Melisa Kankaanpää

Tekoäly valvonnan välineenä

Turvallisuuden ja perusoikeuksien tasapaino EU:n sääntelyssä

Johtamisen akateeminen yksikkö
Julkisoikeus, Pro gradu -tutkielma
Hallintotieteiden maisteri

Vaasa 2025

VAASAN YLIOPISTO
Johtamisen akateeminen yksikkö
Tekijä: Melisa Kankaanpää
Tutkielman nimi: Tekoäly valvonnan välineenä: Turvallisuuden ja perusoikeuksien tasapaino EU:n sääntelyssä
Tutkinto: Hallintotieteiden maisteri
Oppiaine: Julkisoikeus
Työn ohjaaja: Kristian Siikavirta
Valmistumisvuosi: 2025 **Sivumäärä:** **71**

TIIVISTELMÄ:
Turvallisuus on yhteiskunnan keskeinen perusta ja sen takaaminen on yksi valtion tärkeimmistä tehtävistä. Teknologian nopea kehitys, erityisesti tekoälyyn perustuvien valvontajärjestelmien käyttöönotto on muuttanut turvallisuuskäsitystä ja herättänyt kysymyksiä yksilönvapauksien toteutumisesta. Tutkimuksen tarkoituksena on selvittää, miten EU:n valvontatoimissa voidaan tekoälyn kehittyessä tasapainottaa turvallisuus ja perusoikeudet. Erityisesti, miten EU turvaa kansalaisten turvallisuuden ihmisoikeuksia kunnioittaen tekoälyn aikakaudella. Lisäksi tutkimus pyrkii arvioimaan, miten lainsäädäntökehitys voi varmistaa oikeusvaltioperiaatteen toteutumisen ja kansalaisten perusoikeuksien säilymisen muuttuvassa turvallisuusympäristössä. Tutkimus toteutetaan oikeusdogmaattisena analyysinä, jota täydennetään EU-tason päätösten empiirisellä tarkastelulla.

Tutkimuksen keskiössä ovat EU:n perusoikeuskirja (2000/C 364/01), Suomen perustuslaki (731/1999) ja yleinen tietosuoja-asetus (GDPR, EU 2016/679), jotka määrittelevät turvallisuuden ja yksilönvapauksien toteutumisen oikeudellisen perustan. Perusoikeuskirjan 6 artikla turvaa jokaiselle oikeuden vapauteen ja henkilökohtaiseen turvallisuuteen, kun taas Suomen perustuslain 7 § vahvistaa oikeuden elämään, henkilökohtaiseen vapauteen ja turvallisuuteen. Tekoälyyn perustuvat valvontajärjestelmät, kuten kasvojentunnistus ja massavalvonta, ovat laajentaneet viranomaisten toimintamahdollisuuksia. Samalla se herättää oikeudellisia ja eettisiä kysymyksiä liittyen oikeasuhtaisuuden, tarpeellisuusperiaatteen ja oikeusturvan toteutumiseen. Euroopan ihmisoikeustuomioistuimen linjausten mukaan valvonnan on oltava tarkkarajaista ja perusteltua, mikä luo raamit tekoälyn käytölle. EU:n tekoälyasetus (AI Act) pyrkii asettamaan rajoituksia korkean riskin tekoälyjärjestelmien käytölle, mutta kysymys siitä, kuinka pitkälle yksilönvapauksia voidaan rajoittaa turvallisuuden nimissä, on edelleen keskeinen oikeudellinen ja eettinen haaste. Tutkimuksessa havaitaan, että vaikka EU on tunnistanut tekoälyn riskit perusoikeuksille ja ryhtynyt toimiin niiden hallitsemiseksi, tasapainon löytäminen turvallisuuden ja vapauden välille edellyttää jatkuvaa lainsäädännön kehittämistä ja perusoikeuksien asettamista etusijalle.

AVAINSANAT: EU-oikeus, lainsäädäntö, perusoikeudet, tekoäly, turvallisuus, valvonta

Sisällys

Kuviot

Taulukot

Lyhenteet

AI ACT Artificial Intelligence Act (EU: n Tekoälyasetus)

EDRi European Digital Rights (eurooppalainen digitaali-ihmisoikeusjärjestö)

EIT Euroopan ihmisoikeustuomioistuin

EU Euroopan unioni

EYT Euroopan yhteisöjen tuomioistuin

FADO False and Authentic Documents Online (EU:n asiakirjatietojärjestelmä)

FRA European Union Agency for Fundamental Rights (EU:n perusoikeusvirasto)

GDPR General Data Protection Regulation (EU:n yleinen tietosuoja-asetus)

HE Hallituksen esitys eduskunnalle

ISF Internal Security Fund (Sisäisen turvallisuuden rahasto)

PeVM Perustusvaliokunnan mietintö

PeVL Perustusvaliokunnan lausunto

PL Perustuslaki (Suomen perustuslaki 731/1999)

PWC PricewaterhouseCoopers (kansainvälinen asiantuntijayritys)

RL Rikoslaki (Suomen rikoslaki 39/1889)

SEU Sopimus Euroopan unionista (EU:n perussopimus)

SEUT Sopimus Euroopan unionin toiminnasta (EU:n toimintasopimus)

YK Yhdistyneet kansakunnat (United Nations)

YLE Yleisradio (Suomen kansallinen yleisradioyhtiö)

1 Johdanto

Kuvitelkaamme yhteiskunta, jossa jokaista liikettämme seurataan ja henkilöllisyytemme tunnistetaan julkisilla paikoilla. Kehittyneet algoritmit analysoivat käyttäytymistämme ja arvioivat potentiaalista turvallisuusuhkaamme jo ennen kuin itse tiedostamme tilannetta. Onko tämä dystopia vai lähitulevaisuutemme? Tämä kuvattu tilanne toimii johdantona tutkielman teemaan. Tutkielmassa tarkastelen, miksi on tärkeää pohtia tekoälyvalvonnan vaikutuksia perusoikeuksiin. Teknologian nopean kehityksen myötä lähestymme tilannetta, jossa tekoäly ja valvontateknologiat muokkaavat turvallisuuspolitiikkaa Euroopan unionissa (EU). Tämä herättää perustavanlaatuisen kysymyksen: missä kulkee raja turvallisuuden ja yksilönvapauksien välillä?

1.1 Tutkimuksen tausta

Viime vuosina Euroopan unionissa on keskusteltu laajasti siitä, miten tekoälyä[1] voitaisiin hyödyntää turvallisuuden vahvistamisessa ja terrorismin torjunnassa samalla kun kansalaisten perusoikeudet säilyvät suojattuina. [2] Valvonnan tarve ja uusien seurantakeinojen käyttöönotto on usein perusteltu yhteiskuntarauhan ja kansallisen turvallisuuden varmistamisella. [3] Euroopan ihmisoikeustuomioistuimella (EIT) on keskeinen rooli näiden oikeuksien valvonnassa. Kansalaisjärjestöt ovat kuitenkin olleet tästä kehityskulusta huolissaan ja vaatineet lainsäätäjältä koko EU:n laajuista kieltoa biometriselle kohdentamattomalle valvonnalle. [4] Tekoälyn lisääntyvä käyttö valvontateknologioissa nostaa esiin kysymyksiä siitä, kuinka pitkälle valtiot voivat mennä yksilönvapauksien rajoittamisessa kansallisen turvallisuuden nimissä, ja millaisia rajoituksia EIT:n oikeuskäytäntö asettaa tällaisille toimille.

[1] Euroopan parlamentti (2020 päivitetty 2023.) on määritellyt tekoälyn tarkoittavan koneen kykyä käyttää perinteisesti ihmisen älyyn liittyviä taitoja, kuten päättelyä, oppimista, suunnittelemista ja luomista.
[2] Euroopan parlamentti, 2020, s.9.
[3] Wuori, 2003, s. 402.
[4] EDRi, 2020.

Tässä pro gradu -tutkielmassa tarkastellaan sitä, kuinka demokraattiset yhteiskunnat pystyvät tasapainottamaan kansallisen turvallisuuden [5] ja yksilönvapaudet kasvavien terrorismiuhkien ja teknologisen kehityksen aikakaudella. Yksilönvapaudet viittaavat niihin perusoikeuksiin, jotka takaavat yksilön henkilökohtaisen vapauden ja itsemääräämisoikeuden, kuten henkilökohtainen vapaus, liikkumisvapaus ja sananvapaus (Suomen perustuslaki 2 §). Erityisesti tarkastellaan, miten Euroopan unioni pyrkii turvaamaan kansalaistensa turvallisuuden samalla kunnioittaen heidän perusoikeuksiaan. Tutkielman tavoitteena on jatkaa kandidaatintutkielmassani käsittelemääni perusoikeuksien ja turvallisuuden välistä tasapainoa EU:n terrorisminvastaisessa sääntelyssä. Tässä tutkimuksessa laajennan tarkastelua myös tekoälyteknologioihin ja niiden hyödyntämiseen valvontatoimissa turvallisuutta toteuttaessa.

Kansalaisten toimien valvonta on aina ollut olennainen osa valtioiden hallintaa. [6] Valvonta on nykyteknologian ja tekoälyn avulla huomattavasti yksinkertaistunut, sillä sen avulla voidaan samanaikaisesti seurata laajoja alueita ja suuria ihmisjoukkoja. [7] Terrorismin ja vakavan rikollisuuden torjunta on teknologisen kehityksen myötä mahdollistanut entistä laajamittaisemman valvonnan kohdistamisen yksilöihin. [8] Valvonnan käsite liittyy näin ollen olennaisesti turvallisuuden käsitteeseen. Turvallisuuden varmistaminen ja yhteiskuntajärjestyksen ylläpitäminen ovat valtion keskeisimpiä tehtäviä. [9] Tekoälyteknologian kehitys on tehostanut valvontaa ja parantanut turvallisuutta, mutta samalla herättänyt huolta siitä, kuinka paljon se rajoittaa yksilönvapauksia kuten yksityisyyttä ja henkilötietojen suojaa.[10]

---

[5] Turvallisuus määritellään Euroopan perusoikeuskirjan artiklan 6 mukaan: ”Jokaisella on oikeus vapauteen ja henkilökohtaiseen turvallisuuteen”. Suomen perustuslaissa 7§ taas turvallisuus ja vapaus turvataan sanoin: ”Jokaisella on oikeus elämään sekä henkilökohtaiseen vapauteen, koskemattomuuteen ja turvallisuuteen”.

[6] Locke, 2010, s. 2–3.

[7] Kremer, 2017, s. 21–22.

[8] Wuori, 2003, s. 402.

[9] Jansson, 1969, s. 189.

[10] Koillinen, 2002, s. 172.

Euroopan Unionissa yksi 2000-luvun merkittävimmistä uhista on terrorismin uhka.[11] Terrorismi on ollut ilmiö kuitenkin jopa vuosisatoja aikaisemmin kansainvälisten yhteisöjen huolenaiheena[12] ja nykypäivänä terrorismin torjunta on EU:n kansainvälisen yhteisön suurimmista huolista.[13] Terroristisella teolla aiheutetaan merkittävää haittaa valtiolle tai kansainväliselle organisaatiolle (Suomen rikoslaki 19.12.1889/39 §34 a). Terrorismi ilmiönä asettaa haasteita sekä yksilöiden oikeuksille ja vapauksille että valtioiden kyvylle suojella kansalaisiaan. Teknologian kehitys on tuonut mukanaan uusia keinoja terrorismin torjuntaan, ja tekoälyn sekä automaattisten valvontajärjestelmien käyttö on yleistynyt nopeasti. Tekoälyä hyödynnetään nykyisin muun muassa tiedustelussa, riskianalyyseissä ja kasvojentunnistuksessa.[14]

Kasvojentunnistusteknologiaa voidaan hyödyntää esimerkiksi yksilöiden tunnistamiseen reaaliaikaisesta videokuvasta tai tallenteista, tiettyjen henkilöiden paikantamisessa ja liikkeiden seurannassa julkisilla paikoilla. Näiden järjestelmien myötä julkisten tilojen anonymiteetti vähenee ja tekoäly voi analysoida käyttäytymistä sekä tehdä merkittäviä päätöksiä automaattisesti ilman ihmisen välitöntä puuttumista. Myös kameravalvonnasta on tullut yksi julkisen valvonnan runsaasti hyödynnetyistä keinoista. Rikollisuuden määrä saattaa pienentyä pelkästään kameroiden läsnäolon vuoksi, mikäli mahdolliset rikoksentekijät tiedostavat niiden olemassaolon ja valvonnan.[15] Vaikka tekoälyteknologiaa ei vielä ole laajamittaisesti otettu käyttöön Euroopassa, on sen käyttö kasvanut merkittävästi globaalilla tasolla. Esimerkkinä tästä on Venäjän presidentti Vladimir Putinin hallinnon massiivinen valvontajärjestelmä, jossa kasvojentunnistusteknologiaa on käytetty epälojaaleiksi katsottuja kansalaisia vastaan.[16] Tämä tilanne korostaa tekoälyn valvontakäytön riskejä, kun teknologiaa käytetään valtion vallan vahvistamiseen perusoikeuksien kustannuksella.

[11] Ojanen, 2007, s.1054.
[12] Lappi-Seppälä & muut, 2000, s.1163.
[13] Sisäministeriö, 2022:36, s. 9.
[14] Euroopan parlamentti, 2020 päivitetty 2023.
[15] Rikoksentorjunta.fi, 2021.
[16] YLE, 2024.

Kansalaiset ovat yhä enemmän huolissaan terrori-iskun todennäköisyydestä ja 44 % kansalaisista uskoo terrori-iskun tapahtuvan Suomessa vuoden kuluessa.[17] EU:lla on tärkeä rooli terrorismin torjunnassa ja sen direktiivit ja asetukset vaikuttavat suoraan jäsenvaltioihin, sekä niiden lainsäädäntöön. Etenkin perusoikeuksien asema on vahvistunut EU:n oikeusjärjestyksessä 2000-luvulla.[18] Teknologia kehittyy nopeammin kuin lainsäädäntö. Tekoälyä koskevaa erillislainsäädäntöä EU:ssa ei siis vielä ole, mutta tekoälyn eettistä ja vastuullista käyttöä sääntelevä asetus (Artificial Intelligence Act, AI Act) astui voimaan 1.8.2024.[19] Käsittelen tätä säädöstä vielä myöhemmin lisää.

1.2 Tutkielman tavoitteet, tutkimuskysymykset ja rajaus

Teknologisen kehityksen myötä tekoälyyn perustuvat valvontajärjestelmät ovat alkaneet muokata yhteiskuntamme käsitystä turvallisuudesta ja yksilönvapauksista. Erityisesti Euroopan unionissa on herännyt keskustelua siitä, kuinka pitkälle yksilöiden vapauksia voidaan rajoittaa kansallisen turvallisuuden nimissä ja millainen rooli tekoälyllä on tässä tasapainottelussa.[20] Tämän pro gradu -tutkielman tavoitteena on tutkia EU:n suhtautumista tekoälyyn perustuvaan valvontaan ja selvittää, miten tämä suhtautuminen vaikuttaa yksilönvapauksien toteutumiseen ja turvaamiseen. Tavoitteena on ymmärtää, millaisia mahdollisuuksia ja rajoitteita tekoälypohjainen valvontateknologia asettaa EU:n turvallisuusstrategioille ja perusoikeuksien suojelulle. Ongelma syntyy siitä, kuinka turvallisuutta voidaan lisätä vaarantamatta yksityisyyttä ja luomatta valvontayhteiskuntaa.

Tutkimuksessa pyritään vastaamaan seuraaviin kysymyksiin:

1. Miten tekoälypohjaiset valvontajärjestelmät vaikuttavat yksilönvapauksien ja turvallisuuden tasapainoon Euroopan unionin sääntelyssä?

[17] Taloustutkimus, 2017.
[18] Ojanen, 2009, s.132.
[19] Tekoälyasetus (asetus (EU) 2024/1689) on kaikkien aikojen ensimmäinen tekoälyä koskeva oikeudellinen kehys, jolla puututaan tekoälyn riskeihin ja asetetaan Eurooppa maailmanlaajuiseen johtoasemaan.
[20] Hallamaa, 2020, s.88.

2. Millaisia oikeudellisia ja eettisiä ristiriitoja tekoälyteknologian käyttö aiheuttaa valvontatoimissa EU:ssa ja miten niitä voidaan ratkaista lainsäädännöllä?
3. Miten EU:n tekoälypohjaista valvontaa koskeva sääntely on kehittynyt vuosina 2019–2025?

Näiden kysymysten kautta tutkielma pyrkii kartoittamaan ja ymmärtämään EU:n valvontastrategioihin liittyviä ongelmakohtia ja mahdollisuuksia sekä analysoimaan valvontateknologioiden laajentuneen käytön vaikutuksia erityisesti perusoikeuksien näkökulmasta. Tutkimuskysymysten pohjalta tutkimus jakautuu kolmeen alueeseen, jotka vastaavat tutkimuksen osaongelmiin ja luovat tutkimukselle jäsennellyn rakenteen.

Ensimmäinen osaongelma nostaa esille vuonna 2024 voimaan tulleen EU:n tekoälyasetuksen, [21] joka asettaa erityisiä ehtoja tekoälyn käytölle valvonnassa ja pyrkii samalla kieltämään tietyt korkean riskin sovellukset, jotka voisivat vaarantaa yksilönvapaudet. Valvontateknologioiden avulla pyritään ennaltaehkäisemään turvallisuusuhkia, kuten terrorismia ja vakavaa rikollisuutta, mutta samalla tekoälyn tuoma massavalvonta nostaa esiin kysymyksen yksityisyyden suojan heikkenemisestä. Massavalvonta kasvojentunnistusjärjestelmien avulla on nostattanut kysymyksiä siitä, kuinka paljon kansalaisten jokaista liikettä voidaan seurata tehokkaan ja kaikkialla läsnä olevan valvonnan alla. [22] Tällainen konteksti nostaa esiin haasteita myös EU:ssa, voidaanko samantyyppisiä valvontaratkaisuja perustella turvallisuuspolitiikalla? Tutkielmassa käsittelen ainoastaan henkilötietojen suojaa, koska se on keskeisin perusoikeus, johon tekoälypohjainen valvonta suoraan vaikuttaa. Tämän osan tavoitteena on tutkia, kuinka riittävää ja ajantasaista EU-lainsäädäntö on tekoälyn valvontakäyttöä ajatellen ja miten säädökset turvaavat kansalaisten perusoikeudet.

[21] Euroopan parlamentin ja neuvoston asetus (EU) 2024/1689, annettu 13 päivänä kesäkuuta 2024, tekoälyä koskevista yhdenmukaistetuista säännöistä ja asetusten (EY) N:o 300/2008, (EU) N:o 167/2013, (EU) N:o 168/2013, (EU) 2018/858, (EU) 2018/1139 ja (EU) 2019/2144 sekä direktiivien 2014/90/EU, (EU) 2016/797 ja (EU) 2020/1828 muuttamisesta (tekoälyasetus).
[22] Brown & Korff, 2009, s. 131–132.

Toinen osaongelma tarkastelee tekoälypohjaisten valvontajärjestelmien käyttöön liittyviä eettisiä ja oikeudellisia haasteita. Tekoälyn käyttö valvontateknologioissa tuo mukanaan merkittäviä eettisiä haasteita. Tekoälyyn perustuva kasvojentunnistus mahdollistaa kansalaisten laajamittaisen seurannan, mikä on herättänyt huolta demokratian ja oikeusvaltioperiaatteiden toteutumisesta. Tekoälyvalvonnan oikeudelliset rajat ovat monin osin epäselviä, ja lainsäätäjien tulisi asettaa käyttörajoituksia, jotka huomioivat myös tulevaisuuden teknologiset kehitykset. European Digital Rights (EDRi) -järjestö on nostanut esiin huolen siitä, että tekoälyn laajamittainen käyttö voi vaarantaa perusoikeudet erityisesti silloin, kun yksityisyydensuoja jää toissijaiseksi turvallisuuspolitiikan tavoitteiden saavuttamisessa.[23] Tätä tutkimusongelmaa lähestyessä nostan esille tapauksia, joissa tekoälyteknologioiden käyttö on mennyt liian pitkälle.

Kolmas tutkimuskysymys tarkastelee sitä, kuinka EU:n lainsäädäntöpäätökset ovat reagoineet tekoälyn ja automaattisten valvontajärjestelmien lisääntymiseen 2019–2025 vuosina. EU on julkaissut useita säädöksiä 2000-luvun aikana, jotka vaikuttavat tekoälyn käyttöön valvonnassa, mukaan lukien yleinen tietosuoja-asetus (GDPR), tekoälyasetus (AI Act) sekä terrorismin torjuntaan ja lainvalvontaan liittyvät direktiivit. Samalla Euroopan ihmisoikeustuomioistuin on antanut ratkaisuja, jotka ohjaavat jäsenvaltioiden toimintaa tekoälypohjaisen valvonnan suhteen. Tarkastelen EU:n lainsäädäntöpäätösten kehitystä tekoälyn ja automaattisten valvontajärjestelmien osalta ja analysoin merkittävimmät säädöshankkeet, sekä miten nämä toimet ovat vaikuttaneet valvontateknologioiden käyttöön jäsenvaltioissa. Lisäksi pohdin, missä määrin lainsäädäntö on pystynyt vastaamaan teknologian nopeaan kehitykseen ja mihin suuntaan kehityksen voidaan nähdä menevän tulevaisuudessa.

Tutkimus rajautuu EU alueella toteutettavaan valvontaan ja sen sääntelyyn. Vaikka tapausesimerkkejä tuodaan esille maailmanlaajuisesti tekoälyn käytöstä valvonnassa, tutkielman tarkastelu keskittyy ensisijaisesti EU: n sääntelyyn ja sen vaikutuksiin

[23] EDRi, 2024.

jäsenvaltioiden lainsäädännössä. Näin työ pysyy EU- keskeisenä, mutta tarjoaa kuitenkin kontekstin globaalista kehityksestä ja erilaisten sääntelyjärjestelmien eroista. Tutkimuksessa ei käsitellä yksityisen sektorin valvontakäytäntöjä. Näin tutkimuksen fokus säilyy julkisen sektorin ja EU jäsenvaltioiden lainsäädännössä ja valvontakäytännöissä. Rajaus keskittyy myös nimenomaisesti julkisten tilojen valvontaan liittyviin tekoälyteknologioihin, kuten kasvojentunnistusjärjestelmiin ja massavalvontaan. Tekoälyn käyttöä muilla aloilla kuten terveydenhuollossa tai finanssisektorilla ei käsitellä, jotta tutkimus voi keskittyä tekoälyn rooliin turvallisuus- ja valvontakontekstissa. Rajauksen vuoksi tämä tutkielma käsittelee ainoastaan tietosuojaan liittyviä kysymyksiä. Vaikka tutkielmassa käsitellään ongelmallisia valvontateknologioita ja niiden vaikutuksia perusoikeuksiin, tarkastelu rajautuu näiden teknologioiden sääntelyyn ja oikeudellisiin ulottuvuuksiin. Tutkielmassa ei käsitellä rangaistusvastuuta, rikosoikeudellisia seuraamuksia tai niiden soveltamiskäytäntöjä.

