tiedonkeruutoimenpiteisiin ja salaiseen valvontaan. Oikeusperusta ei olisi tarkka eikä ennakoitava, jos lainvalvontadirektiivin 10 artiklan yleinen lauseke vain saatettaisiin osaksi kansallista lainsäädäntöä.

Ennen kuin kansallinen lainsäätäjä luo uuden oikeusperustan mille tahansa biometristen tietojen käsittelylle, jossa käytetään kasvojentunnistusta, olisi **kuultava** toimivaltaista tietosuojaviranomaista.

Lainsäädäntötoimenpiteiden on oltava **tarkoituksenmukaisia** kyseessä olevalla lainsäädännöllä tavoiteltujen laillisten tavoitteiden saavuttamiseksi. **Yleistä etua koskeva tavoite** – oli se sitten miten perustavanlaatuinen tahansa – ei itsessään oikeuta perusoikeuden rajoittamista.

Lainsäädäntötoimenpiteissä olisi **eroteltava** ne henkilöt ja ne olisi kohdistettava niihin henkilöihin, joiden tietojen käsitellään tavoitteen saavuttamiseksi, esimerkiksi tiettyjen vakavien rikosten torjumiseksi. Jos toimenpide koskee yleisesti kaikkia henkilöitä ilman tällaista erottelua, rajoittamista tai poikkeusta, perusoikeuteen puuttuminen on siinä tapauksessa vakavampaa. Puuttuminen on vakavampaa myös silloin, jos tietojenkäsittely koskee merkittävää osaa väestöstä.

Tietoja on käsiteltävä tavalla, jolla varmistetaan EU:n tietosuojasääntöjen ja -periaatteiden sovellettavuus ja tehokkuus. **Tarpeellisuuden ja oikeasuhteisuuden arvioinnissa** on kunkin tilanteen mukaisesti myös tunnistettava ja otettava huomioon kaikki mahdolliset vaikutukset muihin perusoikeuksiin. Jos tietoja käsitellään järjestelmällisesti ilman, että rekisteröidyt tietävät asiasta, se todennäköisesti luo **yleisen tunteen jatkuvasta valvonnasta**. Tämä voi johtaa siihen, että joihinkin tai kaikkiin asianomaisiin perusoikeuksiin, kuten perusoikeuskirjan 1 artiklan mukaiseen ihmisarvoon, perusoikeuskirjan 10 artiklan mukaiseen ajatuksen, omantunnon ja uskonnon vapauteen, perusoikeuskirjan 11 artiklan mukaiseen sananvapauteen sekä perusoikeuskirjan 12 artiklan mukaiseen kokoontumis- ja yhdistymisvapauteen, kohdistuu tukahduttavia vaikutuksia.

Erityisten tietoryhmien, kuten biometristen tietojen, käsittelyä voidaan pitää ”**ehdottoman välttämättömänä**” (lainvalvontadirektiivin 10 artikla) vain, jos henkilötietojen suojaan puututaan ja sitä rajoitetaan vain sen verran, mikä on täysin välttämätöntä, eli ehdottoman tarpeellista, ja minkäänlaista yleistä tai järjestelmällistä käsittelyä ei suoriteta.

Se, että rekisteröity on **nimenomaisesti saattanut valokuvan julkiseksi** (lainvalvontadirektiivin 10 artikla), ei tarkoita, että siihen liittyvät biometriset tiedot, jotka valokuvasta voidaan saada erityisillä teknisillä keinoilla, katsotaan nimenomaisesti julkisiksi saatetuiksi. Palvelun oletusasetuksia, kuten mallien asettamista julkisesti saataville, tai valinnan mahdollisuuden puuttumista, kuten sitä, että mallit saatetaan julkisiksi ilman, että käyttäjä voi muuttaa tätä asetusta, ei pitäisi millään tavoin tulkita niin, että tiedot on nimenomaisesti saatettu julkisiksi.

Lainvalvontadirektiivin 11 artiklassa säädetään **automatisoituja yksittäispäätöksiä** koskevasta kehyksestä. Kasvojentunnistusteknologian käyttö edellyttää erityisten tietoryhmien käyttöä ja voi johtaa profilointiin riippuen siitä, miten ja mihin tarkoitukseen kasvojentunnistusteknologiaa käytetään. Profilointi, joka johtaa luonnollisten henkilöiden syrjintään erityisiin henkilötietoryhmiin kuuluvien tietojen perusteella, on joka tapauksessa kielletty unionin lainsäädännön ja lainvalvontadirektiivin 11 artiklan 3 kohdan mukaisesti.

Lainvalvontadirektiivin 6 artiklassa säädetään, että **eri rekisteröityjen ryhmät on erotettava toisistaan**. Sellaisten rekisteröityjen osalta, joiden osalta ei ole näyttöä siitä, että heidän toiminnallaan voisi olla yhteys, edes epäsuora tai etäinen yhteys, lainvalvontadirektiivin mukaiseen lailliseen tarkoitukseen, oikeuksiin puuttumista ei todennäköisimmin voida oikeuttaa.

Tietojen minimoinnin periaate (lainvalvontadirektiivin 4 artiklan 1 kohdan e alakohta) edellyttää myös, että kaikki videomateriaali, joka ei ole tietojen käsittelyn tarkoituksen kannalta merkityksellistä, olisi aina poistettava tai anonymisoitava (esimerkiksi sumentamalla ja siten, että tietoja ei voida palauttaa takautuvasti) ennen käsittelyn aloittamista.

Rekisterinpitäjän on harkittava huolellisesti, miten se täyttää (tai voiko se täyttää) **rekisteröidyn oikeuksia** koskevat vaatimukset ennen kasvojentunnistusteknologian käytön aloittamista, sillä kasvojentunnistusteknologiaan liittyy usein erityisiin henkilötietoryhmiin kuuluvien tietojen käsittelyä ilman ilmeistä vuorovaikutusta rekisteröidyn kanssa.

Rekisteröidyn oikeuksien tosiasiallinen käyttäminen riippuu siitä, täyttääkö rekisterinpitäjä **tiedonantovelvoitteensa** (lainvalvontadirektiivin 13 artikla). Arvioitaessa, onko kyseessä lainvalvontadirektiivin 13 artiklan 2 kohdan mukainen ”erityistapaus”, on otettava huomioon useita tekijöitä, muun muassa se, kerätäänkö henkilötietoja rekisteröidyn tietämättä, sillä rekisteröidyt voivat käyttää oikeuksiaan tosiasiallisesti vain, jos he ovat tietoisia tietojensa keräämisestä. Jos tehdään päätös yksinomaan kasvojentunnistusteknologian perusteella, rekisteröidyille on tiedotettava automatisoidun päätöksenteon ominaisuuksista.

Jos on **pyydetty pääsyä henkilötietoihin** ja biometriset tiedot on tallennettu ja liitetty henkilöllisyyteen käyttäen myös aakkosnumeerisia tietoja tietojen minimoinnin periaatteen mukaisesti, toimivaltaisen viranomaisen pitäisi pystyä vahvistamaan pääsyä koskeva pyyntö kyseisiä aakkosnumeerisia tietoja käyttämällä tehdyn haun perusteella käynnistämättä muiden henkilöiden biometristen tietojen edelleenkäsittelyä (eli tekemättä hakuja tietokannassa kasvojentunnistusteknologiaa hyödyntäen).

Rekisteröityihin kohdistuvat riskit ovat erityisen vakavia, jos poliisitietokantaan tallennetaan ja/tai muiden tahojen kanssa jaetaan virheellisiä tietoja. Rekisterinpitäjän on **korjattava** tallennetut tiedot ja kasvojentunnistusjärjestelmät vastaavasti (ks. myös lainvalvontadirektiivin johdanto-osan 47 kappale).

Oikeus käsittelyn **rajoittamiseen** on erityisen tärkeää (algoritmiin tai algoritmeihin perustuvan ja siten ehdottomia tuloksia antamattoman) kasvojentunnistusteknologian osalta tilanteissa, joissa kerätään suuria määriä tietoja ja tunnistuksen paikkansapitävyys ja laatu voivat vaihdella.

Ennen kasvojentunnistusteknologian käyttöä on tehtävä pakollinen **tietosuojaa koskeva vaikutustenarviointi** (ks. lainvalvontadirektiivin 27 artikla). Euroopan tietosuojaneuvosto suosittelee tällaisten arviointien tulosten tai ainakin tietosuojaa koskevan vaikutustenarvioinnin keskeisten havaintojen ja päätelmien julkaisemista luottamusta ja avoimuutta lisäävänä toimenpiteenä.

Kasvojentunnistusteknologian käyttöönottoon ja käyttöön liittyy useimmiten korkea rekisteröityjen oikeuksiin ja vapauksiin kohdistuva riski. Sen vuoksi kasvojentunnistusteknologiaa käyttöön ottavan viranomaisen olisi **kuultava** toimivaltaista valvontaviranomaista ennen kyseisen järjestelmän käyttöönottoa.

Biometristen tietojen ainutlaatuisuuden vuoksi kasvojentunnistusteknologian käyttöä aloittavan tai sitä käyttävän viranomaisen olisi kiinnitettävä erityistä huomiota **tietojen käsittelyn turvallisuuteen** lainvalvontadirektiivin 29 artiklan mukaisesti. Lainvalvontaviranomaisen olisi erityisesti varmistettava, että järjestelmä on asiaankuuluvien standardien mukainen ja että siinä käytetään biometristen mallien suojaustoimenpiteitä. Teknologian on oltava tietosuojaperiaatteiden mukainen ja sisällettävä suojatoimia ennen henkilötietojen käsittelyn aloittamista. Sen vuoksi silloinkin, kun lainvalvontaviranomainen aikoo käyttää ulkoisten palveluntarjoajien kasvojentunnistusteknologiaa, sen on esimerkiksi hankintamenettelyn avulla varmistettava, että käyttöön otetaan ainoastaan **sisäänrakennetun ja oletusarvoisen tietosuojan** periaatteisiin perustuvaa kasvojentunnistusteknologiaa.

Lokitiedot (ks. lainvalvontadirektiivin 25 artikla) ovat tärkeä suojatoimi käsittelyn lainmukaisuuden tarkistamiseksi sekä sisäisesti (kyseisen rekisterinpitäjän / henkilötietojen käsittelijän omaehtoinen valvonta) että ulkoisten valvontaviranomaisten toimesta. Kasvojentunnistusjärjestelmien yhteydessä suositellaan lokitietojen säilyttämistä myös viitetietokannan muutoksien sekä tunnistus- tai todentamisyrityksien osalta, mukaan lukien käyttäjä, tulos ja varmuusarvo. Lokitiedot ovat kuitenkin vain yksi **tilivelvollisuuden yleisen periaatteen** olennainen osa (ks. lainvalvontadirektiivin 4 artiklan 4

kohta). Rekisterinpitäjän on pystyttävä osoittamaan, että käsittelyssä noudatetaan lainvalvontadirektiivin 4 artiklan 1–3 kohdassa säädettyjä tietosuojan perusperiaatteita.

Euroopan tietosuojaneuvosto muistuttaa sen ja Euroopan tietosuojavaltuutetun yhteisestä **kehotuksesta kieltää** tietyt käsittelytyypit, jotka liittyvät 1) ihmisten biometriseen etätunnistukseen julkisissa tiloissa, 2) tekoälyyn perustuviin kasvojentunnistusjärjestelmiin, jotka luokittelevat ihmisiä heidän biometristen tietojensa perusteella ryhmiin etnisen alkuperän, sukupuolen, poliittisen tai seksuaalisen suuntautumisen tai muiden syrjintäperusteiden mukaan, 3) kasvojentunnistuksen tai vastaavien teknologioiden käyttöön luonnollisen henkilön tunteiden päättelemiseksi ja 4) lainvalvonnan yhteydessä suoritettavaan henkilötietojen käsittelyyn, joka perustuu tietokantaan, johon henkilötietoja kerätään laajamittaisesti ja summittaisesti, esimerkiksi ”haravoimalla” verkossa saatavilla olevia valokuvia ja kasvokuvia.

Keskeinen suojatoimi kyseessä olevien perusoikeuksien turvaamiseksi on toimivaltaisten tietosuojaviranomaisten suorittama **tehokas valvonta**. Siksi jäsenvaltioiden on varmistettava, että valvontaviranomaisten resurssit ovat asianmukaiset ja riittävät, jotta ne voivat täyttää velvollisuutensa.

Nämä **ohjeet on suunnattu** EU:n ja kansallisen tason lainsäätäjille sekä lainvalvontaviranomaisille ja niiden virkamiehille, jotka ottavat käyttöön ja käyttävät kasvojentunnistusjärjestelmiä. Ohjeet on suunnattu yksityishenkilöille siltä osin kuin ne koskevat heitä yleisesti tai rekisteröityinä, erityisesti rekisteröityjen oikeuksien osalta.

Ohjeiden tarkoituksena on antaa tietoa tietyistä kasvojentunnistusteknologian ominaisuuksista ja lainvalvonnan yhteydessä sovellettavasta oikeuskehyksestä (erityisesti lainvalvontadirektiivistä).

- Lisäksi ohjeet tarjoavat **työkalun, joka tukee tietyn tapauksen arkaluonteisuuden ensimmäistä luokittelua** (liite I).
- Ne sisältävät myös **käytännön ohjeita lainvalvontaviranomaisille, jotka haluavat hankkia kasvojentunnistusjärjestelmän ja käyttää sitä** (liite II).
- Ohjeissa kuvataan myös useita tyypillisiä **käyttötapauksia ja luetellaan lukuisia merkityksellisiä näkökohtia** erityisesti tarpeellisuus- ja oikeasuhteisuustestin kannalta (liite III).

1 JOHDANTO

1. Kasvojentunnistusteknologiaa voidaan käyttää tunnistamaan henkilöitä automaattisesti heidän kasvojensa perusteella. Kasvojentunnistusteknologia perustuu usein tekoälyyn, kuten koneoppimisteknologiaan. Kasvojentunnistusteknologian sovelluksia testataan ja käytetään yhä enemmän eri aloilla. Niitä käyttävät niin yksityishenkilöt, yksityiset organisaatiot kuin julkishallinnotkin. Myös lainvalvontaviranomaiset odottavat hyötyvänsä kasvojentunnistusteknologian käytöstä. Se lupaa ratkaisuja suhteellisen uusiin haasteisiin, kuten tutkintoihin, joissa kerätyn näytön määrä on suuri, mutta myös tunnettuihin ongelmiin, erityisesti tarkkailu- ja etsintätehtäviin tarvittavan henkilöstön puutteeseen.

2. Iso osa kasvaneesta kiinnostuksesta kasvojentunnistusteknologiaa kohtaan perustuu sen tehokkuuteen ja skaalautuvuuteen. Hyötyjen lisäksi teknologiaan ja sen käyttöön liittyy haittoja – myös suuressa mittakaavassa. Henkilötietojoukkoja voidaan analysoida napin painalluksella tuhansittain, ja algoritmisen syrjinnän tai virheellisen tunnistuksen vähäisetkin vaikutukset voivat vaikuttaa vakavasti lukuisten ihmisten toimintaan ja jokapäiväiseen elämään. Jo pelkkä henkilötietojen ja erityisesti

biometristen tietojen käsittelyn laajuus on toinen kasvojentunnistusteknologian keskeinen piirre, sillä käsiteltäessä henkilötietoja puututaan Euroopan unionin perusoikeuskirjan (jäljempänä ’perusoikeuskirja’) 8 artiklan mukaiseen henkilötietojen suojaa koskevaan perusoikeuteen.

3. Sillä, että lainvalvontaviranomaiset käyttävät kasvojentunnistusteknologiaa, on tulevaisuudessa – ja jossain määrin jo nyt – merkittäviä seurauksia yksilöille ja ihmisryhmille, myös vähemmistöille. Näillä seurauksilla on tulevaisuudessa myös huomattavia vaikutuksia ihmisten yhteiselämään sekä yhteiskunnalliseen ja demokraattiseen poliittiseen vakauteen, jossa arvostetaan moniarvoisuuden ja poliittisen opposition suurta merkitystä. Oikeus henkilötietojen suojaan on usein keskeinen edellytys muiden perusoikeuksien takaamiselle. Kasvojentunnistusteknologian käyttö puuttuu huomattavan usein henkilötietojen suojaa koskevan oikeuden lisäksi muihinkin perusoikeuksiin.

4. Sen vuoksi Euroopan tietosuojaneuvosto katsoo, että on tärkeää myötävaikuttaa kasvojentunnistusteknologian meneillään olevaan käyttöönottoon lainvalvonnan alalla, joka kuuluu lainvalvontadirektiivin[1] soveltamisalaan ja niiden kansallisten lakien soveltamisalaan, joilla direktiivi saatetaan osaksi kansallista lainsäädäntöä. Tämän vuoksi tietosuojaneuvosto on laatinut nämä ohjeet. Ohjeiden tarkoituksena on antaa asiaankuuluvaa tietoa EU:n ja kansallisen tason lainsäätäjille sekä lainvalvontaviranomaisille ja niiden virkamiehille, kun ne ottavat käyttöön ja käyttävät kasvojentunnistusjärjestelmiä. Ohjeiden soveltamisala rajoittuu kasvojentunnistusteknologiaan. Muista lainvalvontaviranomaisten käyttämistä biometrisiin tietoihin perustuvien henkilötietojen käsittelytavoista voi kuitenkin aiheutua samanlaisia tai ylimääräisiä riskejä yksityishenkilöille, ryhmille ja yhteiskunnalle, erityisesti jos käsittely tapahtuu etänä. Tietyt näiden ohjeiden näkökohdat voivat tilanteesta riippuen olla hyödyllinen tietolähde myös näissä tapauksissa. Lisäksi yksityishenkilöt, joita ohjeet koskevat yleisesti tai rekisteröityinä, voivat saada niistä tärkeää tietoa erityisesti rekisteröityjen oikeuksista.

5. Ohjeet koostuvat pääasiakirjasta ja kolmesta liitteestä. Tässä pääasiakirjassa esitellään teknologia ja sovellettava oikeuskehys. Liitteessä I on malli, jonka avulla voidaan määritellä joitakin tärkeimpiä näkökohtia perusoikeuksiin puuttumisen vakavuuden luokittelemiseksi tietyllä soveltamisalalla. Liitteessä II on käytännön ohjeita lainvalvontaviranomaisille, jotka haluavat hankkia kasvojentunnistusjärjestelmän ja käyttää sitä. Eri näkökohtien merkityksellisyys riippuu kasvojentunnistusteknologian soveltamisalasta. Liitteessä III on hypoteettisia tapauksia ja niihin liittyvää pohdintaa.

2 TEKNOLOGIA

2.1 Yksi biometrinen teknologia, kaksi erillistä tehtävää

6. Kasvojentunnistus on todennäköisyyteen perustuvaa teknologiaa, jolla voidaan tunnistaa henkilöitä automaattisesti heidän kasvojensa perusteella heidän henkilöllisyytensä määrittämiseksi tai todentamiseksi.

7. Kasvojentunnistusteknologia kuuluu laajempaan biometrisen teknologian luokkaan. Biometriikkaan kuuluvat kaikki automatisoidut prosessit, joita käytetään henkilön tunnistamiseen määrittämällä fyysisiä, fysiologisia tai käyttäytymiseen liittyviä ominaisuuksia (sormenjäljet, iiriksen rakenne, ääni,

[1] Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäätöksen 2008/977/YOS kumoamisesta.

kävely, verisuonikuviot yms.). Nämä ominaisuudet määritellään ”biometrisiksi tiedoiksi”, koska ne mahdollistavat tai vahvistavat kyseisen henkilön yksilöllisen tunnistamisen.

8. Tämä koskee ihmisten kasvoja tai tarkemmin sanottuna niiden teknistä käsittelyä kasvojentunnistuslaitteiden avulla: ottamalla kasvoista kuva (valokuva tai video), jota kutsutaan biometriseksi ”näytteeksi”, voidaan luoda digitaalinen esitys näiden kasvojen erilaisista ominaisuuksista (tätä kutsutaan ”malliksi”).

9. Biometrinen malli on digitaalinen esitys yksilöllisistä ominaisuuksista, jotka on poimittu biometrisestä näytteestä ja jotka voidaan tallentaa biometriseen tietokantaan[2]. Tämän mallin on tarkoitus olla yksilöllinen ja henkilökohtainen, ja se on lähtökohtaisesti pysyvä[3]. Tunnistusvaiheessa laite vertaa tätä mallia muihin aiemmin luotuihin tai suoraan biometrisistä näytteistä, kuten kuvasta, valokuvasta tai videosta löytyvistä kasvoista, laskettuihin malleihin. ”Kasvojentunnistus” on näin ollen kaksivaiheinen prosessi: ensin kerätään kasvokuva ja muunnetaan se malliksi, ja sen jälkeen kyseiset kasvot tunnistetaan vertaamalla vastaavaa mallia yhteen tai useampaan muuhun malliin.

10. Kuten kaikilla biometrisillä prosesseilla, kasvojentunnistuksella voi olla kaksi eri tehtävää:

    - henkilöllisyyden **todentaminen**, jonka tarkoituksena on varmistaa, että henkilö on juuri se henkilö, joka hän väittää olevansa. Tässä tapauksessa järjestelmä vertaa aiemmin (esimerkiksi älykorttiin tai biometriseen passiin) tallennettua biometristä mallia tai näytettä yksittäisiin kasvoihin, esimerkiksi tarkastuspisteeseen saapuvan henkilön kasvoihin, tarkistaakseen, onko kyseessä yksi ja sama henkilö. Tämä toiminto perustuu näin ollen kahden mallin vertailuun. Tätä kutsutaan myös yksi-yhteen-**todentamiseksi**.

    - henkilön **tunnistaminen**, jonka tarkoituksena on löytää henkilö ihmisjoukosta, tietyltä alueelta, kuvasta tai tietokannasta. Tässä tapauksessa järjestelmän on käsiteltävä kaikki tallennetut kasvot, luotava biometrinen malli ja sen jälkeen tarkistettava, vastaako se järjestelmän tiedossa olevaa henkilöä. Tämä toiminto perustuu siis siihen, että yhtä mallia verrataan malli- tai näytetietokantaan (vertailumalleihin). Tätä kutsutaan myös yksi-moneen-tunnistamiseksi. Se voi esimerkiksi yhdistää henkilönnimitietueen (sukunimi, etunimi) kasvoihin, jos vertailu tehdään sukunimiin ja etunimiin yhdistettyjen valokuvien tietokantaan. Siihen voi kuulua myös henkilön seuraaminen väkijoukossa ilman, että henkilön henkilöllisyyteen luodaan välttämättä yhteyttä.

11. Molemmissa tapauksissa käytetyt kasvojentunnistustekniikat perustuvat arvioituun vastaavuuteen mallien, verrattavan mallin ja vertailumallin tai -mallien, välillä. Tästä näkökulmasta katsottuna ne perustuvat todennäköisyyteen. Vertailussa päätellään suurempi tai pienempi todennäköisyys sille, että henkilö on tosiaan kyseinen tunnistettava tai todennettava henkilö. Jos tämä todennäköisyys ylittää järjestelmässä tietyn kynnysarvon, jonka järjestelmän käyttäjä tai kehittäjä on määritellyt, järjestelmä olettaa, että mallit vastaavat toisiaan (syntyy osuma).

12. Vaikka tehtävät – todentaminen ja tunnistaminen – ovat erillisiä, molemmat liittyvät tunnistettua tai tunnistettavaa luonnollista henkilöä koskevien biometristen tietojen käsittelyyn ja ovat siten henkilötietojen käsittelyä ja tarkemmin sanottuna erityisiin henkilötietoryhmiin kuuluvien tietojen käsittelyä.

[2] ”Guidelines on facial recognition” (kasvojentunnistusta koskevat ohjeet), yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä tehdyn yleissopimuksen (yleissopimus 108) nojalla perustettu neuvoa-antava komitea, Euroopan neuvosto, kesäkuu 2021.

[3] Tämä voi riippua biometriikan tyypistä ja rekisteröidyn iästä.

13. Kasvojentunnistus on osa laajempaa videokuvankäsittelytekniikoiden kirjoa. Joillakin videokameroilla voidaan kuvata ihmisiä rajatulta alueelta, erityisesti heidän kasvojaan, mutta näitä kameroita ei voida käyttää sellaisenaan ihmisten automaattiseen tunnistamiseen. Sama pätee yksinkertaiseen valokuvaukseen: kamera ei ole kasvojentunnistusjärjestelmä, sillä ihmisten valokuvia on käsiteltävä tietyllä tavalla biometristen tietojen poimimiseksi.

14. Pelkkä kasvojen havaitseminen niin sanotuilla älykkäillä kameroilla ei myöskään välttämättä tarkoita kasvojentunnistusjärjestelmää. Vaikka digitaaliset tekniikat, joilla havaitaan epänormaalia käytöstä tai väkivaltaisia tapahtumia tai tunnistetaan kasvojen tunteita tai jopa siluetteja, nostavat esiin myös tärkeitä eettisyyteen ja tehokkuuteen liittyviä kysymyksiä, niitä ei voida pitää biometrisinä järjestelminä, jotka käsittelevät erityisiin henkilötietoryhmiin kuuluvia tietoja, jos niiden tarkoituksena ei ole tunnistaa henkilöä yksilöllisesti ja jos kyseinen henkilötietojen käsittely ei käsitä muita erityisiä henkilötietoryhmiä. Nämä esimerkit eivät ole täysin irrallisia kasvojentunnistuksesta, ja niihin sovelletaan joka tapauksessa henkilötietojen suojaa koskevia sääntöjä.[4] Lisäksi tämäntyyppistä havaitsemisjärjestelmää voidaan käyttää yhdessä muiden järjestelmien kanssa, joilla pyritään tunnistamaan henkilö, jolloin sitä voidaan pitää kasvojentunnistusteknologiana.

15. Toisin kuin esimerkiksi videokuvan tallennus- ja käsittelyjärjestelmät, jotka edellyttävät fyysisten laitteiden asentamista, kasvojentunnistus on ohjelmistotoiminto, joka voidaan ottaa käyttöön olemassa olevissa järjestelmissä (kamerat, kuvatietokannat yms.). Tällainen toiminto voidaan näin ollen liittää tai kytkeä moniin eri järjestelmiin ja yhdistää muihin toimintoihin. Tällainen integrointi jo olemassa olevaan infrastruktuuriin edellyttää erityistä huomiota, sillä siihen liittyy riskejä, jotka johtuvat siitä, että kasvojentunnistusteknologia voi olla kitkatonta ja helposti piilotettavissa[5].