Tutkimus toteutetaan lainopillisena analyysinä, jossa keskitytään oikeudellisiin lähteisiin, kuten EU-lainsäädäntöön, kansallisiin säädöksiin ja oikeuskäytäntöihin, jättäen poliittiset ja taloudelliset näkökulmat vähemmälle huomiolle. EU:n tekoälyyn liittyvä sääntelykehys on myös tutkimuksen keskiössä. Tämä kehys sisältää erityisesti EU:n tekoälyasetuksen. Perusoikeuksien varsinainen sisältö ei käy ilmi yksinomaan lain sanamuodosta, vaan hahmottuu vasta tulkinnan ja oikeudellisen soveltamiskäytännön kautta. Tutkimus on merkityksellinen myös siksi, että turvallisuuden tulkitseminen perusoikeudeksi voi paljastaa yksilön intressien ja julkisen vallan kollektiivisten päämäärien mahdolliset yhtymäkohdat tai ristiriidat. Julkisen vallan ja yksilön tavoitteet eivät aina kohtaa täysin, jolloin ristiriitatilanteissa kyse onkin siitä, minkä periaatteen pohjalta ratkaisut tehdään.[24]

[24] Tuori, 1999, s. 920.

1.3 Tutkielman rakenne ja metodi

Tässä tutkimuksessa käytän ensisijaisesti oikeusdogmaattista eli lainopillista tutkimusotetta, jossa pyrin tarkastelemaan ja analysoimaan voimassa olevaa oikeutta, sekä tiedonintressini on sääntelyn vaikutuksia arvioiva.[25] Lainopilla on katsottu olevan perinteisesti sekä tulkinta- että systematisointitehtävä arvioiden säädöksien soveltamista käytännössä. [26] Tulkinnan kautta lainoppi selvittää voimassa olevien oikeusnormien sisältöä.[27] Kyseessä on tällöin tulkintalainoppi eli käytännöllinen lainoppi, johon sisältyy myös oikeusperiaatteiden punninta ja tasapainottaminen. Tutkielman tavoitteena on analysoida esimerkiksi tekoälyasetuksen artikloja ja niiden vaikutusta valvontatoimiin, mikä tekee tutkimuksesta tulkintalainopillisen. Tutkimus pyrkii systematisoimaan ja selkeyttämään oikeudellisia normeja ja niiden tulkintaa.

Tämä metodi sopii erityisen hyvin tutkimukseen, koska tutkimuksen pääpaino on EU:n lainsäädännössä ja sen vaikutuksissa kansalaisten perusoikeuksiin, erityisesti EU:n perusoikeuskirjan, terrorisminvastaisen sääntelyn ja kansallisen lainsäädännön analysoinnissa. Lisäksi tutkimus käsittelee Euroopan ihmisoikeustuomioistuimen ratkaisukäytäntöä, jonka avulla saadaan konkreettisia esimerkkejä tutkielman rinnalle. Husa määrittelee oikeusdogmatiikan korostuvan epätietoisuudesta oikeusjärjestyksen sisällössä.[28] Tämä epätietoisuus on toiminut vaikuttimena myös omassa tutkimuksessani, koska lainsäädäntö on tapauskohtaisesti kuitenkin tulkinnanvaraista. Käytännölliseksi lainopiksi kutsuttu tulkinta sisältää myös periaatteiden punninnan[29]. Juuri tämä korostuu tutkielmassani, kun hahmotan asetuksen periaatteiden merkitystä ja sisältöä perusoikeuksien rajoittamisen näkökulmasta. Oikeusdogmatiikka auttaa hahmottamaan terrorisminvastaisen sääntelyn monimutkaisuutta. Oikeusdogmatiikka tulkitsee ja systematisoi voimassa olevaa lakia.[30]

---

[25] Kolehmainen, 2015, s.2.
[26] Hirvonen, 2011, s. 21–22.
[27] Aarnio, 1989, s. 304 ja Hirvonen, 2011, s. 22.
[28] Husa, Mutanen & Pohjolainen, 2008, s. 20.
[29] Hirvonen, 2011, s. 24.
[30] Hirvonen, 2011, s. 25.

Vaikka tutkimus on pääosin oikeusdogmaattinen, siinä voidaan viitata myös vertailevaan tutkimusotteeseen erityisesti silloin, kun analysoidaan, miten valvontatoimia on toteutettu kansainvälisesti sekä Suomessa. Vertailevan otteen avulla voidaan tarkastella, miten eri oikeusjärjestelmät käsittelevät turvallisuuden ja vapauden välistä jännitettä ja löytää ratkaisuja siihen, miten EU:n lainsäädäntöä voidaan kehittää suojelemaan perusoikeuksia paremmin.[31] Lisäksi tutkimuksessa sovelletaan empiiristä tarkastelua EU:n päätöksiin tekoälysääntelyn osalta. Empiirinen osuus toteutettiin dokumenttianalyysina, jossa tarkasteltiin EU:n lainsäädäntöasiakirjoja, komission tiedonantoja ja parlamentin päätöslauselmia vuosilta 2019–2025. Aineisto kerättiin Euroopan unionin virallisesta lähteestä (EUR-Lex-tietokanta) käyttäen hakutermiä *'tekoäly'*. Dokumenttien analyysissä keskityttiin siihen, kuinka monta kertaa tekoäly mainitaan valvontayhteyksissä ja miten sen sääntelyä perustellaan turvallisuuden ja yksilönvapauksien näkökulmasta.

Tutkimuksessa viittaan yleiseen oikeuskäytäntöön ja lainsäädäntöön.[32] Tutkimusongelmaan voidaan vastata analysoimalla oikeuslähteitä, kuten EU-lainsäädäntöä, kansallisia säädöksiä, kansainvälisiä sopimuksia sekä keskeisiä oikeustapauksia. Tutkimuksen keskeisiä oikeuslähteitä ovat EU:n perusoikeuskirja (2000/C 364/01), Terrorismirikosdirektiivi (2017/541), Tekoälyasetus (EU) 2024/1689, Suomen perustuslaki (731/1999) ja Rikoslaki (19.12.1889/39). Oikeuskäytännössä merkittäviä ovat esimerkiksi Euroopan ihmisoikeustuomioistuimen (EIT) ja Euroopan unionin tuomioistuimen (EUT) ratkaisut, joissa on käsitelty terrorismin torjunnan ja perusoikeuksien suhdetta. Tutkielmassa hyödynnetään myös hallituksen esityksiä (HE) sekä Euroopan komission tiedonantoja (COM) oikeudellisen argumentaation ja säädöspoliittisten taustojen selventämiseksi.

Keskeistä aiempaa tutkimusta aiheesta löytyy muun muassa Ojaselta (2009), joka on tutkinut perusoikeuksien ja turvallisuuden välistä tasapainoa erityisesti EU kontekstissa.

---

[31] Hirvonen, 2011, s.54.
[32] Ojanen, 2009, s.132.

Bruun (2016) on puolestaan syventynyt EU:n sisäisen turvallisuuden strategioihin ja niiden vaikutuksiin perusoikeuksien toteutumiseen. Scheinin (2009) on analysoinut ihmisoikeuksien suojelun ja terrorismin torjunnan suhdetta globaalissa mittakaavassa. Lisäksi Viljanen (2001) on käsitellyt perusoikeuksien rajoittamisedellytyksiä Suomen kontekstissa ja tarjonnut laajan katsauksen siihen, millä perusteilla perusoikeuksia voidaan rajoittaa. Widlund (2020) on tarkastellut kansallisen turvallisuuden käsitettä perusoikeuksien näkökulmasta, pohtien turvallisuuden roolia vapauden edellytyksenä ja toisaalta sen rajoittajana. Aihetta on käsitelty viimeksi muissa pro gradu -tutkielmissa kuten Anni Kaarento (2024) *”Biometrinen etätunnistaminen rikostorjunnassa henkilötietojen suojan näkökulmasta*” ja Jonna Kela (2023) ”*Eurooppalainen tekoäly – Millaista oikeudellista alustaa Euroopan unioni luo tekoälylle?*”.

Vaikka terrorisminvastainen sääntely ja perusoikeuksien suoja ovat laajasti tutkittuja, tutkimusaukko liittyy siihen, miten EU-sääntelyn vaikutukset perusoikeuksiin toteutuvat jäsenvaltioissa käytännössä. Aiemmat tutkimukset ovat painottaneet EU-sääntelyn yleisiä periaatteita, mutta konkreettinen analyysi, erityisesti tekoälyn ja valvontateknologian näkökulmasta on vielä vähäistä. Tekoälyasetuksen vaikutuksia lainvalvontaan ja perusoikeuksiin ei ole kattavasti analysoitu, mikä tekee tästä tutkimuksesta ajankohtaisen, sekä tarpeellisen. Tutkielma on tärkeä, koska se pyrkii antamaan syvällisen analyysin siitä, miten EU:n terrorisminvastaiset toimet ja perusoikeuksien suoja kohtaavat käytännössä, sekä millaisia oikeudellisia ja eettisiä ongelmia näihin liittyy. Lisäksi on vähemmän tutkittu sitä, kuinka uudet turvallisuusuhat, kuten kyberterrorismi, vaikuttavat tulevaisuudessa EU:n lainsäädäntöön.

Tutkielma etenee loogisesti ja systemaattisesti alkaen johdantoluvusta, jossa esitellään tutkimuksen tausta, tavoitteet, tutkimuskysymykset ja rakenne. Toinen luku käsittelee turvallisuutta perusoikeutena, tarkastellen ensin perusoikeuksien määritelmää ja kehitystä keskittyen erityisesti henkilötietojen suojaan. Luvussa käsitellään myös henkilökohtaisen vapauden ja turvallisuuden suhdetta sekä analysoidaan EU:n turvallisuusunionistrategiaa vuosille 2020–2025. Luvun lopuksi tarkastellaan

perusoikeuksien rajoitusedellytyksiä, joiden avulla arvioidaan, missä tilanteissa ja millä perusteilla yksilönvapauksia voidaan rajoittaa turvallisuuden nimissä.

Kolmannessa luvussa siirrytään tekoälyteknologian valvontakäyttöön. Luvussa tarkastellaan, miten tekoälyä hyödynnetään nykypäivänä yhä enemmän kansallisen turvallisuuden takaamisessa ja uhkien tunnistamisessa. Tässä yhteydessä analysoidaan erityisesti tiedustelu- ja valvontateknologioiden, kuten kasvojentunnistuksen ja muun biometrisen valvonnan roolia. Lisäksi luvussa käsitellään tekoälyn käytön eettisiä ja ihmisoikeudellisia ongelmia sekä valvontateknologioiden merkitystä terrorismin torjunnassa. Neljäs luku keskittyy tekoälyasetuksen vaikutuksiin EU:n oikeudellisessa perustassa. Luvussa analysoidaan tekoälyasetuksen ja perusoikeuksien välisiä jännitteitä ja pohditaan, miten sääntely voi tasapainottaa turvallisuuden ja yksilönvapauksien suojan. Lisäksi arvioidaan empiirisesti EU: n päätöksiä tekoälysääntelyn kehittyessä vuosina 2019–2025. Luvun lopussa punnitaan vielä tekoälyn ja tekoälyasetuksen roolia EU: n lainsäädännön tulevaisuudessa.

Viimeisessä luvussa kootaan yhteen tutkimuksen keskeiset havainnot ja johtopäätökset, sekä arvioidaan, kuinka tutkimuskysymyksiin on onnistuttu vastaamaan. Johtopäätöksissä käsitellään myös työn merkitystä ja pohditaan, millaisia jatkotutkimusaiheita tekoälyyn perustuvan valvonnan ja lainsäädännön kehitykseen voisi liittyä tulevaisuudessa. Onko tulevaisuutemme hallittu turvallisuusyhteiskunta vai valvontadystopia? Tätä tasapainoa etsiessään EU pyrkii luomaan sääntelykehikon, joka turvaa kansalaisten oikeudet samalla, kun se vastaa uudenlaisiin turvallisuusuhkiin. Tässä tutkielmassa tarkastellaan, miten EU:n lainsäädäntö ja perusoikeuskehikko ohjaavat tekoälyteknologian käyttöä valvontatarkoituksissa ja miten tämä vaikuttaa yksilönvapauksien ja turvallisuuden väliseen suhteeseen tulevaisuudessa.

2 Turvallisuus perusoikeutena

Viime vuosikymmenien aikana Euroopan unionin turvallisuusympäristö on kokenut merkittäviä muutoksia. Globaalin turvallisuustilanteen epävakaus, kansainvälisen terrorismin kasvava uhka, sekä kyber- ja informaatioturvallisuuden haasteet ovat pakottaneet EU:n jäsenvaltiot arvioimaan uudelleen turvallisuuspolitiikkaa ja tiedustelutoimintojen merkitystä. Näissä muuttuvissa olosuhteissa tiedustelutoiminta on noussut avainasemaan EU:n turvallisuusstrategiassa, jossa keskeisenä tavoitteena on unionin ja sen kansalaisten turvallisuuden varmistaminen.

2.1 Perusoikeuksien määritelmä

Perusoikeudet ovat keskeinen osa Euroopan unionin oikeusjärjestystä ja ne muodostavat perustan EU:n oikeudelliselle kehykselle. EU-oikeus voidaan jakaa primääriseen ja sekundääriseen oikeuteen, jolloin sekundäärinen ei saa olla ristiriidassa primäärisen oikeuden kanssa[33]. EU:n perusoikeudet suojaavat kansalaisten oikeuksia ja vapauksia EU:n toiminnan ja lainsäädännön puitteissa. Kansa voidaan tulkita tarkoittamaan joko kansalaisyhteiskuntaa tai yhteiskuntaa, joka on erityissuhteessa valtioon [34] . Perusoikeuksien tarkoitus on erityisesti taata yksilöille suojaa ja oikeusturvaa EU-oikeuden puitteissa. Perusoikeuksiksi katsotaan yleensä sellaiset oikeudet, joita pidetään yksilön kannalta perustavanlaatuisina ja erityisen tärkeinä, ja jotka siksi on kirjattu perustuslailliseen tasoon [35] . Suomen perustuslaki (731/1999) ja Euroopan unionin perusoikeuskirja (2000/C 364/01) perustuvat samankaltaisiin arvoihin, kuten ihmisoikeuksien kunnioittamiseen, demokratiaan ja oikeusvaltioperiaatteeseen.

Euroopan Unionin perusoikeuskirja on oikeudellisesti sitova EU:n asiakirja, jota EU:n toimielimet ja jäsenvaltiot ovat velvoitettuja noudattamaan. Perusoikeuskirjalla halutaan taata yhteiskunnan muutos, sosiaalinen edistys, sekä tieteen ja tekniikan

[33] Ojanen, 2016, s.50.
[34] Bruun, 2016, s. 246.
[35] Hallberg, 2005.

kehitys. Euroopan Unionin perusoikeuskirja on hyväksytty vuonna 2000 ja se on tullut oikeudellisesti sitovaksi 2009 Lissabonin sopimuksen myötä.[36] Tämä asiakirja luo yhtenäisen ja vahvan perustan perusoikeuksien suojelulle EU:ssa. Perusoikeuskirjan 52 artiklan mukaan oikeuksia ja vapauksia voi rajoittaa ainoastaan suhteellisuusperiaatteen mukaisesti, mikäli rajoitukset ovat välttämättömiä ja vastaavat tarvetta suojella oikeuksia ja vapauksia. Suhteellisuusperiaate edellyttää, että EU:n toimielinten säädökset, päätökset ja muut toimenpiteet eivät saa ylittää tarpeellisia rajoja, jotka liittyvät lainmukaisesti tavoiteltujen päämäärien saavuttamiseen, eivätkä aiheuta kohtuuttoman suuria haittoja verrattuna näihin päämääriin[37]. EIT:n tapauksessa Saksan laki salli viranomaisille laajat valtuudet puhelinten salakuunteluun kansallisen turvallisuuden vuoksi. EIT totesi, että jo pelkkä telekuuntelua sallivan lain olemassaolo merkitsee puuttumista yksilön yksityiselämän suojaan. Tapaus asetti tärkeän ennakkoperiaatteen, jonka mukaan salainen valvonta on sallittua vain tarkoin lailla rajatuissa tilanteissa, ja siihen on liityttävä tehokkaat valvontamekanismit mielivallan estämiseksi.[38]

EU:n perusoikeuskirjan määräykset sitovat kaikkia unionin toimielimiä ja laitoksia[39]. Perusoikeuskirjan 51 artikla kertoo perusoikeuksien velvoittavan kaikkia unionin toimielimiä, laitoksia toissijaisuusperiaatteen mukaisesti. Toissijaisuusperiaate tarkoittaa, että EU toimii vain silloin, kun jäsenvaltiot eivät kykene tehokkaasti saavuttamaan tavoitteitaan keskushallinnon, aluehallinnon tai paikallishallinnon tasolla, sekä kun nämä tavoitteet voidaan paremmin saavuttaa EU:n toiminnan laajuuden ja vaikutusten vuoksi (SEU 5.3 artikla). Perusoikeuskirjan määräykset velvoittavat jäsenvaltioita silloin, kun ne toimivat EU-oikeuden soveltamisen yhteydessä. Perusoikeuskirja on EU-oikeuden perusta ja siksi perusoikeuskirja kuuluu EU:n primäärioikeuden joukkoon ja toimii tulkinnan ja pätevyyden mittarina sekundäärioikeudelle ja EU-oikeuden kansalliselle oikeudelle[40]. Ojanen nostaa esille kaikkea EU-oikeutta sovellettavan osin perusoikeuksiin,

[36] Hallberg, 2005.
[37] Ojanen, 2016, s. 165.
[38] EIT 06.09.1978.
[39] Ojanen, 2016, s. 157.
[40] Ojanen, 2016, s. 40.

vaikka niillä ei ole etusijaa muihin primäärioikeuksiin[41]. Jos Euroopan unionista tehdyn sopimuksen (SEU) 2 artiklassa mainittujen arvojen, kuten oikeusvaltion, demokratian ja ihmisoikeuksien kunnioittamisen toteutumisessa on puutteita, sekä Euroopan unioni että sen jäsenvaltiot altistuvat sisäisille ja ulkoisille uhille.[42]

2.1.1 Henkilötietojen suoja

Yksi keskeinen moderni perusoikeus on henkilötietojen suoja, johon tekoälyvalvonta läheisesti kytkeytyy. Henkilötiedoilla tarkoitetaan kaikenlaisia merkintöjä henkilöstä, josta tämän voisi tunnistaa, kun taas henkilötietojen käsittely on kaikenlaista henkilötietoihin liittyvää käsittelyä.[43] Henkilötiedot kattavat myös tiedot, jotka voidaan yhdistää muihin tietoihin henkilön tunnistamiseksi.[44] *”Tietojen käsittelyn on oltava asianmukaista ja sen on tapahduttava tiettyä tarkoitusta varten ja asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla”* (Perusoikeuskirja 8 artikla). Tekoälyasetus myös korostaa henkilötietojen suojan merkitystä, viitaten erityisesti yleiseen tietosuoja-asetukseen (EU 2016/679) ja asetukseen (EU 2018/1725), jotka säätelevät henkilötietojen käsittelyä EU:ssa. Tekoälyjärjestelmien kehittämisessä ja käytössä on noudatettava näitä säädöksiä varmistaen, että henkilötietojen käsittely on lainmukaista, oikeudenmukaista ja läpinäkyvää (Tekoälyasetus (EU) 2024/1689).

Yksityisyydensuojan periaatteet EU:ssa muodostavat perustan sille, miten henkilötietoja kerätään, käsitellään ja suojataan Euroopan unionissa.[45] Henkilötietojen suojan periaatteita ovat lainmukaisuus, oikeudenmukaisuus ja läpinäkyvyys, tarkoituksen rajoittaminen, tietojen minimointi, tarkkuus, säilytyksen rajoittaminen, eheys ja luottamuksellisuus sekä vastuuvelvollisuus.[46] Henkilötietojensuoja on yhdenmukaistettu

[41] Ojanen, 2009, s. 132.
[42] Mäntylä, 2023, s. 7.
[43] Korhonen, 2005, s. 32.
[44] Taka, 2017, s. 140–141.
[45] Pekola, 2018, s.15.
[46] Kalliojärvi, 2016, s. 31–33.