2.2 Monenlaisia käyttötarkoituksia ja sovelluksia

16. Näiden ohjeiden sekä lainvalvontadirektiivin soveltamisalan lisäksi kasvojentunnistusta voidaan käyttää monenlaisiin tarkoituksiin, sekä kaupalliseen käyttöön että yleiseen turvallisuuteen tai lainvalvontaan liittyvien huolenaiheiden ratkaisemiseen. Kasvojentunnistusta voidaan käyttää monissa eri yhteyksissä: käyttäjän ja palvelun välisessä henkilökohtaisessa suhteessa (sovellukseen pääsy), tiettyyn paikkaan pääsyyn (fyysinen suodatus) tai ilman erityisiä rajoituksia julkisissa tiloissa (kasvojentunnistus paikan päällä). Sitä voidaan käyttää kaikenlaisiin rekisteröityihin: esimerkiksi palvelun asiakas, työntekijä, pelkkä sivustaseuraaja, etsintäkuulutettu tai henkilö, joka on mukana oikeudellisissa tai hallinnollisissa menettelyissä. Jotkin käyttötarkoitukset ovat jo yleisiä ja laajalle levinneitä, toiset taas vielä kokeellisia tai spekulatiivisia. Vaikka nämä ohjeet eivät koske kaikkia tällaisia käyttötarkoituksia ja sovelluksia, Euroopan tietosuojaneuvosto muistuttaa, että ne voidaan panna täytäntöön vain, jos ne ovat sovellettavan oikeuskehyksen ja erityisesti yleisen tietosuoja-asetuksen ja asiaa koskevan kansallisen lainsäädännön mukaisia.[6] Myös lainvalvontadirektiivin soveltamisalalla kasvojentunnistusteknologian avulla käsiteltyjä tietoja voidaan todentamisen tai tunnistamisen lisäksi käsitellä edelleen myös muita tarkoituksia, kuten luokittelua, varten.

17. Tarkemmin sanottuna mahdollisten käyttötarkoitusten laajuutta voitaisiin harkita riippuen siitä, missä määrin ihmiset hallitsevat henkilötietojaan, millaisia tehokkaita keinoja heillä on henkilötietojensa hallitsemiseksi ja tämän teknologian käyttöönottamisen ja käytön aloittamista koskevan oikeuden

[4] Lainvalvontadirektiivin 10 artiklaa (tai yleisen tietosuoja-asetuksen 9 artiklaa) sovelletaan kuitenkin järjestelmiin, joilla ihmisiä luokitellaan ryhmiin heidän biometristen tietojensa perusteella etnisen alkuperän, poliittisen tai seksuaalisen suuntautumisen tai muihin erityisiin henkilötietoryhmiin kuuluvien tietojen mukaan.
[5] Esimerkiksi vartalokameroissa, joita käytetään yhä enemmän käytännössä.
[6] Ks. myös 29. tammikuuta 2020 annetut Euroopan tietosuojaneuvoston ohjeet 3/2019 henkilötietojen käsittelystä videolaitteilla.

käyttämiseksi, millaisia seurauksia heille aiheutuu (jos heidät tunnistetaan tai ei tunnisteta) sekä mikä on suoritetun käsittelyn laajuus. Kyseisen henkilön henkilökohtaiseen laitteeseen (älykortti, älypuhelin tms.) tallennettuun malliin perustuva kasvojentunnistus, jota käytetään henkilöllisyyden todentamiseen ja ainoastaan henkilökohtaiseen käyttöön erityisen käyttöliittymän kautta, ei aiheuta samoja riskejä kuin esimerkiksi käyttö tunnistamistarkoituksiin valvomattomassa ympäristössä, jossa jokaisten valvonta-alueelle tulevien kasvojen mallia verrataan tietokantaan tallennettuihin kattavaan väestömäärään perustuviin malleihin, ilman rekisteröityjen aktiivista osallistumista. Näiden kahden ääripään välillä on hyvin erilaisia käyttötarkoituksia ja niihin liittyviä henkilötietojen suojaa koskevia kysymyksiä.

18. Jotta voidaan havainnollistaa tarkemmin kontekstia, jossa kasvojentunnistusteknologiasta parhaillaan keskustellaan tai sitä otetaan käyttöön joko todentamista tai tunnistamista varten, Euroopan tietosuojaneuvosto katsoo, että on asianmukaista mainita joitakin esimerkkejä. Seuraavat esimerkit ovat pelkästään kuvailevia, eikä niitä tule pitää minkäänlaisena alustavana arviona siitä, ovatko ne tietosuojaa koskevan EU:n säännöstön mukaisia.

Esimerkkejä henkilöllisyyden todentamisesta kasvojentunnistuksen avulla

19. Henkilöllisyyden todentaminen voidaan suunnitella siten, että käyttäjät voivat hallita sitä täysin, esimerkiksi palvelujen tai sovellusten käytön mahdollistamiseksi puhtaasti kotiympäristössä. Näin älypuhelinten omistajat käyttävät kasvojentunnistusta laajasti laitteensa avaamiseen salasanatodentamisen sijaan.

20. Kasvojentunnistusta voidaan käyttää myös sellaisen henkilön henkilöllisyyden tarkistamiseen, joka haluaa saada julkisia tai yksityisiä kolmannen osapuolen palveluita. Tällaiset prosessit tarjoavat siis tavan luoda digitaalinen henkilöllisyys mobiilisovelluksen avulla (älypuhelin, tabletti yms.), jota voidaan sen jälkeen käyttää sähköisten hallinnollisten palveluiden käyttämiseen.

21. Lisäksi kasvojentunnistukseen perustuvalla todentamisella voidaan pyrkiä hallitsemaan fyysistä pääsyä yhteen tai useampaan ennalta määrättyyn paikkaan, kuten rakennuksiin tai tiettyihin rajanylityspaikkoihin. Tätä toimintoa käytetään esimerkiksi tietyssä rajanylitystä varten suoritettavassa tietojenkäsittelyssä, jossa tarkastuspisteellä olevan henkilön kasvoja verrataan hänen henkilöllisyystodistukseensa (passiin tai oleskelulupaan) tallennettuihin kasvoihin.

Esimerkkejä henkilön tunnistamisesta kasvojentunnistuksen avulla

22. Tunnistusta voidaan käyttää monilla, todentamiseen verrattuna jopa monimuotoisemmilla tavoilla. Näitä ovat erityisesti, mutta ei ainoastaan, seuraavat käyttötarkoitukset, joita tällä hetkellä käytetään, kokeillaan tai suunnitellaan EU:ssa:

- tunnistamattoman henkilön (uhrin, epäillyn tms.) etsiminen valokuvatietokannasta henkilön tunnistamista varten
- henkilön liikkeiden seuranta julkisissa tiloissa. Henkilön kasvoja verrataan sellaisten henkilöiden biometrisiin malleihin, jotka liikkuvat tai ovat liikkuneet valvotulla alueella, esimerkiksi silloin, kun matkalaukku jätetään jälkeen tai kun on tapahtunut rikos
- henkilön matkan ja muiden henkilöiden kanssa tapahtuneen myöhemmän vuorovaikutuksen rekonstruointi vertailemalla myöhemmin samoja asioita esimerkiksi henkilön kontaktien tunnistamiseksi

- etsintäkuulutettujen henkilöiden biometrinen etätunnistus julkisissa tiloissa. Kaikkia videovalvontakameroilla paikan päällä tallennettuja kasvoja verrataan reaaliaikaisesti turvallisuusjoukkojen ylläpitämään tietokantaan

- kuvassa olevien ihmisten automaattinen tunnistaminen esimerkiksi heidän suhteidensa tunnistamiseksi sitä käyttävässä sosiaalisessa verkostossa. Kuvaa verrataan kaikkien niiden verkostoon kuuluvien henkilöiden malleihin, jotka ovat antaneet suostumuksensa tähän toimintoon, näiden suhteiden nimellisen tunnistamisen ehdottamiseksi

- palveluiden käyttömahdollisuudet, jotkin käteisautomaatit tunnistavat asiakkaansa vertaamalla kameran tallentamia kasvoja pankin ylläpitämään kasvokuvatietokantaan

- matkustajan matkan seuraaminen matkan tietyssä vaiheessa. Matkan tiettyjen vaiheiden porteille (matkatavaroiden jättöpaikat, lähtöportit yms.) saapuvan henkilön reaaliaikaisesti laskettua mallia verrataan järjestelmään aiemmin rekisteröityjen henkilöiden malleihin.

23. Sen lisäksi, että kasvojentunnistusteknologiaa käytetään lainvalvonnan alalla, käytössä olevien sovellusten laaja kirjo edellyttää kattavaa keskustelua ja poliittista lähestymistapaa, jotta voidaan varmistaa johdonmukaisuus ja yhdenmukaisuus EU:n tietosuojaa koskevan säännöstön kanssa.

2.3 Luotettavuus, tarkkuus ja rekisteröidyille aiheutuvat riskit

24. Kuten kaiken teknologian, myös kasvojentunnistuksen käyttöönottoon voi liittyä haasteita. Ne koskevat erityisesti sen luotettavuutta ja tehokkuutta henkilöllisyyden todentamisessa tai henkilön tunnistamisessa sekä yleisesti ”lähdetietojen” ja kasvojentunnistuskäsittelyn tuloksen laatua ja tarkkuutta.

25. Tällaiset teknologiset haasteet aiheuttavat asianomaisille rekisteröidyille erityisiä riskejä, jotka ovat vielä merkittävämpiä tai vakavampia lainvalvonnan alalla, kun otetaan huomioon mahdolliset vaikutukset rekisteröityihin. Vaikutukset voivat olla oikeudellisia tai muita sellaisia, jotka vaikuttavat heihin samoin merkittävästi. Tässä yhteydessä vaikuttaa myös hyödylliseltä korostaa, että kasvojentunnistusteknologian käyttäminen jälkikäteen ei ole itsessään turvallisempaa, koska yksittäisiä henkilöitä voidaan seurata eri aikoina ja eri paikoissa. Näin ollen kasvojentunnistusteknologian käyttämiseen jälkikäteen liittyy myös erityisiä riskejä, joita on arvioitava tapauskohtaisesti.[7]

26. Kuten EU:n perusoikeusvirasto totesi vuoden 2019 raportissaan, kasvojentunnistusohjelmistojen tarvittavan tarkkuuden määrittäminen on haastavaa: tarkkuutta voidaan arvioida monin eri tavoin, myös tehtävän, tarkoituksen ja käyttöyhteyden mukaan. Kun teknologiaa käytetään paikoissa, joissa käy miljoonia ihmisiä – kuten juna-asemilla tai lentokentillä – virheiden suhteellisen pieni osuus (esimerkiksi 0,01 %)[8] tarkoittaa silti sitä, että satoja ihmisiä merkitään väärin. Lisäksi tiettyjen ihmisryhmien kohdalla vääriä osumia saattaa syntyä todennäköisemmin kuin toisten, kuten kohdassa 3 on kuvattu. Virheiden prosenttiosuuksia voidaan laskea ja tulkita eri tavoin, joten varovaisuus on tarpeen. Lisäksi tarkkuuden ja virheiden osalta kysymykset, jotka liittyvät siihen, miten helposti järjestelmää voidaan huijata esimerkiksi väärennetyillä kasvokuvilla (ns. spoofing), ovat tärkeitä erityisesti lainvalvonnan alalla.[9]

[7] Ks. liitteessä III esitetyt esimerkit.

[8] Tämä tarkkuusprosenttiosuus on peräisin kyseisestä raportista, ja se on paljon parempi kuin algoritmien nykyinen suorituskyky kasvojentunnistussovelluksissa.

[9] ”Facial recognition technology: fundamental rights considerations in the context of law enforcement”, EU:n perusoikeusvirasto, 21. marraskuuta 2019.

27. Tässä yhteydessä Euroopan tietosuojaneuvosto pitää tärkeänä muistuttaa, että riippumatta siitä, käytetäänkö kasvojentunnistusteknologiaa todentamis- tai tunnistamistarkoituksiin, se ei anna ehdotonta tulosta vaan perustuu todennäköisyyksiin, että kahdet kasvot – tai kasvokuvat – vastaavat samaa henkilöä.[10] Tämä tulos heikkenee edelleen, kun kasvojentunnistusta varten syötetyn biometrisen näytteen laatu on heikko. Heikkoa laatua voivat aiheuttaa syötettyjen kuvien epätarkkuus, kameran alhainen resoluutio, liike ja heikko valaistus. Muita tuloksiin merkittävästi vaikuttavia tekijöitä ovat ilmaantuvuus ja ”spoofing”, esimerkiksi silloin, kun rikolliset yrittävät joko välttää kameroita tai huijata kasvojentunnistusteknologiaa. Lukuisissa tutkimuksissa on myös korostettu, että tällaiset algoritmisesta käsittelystä saadut tilastolliset tulokset voivat olla myös vääristyneitä, mikä johtuu erityisesti lähdetietojen laadusta ja koulutustietokannoista tai muista tekijöistä, kuten käyttöönoton sijainnin valinnasta. Lisäksi pitäisi korostaa kasvojentunnistusteknologian vaikutusta muihin perusoikeuksiin, kuten esimerkiksi yksityis- ja perhe-elämän kunnioittamiseen, sananvapauteen ja tiedonvälityksen vapauteen sekä kokoontumis- ja yhdistymisvapauteen.

28. Sen vuoksi on olennaisen tärkeää, että kasvojentunnistusteknologian luotettavuus ja tarkkuus otetaan huomioon kriteereinä arvioitaessa keskeisten tietosuojaperiaatteiden noudattamista lainvalvontadirektiivin 4 artiklan mukaisesti ja erityisesti oikeudenmukaisuuden ja tarkkuuden osalta.

29. Euroopan tietosuojaneuvosto korostaa, että korkealaatuiset tiedot ovat olennaisen tärkeitä korkealaatuisten algoritmien kannalta ja että rekisterinpitäjien on osana tilivelvollisuuttaan arvioitava algoritmista tietojenkäsittelyä säännöllisesti ja järjestelmällisesti varmistaakseen erityisesti tällaisen henkilötietojen käsittelyn tulosten tarkkuuden, oikeudenmukaisuuden ja luotettavuuden. Kasvojentunnistusjärjestelmien arviointiin, kouluttamiseen ja jatkokehittämiseen käytettäviä henkilötietoja voidaan käsitellä ainoastaan riittävän oikeusperustan nojalla ja yhteisten tietosuojaperiaatteiden mukaisesti.

3 SOVELLETTAVA OIKEUSKEHYS

30. Kasvojentunnistusteknologian käyttö liittyy erottamattomasti henkilötietojen, myös erityisiin tietoryhmiin kuuluvien henkilötietojen, käsittelyyn. Lisäksi se vaikuttaa suoraan tai välillisesti useisiin EU:n perusoikeuskirjassa vahvistettuihin perusoikeuksiin. Tämä on erityisen tärkeää lainvalvonnan ja rikosoikeuden alalla. Sen vuoksi kaikessa kasvojentunnistusteknologian käytössä olisi noudatettava tiukasti sovellettavaa oikeuskehystä.

31. Seuraavat tiedot on tarkoitettu käytettäviksi tulevien lainsäädännöllisten ja hallinnollisten toimenpiteiden arvioinnissa sekä voimassa olevan lainsäädännön tapauskohtaisessa täytäntöönpanossa, johon liittyy kasvojentunnistusteknologiaa. Vaatimusten merkityksellisyys vaihtelee tilanteen mukaan. Koska kaikkia tulevia tilanteita ei voida ennakoida, tiedoilla katsotaan tarjottavan vain tukea eikä niitä pidä tulkita tyhjentäväksi luetteloksi.

3.1 Yleinen oikeuskehys – EU:n perusoikeuskirja ja Euroopan ihmisoikeussopimus

3.1.1 Perusoikeuskirjan sovellettavuus

32. EU:n perusoikeuskirja, jäljempänä ’perusoikeuskirja’, koskee unionin toimielimiä, elimiä, laitoksia ja virastoja sekä jäsenvaltioita, kun ne panevat täytäntöön unionin oikeutta.

[10] Tästä todennäköisyydestä käytetään nimitystä ”varmuusarvo”.

33. Lainvalvontadirektiivin 1 artiklan 1 kohdan mukaisen lainvalvontatarkoituksissa suoritettavan biometristen tietojen käsittelyn sääntely nostaa väistämättä esiin kysymyksen perusoikeuksien, erityisesti perusoikeuskirjan 7 artiklan mukaisen yksityiselämän ja viestien kunnioittamista koskevan oikeuden sekä perusoikeuskirjan 8 artiklan mukaisen henkilötietojen suojaa koskevan oikeuden, kunnioittamisesta.

34. Luonnollisista henkilöistä, myös heidän kasvoistaan, tallennetun videokuvan kerääminen ja analysointi tarkoittaa henkilötietojen käsittelyä. Kun kuvaa käsitellään teknisesti, käsittely koskee myös biometrisia tietoja. Luonnollisen henkilön kasvoja koskevien tietojen tekninen käsittely ajan ja paikan suhteen mahdollistaa johtopäätösten tekemisen kyseisten henkilöiden yksityiselämästä. Nämä johtopäätökset voivat koskea kyseisten henkilöiden rodullista tai etnistä alkuperää, terveyttä, uskontoa, arkielämän tapoja, pysyvää tai tilapäistä asuinpaikkaa, päivittäistä tai muuta liikkumista, toimintaa, sosiaalisia suhteita ja sosiaalista ympäristöä. Kasvojentunnistusteknologian käytön yhteydessä mahdollisesti paljastuvien tietojen suuri kirjo osoittaa selvästi, että sillä voi olla vaikutusta perusoikeuskirjan 8 artiklassa vahvistettuun oikeuteen henkilötietojen suojaan mutta myös perusoikeuskirjan 7 artiklassa vahvistettuun oikeuteen yksityisyyteen.

35. Tällaisessa tilanteessa ei ole myöskään poissuljettua, että biometristen (kasvoja koskevien) tietojen kerääminen, analysointi ja jatkokäsittely voi vaikuttaa siihen, miten ihmiset tuntevat olevansa vapaita toimimaan, vaikka toiminta olisi täysin vapaan ja avoimen yhteiskunnan sääntöjen mukaista. Sillä voi myös olla vakavia seurauksia heidän perusoikeuksiensa käyttämiseen, kuten perusoikeuskirjan 1, 10, 11 ja 12 artiklan mukaisiin oikeuksiin, jotka koskevat ajatuksen-, omantunnon- ja uskonnonvapautta, ilmaisunvapautta, vapautta rauhanomaiseen kokoontumiseen sekä yhdistymisvapautta. Tällaiseen käsittelyyn liittyy myös muita riskejä, kuten riski siitä, että asianomaisten viranomaisten keräämiä henkilötietoja käytetään väärin sen seurauksena, että henkilötietoihin on päästy käsiksi ja niitä on käytetty laittomasti, tai esimerkiksi tietoturvaloukkauksen seurauksena. Riskit riippuvat usein käsittelystä ja sen olosuhteista, kuten riski siitä, että poliisivirkamiehet tai muut luvattomat osapuolet pääsevät tietoihin käsiksi ja käyttävät niitä laittomasti. Jotkin riskit liittyvät kuitenkin yksinkertaisesti siihen, että biometriset tiedot ovat ainutlaatuisia. Toisin kuin osoitetta tai puhelinnumeroa, rekisteröity ei voi muuttaa yksilöllisiä ominaisuuksiaan, kuten kasvojaan tai iiristään. Jos biometrisiin tietoihin pääsee käsiksi luvattomasti tai ne julkaistaan vahingossa, ne vaarantuisivat niiden salasanoina tai salausavaimina käytön osalta tai niitä voitaisiin käyttää muihin luvattomiin valvontatoimiin rekisteröidyn vahingoksi.

3.1.2 Perusoikeuskirjassa vahvistettuihin oikeuksiin puuttuminen

36. Biometristen tietojen käsittely kaikissa tilanteissa puuttuu jo itsessään vakavasti perusoikeuksiin. Tämä ei riipu tuloksesta, esimerkiksi positiivisen osuman löytymisestä. Käsittely on perusoikeuksiin puuttumista, vaikka biometrinen malli poistettaisiin välittömästi sen jälkeen, kun vertailu poliisitietokantaan on tehty ja osumaa ei ole löytynyt.

37. Rekisteröityjen perusoikeuksiin puuttuminen voi johtua lainsäädäntötoimesta, jolla joko pyritään rajoittamaan asianomaista perusoikeutta tai jonka seurauksena se rajoittuu[11]. Se voi johtua myös sellaisesta viranomaisen toimesta, jolla on sama tarkoitus tai seuraus, tai jopa sellaisen yksityisen tahon toimesta, jolle on laissa annettu valta käyttää julkista valtaa.

[11] EUT, C-219/91 – Ter Voort, RoC 1992 I-05485, 36f kohta; EUT, C-200/96 – Metronome, RoC 1998 I-1953, 28 kohta.

38. Lainsäädäntötoimenpide, joka toimii henkilötietojen käsittelyn oikeusperustana, puuttuu suoraan perusoikeuskirjan 7 ja 8 artiklassa taattuihin oikeuksiin[12].

39. Biometristen tietojen ja erityisesti kasvojentunnistusteknologian käyttö vaikuttaa monissa tapauksissa myös ihmisarvoa koskevaan oikeuteen, joka taataan perusoikeuskirjan 1 artiklassa. Ihmisarvo edellyttää, että ihmisiä ei kohdella pelkkinä esineinä. Kasvojentunnistusteknologia muuntaa eksistentiaaliset ja erittäin henkilökohtaiset ominaisuudet, kasvonpiirteet, koneellisesti luettavaan muotoon, jotta niitä voitaisiin käyttää ihmisten rekisterikilpenä tai henkilökorttina, jolloin kasvot esineellistetään.

40. Tällainen käsittely voi puuttua myös muihin perusoikeuksiin, kuten perusoikeuskirjan 10, 11 ja 12 artiklan mukaisiin oikeuksiin, sikäli kuin lainvalvontaviranomaisten videovalvonnalla pyritään tukahduttaviin vaikutuksiin tai niitä syntyy sen seurauksena.

41. Lisäksi olisi huolellisesti tarkasteltava mahdollisia riskejä, joita kasvojentunnistusteknologian käyttö lainvalvonnassa aiheuttaa perusoikeuskirjan 47 ja 48 artiklan mukaisen oikeudenmukaista oikeudenkäyntiä koskevan oikeuden ja syyttömyysolettaman osalta. Kasvojentunnistusteknologian käytön tulos, esimerkiksi osuman löytyminen, voi johtaa siihen, että henkilöön kohdistetaan enemmän valvontaa, mutta se voi olla myös ratkaiseva todiste tuomioistuinmenettelyissä. Kasvojentunnistusteknologian puutteet, kuten mahdolliset vinoumat, syrjintä tai virheellinen tunnistus (”väärä positiivinen”), voivat näin ollen aiheuttaa vakavia seurauksia myös rikosoikeudellisissa menettelyissä. Lisäksi todisteiden arvioinnissa voidaan suosia kasvojentunnistusteknologian käytön tulosta, vaikka sen kanssa ristiriitaisia todisteita olisi olemassa (”automaatioharha”).

3.1.3 Oikeuksiin puuttumisen perusteet

42. Perusoikeuskirjan 52 artiklan 1 kohdan mukaan perusoikeuksien ja -vapauksien käyttämistä voidaan rajoittaa vain lailla ja kyseisten oikeuksien ja vapauksien keskeistä sisältöä kunnioittaen. Oikeasuhteisuusperiaatteen mukaisesti rajoituksia voidaan tehdä ainoastaan, jos ne ovat tarpeellisia ja vastaavat tosiasiallisesti Euroopan unionin tunnustamia yleisen edun mukaisia tavoitteita tai tarvetta suojella muiden henkilöiden oikeuksia ja vapauksia.

3.1.3.1 Lailla säädetyt perusteet

43. Perusoikeuskirjan 52 artiklan 1 kohdassa asetetaan vaatimus erityisestä oikeusperustasta. Tämän oikeusperustan on oltava sanamuodoltaan riittävän selkeä, jotta kansalaiset saavat riittävän käsityksen siitä, millä edellytyksillä ja missä tilanteissa viranomaisilla on valtuudet turvautua tiedonkeruutoimenpiteisiin ja salaiseen valvontaan[13]. Siinä on osoitettava riittävän selkeästi viranomaisille annetun harkintavallan laajuus ja käyttötapa, jotta yksilöille voidaan taata demokraattisen yhteiskunnan oikeusvaltioperiaatteen mukainen vähimmäissuoja[14]. Lisäksi lainmukaisuus edellyttää riittäviä turvatoimia sen varmistamiseksi, että erityisesti perusoikeuskirjan 8 artiklan mukaista yksilön oikeutta kunnioitetaan. Näitä periaatteita sovelletaan myös kasvojentunnistusjärjestelmien arviointia, kouluttamista ja jatkokehittämistä varten suoritettavaan henkilötietojen käsittelyyn.

44. Koska biometriset tiedot, joita käsitellään luonnollisen henkilön yksilöllistä tunnistamista varten, kuuluvat lainvalvontadirektiivin 10 artiklassa lueteltuihin erityisiin tietoryhmiin, kasvojentunnistusteknologian eri sovellukset edellyttäisivät useimmissa tapauksissa erityistä lakia,

[12] EUT, C-594/12, 36 kohta; EUT, C-291/12, 23 kohta ja seuraavat kohdat.
[13] EUT, Shimovolos v. Venäjä, 68 kohta, ja Vukota-Bojić v. Sveitsi.
[14] EUT, Piechowicz v. Puola, 212 kohta.

jossa kuvataan tarkasti sovellus ja sen käytön edellytykset. Tämä kattaisi erityisesti rikostyypit ja tarvittaessa asianmukaisen kynnysarvon näiden rikosten vakavuudelle, jotta muun muassa vähäiset rikokset voidaan sulkea soveltamisalan ulkopuolelle tehokkaasti.[15]

3.1.3.2 Perusoikeuskirjan 7 ja 8 artiklassa vahvistetun yksityisyyttä ja henkilötietojen suojaa koskevan perusoikeuden olennainen sisältö

45. Rajoitettaessa perusoikeuksia kussakin tilanteessa kyseisen oikeuden olennaista sisältöä on kuitenkin kunnioitettava. Olennaisella sisällöllä tarkoitetaan asianomaisen perusoikeuden ydintä[16]. Ihmisarvoa on kunnioitettava myös silloin, kun oikeuksia rajoitetaan[17].

46. Seuraavat asiat viittaavat siihen, että oikeuksien loukkaamatonta ydintä on mahdollisesti loukattu:

- Määräys, joka asettaa rajoituksia henkilön yksilöllisestä käyttäytymisestä tai poikkeuksellisista olosuhteista riippumatta[18].
- Tuomioistuimen puoleen kääntyminen ei ole mahdollista tai se on vaikeaa[19].
- Asianomaisen henkilön tilannetta ei oteta huomioon ennen vakavaa rajoitusta[20].
- Perusoikeuskirjan 7 ja 8 artiklan mukaisten oikeuksien osalta: Viestinnän metatietojen laajan keräämisen lisäksi sähköisen viestinnän sisältöä koskevan tiedon hankkiminen voisi loukata näiden oikeuksien olennaista sisältöä[21].
- Perusoikeuskirjan 7, 8 ja 11 artiklan mukaisten oikeuksien osalta: Säännöstö, jonka mukaan yhteyttä yleisölle tarkoitettuihin verkkoviestintäpalveluihin tarjoavien toimijoiden ja hosting-palvelujen tarjoajien on säilytettävä yleisesti ja erotuksetta muun muassa kyseisiin palveluihin liittyvät henkilötiedot[22].
- Perusoikeuskirjan 8 artiklan mukaisiin oikeuksiin viitaten: Tietosuojan ja tietoturvan perusperiaatteiden puuttuminen voisi myös loukata oikeuden ydintä[23].