EU:ssa, mutta jäsenvaltioiden välillä on merkittäviä eroja yksityisyydensuojan ja henkilötietojen suojan täytäntöönpanossa kansallisissa laeissa ja käytännöissä. Henkilötietojen käsittelyssä on noudatettava asianmukaisia lakeja, kuten henkilötietojen käsittelystä poliisitoiminnassa annettua lakia (761/2003), henkilötietolakia (535/1999) ja julkisuuslakia (621/1999).[47] Henkilötietolain 32.1 § edellyttää, että rekisterinpitäjä ryhtyy tarpeellisiin teknisiin ja organisatorisiin toimiin suojatakseen henkilötiedot asiattomalta käytöltä sekä vahingossa tai lainvastaisesti tapahtuvalta käsittelyltä. Henkilötietojen, kuten sormenjälkien säilyttäminen poliisin rekisterissä koskettaa Euroopan ihmisoikeussopimuksen (EIS) 8 artiklan mukaista yksityiselämän suojaa ja siihen puuttumisen on oltava lainmukaisesti perusteltua ja oikeasuhtaisesti toteutettua. Henkilötietojen rekisteröinnin on tarjottava riittävää suojaa mielivaltaa vastaan, ja rekisterissä olevien tietojen on oltava relevantteja sekä sisällöltään että säilytysajaltaan rajattuja rekisteröinnin tavoitteisiin nähden.[48]

Suurien tietomäärien käsittely digitaalisessa ympäristössä on tuonut mukanaan uusia tietoturvauhkia ja mahdollistanut uudenlaisia rikollisuuden muotoja. Etenkin henkilötietojen suoja on noussut keskeiseksi aiheeksi digitaaliaikana, kun yhä enemmän henkilökohtaisia tietoja kerätään ja käsitellään.[49] Euroopan unionin alueella on 2018 voimaan tullut yleinen tietosuoja-asetus (GDPR) antaa yksilöille oikeuden hallita omia henkilötietojaan ja suojella niitä väärinkäytöksiltä. Tietosuoja-asetus nostaa esille rekisteröidyn oikeudet, joihin kuuluu oikeus tarkastaa omat tietonsa, vaatia virheellisten tietojen oikaisua, pyytää tietojen poistamista sekä vastustaa henkilötietojen käsittelyä.[50] Sen oikeusperustana on SEUT 16 artikla, jonka mukaan jokaisella on oikeus henkilötietojensa suojaan.[51] GDPR ei kata oikeushenkilöiden henkilötietojen käsittelyä.[52] Henkilötietojen käsittely kattaa toiminnot tiedon keräämisestä sen hävittämiseen, mikä

[47] Korhonen, 2005, s.56.
[48] EIT 18.04.2013.
[49] Kalliojärvi, 2016, s.16.
[50] Hanninen & muut, 2017, s.13–15.
[51] Raitio, 2016, s.105.
[52] Taka, 2017, s. 32–33.

korostaa vastuuta säilyttää yksityisyys kaikissa tietoelinkaaren vaiheissa.[53] GDPR vahvistaa yksityisyyden suojaa asettamalla sanktioita tietosuojan rikkomuksista edistäen vastuullista datankäsittelyä digitaalisessa ympäristössä.[54] Sen täydentävässä lainsäädännössä korostetaan avoimuuden, tarkoituksenmukaisuuden ja minimoimisen periaatteita.[55]

Kameravalvonta on keskeinen osa julkisten ja yksityisten tilojen turvallisuutta, mutta sen käyttöön liittyy merkittäviä oikeudellisia ja eettisiä kysymyksiä. GDPR antaa yksilöille oikeuden hallita omia henkilötietojaan ja suojella niitä väärinkäytöksiltä.[56] GDPR sekä sitä tarkentava tietosuojalaki (1050/2018) säätelevät kameravalvontaa ja henkilötietojen käsittelyä videovalvonnan yhteydessä. GDPR:n 4 artiklan 1 kohdan mukaan henkilötiedoiksi katsotaan kaikki tiedot, joista yksilö voidaan tunnistaa. Näin ollen myös videomateriaali ja tallennettu ääni ovat henkilötietoja, jos niistä voidaan tunnistaa henkilö. Tämä tarkoittaa, että kameravalvonnan yhteydessä käsiteltäviä tietoja tulee käsitellä samalla tavalla kuin mitä tahansa muita henkilötietoja, kuten nimiä tai yhteystietoja. Henkilötietojen käsittely kameravalvonnassa edellyttää aina GDPR:n 6 artiklan mukaista käsittelyperustetta, jotta se on lainmukaista. Käytännössä kameravalvonnassa yleisimmät käsittelyperusteet ovat:

1. *6 artiklan 1 kohdan e alakohta, jonka mukaan tietojen käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai julkisen vallan käyttämiseksi.*
2. *6 artiklan 1 kohdan f alakohta, jonka mukaan käsittely on tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi.*

Valvontaviranomaisten rooli liittyy tietosuojavaltuutetun tehtävään valvoa henkilötietojen käsittelyn lainmukaisuutta.[57] GDPR asettaa tiukat vaatimukset

[53] Sanjay, 2020, s.45–47.
[54] Sanjay, 2020, s.17.
[55] HE 9/2018, s. 2.
[56] Hanninen & muut, 2017, s.13.
[57] Pekola, 2018, s.61–77.

henkilötietojen siirtämiselle EU:n ulkopuolisiin maihin, varmistaen, että henkilötietojen suojan taso säilyy myös tietojen siirrossa.[58] GDPR tunnustaa tietosuojan perusoikeudeksi EU:ssa, mutta se ei ole absoluuttinen oikeus. Rajoitukset ovat sallittuja tietyissä olosuhteissa, kunhan ne ovat lain mukaisia ja täyttävät EU:n tai muiden tunnustettujen yleisen edun tavoitteet. [59] Kuitenkin GDPR:n laaja soveltamisala ja jotkut epäselvät käsitteet, kuten *"käyttäytymisen seuranta",* voivat aiheuttaa juridista epävarmuutta ja haasteita sekä EU:n sisällä että kansainvälisesti. Tämä korostaa tarvetta jatkuvasti arvioida ja tulkita GDPR:n säännöksiä huomioiden teknologian kehitys ja kansainvälinen yhteistyö. [60] EIT:n tapaus käsitteli Ison-Britannian 9/11-iskujen jälkeen omaksumaa poikkeustoimea, jossa useita ulkomaalaisia terroristiepäiltyjä pidettiin vangittuina toistaiseksi ilman syytettä. Tuomioistuin totesi, että ulkomaalaisten epäiltyjen määräaikainen, toistaiseksi jatkuva säilöönotto ilman syytettä rikkoi oikeutta henkilökohtaiseen vapauteen (EIS 5 artikla) eikä ollut välttämätöntä demokraattisessa yhteiskunnassa. [61]

Lisäksi Euroopan tietosuojaneuvosto (European Data Protection Board, EDPB) on laatinut ohjeita tietosuoja-asetuksen soveltamisesta videolaitteilla toteutettuun valvontaan. GDPR rajoittaa biometrisen tiedon keruuta ilman selkeää suostumusta, mikä estää esimerkiksi tekoälypohjaisten valvontajärjestelmien vapaan käytön julkisissa tiloissa.[62] GDPR lähtökohtaisesti kieltää täysin automatisoidun päätöksenteon, paitsi jos henkilö on antanut siihen suostumuksensa tai siitä on säädetty laissa, joka samalla takaa yksilölle riittävät suojatoimet.[63] Kameravalvontaa harjoittavan organisaation tulee laatia 30 artiklan mukainen seloste käsittelytoimista, jossa kuvataan, miten henkilötietoja käsitellään ja mihin tarkoitukseen niitä käytetään. Lisäksi rekisteröidyt ovat informoitava tietojen käsittelystä 13 artiklan mukaisesti, mikä tarkoittaa muun muassa sitä, että

[58] Taka, 2017, s. 127.
[59] Taka, 2017, s.23.
[60] Taka, 2017, s.143.
[61] EIT 19.02.2009.
[62] Haenlein & Kaplanin, 2019, s. 8.
[63] Raskulla, 2023, s. 11.

kameravalvonnasta on ilmoitettava selkein varoituskyltin. Rekisteröityjen oikeuksien osalta 15 artiklassa määritetään yksilön oikeus saada pääsy tietoihinsa (GDPR 2016/679).

Nykyteknologia tekee henkilötiedoista läpinäkyviä ja helposti jaettavia. Tämä korostaa tarvetta laajalle ja harkitulle lainsäädännölle, joka rajoittaa ja valvoo yksityisyyden loukkauksia sekä luo vahvoja normeja tiedon jakamiselle ja suojaamiselle. [64] Tietosuojalainsäädännön periaatteet voidaan jakaa yleisiin periaatteisiin, jotka koskevat kaikkia, henkilötietojen käsittelijöitä koskeviin periaatteisiin sekä yksilön oikeuksia koskeviin periaatteisiin. Yleiset periaatteet kattavat muun muassa lakisääteisyyden, avoimuuden, tarpeellisuuden ja tietoturvan. Henkilötietojen käsittelijöitä koskevat periaatteet sisältävät esimerkiksi tarpeellisuuden ja huolellisuusvelvoitteen, kun taas yksilön oikeuksiin liittyvät periaatteet korostavat suostumuksen ensisijaisuutta ja tarkastusoikeutta.[65] Euroopan tietosuojadirektiivissä (direktiivi 95/46/EY), määritellään periaatteita datanvalvojille ja -käsittelijöille sekä oikeuksia tiedon kohteille, ja miten näitä periaatteita on haastettu EU:n turvallisuuspolitiikalla.[66]

2.1.2 Henkilökohtainen vapaus ja turvallisuus

Kansallisen turvallisuuden kannalta yhteiskunnan keskeisiä toimintoja ovat muun muassa valtionhallinto, kansainvälinen yhteistyö, puolustusvalmius, sisäinen turvallisuus, talous- ja infrastruktuurijärjestelmien toiminta, väestön toimeentulo ja toimintakyky sekä psyykkinen kriisinkestävyys. Mietinnön mukaan uhkia kansalliselle turvallisuudelle muodostavat ne tekijät, jotka kohdistuvat näihin yhteiskunnan perustoimintoihin. [67] Yksilön vapauksia ei saa rajoittaa kohtuuttomasti ja toimenpiteiden on oltava oikeasuhteisia ja välttämättömiä uhkan torjumiseksi. Kansallisen turvallisuuden kannalta uhka kohdistuu useimmiten koko yhteiskuntaan, valtioon tai muuhun laajaan kollektiiviseen ryhmään, kuten tiettyyn kansanryhmään. [68] Jäsenvaltion ottaessa

[64] Sanjay, 2020, s.5.
[65] Kalliojärvi, 2016, s. 31.
[66] Gonçalves & muut, 2013.
[67] Puolustusministeriö, 2010, s. 1–3.
[68] Widlund, 2020, s.141.

käyttöön toimenpiteitä rajoittaen niillä perusoikeuksia, pelkkä vetoaminen kansalliseen turvallisuuteen ei riitä, vaan jäsenvaltion vastuulla on myös perustella rajoituksen tarve.[69]

Henkilökohtainen turvallisuus on yksilön oikeus elää ja liikkua turvallisesti ilman pelkoa. Turvallisuus perusoikeutena voidaan nähdä epäitsenäisenä ja yksilökohtaiseen vapauteen liittyvänä oikeutena [70] . *”Korostaa julkisen vallan positiivisia toimintavelvoitteita yhteiskunnan jäsenten suojaamiseksi rikoksilta ja muilta heihin kohdistuvilta oikeudenvastaisilta teoilta, olivatpa niiden tekijät julkisen vallan käyttäjiä tai yksityisiä tahoja.” [71]* Turvallisuuden käsite voidaan jakaa kahteen turvallisuuden ulottuvuuteen, jotka ovat yksilöllinen ja kollektiivinen. Yksilöllinen turvallisuus tarkoittaa sekä yksilön oikeutta tulla suojatuksi että hänen subjektiivista kokemustaan turvassa olemisesta. Kollektiivinen turvallisuus puolestaan jakautuu yleiseen yhteiskuntarauhaan (public safety) ja kansalliseen turvallisuuteen (national security). [72] Kun yksilöllinen ja kollektiivinen turvallisuus toteutuvat rinnakkain, voidaan turvallisuutta pitää sekä yksilön oikeutena että perusteltuna syynä perusoikeuksien rajoittamiselle. [73] Perinteisesti turvallisuus on nähty valtion ylläpitämänä järjestyksenä, jossa julkinen valta käyttää valvontatoimia rikollisuuden torjumiseksi.

Euroopan unionin perusoikeuskirja kokoaa yhteen, vahvistaa ja suojaa perusoikeuksien toteutumista kaikille EU:n kansalaisille, sekä sillä halutaan myös taata turvallisuus jokaiselle. Perusoikeuskirjan 6 artikla muotoilee turvallisuuden seuraavasti: ”*Jokaisella on oikeus vapauteen ja henkilökohtaiseen turvallisuuteen*”. [74] Tämä korostaa yksilöiden oikeutta kokea olonsa turvalliseksi ja suojatuksi, joka voi toteutua esimerkiksi vapaalla liikkuvuudella ilman pelkoa väkivallasta, tehokkaalla poliisi toiminnalla ja huolenpidolla yhteiskunnan heikoimmassa asemassa olevista. Bruun nostaa esille EU:n sisäisen

[69] Ojanen, 2016, s. 165.
[70] Bruun, 2016, s. 248.
[71] HE 309/1993 vp, s. 3.
[72] Tuori, 1999, s. 923.
[73] Tuori, 1999, s. 920.
[74] Bruun, 2016, s. 245.

turvallisuuden strategiassa 2007 mainittavan turvallisuuden olevan perusoikeus [75]. Tekoälyasetuksessa pyritään takaamaan turvallisuuden toteutuminen korkean turvallisuustason tekoälyjärjestelmien käytössä. Tämä sisältää riskienhallintatoimenpiteet, joilla pyritään estämään tekoälyjärjestelmien mahdolliset haitalliset vaikutukset yksilöiden turvallisuuteen ja perusoikeuksiin (Tekoälyasetus (EU) 2024/1689).

2.2 EU:n turvallisuusunioninstrategia 2020–2025

Euroopan komissio on laatinut EU:n turvallisuusunioninstrategian vuosille 2020–2025 joka määrittelee Euroopan unionin lähestymistavan turvallisuuden varmistamiseen muuttuvassa uhkaympäristössä. Turvallisuusunioninstrategia 2020–2025 ei ainoastaan keskity perinteiseen rikostorjuntaan, vaan se myös avaa mahdollisuuden tekoälyn käyttöön turvallisuuden lisäämiseksi. EU:n turvallisuusunionistrategian painopisteitä ovat terrorismin ja järjestäytyneen rikollisuuden ehkäisy, kyberturvallisuuden vahvistaminen sekä tiedonvaihdon ja tutkimusyhteistyön edistäminen. [76] Strategia keskittyy neljään pääalueeseen:

1. Tulevaisuuden kannalta kestävän turvallisuusympäristön varmistaminen: Tavoitteena on suojella kriittistä infrastruktuuria ja parantaa kyberturvallisuutta, jotta yhteiskunnan elintärkeät toiminnot voivat jatkua häiriöttä.
2. Muuttuviin uhkiin reagoiminen: Strategia pyrkii torjumaan uusia uhkia, kuten kyberrikollisuutta, laitonta verkkosisältöä ja hybridiuhkia, jotka voivat vaarantaa EU:n turvallisuuden.
3. Euroopan suojeleminen terrorismin ja järjestäytyneen rikollisuuden torjunnan avulla: Tässä keskitytään estämään radikalisoitumista, parantamaan lainvalvontaviranomaisten yhteistyötä ja vahvistamaan rajaturvallisuutta.

[75] Bruun, 2016, s. 257.
[76] COM/2020/605 final, s. 17.

4. Vahvan turvallisuusekosysteemin rakentaminen: Tavoitteena on edistää tiedonvaihtoa, tutkimusta ja innovointia sekä parantaa yhteistyötä eri toimijoiden välillä turvallisuuden takaamiseksi.

Tämä strategia on todistanut turvallisuuden olevan monialainen kysymys, joka ulottuu lähes kaikille elämänalueille ja vaikuttaa moniin politiikanaloihin. Se pyrkii yhdistämään nämä palaset ja luomaan todellisen turvallisuusekosysteemin, jossa digitaalisten ja fyysisten uhkien sekä sisäisten ja ulkoisten turvallisuusnäkökohtien välinen kahtiajako poistetaan. [77] Lisäksi strategia painottaa, että turvallisuus ja perusoikeuksien kunnioittaminen täydentävät toisiaan. Turvallisuustoimien on aina perustuttava yhteisiin arvoihin, kuten demokratiaan, oikeusvaltioperiaatteeseen ja perusoikeuksien kunnioittamiseen.[78] Strategian mukaan uudet teknologiat, kuten tekoäly ja biometrinen valvonta, voivat tuoda lisäarvoa turvallisuuspolitiikkaan, mutta niiden käyttö edellyttää tiukkaa oikeudellista valvontaa. Tämä alleviivaa EU:n sitoutumista perusoikeuksiin turvallisuuspolitiikan kehittämisessä ja tuo esiin sääntelyhaasteet, joita tekoälypohjaisen valvonnan laajentuminen aiheuttaa.[79]

Turvallisuusunioninstrategian (2020–2025) toteutuksessa on jo saavutettu merkittäviä edistysaskeleita. Komission toukokuussa 2024 julkaisema seitsemäs edistymiskertomus osoittaa, että EU on parantanut valmiuksiaan vastata turvallisuushaasteisiin useilla keskeisillä osa-alueilla. EU on kehittänyt uusia välineitä radikalisoitumisen ehkäisemiseksi, kuten koulutusohjelmia ja tiedonvaihtomekanismeja jäsenvaltioiden välillä. Näiden toimien ansiosta on onnistuttu estämään useita terrori-iskuja ja vähentämään radikalisoitumista erityisesti nuorten keskuudessa. EU:n terrorisminvastainen agenda hyväksyttiin joulukuussa 2020, määrittäen toimet terrorismin ehkäisemiseksi. Asetus terroristisen sisällön levittämisen estämisestä verkossa (EU 2021/784) tuli voimaan kesäkuussa 2022, velvoittaen palveluntarjoajat

[77]COM/2020/605 final.
[78] COM/2022/720, johdanto.
[79] COM/2020/605 final, s. 13.

poistamaan terroristista sisältöä nopeasti. EU:n radikalisoitumisen ehkäisyn tietokeskus perustettiin kesäkuussa 2024, edistäen tietojen ja hyvien käytäntöjen vaihtoa jäsenvaltioiden välillä. Lisäksi rajaturvallisuutta ja lainvalvontayhteisöä on vahvistettu Euroopan raja- ja merivartioviraston (Frontex) mandaatin laajentaminen on parantanut EU:n ulkorajojen valvontaa ja yhteistyötä jäsenvaltioiden välillä, sekä Schengenin tietojärjestelmän (SIS) uudistaminen on tehostanut tietojenvaihtoa ja rikollisten tunnistamista EU:n alueella.[80]

Nämä toimet ovat parantaneet EU:n valmiuksia vastata monimuotoisiin turvallisuusuhkiin, kuten kyberhyökkäyksiin, terrorismiin ja järjestäytyneeseen rikollisuuteen, sekä vahvistaneet jäsenvaltioiden välistä yhteistyötä turvallisuuden alalla. Tämä strategia korostaa, että turvallisuuden turvaaminen on koko yhteiskunnan yhteinen tehtävä. Sen toteutus vaatii yhteistyötä EU:n toimielinten, jäsenvaltioiden, yritysten ja kansalaisten välillä. Lisäksi EU pyrkii vahvistamaan yhteistyötä kolmansien maiden ja kansainvälisten organisaatioiden kanssa turvallisuuden edistämiseksi sekä hybridiuhkien ja kyberrikollisuuden torjumiseksi. Näiden toimenpiteiden tarkoituksena on luoda dynaaminen ja tehokas turvallisuusyhteisö, joka vastaa nykypäivän ja tulevaisuuden haasteisiin.[81]

2.3 Perusoikeuksien rajoitusedellytykset

Perus- ja ihmisoikeudet eivät ole täysin ehdottomia, vaan niitä voidaan tietyin edellytyksin rajoittaa. Poikkeuksena ovat eräät ehdottomat oikeudet, kuten kidutuksen ja kuolemanrangaistuksen kielto, joista ei voida poiketa edes poikkeusoloissa tai sodan aikana[82]. Kansallisen turvallisuuden perustavana ajatuksena voidaan pitää raison d'État -periaatetta, jonka mukaan valtio voi rajoittaa yksilön oikeuksia tilanteissa, joissa sen keskeiset edut, kuten kansallinen turvallisuus, valtiollinen itsenäisyys tai yhteiskunnan

[80] COM/2024/198 final/2.
[81] COM/2020/605 final, s. 7 ja 23-26.
[82] Ojanen, 2009, s. 164.

vakaus ovat uhattuina. [83] Perusoikeuksien rajoittaminen merkitsee kyseisen perusoikeussäännöksen soveltamisalan oikeuden supistamista tai yksilön oikeusasemaan vaikuttamista viranomaistoimin. Näin ollen yksilö ei voi käyttää kyseistä perusoikeutta täysimääräisesti. [84] Jos kaikkien perusoikeuksien rajoittamisen edellytysten on täytyttävä yhtä aikaa, henkilökohtaisen turvallisuuden käyttäminen perusteena muiden perusoikeuksien rajoittamiselle muodostaa selvästi korkean vaatimustason.[85]

Perusoikeuksien rajoitusedellytyksillä määritellään rajat sille, miten perusoikeuksiin voidaan asianmukaisesti puuttua laillisuuden ja oikeutuksen varmistamiseksi. Ne ovat kirjattu EU:n perusoikeuskirjan 52 artiklaan, ja samat periaatteet ilmenevät myös Suomen perustuslakivaliokunnan linjauksissa (PeVM 25/1994 vp). Perusoikeuskirjan 52.1 artiklassa määritellään rajoittamisen edellytysten toteutuvan ainoastaan lailla, kyseisten vapauksien ja oikeuksien sisällöt kunnioittaen. Poikkeusolojen, kuten Suomeen kohdistuvan aseellisen hyökkäyksen tai muun vakavan uhan vallitessa, voidaan lailla säätää välttämättömistä poikkeuksista perusoikeuksiin (Perustuslaki 23§). Perusoikeuden rajoittamisen arviointi tapahtuu perusoikeuksien rajoittamista koskevan seitsemänkohtaisen yleisen opinkokonaisuuden mukaisesti: [86]

Lailla säätämisen vaatimus: Rajoitusten tulee perustua eduskuntalakiin.
Täsmällisyys- ja tarkkarajaisuusvaatimus: Rajoitusten on oltava tarkkarajaisia ja riittävän täsmällisesti määriteltyjä.
Hyväksyttävyysvaatimus: Rajoitusperusteiden tulee olla perusoikeusjärjestelmän kannalta hyväksyttäviä, painavan yhteiskunnallisen tarpeen vaatimia.
Ydinalueen koskemattomuuden vaatimus: Tavallisella lailla ei voida säätää perusoikeuden ytimeen ulottuvaa rajoitusta.

[83] Widlund, 2020, s. 146.
[84] Tuori, 1999, s. 433.
[85] Bruun, 2016, s. 252.
[86] Lainkirjoittajan opas, 4.1.13.

Suhteellisuusvaatimus: Rajoitusten tulee olla välttämättömiä tavoitteen saavuttamiseksi sekä laajuudeltaan oikeassa suhteessa perusoikeuksien suojaamaan oikeushyvään ja rajoituksen taustalla olevan yhteiskunnallisen intressin painoarvoon.
Oikeusturvavaatimus: Perusoikeutta rajoitettaessa on huolehdittava riittävistä oikeusturvajärjestelyistä.
Ihmisoikeusvelvoitteiden noudattamisen vaatimus: Rajoitukset eivät saa olla ristiriidassa Suomen kansainvälisten ihmisoikeusvelvoitteiden kanssa.