3.1.3.3 Laillinen tarkoitus

47. Kuten kohdassa 3.1.3 jo selitettiin, perusoikeuksien rajoittamisen on vastattava tosiasiallisesti Euroopan unionin tunnustamia yleisen edun mukaisia tavoitteita tai tarvetta suojella muiden henkilöiden oikeuksia ja vapauksia.

48. Unioni tunnustaa sekä Euroopan unionista tehdyn sopimuksen 3 artiklassa mainitut tavoitteet että muut perussopimusten erityismääräyksillä suojatut edut[24], jotka koskevat muun muassa vapautta, turvallisuutta ja oikeudenmukaisuutta sekä rikollisuuden ehkäisemistä ja torjuntaa. Unionin olisi kansainvälisissä suhteissaan edistettävä rauhaa ja turvallisuutta sekä ihmisoikeuksien suojelua.

49. Tarve suojella muiden henkilöiden oikeuksia ja vapauksia viittaa Euroopan unionin tai sen jäsenvaltioiden lainsäädännöllä suojeltujen henkilöiden oikeuksiin. Arviointi on tehtävä siten, että

[15] Ks. esimerkiksi Euroopan unionin tuomioistuimen tuomiot asioissa C-817/19, Ligue des droits humains, 151 f kohta, ja C-207/16, Ministerio Fiscal, 56 kohta.
[16] EUT, C-279/09, RoC 2010 I-13849, 60 kohta.
[17] Euroopan unionin perusoikeuskirjan selitykset, I luku, 1 artiklan selitys, EUVL C 303, 14.12.2007, s. 17–35.
[18] EUT, C-601/15, 52 kohta.
[19] EUT, C-400/10, RoC 2010 I-08965, 55 kohta.
[20] EUT, C-408/03, RoC 2006 I-02647, 68 kohta.
[21] EUT, C-203/15 – Tele2 Sverige, 101 kohta, ja sen viittaus asioihin EUT, C-293/12 ja C-594/12, 39 kohta.
[22] EUT, C--512/18, La Quadrature du Net, 209 kohta ja sitä seuraavat kohdat.
[23] EUT, C-594/12, 40 kohta.
[24] Perusoikeuskirjan selitykset, I luku, 52 artiklan selitys, EUVL C 303, 14.12.2007, s. 17–35.

pyritään sovittamaan yhteen asianomaisten oikeuksien suojaa koskevat vaatimukset ja saada aikaan oikeudenmukainen tasapaino niiden välillä[25].

3.1.3.4 Tarpeellisuus ja oikeasuhteisuustesti

50. Kun on kyse perusoikeuksiin puuttumisesta, kansallisen ja unionin lainsäätäjän harkintavalta voi osoittautua rajalliseksi. Tämä riippuu useista tekijöistä, kuten kyseessä olevasta alasta, kyseessä olevan perusoikeuskirjassa taatun oikeuden luonteesta, puuttumisen luonteesta ja vakavuudesta sekä puuttumisen tavoitteesta[26]. Lainsäädäntötoimenpiteiden on oltava tarkoituksenmukaisia kyseessä olevalla lainsäädännöllä tavoiteltujen laillisten tavoitteiden saavuttamiseksi. Toimenpide ei myöskään saa ylittää sitä, mikä on tarkoituksenmukaista ja tarpeellista näiden tavoitteiden saavuttamiseksi[27]. Yleistä etua koskeva tavoite – oli se kuinka perustavanlaatuinen tahansa – ei itsessään oikeuta perusoikeuden rajoittamista[28].

51. Unionin tuomioistuimen vakiintuneen oikeuskäytännön mukaan henkilötietojen suojaan liittyviä poikkeuksia ja rajoituksia on sovellettava vain siinä määrin kuin se on ehdottoman välttämätöntä[29]. Tämä tarkoittaa myös sitä, että tavoitteen saavuttamiseksi ei ole käytettävissä vähemmän oikeuksiin puuttuvia keinoja. Mahdolliset vaihtoehdot, kuten – tarkoituksesta riippuen – henkilöstön lisääminen, tiheämmin toteutettava valvonta tai katuvalaistuksen lisääminen, on määritettävä ja arvioitava huolellisesti. Lainsäädäntötoimenpiteissä olisi eroteltava ne henkilöt ja ne olisi kohdistettava niihin henkilöihin, joita ne koskevat, tavoitteen saavuttamiseksi, esimerkiksi tiettyjen vakavien rikosten torjumiseksi. Jos toimenpide koskee yleisesti kaikkia henkilöitä ilman tällaista erottelua, rajoitusta tai poikkeusta, perusoikeuksiin puuttuminen on siinä tapauksessa vakavampaa[30]. Puuttuminen on vakavampaa myös silloin, jos tietojenkäsittely koskee merkittävää osaa väestöstä[31].

52. Perusoikeuskirjan 8 artiklan 1 kohdassa säädetystä nimenomaisesta velvoitteesta johtuva henkilötietojen suoja on erityisen tärkeä perusoikeuskirjan 7 artiklassa vahvistetun yksityiselämän kunnioittamista koskevan oikeuden kannalta[32]. Lainsäädännössä on säädettävä kyseisen toimenpiteen laajuutta ja soveltamista koskevista selkeistä ja täsmällisistä säännöistä sekä suojatoimista, jotta henkilöillä, joiden tietoja on käsitelty, on riittävät takeet siitä, että heidän henkilötietojaan suojellaan tehokkaasti väärinkäytösten riskiltä, laittomalta pääsyltä kyseisiin tietoihin tai niiden laittomalta käytöltä.[33] Tällaisten suojatoimien tarve on erityisen suuri silloin, kun henkilötietoja käsitellään

---

[25] Jarass GrCh, 3. Aufl. 2016, EU-Grundrechte-Charta Art. 52 Rn. 31–32.

[26] EUT, C-594/12, 47 kohta ja seuraavat lähteet: ks. analogisesti ihmisoikeussopimuksen 8 artiklan osalta Euroopan ihmisoikeustuomioistuimen tuomio asioissa S ja Marper v. Yhdistynyt kuningaskunta (suuri jaosto), nro 30562/04 ja nro 30566/04, 102 kohta, CEDH 2008-V.

[27] EUT, C-594/12, 46 kohta ja seuraavat lähteet: asia C-343/09, Afton Chemical, EU:C:2010:419, 45 kohta; Volker und Markus Schecke ja Eifert, EU:C:2010:662, 74 kohta; asiat C-581/10 ja C-629/10, Nelson ym., EU:C:2012:657, 71 kohta; asia C-283/11, Sky Österreich, EU:C:2013:28, 50 kohta; ja asia C-101/12, Schaible, EU:C:2013:661, 29 kohta.

[28] EUT, C-594/12, 51 kohta.

[29] EUT, C-594/12, 52 kohta ja seuraavat lähteet: tuomio IPI, C-473/12, EU:C:2013:715, 39 kohta oikeuskäytäntöviittauksineen.

[30] EUT, C-594/12, 57 kohta.

[31] EUT, C-594/12, 56 kohta.

[32] EUT, C-594/12, 53 kohta.

[33] EUT, C-594/12, 54 kohta ja seuraavat lähteet: ks. analogisesti Euroopan ihmisoikeussopimuksen 8 artiklan osalta Euroopan ihmisoikeustuomioistuimen tuomiot asioissa Liberty ym. v. Yhdistynyt kuningaskunta, 1.7.2008, nro 58243/00, 62 ja 63 kohta; Rotaru v. Romania, 57–59 kohta ja S ja Marper v. Yhdistynyt kuningaskunta, 99 kohta.

automaattisesti ja kun on olemassa merkittävä riski, että tietoihin päästään käsiksi laittomasti[34]. Lisäksi se, että kasvojentunnistusteknologian käyttöönottoon myönnetään lupa sisäisesti tai ulkoisesti, esimerkiksi oikeudellisesti, voi myös toimia suojatoimena, ja se voi osoittautua välttämättömäksi tietyissä tapauksissa, joissa oikeuksiin puuttuminen on vakavaa.[35]

53. Annettuja sääntöjä on mukautettava kyseessä olevaan tilanteeseen huomioon ottaen esimerkiksi käsiteltävien tietojen määrä, tietojen luonne[36] ja riski, että tietoihin päästään käsiksi laittomasti. Tämä edellyttää sääntöjä, joilla säännellään erityisesti kyseisten tietojen suojaamista ja turvallisuutta selkeästi ja täsmällisesti, jotta voidaan varmistaa tietojen täydellinen eheys ja luottamuksellisuus[37].

54. Rekisterinpitäjän ja henkilötietojen käsittelijän välisen suhteen osalta ei pidä sallia, että henkilötietojen käsittelijät ottavat huomioon ainoastaan taloudelliset näkökohdat määrittäessään henkilötietojen tietoturvan tasoa, sillä tämä voi vaarantaa tietosuojan riittävän korkean tason[38].

55. Säädöksessä on säädettävä aineellisista ja menettelyitä koskevista edellytyksistä ja objektiivisista kriteereistä, joiden avulla määritetään toimivaltaisten viranomaisten tietoihin pääsyn ja niiden myöhemmän käytön rajat. Rikosten ennalta estämistä, paljastamista tai niihin liittyviä syytetoimia varten kyseessä olevat rikokset olisi katsottava riittävän vakaviksi, jotta ne oikeuttavat perusoikeuskirjan 7 ja 8 artiklassa vahvistettuihin perusoikeuksiin puuttumisen laajuuden ja vakavuuden[39].

56. Tietoja on käsiteltävä siten, että varmistetaan EU:n tietosuojasääntöjen sovellettavuus ja vaikutus. Tämä koskee erityisesti perusoikeuskirjan 8 artiklaa, jonka mukaan tietosuojaa ja -turvaa koskevien vaatimusten noudattamista valvoo riippumaton viranomainen. Maantieteellisellä paikalla, jossa käsittely tapahtuu, voi olla tällaisessa tilanteessa merkitystä[40].

57. Henkilötietojen käsittelyn eri vaiheiden osalta tietoryhmät on erotettava toisistaan sen perusteella, miten hyödyllisiä ne mahdollisesti ovat kyseessä olevan tavoitteen kannalta, tai kyseessä olevien henkilöiden mukaan[41]. Käsittelyn edellytysten määrittämisen, esimerkiksi tietojen säilytysajan määrittämisen, on perustuttava objektiivisiin kriteereihin sen varmistamiseksi, että oikeuksiin puututaan vain sen verran kuin on ehdottoman välttämätöntä[42].

58. Tarpeellisuuden ja oikeasuhteisuuden arvioinnissa on tunnistettava ja otettava huomioon kunkin tilanteen perusteella kaikki seuraukset, jotka kuuluvat muiden perusoikeuksien, kuten perusoikeuskirjan 1 artiklan mukaisen ihmisarvon, perusoikeuskirjan 10 artiklan mukaisen ajatuksen-, omantunnon- ja uskonnonvapauden, perusoikeuskirjan 11 artiklan mukaisen sananvapauden sekä perusoikeuskirjan 12 artiklan mukaisen kokoontumis- ja yhdistymisvapauden, piiriin.

---

[34] EUT, C-594/12, 55 kohta, ja seuraavat lähteet: ks. analogisesti Euroopan ihmisoikeussopimuksen 8 artiklan osalta Euroopan ihmisoikeustuomioistuimen tuomiot asiassa S ja Marper v. Yhdistynyt kuningaskunta, 103 kohta ja asiassa M. K. v. Ranska, 18.4.2013, nro 19522/09, 35 kohta.

[35] Euroopan ihmisoikeustuomioistuimen asia Szabó ja Vissy v. Unkari, 73–77 kohta.

[36] Ks. myös teknisiä ja organisatorisia toimenpiteitä koskevat tiukennetut vaatimukset erityisiin tietoryhmiin kuuluvia tietoja käsiteltäessä, lainvalvontadirektiivin 29 artiklan 1 kohta.

[37] EUT, C-594/12, 66 kohta.

[38] EUT, C-594/12, 67 kohta.

[39] EUT, C-594/12, 60 ja 61 kohta.

[40] EUT, C-594/12, 68 kohta.

[41] EUT, C-594/12, 63 kohta.

[42] EUT, C-594/12, 64 kohta.

59. Lisäksi on pidettävä vakavana, että jos tietoja käsitellään järjestelmällisesti rekisteröityjen tietämättä, se todennäköisesti luo yleisen käsityksen jatkuvasta valvonnasta[43]. Tämä voi johtaa tukahduttaviin vaikutuksiin joidenkin tai kaikkien kyseessä olevien perusoikeuksien osalta.

60. Kasvojentunnistukseen liittyvien lainsäädäntötoimenpiteiden tarpeellisuuden ja oikeasuhteisuuden arvioinnin helpottamiseksi ja toteuttamiseksi lainvalvonnan alalla kansalliset ja unionin lainsäätäjät voisivat hyödyntää saatavilla olevia, erityisesti tätä tehtävää varten suunniteltuja käytännön välineitä. Erityisesti voitaisiin käyttää Euroopan tietosuojavaltuutetun tarjoamaa tarpeellisuuden ja oikeasuhteisuuden arviointia koskevaa välineistöä[44].

3.1.3.5 Perusoikeuskirjan 52 artiklan 3 kohta ja 53 artikla (suojan taso, myös suhteessa Euroopan ihmisoikeussopimuksen suojan tasoon)

61. Perusoikeuskirjan 52 artiklan 3 kohdan ja 53 artiklan mukaan Euroopan ihmisoikeussopimuksessa taattuja oikeuksia vastaavien perusoikeuskirjan oikeuksien merkityksen ja kattavuuden on oltava samat kuin Euroopan ihmisoikeussopimuksessa vahvistettujen oikeuksien merkityksen ja kattavuuden. Vaikka Euroopan ihmisoikeussopimuksesta on löydettävissä vastine erityisesti perusoikeuskirjan 7 artiklalle, näin ei ole perusoikeuskirjan 8 artiklan osalta[45]. Perusoikeuskirjan 52 artiklan 3 kohta ei estä unionia määräämästä tätä laajemmasta suojasta. Koska Euroopan ihmisoikeussopimus ei ole virallisesti unionin lainsäädäntöön sisällytetty oikeudellinen väline, unionin lainsäädäntöä on toteutettava perusoikeuskirjassa taattujen perusoikeuksien perusteella[46].

62. Euroopan ihmisoikeussopimuksen 8 artiklan mukaan viranomaiset eivät saa puuttua tämän yksityis- ja perhe-elämän kunnioittamista koskevan oikeuden käyttämiseen, paitsi jos se on lainsäädännön mukaista ja demokraattisessa yhteiskunnassa välttämätöntä kansallisen tai yleisen turvallisuuden tai maan taloudellisen hyvinvoinnin vuoksi, järjestyshäiriöiden tai rikosten ehkäisemiseksi, terveyden tai moraalin suojelemiseksi tai muiden henkilöiden oikeuksien ja vapauksien suojelemiseksi.

63. Euroopan ihmisoikeussopimuksessa asetetaan myös vaatimuksia sille, miten rajoituksia voidaan tehdä. Oikeusvaltioperiaatteen lisäksi yksi perusvaatimuksista on ennakoitavuus. Ennakoitavuutta koskevan vaatimuksen täyttämiseksi lainsäädännön on oltava sanamuodoltaan riittävän selkeää, jotta kansalaiset saavat riittävän käsityksen siitä, missä tilanteissa ja millä edellytyksillä viranomaisilla on valtuudet turvautua tällaisiin toimenpiteisiin[47]. Euroopan unionin tuomioistuin ja EU:n tietosuojalainsäädäntö tunnustavat tämän vaatimuksen (ks. kohta 3.2.1.1).

64. Euroopan ihmisoikeussopimuksen 8 artiklan mukaisia oikeuksia tarkentavia yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä tehdyn yleissopimuksen[48] määräyksiä on myös noudatettava täysimääräisesti. On kuitenkin otettava huomioon, että nämä määräykset ovat vain vähimmäisvaatimuksia voimassa olevan unionin lainsäädännön kannalta.

---

[43] EUT, C-594/12, 37 kohta.

[44] Euroopan tietosuojavaltuutettu: ”Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A toolkit” (11.4.2017), Euroopan tietosuojavaltuutettu: ”EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data” (19.12.2019).

[45] EUT, C-203/15, Tele2 Sverige, 129 kohta.

[46] EUT, C-311/18, 99 kohta.

[47] Euroopan ihmisoikeustuomioistuin, tuomio asiassa COPLAND v. YHDISTYNYT KUNINGASKUNTA, 3.4.2007, valitus nro 62617/00, 46 kohta.

[48] ETS N:o 108.

3.2 Erityinen oikeuskehys – lainvalvontatarkoituksessa käsiteltyjen henkilötietojen suojasta annettu direktiivi

65. Lainvalvontatarkoituksessa käsiteltyjen henkilötietojen suojasta annetussa direktiivissä (lainvalvontadirektiivi) säädetään tietystä kasvojentunnistusteknologian käyttöä koskevasta kehyksestä. Ensinnäkin lainvalvontadirektiivin 3 artiklan 13 kohdassa määritellään termi ”biometriset tiedot”[49]. Tarkempia tietoja on edellä kohdassa 2.1. Toiseksi 8 artiklan 2 kohdassa selvennetään, että jotta tietojen käsittely olisi laillista, sen on paitsi oltava välttämätöntä lainvalvontadirektiivin 1 artiklan 1 kohdassa mainittujen tarkoitusten kannalta mutta myös säänneltyä kansallisella lainsäädännöllä, jossa täsmennetään vähintään käsittelyn tavoitteet, käsiteltävät henkilötiedot ja käsittelyn tarkoitus. Muita biometristen tietojen kannalta erityisen merkityksellisiä säännöksiä ovat lainvalvontadirektiivin 10 ja 11 artikla. Direktiivin 10 artiklaa on luettava yhdessä direktiivin 8 artiklan kanssa[50]. Direktiivin 4 artiklassa säädettyjä henkilötietojen käsittelyn periaatteita olisi aina noudatettava, ja niiden olisi ohjattava kaikkea kasvojentunnistusteknologian avulla tehtävän mahdollisen biometrisen käsittelyn arviointia.

3.2.1 Erityisiä tietoryhmiä koskeva käsittely lainvalvontatarkoituksia varten

66. Lainvalvontadirektiivin 10 artiklan mukaan erityisten tietoryhmien, kuten biometristen tietojen, käsittely on sallittua vain, kun se on ehdottoman välttämätöntä ja kun siihen sovelletaan rekisteröidyn oikeuksia ja vapauksia koskevia asianmukaisia suojatoimia. Tämän lisäksi se on sallittua ainoastaan rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi, jos se sallitaan unionin tai jäsenvaltion lainsäädännössä, tai jos tällainen käsittely liittyy tietoihin, jotka rekisteröity on nimenomaisesti saattanut julkisiksi. Tässä yleisessä lausekkeessa korostetaan erityisiä tietoryhmiä koskevan käsittelyn arkaluonteisuutta.

3.2.1.1 Käsittely sallitaan unionin tai jäsenvaltion lainsäädännössä

67. Tarvittavan lainsäädäntötoimenpidetyypin osalta lainvalvontadirektiivin johdanto-osan 33 kappaleessa todetaan seuraavaa: ”[k]un tässä direktiivissä viitataan jäsenvaltion lainsäädäntöön, oikeusperustaan tai lainsäädäntötoimeen, siinä ei välttämättä edellytetä parlamentissa hyväksyttyä säädöstä, sanotun kuitenkaan rajoittamatta asianomaisen jäsenvaltion perustuslaillisen järjestyksen edellyttämien vaatimusten soveltamista”[51].

68. Perusoikeuskirjan 52 artiklan 1 kohdan mukaan perusoikeuskirjassa tunnustettujen oikeuksien ja vapauksien käyttämistä ”voidaan rajoittaa ainoastaan lailla”. Tämä vastaa Euroopan ihmisoikeussopimuksen 8 artiklan 2 kohdan ilmaisua ”kun laki sen sallii”, mikä tarkoittaa sovellettavan lainsäädännön mukaista käytäntöä mutta liittyy myös kyseessä olevan lain laatuun vaikuttamatta säädöksen luonteeseen ja edellyttää sen olevan oikeusvaltioperiaatteen mukainen.

69. Lainvalvontadirektiivin johdanto-osan 33 kappaleessa todetaan lisäksi seuraavaa: ”[k]yseisen jäsenvaltion lainsäädännön, oikeusperustan tai lainsäädäntötoimen olisi kuitenkin oltava selkeä ja täsmällinen ja sen soveltamisen olisi oltava asianosaisten kannalta ennakoitavissa unionin tuomioistuimen ja Euroopan ihmisoikeustuomioistuimen oikeuskäytännön mukaisesti. Tämän

[49] Lainvalvontadirektiivin 3 artiklan 13 kohta: ’biometrisillä tiedoilla’ tarkoitetaan kaikkia luonnollisen henkilön fyysisiin ja fysiologisiin ominaisuuksiin tai käyttäytymiseen liittyvällä teknisellä käsittelyllä saatuja henkilötietoja, kuten kasvokuvia tai sormenjälkitietoja, joiden perusteella kyseinen luonnollinen henkilö voidaan tunnistaa tai kyseisen henkilön tunnistaminen voidaan varmistaa.

[50] WP258, ”Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)” (lausunto joistakin lainvalvontadirektiivin (EU) 2016/680 keskeisistä kysymyksistä), s. 7.

[51] Harkittavan lainsäädäntötoimenpidetyypin on oltava unionin tai kansallisen lainsäädännön mukainen. Riippuen siitä, missä määrin rajoituksella puututaan perusoikeuksiin, kansallisella tasolla voidaan vaatia tiettyä lainsäädäntötoimenpidettä, jossa otetaan huomioon vaatimustaso.

direktiivin soveltamisalaan kuuluvaa henkilötietojen käsittelyä sääntelevässä jäsenvaltion lainsäädännössä olisi määritettävä ainakin tavoitteet, käsiteltävät henkilötiedot, käsittelyn tarkoitukset, menettelyt henkilötietojen eheyden ja luottamuksellisuuden säilyttämiseksi sekä menettelyt tietojen tuhoamiseksi".

70. Kansallisen lainsäädännön on oltava sanamuodoltaan riittävän selkeää, jotta rekisteröidyt saattavat riittävän käsityksen siitä, missä tilanteissa ja millä edellytyksillä rekisterinpitäjät voivat turvautua tällaisiin toimenpiteisiin. Tähän kuuluvat myös käsittelyn mahdolliset edellytykset, kuten tietyntyyppiset todisteet sekä oikeudellisen tai sisäisen luvan välttämättömyys. Asianomainen laki voi olla teknologianeutraali, jos siinä otetaan riittävästi huomioon kasvojentunnistusjärjestelmien suorittaman henkilötietojen käsittelyn erityiset riskit ja ominaispiirteet. Lainvalvontadirektiivin sekä Euroopan unionin tuomioistuimen (EUT) ja Euroopan ihmisoikeustuomioistuimen oikeuskäytännön mukaisesti on olennaista, että lainsäädäntötoimenpiteet, joiden tarkoituksena on tarjota oikeusperusta kasvojentunnistustoimenpiteelle, ovat rekisteröityjen ennakoitavissa.

71. Lainsäädäntötoimenpiteeseen ei voida vedota lakina, jolla sallitaan biometristen tietojen käsittely kasvojentunnistusjärjestelmän avulla lainvalvontatarkoituksiin, jos kyse on vain lainvalvontadirektiivin 10 artiklan yleisen lausekkeen saattamisesta osaksi kansallista lainsäädäntöä.

72. Biometristen tietojen lisäksi lainvalvontadirektiivin 10 artiklassa säännellään muihin erityisiin tietoryhmiin kuuluvien tietojen, kuten seksuaalisen suuntautumisen, poliittisten mielipiteiden ja uskonnollisten vakaumusten, käsittelystä, kattaen täten hyvin monenlaisen käsittelyn. Lisäksi tällaisesta säännöksestä puuttuisivat erityisvaatimukset, jotka koskevat sitä, missä tilanteissa ja millä edellytyksillä lainvalvontaviranomaiset voisivat turvautua kasvojentunnistusteknologian käyttöön. Muun tyyppisiin tietoihin ja erityisten suojatoimien nimenomaiseen tarpeeseen ilman lisätarkennuksia tehdyn viittauksen vuoksi kansallista säännöstä, jolla lainvalvontadirektiivin 10 artikla saatetaan osaksi kansallista lainsäädäntöä ja jonka sanamuoto on yhtä lailla yleinen ja abstrakti, ei voida käyttää oikeusperustana biometristen tietojen käsittelylle, johon liittyy kasvojentunnistusta, koska säännös ei olisi täsmällinen ja ennakoitava. Lainvalvontadirektiivin 28 artiklan 2 kohdan tai 46 artiklan 1 kohdan c alakohdan mukaisesti ennen kuin lainsäätäjä luo uuden oikeusperustan mille tahansa biometristen tietojen käsittelylle, jossa käytetään kasvojentunnistusta, olisi kuultava kansallista tietosuojaviranomaista.

3.2.1.2 Ehdoton välttämättömyys

73. Käsittelyä voidaan pitää "ehdottoman välttämättömänä" vain, jos henkilötietojen suojaan puututaan ja sitä rajoitetaan vain sen verran kuin on täysin välttämätöntä[52]. Ilmaisun "ehdottoman välttämätön" lisääminen tarkoittaa sitä, että lainsäätäjä on tarkoittanut, että erityisiä tietoryhmiä koskeva käsittely tapahtuu ainoastaan jopa tarpeellisuutta koskevia edellytyksiä tiukemmilla edellytyksillä (ks. edellä kohta 3.1.3.4). Tämä vaatimus olisi tulkittava ehdottomaksi. Se rajoittaa lainvalvontaviranomaiselle välttämättömyystestissä sallitun harkintamarginaalin ehdottomaan minimiin. Euroopan unionin tuomioistuimen vakiintuneen oikeuskäytännön mukaan "ehdottoman välttämättömyyden" edellytys liittyy myös tiiviisti niiden objektiivisten kriteerien vaatimukseen, joilla määritetään, missä tilanteissa ja millä edellytyksillä käsittely voidaan suorittaa, mikä sulkee pois kaiken yleisluonteisen tai järjestelmällisen käsittelyn[53].

[52] Yksityiselämän kunnioittamista koskevaa perusoikeutta koskeva vakiintunut oikeuskäytäntö, ks. EUT, asia C-73/07, 56 kohta (Satakunnan Markkinapörssi ja Satamedia); EUT, asiat C-92/09 ja C-93/09, 77 kohta (Schecke ja Eifert); EUT, asia C-594/12, 52 kohta (Digitaaliset oikeudet); EUT, asia C-362/14, 92 kohta (Schrems).
[53] EUT, asia C-623/17, 78 kohta.

3.2.1.3 Nimenomaisesti julkisiksi saattaminen

74. Arvioitaessa, liittyykö käsittely tietoihin, jotka rekisteröity on nimenomaisesti saattanut julkisiksi, on muistettava, että valokuvaa sellaisenaan ei järjestelmällisesti katsota biometriseksi tiedoksi[54]. Näin ollen se, että rekisteröity on nimenomaisesti saattanut valokuvan julkiseksi, ei tarkoita, että siihen liittyvät biometriset tiedot, jotka valokuvasta voidaan saada erityisillä teknisillä keinoilla, katsotaan nimenomaisesti julkisiksi saatetuiksi.

75. Jotta biometristen tietojen, kuten henkilötietojen yleisesti, voidaan katsoa olevan rekisteröidyn nimenomaisesti julkisiksi saattamia, rekisteröidyn on täytynyt tarkoituksellisesti asettaa biometrinen malli (eikä pelkästään kasvokuva) vapaasti saataville ja julkiseksi avoimen lähteen kautta. Jos kolmas osapuoli paljastaa biometriset tiedot, ei voida katsoa, että rekisteröity on nimenomaisesti saattanut tiedot julkisiksi.

76. Ei myöskään riitä, että rekisteröidyn käyttäytymistä tulkitaan, jotta voitaisiin katsoa, että biometriset tiedot on nimenomaisesti saatettu julkisiksi. Esimerkiksi sosiaalisten verkostojen tai verkkoalustojen osalta Euroopan tietosuojaneuvosto katsoo, että se, että rekisteröity ei ole käynnistänyt tai asettanut erityisiä yksityisyysominaisuuksia, ei riitä perusteeksi katsoa, että kyseinen rekisteröity on nimenomaisesti saattanut henkilötietonsa julkisiksi ja että näitä tietoja (esim. valokuvia) voidaan käsitellä ja muuttaa biometrisiksi malleiksi ja käyttää tunnistamistarkoituksiin ilman rekisteröidyn suostumusta. Yleisemmällä tasolla palvelun oletusasetuksia, kuten mallien asettamista julkisesti saataville, tai valinnan mahdollisuuden puuttumista, kuten sitä, että mallit saatetaan julkisiksi ilman, että käyttäjä voi muuttaa tätä asetusta, ei pitäisi millään tavalla tulkita siten, että tiedot on nimenomaisesti saatettu julkisiksi.

3.2.2 Automatisoidut yksittäispäätökset, profilointi mukaan lukien

77. Lainvalvontadirektiivin 11 artiklan 1 kohdassa säädetään jäsenvaltioiden velvollisuudesta kieltää yleisesti päätökset, jotka perustuvat pelkästään automatisoituun käsittelyyn, profilointi mukaan lukien, ja joilla on rekisteröityä koskevia kielteisiä oikeusvaikutuksia tai jotka vaikuttavat häneen merkittävästi. Poikkeuksena tähän yleiseen kieltoon tällainen käsittely voi olla mahdollista vain, jos se on sallittu unionin tai jäsenvaltion lainsäädännössä, jota sovelletaan rekisterinpitäjään ja jossa säädetään asianmukaisista suojatoimista rekisteröidyn oikeuksien ja vapauksien suojaamiseksi. Tämä koskee vähintään oikeutta vaatia, että rekisterinpitäjän puolelta tietojenkäsittelyyn osallistuu luonnollinen henkilö. Tätä poikkeusta voidaan käyttää vain rajoitetusti. Tätä kynnystä sovelletaan tavallisiin (eli ei erityisiin) henkilötietoryhmiin. Lainvalvontadirektiivin 11 artiklan 2 kohdan mukaiseen poikkeukseen sovelletaan vieläkin korkeampaa kynnystä, ja sitä käytetään rajoitetummin. Siinä korostetaan uudelleen, että ensimmäisen kohdan mukaiset päätökset eivät saa perustua erityisiin tietoryhmiin, etenkään biometrisiin tietoihin tarkoituksena luonnollisen henkilön yksilöllinen tunnistaminen. Poikkeusta voidaan soveltaa vain, jos on toteutettu asianmukaiset toimenpiteet rekisteröidyn oikeuksien ja vapauksien sekä asianomaisen luonnollisen henkilön oikeutettujen etujen suojaamiseksi. Tätä poikkeusta on tarkasteltava lainvalvontadirektiivin 10 artiklan sääntöjen lisäksi ja ottaen ne huomioon.

78. Kasvojentunnistusjärjestelmästä riippuen edes luonnollisen henkilön suorittama kasvojentunnistuksen tulosten arviointi ei välttämättä anna itsessään riittävää takuuta yksilön

[54] Ks. yleisen tietosuoja-asetuksen johdanto-osan 51 kappale: ”valokuvien käsittelyä ei olisi automaattisesti katsottava henkilötietojen erityisryhmien käsittelyksi, koska valokuvat kuuluvat biometristen tietojen määritelmän piiriin ainoastaan siinä tapauksessa, että niitä käsitellään erityisin teknisin menetelmin, jotka mahdollistavat luonnollisen henkilön yksilöllisen tunnistamisen tai todentamisen ”.

oikeuksien ja erityisesti henkilötietojen suojaa koskevan oikeuden kunnioittamisesta, kun otetaan huomioon itse käsittelystä mahdollisesti aiheutuvat vinoutumat ja virheet. Lisäksi luonnollisen henkilön suorittamaa käsittelyä voidaan pitää suojatoimenpiteenä vain, jos kyseinen henkilö voi kriittisesti kyseenalaistaa kasvojentunnistusteknologian tulokset suorittamansa käsittelyn aikana. On olennaisen tärkeää, että henkilö ymmärtää kasvojentunnistusjärjestelmää ja sen rajoja sekä pystyy tulkitsemaan sen tuloksia oikein. On myös välttämätöntä luoda sellainen työpaikka ja organisaatio, joka torjuu automaatioharhan vaikutuksia ja välttää edistämästä tulosten kritiikitöntä hyväksymistä esimerkiksi kiireen, raskaiden menettelyjen ja mahdollisten kielteisten uraan kohdistuvien vaikutusten vuoksi.

79. Lainvalvontadirektiivin 11 artiklan 3 kohdan mukaan profilointi, jonka tuloksena luonnollisia henkilöitä syrjitään erityisten henkilötietoryhmien, kuten biometristen tietojen, perusteella, on kiellettyä unionin oikeuden mukaisesti. Lainvalvontadirektiivin 3 artiklan 4 kohdan mukaan ’profiloinnilla’ tarkoitetaan mitä tahansa henkilötietojen automaattista käsittelyä, jossa henkilötietoja käyttämällä arvioidaan luonnollisen henkilön tiettyjä henkilökohtaisia ominaisuuksia, erityisesti analysoidaan tai ennakoidaan ominaisuuksia, jotka liittyvät kyseisen luonnollisen henkilön työsuoritukseen, taloudelliseen tilanteeseen, terveyteen, henkilökohtaisiin mieltymyksiin, kiinnostuksen kohteisiin, luotettavuuteen, käyttäytymiseen, sijaintiin tai liikkeisiin. Pohdittaessa, onko toteutettu asianmukaisia toimenpiteitä rekisteröidyn oikeuksien ja vapauksien sekä asianomaisen luonnollisen henkilön oikeutettujen etujen suojaamiseksi, on pidettävä mielessä, että kasvojentunnistusteknologian käyttö voi johtaa profilointiin riippuen kasvojentunnistusteknologian käyttötavasta ja -tarkoituksesta. Unionin lainsäädännön ja lainvalvontadirektiivin 11 artiklan 3 kohdan mukaisesti profilointi, joka johtaa luonnollisten henkilöiden syrjintään erityisten henkilötietoryhmien perusteella, on joka tapauksessa kielletty.

3.2.3 Rekisteröityjen ryhmät

80. Lainvalvontadirektiivin 6 artiklassa säädetään, että eri rekisteröityjen ryhmät on erotettava toisistaan. Tämä erottaminen on tehtävä tarvittaessa ja mahdollisuuksien mukaan. Erottamisella on oltava vaikutus tapaan, jolla tietoja käsitellään. Lainvalvontadirektiivin 6 artiklassa annetuista esimerkeistä voidaan päätellä, että yleisesti ottaen henkilötietojen käsittelyn on täytettävä tarpeellisuuden ja oikeasuhteisuuden kriteerit myös rekisteröityjen ryhmän osalta[55]. Lisäksi voidaan päätellä, että sellaisten rekisteröityjen osalta, joiden osalta ei ole näyttöä siitä, että heidän käyttäytymisellään saattaisi olla edes välillinen tai kaukainen yhteys lainvalvontadirektiivin mukaiseen lailliseen tarkoitukseen, puuttumista ei todennäköisimmin voida perustella[56]. Jos lainvalvontadirektiivin 6 artiklan mukainen erottaminen ei ole sovellettavissa tai mahdollista, poikkeus kyseisen artiklan säännökseen on otettava tarkasti huomioon arvioitaessa puuttumisen tarpeellisuutta ja oikeasuhteisuutta. Eri rekisteröityjen ryhmien erottaminen näyttää olevan olennainen vaatimus kasvojentunnistusteknologiaa hyödyntävässä henkilötietojen käsittelyssä, kun otetaan huomioon myös mahdolliset väärät positiiviset tai väärät negatiiviset osumat, joilla voi olla merkittäviä vaikutuksia sekä rekisteröityjen kannalta että tutkinnan aikana.

81. Kuten edellä on todettu, unionin lainsäädäntöä täytäntöön pantaessa on noudatettava Euroopan unionin perusoikeuskirjan määräyksiä (ks. perusoikeuskirjan 52 artikla). Lainvalvontadirektiivissä säädettyä kehystä ja kriteerejä on siksi luettava perusoikeuskirja huomioon ottaen. EU:n ja sen jäsenvaltioiden säädökset eivät saa jäädä tätä toimenpidettä vähäisimmiksi, ja niissä on varmistettava perusoikeuskirjan täysimääräiset vaikutukset.

[55] Ks. myös EUT, C-594/12, 56–59 kohta.
[56] Ks. myös EUT, C-594/12, 58 kohta.

3.2.4 Rekisteröidyn oikeudet

82. Euroopan tietosuojaneuvosto on jo antanut ohjeita yleisen tietosuoja-asetuksen mukaisista rekisteröityjen oikeuksista eri näkökohtien osalta[57]. Lainvalvontadirektiivissä säädetään samanlaisista rekisteröityjen oikeuksista, ja tätä koskevia yleisiä ohjeita on annettu 29 artiklan mukaisen tietosuojatyöryhmän lausunnossa, jonka Euroopan tietosuojaneuvosto on hyväksynyt[58]. Tietyissä tilanteissa lainvalvontadirektiivissä sallitaan joitakin rajoituksia näihin oikeuksiin. Tällaisten rajoitusten parametreja käsitellään tarkemmin kohdassa 3.2.4.6 ”Lailliset rajoitukset rekisteröidyn oikeuksiin”.

83. Vaikka kaikkia lainvalvontadirektiivin III luvussa lueteltuja rekisteröidyn oikeuksia sovelletaan luonnollisesti myös kasvojentunnistusteknologian avulla tapahtuvaan henkilötietojen käsittelyyn, seuraavassa luvussa keskitytään tiettyihin oikeuksiin ja näkökohtiin, joista saattaa olla erityisen tärkeää saada ohjeita. Kyseisessä kasvojentunnistusteknologian avulla tapahtuvassa käsittelyssä, joka täyttää edellisessä luvussa kuvatut lakisääteiset vaatimukset, on lisäksi noudatettava tätä lukua ja sen analyysia.

84. Kun otetaan huomioon kasvojentunnistusteknologian avulla tapahtuvan henkilötietojen käsittelyn luonne (erityisten henkilötietoryhmien käsittely usein ilman ilmeistä vuorovaikutusta rekisteröidyn kanssa), rekisterinpitäjän on pohdittava huolellisesti, miten se voi (tai voiko se) täyttää lainvalvontadirektiivin vaatimukset, ennen kuin tällainen käsittely aloitetaan, erityisesti analysoimalla huolellisesti

- keitä rekisteröidyt ovat (usein muitakin kuin se henkilö / ne henkilöt, joka/jotka ovat käsittelyn tarkoituksen pääasiallinen kohde)
- miten rekisteröidyt saadaan tietoisiksi kasvojentunnistusteknologian avulla tapahtuvasta käsittelystä (ks. kohta 3.2.4.1)
- miten rekisteröidyt voivat käyttää oikeuksiaan (tässä yhteydessä sekä tiedonsaanti- ja tietoihin pääsyoikeuden että tietojen oikaisemista tai käsittelyn rajoittamista koskevan oikeuden säilyttäminen voi olla erityisen haasteellista, jos kasvojentunnistusteknologiaa käytetään kaikkiin paitsi yksi-yhteen-todentamiseen, joka tapahtuu suorassa kontaktissa rekisteröityyn).

3.2.4.1 Oikeuksien ja tietojen saattaminen rekisteröityjen tietoon tiiviisti esitetyssä, ymmärrettävässä ja helposti saatavilla olevassa muodossa

85. Kasvojentunnistusteknologiaan liittyy haasteita, jotka koskevat sen varmistamista, että rekisteröidyt ovat tietoisia biometristen tietojensa käsittelystä. Erityisen haastavaa on, jos lainvalvontaviranomainen analysoi kasvojentunnistusteknologian avulla videomateriaalia, joka on peräisin kolmannelta osapuolelta tai jonka kolmas osapuoli on toimittanut, sillä lainvalvontaviranomaisella on vain vähän, useimmiten ei ollenkaan, mahdollisuuksia ilmoittaa rekisteröidylle asiasta tiedonkeruun aikana (esimerkiksi paikan päällä olevalla kyltillä). Kaikki videomateriaali, joilla ei ole merkitystä tutkinnan (tai käsittelytarkoituksen) kannalta, olisi aina poistettava tai anonymisoitava ennen biometristen tietojen käsittelyn aloittamista (esimerkiksi sumentamalla ilman mahdollisuutta palauttaa tietoja jälkikäteen). Näin vältetään riski siitä, että lainvalvontadirektiivin 4 artiklan 1 kohdan e alakohdassa säädettyä minimointiperiaatetta ja 13 artiklan 2 kohdassa säädettyjä tiedonantovelvoitteita ei noudateta. On rekisterinpitäjän vastuulla arvioida, mitkä tiedot ovat rekisteröidyn oikeuksien käyttämisen kannalta merkityksellisiä, ja varmistaa, että

[57] Ks. esim. Euroopan tietosuojaneuvosto, ”Guidelines 01/2022 on data subject rights – Right of access”, ja Euroopan tietosuojaneuvosto, ”Ohjeet 3/2019 henkilötietojen käsittelystä videolaitteilla”.
[58] WP258, ”Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)” (lausunto joistakin lainvalvontadirektiivin (EU) 2016/680 keskeisistä kysymyksistä).

tarvittavat tiedot toimitetaan. Rekisteröidyn oikeuksien tehokas käyttö riippuu siitä, täyttääkö rekisterinpitäjä tiedonantovelvoitteensa.

86. Lainvalvontadirektiivin 13 artiklan 1 kohdassa säädetään, mitä vähimmäistietoja rekisteröidylle on yleensä annettava. Nämä tiedot voidaan toimittaa rekisterinpitäjän verkkosivustolla, painetussa muodossa (esimerkiksi pyynnöstä saatavilla oleva esite) tai muuten rekisteröidyn helposti saatavilla olevissa tietolähteissä. Rekisterinpitäjän on joka tapauksessa varmistettava, että ainakin seuraavat tiedot toimitetaan tehokkaasti:

- rekisterinpitäjän, myös tietosuojavastaavan, henkilöllisyys ja yhteystiedot
- käsittelyn tarkoitus ja se, että käsittely tapahtuu kasvojentunnistusteknologian avulla
- oikeus tehdä valitus valvontaviranomaiselle ja tällaisen viranomaisen yhteystiedot
- oikeus pyytää pääsyä henkilötietoihin ja niiden oikaisemista tai poistamista sekä henkilötietojen käsittelyn rajoittamista.

87. Lisäksi kansallisessa lainsäädännössä määritellyissä erityistapauksissa, joiden on oltava lainvalvontadirektiivin 13 artiklan 2 kohdan mukaisia[59], kuten esimerkiksi kasvojentunnistusteknologian avulla tapahtuvan käsittelyn yhteydessä, seuraavat tiedot on annettava suoraan rekisteröidylle:

- käsittelyn oikeusperusta
- tiedot siitä, missä henkilötiedot on kerätty rekisteröidyn tietämättä
- henkilötietojen säilytysaika tai, jos tämä ei ole mahdollista, perusteet, joiden mukaan kyseinen aika määritetään
- tarvittaessa henkilötietojen vastaanottajaryhmät (mukaan lukien kolmannet maat tai kansainväliset järjestöt).

88. Vaikka lainvalvontadirektiivin 13 artiklan 1 kohta koskee yleisön saataville saatettavia yleisluonteisia tietoja, lainvalvontadirektiivin 13 artiklan 2 kohdassa säädetään lisätiedoista, jotka on annettava rekisteröidylle tietyissä erityistapauksissa, esimerkiksi silloin, kun tietoja kerätään suoraan rekisteröidyltä tai välillisesti rekisteröidyn tietämättä[60]. Lainvalvontadirektiivin 13 artiklan 2 kohdassa ei ole selkeää määritelmää siitä, mitä ”erityistapauksilla” tarkoitetaan. Siinä viitataan kuitenkin tilanteisiin, joissa rekisteröidyille on tiedotettava heitä nimenomaisesti koskevasta käsittelystä ja heille on annettava asianmukaiset tiedot, jotta he voivat käyttää oikeuksiaan tehokkaasti. Euroopan tietosuojaneuvosto katsoo, että arvioitaessa, onko kyseessä ”erityistapaus”, on otettava huomioon useita tekijöitä, muun muassa se, kerätäänkö henkilötietoja rekisteröidyn tietämättä, sillä rekisteröidyt voivat käyttää oikeuksiaan tehokkaasti vain, jos he ovat tietoisia tietojensa keräämisestä. Muita esimerkkejä ”erityistapauksista” voivat olla tilanteet, joissa henkilötietoja käsitellään edelleen kansainvälisessä rikosoikeudellisessa yhteistyömenettelyssä tai joissa henkilötietoja käsitellään peitetoimien yhteydessä kansallisen lainsäädännön mukaisesti. Lisäksi lainvalvontadirektiivin johdanto-osan 38 kappaleesta seuraa, että jos päätöksiä tehdään pelkästään kasvojentunnistusteknologian perusteella, rekisteröidyille on ilmoitettava automatisoidun

[59] Esim. Saksan liittovaltion tietosuojalain 56 §:n 1 momentti, jossa säädetään muun muassa, mitä tietoja rekisteröidyille on annettava peiteoperaatioissa.
[60] WP258, ”Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)” (lausunto joistakin lainvalvontadirektiivin (EU) 2016/680 keskeisistä kysymyksistä), s. 17–18.

päätöksenteon piirteistä. Tämä viittaa myös siihen, että kyseessä on erityistapaus, jossa rekisteröidylle on toimitettava lisätietoja lainvalvontadirektiivin 13 artiklan 2 kohdan mukaisesti[61].

89. Lopuksi olisi pantava merkille, että lainvalvontadirektiivin 13 artiklan 3 kohdan mukaan jäsenvaltiot voivat hyväksyä lainsäädäntötoimenpiteitä, joilla rajoitetaan velvoitetta antaa tietoja erityistapauksissa tiettyjen tavoitteiden osalta. Tätä sovelletaan siinä määrin ja niin kauan kuin tällainen toimenpide on tarpeellinen ja oikeasuhteinen toimenpide demokraattisessa yhteiskunnassa ottaen asianmukaisesti huomioon rekisteröidyn perusoikeudet ja oikeutetut edut.

3.2.4.2 Oikeus saada pääsy tietoihin

90. Yleisesti ottaen rekisteröidyllä on oikeus saada myönteinen tai kielteinen vahvistus kaikesta henkilötietojensa käsittelystä ja, jos vastaus on myönteinen, pääsy itse henkilötietoihin sekä lisätiedot, jotka luetellaan lainvalvontadirektiivin 14 artiklassa. Kasvojentunnistusteknologian osalta, kun biometriset tiedot on tallennettu ja liitetty henkilöllisyyteen käyttäen myös aakkosnumeerisia tietoja, toimivaltaisen viranomaisen pitäisi pystyä vahvistamaan pääsyä koskeva pyyntö kyseisiä aakkosnumeerisia tietoja käyttämällä tehdyn haun perusteella käynnistämättä muiden henkilöiden biometristen tietojen edelleenkäsittelyä (eli tekemättä hakuja tietokannassa kasvojentunnistusteknologian avulla). Tietojen minimoinnin periaatetta on noudatettava, eikä tietoja tule säilyttää enempää kuin on käsittelyn tarkoituksen kannalta tarpeellista.

3.2.4.3 Oikeus henkilötietojen oikaisemiseen

91. Koska kasvojentunnistusteknologia ei tuota absoluuttisen tarkkoja tuloksia, on erityisen tärkeää, että rekisterinpitäjät ovat valppaina henkilötietojen oikaisua koskevien pyyntöjen suhteen. Näin voi olla myös silloin, jos rekisteröity on kasvojentunnistusteknologian perusteella luokiteltu virheelliseen ryhmään, esimerkiksi jos hänet on virheellisesti luokiteltu epäiltyjen ryhmään videokuvassa tapahtuvasta toiminnasta tehdyn ensimmäisen olettamuksen perusteella. Rekisteröityihin kohdistuvat riskit ovat erityisen vakavia, jos tällaisia virheellisiä tietoja tallennetaan poliisitietokantaan ja/tai jaetaan muiden tahojen kanssa. Rekisterinpitäjän on korjattava tallennetut tiedot ja kasvojentunnistusjärjestelmät vastaavasti (ks. lainvalvontadirektiivin johdanto-osan 47 kappale).

3.2.4.4 Oikeus tietojen poistamiseen

92. Jos kasvojentunnistusteknologiaa ei käytetä yksi-yhteen-todentamiseen, se merkitsee useimmissa tapauksissa sitä, että rekisteröityjen biometrisiä tietoja käsitellään suuria määriä. Sen vuoksi on tärkeää, että rekisterinpitäjä harkitsee etukäteen, missä käsittelyn tarkoituksen ja tarpeellisuuden rajat kulkevat, jotta lainvalvontadirektiivin 16 artiklan mukainen tietojen poistamista koskeva pyyntö voidaan käsitellä ilman aiheetonta viivytystä (sillä rekisterinpitäjän on muun muassa poistettava henkilötiedot, joita käsitellään laajemmin kuin mitä lainvalvontadirektiivin 4, 8 ja 10 artiklan mukainen sovellettava lainsäädäntö sallii).

3.2.4.5 Oikeus tietojen käsittelyn rajoittamiseen

93. Jos rekisteröity kiistää tietojen paikkansapitävyyden eikä tietojen paikkansapitävyyttä voida varmistaa (tai jos henkilötietoja on säilytettävä tulevaa todistusaineistoa varten), rekisterinpitäjällä on velvollisuus rajoittaa kyseisen rekisteröidyn henkilötietojen käsittelyä lainvalvontadirektiivin 16 artiklan mukaisesti. Tämä on erityisen tärkeää kasvojentunnistusteknologian (joka perustuu algoritmiin tai algoritmeihin ja ei sen vuoksi anna koskaan ehdottomia tuloksia) suhteen tilanteissa, joissa kerätään suuria määriä tietoja ja tunnistuksen tarkkuus ja laatu voivat vaihdella. Jos (esimerkiksi

[61] Huomaa lainvalvontadirektiivin 13 artiklan 1 kohdassa olevan ilmaisun ”asettaa rekisteröidyn saataville” ja 13 artiklan 2 kohdassa olevan ilmaisun ”antaa rekisteröidylle” välinen ero. Lainvalvontadirektiivin 13 artiklan 2 kohdan mukaan rekisterinpitäjän on varmistettava, että rekisteröity saa tiedot, ja tietojen julkaiseminen verkkosivustolla ei riitä.

rikospaikalta saatu) videomateriaali on huonolaatuista, väärien positiivisten tulosten riski kasvaa. Väärien positiivisten tai väärien negatiivisten tulosten riskiä lisää myös se, jos tarkkailulistalla olevia kasvokuvia ei päivitetä säännöllisesti. Erityistapauksissa, joissa tietoja ei voida poistaa, koska on perusteltua uskoa, että niiden poistaminen voisi vaikuttaa rekisteröidyn oikeutettuihin etuihin, tietojen käsittelyä olisi sen sijaan rajoitettava ja tietoja käsiteltävä ainoastaan sitä tarkoitusta varten, joka esti niiden poistamisen (ks. lainvalvontadirektiivin johdanto-osan 47 kappale).

3.2.4.6 Lailliset rajoitukset rekisteröidyn oikeuksiin

94. Rekisterinpitäjän tiedonantovelvoitteiden ja rekisteröityjen tietoihin pääsyä koskevan oikeuden rajoitukset ovat sallittuja vain, jos niistä säädetään laissa, jonka on puolestaan oltava välttämätön ja oikeasuhteinen toimenpide demokraattisessa yhteiskunnassa ottaen asianmukaisesti huomioon kyseisen luonnollisen henkilön perusoikeudet ja oikeutetut edut (ks. lainvalvontadirektiivin 13 artiklan 3 kohta, 13 artiklan 4 kohta, 15 artikla ja 16 artiklan 4 kohta). Kun kasvojentunnistusteknologiaa käytetään lainvalvontatarkoituksiin, voidaan olettaa, että sitä käytetään tilanteissa, joissa asiasta rekisteröidylle ilmoittaminen tai tietoihin pääsyn salliminen olisi haitallista käsittelyn tarkoituksen kannalta. Tämä koskee esimerkiksi rikosten poliisitutkintaa tai kansallisen tai yleisen turvallisuuden suojelemista.

95. Oikeus saada pääsy tietoihin ei automaattisesti tarkoita pääsyä kaikkiin tietoihin esimerkiksi rikosasiassa, jossa henkilön henkilötietoja esiintyy. Oikeutta voitaisiin rajoittaa esimerkiksi rikostutkinnan aikana.

3.2.4.7 Oikeuksien käyttäminen valvontaviranomaisen välityksellä

96. Tapauksissa, joissa lainvalvontadirektiivin III luvun mukaisten oikeuksien käyttämiselle on laillisia rajoituksia, rekisteröity voi pyytää tietosuojaviranomaista käyttämään oikeuksiaan puolestaan tarkistamalla rekisterinpitäjän suorittaman käsittelyn lainmukaisuuden. Rekisterinpitäjän on ilmoitettava rekisteröidylle mahdollisuudesta käyttää oikeuksia tällä tavalla (ks. lainvalvontadirektiivin 17 artikla ja 46 artiklan 1 kohdan g alakohta). Kasvojentunnistusteknologian osalta tämä tarkoittaa, että rekisterinpitäjän on varmistettava, että käytössä on asianmukaisia toimenpiteitä, jotta tällainen pyyntö voidaan käsitellä, esimerkiksi mahdollistamalla tallennetun aineiston etsiminen edellyttäen, että rekisteröity antaa riittävät tiedot henkilötietojensa löytämiseksi.