Taulukko 3 Perusoikeuksien rajoitusedellytykset PeVM 25/1994 vp

Ensimmäinen rajoitusedellytys takaa sen, että perusoikeuksien rajoituksista ei voida säätää esimerkiksi asetuksilla, vaan niiden säätäminen kuuluu eduskunnalle lainsäätäjänä.[87] Toinen perusoikeuksien rajoitusedellytys täsmällisyys ja tarkkarajaisuus liittyy ensimmäiseen vaikutukseen. Terrorisminvastaisessa sääntelyssä esimerkiksi liikkumisvapautta rajoitettaessa rajoituksen on ilmettävä laista tarkasti, sekä täsmällisesti. Vaatimuksen mukaan laista tulisi ilmetä rajoituksen laajuus ja täsmälliset edellytykset. [88]

Hyväksyttävyysvaatimusta tarkasteltaessa punnitaan suojattavaa etua ja rajoittavaa oikeutta. Perustuslakivaliokunta korostaa ihmisoikeussopimuksen merkityksellisyyttä ja siinä olevien rajoitusperusteiden merkitystä arvioitaessa hyväksyttävyyttä. Euroopan ihmisoikeussopimuksen lisäpöytäkirjan 2 artiklan perusteella liikkumisvapautta voidaan rajoittaa muun muassa kansallisen ja yleisen turvallisuuden takaamiseksi. Ydinalueen koskemattomuuden vaatimus on yksiselitteinen ja tarkoittaa ettei perusoikeuden ydinalueeseen saa puuttua. [89] Tätä yleensä sovelletaan yhdessä suhteellisuusvaatimuksen kanssa, joka vaatii rajoituksen oltava välttämättömiä ja oikeassa suhteessa tavoiteltuun päämäärään, jonka takia pelkkä terrorismin torjunta ei itsessään riitä perusoikeuksien rajoittamiseen. Viimeiset rajoitusedellytykset ovat

[87] Viljanen, 2001, s.65–67.
[88] HE 309/1993 vp, s. 4.
[89] PeVM 25/1994 vp, s. 5.

yksiselitteisempiä. Oikeusturvavaatimus takaa terrorismista epäillylle henkilölle oikeuden turvautua oikeusturvajärjestelyihin ja muutoksenhakuun.[90]

Perusoikeuksiin kohdistettavat rajoitusedellytykset ovat kumulatiivisia, joka tarkoittaa sitä, että kaikkien rajoitusedellytysten on täytyttävä, jotta rajoitus olisi sallittu [91]. Rajoitusedellytykset toimivat vain osittain arviointiperusteena silloin, kun perusoikeuksia rajoitetaan, ja nämä perusoikeudet on muotoiltu julkisen vallan turvaamis- ja edistämisvelvollisuuden näkökulmasta. [92] Perusoikeusrajoituksista pystytään erottamaan vielä perusoikeuspoikkeukset, jotka rajoittavat ja puuttuvat perusoikeuteen laajemmin kuin perustuslaki. Tällaisia lähtökohtaisesti kiellettyjä rajoituksia voidaan poikkeuslailla säätää kiireellisesti 5/6 enemmistöllä, edellyttäen yhä poikkeuksien noudattavan perustuslain 73 §. Demokraattisissa yhteiskunnissa kansalaiset usein vastustavat yksilön perusvapauksien rajoituksia. Yhdysvalloissa tämä näkyi erityisesti vuoden 2001 terrori-iskujen jälkeen. Silloin säädetty Patriot Act laajensi viranomaisten toimivaltuuksia. Sen pykälä 213 antaa viranomaisille laajat oikeudet salaisiin ja yksilön yksityisyyteen kohdistuviin tiedonhankintakeinoihin. Pykälä 213 sisälsi myös oikeusturvaa heikentävän kohdan, sillä se mahdollisti viranomaisille harkintavallan viivästyttää tiedottamista salaisen kotietsinnän kohteeksi joutuneelle henkilölle. [93]

Perusoikeuden rajoittamiselle tulee olla aina hyvin perustellut syyt. Perustuslain 10 §:n 4 momentin mukaan lailla voidaan säätää välttämättömistä rajoituksista, jotka uhkaavat kansallista turvallisuutta. Suomi edistää kansallista yhteistyötä esimerkiksi tekemällä yhteistyötä maahantulolupien väärinkäytön estämiseksi Schengen alueella.[94] Kansallisen turvallisuuden uhan tulee olla laissa tarkkarajaisesti määritelty, jotta sen perusteella voidaan oikeudellisesti kestävällä tavalla kohdistaa rajoituksia yksilön perusoikeuksiin.[95] Esimerkiksi asetus tai muu lakia alemman asteinen säädös ole tähän riittävä. Käytännön

[90] PeVL 23/1997 vp, s. 2.
[91] Ojanen, 2009, s. 166.
[92] Hallberg, 2005.
[93] Finan, 2007, 281–292.
[94] Sisäministeriö, 2022:36, s. 14.
[95] Bossong, 2012, s. 61–63.

tasolla vakaviksi katsottuja kansalliseen turvallisuuteen kohdistuvia uhkia on lueteltu tyhjentävästi poliisilain 5 a luvun 3 §:ssä. Näitä ovat muun muassa terrorismi, ulkomainen tiedustelutoiminta sekä joukkotuhoaseiden suunnittelu, valmistaminen, levittäminen ja käyttö. Lisäksi kansainvälisen oikeuden näkökulmasta Yhdistyneiden kansakuntien turvallisuusneuvosto voi YK:n peruskirjan VII luvun nojalla määrätä jäsenvaltioita sitovista pakotteista tilanteissa, joissa se on todennut rauhan rikkoutumisen uhan, rauhan rikkomisen tai hyökkäysteon olemassaolon. [96]

Suhteellisuusperiaate edellyttää, että perusoikeusrajoitukset ovat paitsi tarpeellisia ja laillisia myös suhteessa tavoiteltuun päämäärään. [97] Vaikka turvallisuus on perusoikeus ja valtion keskeinen tehtävä, sitä ei voida toteuttaa keinoilla, jotka kohtuuttomasti rajoittavat muita perusoikeuksia. [98] Tietojen säilyttämistä koskeva data retention -direktiivi (2006/24/EY), joka velvoitti teleoperaattorit säilyttämään käyttäjien yhteystietoja viranomaisten käyttöön, mitätöitiin Euroopan unionin tuomioistuimen ratkaisuissa Digital Rights Ireland (C-293/12 ja C-594/12) sekä Tele2 Sverige (C-203/15). Ensiksi mainitussa tapauksessa EUT katsoi, että direktiivi loukkasi yksityiselämän ja henkilötietojen suojaa (EU:n perusoikeuskirjan 7 ja 8 artiklat), koska se mahdollisti yleisen ja erottelemattoman tietojen säilyttämisen ilman riittäviä oikeusturvakeinoja. Tele2 Sverige -ratkaisussa tuomioistuin vahvisti, että jopa kansallisen turvallisuuden nimissä massaluonteinen tiedonkeruu on suhteetonta, ellei siihen liity tarkkoja laillisia rajoituksia ja riippumatonta valvontaa. [99] Nämä ratkaisut muodostavat tärkeän oikeuskäytännöllisen viitekehyksen sille, millaiset rajoitukset perusoikeuksiin ovat EU-oikeuden näkökulmasta hyväksyttäviä ja miten valvonnan keinot on suhteutettava oikeudenmukaisesti yksilönvapauksiin.

Suomessa päätökset vaikuttivat muun muassa perustuslain 10 §:n muuttamista koskevaan hallituksen esitykseen, jossa käsiteltiin luottamuksellisen viestin salaisuuden

[96] Hallberg, 2005.
[97] Ojanen, 2016, s. 165.
[98] C-293/12 ja C-594/12, kohta 69.
[99] C-293/12 ja C-594/12, kohdat 39 ja 65.

suojaa ja sen rajoituksia.[100] Perustuslain (731/1999) 10 §, joka turvaa yksityiselämän suojan muutettiin siten, että lailla voidaan säätää tiedonhankinnasta sellaiseen sotilaalliseen toimintaan tai muuhun siihen rinnastettavaan vakavaan uhkaan, joka kohdistuu kansalliseen turvallisuuteen. Muutoksen myötä tällainen tiedonhankinta voidaan katsoa perusoikeuden rajoituksena hyväksyttäväksi, mikäli se täyttää perusoikeuksien rajoittamiselle asetetut vaatimukset, kuten laillisuus-, tarkkarajaisuus- ja välttämättömyysperiaatteen.[101] EIT on todennut, että vaikka salainen valvonta loukkaa yksityiselämän suojaa, tietyissä olosuhteissa se on perusteltua kansallisen turvallisuuden vuoksi. Valtion harjoittama salainen tiedustelu voi olla hyväksyttävää, mikäli se on välttämätöntä demokraattisessa yhteiskunnassa ja säädetty lailla riittävän tarkasti. Kansallisen turvallisuuden nimissä toteutettava tiedustelun tulee noudattaa oikeusvaltioperiaatteita ja varmistaa riittävät oikeussuojakeinot.[102] Tuomioistuin on toistuvasti arvostellut lainsäädäntöä siitä, että se ei huomioi riittävällä laajuudella perus- ja ihmisoikeuksia tietoliikennetiedustelun yhteydessä.[103]

[100] HE 198/2017 vp, s. 5.
[101] Widlund & Paasonen, 2021, s.34.
[102] EIT 06.09.1978.
[103] Miller, 2010, s. 369–371.

3 Tekoäly valvontatoimissa

Tekoälyteknologiaa käytetään laajasti valvontatarkoituksiin. Tekoälyä voidaan luokitella eri tavoin sen toiminnallisuuden mukaan, mutta valvontateknologiassa erityisesti analyyttinen ja ihmislähtöinen tekoäly ovat keskeisiä. Analyyttinen tekoäly käsittelee suuria tietomassoja ja tunnistaa kaavamaisuuksia, kun taas ihmislähtöinen tekoäly mahdollistaa esimerkiksi vuorovaikutuksen viranomaisten ja järjestelmien välillä. [104] Tekoälyn vaikutuksia valvontateknologioissa voidaan tarkastella sekä teknisellä tasolla (esim. uhkamallinnus) että yhteiskunnallisella tasolla (esim. vaikutukset yksilön oikeuksiin).[105]

3.1 Tiedustelu- ja valvontateknologiat

Valtiot ovat aina hyödyntäneet valvontaa, salaista tiedonhankintaa ja tiedustelua kansalaistensa, sekä turvallisuusuhkien seurannassa. Tiedustelutoiminnalla tarkoitetaan toimintaa, jonka tarkoituksena on hankkia toisen valtion etujen vastaisesti tietoa, jonka salassa pitämiseen kohdevaltioilla on erityinen ja perusteltu intressi. Tällainen toiminta tapahtuu tyypillisesti tiedustelua harjoittavan valtion hyväksi ja kohdevaltion vahingoksi.[106] Perinteisten menetelmien rinnalle on noussut sähköinen valvonta, jonka merkitys on kasvanut erityisesti 2000-luvulla terrorismin uhan myötä. [107] Tiedustelua voidaan jakaa kansainvälisesti: avointen lähteiden tiedustelu (Open source intelligence, OSINT), signaalitiedustelu (Signals intelligence, SIGINT), henkilötiedustelu (Human intelligence, HUMINT), paikka- ja olosuhdetiedustelu (Geospatial intelligence, GEOINT), sekä mittaus- ja tunnusmerkkitiedustelu (Measurement and signatures intelligence, MASINT). Esimerkiksi SIGINT-tiedustelussa tekoäly voi analysoida suuria määriä viestiliikennettä, kun taas OSINT-sovelluksissa algoritmit pystyvät tunnistamaan potentiaalisia uhkia sosiaalisesta mediasta. [108]

---

[104] Haenlein & Kaplanin, 2019, s. 7 ja 9.
[105] Traficom, 2021, s.5.
[106] Lohse & muut, 2019, s.34.
[107] Paasonen & Widlund, 2023.
[108] Lohse & muut, 2019, s.19.

Rikostorjunta oikeusvaltiossa tulee arvioida aina tapauskohtaisesti. Vaikka tiedustelutoiminta nähdään usein periaatteessa neutraalina, sen hyväksyttävyys syntyy vasta silloin, kun toimenpiteet on kohdistettu selkeästi hyväksyttävän ja perustellun tavoitteen saavuttamiseen.[109] Rikostorjunta perustuu laillisuusperiaatteeseen ja vallan rajoihin, joita on korostettu jo valistusajan filosofiassa. Erityisesti Rechtsstaat-mallissa ja Rule of Law -ajattelussa painotetaan valvonnan oikeudellisia rajoja, lainkäytön ennakoitavuutta, sekä tuomioistuimen roolia, joita massavalvonnan teknologiat haastavat.[110] Tekoälyjärjestelmien sääntelyä ohjaavat standardit ja lainsäädäntö, kuten ISO/IEC-standardit ja EU:n yleinen tietosuoja-asetus (GDPR). [111] International Organization for Standardization (ISO) ja International Electrotechnical Commission (IEC) ovat kaksi merkittävintä standardointijärjestöä. Ne mahdollistavat sen, että eri maiden ja organisaatioiden järjestelmät voivat toimia saumattomasti yhdessä, sekä ne tarjoavat kansainvälisesti tunnustettuja turvallisuusstandardeja.[112]

Tiedustelutoiminnan määrittely ja sääntely kuuluvat pääasiassa jäsenvaltioiden kansallisen lainsäädännön piiriin. EU:n lainsäädäntö tukee kansainvälistä yhteistyötä ja tiedonvaihtoa tiedustelukysymyksissä, erityisesti terrorismiin ja rajat ylittävään rikollisuuteen liittyen. Myös Euroopan ihmisoikeussopimuksella, erityisesti yksityiselämän suojaa koskevilla määräyksillä on ollut vaikutusta EU:n tiedustelutoiminnan oikeudellisiin perusteisiin.[113] Uusissa tiedustelulaeissa korostetaan henkilötietojen suojan merkitystä sillä ne sallivat viranomaisille oikeuden salaiseen tiedonhankintaan. Erityisesti tietoliikennetiedustelua suorittavien viranomaisten tulee hakea lupa tuomioistuimelta, kun käytetään menetelmiä, jotka puuttuvat luottamuksellisen viestin salaisuuden suojaan.[114]

[109] Widlund & Paasonen, 2021, s.9.
[110] Mäntylä, 2023, s. 5.
[111] Traficom, 2021, s.10.
[112] Dunkelman & muut, 2017.
[113] Kalliojärvi, 2016, s. 40–42.
[114] Hietanen & Arkia, 2017, s.102.

Tiedustelupalveluiden toiminnan valvonta on olennainen osa demokraattisen yhteiskunnan periaatteita ja tekoälyjärjestelmät ovat luotu niiden toimintaa tukeviksi, ei itsenäisesti rikoksia ratkoviksi. Tiedustelutoiminnan laillisuusvalvonnasta vastaa tiedusteluvalvontavaltuutettu, joka toimii riippumattomana viranomaisena. Valtuutetun tehtävänä on valvoa paitsi tiedustelutoiminnan lainmukaisuutta myös suojelupoliisin toimintaa siltä osin kuin se liittyy perusoikeuksiin, yksityisyyden suojaan ja muuhun perusoikeuksien toteutumiseen. (Laki tiedustelutoiminnan valvonnasta 18.1.2019/121) Poliisi noudattaa tekoälyjärjestelmien käytössä eettisiä periaatteita ja perusoikeuksia, kuten yksityisyyden suojaa ja yhdenvertaisuutta, varmistaen että käyttö tapahtuu lain ja määräysten mukaisesti.[115]

Mikäli EU:n kansalainen uskoo, että EU:n toimielin on rikkonut tämän oikeutta yksityisyyteen käyttämällä henkilötietoja väärin, voi valituksen tehdä tietosuojavaltuutetulle.[116] EIT totesi päätöksessään, että poliisin mahdollisuus pysäyttää ja tutkia henkilöitä ilman rikosepäilyä rikkoi yksityiselämän suojaa (EIS 8 artikla). Terrorismilain 44 § antoi viranomaisille liian laajat ja valvomattomat toimivaltuudet. Euroopan ihmisoikeustuomioistuimen tuomio johti Britannian lainsäädännön muutoksiin. Päätös korostaa valvontatoimien tarkkaa sääntelytarvetta, jotta ne eivät johda mielivaltaisiin toimenpiteisiin. [117] Väärin toteutettu tiedustelu voi heikentää luottamusta. Nousee esille kysymys, voiko tiedustelua toteuttaa lainmukaisesti, läpinäkyvästi ja perusoikeudet turvaten?[118]

Vuonna 1992 säädettiin laki TeletoimintaL 676/92, joka määritteli poliisin valtuudet saada teleyrityksiltä puhelinliikenteen tunnistetietoja osana salaista tiedonhankintaa. Tänä päivänä kaikki poliisin salaisen tiedonhankinnan toimivaltuudet perustuvat lain tasoisiin säädöksiin.[119] Vuosikymmeniä jatkunut yhteiskunnallinen keskustelu poliisin

[115] Sisäministeriö, 2024.
[116] Raitio, 2016, s. 106.
[117] EIT 12.01.2010.
[118] Hietanen & Arkia, 2017, s. 104–105.
[119] Hankilanoja, 2014, s.69–70.

telekuunteluoikeuksista havainnollistaa, kuinka haastavaa uusien tiedonhankintavaltuuksien perusteleminen ja käyttöönotto on.[120] Suomessa poliisi on käyttänyt kasvojentunnistusohjelmaa rikollisten kiinniottamisessa vuodesta 2014 alkaen ja poliisi on kuvannut kokemuksia järjestelmästä positiivisiksi. Valtiovarainministeriön vuonna 2023 julkaisema selvitys tarkastelee, miten koneoppimista voidaan hyödyntää julkisen hallinnon digitaalisen turvallisuuden teknisessä valvonnassa. Koneoppiminen voi parantaa uhkien havaitsemista ja vähentää manuaalista työkuormaa, mutta siihen liittyy myös haasteita, kuten väärien hälytysten riski. [121] Poliisilain 2§ tiedustelumenetelmiksi siviilitiedustelussa voidaan sisältää telekuuntelu, tietojen hankkiminen telekuuntelun sijasta ja televalvonta. Tekninen kuuntelu tarkoittaa viestin tai keskustelun, joka ei ole tarkoitettu ulkopuolisille ja johon kuuntelija ei osallistu, seuraamista, tallentamista tai käsittelyä teknisin välinein tietyn henkilön tai ryhmän toiminnan tai viestinnän sisällön selvittämiseksi (SotTiedL 26.1 §). [122]

Tekoälypohjaiset valvontajärjestelmät vertaavat valvontakamerakuvia poliisin omiin rekistereihin, kuten passikuviin tunnistaakseen epäiltyjä. Poliisitarkastaja Pekka Sallisen mukaan järjestelmä on ollut merkittävä apu rikosten selvittämisessä. Esimerkiksi vuonna 2019 poliisi teki noin 1 000 kasvojentunnistushakua, jotka johtivat useisiin pidätyksiin. Teknologiaa on käytetty erityisesti vakavien rikosten, kuten ryöstöjen ja pahoinpitelyjen tutkinnassa. [123] Rajavartiolaitoksella on Suomessa oikeudet reaaliaikaiseen kasvojentunnistukseen, mutta tietoa sen käytöstä on ollut vaikea saada. [124] Algoritmivirheet voivat johtaa vakaviin seuraamuksiin, erityisesti jos kasvojentunnistuksen tuottamaa tietoa käytetään oikeudenkäynneissä todisteena tai tukemaan syytteitä. Tällaisissa tilanteissa virheellinen, mutta teknisesti luotettavalta vaikuttava tunnistus voi johtaa syyttömän henkilön tuomitsemiseen. [125]

---

[120] Hankilanoja, 2014, s. 70–71 ja 77.
[121] Valtiovarainministeriö, 2023.
[122] Lohse & muut, 2019, s. 168.
[123] YLE, 2020.
[124] Ojanen & muut, 2022, s. 27.
[125] Buolamwini & Gebru, 2018, s. 1.

3.2 Ongelmallisia valvontateknologioita ihmisoikeuksien kannalta

EU:n lainsäädäntö pyrkii suojaamaan perusoikeuksia, mutta tekoälyn käyttö turvallisuus- ja tiedustelutarkoituksissa on aiheuttanut merkittäviä haasteita.[126] EU:ssa on yleistynyt tekoälyn käyttö reaaliaikaisessa valvonnassa, kuten kasvojentunnistusjärjestelmissä, automaattisessa rekisterikilpien tunnistamisessa ja julkisen tilan kameravalvonnassa. Euroopan unionin perusoikeusviraston (FRA) mukaan tällainen laajamittainen valvonta uhkaa yksityisyyttä, sananvapautta ja liikkumisvapautta, koska kansalaisilla ei ole mahdollisuutta tietää missä, milloin ja miten heidän tietojaan käsitellään.[127] Massavalvonnan on myös katsottu uhkaavan eurooppalaisen yhteiskunnan perusarvoja ja -vapauksia.[128] Kansalaisjärjestöt ovat lisäksi varoittaneet, että tekoälypohjainen massavalvonta voi johtaa *”chilling effect”* -ilmiöön. Tällöin valvonnan uhka hillitsee kansalaisten halukkuutta käyttää perusoikeuksiaan ja ihmiset saattavat välttää sananvapauden käyttämistä tai julkisiin kokoontumisiin osallistumista pelätessään tulevansa valvotuiksi.[129]

Tekoälyyn perustuvat valvontajärjestelmät voivat analysoida valvontakamerakuvia reaaliajassa ja verrata niitä tietokantoihin, mikä helpottaa rikollisten tunnistamista ja seuraamista. Uhkamallinnuksen periaate perustuu historiallisen datan analysointiin, mikä mahdollistaa ennaltaehkäisevän toiminnan.[130] Aikaisemmin ennaltaehkäisevissä toimissa on huomioitu erityisesti pitkään jatkuneet ratkaisemattomat konfliktit, ihmisoikeuksien rikkomukset sekä kansallisuuteen tai uskontoon perustuva syrjintä.[131] Uhkamallinnus (threat modeling) on yksi keskeisistä sovelluksista, jonka avulla pyritään tunnistamaan mahdollisia turvallisuusuhkia analysoimalla mitkä asiat voivat mennä pieleen ja niiden tietoturvavaikutuksia.[132] Esimerkiksi ennakoiva poliisitoiminta

[126] FRA, 2020, s. 57–58.
[127] FRA, 2020, s- 32–36 ja 61–64.
[128] Brown & Korff, 2009, s. 131–132.
[129] Amnesty, 2020.
[130] Traficom, 2021, s.5.
[131] Scheinin, 2009, s. 519.
[132] Traficom, 2021, s. 24.

(predictive policing) käyttää tilastollisia malleja arvioimaan, millä alueilla rikoksia todennäköisimmin tapahtuu. Tavoitteena ei ole pelkästään reagoida rikoksiin, vaan estää ne jo ennen tapahtumista. Ennakoiva poliisitoiminta kuuluu EU: n tekoälyasetusehdotuksen (COM/2021/206 final) piiriin ja on luokiteltu suurriskiseksi tekoälyjärjestelmäksi.[133] Privacy by design ja privacy by default, ovat keskeisiä välineitä ennakoivassa sääntelyssä, sillä ne velvoittavat ottamaan tietosuojan huomioon jo järjestelmien suunnitteluvaiheessa ja varmistamaan, että oletusasetukset turvaavat käyttäjän yksityisyyden (GDPR, 25 artikla).

Lisäksi teknisen tason haasteisiin kuuluu järjestelmien luotettavuus ja väärien hälytysten määrä. Metropolitan Police suoritti kasvojentunnistusteknologian kokeiluja julkisilla paikoilla massavalvontana ja havaitsi, että järjestelmän tunnistukset olivat virheellisiä 81 % tapauksista. Tämä johti useiden syyttömien kansalaisten tarkastuksiin ja herätti huolta teknologian luotettavuudesta sekä sen vaikutuksista yksityisyyteen ja kansalaisoikeuksiin. [134] Algoritmien harhaisuus (bias) on merkittävä riski sillä tekoälymallit oppivat datasta, joka voi heijastaa historiallisia vinoumia. Esimerkiksi Yhdysvalloissa eräät algoritmit ovat tuottaneet ennusteita, jotka painottavat tiettyjen etnisten ryhmien tai alueiden rikollisuutta historiallisten tietojen perusteella. Vuonna 2016 ProPublica-tutkimus osoitti, että COMPAS-niminen ennustetyökalu arvioi mustien rikoksenuusijoiden riskin huomattavasti suuremmaksi kuin valkoisten, vaikka tosiasiallisesti uusimisriski oli yhtäläinen. [135] Tekoälyjärjestelmät voivat tahattomasti vahvistaa tai luoda uusia ennakkoluuloja, mikä voi johtaa syrjintään lainvalvonnassa.[136]

Samoin rikosoikeudellisessa päätöksenteossa käytetyt tukijärjestelmät voivat olla rodullisesti puolueellisia, jos ne perustuvat historiallisiin datajoukkoihin, joissa esiintyy syrjiviä käytäntöjä. [137] Järjestelmät käyttävät historiallisia tietoja, jotka voivat olla

[133] Rikoksentorjunta.fi, 2021.
[134] Jee, 2019.
[135] Barenstein, 2019, s. 2.
[136] Euroopan parlamentti, 2023.
[137] Haenlein & Kaplanin, 2019, s. 10.

harhaanjohtavia tai vinoutuneita.[138] Robert Julian-Borchak Williams, afroamerikkalainen mies, pidätettiin virheellisesti Detroitissa kasvojentunnistusjärjestelmän perusteella. Järjestelmä yhdisti hänen kuvansa väärin valvontakameran tallenteeseen, mikä johti perusteettomaan pidätykseen. [139] Tekoälypohjaiset kasvojentunnistusjärjestelmät tunnistivat tummaihoiset naiset jopa 34 % heikommin kuin vaaleaihoiset miehet, mikä osoittaa koneoppimisen vinoumien vakavat seuraukset.[140] Yksi keskeinen ongelma on, että syrjintä voi syntyä myös epäsuorasti. Esimerkiksi algoritmit voivat käyttää postinumeroita luokitellakseen ihmisiä, vaikka postinumero ei sinänsä ole syrjintäperuste. [141] Kiinassa on ollut käytössä sosiaalinen luottoluokitusjärjestelmä (Social Credit System, SCS). Se on laaja valvontajärjestelmä, jonka tavoitteena on seurata ja ohjata kansalaisten käyttäytymistä. Järjestelmä palkitsee valtion normien mukaisen toiminnan ja rankaisee esimerkiksi rikoksista tai muusta ei-toivotusta käytöksestä. Pisteytys vaikuttaa suoraan ihmisten arkeen, kuten mahdollisuuteen saada asunto, koulutus tai matkustaa. Valvonta ulottuu syvälle yksityiselämään, seuraten muun muassa ostotottumuksia ja sosiaalista kanssakäymistä.[142]

Valvonnan rajoitukset on kohdennettu erityisesti henkilötietojen keruuseen ja käyttöön, mikä on keskeistä massavalvonnan ja yksityisyyden menetyksen riskien ehkäisemisessä.[143] Pegasus on israelilaisen NSO Groupin kehittämä vakoiluohjelma, joka mahdollistaa puhelimien etävalvonnan ilman kohteen tietoisuutta. Ohjelmaa on käytetty erityisesti hallitusten toimesta vakoilemaan toimittajia, ihmisoikeusaktivisteja ja oppositiopoliitikkoja ympäri maailmaa. Esimerkiksi vuonna 2021 Pegasus-projektiksi nimetty journalistinen yhteistyö paljasti, että tuhansia henkilöitä oli valvottu tällä ohjelmalla. Ihmisoikeusjärjestöt ovat vaatineet valvontaa tällaisten teknologioiden myynnille, kunnes niihin voidaan soveltaa kansainvälisiä ihmisoikeusstandardeja. [144]

---

[138] FRA, 2020, s. 68–72.
[139] Civil Rights Litigation Clearinghouse, 2021.
[140] Buolamwini & Gebru, 2018.
[141] Ojanen & muut, 2022, 47–48.
[142] Paasonen & Widlund, 2023.
[143] GDPR, johdanto-osa kohta 39.
[144] Amnesty, 2021.

Amnesty International on vaatinut EU:ssa kasvojentunnistusteknologian käytön kieltoa kokonaan massavalvonnassa.[145] Euroopan ihmisoikeustuomioistuimen ratkaisu osoittaa, kuinka laajamittainen massavalvonta voi loukata yksilön oikeuksia. Tapauksessa EIT katsoi, että Iso-Britannian harjoittama tiedustelutietojen laajamittainen kerääminen ja analysointi rikkoi Euroopan ihmisoikeussopimuksen 8 artiklan mukaista yksityiselämän suojaa. EIT korosti päätöksessään, että tiedusteluviranomaisten toiminta edellyttää tarkkarajaista lainsäädäntöä ja tehokkaita oikeussuojakeinoja.[146]

Intiassa digitaalinen valvonta on laajentunut merkittävästi, uhaten yksityisyyttä ja kansalaisoikeuksia. Hallitus on siirtynyt kohdennetusta valvonnasta massavalvontaan ilman riittävää oikeudellista sääntelyä. Tärkeitä järjestelmiä ovat Central Monitoring System (CMS), joka mahdollistaa reaaliaikaisen viestinnän seurannan ilman ulkopuolista valvontaa, sekä Aadhaar, joka on maailman suurin biometrinen tunnistusjärjestelmä.[147] CMS : n tehtävänä on torjua kansallisia turvallisuusuhkia, kuten terrorismia ja kyberhyökkäyksiä, mutta järjestelmä toimii ilman kattavaa oikeudellista sääntelyä ja selkeitä tarkastusmekanismeja.[148] Aadhaar on Intian valtakunnallinen biometrinen tunnistusjärjestelmä, joka on rekisteröinyt lähes kaikkien aikuisten henkilötietoja. Järjestelmä perustuu 12-numerisiin tunnisteisiin, joihin liitetään sormenjäljet, iiris- ja kasvojentunnistustiedot sekä perustiedot.[149] Sosiaalisen median valvonta ja sensuuri ovat lisääntyneet ja hallitus käyttää tekoälyä kansalaisten verkkokäyttäytymisen seuraamiseen. Lisäksi yksityiset teknologiayritykset toimittavat valvontatyökaluja hallitukselle, mikä kytkee yritysten ja valtion edut yhteen.[150]

Samanaikaisesti valvontateknologian kehitys on tuonut mukanaan uusia työkaluja, joita hallitukset ja lainvalvontaviranomaiset hyödyntävät. Kasvojentunnistus ja dronet ovat yhä yleisempiä julkisilla paikoilla, joista esimerkkinä Clearview AI, jonka käyttö

[145] Amnesty, 2020.
[146] EIT 25.05.2021.
[147] Mahapatra, 2021, s. 14–17.
[148] Joshi, 2013, s. 1–3.
[149] Rao & Nair, 2019, 469–481.
[150] Mahapatra, 2021, s. 14–17.

poliisitoiminnassa on noussut esille valvonnassa. Järjestelmässä on kritisoitu sitä, että se käyttää kuvia, jotka on kerätty ilman käyttäjien suostumusta[151] . Clearview AI:n kasvojentunnistusjärjestelmä perustuu laajamittaiseen datankeruuseen, jossa käytetään julkisista lähteistä, kuten sosiaalisesta mediasta kerättyjä kuvia. Sen käyttö poliisitoiminnassa on herättänyt huolta erityisesti yksityisyyden suojan ja GDPR-rikkomusten näkökulmasta. Tätä teknologiaa on käytetty erityisesti lainvalvonnassa ja turvallisuussektorilla. Italian tietosuojaviranomainen (Garante) määräsi Clearview'lle 20 miljoonan euron sakot GDPR-rikkomuksista ja kielsi yhtiötä keräämästä ja käyttämästä kansalaisten biometrisiä tietoja. Kritiikki kohdistuu erityisesti siihen, että yritys kerää ja käyttää henkilötietoja ilman asianomaisten suostumusta, mikä voi johtaa vakaviin yksityisyyden loukkauksiin.[152]

Tekoälypohjainen valvonta voi lisätä turvallisuudentunnetta, mutta jos sen käyttö ei ole läpinäkyvää tai demokraattisesti valvottua, se saattaa samalla heikentää luottamusta viranomaisiin. Läpinäkyvyyttä edellytetään erityisesti deepfake-teknologialta, joka voi vääristää julkista keskustelua tai johtaa disinformaation leviämiseen.[153] EU:ssa tiedon saatavuuden periaate tukee sisäisen turvallisuuden viranomaisten pääsyä tietoihin jäsenvaltioissa, mikä heijastaa turvallisuuden ja yksityisyyden yhteensovittamista.[154] Tiedustelupalvelut hyödyntävät laajamittaista valvontaa, joka kerää tietoja suurilta väestöryhmiltä ilman rikosepäilyä. Tuomioistuin on arvostellut tietojen säilyttämisen ehtoja, kuten tietojen säilyttämistä unionin alueella, koska niitä ei ole määritelty riittävän tarkasti. Tämä altistaa tiedot ennakoimattomalle käsittelylle ja urkinnalle.[155] FRA-raportin mukaan monet tekoälyyn perustuvat hallinnolliset päätökset, kuten viisumihakemusten hylkääminen tehdään ilman, että kansalaiset voivat riittävästi ymmärtää päätöksen perusteita tai haastaa sitä oikeusteitse.[156]

---

[151] Ojanen & muut, 2022, s. 67.
[152] Italian Data Protection Authority, 2022.
[153] Euroopan parlamentti, 2023 päivitetty 2024.
[154] Gonçalves & muut, 2013.
[155] Ollila, 2014, s. 815.
[156] FRA, 2022, s. 167–170.

Erityisen ongelmallisia ovat *”mustan laatikon”* järjestelmät, joiden päätöksentekoprosessi ei ole avoin edes viranomaisille.[157] Algoritmien mustan laatikon ongelma tarkoittaa, että niiden tekemien päätösten taustalla olevia syitä on vaikea jäljittää, joka vaikeuttaa päätösten perustelemista ja oikeudenmukaisuuden arviointia.[158] Mustan laatikon ongelma vaikeuttaa oikeuden toteutumista, koska yksilö ei voi ymmärtää päätöksen perusteluja eikä käyttää tehokkaita oikeussuojakeinoja. Tämä on vastoin perusoikeuskirjan 41 artiklan mukaista oikeutta tulla kuulluksi ja saada perusteltu päätös. Syväoppiminen (Deep Learning), joka muodostaa monien tekoälysovellusten perustan on luonteeltaan kuin musta laatikko. Sen tuottaman tuloksen laatu on arvioitavissa, mutta prosessi sen kehityksen takana jää usein hämäräksi. [159] Esittelemäni tapaukset osoittavat, kuinka demokratia voi ajautua autoritäärisiin valvontakäytäntöihin teknologian avulla. Tämä alleviivaa oikeusvaltioperiaatteen merkitystä. Valvontavallankäytön on aina tapahduttava laillisesti säädellyissä rajoissa (PL 2 § 3 mom.) ja tuomioistuinvalvonnassa, jotta demokratia säilyy teknologian kehittyessä.

3.3 Terrorismin torjunta tekoälyllä

Terroriteot on luokiteltu sotarikoksiksi Geneven yleissopimusten mukaan, jotka hyväksyttiin vuonna 1949. [160] Terrorismin torjunta on noussut merkittäväksi huolenaiheeksi kansainvälisellä tasolla, erityisesti Yhdysvalloissa vuoden 2001 WTC-iskujen jälkeen.[161] Iskuilla oli vaikutus koko maailmaan, vaikka ne tapahtuivatkin kaukana Euroopasta. Terrorismi on ollut ilmiö kuitenkin jopa vuosisatoja aikaisemmin kansainvälisten yhteisöjen huolenaiheena. Euroopan unionissa terrorismin torjunnan ajankohtaisuutta, sekä uhkaa ovat lisänneet tuhoisat pommi-iskut Madridissa (2004), Lontoossa (2005) ja Pariisissa (2015). Tämän lisäksi EU:n alueella on ollut useita

[157] FRA, 2020, s. 11.
[158] Ojanen & muut, 2022, s. 57.
[159] Haenlein & Kaplanin, 2019, s. 8.
[160] Esko, 2017, s. 107.
[161] Scheinin, 2009, s. 507.

pienempiä iskuja.[162] Europolin raportin mukaan vuonna 2020 EU:n alueella tapahtui yhteensä 57 terrori-iskun yritystä, johon on laskettu mukaan myös epäonnistuneet ja estetyt iskut. Kun taas esimerkiksi 2010 vuonna lukema oli 208, joten tilastoista nähden luvut ovat huomattavasti laskussa.[163]

Euroopan unionin terrorisminvastaiset toimet perustuvat EU:n toiminnasta tehdyn sopimuksen (SEUT) V osaston säännöksiin, erityisesti artikloihin 83 ja 87, jotka koskevat rikosasioiden ja poliisiviranomaisten välistä yhteistyötä. Vuonna 2005 seitsemän Keski-Euroopan valtiota allekirjoitti Prümin sopimuksen, jonka tavoitteena on vahvistaa rajat ylittävää yhteistyötä erityisesti terrorismin ja kansainvälisen rikollisuuden torjunnassa (Prümin sopimus 55/2007). Suomi liittyi myöhemmin tähän sopimukseen, joka sisältää säännöksiä tietojenvaihdosta ja aseistettujen turvahenkilöiden käytöstä lentoliikenteessä. [164] Kielteiset vaikutukset perusoikeuksiin terrorisminvastaisessa sääntelyssä voivat ilmetä viranomaisten tietojenvaihdon rajoituksina, mikä vaikuttaa ihmisten yksityisyyden suojaan, tietosuojaan ja liikkumisvapauksiin. [165] Vuonna 2002 tehdyssä Eurobarometri-tutkimuksessa on todettu EU:n kansalaisten pitävän kansainvälistä terrorismia kaikkein pelottavimpana vaarana. Tutkimuksen mukaan koko EU:n keskiarvo oli 82 prosenttia vastanneista. [166] Terrorismi käsitteenä on edelleen ensisijaisesti ei-oikeudellinen, vaikka terroristinen toiminta onkin rikollista ja siihen puututaan myös oikeudellisin keinoin[167].

Terrorismi ilmiönä voidaan ymmärtää toimintana, joka sisältää poliittisia tai yhteiskunnallisia päämääriä edistäviä tekoja, joihin liittyy kansallisen lain tai kansainvälisen oikeuden vastaisuutta, väkivallan käyttöä tai sillä uhkaamista sekä pyrkimystä aiheuttaa levottomuutta tai pelkoa väestössä. [168] Terroristisessa

[162] Lappi-Seppälä & muut, 2000, s. 1163.
[163] Statista, 2023.
[164] Lappi-Seppälä & muut, 2000, s. 1168.
[165] Ojanen, 2007, s. 1067–1069.
[166] Eurobarometri-tutkimus nro 58.1, loka-marraskuu 2002. *Eurobarometri-tutkimus suoritettiin loka-marraskuussa 2002. Vastaajia oli runsaat 16000 yi 15-vuotiasta eri EU-maiden kansalaisista.*
[167] Esko, 2017, s. 106.
[168] Bossong, 2012, s.5.

tarkoituksessa toimijoiden motiivit voivat liittyä pyrkimykseen saavuttaa *"kansallinen vapaus"* tai vastaava päämäärä, joka kytkeytyy tiettyjen väestöryhmien etnisiin, kansallisiin tai uskonnollisiin pyrkimyksiin. Lisäksi on olemassa ryhmiä, joiden poliittiset tavoitteet ovat varsin epäselviä. [169] Yleisimpiä terroristisia tekotapoja ovat yksinkertaisesti toteutettavat iskut ja tekovälineenä helposti saatavat välineet, kuten teräaseet ja ajoneuvot, mutta etenkin konflikti alueilla räjähteet ja ampuma-aseet ovat yleisiä [170] . Suomessa rikoslain 34 a luku määrittelee terroristisessa tarkoituksessa tehtävät rikokset. Terrorismirikos voidaan nähdä koostuvan terroristisesta tarkoituksesta (RL 34a:6) ja tietystä tekomuodosta (RL 34a:1). Rikoslain 34 a luvun n 6 §:n 1 momentti määrittää ”Rikoksentekijällä on terroristinen tarkoitus, jos hänen tarkoituksenaan on:”

> *1) aiheuttaa vakavaa pelkoa väestön keskuudessa;*
> *2) pakottaa oikeudettomasti jonkin valtion hallitus tai muu viranomainen taikka kansainvälinen järjestö tekemään, sietämään tai tekemättä jättämään jotakin;*
> *3) oikeudettomasti kumota jonkin valtion valtiosääntö tai muuttaa sitä tai horjuttaa vakavasti valtion oikeusjärjestystä taikka aiheuttaa erityisen suurta vahinkoa valtiontaloudelle tai valtion yhteiskunnallisille perusrakenteille; tai*
> *4) aiheuttaa erityisen suurta vahinkoa kansainvälisen järjestön taloudelle tai sellaisen järjestön muille perusrakenteille.*

Terroristijärjestöt ja -verkostot ovat dynaamisia toimijoita, jotka mukautuvat toimintaympäristön muutoksiin hyödyntäen sekä muita rajat ylittävän rikollisuuden muotoja että uutta teknologiaa. Ne käyttävät hyväkseen muun muassa tietoverkkoja sekä materiaaleja, joita voidaan soveltaa joukkotuhoaseiden valmistuksessa[171]. Internet on muodostunut keskeiseksi välineeksi terroristisessa toiminnassa, sillä sen kautta voidaan levittää ideologista propagandaa, harjoittaa psykologista vaikuttamista sekä rekrytoida kannattajia. Verkkoympäristön tarjoama anonymiteetti puolestaan vaikeuttaa viranomaisten ennaltaehkäisevää toimintaa ja tiedustelullista valvontaa.[172] Terroristiverkostot helpottavat myös koulutusoppaiden ja propagandan levittämistä verkossa, ja tällä hetkellä tallaisia verkkosivustoja arvellaan olevan jopa 5000 [173] .

---

[169] Härkönen, 2006, s.217.
[170] Sisäministeriö 2022:36, s. 9.
[171] Lohse & muut, 2019, s.30.
[172] Bossong, 2012, s. 113–114.
[173] Lefrancois, 2008, s. 1.

Euroopan unionin tulisi torjua nykyaikaista terrorismia, sekä siihen liittyviä uusia menetelmiä samalla määrätietoisuudella kuin torjuessa perinteistä terrorismia[174].

Tekoälyjärjestelmiä voidaan hyödyntää rikollisiin tarkoituksiin ja lisäksi ne helpottavat vainoamista ja muita rikoksia, jotka perinteisin keinoin olisivat vaikeampia, työläämpiä tai riskialttiimpia toteuttaa.[175] Suojelupoliisin arvion mukaan terrorismin uhka Suomessa on neliportaisella asteikolla tasolla kaksi, mikä merkitsee kohonnutta uhkaa. Äärioikeiston uhka on aikaisempia vuosia huolestuttavampi, vaikka terrorismin luokittelu asteikko on säilynyt Suomessa samana jo vuodesta 2017 asti. Merkittävimmän terrorismin uhan Suomessa muodostavat yhä yksittäiset toimijat tai pienryhmät, joiden toiminta saa innoituksensa radikaali-islamistisesta propagandasta tai terroristijärjestöjen esittämistä kehotuksista. Viimeaikaiset tiedustelutiedot viittaavat siihen, että Suomessa on havaittu aiempaa vakavampia terroriuhkaan liittyviä suunnitelmia ja hankkeita.[176] 1990-luvun jälkeen kansainvälisten terrori-iskujen kokonaismäärä on yleisesti vähentynyt. Vaikka yksittäisten iskujen lukumäärä on pienentynyt, iskuihin liittyvien ihmisten kuolemantapausten määrä on kasvanut. [177] Suojelupoliisin terrorismin torjunnan kohdehenkilöitä on noin 350[178].

Tekoälyjärjestelmistä on hyötyä myös turvallisuusviranomaisten työssä. FADO (False and Authentic Documents Online) on EU:n jäsenmaiden välinen tietokanta, johon kerätään tietoa aidoista ja väärennetyistä matkustusasiakirjoista. Sen avulla rajaviranomaiset voivat tarkistaa passien, henkilökorttien ja muiden matkustusasiakirjojen aitouden.[179] Matkustajatietoyksikkö [180] käsittelee matkustajarekisteritietoja tunnistaakseen henkilöitä, joilla saattaa olla osallisuutta vakavaan rikollisuuteen tai esimerkiksi terrorismiin (657/2019, 7 §). Tiedonsiirrossa sekä tietoja luovuttava että vastaanottava

[174] Barrot, 2008, s. 5.
[175] Kallioniemi, 2022, s. 20.
[176] Suojelupoliisi, kansallinen terrorismin uhka-arvio 2023.
[177] Härkönen, 2006, s. 218.
[178] Lohse & muut, 2019, s. 30–31.
[179] COM/2023/0729.
[180] *Matkustajatietoyksikkö on poliisin, Tullin tai Rajavartiolaitoksen yhteistoiminnasta annetun lain (687/2009) 5 §: ssä ilmoitettu PTR-rikostiedusteluyksikkö (657/2019, 5 §).*

taho toimivat rekisterinpitäjinä, huolehtien tietosuoja-asetuksen mukaisesta menettelystä. [181] Euroopan Unioni on toteuttanut ohjeistuksia, jotka määräävät lentoliikenteen operaattoreita kokoamaan tietoja matkustajistaan, kuten henkilötiedot, matkan ajankohdat sekä kontaktitiedot. Tämä herättää huolta yksityisyyden suojasta ja herättää keskustelua siitä, miten kauan tietoja on oikeutettu säilömään ja hyödyntämään. [182] Fado Järjestelmään ollaan kehittämässä tekoälypohjaisia tunnistusmenetelmiä, joiden avulla asiakirjojen aitous voidaan varmentaa nopeasti ja auttaa torjumaan asiakirjaväärennöksiä ja laitonta maahanmuuttoa.[183]

Suomen terrorismirikoksia koskeva lainsäädäntö pohjautuu vahvasti kansainvälisiin velvoitteisiin ja oikeudellisiin sitoumuksiin. [184] Oikeusministeriö on käynnistänyt terrorisminlainsäädännön kokonaisuudistuksen 2023 vuoden loppupuolella, jonka tavoitteena on vastata nykyisiin terrorismin uhkiin, poistaa sääntelyn vaikeaselkoisuus ja tiukentaa terrorismirikoksista määrättäviä rangaistuksia. Lainsäädännön uudistamisen tulee noudattaa kansainvälisiä velvoitteita ja kunnioittaa perus- ja ihmisoikeuksia.[185] Suojelupoliisi on käynnistänyt marraskuussa 2023 EU:n sisäisen turvallisuuden rahaston (ISF) osarahoittaman hankkeen, jonka tavoitteena on kehittää tekoälypohjaisia työkaluja tiedusteluanalyysin tueksi. Kehitettävien työkalujen avulla suuria tietomääriä voidaan luokitella ja analysoida tekoälyn tukemana, mikä vähentää manuaalisen työn tarvetta.[186] Tiedustelutoimenpiteillä pystytään estämään terroritekoja, ja sitä kautta ylläpitämään valtakunnan sisäistä turvallisuutta ja yhteiskunta rauhaa.[187]

[181] Hanninen & muut, 2017, s. 94.
[182] HE 55/2018, s. 22 ja s. 27.
[183] COM/2023/0729.
[184] Esko, 2017, s. 116.
[185] Oikeusministeriö, 2023.
[186] Suojelupoliisi, 2023.
[187] Lohse, 2005, s. 1187.