3.2.5 Muut lakisääteiset vaatimukset ja suojatoimet

3.2.5.1 27 artikla – tietosuojaa koskeva vaikutustenarviointi

97. Tietosuojaa koskeva vaikutustenarviointi ennen kasvojentunnistusteknologian käyttöä on pakollinen vaatimus, sillä tietyntyyppinen käsittely etenkin uutta teknologiaa käytettäessä todennäköisesti aiheuttaa käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset huomioon ottaen luonnollisten henkilöiden oikeuksien ja vapauksien kannalta korkean riskin. Koska kasvojentunnistusteknologian käyttö sisältää erityisiin tietoryhmiin kuuluvien tietojen järjestelmällistä automaattista käsittelyä, voitaisiin olettaa, että tällaisissa tapauksissa rekisterinpitäjä olisi pääsääntöisesti velvollinen suorittamaan tietosuojaa koskevan vaikutustenarvioinnin. Tietosuojaa koskevan vaikutustenarvioinnin olisi sisällettävä vähintään yleinen kuvaus suunnitelluista käsittelytoimista, arvio käsittelytoimien tarpeellisuudesta ja oikeasuhteisuudesta suhteessa tarkoituksiin, arvio rekisteröityjen oikeuksiin ja vapauksiin kohdistuvista riskeistä, kyseisten riskien torjumiseksi suunnitellut toimenpiteet, suojatoimet, turvatoimet ja mekanismit, joilla taataan henkilötietojen suojaaminen ja osoitetaan vaatimustenmukaisuus. Euroopan tietosuojaneuvosto suosittelee tällaisten arviointien tulosten tai

ainakin tietosuojaa koskevan vaikutustenarvioinnin keskeisten havaintojen ja päätelmien julkaisemista luottamusta ja avoimuutta lisäävänä toimenpiteenä[62].

3.2.5.2 28 artikla – valvontaviranomaisen ennakkokuuleminen

98. Lainvalvontadirektiivin 28 artiklan mukaan rekisterinpitäjän tai henkilötietojen käsittelijän on kuultava valvontaviranomaista ennen henkilötietojen käsittelyä, jos a) tietosuojaa koskeva vaikutustenarviointi osoittaa, että käsittely aiheuttaa korkean riskin, ellei rekisterinpitäjä toteuta toimenpiteitä riskin lieventämiseksi; tai b) tietojen käsittely on sen luonteista, että siihen sisältyy muutoin, erityisesti uusien tekniikoiden, mekanismien tai menettelyjen käytön johdosta, rekisteröityjen oikeuksien ja vapauksien kannalta korkea riski. Kuten näiden ohjeiden kohdassa 2.3 on jo selitetty, Euroopan tietosuojaneuvosto katsoo, että useimpiin kasvojentunnistusteknologian käyttöönotto- ja käyttötapauksiin liittyy korkea riski rekisteröityjen oikeuksien ja vapauksien kannalta. Sen vuoksi kasvojentunnistusteknologiaa käyttöön ottavan viranomaisen olisi tietosuojaa koskevan vaikutustenarvioinnin suorittamisen lisäksi kuultava toimivaltaista valvontaviranomaista ennen kyseisen järjestelmän käyttöönottoa.

3.2.5.3 29 artikla – tietojenkäsittelyn turvallisuus

99. Koska biometriset tiedot ovat yksilöllisiä, rekisteröity ei voi muuttaa niitä, jos ne vaarantuvat esimerkiksi tietoturvaloukkauksen seurauksena. Sen vuoksi kasvojentunnistusteknologiaa käyttöönottavan ja/tai käyttävän toimivaltaisen viranomaisen olisi kiinnitettävä erityistä huomiota käsittelyn turvallisuuteen lainvalvontadirektiivin 29 artiklan mukaisesti. Lainvalvontaviranomaisen olisi erityisesti varmistettava, että järjestelmä on asiaankuuluvien standardien mukainen, ja toteutettava toimenpiteitä biometristen mallien suojaamiseksi[63]. Tämä velvoite on vieläkin tärkeämpi, jos lainvalvontaviranomainen käyttää palveluntarjoajana kolmatta osapuolta (tietojen käsittelijä).

3.2.5.4 20 artikla – sisäänrakennettu ja oletusarvoinen tietosuoja

100. Sisäänrakennetun ja oletusarvoisen tietosuojan tarkoituksena on lainvalvontadirektiivin 20 artiklan mukaisesti varmistaa, että tietosuojaa koskevat periaatteet ja suojatoimet, kuten tietojen minimointi ja tietojen tallentamisen rajoittaminen, sisällytetään teknologiaan asianmukaisten teknisten ja organisatoristen toimenpiteiden, kuten pseudonymisoinnin, avulla jo ennen henkilötietojen käsittelyn aloittamista ja että näitä periaatteita ja suojatoimia sovelletaan koko teknologian elinkaaren ajan. Koska luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuu korkea riski, tällaisten toimenpiteiden valinta ei saisi riippua yksinomaan taloudellisista näkökohdista[64], vaan sen sijaan olisi pyrittävä valitsemaan kehittyneintä tietosuojateknologiaa. Vastaavasti, jos lainvalvontaviranomainen aikoo soveltaa ja käyttää ulkopuolisten palveluntarjoajien kasvojentunnistusteknologiaa, sen on varmistettava esimerkiksi hankintamenettelyllä, että käyttöön otetaan ainoastaan sisäänrakennetun ja oletusarvoisen tietosuojan periaatteisiin perustuvaa kasvojentunnistusteknologiaa[65]. Tämä merkitsee myös sitä, että kasvojentunnistusteknologian toiminnan läpinäkyvyyttä ei rajoiteta viittaamalla liikesalaisuuteen tai teollis- ja tekijänoikeuksiin.

---

[62] Lisätietoja on tietosuojaryhmän ohjeissa tietosuojaa koskevasta vaikutustenarvioinnista ja keinoista selvittää ”liittyykö käsittelyyn todennäköisesti korkea riski”, WP248 rev.01.

[63] Ks. esimerkiksi ISO/IEC 24745: ”Information security, cybersecurity and privacy protection – Biometric information protection” (Tietoturva, kyberturvallisuus ja yksityisyyden suoja – biometristen tietojen suojaaminen).

[64] Ks. lainvalvontadirektiivin johdanto-osan 53 kappale.

[65] Lisätietoja on Euroopan tietosuojaneuvoston sisäänrakennettua ja oletusarvoista tietosuojaa koskevissa ohjeissa (https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf).

3.2.5.5 25 artikla – lokitiedot

101. Lainvalvontadirektiivissä säädetään eri menetelmistä, joilla rekisterinpitäjä tai henkilötietojen käsittelijä voi osoittaa käsittelyn lainmukaisuuden ja varmistaa tietojen eheyden ja tietoturvan. Tältä osin järjestelmälokitiedot ovat erittäin hyödyllinen väline ja tärkeä suojatoimi käsittelyn lainmukaisuuden tarkistamiseksi sekä sisäisesti (ts. omaehtoinen valvonta) että ulkoisten valvontaviranomaisten, kuten tietosuojaviranomaisten, toimesta. Lainvalvontadirektiivin 25 artiklan mukaan ainakin seuraavista automatisoiduissa käsittelyjärjestelmissä suoritettavista käsittelytoimista on säilytettävä lokitiedot: tietojen kerääminen, muuttaminen, kysely, luovuttaminen siirrot mukaan lukien, yhdistäminen ja poistaminen. Lisäksi kyselyjä ja luovutuksia koskevien lokitietojen avulla olisi pystyttävä toteamaan kyseisten toimien perusteet, toteutuspäivä ja -aika sekä mahdollisuuksien mukaan henkilötietoja hakeneen tai niitä luovuttaneen henkilön tiedot ja näiden henkilötietojen vastaanottajien henkilöllisyys. Lisäksi kasvojentunnistusjärjestelmien yhteydessä suositellaan lokitietojen säilyttämistä seuraavista lisäkäsittelytoimista (osittain lainvalvontadirektiivin 25 artiklassa säädettyjen toimien lisäksi):

- Viitetietokannan muutokset (lisääminen, poistaminen tai päivitys). Lokitiedoissa olisi säilytettävä kopio asianomaisesta (lisätystä, poistetusta tai päivitetystä) kuvasta, jos käsittelytoimien lainmukaisuutta tai tuloksia ei voida muutoin tarkistaa.

- Tunnistamis- tai todentamisyritykset, mukaan lukien tulos ja varmuusarvo. Tietojen minimointiperiaatetta olisi sovellettava tiukasti siten, että lokitiedoissa säilytetään vain viitetietokannan kuvan tunniste sen sijaan, että säilytettäisiin itse viitekuva. Lokitietojen säilyttämistä syötetyistä biometrisistä tiedoista olisi vältettävä, ellei se ole välttämätöntä (esimerkiksi vain, jos on löytynyt osuma).

- Tunnistus- tai todentamisyritystä pyytäneen käyttäjän tiedot.

- Kaikkia järjestelmien lokitietoihin tallennettuja henkilötietoja koskevat tiukat käyttötarkoitusrajoitukset (esim. tarkastukset), eikä niitä saa käyttää muihin tarkoituksiin (esim. jotta henkilö voidaan edelleen tunnistaa tai hänen henkilöllisyytensä todentaa hyödyntämällä viitetietokannoista poistettua kuvaa). Lokitietojen eheyden varmistamiseksi olisi toteutettava turvatoimia, ja automaattiset seurantajärjestelmät lokitietojen väärinkäytön havaitsemiseksi ovat erittäin suositeltavia. Viitetietokannan lokitietojen osalta turvatoimien olisi oltava vastaavat kuin viitetietokannassa, kun säilytetään kasvokuvia. Lisäksi olisi toteutettava automaattisia menettelyjä, joilla varmistetaan lokitietojen säilytysajan täytäntöönpano.

3.2.5.6 4 artiklan 4 kohta – tilivelvollisuus

102. Rekisterinpitäjän on voitava osoittaa, että käsittely on lainvalvontadirektiivin 4 artiklan 1–3 kohdan periaatteiden mukaista (ks. lainvalvontadirektiivin 4 artiklan 4 kohta). Järjestelmän järjestelmällinen ja ajantasainen dokumentointi (mukaan lukien päivitykset, parannukset ja algoritminen koulutus), tekniset ja organisatoriset toimenpiteet (mukaan lukien järjestelmän suorituskyvyn seuranta ja mahdollinen luonnollisen henkilön osallistuminen käsittelyyn) ja henkilötietojen käsittely ovat tässä suhteessa ratkaisevan tärkeitä. Käsittelyn lainmukaisuuden osoittamiseksi lainvalvontadirektiivin 25 artiklan mukainen lokitietojen säilyttäminen (ks. kohta 3.2.5.5) on erityisen tärkeää. Tilivelvollisuuden periaate ei koske ainoastaan järjestelmää ja henkilötietojen käsittelyä vaan myös menettelyihin liittyvien suojatoimien dokumentointia, kuten tarpeellisuutta ja oikeasuhteisuutta koskevia arviointeja, tietosuojaa koskevia vaikutustenarviointeja, sisäisiä kuulemisia (esim. johdon hyväksyntä hankkeelle tai sisäiset päätökset varmuusarvoista) ja ulkoisia kuulemisia (esim. tietosuojaviranomainen). Liitteessä II on useita tähän liittyviä näkökohtia.

3.2.5.7 47 artikla – tehokas valvonta

103. Toimivaltaisten tietosuojaviranomaisten suorittama tehokas valvonta on yksi tärkeimmistä suojatoimista niiden henkilöiden perusoikeuksien ja -vapauksien turvaamiseksi, joihin kasvojentunnistusteknologian käyttö vaikuttaa. Samalla on varmistettava, että jokaisella tietosuojaviranomaisella on tarvittavat henkilöresurssit, tekniset ja taloudelliset resurssit, tilat ja infrastruktuuri, jotta ne voivat hoitaa tehtävänsä ja käyttää toimivaltaansa tehokkaasti[66]. Käytettävissä olevan henkilöstön määrääkin tärkeämpiä ovat asiantuntijoiden taidot, joiden olisi katettava laajasti eri kysymyksiä rikostutkinnasta ja poliisiyhteistyöstä massadata-analytiikkaan ja tekoälyyn. Sen vuoksi jäsenvaltioiden olisi varmistettava, että valvontaviranomaisten resurssit ovat asianmukaiset ja riittävät, jotta ne voivat täyttää rekisteröityjen oikeuksien suojelemista ja kaiken tätä koskevan kehityksen tiivistä seuraamista koskevat velvollisuutensa.[67]

4 PÄÄTELMÄT

104. Kasvojentunnistusteknologian käyttöön liittyy erottamattomasti suuren henkilötietomäärän, myös erityisiin tietoryhmiin kuuluvien tietojen, käsittely. Kasvot ja yleisemmin biometriset tiedot liittyvät pysyvästi ja peruuttamattomasti henkilön henkilöllisyyteen. Kasvojentunnistuksen käytöllä on näin ollen suora tai välillinen vaikutus moniin EU:n perusoikeuskirjassa vahvistettuihin perusoikeuksiin ja -vapauksiin, jotka voivat ulottua yksityisyyden suojaa ja tietosuojaa pidemmälle, kuten esimerkiksi ihmisarvoon, liikkumisvapauteen ja kokoontumisvapauteen. Tämä on erityisen tärkeää lainvalvonnan ja rikosoikeuden alalla.

105. Euroopan tietosuojaneuvosto ymmärtää, että lainvalvontaviranomaisilla on oltava käytettävissään parhaat mahdolliset välineet, jotta ne pystyvät tunnistamaan nopeasti terroritekojen ja muiden vakavien rikosten tekijät. Tällaisia välineitä olisi kuitenkin käytettävä tarkkaan sovellettavan oikeuskehyksen mukaisesti ja vain tapauksissa, joissa ne täyttävät tarpeellisuus- ja oikeasuhteisuusvaatimukset, kuten perusoikeuskirjan 52 artiklan 1 kohdassa määrätään. Vaikka nykyaikaiset teknologiat voivat olla osa ratkaisua, ne eivät kuitenkaan suinkaan ole ”ihmelääke”.

106. Tietyt kasvojentunnistusteknologian käyttötapaukset aiheuttavat kohtuuttoman suuria riskejä yksilöille ja yhteiskunnalle (”rajat, joita ei ylitetä”). Näistä syistä Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu ovat vaatineet niiden kieltämistä yleisesti[68].

107. Erityisesti yksilöiden biometrinen etätunnistaminen julkisissa tiloissa aiheuttaa korkean riskin yksilöiden yksityiselämään tunkeutumisesta, eikä sille ole sijaa demokraattisessa yhteiskunnassa, koska se on luonteeltaan joukkovalvontaa. Samalla tavoin Euroopan tietosuojaneuvosto katsoo, että tekoälypohjaiset kasvojentunnistusjärjestelmät, jotka luokittelevat yksilöt heidän biometristen tietojensa perusteella ryhmiin etnisen alkuperän, sukupuolen sekä poliittisen tai seksuaalisen suuntautumisen mukaan, eivät ole perusoikeuskirjan mukaisia. Euroopan tietosuojaneuvosto on lisäksi vakuuttunut siitä, että kasvojentunnistuksen tai vastaavien tekniikoiden käyttö luonnollisen henkilön tunteiden päättelemiseksi on erittäin epätoivottavaa ja se olisi kiellettävä, mahdollisesti muutamaa

[66] Ks. komission tiedonanto ”Ensimmäinen kertomus lainvalvontatarkoituksessa käsiteltyjen henkilötietojen suojaa koskevan direktiivin (EU) 2016/680 soveltamisesta ja toimivuudesta”, COM(2022) 364 final, kohta 3.4.1.

[67] Ks. ”Contribution of the EDPB to the European Commission’s evaluation of the Data Protection Law Enforcement Directive (LED) under Article 62”, kohta 14, , https://edpb.europa.eu/system/files/2021-12/edpb_contribution_led_review_en.pdf

[68] Ks. Euroopan tietosuojaneuvoston ja Euroopan tietosuojavaltuutetun yhteinen lausunto 5/2021 ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi tekoälyä koskevista yhdenmukaistetuista säännöistä (tekoälysäädös), https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf

asianmukaisesti perusteltua poikkeusta lukuun ottamatta. Lisäksi Euroopan tietosuojaneuvosto katsoo, että lainvalvonnan yhteydessä toteutettava henkilötietojen käsittely, joka perustuu tietokantaan, joka muodostetaan keräämällä henkilötietoja laajamittaisesti ja ilman valikointia esimerkiksi ”haravoimalla” verkossa saatavilla olevia, erityisesti sosiaalisten verkostojen kautta saataville asetettuja, valokuvia ja kasvokuvia, ei olisi sellaisenaan unionin lainsäädännössä säädetyn ehdottoman välttämättömyyden vaatimuksen mukaista.

5 LIITTEET

Liite I: Tukimalli

Liite II: Käytännön ohjeita lainvalvontaviranomaisten kasvojentunnistushankkeiden hallinnointiin

Liite III: Käytännön esimerkkejä

LIITE I – MALLI TAPAUSTEN KUVAUSTA VARTEN

(Sisältää tietoruutuja tapauksessa käsiteltyjä näkökohtia varten)

Henkilötietojen käsittelyn kuvaus:

- Henkilötietojen käsittelyn kuvaus, asiayhteys (rikossuhde), tarkoitus

Tietolähde:

- Rekisteröityjen tyypit: ☐ kaikki kansalaiset ☐ tuomitut ☐ epäillyt ☐ lapset ☐ muut haavoittuvassa asemassa olevat rekisteröidyt
- Kuvan lähde: ☐ julkiset tilat ☐ internet ☐ yksityinen yhteisö ☐ muut yksityishenkilöt ☐ muu .....
- Yhteys rikokseen: ☐ Suora ajallinen yhteys ☐ , ei suoraa ajallista yhteyttä ☐ Suora maantieteellinen yhteys☐ , ei suoraa maantieteellistä yhteyttä

  ☐ Ei ole tarpeen
- Tietojen keräystapa: ☐ etäyhteys ☐ , koppi tai valvottu ympäristö
- Asiayhteys – vaikuttaa muihin perusoikeuksiin:

  ☐ ei

  kyllä, mihin: ☐ kokoontumisvapauteen

  ☐ sananvapauteen

  ☐ useisiin:.....
- Rekisteröityä koskevien tietojen muut mahdolliset lähteet:

  ☐ henkilöllisyystodistus ☐ julkisen puhelimen käyttö

  ☐ ajoneuvon rekisterikilpi

  ☐ muu .....

Viitetietokanta (johon kerättyjä tietoja verrataan):

- Spesifisyys: ☐ yleiset tietokannat ☐ rikosalueeseen liittyvät erityistietokannat
- Kuvaus siitä, miten nämä viitetietokannat on koottu (ja oikeusperusta)
- Tietokannan tarkoituksen muuttaminen (esim. ensisijainen tavoite oli yksityisomaisuuden turvaaminen): ☐ KYLLÄ

  ☐ EI

Algoritmi:

- Käsittelytyyppi: ☐ yksi-yhteen-todentaminen ☐ yksi-moneen-tunnistaminen
- Tarkkuutta koskevat näkökohdat
- Tekniset suojatoimet

Tulos:

- Vaikutus ☐ suora (esim. rekisteröity voidaan pidättää, häntä voidaan kuulustella, diskriminoiva kohtelu)
  ☐ ei suora (käytetään tilastollisiin malleihin, ei vakavia oikeustoimia rekisteröityjä vastaan)
- Automaattinen päätös: ☐ KYLLÄ ☐ EI
- Säilytyksen kesto

Oikeudellinen arviointi:

- Tarpeellisuuden ja oikeasuhteisuuden arviointi – tarkoitus / rikoksen vakavuus / niiden henkilöiden määrä, jotka eivät ole osallisina mutta joihin käsittely vaikuttaa
- Miten rekisteröidylle tiedotetaan asiasta ennakkoon: ☐ saavuttaessa tietylle alueelle
  ☐ yleisesti lainvalvontaviranomaisen verkkosivustolla
  ☐ tietyn käsittelyn osalta lainvalvontaviranomaisen verkkosivustolla
  ☐ muu .....
- Sovellettava oikeuskehys:
  ☐ lainvalvontadirektiivi kansalliseen lainsäädäntöön pääosin kopioituna
  ☐ lainvalvontaviranomaisten suorittamaa biometristen tietojen käyttöä koskeva yleinen kansallinen lainsäädäntö
  ☐ kyseistä käsittelyä (kasvojentunnistus) koskeva kansallinen erityislainsäädäntö kyseisen toimivaltaisen viranomaisen osalta
  ☐ kyseistä käsittelyä (automaattinen päätös) koskeva kansallinen erityislainsäädäntö

PÄÄTELMÄT:

Yleisiä huomioita siitä, onko kuvattu käsittely todennäköisesti EU:n lainsäädännön mukaista (ja joitakin viittauksia oikeudellisiin edellytyksiin)

LIITE II – KÄYTÄNNÖN OHJEITA LAINVALVONTAVIRANOMAISTEN KASVOJENTUNNISTUSHANKKEIDEN HALLINNOINTIIN

Tässä liitteessä annetaan joitakin käytännön lisäohjeita lainvalvontaviranomaisille, jotka aikovat käynnistää hankkeen, johon liittyy kasvojentunnistusteknologiaa. Liitteessä annetaan lisätietoa organisatorisista ja teknisistä toimenpiteistä, jotka on otettava huomioon hankkeen aloituksen aikana. Liitettä ei pidä katsoa tyhjentäväksi luetteloksi toteutettavista toimista/toimenpiteistä. Sitä olisi myös tarkasteltava yhdessä Euroopan tietosuojaneuvoston henkilötietojen käsittelyä videolaitteilla koskevien ohjeiden 3/2019[69] sekä kaikkien tekoälyn käyttöön liittyvien EU:n ja ETA:n asetusten ja Euroopan tietosuojaneuvoston ohjeiden kanssa.

Tämän liitteen ohjeet perustuvat oletukseen, että lainvalvontaviranomaiset hankkivat kasvojentunnistusteknologiaa (käyttövalmiina tuotteina). Jos lainvalvontaviranomainen aikoo kehittää (kouluttaa edelleen) kasvojentunnistusteknologiaa, kehittämisen aikana käytettävien tarvittavien koulutus-, validointi- ja testausdatajoukkojen sekä kehitysympäristöä koskevien tehtävien ja toimenpiteiden valintaan sovelletaan lisävaatimuksia. Samoin käyttövalmis tuote voi edellyttää lisämukautuksia aiottua käyttötarkoitusta varten, missä tapauksessa edellä mainitut testaus-, validointi- ja koulutusdatajoukkojen valintaa koskevat vaatimukset on täytettävä.

Samaan lainvalvontaviranomaiseen kuuluminen ei yksinään anna täyttä pääsyä biometrisiin tietoihin. Kuten muidenkin henkilötietoryhmien osalta, tiettyä lainvalvontatarkoitusta varten tietyn oikeusperustan nojalla kerättyjä biometrisiä tietoja ei voida käyttää ilman asianmukaista oikeusperustaa eri lainvalvontatarkoituksiin (direktiivin (EU) 2016/680 (lainvalvontadirektiivi) 4 artiklan 2 kohta). Myös kasvojentunnistustyökalun kehittäminen tai kouluttaminen katsotaan eri tarkoitukseksi, ja olisi arvioitava, onko biometristen tietojen käsittely suorituskyvyn mittaamista tai teknologian kouluttamista varten, jotta alhaisen suorituskyvyn aiheuttamia rekisteröityihin kohdistuvia vaikutuksia voidaan välttää, tarpeellista ja oikeasuhteista käsittelyn alkuperäinen tarkoitus huomioon ottaen.

1. TEHTÄVÄT JA VASTUUALUEET

Kun lainvalvontaviranomainen käyttää kasvojentunnistusteknologiaa lainvalvontadirektiivin soveltamisalaan kuuluvien tehtäviensä suorittamiseen (muun muassa rikosten ennalta estäminen, tutkiminen, paljastaminen tai rikoksiin liittyvät syytetoimet lainvalvontadirektiivin 3 artiklan mukaisesti), sitä voidaan pitää kasvojentunnistusteknologian rekisterinpitäjänä. Lainvalvontaviranomaiset koostuvat kuitenkin useista yksiköistä tai osastoista, jotka voivat osallistua tähän käsittelyyn joko määrittelemällä kasvojentunnistusteknologian käyttöprosessin tai käyttämällä sitä käytännössä. Tämän teknologian erityispiirteiden vuoksi voi olla tarpeen ottaa mukaan eri yksiköitä joko tukemaan sen suorituskyvyn mittaamista tai kouluttamaan sitä edelleen.

Lainvalvontaviranomaisilla on useita sidosryhmiä[70], jotka voi olla tarpeellista ottaa mukaan hankkeisiin, joihin liittyy kasvojentunnistusteknologiaa:

[69] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en.

[70] Seuraavat tehtävät kuvaavat eri sidosryhmiä ja niiden vastuualueita kasvojentunnistushankkeessa. Tässä liitteessä tehtävien kuvaamiseen käytetyt ilmaukset eivät ole ehdottomia, ja kunkin lainvalvontaviranomaisen on

- Ylin johto – hyväksyy hankkeen sen jälkeen, kun riskit on suhteutettu mahdollisiin hyötyihin.
- Lainvalvontaviranomaisen oikeudellinen yksikkö ja/tai tietosuojavastaava – avustaa tietyn kasvojentunnistushankkeen täytäntöönpanon lainmukaisuuden arvioinnissa ja tietosuojaa koskevan vaikutustenarvioinnin toteuttamisessa sekä varmistaa, että rekisteröityjen oikeuksia kunnioitetaan ja käytetään.
- Prosessin omistaja – toimii toimivaltaisen lainvalvontaviranomaisen erityisyksikkönä hankkeen kehittämiseksi, päättää kasvojentunnistusteknologiahankkeen yksityiskohdista, mukaan lukien järjestelmän suorituskykyvaatimukset, päättää asianmukaisesta oikeudenmukaisuusmittarista, määrittää varmuusarvon[71], asettaa hyväksyttävät raja-arvot vinoutumille, tunnistaa mahdolliset riskit, joita kasvojentunnistushanke aiheuttaa yksilöiden oikeuksille ja vapauksille (kuulemalla myös tietosuojavastaavaa ja tietoteknistä tekoäly- ja/tai datatiedeosastoa (ks. jäljempänä), ja esittelee ne ylimmälle johdolle. Prosessin omistaja kuulee myös viitetietokannan hallinnoijaa ennen kuin tekee päätöksen kasvojentunnistushankkeen yksityiskohdista saadakseen käsityksen sekä viitetietokannan käyttötarkoituksesta että sen teknisistä yksityiskohdista. Jos hankittu kasvojentunnistusteknologia koulutetaan uudelleen, prosessin omistaja vastaa myös koulutusdatajoukon valinnasta. Koska prosessin omistaja on yksikkö, jonka tehtävänä on kehittää ja päättää hankkeen yksityiskohdat, se vastaa tietosuojaa koskevan vaikutustenarvioinnin toteuttamisesta.
- Tietotekninen tekoäly- ja/tai datatiedeosasto – avustaa tietosuojaa koskevan vaikutustenarvioinnin toteuttamisessa, selittää järjestelmän suorituskyvyn, oikeudenmukaisuuden[72] ja mahdollisten vinoutumien mittaamiseen käytettävissä olevat mittarit ja ottaa käyttöön teknologian ja tekniset suojatoimet, joilla estetään luvaton pääsy kerättyihin tietoihin, kyberhyökkäykset yms. Jos hankittua kasvojentunnistusteknologiaa koulutetaan uudelleen, tietotekninen tekoäly- tai datatiedeosasto kouluttaa järjestelmän prosessin omistajan toimittaman koulutusdatajoukon pohjalta. Tämä osasto vastaa myös sellaisten toimenpiteiden käynnistämisestä, joilla hillitään prosessin omistajien yhdessä tunnistamia riskejä (esim. tekoälykohtaiset riskit, kuten mallin päättelyhyökkäykset).
- Loppukäyttäjät (kuten poliisivirkamiehet kentällä tai rikosteknisissä laboratorioissa) – suorittavat vertailun tietokantaan, tarkastavat tulokset kriittisesti ottaen huomioon aiemmat todisteet ja antavat palautetta prosessin omistajalle väärien positiivisten tulosten ja mahdollisen syrjinnän merkkien osalta.
- Viitetietokannan hallinnoija – toimivaltaisen lainvalvontaviranomaisen erityisyksikkö, joka vastaa viitetietokannan eli tietokannan, johon kuvia verrataan, kokoamisesta ja hallinnoinnista, mukaan lukien kasvokuvien poistaminen määritetyn säilytysajan jälkeen. Tällainen tietokanta voidaan luoda erityisesti suunniteltua kasvojentunnistushanketta varten tai se voi olla olemassa jo entuudestaan yhteensopivia tarkoituksia varten. Viitetietokannan hallinnoija vastaa sen määrittämisestä, milloin ja missä tilanteissa kasvokuvia voidaan tallentaa, sekä niiden tietojen säilyttämistä koskevien vaatimusten määrittämisestä (ajan tai muiden kriteerien mukaisesti).

määriteltävä ja jaettava vastaavat tehtävät oman organisaationsa mukaisesti. Voi olla, että yksikköön kertyy useampi kuin yksi rooli, esimerkiksi prosessin omistaja ja viitetietokannan hallinnoija tai prosessin omistaja ja tietotekninen tekoäly- ja/tai datatiedeosasto (jos prosessin omistajan yksikössä on kaikki tarvittava tekninen tietämys).