4 Tekoälyasetuksen merkitys EU:n oikeusjärjestyksessä

Tekoälyltä puuttuu yksiselitteinen määritelmä, mutta sen keskeisiä piirteitä ovat itsenäisyys, sopeutumiskyky ja koneoppiminen, jotka erottavat sen perinteisistä tietojärjestelmistä. Koneoppiminen voi tapahtua eri autonomisuuden asteilla ja erityisesti syväoppiminen kehittyy pitkälti ilman ihmisen jatkuvaa valvontaa.[188]

4.1 Jännitteet EU:n tekoälyasetuksen ja perusoikeuksien välillä

Euroopan komissio esitti huhtikuussa 2021 ehdotuksen maailman ensimmäisestä tekoälyä koskevaksi asetukseksi, joka tunnetaan nimellä Tekoälyasetus, jonka Euroopan parlamentti ja neuvosto hyväksyivät joulukuussa 2023. (Tekoälyasetus 2024/1689) Säädöksen tavoitteena on luoda yhtenäiset säännöt tekoälyjärjestelmien kehittämiselle, markkinoille saattamiselle ja käytölle Euroopan unionissa. Säädöksellä pyritään varmistamaan, että tekoälyjärjestelmät ovat turvallisia, perusoikeuksia kunnioittavia ja EU:n arvojen mukaisia. Tekoälyasetus astui voimaan 1. elokuuta 2024.[189] Euroopan neuvoston tekoälyä ja perusoikeuksia koskeva puiteyleissopimus (2024/2218) tarjoaa kansainvälisen sääntelykehyksen, joka tukee EU:n omaa tekoälystrategiaa ja sen lainsäädäntöä. Sopimus on merkittävä askel kohti tekoälyn eettistä ja oikeudellisesti kestävää kehitystä, mutta samalla se jättää kansallisen turvallisuuden tekoälyn käytön jäsenvaltioiden päätettäväksi. Tämä voi aiheuttaa ristiriitoja sääntelyn yhtenäisyyden ja valvontateknologian hyväksyttävyyden välillä.[190]

Tekoälyvaliokunta perustettiin ohjaamaan ja säätelemään tekoälyn käyttöä antamalla suosituksia lainsäätäjille, muun muassa reunaehdoista, teknisistä standardeista ja riskienhallinnasta. (2020/2684RSO) Perustuslakivaliokunnan lausunnossa korostetaan, että sääntelyn tulee turvata muun muassa yksityisyyden suoja, syrjimättömyys ja oikeudenmukainen oikeudenkäynti, erityisesti silloin, kun tekoälyä käytetään julkisessa

[188] Raskulla, 2023, s. 3.
[189] Euroopan komissio, 2024.
[190] EU 2024/2218.

hallinnossa ja rikostorjunnassa.[191] Perustuslakivaliokunta tarkasteli tietosuoja-asetuksen ja tekoälyn yhdistelmää ja huomautti, että tekoälyn päätöksenteon läpinäkyvyys ja oikeussuojakeinot ovat erityisen tärkeitä perusoikeuksien näkökulmasta. [192] Yleiseurooppalaisen sopimuksen avulla pyritään yhdistämään tekoälyä ja oikeusvaltioperiaatetta, jotka takaavat tekoälyn läpinäkyvyyttä, perus- ja ihmisoikeuksien suojan, sekä valvonta- ja vastuumekanismit. [193] EU on pyrkinyt sääntelemään tekoälyn käyttöä osana laajempaa turvallisuuspolitiikkaansa. EU:n turvallisuusunionistrategia, esittää tekoälyn keskeisenä työkaluna rikostorjunnassa, terrorismin ehkäisyssä ja rajavalvonnassa.[194] Tämä linjaus näkyy myös kansallisessa sääntelyssä, joka sääntelee henkilötietojen käsittelyä rikosasioissa ja kansallisen turvallisuuden ylläpitämisessä.[195]

Tekoälyn sääntely merkitsee sen asteittaista oikeudellistumista, mikä heijastuu vaatimuksina sääntelyn ennakoitavuudelle, lainalaisuudelle ja yksilön oikeussuojalle. Tämä tekee tekoälypohjaisesta valvonnasta julkisen vallan käyttämää toimintaa, johon tulee voida soveltaa oikeusvaltioperiaatteen ydinkriteerejä.[196] Tekoälyasetus perustuu riskiperusteiseen lähestymistapaan, jossa tekoälyjärjestelmät luokitellaan niiden aiheuttaman riskin perusteella. Lähestymistapa perustuu riskiarviointiin, jossa tekoälyn käytön vaikutukset ihmisiin ja yhteiskuntaan määrittävät sen sääntelytarpeen. [197] Tekoälyasetusehdotuksessa tekoälyjärjestelmät luokitellaan niiden käyttötarkoituksen perusteella neljään riskitasoon:

1. Ei-hyväksyttävä riski: Tällaiset järjestelmät katsotaan vakavaksi uhaksi kansalaisten perusoikeuksille ja turvallisuudelle, ja ne kielletään kokonaan. Esimerkkejä ovat valtiollinen sosiaalinen pisteytys yksilön käyttäytymisen

[191] PeVL 37/2021 vp, s. 3–4.
[192] PeVL 14/2018 vp, s. 5–6.
[193] EU 2022/2349.
[194] COM/2020/605 final.
[195] HE 31/2018 vp, s. 12.
[196] Widlund, 2024, s. 104-105.
[197] Kallioniemi, 2022, s.259.

perusteella sekä tekoälyä hyödyntävät puhuvat lelut, jotka voivat houkutella lapsia vaaralliseen toimintaan.

2. Suuri riski: Tekoälyjärjestelmät, jotka voivat vaarantaa yksilöiden terveyttä, turvallisuutta tai perusoikeuksia, ja ne kohdistuvat muun muassa kriittiseen infrastruktuuriin (esim. liikenne), koulutukseen (esim. kokeiden pisteytys), terveydenhuollon turvallisuuskomponentteihin (esim. robottikirurgia), rekrytointiin ja työelämään (esim. CV:n lajittelu), olennaisiin palveluihin (esim. luottopisteytys), lainvalvontaan (esim. todisteiden arviointi) sekä maahanmuuttoon ja rajavalvontaan.
3. Vähäinen riski: Näissä järjestelmissä edellytetään läpinäkyvyyttä ja selkeyttä käyttäjälle. Esimerkiksi palvelubottien tulee ilmoittaa selvästi, että vuorovaikutus tapahtuu tekoälyn eikä ihmisen kanssa.
4. Minimaalinen riski: Suurin osa tekoälyjärjestelmistä kuuluu tähän luokkaan. Näihin kuuluvat esimerkiksi roskapostisuodattimet ja tekoälyä hyödyntävät pelisovellukset. Näihin ei kohdistu asetuksen mukaisia velvoitteita, mutta toimijat voivat halutessaan noudattaa vapaaehtoisia eettisiä ohjeistuksia ja käytännesääntöjä.[198]

Käytännössä tämä tarkoittaa, että tekoälyjärjestelmien kehittäjien ja käyttäjien on arvioitava järjestelmiensä riskitaso ja varmistettava, että ne täyttävät säädöksen mukaiset vaatimukset. Ei-hyväksyttäviä ovat kaikki sellaiset käyttötarkoitukset, jotka ovat Euroopan unionin keskeisten arvojen vastaisia. Ne ovat yksityiskohtaisesti määritelty asetusehdotuksen 5 artiklassa. Selkeämmin nämä kielletyt käyttötarkoitukset on kuvattu työ- ja elinkeinoministeriön muistiossa EU/2021/0414 kohdassa 3.4. Kiellettyjä tekoälyn käyttötarkoituksia ovat alitajuinen manipulointi, joka voi aiheuttaa fyysistä, psyykkistä tai materiaalista haittaa. Reaaliaikainen biometrinen etätunnistus julkisilla paikoilla on pääosin kielletty paitsi erityistapauksissa, kuten kadonneiden lasten etsinnässä, turvallisuusuhkien torjunnassa tai rikoksentekijän paikantamisessa.[199]

[198] COM/2021/206final s. 13.
[199] Kallioniemi, 2022, s. 259–260.

Asetusehdotuksen toinen tekoälyjärjestelmien käyttöluokka koskee suuren riskin tekoälyjärjestelmiä. Suuririskisistä tekoälyjärjestelmistä säädetään asetusehdotuksen artiklassa 6, minkä lisäksi suuririskisten käyttötarkoitusten piiriä on täsmennetty asetusehdotuksen liitteessä II. Viranomaisaineistossa myös korkean riskin tekoälyjärjestelmät on selkeimmin määritelty työ- ja elinkeinoministeriön muistiossa EU/2021/0414 kohdassa 3.5. Korkean riskin tekoälyjärjestelmien käyttö on rajattava tapauksiin, joissa järjestelmillä on merkittävä haitallinen vaikutus ihmisten terveyteen, turvallisuuteen tai perusoikeuksiin Euroopan unionin alueella. [200] Esimerkiksi suuririskisten järjestelmien osalta vaaditaan tiukkoja vaatimuksia, kuten riskejä lieventäviä järjestelmiä, laadukasta data-aineistoa, ihmisen valvontaa ja käyttäjälle annettavia selkeitä tietoja.[201]

Tekoälyasetuksen tavoitteena on varmistaa, että Euroopan unionissa käytettävät tekoälyjärjestelmät ovat turvallisia sekä perusoikeuksia ja unionin arvoja kunnioittavia. Liian tiukka sääntely voi hidastaa tekoälyteknologian kehitystä ja käyttöönottoa, kun taas liian löyhä sääntely saattaa johtaa perusoikeuksien, kuten yksityisyyden suojan, vaarantumiseen.[202] Tekoälyjärjestelmien monimutkaisuus ja läpinäkymättömyys, kuten algoritmien päätöksentekoprosessien ymmärtäminen ja mahdollisten syrjivien vaikutusten havaitseminen voivat vaikeuttaa perusoikeusvaikutusten arviointia. Säädöksen tehokas täytäntöönpano edellyttää jäsenvaltioiden viranomaisilta riittäviä resursseja ja asiantuntemusta valvoa tekoälyjärjestelmien noudattamista perusoikeuksia koskevien vaatimusten osalta. Tämä voi olla haasteellista erityisesti nopeasti kehittyvän teknologian ja resurssien rajallisuuden vuoksi. [203] Vaikka tekoälyn riskit on otettava huomioon, on yhtä tärkeää hyödyntää tekoälyn mahdollisuudet tavalla, joka edistää yhdenvertaisuutta ja innovaatioita eikä lisää eriarvoisuutta.[204]

[200] Kallioniemi, 2022, s. 260–261.
[201] Euroopan komissio, 2024.
[202] PWC, 2024.
[203] PWC, 2024.
[204] Ojanperä, 2023, s. 126.

EU:n tekoälyasetus pyrkii tasapainottamaan teknologisen kehityksen ja kansalaisten perusoikeuksien suojelun. Artikla 5 kieltää reaaliaikaisen biometrisen valvonnan julkisilla paikoilla, mutta sallii poikkeuksia kansallisen turvallisuuden ja rikosten estämisen perusteella. Tämä voi kuitenkin olla ristiriidassa perusoikeuskirjan artiklojen 7 ja 8 kanssa, jotka takaavat yksityiselämän ja henkilötietojen suojan. Korkean riskin tekoälyjärjestelmien sääntelyllä (artiklat 6 ja 60) pyritään minimoimaan mahdolliset haitat erityisesti oikeusjärjestelmässä. Tekoälyn käyttö lainvalvonnassa voi kuitenkin artiklan 21 vastaisesti johtaa syrjintään, jos algoritmien koulutusaineisto on vinoutunutta tai niiden valvonta on puutteellista. Lisäksi artikla 60 sallii korkean riskin tekoälyjärjestelmien testaamisen todellisissa olosuhteissa ennen markkinoille saattamista, mikä voi altistaa henkilöitä epäeettisille käytännöille. Erityisesti jos osallistujien tietoiseen suostumukseen (artikla 61) ei kiinnitetä riittävästi huomiota.

Tekoäly pystyy analysoimaan valtavia tietomääriä, jonka takia laillinen sääntely on ratkaisevan tärkeää perusoikeuksien turvaamiseksi. [205] Euroopan komissio päätti tammikuussa 2024 perustaa Euroopan tekoälytoimiston (AI Office). Sen keskeisiin tehtäviin kuuluu yleiskäyttöisten tekoälymallien, kuten kehittyneiden kielimallien ja valvontajärjestelmien seuranta, sekä niiden vaikutusten arviointi perusoikeuksiin ja turvallisuuteen. Lisäksi toimisto valvoo ja tutkii mahdollisia tekoälymääräysten rikkomuksia, erityisesti korkean riskin tekoälyjärjestelmien osalta. Se kehittää myös välineitä ja menetelmiä järjestelmien riskinarviointiin. Tekoälytoimisto edistää kansainvälistä yhteistyötä G7-maiden ja kansainvälisten järjestöjen kanssa. [206] EU:n tekoälyasetuksen artiklan 64 mukaisesti tekoälytoimisto yhdessä Euroopan tekoälylautakunnan kanssa vastaa asetuksen toimeenpanon ja markkinavalvonnan koordinoinnista koko unionin alueella.[207]

[205] Ojanperä, 2023, s. 173.
[206] C/2024/1459.
[207] C/2024/390.

4.2 EU:n tekoälysääntelyn kehitys vuosina 2019–2025

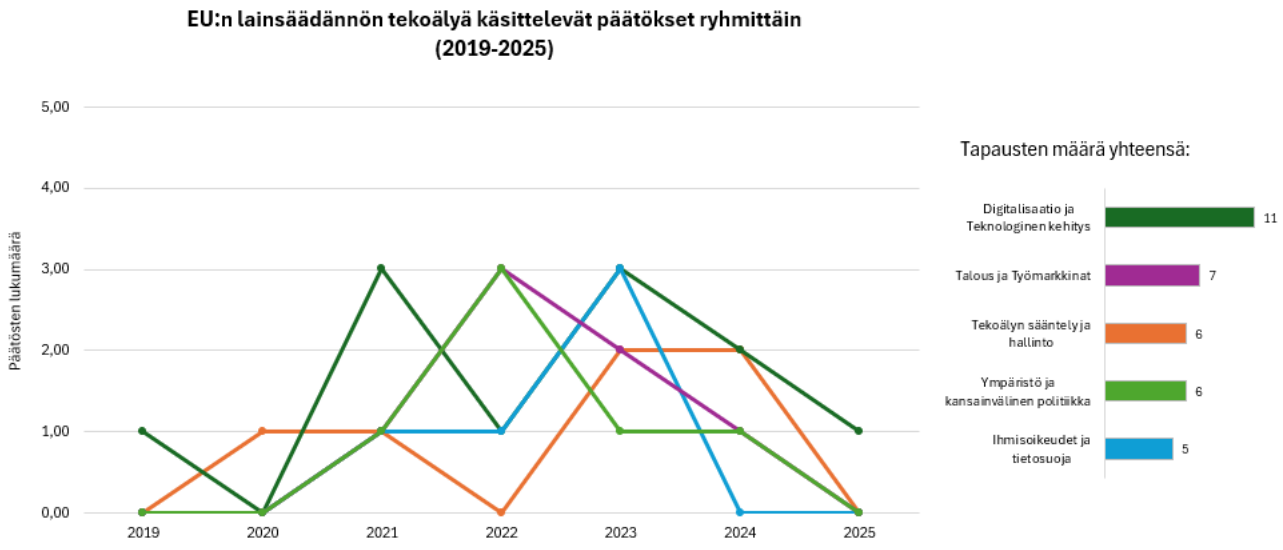
Tekoälyn nopea kehitys on lisännyt merkittävästi tarvetta yhteiseurooppalaiselle ohjaukselle, jotta uudet teknologiat hyödyttäisivät yhteiskuntaa eivätkä vaarantaisi perusoikeuksia tai turvallisuutta. Tässä alaluvussa syvennytään konkreettisiin päätöksiin ja säädöksiin, jotka Euroopan unioni on vuosina 2019–2025 hyväksynyt tai esittänyt ja joiden tarkoituksena on säädellä tekoälyn käyttöä eri osa-alueilla. Kuten seuraava taulukko osoittaa, päätösten määrä ja painopisteet vaihtelevat vuosittain, mikä kertoo paitsi EU:n poliittisista painotuksista myös globaalista kehityksestä tekoälyn alalla:

Ryhmä	Päätösnumero	Päätöksen nimi
Tekoälyn Sääntely ja hallinto	2020/2684(RSO)	Tekoälyvaliokunnan asettaminen
	2021/2802(RSO)	Erityisvaliokuntien ja tutkintavaliokunnan jäsenmääristä
	(EU) 2022/2349	Neuvottelut tekoälyä ja oikeusvaltioperiaatetta koskevasta yleissopimuksesta
	(YUTP) 2022/2269	Vastuullisen tekoälyinnovaation edistäminen rauhaa ja turvallisuutta varten hanke
	C/2024/390	Euroopan tekoälytoimiston perustaminen
	(EU) 2024/2218	Tekoälyä ja ihmisoikeuksia koskevan puiteyleissopimuksen allekirjoittaminen
Digitalisaatio ja Teknologinen Kehitys	(EU) 2019/1765	Sähköisten terveyspalvelujen viranomaisverkoston perustaminen
	(EU) 2021/764	Horisontti Eurooppa erityisohjelman perustaminen ja 2013/743/EU kumoaminen
	(EU) 2021/820	Innovaatio- ja teknologiainstituutin strateginen innovaatio-ohjelma 2021-2027
	(EU) 2021/2084	Unionin osallistuminen metrologiaa koskevaan kumppanuuteen
	(EU) 2022/2481	Digitaalinen vuosikymmen 2030 -ohjelma
	(EU) 2023/729	FADO-järjestelmän tekninen rakenne
	(EU) 2023/1353	Digitalisaatiotavoitteiden saavuttamisen mittarit
	C/2023/4288 final	Digitaalisen vuosikymmenen suorituskykyindikaattorit
	(EU) 2024/459	Eurooppalaisen digitaali-infrastuktuurikonsortion perustamisesta
	C/2024/0391 final	Eurooppalaisen digitaali-infrastuktuurikonsortion perustamisesta
	C/2025/341	Euroopan parlamentin avointa dataa koskevista säännöksistä
Ihmisoikeudet ja Tietosuoja	(EU) 2021/27	Biometristen tietojen avulla tapahtuvan joukkovalvonnan kieltämistä koskeva kansalaisaloite
	(EU) 2022/254	Korean tietosuojalain riittävä henkilötietojen suojan taso
	(EU) 2023/1338	Lastentuotteiden turvallisuusvaatimukset
	C/2023/4099 final	Lastentuotteiden turvallisuusvaatimusten standardien täytyttävä
	(EU) 2023/1795	EU:n ja Yhdysvaltojen tietosuojakehityksen tietosuojan riittävyys
Talous ja Työmarkkinat	(EU) 2021/1868	Jäsenvaltioiden työllisyyspolitiikan suuntaviivoista (2021)
	(EU) 2022/1920	Valtiontuki Romanian yritykselle Complexul Energetic Oltenia SA
	(EU) 2022/2296	Jäsenvaltioiden työllisyyspolitiikan suuntaviivoista (2022)
	230/22/KOL	Tutkimus- ja kehitystoiminnan valtiontuki
	(EU) 2023/936	Euroopan osaamisen teemavuodesta
	(EU) 2023/2528	Jäsenvaltioiden työllisyyspolitiikan suuntaviivoista (2023)
	(EU) 2024/3134	Jäsenvaltioiden työllisyyspolitiikan suuntaviivoista (2024)
Ympäristö ja Kansainvälinen Politiikka	(EU) 2021/1094	Hiili- ja terästutkimusrahaston ohjelman hyväksyminen ja suuntaviivojen 2008/376/EY muuttaminen
	(EU) 2022/591	Unionin ympäristöalan toimintaohjelma
	(YUTP) 2022/582	Rajoittavat toimenpiteet Ukrainan toimiin vaikuttavan päätöksen 2014/145/YUTP muuttamisesta
	(YUTP) 2022/2320	Innovoinnin vapauttaminen: mahdollistavat teknologiat ja kansainvälinen turvallisuus hanke
	(YUTP) 2023/572	Rajoittavat toimenpiteet Ukrainan toimiin vaikuttavan päätöksen 2014/145/YUTP muuttamisesta

Taulukko 4 EU:ssa tehdyt päätökset tekoälystä 2019–2025

Aineisto on haettu EUR-Lex tietokannasta etsimällä EU:n lainsäädännöstä päätökset, joissa mainitaan sana *”tekoäly”.* Hakutulokset rajattiin vuosille 2015–2024, jolloin löydettiin yhteensä 35 EU lainsäädännön tapausta. Vaikka rajaus tehtiin 2015 vuodesta asti, hakutuloksia saatiin ainoastaan 2019–2025 vuosilta. Aineiston analyysissa

sovellettiin määrällistä tutkimusotetta, jossa kartoitettiin tekoälyn mainintojen esiintymistä ja jakaantumista eri oikeudellisiin asiakirjoihin. Päätökset luokiteltiin viiteen ryhmään: Tekoälyn sääntely ja hallinto, Digitalisaatio ja teknologinen kehitys, Ihmisoikeudet ja tietosuoja, Talous ja valtiontuki, sekä Ympäristö ja kansainvälinen politiikka. Näiden ryhmien avulla pyrittiin hahmottamaan tekoälysääntelyn laajuutta ja painopistealueita EU-lainsäädännössä. Luokittelu tehtiin asiakirjojen ensisijaisen sääntelykohteen perusteella, jolloin huomioitiin asiakirjan rakenne, avainsanat sekä aiempaan EU-lainsäädäntöön tehdyt viittaukset. Näin syntynyt kokonaisuus sisälsi paitsi suoria viittauksia tekoälyyn, myös epäsuoria mainintoja esimerkiksi massavalvontaa ja dataintensiivisiä teknologioita käsittelevissä asiakirjoissa. Huomionarvoista on, ettei yksikään näistä tapauksista liity suoraan Euroopan unionin tuomioistuimen (EUT) ratkaisuihin. Tämä viittaa siihen, että tekoälyä koskeva sääntely on vasta kehittymässä oikeuskäytännön tasolla ja painopiste on toistaiseksi ollut lainsäädännössä ja ohjausasiakirjoissa. Taulukon pohjalta tuloksia visualisoitiin kaavion avulla.:



Kuvio 2 EU:n lainsäädännön tekoälyä käsittelevät päätökset ryhmittäin (2019–2025)

Tekoälyyn liittyvien mainintojen nopea kasvu vuosien 2019–2025 aikana korreloi Euroopan komission ja EU:n lainsäädäntöelinten lisääntyneen kiinnostuksen kanssa tekoälyteknologioiden sääntelyyn ja vaikutuksiin yksilönvapauksien näkökulmasta. Kun

sama haku suoritettiin 2014–2019 vuosilta, hakutuloksia saatiin ainoastaan kaksi kappaletta, ja nyt vuosien 2019–2025 aikana tuloksia oli 35 kappaletta. vuonna 2018 julkaistu Euroopan komission tiedonanto "*Koordinoitu tekoälysuunnitelma*" loi perustan EU:n laajamittaiselle tekoälystrategialle, jonka toimeenpano on näkynyt konkreettisina säädöksinä vuodesta 2019 eteenpäin.[208] Toiseksi tekoälyn käyttöön liittyvät riskit ja eettiset kysymykset nousivat esiin kansainvälisessä keskustelussa, mikä vaikutti EU:n sääntelyyn. Esimerkiksi Kiinan laajamittaiset valvontateknologiat ja Yhdysvaltojen tekoälyalan dominointi loivat painetta Euroopalle kehittää omia sääntelymallejaan.