[71] Varmuusarvo on ennusteen (osuman) varmuustaso todennäköisyyden muodossa. Esimerkiksi vertaamalla kahta mallia voidaan 90 prosentin varmuudella todeta, että ne kuuluvat samalle henkilölle. Varmuusarvo on eri asia kuin kasvojentunnistusteknologian suorituskyky, mutta varmuusarvo vaikuttaa suorituskykyyn. Mitä korkeampi varmuutta koskeva kynnysarvo on, sitä vähemmän vääriä positiivisia ja enemmän vääriä negatiivisia tuloksia kasvojentunnistusteknologian tuloksissa on.

[72] Oikeudenmukaisuus voidaan määritellä epäoikeudenmukaisen, laittoman syrjinnän, kuten sukupuoleen tai rotuun perustuvan eriarvoisen kohtelun, puuttumiseksi.

Koska useimmissa tapauksissa kasvojentunnistusteknologian käyttöönottoon ja käyttöön liittyy luontaisesti korkea riski rekisteröityjen oikeuksien ja vapauksien kannalta, tietosuojaviranomaisen olisi myös osallistuttava lainvalvontadirektiivin 28 artiklassa edellytettyyn ennakkokuulemiseen.

2. ALKUVAIHE / ENNEN KASVOJENTUNNISTUSJÄRJESTELMÄN HANKINTAA

Lainvalvontaviranomaisen prosessin omistajalla olisi ensin oltava selkeä käsitys prosessista tai prosesseista kasvojentunnistusteknologian käyttämiseksi (käyttötapaus/-tapaukset), ja hänen olisi varmistettava, että suunnitellulle käyttötapaukselle on oikeusperusta. Tämän perusteella on toteutettava seuraavat toimet:

- Käyttötapauksen virallinen kuvaus. On kuvattava ratkaistava ongelma ja se, miten kasvojentunnistusteknologia tarjoaa siihen ratkaisun, sekä annettava yleiskuvaus prosessista (tehtävästä), jossa sitä käytetään. Tältä osin lainvalvontaviranomaisten olisi dokumentoitava ainakin seuraavat seikat[73]:
  - Prosessissa tallennettujen henkilötietojen ryhmät.
  - Tavoitteet ja konkreettiset tarkoitukset, joihin kasvojentunnistusteknologiaa käytetään, mukaan lukien rekisteröidylle osuman löytymisen jälkeen mahdollisesti aiheutuvat seuraukset.
  - Milloin ja miten kasvokuvat kerätään (mukaan lukien tiedot keruun asiayhteydestä, esimerkiksi lentoaseman portilla, rikoksen tapahtumapaikkana olleen liikkeen ulkopuolella olevien valvontakameroiden videot ja niiden rekisteröityjen ryhmät, joiden biometrisiä tietoja käsitellään).
  - Tietokanta, johon kuvia verrataan (viitetietokanta), sekä tiedot siitä, miten tietokanta on luotu, sen koko ja sen sisältämien biometristen tietojen laatu.
  - Lainvalvontaviranomaisten toimijat, joilla on lupa käyttää kasvojentunnistusjärjestelmää ja toimia sen mukaisesti lainvalvonnan yhteydessä (prosessin omistajan on määriteltävä toimijoiden profiilit ja käyttöoikeudet).
  - Syöttötietojen suunniteltu säilytysaika tai ajankohta, joka määrittää säilytysajan päättymisen (kuten sen rikosoikeudellisen menettelyn päättäminen tai loppuminen kansallisen prosessioikeuden mukaisesti, jota varten tiedot on alun perin kerätty), sekä mahdolliset myöhemmät toimet (kyseisten tietojen poistaminen, anonymisointi ja käyttö tilasto- tai tutkimustarkoituksiin yms.).
  - Lokitietojen säilyttäminen, lokitietojen saatavuus ja säilytettävät tiedot.
  - Suorituskykymittarit (esim. paikkansapitävyys, tarkkuus, saanti, F1-arvo) ja niiden alhaisimmat hyväksyttävät kynnysarvot.[74]

[73] Liitteessä I on luettelo seikoista, jotka auttavat rekisterinpitäjää kuvailemaan kasvojentunnistusteknologian käyttötapauksen.

[74] Kasvojentunnistusjärjestelmien suorituskyvyn arvioimiseksi on olemassa erilaisia mittareita. Kukin mittari antaa erilaisen kuvan järjestelmän tuloksista. Se, onnistuvatko mittarit antamaan riittävän kuvan siitä, onko kasvojentunnistusjärjestelmän suorituskyky hyvä vai ei, riippuu kasvojentunnistusteknologian käyttötapauksesta. Jos tavoitteena on saavuttaa korkea prosenttiosuus kasvo-osumien löytymisessä oikein, voidaan käyttää tarkkuuden ja saannin kaltaisia mittareita. Nämä mittarit eivät kuitenkaan mittaa sitä, miten hyvin kasvojentunnistusteknologia käsittelee negatiivisia esimerkkejä (kuinka moni järjestelmän löytämistä osumista oli virheellisiä). Tietoteknisen tekoäly- ja datatiedeosaston tukeman prosessin omistajan olisi voitava asettaa suorituskykyä koskevat vaatimukset ja ilmaista ne parhaiten soveltuvalla mittarilla kasvojentunnistusteknologian käyttötapauksen mukaan.

- Arvio siitä, kuinka moneen ihmiseen kasvojentunnistusteknologiaa käytetään ja missä ajassa tai tilanteessa.

- Tarpeellisuuden ja oikeasuhteisuuden arviointi[75]. Tämän teknologian olemassaolo ei saisi olla syynä sen käyttämiseen. Prosessin omistajan on ensin arvioitava, onko suunnitellulle tietojenkäsittelylle olemassa asianmukainen oikeusperusta. Tätä varten on kuultava tietosuojavastaavaa ja oikeudellista yksikköä. Kasvojentunnistusteknologian käyttöönoton syynä olisi oltava se, että se on tarpeellinen ja oikeasuhteinen ratkaisu erikseen määriteltyyn lainvalvontaviranomaisten ongelmaan. Tätä on arvioitava tarkoituksen / rikoksen vakavuuden / niiden henkilöiden määrän perusteella, jotka eivät ole osallisina mutta joihin kasvojentunnistusjärjestelmä vaikuttaa. Lainmukaisuuden arvioinnissa olisi otettava huomioon ainakin seuraavat: lainvalvontadirektiivi[76], yleinen tietosuoja-asetus[77] [78], kaikki tekoälyä koskevat voimassa olevat oikeuskehykset[79] ja kaikki tietosuojaviranomaisten tarjoamat ohjeet (kuten Euroopan tietosuojaneuvoston ohjeet 3/2019 henkilötietojen käsittelystä videolaitteilla[80]). Näitä EU:n säädöksiä olisi aina tuettava sovellettavilla kansallisilla vaatimuksilla erityisesti rikosprosessioikeuden alalla. Oikeasuhteisuuden arvioinnissa olisi määritettävä ne rekisteröityjen perusoikeudet, joihin tietojen käsittely voi vaikuttaa (yksityisyyden suojan ja tietosuojan lisäksi). Siinä olisi myös kuvailtava ja otettava huomioon kasvojentunnistusjärjestelmälle käyttötapauksessa asetetut rajoitukset (tai niiden puuttuminen). Esimerkiksi se, toimiiko järjestelmä keskeytyksettä vai väliaikaisesti ja rajoittuuko se johonkin tiettyyn maantieteelliseen alueeseen.
- Tietosuojaa koskeva vaikutustenarviointi[81]. Tietosuojaa koskevaa vaikutustenarviointi olisi tehtävä, koska kasvojentunnistusteknologian käyttöönotto lainvalvonnan alalla voi helposti aiheuttaa korkean riskin yksilöiden oikeuksien ja vapauksien kannalta[82]. Tietosuojaa koskevan vaikutustenarvioinnin olisi sisällettävä erityisesti: yleinen kuvaus suunnitelluista

[75] Järjestelmän räätälöinnin ja käytön osalta voidaan harkita lisätoimenpiteitä tarpeellisuuden varmistamiseksi, joten käyttötapauksen kuvausta voidaan myös hieman muuttaa tarpeellisuuden ja oikeasuhteisuuden arvioinnin aikana.

[76] Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten.

[77] Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta.

[78] Tapauksissa, joissa kasvojentunnistusteknologian käytön tutkimiseen pyrkivässä tieteellisessä hankkeessa on käsiteltävä henkilötietoja mutta tällainen käsittely ei kuulu lainvalvontadirektiivin 4 artiklan 3 kohdan soveltamisalaan, sovelletaan yleensä yleistä tietosuoja-asetusta (lainvalvontadirektiivin 9 artiklan 2 kohta). Lainvalvontadirektiiviä sovelletaan kuitenkin pilottihankkeisiin, joiden jälkeen toteutetaan lainvalvontatoimia.

[79] On esimerkiksi annettu ehdotus Euroopan parlamentin ja neuvoston asetukseksi tekoälyä koskevista yhdenmukaistetuista säännöistä (tekoälysäädös) ja tiettyjen unionin säädösten muuttamisesta, mutta tätä ei ole vielä vahvistettu asetukseksi.

[80] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en.

[81] Lisäohjeita tietosuojaa koskevasta vaikutustenarvioinnista on tietosuojaryhmän ohjeissa tietosuojaa koskevasta vaikutustenarvioinnista ja keinoista selvittää ”liittyykö käsittelyyn todennäköisesti” asetuksessa (EU) 2016/679 tarkoitettu ”korkea riski”, WP248 rev.01., saatavilla osoitteessa https://ec.europa.eu/newsroom/article29/items/611236, ja Euroopan tietosuojavaltuutetun ohjeissa ”Accountability on the ground toolkit, Part II”, saatavilla osoitteessa https://edps.europa.eu/node/4582_en

[82] Kasvojentunnistusteknologia voi kuulua käyttötapauksesta riippuen seuraavien korkean riskin käsittelyn kriteerien piiriin (Ohjeet tietosuojaa koskevasta vaikutustenarvioinnista, WP248 rev.01): järjestelmällinen valvonta, tietojen laajamittainen käsittely, tietokokonaisuuksien sovittaminen yhteen tai yhdistäminen, uusien teknisten tai organisatoristen ratkaisujen innovatiivinen käyttö tai soveltaminen.

tietojenkäsittelytoimista[83], arvio rekisteröityjen oikeuksiin ja vapauksiin kohdistuvista riskeistä[84], suunnitellut toimenpiteet näiden riskien torjumiseksi, suojatoimet, turvatoimet ja mekanismit henkilötietojen suojan varmistamiseksi ja vaatimustenmukaisuuden osoittamiseksi. Tietosuojaa koskeva vaikutustenarviointi on jatkuva prosessi, joten tietojenkäsittelyn kaikki uudet elementit olisi lisättävä siihen ja riskinarviointi päivitettävä hankkeen jokaisessa vaiheessa.

- Ylimmän johdon hyväksynnän hankkiminen selittämällä rekisteröityjen oikeuksiin ja vapauksiin kohdistuvat (käyttötapauksesta ja teknologiasta johtuvat) riskit ja vastaavat riskienhallintasuunnitelmat.

3. HANKINNAN AIKANA JA ENNEN KASVOJENTUNNISTUSTEKNOLOGIAN KÄYTTÖÖNOTTOA

- Kasvojentunnistusteknologian (algoritmin) valintaperusteista päättäminen. Prosessin omistajan olisi päätettävä algoritmin valintaperusteista tietoteknisen tekoäly- ja/tai datatiedeosaston avulla. Käytännössä niihin sisältyisivät käyttötapauksen kuvauksessa määritetyt oikeudenmukaisuus- ja suorituskykymittarit. Näihin perusteisiin olisi sisällyttävä myös tiedot, jotka liittyvät tietoihin, joilla algoritmi on koulutettu. Koulutus-, testaus- ja validointijoukon on sisällettävä riittävästi näytteitä niiden rekisteröityjen kaikista ominaisuuksista, joihin kasvojentunnistusteknologiaa käytetään (ottaen huomioon esimerkiksi ikä, sukupuoli ja rotu), vinoutumien vähentämiseksi. Kasvojentunnistusteknologian tarjoajan olisi annettava kasvojentunnistusteknologian koulutus-, testaus- ja validointidatajoukkoja koskevat tiedot ja mittarit ja kuvattava toimenpiteet, jotka on toteutettu mahdollisen laittoman syrjinnän ja vinoutumien mittaamiseksi ja vähentämiseksi. Prosessin omistajan on mahdollisuuksien mukaan tarkistettava, oliko tarjoajalla oikeusperusta kyseisen datajoukon käyttämiseen algoritmien kouluttamista varten (tarjoajan saataville asettamien tietojen perusteella). Prosessin omistajan olisi myös varmistettava, että kasvojentunnistusteknologian tarjoaja soveltaa biometrisiin tietoihin liittyviä turvallisuusstandardeja, kuten ISO/IEC 24745 -standardia, jossa annetaan ohjeita biometristen tietojen suojaamiseen erilaisilla vaatimuksilla, jotka koskevat salassapitoa, eheyttä ja uusimista/kumoamista säilyttämisen ja siirtämisen aikana, sekä biometristen tietojen turvallista ja yksityisyyttä kunnioittavaa hallinnointia ja käsittelyä koskevia vaatimuksia ja ohjeita.

- Algoritmin uudelleenkouluttaminen (tarvittaessa). Prosessin omistajan olisi varmistettava, että kasvojentunnistusjärjestelmän hienosäätäminen paremman tarkkuuden saavuttamiseksi ennen sen käyttöä on myös osa hankittuja palveluja. Jos hankitun kasvojentunnistusjärjestelmän lisäkoulutus on tarpeen tarkkuustavoitteiden täyttämiseksi, prosessin omistajan on uudelleenkouluttamisesta päättämisen lisäksi päätettävä käytettävästä riittävästä ja edustavasta datajoukosta tietoteknisen tekoäly- ja/tai datatiedeosaston avulla ja tarkistettava tämän tietojen käytön lainmukaisuus.
- Asianmukaisten suojatoimien asettaminen turvallisuuteen, vinoutumiin ja heikkoon suorituskykyyn liittyvien riskien hallitsemiseksi. Tähän sisältyy sellaisen prosessin käyttöönotto, jolla seurataan kasvojentunnistusteknologian käyttöä sen käyttöönoton jälkeen (lokitiedot ja palaute tulosten tarkkuutta ja oikeudenmukaisuutta varten). Lisäksi on varmistettava, että

[83] Käsittelyn kuvaus sekä tarpeellisuuden ja oikeasuhteisuuden arviointi, jotka on jo kuvattu edeltävissä kohdissa, ovat riskinarvioinnin lisäksi osa tietosuojaa koskevaa vaikutustenarviointia. Tarvittaessa tietosuojaa koskevassa vaikutustenarvioinnissa esitetään yksityiskohtaisempi kuvaus henkilötietovirroista.

[84] Rekisteröityihin kohdistuvien riskien arvioinnin olisi sisällettävä riskit, jotka liittyvät vertailtavien kasvokuvien paikkaan (paikallinen/etäyhteys), henkilötietojen käsittelijöihin tai alihankkijoina toimiviin käsittelijöihin liittyvät riskit sekä koneoppimiseen liittyvät riskit sitä sovellettaessa (esim. datamyrkytys, ristiriitaiset esimerkit).

joillekin koneoppimis- ja kasvojentunnistusjärjestelmille ominaiset riskit (esim. datamyrkytys, ristiriitaiset esimerkit, mallin inversio, white box -päättely) määritetään ja että niitä mitataan ja lievennetään. Prosessin omistajan olisi myös asetettava asianmukaisia suojatoimia sen varmistamiseksi, että uudelleenkoulutukseen käytettävään datajoukkoon sisältyvien biometristen tietojen säilyttämisvaatimuksia noudatetaan.

- Kasvojentunnistusjärjestelmän dokumentointi. Tähän olisi sisällyttävä yleinen kuvaus kasvojentunnistusjärjestelmästä, yksityiskohtainen kuvaus kasvojentunnistusjärjestelmän elementeistä ja sen luomisprosessista, yksityiskohtaiset tiedot kasvojentunnistusjärjestelmän seurannasta, toiminnasta ja valvonnasta sekä yksityiskohtainen kuvaus sen riskeistä ja riskienhallintatoimenpiteistä. Tähän dokumentointiin kuuluu edellisissä vaiheissa toteutetun kasvojentunnistusjärjestelmän kuvauksen keskeisiä osia (ks. edellä), mutta niitä täydennetään tiedoilla, jotka liittyvät suorituskyvyn seurantaan ja järjestelmään tehtävien muutosten soveltamiseen, mukaan lukien kaikki mahdolliset versiopäivitykset ja/tai uudelleenkouluttaminen.
- Käyttöoppaiden laatiminen sisältäen teknologiaa ja käyttötapauksia koskevat selitykset. Käyttöoppaissa on selitettävä selkeästi kaikki kasvojentunnistusteknologian käyttötapaukset ja -edellytykset.
- Teknologian käyttöä koskevan koulutuksen antaminen loppukäyttäjille. Tällaisissa koulutuksissa on selitettävä teknologian valmiudet ja rajoitukset, jotta käyttäjät saavat käsityksen tilanteista, joissa sen käyttö on tarpeellista, sekä tapauksista, joissa se voi olla epätarkka. Tällaiset koulutukset auttavat myös vähentämään riskejä, jotka liittyvät siihen, että algoritmin tuloksia ei tarkisteta/kritisoida.
- Tietosuojaviranomaisen kuuleminen lainvalvontadirektiivin 28 artiklan 1 kohdan b alakohdan mukaisesti. Tietojen tarjoaminen lainvalvontadirektiivin 13 artiklan mukaisesti, jotta rekisteröidyt saavat tietoa käsittelystä ja oikeuksistaan. Näissä rekisteröidyille tarkoitetuissa ilmoituksissa on käytettävä asianmukaista kieltä, jotta he pystyvät saamaan käsityksen käsittelystä, ja niissä on selitettävä teknologian peruselementit, mukaan lukien tarkkuusasteet, koulutusdatajoukot ja toteutetut toimenpiteet, joilla pyritään välttämään syrjintää ja algoritmin heikkoa tarkkuutta.

4. SUOSITUKSET KASVOJENTUNNISTUSTEKNOLOGIAN KÄYTTÖÖNOTON JÄLKEEN

- Ihmisen osallistumisen ja tulosten valvonnan varmistaminen. Yksilöä koskevia toimenpiteitä ei tule koskaan toteuttaa pelkästään kasvojentunnistusteknologian tulosten perusteella (tämä merkitsisi lainvalvontadirektiivin 11 artiklan rikkomista, kun automatisoiduilla yksittäispäätöksillä on oikeudellisia tai muita vastaavia vaikutuksia rekisteröityyn). On varmistettava, että lainvalvontaviranomaisen virkamies tarkastaa kasvojentunnistusteknologian tulokset. Lisäksi on varmistettava, että lainvalvontaviranomaisen käyttäjät välttävät automaatioharhaa tutkimalla ristiriitaisia tietoja ja kyseenalaistamalla kriittisesti teknologian tulokset. Tämän vuoksi loppukäyttäjien jatkuva kouluttaminen ja tietoisuuden lisääminen on tärkeää. Ylimmän johdon olisi kuitenkin varmistettava, että käytettävissä on riittävästi henkilöresursseja tehokkaan valvonnan toteuttamiseksi. Tämä edellyttää, että jokaiselle virkamiehelle annetaan riittävästi aikaa kyseenalaistaa kriittisesti teknologian tulokset. Kirjataan, mitataan ja arvioidaan, missä määrin ihmisen suorittama valvonta muuttaa kasvojentunnistusteknologian alkuperäistä päätöstä.
- Kasvojentunnistusteknologian ”mallin muutoksen” (”model drift”, suorituskyvyn heikkeneminen) seuranta ja siihen puuttuminen, kun mallia laaditaan.
- Sellaisen prosessin käyttöönottaminen, jolla riskejä ja turvatoimia arvioidaan uudelleen säännöllisesti ja aina, kun teknologia tai käyttötapaus muuttuu.

- Kaikkien järjestelmään tehtyjen muutosten dokumentointi koko sen elinkaaren ajan (esim. päivitykset, uudelleenkoulutus).
- Rekisteröityjen tietopyyntöjen käsittelemistä koskevan prosessin ja siihen liittyvien teknisten valmiuksien käyttöönottaminen. Tekniset valmiudet tietojen poimimiseen tapauksissa, joissa tiedot on annettava rekisteröidyille, on oltava käytössä ennen kuin yhtään pyyntöä esitetään.
- Sen varmistaminen, että käytössä on menettelyjä tietoturvaloukkauksia varten. Jos tapahtuu henkilötietoja koskeva tietoturvaloukkaus, johon liittyy biometrisiä tietoja, riskit ovat todennäköisesti korkeita. Tässä tapauksessa kaikkien asianomaisten käyttäjien olisi oltava tietoisia noudatettavista menettelyistä, tietosuojavastaavalle olisi ilmoitettava asiasta välittömästi ja rekisteröidyille olisi ilmoitettava asiasta.

LIITE III – KÄYTÄNNÖN ESIMERKKEJÄ

Kasvojentunnistusta voidaan käyttää monissa eri käytännön tilanteissa ja moniin eri tarkoituksiin, kuten valvotuissa ympäristöissä, esimerkiksi rajanylityspaikoilla, vertailussa poliisitietokantojen tietojen tai rekisteröidyn nimenomaisesti julkisiksi saattamien henkilötietojen kanssa tai suorassa kamerakuvassa (reaaliaikainen kasvojentunnistus). Näin ollen henkilötietojen suojaan ja muihin perusoikeuksiin ja -vapauksiin kohdistuvat riskit vaihtelevat huomattavasti eri käyttötapauksissa. Jotta voitaisiin helpottaa tarpeellisuuden ja oikeasuhteisuuden arviointia, joka pitäisi suorittaa ennen päätöstä kasvojentunnistuksen mahdollisesta käyttöönotosta, näissä ohjeissa esitetään luettelo, joka ei ole kaikenkattava, kasvojentunnistusteknologian mahdollisista sovelluksista lainvalvonnan alalla.

Esitetyt ja arvioidut tapaukset perustuvat **hypoteettisiin** tilanteisiin, ja niiden tarkoituksena on havainnollistaa tiettyjä konkreettisia kasvojentunnistusteknologian käyttötarkoituksia, helpottaa tapauskohtaista harkintaa sekä luoda yleinen kehys teknologian käytölle. Tapausten tarkoituksena ei ole olla kaikenkattavia, eivätkä ne vaikuta kansallisen valvontaviranomaisen käynnissä oleviin tai tuleviin menettelyihin, jotka koskevat kasvontunnistusteknologian suunnittelua, kokeilua tai käyttöönottoa. Näiden tapausten esittämisen tarkoituksena on ainoastaan havainnollistaa tässä asiakirjassa jo annettuja, poliittisille päättäjille, lainsäätäjille ja lainvalvontaviranomaisille suunnattuja ohjeita niiden suunnitellessa kasvojentunnistusteknologian käyttöönottoa, jotta voidaan varmistaa, että henkilötietojen suojaa koskevaa EU:n säännöstöä noudatetaan kaikilta osin. Tässä yhteydessä on pidettävä mielessä, että jopa samankaltaisissa tilanteissa, joissa käytetään kasvojentunnistusteknologiaa, tietyt tekijät tai niiden puuttuminen voivat johtaa erilaiseen tulokseen tarpeellisuuden ja oikeasuhteisuuden arvioinnissa.

1 TAPAUS 1

1.1. Kuvaus

Automaattinen rajavalvontajärjestelmä, joka mahdollistaa automaattisen rajanylityksen todentamalla EU:n kansalaisten ja muiden rajaa ylittävien matkustajien sähköiseen matkustusasiakirjaan tallennetun biometrisen kuvan ja toteamalla, että matkustaja on asiakirjan laillinen haltija.

Tällainen todentaminen käsittää vain yksi-yhteen-kasvojentunnistamista, ja se suoritetaan valvotussa ympäristössä (esim. lentoaseman automaattiporteilla). Rajaa ylittävän matkustajan biometriset tiedot kerätään, kun häntä nimenomaisesti kehotetaan katsomaan automaattiportin kameraan, ja niitä verrataan esitetyn, erityisten teknisten vaatimusten mukaisesti myönnetyn asiakirjan (passi, henkilökortti tms.) biometrisiin tietoihin.

Vaikka tällaisissa tapauksissa käsittely ei periaatteessa kuulu lainvalvontadirektiivin soveltamisalaan, todentamisen tulosta voidaan käyttää myös henkilön (aakkosnumeeristen) tietojen vertaamiseen lainvalvontatietokantoihin osana rajavalvontaa, ja se voi siten johtaa toimiin, joilla on rekisteröidyn kannalta merkittäviä oikeudellisia vaikutuksia, kuten pidättäminen SIS-järjestelmään tehdyn kuulutuksen perusteella. Erityistilanteissa biometrisiä tietoja voidaan käyttää myös osumien etsimiseen lainvalvontatietokannoista (jolloin tässä vaiheessa suoritettaisiin yksi-moneen-tunnistaminen).

Biometrisen kuvan käsittelyn tuloksella on suora vaikutus rekisteröityyn: ainoastaan todentamisen onnistuminen mahdollistaa rajanylityksen. Jos tunnistaminen ei onnistu, rajavartijoiden on suoritettava toinen tarkastus varmistaakseen, että rekisteröity on eri henkilö kuin henkilöllisyystodistuksessa kuvattu.

Jos havaitaan SIS-kuulutus tai kansallinen kuulutus, rajavartijoiden on suoritettava toinen todentaminen ja tarvittavat lisätarkastukset ja ryhdyttävä sen jälkeen tarvittaviin toimenpiteisiin, esimerkiksi pidätettävä henkilö ja ilmoitettava asiasta asianomaisille viranomaisille.

Tietolähde:
- Rekisteröityjen tyypit: ☒ kaikki rajoja ylittävät henkilöt
- Kuvan lähde: ☒ muu (henkilöllisyystodistus)
- Yhteys rikokseen: ☒ ei ole tarpeen
- Tietojen keräystapa: ☒ koppi tai valvottu ympäristö
- Asiayhteys – vaikuttaa muihin perusoikeuksiin: Kyllä, mihin: ☒ oikeus vapaaseen liikkuvuuteen ☒ oikeus turvapaikkaan

Viitetietokanta (johon kerättyjä tietoja verrataan):
- Spesifisyys: ☒ erityiset rajavalvontaan liittyvät tietokannat

Algoritmi:
- Todentamisen tyyppi: ☒ yksi-yhteen-todentaminen

Tulos:
- Vaikutus: ☒ suora (rekisteröidyn pääsy sallitaan tai evätään)
- Automaattinen päätös: ☒ kyllä

1.2. Sovellettava oikeuskehys

Vuodesta 2004 lähtien jäsenvaltioiden myöntämissä passeissa ja muissa matkustusasiakirjoissa on neuvoston asetuksen (EY) N:o 2252/2004[85] mukaisesti oltava biometrinen kasvokuva, joka on tallennettu asiakirjaan upotettuun elektroniseen siruun.

Schengenin rajasäännöstössä[86] säädetään ulkorajoilla tehtäviä henkilötarkastuksia koskevista vaatimuksista. EU:n kansalaisten ja muiden henkilöiden, joilla on oikeus vapaaseen liikkuvuuteen unionin lainsäädännön nojalla, vähimmäistarkastusten olisi koostuttava heidän matkustusasiakirjojensa tarkistamisesta tarvittaessa teknisten laitteiden avulla. Schengenin rajasäännöstöä on sittemmin muutettu asetuksella (EU) 2017/2225[87], jossa on otettu käyttöön muun muassa ”automaattiporttien”, ”automaattisen rajatarkastusjärjestelmän” ja ”itsepalvelujärjestelmän” määritelmät sekä mahdollisuus käsitellä biometrisiä tietoja rajatarkastusten suorittamista varten.

Näin ollen voitaisiin olettaa, että on olemassa selkeä ja ennakoitavissa oleva oikeusperusta, joka oikeuttaa tämäntyyppisen henkilötietojen käsittelyn. Lisäksi oikeuskehys on hyväksytty unionin tasolla, ja sitä sovelletaan suoraan jäsenvaltioihin.

1.3. Tarpeellisuus ja oikeasuhteisuus – tarkoitus / rikoksen vakavuus

EU:n kansalaisten henkilöllisyyden todentaminen automaattisessa rajavalvonnassa heidän biometrisen kuvansa avulla on osa EU:n ulkorajoilla tehtäviä rajatarkastuksia. Näin ollen se liittyy suoraan rajaturvallisuuteen ja palvelee unionin tunnustamaa yleistä etua koskevaa tavoitetta. Lisäksi rajatarkastusautomaatit nopeuttavat matkustajien käsittelyä ja vähentävät inhimillisten virheiden riskiä. Lisäksi tässä tapauksessa oikeuksiin puuttumisen laajuus, määrä ja intensiteetti ovat paljon vähäisempiä verrattuna muihin kasvojentunnistuksen muotoihin. Biometristen tietojen käsittely

[85] Neuvoston asetus (EY) N:o 2252/2004, annettu 13 päivänä joulukuuta 2004, jäsenvaltioiden myöntämien passien ja matkustusasiakirjojen turvatekijöitä ja biometriikkaa koskevista vaatimuksista.
[86] Euroopan parlamentin ja neuvoston asetus (EU) 2016/399, annettu 9 päivänä maaliskuuta 2016, henkilöiden liikkumista rajojen yli koskevasta yhteisön säännöstöstä (Schengenin rajasäännöstö).
[87] Euroopan parlamentin ja neuvoston asetus (EU) 2017/2225, annettu 30 päivänä marraskuuta 2017, asetuksen (EU) 2016/399 muuttamisesta rajanylitystietojärjestelmän käytön osalta.

aiheuttaa kuitenkin rekisteröidyille lisäriskejä, joihin kasvojentunnistusteknologiaa käyttöönottavan ja käyttävän toimivaltaisen viranomaisen on puututtava ja joita sen on lievennettävä asianmukaisesti.

1.4. Päätelmät

EU:n kansalaisten henkilöllisyyden todentaminen automaattisen rajavalvonnan yhteydessä on tarpeellinen ja oikeasuhteinen toimenpide, kunhan käytössä on asianmukaisia suojatoimia, erityisesti käyttötarkoituksen rajoittamisen, tietojen laadun, avoimuuden ja korkean turvallisuustason periaatteiden soveltaminen.

2 TAPAUS 2

2.1. Kuvaus

Lainvalvontaviranomaiset perustavat järjestelmän lapsikaappausten uhrien tunnistamiseksi. Valtuutettu poliisivirkamies voi tiukoin edellytyksin verrata siepatuksi epäillyn lapsen biometrisiä tietoja lapsikaappauksen uhreja koskevaan tietokantaan yksinomaan sellaisten alaikäisten tunnistamiseksi, jotka saattavat vastata sellaisen kadonneen lapsen kuvausta, jota koskien on aloitettu tutkinta ja josta on tehty kuulutus.

Kyseessä oleva käsittely olisi kadonneen lapsen kuvausta mahdollisesti vastaavan henkilön kasvojen tai kuvan vertaamista tietokantaan tallennettuihin kuviin. Tällainen käsittely suoritettaisiin erityistapauksissa eikä järjestelmällisesti.

Tietokanta, johon vertailu tehdään, kootaan sellaisten kadonneiden lasten kuvista, joiden osalta on ilmoitettu epäillystä lapsikaappauksesta, lapsen henkeä tai fyysistä koskemattomuutta uhkaavasta vaarasta, ja aloitettu rikostutkinta oikeusviranomaisen alaisuudessa ja joista on tehty lapsikaappausta koskeva kuulutus. Tietoja kerätään toimivaltaisen lainvalvontaviranomaisen eli poliisivirkamiesten, joilla on valtuudet suorittaa oikeudellisia poliisioperaatioita, vahvistamien menettelyjen puitteissa. Tallennettujen henkilötietojen ryhmät ovat seuraavat:

- henkilöllisyys, kutsumanimi, peitenimi, sukunimi, kansalaisuus, osoitteet, sähköpostiosoitteet, puhelinnumerot
- syntymäaika ja -paikka
- vanhempia koskevat tiedot
- valokuva, jonka tekniset ominaisuudet mahdollistavat kasvojentunnistuslaitteen käytön, ja muut valokuvat.

Valtuutetun virkamiehen on myös tarkistettava ja vahvistettava vertailun tulokset, jotta vertailun tuloksilla voidaan täydentää aiempia todisteita ja jotta voidaan sulkea pois mahdolliset väärät positiiviset tulokset.

Lasten kuvia ja henkilötietoja voidaan säilyttää vain kuulutuksen keston ajan, ja ne on poistettava välittömästi sen jälkeen, kun rikosoikeudellinen menettely, jota varten ne on tallennettu tietokantaan, on päättynyt tai lopetettu kansallisten menettelyjen mukaisesti.

Vaikka tietokannassa olevien biometristen tietojen säilytysaika voidaan määritellä suhteellisen pitkäksi kansallisen lainsäädännön mukaisesti, rekisteröidyn oikeuksien, erityisesti tietojen oikaisemista ja poistamista koskevan oikeuden, käyttäminen tarjoaa lisätakuun, joka rajoittaa puuttumista asianomaisten rekisteröityjen henkilötietojen suojaa koskevaan oikeuteen.

Tietolähde:

- Rekisteröityjen tyypit: ☒ lapset
- Kuvan lähde ☒ muu: ei ennalta määritelty, epäilty lapsikaappauksen uhri
- Yhteys rikokseen ☒ ei suoraa ajallista yhteyttä ☒ ei suoraa maantieteellistä yhteyttä
- Tietojen keräystapa: ☒ koppi tai valvottu ympäristö
- Asiayhteys: vaikuttaa muihin perusoikeuksiin ☒ kyllä, mihin: ☒ useisiin

Viitetietokanta (johon kerättyjä tietoja verrataan):

- Spesifisyys ☒ erityistietokanta

Algoritmi:

- Todentamisen tyyppi: ☒ yksi-moneen-tunnistaminen

Tulos:

- Vaikutus ☒ suora
- Automaattinen päätös: ☒ EI, valtuutetun virkamiehen suorittama pakollinen tarkistus

Oikeudellinen arviointi:

- Sovellettava oikeuskehys: ☒ tätä käsittelyä (kasvojentunnistus) koskeva kansallinen erityislainsäädäntö

2.2. Sovellettava oikeuskehys

Kansallisessa lainsäädännössä säädetään erityisestä oikeuskehyksestä, jolla tietokanta perustetaan ja jolla määritetään käsittelyn tarkoitukset sekä kriteerit, joiden perusteella tietokantaan voidaan kerätä tietoja, siihen voidaan saada pääsy ja sitä voidaan käyttää. Sen täytäntöönpanon edellyttämissä lainsäädäntötoimenpiteissä säädetään myös säilytysajan määrittämisestä ja viitataan sovellettaviin eheyden ja luottamuksellisuuden periaatteisiin. Lainsäädäntötoimenpiteissä säädetään myös menettelyistä tietojen toimittamiseksi rekisteröidylle ja tässä tapauksessa vanhempainvastuunkantajalle tai -kantajille sekä rekisteröityjen oikeuksien käyttämisestä ja tarvittaessa mahdollisista rajoituksista. Lainsäädäntötoimenpidettä koskevan ehdotuksen valmistelun aikana oli kuultava kansallista valvontaviranomaista.

2.3. Tarpeellisuus ja oikeasuhteisuus – tarkoitus / rikoksen vakavuus / niiden henkilöiden määrä, jotka eivät ole osallisina mutta joihin käsittely vaikuttaa

Käsittelyn edellytykset ja suojatoimet

Valtuutettu virkamies voi suorittaa kasvojentunnistusvertailun ainoastaan viimeisenä keinona, ellei muita, oikeuksiin vähemmän puuttuvia keinoja ole käytettävissä ja jos se on ehdottoman välttämätöntä, esimerkiksi jos matkustavan alaikäisen henkilöllisyystodistuksen aitoudesta on epäilyjä ja/tai kun on tarkasteltu aiemmin kerättyjä todisteita ja aineistoa, jotka viittaavat mahdolliseen vastaavuuteen rikostutkinnan kohteena olevan kadonneen lapsen kuvauksen kanssa.

Käytössä on myös lisäsuojatoimi, eli pakollinen valtuutetun virkamiehen suorittama kasvojentunnistusvertailun tarkistaminen ja varmentaminen, jotta vertailun tuloksella voidaan tukea aiempia todisteita ja jotta voidaan sulkea pois mahdolliset väärät positiiviset tulokset.

Tavoite

Tietokannan perustaminen palvelee tärkeitä yleisen edun mukaisia tavoitteita, erityisesti rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa ja muiden henkilöiden oikeuksien ja vapauksien suojaamista. Tietokannan perustaminen ja suunniteltu henkilötietojen käsittely näyttää edistävän sieppauksen uhriksi joutuneiden lasten tunnistamista, ja sen vuoksi sitä voidaan pitää toimenpiteenä, jolla voidaan tukea laillista tavoitetta tutkia tällaisia rikoksia ja nostaa niistä syytteitä.

Tietokannan tarkoitus ja kokoaminen

Henkilötietojen käsittelyn tarkoitukset on määritelty selkeästi laissa, ja tietokantaa saa käyttää ainoastaan sellaisten kadonneiden lasten tunnistamiseen, joiden osalta on ilmoitettu epäillystä lapsikaappauksesta ja käynnistetty rikostutkinta oikeusviranomaisen valvonnassa ja joista on tehty lapsikaappausta koskeva kuulutus. Laissa säädetyillä tietokannan kokoamisen edellytyksillä pyritään rajoittamaan tiukasti tietokantaan sisällytettävien rekisteröityjen ja henkilötietojen määrää. Lapsen vanhempainvastuunkantajalle on ilmoitettava suoritetusta käsittelystä ja lapsen oikeuksien käyttämisen edellytyksistä tunnistustarkoitusta varten suoritettavan biometrisen käsittelyn tai tietokantaan tallennettujen lapsen henkilötietojen suhteen.

2.4. Päätelmät

Kun otetaan huomioon suunnitellun käsittelyn tarpeellisuus ja oikeasuhteisuus sekä lapsen etu suoritettaessa tällaista henkilötietojen käsittelyä ja edellyttäen, että on olemassa riittävät takeet rekisteröidyn oikeuksien käytön varmistamiseksi, etenkin, kun otetaan huomioon, että käsittely koskee lasten tietoja, voidaan katsoa, että tällainen kasvojentunnistuskäsittely on todennäköisesti EU:n lainsäädännön mukaista.

Kun lisäksi otetaan huomioon käsittelyn tyyppi ja käytetty teknologia, johon liittyy korkea riski kyseessä olevan rekisteröidyn oikeuksien ja vapauksien kannalta, Euroopan tietosuojaneuvosto katsoo, että suunniteltuun käsittelyyn liittyvää lainsäädäntötoimenpidettä koskevan ehdotuksen, jonka kansallinen parlamentti hyväksyy, tai tällaiseen lainsäädäntötoimenpiteeseen perustuvan sääntelytoimenpiteen laatimisen yhteydessä on kuultava ennakolta valvontaviranomaista, jotta varmistetaan johdonmukaisuus sovellettavan oikeuskehyksen kanssa sekä sen noudattaminen (ks. lainvalvontadirektiivin 28 artiklan 2 kohta).

3 TAPAUS 3

3.1. Kuvaus

Poliisin puuttuessa mellakoihin ja tutkiessa niitä jälkikäteen useita henkilöitä on tunnistettu epäillyiksi esimerkiksi aiempien tutkintojen perusteella, joissa on käytetty valvontakamerakuvaa tai todistajia. Näiden epäiltyjen kuvia verrataan kuviin henkilöistä, jotka ovat tallentuneet valvontakameroiden tai mobiililaitteiden kuvaan rikospaikalla tai sitä ympäröivillä alueilla.

Saadakseen yksityiskohtaisempia todisteita henkilöistä, joiden epäillään osallistuneen mielenosoitukseen liittyviin mellakoihin, poliisi luo tietokannan, joka koostuu kuvamateriaalista, jolla on löyhä paikallinen ja ajallinen yhteys mellakoihin. Tietokanta sisältää kansalaisten poliisille lataamia yksityisiä tallenteita, julkisen liikenteen valvontakameroista saatua materiaalia, poliisin omistamaa videovalvontamateriaalia ja tiedotusvälineiden julkaisemaa materiaalia ilman erityisiä rajoituksia tai suojatoimia. Näyttö vakavasta rikollisesta toiminnasta ei ole edellytys tiedostojen keräämiselle tietokantaan. Näin ollen henkilöt, jotka eivät ole olleet mukana mellakoissa, tallennetaan tietokantaan. Tämä tarkoittaa merkittävää prosenttiosuutta paikallisväestöstä, joka sattui kulkemaan ohi

mielenosoituksen aikana tai joka osallistui mielenosoitukseen mutta ei mellakoihin. Tämä tarkoittaa tuhansia video- ja kuvatiedostoja.

Kasvojentunnistusohjelmiston avulla kaikille näissä tiedostoissa esiintyville kasvoille annetaan yksilölliset kasvotunnukset. Tämän jälkeen yksittäisten epäiltyjen kasvoja verrataan automaattisesti näihin kasvotunnuksiin. Tuhansien video- ja kuvatiedostojen kaikista biometrisistä malleista koostuvaa tietokantaa säilytetään, kunnes kaikki mahdolliset tutkimukset on saatettu päätökseen. Asiasta vastaavat virkamiehet käsittelevät positiiviset osumat ja päättävät sen jälkeen jatkotoimista. Niihin voi kuulua tietokannassa olevan tiedoston liittäminen kyseessä olevan henkilön rikostiedostoon sekä lisätoimenpiteet, kuten kyseisen henkilön kuulustelu tai pidättäminen.

Kansallisessa laissa on yleinen säännös, jonka mukaan biometristen tietojen käsittely luonnollisen henkilön yksilöllistä tunnistamista varten on sallittua, jos se on ehdottoman välttämätöntä ja jos siinä sovelletaan kyseisen henkilön oikeuksia ja vapauksia koskevia asianmukaisia suojatoimia.

Tietolähde:

- Rekisteröityjen tyypit: ☒ kaikki henkilöt
- Kuvan lähde: ☒ julkiset tilat ☒ yksityinen taho ☒ muut yksityishenkilöt ☒ muu: tiedotusvälineet
- Yhteys rikokseen: ☒ ei välttämättä suoraa maantieteellistä tai ajallista yhteyttä
- Tietojen keräystapa: ☒ etäyhteys
- Asiayhteys – vaikuttaa muihin perusoikeuksiin: kyllä, mihin: ☒ kokoontumisvapauteen
- Rekisteröityä koskevien tietojen muut saatavilla olevat lähteet:
  ☒ muu: ei ole poissuljettu (kuten pankkiautomaattien käyttö tai sisäänkäynti kauppoihin), koska kuvien ottamisen syitä ei voida hallita

Viitetietokanta (johon kerättyjä tietoja verrataan):

- Spesifisyys: ☒ rikosalueeseen liittyvät erityistietokannat

Algoritmi:

- Käsittelytyyppi: ☒ yksi-moneen-tunnistaminen

Tulos:

- Vaikutus: ☒ suora (esim. rekisteröity voidaan pidättää, häntä voidaan kuulustella)
- Automaattinen päätös: ☒ EI
- Säilytyksen kesto: kunnes kaikki mahdolliset tutkimukset on saatettu päätökseen

Oikeudellinen arviointi:

- Miten rekisteröidylle tiedotetaan asiasta ennakkoon: ☒ yleisesti lainvalvontaviranomaisen verkkosivustolla
- Sovellettava oikeuskehys: ☒ lainvalvontadirektiivi kansalliseen lainsäädäntöön pääosin kopioituna ☒ yleinen kansallinen lainsäädäntö, joka koskee lainvalvontaviranomaisten suorittamaa biometristen tietojen käyttöä

3.2. Sovellettava oikeuskehys

Kuten edellä on selvennetty, oikeusperustat, joissa pelkästään toistetaan lainvalvontadirektiivin 10 artiklan yleinen lauseke, eivät ole sanamuodoltaan riittävän selkeitä, jotta henkilöt saisivat riittävän käsityksen siitä, millä edellytyksillä ja missä tilanteissa lainvalvontaviranomaiset voivat käyttää julkisista tiloista peräisin olevia videovalvontatallenteita luodakseen henkilöiden kasvoista biometrisen mallin ja verrata sitä esimerkiksi poliisitietokantoihin, muihin saatavilla oleviin

valvontakameratallenteisiin tai yksityisiin tallenteisiin. Tämän vuoksi tässä tapauksessa vahvistettu oikeuskehys ei täytä vähimmäisvaatimuksia, jotta sitä voitaisiin käyttää oikeusperustana.

3.3. Tarpeellisuus ja oikeasuhteisuus

Tässä esimerkissä käsittely herättää useita huolenaiheita tarpeellisuus- ja oikeasuhteisuusperiaatteiden suhteen useista syistä:

Henkilöitä ei epäillä vakavasta rikoksesta. Näyttö vakavasta rikollisesta toiminnasta ei ole edellytys kuvamateriaalia sisältävän tietokannan tiedostojen käytölle. Suora ajallinen ja maantieteellinen yhteys rikokseen ei myöskään ole edellytys tietokannan tiedostojen käytölle. Tämä johtaa siihen, että merkittävä osa paikallisväestöstä tallennetaan biometriseen tietokantaan mahdollisesti usean vuoden ajaksi, kunnes kaikki tutkimukset on saatu päätökseen.

Rikospaikkatietokantaa ei ole rajoitettu kuviin, jotka täyttävät oikeasuhteisuusvaatimukset, joten vertailtavien kuvien määrä on rajaton. Tämä on ristiriidassa tietojen minimoinnin periaatteen kanssa. Pienempi kuvamäärä mahdollistaisi myös sen, että voitaisiin harkita keinoja, jotka eivät perustu algoritmeihin ja jotka puuttuvat oikeuksiin pienemmässä mittakaavassa, kuten supertunnistajia.[88]

Koska esimerkki koskee mielenosoituksen ympäristöä, on myös todennäköistä, että kuvat paljastavat mielenosoitukseen osallistuneiden poliittisia mielipiteitä, jotka kuuluvat toiseen erityiseen tietoluokkaan, johon tämä tapaus mahdollisesti vaikuttaa. Tässä tapauksessa on epäselvää, miten näiden tietojen kerääminen voidaan estää ja millä suojatoimilla. Lisäksi kun rekisteröidyt saavat tietää, että heidän osallistumisensa mielenosoitukseen on johtanut heidän merkitsemiseensä biometriseen poliisitietokantaan, sillä voi olla vakavia tukahduttavia vaikutuksia heidän kokoontumisoikeutensa käyttämiseen tulevaisuudessa.

Tietokannassa olevia biometrisiä malleja voidaan myös verrata toisiinsa. Näin poliisi voi paitsi etsiä tiettyä henkilöä kaikesta aineistostaan myös rekonstruoida henkilön käyttäytymismallin useiden päivien ajalta. Poliisi voi myös kerätä lisätietoja henkilöistä, kuten sosiaalisista yhteyksistä ja poliittisesta osallistumisesta.

Puuttumista oikeuksiin lisää se, että tietoja käsitellään rekisteröityjen tietämättä.

Kun otetaan huomioon, että ihmiset tallentavat valokuvia ja videoita jatkuvasti ja että jopa kaikkialla läsnä olevien valvontakameroiden tallentamaa kuvaa voidaan analysoida biometrisesti, tämä voi johtaa vakaviin tukahduttaviin vaikutuksiin.

Yksityisten valokuvien ja videoiden laaja käyttö, mukaan lukien mahdollinen väärinkäyttö, kuten ilmianto, on toinen huolenaihe. Koska väärinkäyttö, kuten ilmianto, on yleensä myös rikosoikeudellisille menettelyille ominainen riski, riski on huomattavasti korkeampi käsiteltävien tietojen skaalautuvuuden ja kyseessä olevien henkilöiden määrän osalta, sillä ihmiset voivat ladata järjestelmään myös materiaalia, joka liittyy tiettyyn henkilöön tai henkilöryhmään, josta he eivät pidä. Poliisin esittämät pyynnöt ladata valokuvia ja videoita saattavat johtaa siihen, että ihmisten kynnys toimittaa materiaalia on hyvin matala, varsinkin kun se on mahdollista tehdä nimettömänä tai ainakin ilman, että poliisiasemalle tarvitsee saapua ja tunnistautua.

[88] Eli henkilöitä, joiden kyky tunnistaa kasvoja on poikkeuksellinen. Ks. myös: ”Face Recognition by Metropolitan Police Super-Recognisers”, 26.2.2016, DOI: 10.1371/journal.pone.0150036, https://pubmed.ncbi.nlm.nih.gov/26918457/.

3.4. Päätelmät

Esimerkissä ei ole erityistä säännöstä, joka voisi toimia oikeusperustana. Vaikka riittävä oikeusperusta olisikin olemassa, tarpeellisuus- ja oikeasuhteisuusvaatimukset eivät kuitenkaan täyttyisi, mikä johtaisi siihen, että yksityiselämän kunnioittamista ja henkilötietojen suojaa koskeviin perusoikeuskirjan mukaisiin rekisteröidyn oikeuksiin puututtaisiin suhteettomasti.

4 TAPAUS 4

4.1. Kuvaus

Poliisi ottaa käyttöön tavan, jolla voidaan tunnistaa valvontakameran kuvaan tallentuneet vakavaan rikokseen syyllistyneet epäillyt jälkikäteen kasvojentunnistusteknologian avulla. Virkamies valitsee manuaalisesti rikospaikalta tai muualta esitutkinnan yhteydessä kerätystä videomateriaalista epäiltyjen kuvan tai kuvat ja lähettää ne rikostekniselle osastolle. Rikostekninen osasto käyttää kasvojentunnistusteknologiaa verratakseen näitä kuvia henkilöiden kuviin, jotka poliisi on aiemmin kerännyt tietokantaan (ns. kuvailutietokanta, joka koostuu epäillyistä ja aiemmin tuomituista). Kuvailutietokantaa analysoidaan tätä menettelyä varten – väliaikaisesti ja eristetyssä ympäristössä – kasvojentunnistusteknologialla, jotta vertailu voidaan suorittaa. Vertailtujen henkilöiden oikeuksiin ja etuihin puuttumisen minimoimiseksi vain harvalla rikosteknisen osaston työntekijällä on lupa varsinaisen vertailumenettelyn suorittamiseen, tietoihin pääsee käsiksi vain ne virkamiehet, joille kyseinen tiedosto on uskottu, ja tulokset tarkastetaan manuaalisesti ennen niiden toimittamista tutkivalle virkamiehelle. Biometrisiä tietoja ei toimiteta valvotun, eristetyn ympäristön ulkopuolelle. Vain tulosta ja kuvaa (ei biometristä mallia) käytetään edelleen tutkinnassa. Työntekijät saavat erityiskoulutusta tätä käsittelyä koskevista säännöistä ja menettelyistä, ja kaikki henkilötietojen ja biometristen tietojen käsittely on määritelty riittävästi kansallisessa lainsäädännössä.

Tietolähde:

- Rekisteröityjen tyypit: ☒ valvontakameratallenteista tunnistetut epäillyt
- Kuvan lähde: ☒ julkiset tilat ☒ internet
- Yhteys rikokseen: ☒ suora ajallinen yhteys
  ☒ suora maantieteellinen yhteys
- Tietojen keräystapa: ☒ etäyhteys
- Asiayhteys – vaikuttaa muihin perusoikeuksiin: kyllä, mihin: ☒ kokoontumisvapauteen ☒ sananvapauteen ☒ useisiin: __

Viitetietokanta (johon kerättyjä tietoja verrataan):

- Spesifisyys: ☒ rikosalueeseen liittyvät erityistietokannat

Algoritmi:

- Käsittelytyyppi: ☒ yksi-moneen-tunnistaminen

Tulos:

- Vaikutus: ☒ suora (esim. rekisteröity pidätetään, häntä kuulustellaan)
- Automaattinen päätös: ☒ EI

Oikeudellinen arviointi:

- Sovellettava oikeuskehys: ☒ kyseistä käsittelyä (kasvojentunnistus) koskeva kansallinen erityislainsäädäntö kyseisen toimivaltaisen viranomaisen osalta

4.2. Sovellettava oikeuskehys

Tässä tapauksessa kansallisessa lainsäädännössä säädetään, että biometrisiä tietoja voidaan käyttää rikosteknisen analyysin suorittamiseen, kun se on ehdottoman välttämätöntä vakavasta rikoksesta epäiltyjen tunnistamiseksi vertaamalla kuvailutietokannassa olevia kuvia. Kansallisessa lainsäädännössä täsmennetään, mitä tietoja voidaan käsitellä, sekä menettelyt henkilötietojen eheyden ja luottamuksellisuuden säilyttämiseksi ja tietojen hävittämiseksi, mikä antaa riittävät takeet väärinkäyttö- ja mielivaltaisuusriskiä vastaan.