Kaavion mukaan vuosina 2020–2022 etenkin digitalisaatiota ja teknologista kehitystä koskevien päätösten lukumäärä on kasvanut. Tässä vaiheessa EU on pyrkinyt vauhdittamaan investointeja tekoälyn tutkimukseen ja käyttöönottoon, mikä näkyy esimerkiksi Horisontti Eurooppa -ohjelmassa, joka on Euroopan unionin tutkimuksen ja innovoinnin puiteohjelma kaudelle 2021–2027. Ohjelman tavoitteena on vahvistaa EU:n tieteellistä ja teknologista perustaa, edistää innovaatioita ja vastata keskeisiin globaaleihin haasteisiin. Ohjelman perustana on Euroopan parlamentin ja neuvoston asetus (EU) 2021/695, jonka pohjalta neuvosto antoi 10. toukokuuta 2021 päätöksen (EU) 2021/764, jolla perustettiin erityisohjelma Horisontti Euroopan toteuttamiseksi. [209] Tekoälyn nopea käyttöönotto julkisella ja yksityisellä sektorilla on lisännyt tarvetta oikeudellisille kehyksille, jotka varmistavat teknologian vastuullisen käytön. Vuodesta 2021 alkaen tekoälyn tietosuojavaikutuksia ja ihmisoikeusulottuvuuksia koskevat päätökset ovat lisääntyneet. Esimerkiksi huhtikuussa 2021 Euroopan komissio esitti tekoälypaketin, joka sisältää ehdotuksen tekoälyä koskevaksi sääntelykehykseksi ja siihen liittyvän vaikutustenarvioinnin.[210]

Vuodesta 2023 alkaen ihmisoikeus- ja tietosuojakysymykset, kuten biometrisen joukkovalvonnan kieltämistä koskevat ehdotukset ovat nousseet esiin, mikä heijastaa

[208] COM/2018/795 final.
[209] (EU) 2021/764.
[210] COM/2018/237 final.

kansalaisten huolta massavalvonnasta ja tarvetta selkeälle oikeudelliselle kehikolle. Euroopan komission tekoälystrategiassa korostetaan huippuosaamista ja luottamusta, pyrkien varmistamaan, että tekoäly on ihmiskeskeistä ja luotettavaa. Sääntelyllä pyritään varmistamaan tekoälyn vastuullinen ja turvallinen käyttö. EU:n tiukka sääntelykehys saattaa asettaa rajoitteita yritysten tekoälykehitykselle. Toisaalta EU:n lähestymistapa korostaa eettisiä periaatteita, yksityisyydensuojaa ja läpinäkyvyyttä, mikä voi pitkällä aikavälillä lisätä luottamusta tekoälyyn. Sääntelyllä on siis kaksijakoinen vaikutus. Lyhyellä aikavälillä se voi hidastaa teknologista kehitystä, mutta pitkällä aikavälillä edistää kestävää ja vastuullista tekoälyekosysteemiä EU:ssa.

Se, että tekoälyyn liittyviä tapauksia ei ole vielä käsitelty Euroopan unionin tuomioistuimessa saattaa viitata siihen, että sääntelyn oikeudellinen soveltaminen ja mahdolliset kiistat ovat vielä varhaisessa vaiheessa. Analyysi osoittaa, että tekoäly on nousemassa merkittäväksi sääntelykohteeksi EU-oikeudessa. Vaikka oikeuskäytännön tasolla tekoälyyn liittyviä ratkaisuja ei ole vielä nähty, lainsäädännöllinen keskustelu on kiihtynyt merkittävästi vuodesta 2015 lähtien.

EU:n tekoälysääntelyn kehitys vuosina 2019–2025 viittaa siihen, että tekoälyn oikeudellinen kehys tulee edelleen laajenemaan ja monimutkaistumaan. Seuraavina vuosina voidaan odottaa lainsäädännön täsmentymistä ja uusien ohjeistusten käyttöönottoa tekoälyn eettisistä ja oikeudellisista reunaehdoista sekä ensimmäisiä oikeudellisia ennakkotapauksia, joissa EUT ottaa kantaa tekoälyyn liittyviin sääntelykiistoihin. Lisäksi on todennäköistä, että tekoälyyn liittyvä geopoliittinen ulottuvuus korostuu entisestään, kun EU pyrkii määrittelemään oman sääntelymallinsa suhteessa esimerkiksi Yhdysvaltoihin ja Kiinaan. Jatkossa sääntelyssä voi myös painottua sektorikohtainen lähestymistapa, jossa tekoälyä koskevat vaatimukset eriytyvät eri toimialoille, kuten terveydenhuoltoon, finanssialalle ja julkiseen hallintoon. Tämän kehityksen myötä tekoälyn sääntely EU:ssa tulee yhä kiinteämmin osaksi laajempaa digitaalista ja taloudellista strategiaa.

4.3 Tekoälyasetuksen rooli EU:n lainsäädännön tulevaisuudessa

EU:n Tekoälyasetus ei ole pelkästään nykyhetken sääntelyväline, vaan se ohjaa myös tulevaisuuden lainsäädäntöä teknologian hallinnassa. Lainsäädännön kehityksen tulee perustua jatkuvaan oikeusperiaatteiden arviointiin, jotta sääntely vastaa teknologian kehitystä. Sääntely jää usein teknologian kehityksen jälkeen. Viljanen kutsuu tätä "*reaktiiviseksi sääntelyksi*", joka toimii vasta kriisin jälkeen.[211] Tekoälyasetus luo pohjan tekoälyn vastuulliselle kehitykselle ja käytölle EU:ssa. Vastuullisuus on keskeinen osa kestävää tuottavuuden kasvua. Tekoälyn strateginen hyödyntäminen ei saisi perustua pelkkään tehokkuuteen, vaan sen tulisi tukea myös hyvinvointia, osallisuutta ja yhteiskunnallista kestävyyttä. [212] Artiklat 95 ja 96 korostavat vapaaehtoisten käytännesääntöjen ja ohjeistusten merkitystä, jotka täydentävät sitovia sääntöjä ja tukevat eettisesti kestävää tekoälykehitystä (Tekoälyasetus EU 2024/1689). Koska kovaa lainsäädäntöä ei aina voida tuottaa riittävän nopeasti, Viljanen painottaa pehmeän sääntelyn (esim. käytännesäännöt, ohjeistukset ja suositukset) kasvavaa roolia teknologian eettisten haasteiden hallinnassa. Näillä voidaan paikata lainsäädännön aukkoja ainakin tilapäisesti.[213]

Suomessa tuomioistuimilla on ratkaisupakko, eli niiden on käsiteltävä kaikki niille tulevat tapaukset voimassa olevan lainsäädännön pohjalta, vaikka tekoälyn erityispiirteitä ei olisikaan suoraan huomioitu nykyisissä säädöksissä.[214] EU:n nykyinen sääntely, kuten tietosuoja-asetus ja tekoälyasetus, eivät riitä kattamaan tekoälyn kaikkia oikeudellisia riskejä. FRA suosittelee perusoikeusvaikutusten arviointia (Fundamentals Rights Impact Assessment, FRIA), mutta se ei ole pakollinen. Tekoälyn kehittäjien oikeudellinen vastuu on epäselvä, mikä voi johtaa tilanteisiin, joissa algoritmin tekemä virheellinen päätös ei johda vastuuseen. [215] EU:n Tekoälyasetus kytkeytyy tiiviisti muihin unionin lainsäädäntöihin. Tekoälyasetuksen artiklat 102–110 päivittävät ja täydentävät aiempia

[211] Viljanen, 2023, s. 1206.
[212] Hallamaa, 2020, s. 87.
[213] Viljanen, 2023, s. 1220.
[214] Kallioniemi, 2022, s. 250.
[215] FRA, 2020, s. 87–91.

asetuksia ja direktiivejä esimerkiksi liikenteen ja terveydenhuollon osalta, mikä korostaa tekoälyasetuksen merkitystä osana laajempaa sääntelykehystä. Sääntelyn tulee ottaa huomioon tekoälyn käyttökonteksti esimerkiksi terveydenhuollossa, hallinnossa tai turvallisuudessa, koska eri aloilla tarvitaan erilaisia oikeudellisia kehyksiä.[216] Lisäksi artikla 112 sisältää arviointi- ja tarkistusmekanismit, jotka takaavat säädöksen ajantasaisuuden ja mukautumisen teknologian kehitykseen. (Tekoälyasetus 2024/1689) Euroopan parlamentti on painottanut, että tekoälyasetuksen jatkuva päivitys on keskeistä teknologian kehityksen ja oikeudellisen varmuuden takaamiseksi.[217]

Julkinen sektori toimii paitsi tekoälyn eettisen kehittämisen säätelijänä myös sen merkittävänä hyödyntäjänä. Sen rooli on keskeinen, koska se voi asettaa toimintatapoja ohjaavia standardeja ja luoda vastuullisuuden kannalta kriittisiä pelisääntöjä samalla hyödyntäen tekoälyä omassa palvelutuotannossaan.[218] Valvonnan on oltava tasapainoista ja läpinäkyvää, jotta se palvelee koko yhteiskuntaa ja tukee perusoikeuksien toteutumista.[219] Digitaalinen vuosikymmen 2030-ohjelma (Digital Decade Policy Programme 2030, DDPP) on EU:n strateginen aloite, jonka tavoitteena on vahvistaa Euroopan digitaalista suvereniteettia ja vauhdittaa tekoälyn sekä muiden kehittyneiden teknologioiden käyttöönottoa. Se tukee tekoälystrategiaa, joka vahvistaa unionin kilpailukykyä ja teknologista itsenäisyyttä.[220] Ohjelma pyrkii vähentämään riippuvuutta kolmansien maiden teknologiasta ja varmistamaan, että digitalisaatio tukee EU:n taloutta, turvallisuutta ja julkisia palveluita.[221] Ohjelman toimeenpanoa seurataan yksityiskohtaisilla mittareilla, jotka määrittävät digitalisaation etenemistä jäsenvaltioissa. Digitaalinen vuosikymmen asettaa neljä keskeistä tavoitetta vuoteen 2030 mennessä:

[216] Viljanen, 2023, s. 1220.
[217] Euroopan parlamentti, 2023 päivitetty 2024.
[218] Ojanen & muut, 2022, s. 112.
[219] Paasonen & Widlund, 2023.
[220] Euroopan komissio, 2024.
[221] C/2023/4288.

1. Digitaaliset taidot ja tekoälyosaaminen: 80 % EU-kansalaisista osaa käyttää digitaalisia palveluita ja tekoälyä hyödyntäviä järjestelmiä. Lisäksi vähintään 20 miljoonaa ICT-asiantuntijaa työskentelee EU:ssa tekoälyosaamisen parissa.
2. Turvalliset ja kestävät digitaaliset infrastruktuurit: Kaikille EU-kansalaisille tarjotaan gigabittiluokan verkkoyhteydet ja 5G-kattavuus. EU:n puolijohdeteollisuuden osuus maailmanmarkkinoista pyritään nostamaan 20 %: iin, ja lisäksi rakennetaan 10 000 ilmastoneutraalia, korkean tietoturvan reunalaskentakeskusta tekoälyn ja hajautetun tiedon käsittelyn tueksi.
3. Yritysten digitalisaatio ja tekoälyn käyttöönotto: 75 % EU:n yrityksistä hyödyntää tekoälyä, pilvipalveluita tai big data -teknologioita, ja 90 % pk-yrityksistä saavuttaa perustason digitaalisen kyvykkyyden. Lisäksi ohjelma tukee tekoäly-startupeja ja pyrkii kaksinkertaistamaan EU:ssa toimivien yksisarvisyritysten määrän.
4. Julkisten palveluiden digitalisaatio: Kaikki julkiset palvelut ovat saatavilla verkossa, mukaan lukien tekoälyavusteiset terveyspalvelut. Lisäksi kaikille kansalaisille taataan pääsy sähköisiin potilastietoihin ja turvalliseen sähköiseen tunnistautumiseen (eID). [222]

Tekoälyasetuksen täysimääräinen soveltaminen alkaa 1. elokuuta 2026. Ensisijainen vaikutus tekoälyasetuksella on sen riskiperusteisessa lähestymistavassa, joka yhdistää teknologian innovaation hallinnan ja eettiset periaatteet. Tekoälyasetus tuo mukanaan järjestelmällisen tavan arvioida riskejä, luokitella niitä ja asettaa vastuita toimijoille eri tasoilla. Suomessa useat viranomaiset, kuten Verohallinto, Kela, Tulli ja Finanssivalvonta, hyödyntävät automaatiota päätöksenteossa. Algoritmit suorittavat osan päätöksistä itsenäisesti, mikä nopeuttaa prosesseja ja tehostaa hallinnon toimintaa.[223] Tuottavuutta edistävät tekoälyratkaisut voivat myös sisältää riskejä, kuten vinoutuneita algoritmeja.

[222] EU 2022/2481.
[223] Raskulla, 2023, s. 19.

Näiden ennakoimiseksi eettinen arviointikehikko tarjoaa rakenteen, jonka avulla voidaan tarkastella tekoälyn vaikutuksia järjestelmällisesti koko sen elinkaaren ajan.[224]

Tekoälyn aiheuttama eriarvoisuus on monimutkainen haaste, johon yksi vaihtoehto on panostaa laadukkaaseen koulutukseen ja uudelleenkoulutukseen, jotta ihmiset voivat sopeutua muuttuvaan työelämään hyödyntämällä tekoälyn tarjoamia mahdollisuuksia. Yksi ehdotettu ratkaisu on perustulo, joka turvaisi kaikkien toimeentuloa, sekä robottivero, joka kohdistuisi yrityksiin, jotka korvaavat ihmistyövoimaa tekoälyllä.[225] Epätäsmällinen sääntely voi luoda epävarmuutta markkinoilla ja hidastaa innovaatioita Euroopassa.[226] Ennakkoluontoisen perusoikeusvaikutusten arviointi on integroitava osaksi järjestelmän käyttöönottoa ja siinä on muun muassa kuvattava järjestelmän käyttötarkoitus, käyttöyhteys, kohderyhmät, potentiaaliset haitat eri ihmisryhmille sekä suunnitellut toimenpiteet riskien lieventämiseksi.[227] Perusoikeuksien ennakkoarvioinnin vaatimus on uutta EU-lainsäädännössä ja heijastelee oikeusvaltioperiaatteen edellyttämää huolellisuusvelvoitetta. Julkisen vallan on ennakolta arvioitava ja ehkäistävä tekoälyn mahdolliset negatiiviset vaikutukset kansalaisten oikeuksiin.[228]

Tekoälyjärjestelmien käyttö voi myös täyttää rikoslain (38:9 §) tarkoittaman tietosuojarikoksen, sillä ne käsittelevät ja hallinnoivat henkilötietoja. Vaikka tietosuojarikoksen kaltaista sääntelyä voitaisiin soveltaa tekoälyn käyttöön, nykyinen asetusehdotus on rikosoikeudellisen laillisuusperiaatteen (PL 2 §) näkökulmasta liian epätäsmällinen. Tämä herättää kysymyksen siitä, voidaanko yksilön oikeuksia tehokkaasti suojella, jos itse sääntelyjärjestelmä perustuu vielä hahmottumattomiin teknisiin ja käsitteellisiin raameihin. Erityisesti tekoälyn määritelmän ja opetusaineiston laadun epäselvyydet tekevät siitä epävarman perustan sääntelylle. Sääntelyn laajuuden, vastuunjaon ja eettisten kysymysten tarkentaminen on välttämätöntä, jotta tekoälyn

[224] Ojanen & muut, 2022, s. 112.
[225] Ojanperä, 2023, s. 132.
[226] Kallioniemi, 2022, s. 273.
[227] EU 2024/1689.
[228] FRA, 2020, s.9–10.

hyödyt voidaan maksimoida ilman, että innovaatiot estyvät tai perusoikeudet vaarantuvat. [229]

Lainsäädäntökehitys tähtää myös yksilöiden oikeusturvan vahvistamiseen. EU-tasolla on valmisteilla säädös tekoälyn aiheuttamasta vastuusta ja vahingonkorvausvelvollisuudesta (AI Liability -direktiiviehdotus), joka varmistaa, että kansalaisilla on mahdollisuus saada korvausta, mikäli tekoälyjärjestelmän toiminta johtaa virheeseen ja oikeudenloukkaukseen.[230] Tekoälyasetuksessa on säädetty suurista hallinnollisista sakoista sääntöjen rikkomisesta: vakavimmista rikkomuksista jopa 7 % globaalista liikevaihdosta tai 35 miljoonaa euroa (kumpi vain on suurempi). [231] Näin korkeat sanktiot viestivät, että EU suhtautuu tekoälyn väärinkäytön ehkäisyyn yhtä vakavasti kuin tietosuojarikkomuksiin. Tekoälyasetus kuuluu EU:n oikeuden suoraan sovellettaviin asetuksiin, eli sitä ei tarvitse erikseen saattaa voimaan kansallisella lainsäädännöllä. EU käyttää yhä useammin suoraan sovellettavia säädöksiä teknologia-alalla, josta muita esimerkkejä ovat muun muassa Data Governance Act (2022), Data Act (2023) ja Digital Services Act (2022), joiden tavoitteena on varmistaa nopea, yhtenäinen ja oikeusvarma sääntely koko unionin alueella. Tekoälyn käyttö edellyttää uudelleenajattelua: tekoäly toimii pikemminkin yhteistyökumppanina kuin pelkkänä työkaluna.[232]

[229] Kallioniemi, 2022, s. 264.
[230] Euroopan parlamentti, 2023.
[231] EU 2024/1689.
[232] Ojanperä, 2023, s. 127.

5 Johtopäätökset

Tutkimuksen perusteella voidaan todeta, että tekoälypohjainen valvonta tarjoaa viranomaisille uusia ja tehokkaita työkaluja turvallisuuden lisäämiseksi, mutta samalla se haastaa perusoikeuksien toteutumisen.[233] Tekoälyllä tehostetut valvontajärjestelmät uhkaavat siirtää tasapainoa liiallisesti turvallisuuden suuntaan, ellei niitä säännellä tarkkarajaisesti ja johdonmukaisesti perusoikeusnormien pohjalta. Erityisesti yksityisyyden ja henkilötietojen suoja asettavat tiukkoja rajoja tekoälyn hyödyntämiselle massavalvonnassa (GDPR, 5 artikla). Euroopan unionin perusoikeusjärjestelmässä lähtökohtana on, että rajoitusten on perustuttava lakiin, oltava välttämättömiä ja oikeasuhtaisia demokraattisessa yhteiskunnassa. (EU:n perusoikeuskirja 52 art. PL 2 ja 10 §.) Tiedustelulainsäädännössä perusoikeuksiin puuttumista on perusteltu yhteisen turvallisuuden, yhteiskuntajärjestyksen ja elintärkeiden toimintojen suojelulla.[234] Yhteisön etu toteutuu yksilöiden oikeuksia turvaamalla, esimerkiksi ennakoivan valvonnan avulla estetty terroriteko turvaa kansalaisten oikeuden elämään ja turvallisuuteen.[235]

Ensimmäinen tutkimuskysymys käsitteli sitä, kuinka EU:n tekoälysääntely turvaa perusoikeudet turvallisuuden varjolla. EU on jo huomioinut perusoikeuksien ja turvallisuuden tasapainoa tekoälyn sääntelyssä. Esimerkkinä 2024 voimaan astunut tekoälyasetus, jossa velvoitetaan kehittäjiä ja käyttäjiä noudattamaan riskinarviointeja, dokumentointia, läpinäkyvyyttä ja ihmisen valvontaa päätöksenteossa.[236] Euroopan ihmisoikeustuomioistuimen oikeuskäytännön mukaan valvonnan on oltava tarkkarajaista, ja sen välttämättömyys on osoitettava konkreettisesti. Massavalvonnalta puuttuu usein konkreettinen näyttö sen tehokkuudesta, jolloin se on ongelmallinen perusoikeusnäkökulmasta.[237] Kansallisen turvallisuuden nimissä toteutettu valvonta ei

[233] COM/2020/605 final.
[234] HE 202/2017 vp, s. 114.
[235] Bruun, 2016, s. 247.
[236] COM/2021/206 final, s. 13.
[237] FRA, 2022, s. 178.

aina ole oikeasuhtaista. Esimerkiksi laaja tietoliikennetiedustelu tai kasvojentunnistusteknologioiden käyttö voi johtaa massavalvontaan, joka asettaa kyseenalaiseksi perusoikeuksien rajoittamisen välttämättömyyden ja oikeasuhtaisuuden . [238] Massavalvonnan käyttö edellyttää siis aina kriittistä harkintaa. Sen tulee olla viimesijainen keino, jolla on aidosti merkittävä turvallisuusvaikutus suhteessa aiheutuviin oikeudenrajoituksiin.

Toinen tutkimuskysymys nosti esille tekoälypohjaisten valvontajärjestelmien käytön eettisiä ja oikeudellisia haasteita. Haaste tekoälyvalvonnassa liittyy yksityisyydensuojaan, syrjintään ja läpinäkyvyyteen, tekoäly on niin hyvä kuin sen käyttämä data. Jos valvontajärjestelmän syöte- tai opetusdata on vinoutunutta, seurauksena voi olla järjestelmällistä syrjintää. Euroopan unionin perusoikeuskirjan 21 artikla kieltää syrjinnän, mutta on havaittu, että tietyt tekoälysovellukset toimivat heikommin vähemmistöjen kohdalla. [239] Esimerkiksi kasvojentunnistus on tutkitusti vähemmän tarkkaa ihonväriltään vähemmistöryhmiin kuuluvien osalta. [240] Samalla tekoälyjärjestelmien päätöksenteko voi olla läpinäkymätöntä (musta laatikko), mikä vaikeuttaa oikeusturvaa ja nostaa ongelman siitä, kenen vastuulla toimet ovat.[241] Tämä haastaa oikeusvaltioperiaatetta ja rikosprosessuaalisia oikeuksia.

Kolmanneksi kysyttiin, miten EU:n lainsäädäntöpäätökset ovat reagoineet tekoälyn yleistymiseen valvonnassa vuosina 2019–2025. Tältä osin havaittiin, että EU on reagoinut varsin aktiivisesti. Se on antanut uutta lainsäädäntöä, kuten mainitun tekoälyasetuksen sekä päivittänyt terrorismin torjuntaa ja poliisiyhteistyötä koskevia säädöksiä, sekä kehittänyt strategioita, joilla pyritään ohjaamaan tekoälyn käyttöä jäsenvaltioissa. EU on siis tunnistanut tekoälyn tuomat uudet riskit. Kuitenkin sääntely on osin jälkikäteistä reagointia teknologian kehitykseen, mikä on johtanut keskusteluun sääntelyn riittävyydestä. Tekoälyn yleistymisen alkuvaiheessa korostuivat digitalisaation

[238] Hankilanoja, 2014, s. 78.
[239] FRA, 2022, s. 59.
[240] Buolamwini & Gebru, 2018.
[241] FRA, 2020, s. 11.

edistäminen, mutta vuodesta 2023 alkaen painopiste on siirtynyt yhä enemmän perusoikeuksien suojaan, konkreettisena esimerkkinä biometrisen joukkovalvonnan kiellon nouseminen esille EU-tason linjauksissa.

Lainsäädännöllä pitää pyrkiä ratkaisemaan edellä mainittuja ristiriitoja. Ensinnäkin on oikeudellisesti varmistettava, että kaikki tekoälyn käyttö valvontatarkoituksiin perustuu laintasoiseen sääntelyyn, joka täyttää perusoikeuksien rajoitusedellytykset. [242] Lainsäätäjän on määriteltävä tarkasti missä tilanteissa viranomaiset saavat käyttää kasvojentunnistusta tai koneoppivia analyysijärjestelmiä, mihin tarkoitukseen, ja millaisin keinoin niiden käyttöä seurataan. Henkilötietojen automaattinen käsittely profilointitarkoituksessa on lähtökohtaisesti kielletty, ellei esimerkiksi kansallinen turvallisuus sitä salli, ja silloinkin rekisteröidyllä on oikeus saada tietoa käsittelystä.[243] Automaattinen profilointi ei saa johtaa henkilöä koskeviin oikeusvaikutuksiin ilman ihmisen tekemää arviointia. Tämä periaate sisältyy myös GDPR:n 22 artiklaan.