4.3. Tarpeellisuus ja oikeasuhteisuus

Kasvojentunnistuksen käyttö on selvästi manuaalista vertailua tehokkaampaa ajallisesti rikosteknisellä tasolla. Etukäteen tehtävällä kuvien manuaalisella valinnalla rajoitetaan oikeuksiin puuttumista verrattuna siihen, että koko videomateriaalia verrataan tietokantaan, ja tällä tavoin erotetaan joukosta vain ne henkilöt, joita tavoite eli vakavan rikollisuuden torjunta koskee, ja kohdennetaan käsittely heihin. On kuitenkin edelleen tärkeää harkita, voidaanko vertailu tehdä manuaalisesti kohtuullisessa ajassa, riippuen käsiteltävänä olevasta tapauksesta. Niiden henkilöiden määrän rajoittaminen, joilla on pääsy teknologiaan ja henkilötietoihin, sekä se, että biometrisiä malleja ei säilytetä tai käytetä myöhemmin tutkinnassa, vähentää vaikutuksia yksityisyyttä ja tietosuojaa koskeviin oikeuksiin. Lisäksi tulosten manuaalinen tarkistaminen vähentää väärien positiivisten tulosten riskiä.

4.4. Päätelmät

On tärkeää, että kansallinen lainsäädäntö tarjoaa asianmukaisen oikeusperustan biometristen tietojen käsittelylle sekä kansalliselle tietokannalle, johon kuvia verrataan. Tässä tapauksessa tietosuojaoikeuksiin puuttumisen rajoittamiseksi on otettu käyttöön useita toimenpiteitä, kuten oikeusperustassa määritellyt kasvojentunnistusteknologian käytön edellytykset, niiden henkilöiden lukumäärä, joilla on pääsy teknologiaan ja biometrisiin tietoihin, sekä manuaaliset tarkistukset. Kasvojentunnistusteknologia parantaa merkittävästi poliisin rikosteknisen osaston tutkintatyön tehokkuutta ja perustuu lakiin, jonka mukaan poliisi voi käsitellä biometrisiä tietoja silloin, kun se on ehdottoman välttämätöntä. Täten kasvojentunnistusteknologian käyttöä voidaan pitää laillisena puuttumisena yksilön oikeuksiin.

5 TAPAUS 5

5.1. Kuvaus

Biometrinen etätunnistus tarkoittaa sitä, että henkilöiden henkilöllisyys määritetään biometristen tunnisteiden (kasvokuva, kävely, iiris jne.) avulla etäältä, julkisessa tilassa ja jatkuvalla tavalla vertaamalla niitä tietokantaan tallennettuihin (biometrisiin) tietoihin[89]. Biometrinen etätunnistus suoritetaan reaaliajassa, jos kuvamateriaalin kerääminen, vertailu ja tunnistus tapahtuvat ilman merkittävää viivettä.

Ennen kunkin reaaliaikaisen biometrisen etätunnistuksen aloittamista poliisi laatii tutkinnan yhteydessä tarkkailulistan kiinnostavista henkilöistä. Se koostuu henkilöiden kasvokuvista. Jos tiedustelutiedot viittaavat siihen, että henkilöt tulevat olemaan tietyllä alueella, kuten ostoskeskuksessa tai julkisella aukiolla, poliisi päättää, milloin, missä ja kuinka kauan biometristä etätunnistusta käytetään.

Toimintapäivänä kentälle sijoitetaan poliisiauto, joka toimii valvontakeskuksena ja jonka kyydissä on ylempi poliisivirkamies. Autossa on näyttöjä, joilla näkyy kuvaa lähistöllä sijaitsevista

[89] https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

valvontakameroista. Joko kamerat on asennettu tilapäisesti tai näytöt on yhdistetty jo asennettujen kameroiden videovirtoihin. Kun jalankulkijat kulkevat kameroiden ohi, teknologia eristää kasvokuvat, muuntaa ne biometriseksi malliksi ja vertaa niitä tarkkailulistalla olevien henkilöiden biometrisiin malleihin.

Jos havaitaan mahdollinen osuma tarkkailulistan ja kameroiden ohi kulkevien henkilöiden välillä, autossa oleville poliisivirkamiehille lähetetään hälytys. Jos hälytys on positiivinen, he ilmoittavat asiasta kentällä oleville poliisivirkamiehille esimerkiksi radiolaitteen välityksellä. Tämän jälkeen kentällä oleva virkamies päättää, puututaanko asiaan, lähestytäänkö henkilöä tai loppujen lopuksi pidätetäänkö hänet. Virkamiehen paikan päällä toteuttamat toimenpiteet kirjataan ylös. Kun kyseessä on huomaamaton tarkastus, kerätyt tiedot (kuten se, kenen kanssa henkilö on, mitä heillä on yllään ja minne he ovat menossa) tallennetaan.

Kansallisessa laissa, johon viitataan, on yleinen säännös, jonka mukaan biometristen tietojen käsittely luonnollisen henkilön yksilöllistä tunnistamista varten on sallittua, jos se on ehdottoman välttämätöntä ja jos siinä sovelletaan kyseisen henkilön oikeuksia ja vapauksia koskevia asianmukaisia suojatoimia.

Tietolähde:

- Rekisteröityjen tyypit: ☒ kaikki henkilöt
- Kuvan lähde: ☒ julkiset tilat
- Yhteys rikokseen: ☒ ei välttämättä suoraa maantieteellistä tai ajallista yhteyttä
- Tietojen keräystapa: ☒ etäyhteys
- Asiayhteys – vaikuttaa muihin perusoikeuksiin: kyllä, mihin: ☒ kokoontumisvapauteen ☒ sananvapauteen ☒ useisiin
- Rekisteröityä koskevien tietojen muut saatavilla olevat lähteet:
  ☒ muu: ei poissuljettu (esim. pankkiautomaattien käyttö tai sisäänkäynti kauppoihin)

Viitetietokanta (johon kerättyjä tietoja verrataan):

- Spesifisyys: ☒ rikosalueeseen liittyvät erityistietokannat

Algoritmi:

- Käsittelytyyppi: ☒ yksi-moneen-tunnistaminen

Tulos:

- Vaikutus: ☒ suora (esim. rekisteröity pidätetään, häntä kuulustellaan)
- Automaattinen päätös: ☒ EI
- Säilytyksen kesto: kunnes kaikki mahdolliset tutkimukset on saatettu päätökseen

Oikeudellinen arviointi:

- Miten rekisteröidylle tiedotetaan asiasta ennakkoon: ☒ yleisesti lainvalvontaviranomaisen verkkosivustolla
- Sovellettava oikeuskehys: ☒ lainvalvontadirektiivi kansalliseen lainsäädäntöön pääosin kopioituna ☒ yleinen kansallinen lainsäädäntö, joka koskee lainvalvontaviranomaisten suorittamaa biometristen tietojen käyttöä

5.2. Sovellettava oikeuskehys

Oikeusperustat, joissa pelkästään toistetaan lainvalvontadirektiivin 10 artiklan yleinen lauseke, eivät ole sanamuodoltaan riittävän selkeitä, jotta henkilöt saisivat riittävän käsityksen siitä, millä

edellytyksillä ja missä olosuhteissa lainvalvontaviranomaiset voivat käyttää julkisista tiloista peräisin olevia valvontakameratallenteita luodakseen henkilöiden kasvoista biometrisen mallin ja verrata sitä poliisitietokantoihin. Tässä tapauksessa mainittu oikeuskehys ei näin ollen täytä vähimmäisvaatimuksia, jotta sitä voitaisiin käyttää oikeusperustana.[90]

5.3. Tarpeellisuus ja oikeasuhteisuus

Tarpeellisuuden ja oikeasuhteisuuden kynnys on sitä korkeammalla, mitä syvempää oikeuksiin puuttuminen on. Julkisissa tiloissa tapahtuvalla biometrisellä etätunnistuksella on useita seurauksia perusoikeuksien kannalta:

Tapauksessa valvotaan jokaista ohikulkijaa kyseisessä julkisessa tilassa. Näin ollen se vaikuttaa vakavasti väestön kohtuulliseen odotukseen olla anonyymi julkisissa tiloissa[91]. Tämä on edellytys monille demokraattisen prosessin osa-alueille, kuten päätökselle liittyä kansalaisyhdistykseen, käydä kokoontumisissa ja tavata ihmisiä kaikista sosiaalisista ja kulttuurisista taustoista, osallistua poliittiseen mielenosoitukseen ja vierailla kaikenlaisissa paikoissa. Anonymiteetti julkisissa tiloissa on olennaisen tärkeä, jotta tietoja ja ajatuksia voidaan kerätä ja vaihtaa vapaasti. Sen avulla säilytetään mielipiteiden moninaisuus, vapaus rauhanomaiseen kokoontumiseen, yhdistymisvapaus sekä vähemmistöjen suojelu ja tuetaan vallanjaon ja keskinäisen valvonnan periaatteita. Anonymiteetin heikentäminen julkisissa tiloissa voi aiheuttaa vakavia tukehduttavia vaikutuksia kansalaisille. He voivat pidättäytyä tietyistä toimista, jotka ovat täysin vapaan ja avoimen yhteiskunnan sääntöjen mukaisia. Tämä vaikuttaisi yleiseen etuun, sillä demokraattinen yhteiskunta edellyttää kansalaistensa itsemääräämisoikeutta ja osallistumista demokraattiseen prosessiin.

Jos tällaista teknologiaa käytetään, pelkkä kadulla, metroon tai leipomoliikkeeseen käveleminen kyseisellä alueella johtaa siihen, että lainvalvontaviranomaiset keräävät henkilötietoja, myös biometrisiä tietoja, ja että ensimmäisessä tapauksessa niitä myös verrataan poliisitietokantoihin. Tilanne, jossa sama tehtäisiin sormenjälkiä ottamalla, olisi selvästi suhteeton.

Niiden rekisteröityjen määrä, joihin kasvojentunnistusteknologian käyttö vaikuttaa, on erittäin suuri, sillä se vaikuttaa kaikkiin, jotka kävelevät asianomaisen julkisen alueen ohi. Lisäksi tapaukset tarkoittaisivat biometristen tietojen automaattista massakäsittelyä sekä biometristen tietojen massavertailua poliisitietokantoihin.

Eurooppalaisessa oikeuskäytännössä massavalvonta on kielletty (esimerkiksi Euroopan ihmisoikeustuomioistuin katsoi asiassa S. ja Marper v. Yhdistynyt kuningaskunta, että biometristen tietojen valikoimaton säilyttäminen on suhteeton puuttuminen yksityisyyttä koskevaan oikeuteen, koska sitä ei voida pitää välttämättömänä demokraattisessa yhteiskunnassa).

Biometrisen etätunnistuksen taipumus massavalvontaan on niin suuri, että luotettavia rajoituskeinoja ei ole. Se eroaa sellaisenaan olennaisesti videovalvonnasta, sillä videomateriaalin mahdollinen käyttö ilman biometristä tunnistusta puuttuu jo voimakkaasti mutta samalla rajoitetusti oikeuksiin, kun taas jos käytetään kasvojentunnistusteknologiaa, videovalvontajärjestelmä, joka on jo levinnyt laajalle ja joka toimii pääasiallisena tietolähteenä, muuttuu laadullisesti. Lisäksi, erityisesti kun otetaan

[90] Tapauksissa, joissa kasvojentunnistusteknologian käytön tutkimiseen pyrkivässä tieteellisessä hankkeessa olisi käsiteltävä henkilötietoja mutta tällainen käsittely ei kuulu lainvalvontadirektiivin 4 artiklan 3 kohdan tai unionin lainsäädännön soveltamisalaan, sovelletaan yleistä tietosuoja-asetusta. Lainvalvontadirektiiviä sovelletaan kuitenkin pilottihankkeisiin, joiden jälkeen toteutetaan lainvalvontatoimia.

[91] Euroopan tietosuojaneuvoston vastaus Euroopan parlamentin jäsenille Clearview-tekoälyn kehittämästä kasvojentunnistussovelluksesta, 10. kesäkuuta 2020, viite: OUT2020-0052.

huomioon oletetut tukahduttavat vaikutukset, jo olemassa olevien videovalvontalaitteistojen käytön mahdolliset rajoitukset eivät ole näkyviä, eikä yleisö näin ollen luota niihin.

Poliisiviranomaisten suorittamassa biometrisessä etätunnistuksessa kaikkia kohdellaan mahdollisena epäiltynä. Oikeusvaltioperiaatetta noudattavassa valtiossa kansalaisten oletetaan kuitenkin olevan oikeamielisiä siihen saakka, kunnes heidän voidaan todistaa käyttäytyneen väärin. Tämä periaate on otettu osittain huomioon myös lainvalvontadirektiivissä, jossa korostetaan tarvetta tehdä mahdollisuuksien mukaan ero rikoksista tuomittujen tai epäiltyjen ja sellaisten henkilöjen kohtelun välillä, joita ei ole tuomittu tai joita ei epäillä rikollisesta toiminnasta. Tuomittujen ja epäiltyjen osalta lainvalvontaviranomaisilla on oltava vakavat perusteet uskoa heidän ”syyllistyneen tai olevan syyllistymässä rikokseen” (lainvalvontadirektiivin 6 artiklan a alakohta).

Liikenteen solmukohdissa tai julkisissa tiloissa lainvalvontaviranomaisten käyttämä teknologia, jolla voidaan tunnistaa yksilöllisesti yksittäinen henkilö ja jäljittää ja analysoida hänen olinpaikkansa ja liikkeensä, paljastaa jopa kaikkein arkaluonteisimpia tietoja henkilöstä (jopa seksuaaliset mieltymykset, uskonto, terveysongelmat). Tämä tuo mukanaan valtavan riskin siitä, että tietoihin päästään ja niitä käytetään laittomasti.

Sellaisen järjestelmän asentaminen, joka mahdollistaa henkilön käyttäytymisen ja ominaisuuksien ytimen paljastamisen, johtaa voimakkaisiin tukehduttaviin vaikutuksiin. Se saa ihmiset kyseenalaistamaan sen, kannattaako heidän osallistua tiettyyn mielenosoitukseen, mikä vahingoittaa demokraattista prosessia. Myös tapaaminen ja nähdyksi tuleminen julkisesti sellaisen ystävän kanssa, jolla tiedetään olevan vaikeuksia poliisin kanssa tai jonka tiedetään käyttäytyvän ainutlaatuisella tavalla, saatetaan nähdä kriittisenä asiana, koska se johtaisi järjestelmän algoritmin ja siten lainvalvontaviranomaisten kiinnostumiseen.

Haavoittuvassa asemassa olevien rekisteröityjen, kuten lasten, suojelu on mahdotonta. Lisäksi tämä vaikuttaa henkilöihin, joiden ammatillinen etu – ja usein vastaava oikeudellinen velvollisuus – vaatii, että he pitävät yhteytensä luottamuksellisina, kuten toimittajiin, asianajajiin ja pappeihin. Tämä voisi johtaa esimerkiksi lähteen ja toimittajan tai sen paljastumiseen, että henkilö on kääntynyt puolustusasianajajan puoleen. Ongelma ei koske vain satunnaisia julkisia paikkoja, joissa esimerkiksi toimittajat ja heidän lähteensä tapaavat, vaan luonnollisesti myös julkisia tiloja, joita tarvitaan instituutioiden tai alan ammattilaisten lähestymiseen tai käyttämiseen.

Lisäksi kasvojentunnistusteknologian aiheuttama epämukavuus voi johtaa siihen, että ihmiset muuttavat käyttäytymistään, välttelevät paikkoja, joissa kasvojentunnistusteknologiaa käytetään, ja vetäytyvät siten sosiaalisesta elämästä ja kulttuuritapahtumista. Kasvojentunnistusteknologian käyttöönoton laajuudesta riippuen vaikutus ihmisiin voi olla niin merkittävä, että se vaikuttaa heidän kykyynsä elää ihmisarvoista elämää[92].

Näin ollen on erittäin todennäköistä, että se vaikuttaa henkilötietojen suojaa koskevan oikeuden olennaiseen sisältöön, sen loukkaamattomaan ytimeen. Tähän viittaa vahvasti (ks. ohjeiden kohta 3.1.3.2) erityisesti seuraavat seikat: lainvalvontaviranomaiset käsittelevät laajamittaisesti ja automaattisesti ihmisten ainutlaatuisia biologisia ominaisuuksia uskottavuuteen perustuvilla algoritmeilla, joiden tulokset ovat vain rajoitetusti selitettävissä. Yksityisyyden suojaa ja tietosuojaa koskevia rajoituksia sovelletaan henkilön yksilöllisestä käyttäytymisestä tai häntä koskevasta tilanteesta riippumatta. Tilastollisesti lähes kaikki rekisteröidyt, joihin tämä puuttuminen vaikuttaa,

92 https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf, sivu 20.

ovat lainkuuliaisia henkilöitä. Mahdollisuudet tarjota tietoa rekisteröidylle ovat rajalliset. Useimmissa tapauksissa oikeussuojakeinojen käyttö on mahdollista vasta jälkikäteen.

Tukeutuminen uskottavuuteen perustuvaan järjestelmään, jonka selitettävyys on rajallinen, voi johtaa vastuun hajautumiseen ja puutteelliseen oikeussuojaan ja voi kannustaa laiminlyönteihin.

Kun tällaista järjestelmää, jota voidaan käyttää myös olemassa oleviin valvontakameroihin, käytetään hyvin vähäisin ponnistuksin ja ilman, että se on yksilöiden nähtävissä, sitä voidaan käyttää väärin ja sen avulla voidaan laatia järjestelmällisesti ja nopeasti luetteloita henkilöistä etnisen alkuperän, sukupuolen, uskonnon yms. mukaan. Periaate, jonka mukaan henkilötietoja käsitellään ennalta määriteltyjen kriteerien, kuten henkilön olinpaikan ja kuljetun reitin, perusteella, on jo käytössä[93], ja se on taipuvainen syrjintään.

Käsiteltävien tietojen arkaluonteisuuden, ilmaisuvoiman ja määrän mukaan järjestelmät, joita käytetään kasvojen etätunnistukseen julkisissa tiloissa, ovat alttiita väärinkäytöksille, joilla on haitallisia vaikutuksia asianomaisten henkilöiden kannalta. Tällaisia tietoja voidaan myös helposti kerätä ja käyttää väärin keskinäisen valvonnan periaatteen keskeisten toimijoiden, kuten poliittisen opposition, virkamiesten ja toimittajien, painostamiseksi.

Lisäksi kasvojentunnistusjärjestelmiin sisältyy usein voimakkaita rotuun ja sukupuoleen liittyviä vinouttavia tekijöitä: väärät positiiviset tulokset vaikuttavat suhteettoman paljon värillisiin ihmisiin ja naisiin[94], mikä johtaa syrjintään. Väärästä positiivisesta tuloksesta johtuvat poliisitoimenpiteet, kuten etsinnät ja pidätykset, leimaavat näitä ryhmiä entisestään.

5.4. Päätelmät

Edellä mainituissa tapauksissa, jotka koskevat biometristen tietojen etäkäsittelyä julkisissa tiloissa tunnistamistarkoituksia varten, ei saavuteta oikeudenmukaista tasapainoa kilpailevien yksityisten ja yleisten etujen välillä, mikä merkitsee suhteetonta puuttumista perusoikeuskirjan 7 ja 8 artiklan mukaisiin rekisteröidyn oikeuksiin.

6 TAPAUS 6

6.1. Kuvaus

Yksityinen taho tarjoaa sovelluksen, johon kerätään kasvokuvia internetistä tietokannan luomiseksi. Käyttäjä, esimerkiksi poliisi, voi tämän jälkeen ladata sovellukseen kuvan, ja biometrisen tunnistuksen avulla sovellus yrittää löytää sille vastaavuuden tietokannassaan olevista kasvokuvista tai biometrisistä malleista.

Paikallinen poliisilaitos tutkii rikosta, joka on tallentunut videolle, josta useita mahdollisia silminnäkijöitä ja epäiltyjä ei pystytä tunnistamaan vertaamalla kerättyjä tietoja sisäisiin tietokantoihin tai tiedustelutietoihin. Kerättyjen tietojen perusteella henkilöitä ei ole rekisteröity mihinkään olemassa

[93] Ks. Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/681, annettu 27 päivänä huhtikuuta 2016, matkustajarekisteritietojen (PNR) käytöstä terrorismirikosten ja vakavan rikollisuuden ennalta estämistä, paljastamista ja tutkintaa sekä tällaisiin rikoksiin liittyviä syytetoimia varten, 6 artikla, ja Euroopan parlamentin ja neuvoston asetus (EU) 2018/1240, annettu 12 päivänä syyskuuta 2018, Euroopan matkustustieto- ja -lupajärjestelmän (ETIAS) perustamisesta ja asetusten (EU) N:o 1077/2011, (EU) N:o 515/2014, (EU) 2016/399, (EU) 2016/1624 ja (EU) 2017/2226 muuttamisesta, 33 artikla.

[94] https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

olevaan poliisitietokantaan. Poliisi päättää käyttää edellä kuvattua, yksityisen yrityksen tarjoamaa työkalua henkilöiden tunnistamiseksi biometrisen tunnistuksen avulla.

Tietolähde:

- Rekisteröityjen tyypit: ☒ kaikki kansalaiset (silminnäkijät) ☒ tuomitut ☒ epäillyt
- Kuvan lähde: ☒ videomateriaali, joka on peräisin julkisesta paikasta tai kerätty muualta esitutkinnan yhteydessä
- Yhteys rikokseen: ☒ ei ole tarpeen
- Tietojen keräystapa: ☒ etäyhteys
- Asiayhteys – vaikuttaa muihin perusoikeuksiin: kyllä, mihin: ☒ kokoontumisvapauteen ☒ sananvapauteen ☒ useisiin: __

Viitetietokanta (johon kerättyjä tietoja verrataan):

- Spesifisyys: ☒ yleiset tietokannat, jotka on koottu internetistä peräisin olevilla tiedoilla

Algoritmi:

- Käsittelytyyppi: ☒ yksi-moneen-tunnistaminen

Tulos:

- Vaikutus ☒ suora (esim. rekisteröidyn pidättäminen, kuulustelu, diskriminoiva kohtelu)
- Automaattinen päätös: ☒ EI

Oikeudellinen arviointi:

- Miten rekisteröidylle tiedotetaan asiasta ennakkoon: ☒ ei tiedoteta

6.2. Sovellettava oikeuskehys

Kun yksityinen taho tarjoaa palvelua, johon sisältyy henkilötietojen käsittelyä, jonka tarkoituksen ja keinot se määrittää (tässä tapauksessa kuvien kerääminen internetistä tietokannan luomiseksi), kyseisellä yksityisellä taholla on oltava oikeusperusta tälle käsittelylle. Lisäksi lainvalvontaviranomaisella, joka päättää käyttää tätä palvelua omiin tarkoituksiinsa, on oltava oikeusperusta käsittelylle, jonka tarkoitukset ja keinot se määrittää. Jotta lainvalvontaviranomainen voi käsitellä biometrisiä tietoja, on oltava oikeuskehys, jossa määritellään tavoite, käsiteltävät henkilötiedot, käsittelyn tarkoitukset, menettelyt henkilötietojen eheyden ja luottamuksellisuuden säilyttämiseksi sekä menettelyt henkilötietojen tuhoamiseksi.

Tässä tapauksessa henkilötietoja kerätään laajamittaisesti henkilöiltä, jotka eivät ole tietoisia heidän tietojensa keräämisestä. Tällainen käsittely voisi olla laillista vain hyvin poikkeuksellisissa tilanteissa. Riippuen siitä, missä tietokanta sijaitsee, tällaisen palvelun käyttäminen voi edellyttää henkilötietojen ja/tai erityisiin henkilötietoryhmiin kuuluvien tietojen siirtämistä Euroopan unionin ulkopuolelle (poliisi siirtää tiedot esimerkiksi ”lähettämällä” valvontakameran videolla näkyvän tai muulla keruutavalla saadun kasvokuvan), jolloin kyseiselle siirrolle on erityisiä edellytyksiä (ks. lainvalvontadirektiivin 39 artikla).

Tässä tapauksessa ei ole erityisiä sääntöjä, jotka sallisivat lainvalvontaviranomaisille tällaisen käsittelyn.

6.3. Tarpeellisuus ja oikeasuhteisuus

Se, että lainvalvontaviranomaiset käyttävät palvelua, tarkoittaa, että henkilötietoja jaetaan sellaisen yksityisen tahon kanssa, joka käyttää tietokantaa, johon henkilötietoja kerätään rajoittamattomasti ja

laajamittaisesti. Kerättyjen henkilötietojen ja lainvalvontaviranomaisen tavoitteen välillä ei ole yhteyttä. Se, että lainvalvontaviranomainen jakaa tietoja yksityiselle taholle, tarkoittaa myös sitä, että viranomaisella ei ole valtaa päättää tiedoista, joita yksityinen taho käsittelee, ja että rekisteröityjen on erittäin vaikeaa käyttää oikeuksiaan, koska he eivät ole tietoisia siitä, että heidän tietojaan käsitellään tällä tavoin. Tämä asettaa hyvin korkean kynnyksen tilanteille, joissa tällainen käsittely voisi edes tapahtua. On kyseenalaista, täyttäisikö mikään tavoite direktiivissä asetetut vaatimukset, sillä yksityisyyttä ja tietosuojaa koskeviin oikeuksiin voidaan soveltaa poikkeuksia ja rajoituksia vain, jos se on ehdottoman välttämätöntä. Vakavien rikosten torjunnan tehokkuutta koskeva yleinen etu ei itsessään oikeuta käsittelyä, jos tällaisia suuria tietomääriä kerätään valikoimatta. Tämä käsittely ei näin ollen täyttäisi tarpeellisuus- ja oikeasuhteisuusvaatimuksia.

6.4. Päätelmät

Koska direktiivin 4 ja 10 artiklan vaatimukset täyttäviä selkeitä, täsmällisiä ja ennakoitavia sääntöjä ei ole ja koska ei ole näyttöä siitä, että kyseinen käsittely olisi ehdottoman välttämätöntä tavoitteiden saavuttamiseksi, voidaan päätellä, että tämän sovelluksen käyttö ei täyttäisi tarpeellisuus- ja oikeasuhteisuusvaatimuksia ja että se merkitsisi suhteetonta puuttumista perusoikeuskirjan mukaisiin yksityiselämän kunnioittamista ja henkilötietojen suojaa koskeviin rekisteröityjen oikeuksiin.