Sääntelyn kehittämisessä tulisi painottaa joustavuutta ja ennakoivuutta. On tarpeen luoda mekanismeja, joilla lainsäädäntöä voidaan päivittää nopeammin teknologian kehittyessä. Kansalaisilla on oltava mahdollisuus tietää, missä ja miten heidän tietojaan käytetään tekoälyn avulla viranomaistoiminnassa. Voisiko EU esimerkiksi luoda rekisterin julkisista tekoälyvalvontajärjestelmistä, joihin kansalaisilla olisi vapaa pääsy? Tällaiset toimet voisivat vahvistaa luottamusta viranomaisten toimintaan. EU on jo sisällyttänyt lainsäädäntöön periaatteita kuten privacy by design ja privacy by default, mutta niitä voisi laajentaa tekoälyn kontekstiin. (GDPR 25 artikla) Esimerkiksi vaatimalla, että jokainen valvontaan käytettävä tekoälyjärjestelmä sisältää sisäänrakennettuja suojatoimia, kuten automaattisen tietojen anonymisoinnin tietyssä käsittelyvaiheessa tai algoritmiin integroidun eettisen tarkistimen, joka estää syrjivien vinoumien syntymistä. Oikeudellisten normien ja eettisten periaatteiden tulee kulkea käsi kädessä. Lait antavat rajat, mutta viranomaisten on omassa toiminnassaan noudatettava eettisiä

[242] ks. Viljanen 2001, taulukko.
[243] Hanninen & muut, 2017, s.13–15.

ohjeita ja kunnioitettava kansalaisten perusoikeuksia. Kansalaisten osallistaminen on myös tärkeää. Lainsäädännön kehittämisessä tulee kuulla kansalaisyhteiskuntaa, asiantuntijoita sekä kansalaisia, jotta sääntely vastaa yhteiskunnan arvoja ja huolia. Tekoälyn roolista turvallisuuspolitiikassa käytävän keskustelun ei pidä rajoittua vain teknisiin tai juridisiin piireihin.

Tämä tutkielma nostaa esiin myös jatkotutkimustarpeita, jotka ovat tärkeitä sääntelyn ja oikeuskäytännön kehittämiseksi. Yksi keskeinen jatkotutkimusalue on tekoälyvalvonnan tehokkuuden arviointi suhteessa perusoikeusvaikutuksiin. Toinen tärkeä tutkimusaihe on oikeudellinen vastuu ja oikeusturvakeinot. Jos yksilö joutuu esimerkiksi väärän positiivisen tunnistuksen vuoksi perusteettomasti pidätetyksi tai tarkkailun kohteeksi, ovatko nykyiset oikeusturvakeinot, kuten muutoksenhaku tai vahingonkorvaus riittäviä? EU on lähtenyt omalle linjalleen tekoälyn sääntelyssä, joten olisi arvokasta tutkia miten EU:n malli vertautuu globaalilla tasolla, jossa valvontateknologioita käytetään enemmän valtion työvälineenä. Lopuksi on syytä korostaa, että tekoälyn ja valvonnan suhde on jatkuvasti kehittyvä ilmiö.

Tämä pro gradu -tutkielma on osoittanut, että EU:ssa on tunnistettu tekoälyyn liittyvät uhat perusoikeuksille ja toimiin on ryhdytty lainsäädännön keinoin niiden hallitsemiseksi . Johtopäätöksenä voidaan todeta, että tasapaino turvallisuuden ja vapauden välillä on saavutettavissa vain jatkuvan vuoropuhelun kautta. Lainsäädännön, teknologian ja yhteiskunnan välinen dialogi on välttämätöntä. Sääntelyä on päivitettävä ja kehitettävä nopeammin, viranomaisten on sitouduttava lainsäädännön sääntöihin perusoikeuksien kunnioittamisessa. Kansalaisten on saatava äänensä kuuluviin siinä, mihin suuntaan valvontayhteiskuntaa vai oikeusvaltiota kehitetään. Mikäli tämä vuoropuhelu onnistuu, tulevaisuutemme ei ole pelkkä valvontayhteiskunta, vaan turvallisuutta ja vapautta aidosti yhteensovittava eurooppalainen yhteisö. Jää nähtäväksi, kuinka hyvin EU pystyy säilyttämään tämän jännitteen tasapainon tekoälyn kehittyessä. Ainakin suunta on selvä, ihmisoikeudet on asetettu keskiöön myös tekoälyn aikakaudella.

Lähteet

Aarnio, A. (1989). *Laintulkinnan teoria – Yleisen oikeustieteen oppikirja*. Werner Söderström Osakeyhtiö, Helsinki.

Amnesty. (2020). *Amnesty International Calls for Ban on the Use of Facial Recognition Technology for Mass Surveillance.* Noudettu 12.11.2024 osoitteesta: https://www.amnesty.org/en/latest/research/2020/06/amnesty-international-calls-for-ban-on-the-use-of-facial-recognition-technology-for-mass-surveillance/

Amnesty. (2021). *Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally*. Noudettu 12.11.2024 osoitteesta: https://www.amnesty.org/en/latest/news/2021/07/the-pegasus-project-2/

Barenstein, M. (2019). *ProPublica's COMPAS Data Revisited.* Noudettu 09.10.2024 osoitteesta: https://arxiv.org/pdf/1906.04711

Bossong, R. (2012). *The Evolution of EU Counterterrorism: European Security Policy After 9/11.* Ebook Central.

Brown, I. & Korff, D. (2009). *Terrorism and the Proportionality of Internet Surveillance.* European Journal of Criminology, 6(2), 119–134.

Bruun, N. (2016). *EU:n turvallisuusstrategiat ja niiden oikeudelliset vaikutukset*. Oikeuspoliittisen tutkimuslaitoksen tutkimuksia.

Buolamwini & Gebru. (2018). *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification.* Noudettu 10.10.2025 osoitteesta: https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

Civil Rights Litigation Clearinghouse. (2021). *Williams v. City of Detroit, Case No. 2:21-cv-10827*. U.S. District Court for the Eastern District of Michigan. Noudettu 02.10.2025 osoitteesta https://clearinghouse.net/case/44401/

Dunkelman, O., Luykx A. & Perrin L. (2017). *A Statement of Standardization.*

EDRi. (13.05.2020) *Ban Biometric Mass Surveillance*! Noudettu 13.09.2024 osoitteesta: https://edri.org/our-work/blog-ban-biometric-mass-surveillance/

EDRi. (27.05.2024*). How to fight Biometric Mass Surveillance after the AI Act: A legal and practical guide*. Noudettu 18.12.2024 osoitteesta: https://edri.org/our-work/how-to-fight-biometric-mass-surveillance-after-the-ai-act-a-legal-and-practical-guide/

Esko, A. (2017). *Kansainvälinen oikeus, terrorismi ja sodankäynti.* Defensor Legis N:o 1/2017 s. 102–117. Edilex.

Eurobarometritutkimus nro 58.1, loka-marraskuu. (2002). *Mitä Euroopan unionin kansalaiset pelkäävät.*

Euroopan komissio. (2024). *Tekoälyasetus tulee voimaan.* Noudettu 13.03.2025 osoitteesta: https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_fi

Euroopan parlamentti. (2020). *Opportunities of Artificial Intelligence.* Noudettu 02.03.2025 osoitteesta: Opportunities of Artificial Intelligence

Euroopan parlamentti. (2020). päivitetty 2023. *Artificial intelligence: threaths and opportunities.* Noudettu 14.11.2024 osoitteesta: https://www.europarl.europa.eu/topics/en/article/20200918STO87404/artificialintelligence-threats-and-opportunities

Euroopan parlamentti. (2023) päivitetty (2024). *EU:n Tekoälyasetus on ensimmäinen laatuaan.* Noudettu 01.10.2024 osoitteesta: https://www.europarl.europa.eu/topics/fi/article/20230601STO93804/eu-n-tekoalysaados-on-ensimmainen-laatuaan

Euroopan unionin perusoikeusvirasto (FRA). (2020). *Getting the future right – Artificial intelligence and fundamental rights.* Noudettu 05.01.2025 osoitteesta: https://bin.yhdistysavain.fi/1586428/rg7sk3iw1GBjdjwMhxoy0VdVqT/FRA%20-%20Teko%C3%A4ly%20ja%20perusoikeudet%20-%20raportti.pdf

Euroopan unionin perusoikeusvirasto. (2022). *Fundamental Rights Report 2022.* Noudettu 09.03.2025 osoitteesta: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2022-fundamental-rights-report-2022_en.pdf

Gonçalves, M. E., & Andrade Jesus, I. (2013). *Security policies and the weakening of personal data protection in the European Union.* Teoksessa *Computer Law & Security Review*, Volume 29, Issue 3. s. 255-263. https://www.sciencedirect.com/science/article/pii/S026736491300037X?via%3Dihub

Haenlein & Kaplanin. (2019). *A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence*. ResearchGate.

Hallamaa, J. (2020). *Tulevaisuuden teknologiat ja tekoälyn etiikka*. Helsingin yliopisto.

Hallberg, P. (2005). *Perusoikeudet*. Almatalent.

Hankilanoja, A. (2014). *Poliisin salainen tiedonhankinta.* Talentum.

Hanninen, M., Laine E., Rantala K., Rusi M. & Varhela M. (2017). *Henkilötietojen käsittely: EU-tietosuoja-asetuksen vaatimukset*. Kauppakamari.

Hietanen, H. & Arkia, N. (2017). *Tiedustelulaki ja tuomioistuin prosessin luotettavuus*. Edilex.

Hirvonen, A. (2011). *Mitkä metodit? Opas oikeustieteen metodologiaan*. Helsingin yliopisto.

Husa J, Mutanen A & Pohjalainen T. (2008). *Kirjoitetaan juridiikkaa*. Talentum.

Härkönen, H. (2006). *Terroristiryhmän rikosoikeudellinen sääntely.* Lakimies 2/2006 s. 216–235. Edilex.

Italian Data Protection Authority (Garante per la protezione dei dati personali). (2022). *Ordinanza ingiunzione nei confronti di Clearview AI - 10 febbraio 2022.* Noudettu 14.11.2024 osoitteesta: https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9751362

Jansson, J. (1969). *Politiikan teoria*. Tammi.

Jee, C. (2019). *London police's face recognition system gets it wrong 81 % of the time.* Mit Technology Review. Noudettu 01.02.2025 osoitteesta: https://www.technologyreview.com/2019/07/04/134296/london-polices-face-recognition-system-gets-it-wrong-81-of-the-time/

Joshi, R. (2013). *India's Central Monitorin system*. Takshashila institution.

Kalliojärvi, T. (2016). *EU:n yleinen tietosuoja-asetus: tietoturvallisuudesta henkilötietojen käsittelyssä.* Edilex.

Kallioniemi, I. (2022). Tekoälyoikeus – varallisuusoikeuden ja riskienhallinnan kysymyksiä. Alma Talent.

Koillinen, M. (2002). *Henkilötietojen suoja itsenäisenä perusoikeutena.* Oikeus 2002(42)2, s. 171–193.

Kolehmainen, A. (2015). *Tutkimusongelma ja metodi lainopillisessa työssä. Teoksessa Oikeustieteellinen opinnäyte* – Artikkeleita oikeustieteellisten opinnäytteiden vaatimuksista, metodista ja arvostelusta. Edilex.

Korhonen, R. (2005). *Poliisin valvontakeinot ja kansalaisten yksityisyyden* suoja. Edilex.

Kremer, J. (2017). *The end of freedom in public places? Privacy problems arising from surveillance of the European public space*. Unigrafia.

Lappi-Seppälä T., Rautio I., Hakamies K., Helenius D., Koskinen P., Majanen M., Melander S., Nuotio K., Nuutila A. & Ojala T. (2000). *Rikosoikeus*. Almatalent.

Lefrancois, R. & Barrot J. (2008). *Euroopan Parlamentin keskustelut*. Noudettu 10.10.2024 osoitteesta: https://www.europarl.europa.eu/doceo/document/CRE-6-2008-09-23_FI.pdf .

Locke, J. (2010). *Eavesdropping: An Intimate History.* Oxford University Press.

Lohse, M. (2005). *Rikostiedustelu terrorismin torjunnassa*. Defensor Legis N:o 6/2005. Edilex.

Lohse, M., Meriniemi M. & Honkanen K. (2019). *Tiedustelumenetelmät*. Almatalent.

Mahapatra, S. (2021). *Digital Surveillance and the Threat to Civil Liberties in India*. Giga Focus.

Mäntylä, N. (2023). *Eurooppalainen oikeusvaltio tänään ja huomenna*. Teoksessa Tieto, valta ja vaikuttaminen oikeusvaltiossa. Gaudeamus oy.

Oikeusministeriö. (2013). *Lainkirjoittajan opas (4.1.13) Säädösvalmistelun ohjeistus*. Finlex.

Oikeusministeriö. (2023). *Terrorismilainsäädännön kokonaisuudistus käynnistyy*. Noudettu 11.02.2025 osoitteesta: https://oikeusministerio.fi/-/terrorismilainsaadannon-kokonaisuudistus-kaynnistyy

Ojanen, A., Sahlgren O., Vaiste J., Björk A., Mikkonen J., Kimppa K., Laitinen A. & Oljakka N. (2022). *Algoritmien syrjintä ja yhdenvertaisuuden edistäminen*. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 2022:54.

Ojanen, T. (2007). *Perus- ja ihmisoikeudet terrorismin vastatoimissa Euroopan unionissa*. Lakimies 7–8/2007 s. 1053–1074. Edilex.

Ojanen, T. (2009). *Perus- ja ihmisoikeudet EU-säädösten toimeenpanolakien säätämisessä*. s. 129–174. Teoksessa Puhuri käy: Muuttuva suomalainen ja eurooppalainen valtiosääntömme. Edilex. Ojanen T. (2016). *EU-oikeuden perusteita*. Edita Oy.

Ojanperä, T. (2023). *Tekoälyn vallankumous: käsikirja.* Alma Talent.

Ollila, R. (2014). *Henkilötietojen suoja EU:n perusoikeutena*. Edilex.

Ortamo, P. (2020). YLE. *Poliisi on saanut rikollisia kiinni kasvoja tunnistavan tekoälyn avulla ja haluaisi laajentaa valtuutuksiaan – testasimme, miten kone toimii.* Noudettu 14.11.2024 osoitteesta: https://yle.fi/a/3-11448002

Paasonen, J. & Widlund J. (2023) *Oikeusvaltio ja valvontavaltio. Sähköisen valvonnan haasteet yksityisyydelle ja tietosuojalle*. Teoksessa Tieto, valta ja vaikuttaminen oikeusvaltiossa. Gaudeamus oy.

Pekola, S. (2018) *Tiedustelu oikeusvaltiossa*. Edilex.

Puolustusministeriö. (2010). *Yhteiskunnan turvallisuusstrategia*. Valtioneuvoston periaatepäätös 16.12.2010.

PWC. (2024). *Tekoälyn haasteet ja mahdollisuudet: juridiikan ja riskienhallinnan kysymyksiä.* Noudettu 02.03.2025 osoitteesta: https://uutishuone.pwc.fi/tekoalyn-haasteet-ja-mahdollisuudet-juridiikan-ja-riskienhallinnan-kysymyksia/

Raitio, J. (2016). *Euroopan unionin oikeus*. Almatalent.

Rao, U. & Nair V. (2019). *Aadhaar: Governing with Biometrics*. teoksessa South Asia. Journal of South Asian Studies. Taylor & Francis.

Raskulla, S. (2023). *Tekoäly oikeusvaltiossa? Automaattinen päätöksenteko ja julkisen vallan käyttö.* Teoksessa Tieto, valta ja vaikuttaminen oikeusvaltiossa. Gaudeamus oy.

Rikoksentorjuna.fi. (2021). *Ennakoiva poliisitoiminta – kiistanalainen poliisin työkalu*. Noudettu 18.3.2025 osoitteesta https://rikoksentorjunta.fi/-/haaste-ennakoiva-poliisitoiminta

Roslund, R. (2024). YLE. *Tietovuoto: Putin luo massiivista valvontajärjestelmää – Navalnyin hautajaisiin osallistuneita pidätettiin tekoälyn avulla.* Noudettu 03.10.2024 osoitteesta: https://yle.fi/a/74-20080980

Sanjay, S. (2020). *Data privacy and GDPR Handbook.* Ebook Central.

Scheinin, M. (2009). *Taloudellisten, sosiaalisten ja sivistyksellisten oikeuksien suoja terrorismia torjuttaessa.* Teoksessa Puhuri käy: muuttuva suomalainen ja eurooppalainen valtiosääntömme. Edilex.

Sisäministeriö. (2022:36). *Kansallinen terrorismintorjunnan strategia 2022–2025. Valtioneuvosto.*

Sisäministeriö. (2024). *EU päätti tekoälylle pelisäännöt – näin se vaikuttaa poliisin toimintaan.*

Statista. (2023). *Number of failed, foiled or completed terrorist attacks in the European Union (EU) from 2010 to 2022, by affiliation*. Noudettu 14.11.2024 osoitteesta: https://www.statista.com/statistics/746562/number-of-arrested-terror-suspects-in-the-european-union-eu/

Suojelupoliisi. (2023). *Suojelupoliisissa käynnistyy EU:n osarahoittama tekoälyä soveltava järjestelmähanke.* Noudettu 12.03.2025 osoitteesta: https://supo.fi/-/suojelupoliisissa-kaynnistyy-eu-n-osarahoittama-tekoalya-soveltava-jarjestelmahanke

Taka, A. (2017). *Cross-border application of EU's general data protection regulation* (GDPR).

Taloustutkimus. (2017). *Terrori-iskun todennäköisyys Suomessa vuoden kuluttua*. Noudettu 13.11.2024 osoitteesta: https://yle.fi/a/3-9560214.

Traficom. (2021). *Tekoälyn soveltamisen kyberturvallisuus ja riskienhallinta*. Noudettu 11.11.2024 osoitteesta: https://www.traficom.fi/sites/default/files/media/publication/Teko%C3%A4lyn%20soveltamisen%20kyberturvallisuus%20ja%20riskienhallinta.pdf

Tuori, K. (1999). *Eri perusoikeuksista. Yleinen järjestys ja turvallisuus – perusoikeusko?* Lakimies 98(6–7) 1999, s. 920–931.

Valtiovarainministeriö. (2023). *Digitaalista turvallisuutta voidaan parantaa koneoppimisella.* Noudettu 14.11.2024 osoitteesta: https://valtioneuvosto.fi/-/10623/digitaalista-turvallisuutta-voidaan-parantaa-koneoppimisella

Viljanen, M. (2001). *Perusoikeuksien rajoitusedellytykset*. Helsinki: Lakimiesliiton Kustannus.

Viljanen, M. (2023). *Menikö juna jo? Tekoälyn sääntelemisen mahdollisuuksista*. Edilex

Widlund, J. & Paasonen J. (2021). *Kansallisen turvallisuuden käsite: oikeutta vai politiikkaa?* Edilex.

Widlund, J. (2020). *Kansallinen turvallisuus: vapauden ehto vai rajoitus?* Oikeus 2/2020 s. 134–153. Edilex.

Wuori, M., (2003). *Turmiollista turvallisuutta*. Oikeus 4/2003, s. 397–411.

SÄÄDÖKSET

EU:n Perusoikeuskirja (2000/C 364/01)

EU:n tekoälyasetus (Euroopan parlamentin ja neuvoston asetus (EU) 2024/1689 tekoälysääntelystä)

Laki tiedustelutoiminnan valvonnasta (121/2019)

Poliisilaki (657/2019)

Rikoslaki (19.12.1889/39)

Suomen perustuslaki (731/1999)

Terrorismidirektiivi (Euroopan parlamentin ja neuvoston direktiivi (EU) 2017/541)

Yleinen tietosuoja-asetus (GDPR) (EU 2016/679)

Virallislähteet

HE 309/1993 vp. *Hallituksen esitys Eduskunnalle perustuslakien perusoikeussäännösten muuttamisesta.*

HE 198/2017 vp. *Hallituksen esitys eduskunnalle laiksi Suomen perustuslain 10 §:n muuttamisesta.*

HE 9/2018. *Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi.*

HE 31/2018 vp. *Hallituksen esitys eduskunnalle laiksi henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä sekä eräiksi siihen liittyviksi laeiksi.*

HE 55/2018. *Hallituksen esitys eduskunnalle laiksi lentoliikenteen matkustajarekisteritietojen käytöstä terrorismin ja vakavan rikollisuuden torjunnassa sekä eräiksi siihen liittyviksi laeiksi.*

PeVM 25/1994 vp. *Perustuslakivaliokunnan mietintö n:o 25 hallituksen esityksestä perustuslakien perusoikeussäännösten muuttamisesta.*

PeVL 23/1997 vp. *Hallituksen esitys oikeudenkäyttöä, viranomaisia ja yleistä järjestystä vastaan kohdistuvia rikoksia sekä seksuaalirikoksia koskevien säännösten uudistamiseksi.*

PeVL 14/2018 vp. *Perustuslakivaliokunnan lausunto hallituksen esityksestä eduskunnalle*

EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi.

PeVL 37/2021 vp. *Perustuslakivaliokunnan lausunto valtioneuvoston kirjelmästä eduskunnalle komission ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi tekoälyn harmonisoiduksi sääntelyksi (Artificial Intelligence Act).*

COM (2018) 237 final. *Komission tiedonanto Euroopan parlamentille, Eurooppa-neuvostolle, neuvostolle, Euroopan talous- ja sosiaalikomitealle sekä alueiden komitealle: Koordinoitu tekoälysuunnitelma.*

COM (2018) 795 final. *Komission tiedonanto Euroopan parlamentille, Eurooppa-neuvostolle, neuvostolle, Euroopan talous- ja sosiaalikomitealle sekä alueiden komitealle: Koordinoitu tekoälysuunnitelma.*

COM (2020) 65 final. *Komission valkoinen kirja tekoälyn sääntelystä ja kehittämisestä Euroopassa.*

COM (2020) 605 final. *EU: n turvallisuusunioninstrategiasta.*

COM (2021) 206 final. *Komission tiedonanto Euroopan parlamentille ja neuvostolle EU:n tekoälystrategian etenemisestä.*

COM (2022/720). *Komission asetus Euroopan unionin toiminnasta tehdyn sopimuksen 101 artiklan 3 kohdan soveltamisesta tiettyihin vertikaalisten sopimusten ja yhdenmukaistettujen menettelytapojen ryhmiin.*

COM (2023/0729). *Komission täytäntöönpanopäätös (EU) 2023/729, jossa säädetään Euroopan raja- ja merivartioston asiakirjahallintajärjestelmästä.*

COM (2024/198) final/2. *Komission tiedonanto EU:n turvallisuusunionistrategian täytäntöönpanon edistymisestä ja tulevista toimista.*

Oikeuskäytäntö

EIT 06.09.1978. *Klass ym. v. Saksa.*

EIT 19.02.2009. *A. ym. v. Yhdistynyt kuningaskunta.*

EIT 12.01.2010. *Gillan ja Quinton v. Yhdistynyt kuningaskunta.*

EIT 18.04.2013. *M.K. v. Ranska.*

EIT 25.05.2021. *Big Brother Watch ym. v. Yhdistynyt kuningaskunta.*

EU 2022/2349. *Euroopan unionin puolesta käytävien neuvottelujen aloittamisen valtuuttamisesta Euroopan neuvoston tekoälyä, ihmisoikeuksia, demokratiaa ja oikeusvaltioperiaatetta koskevasta yleissopimuksesta.*

EU 2022/2481. *Digitaalinen vuosikymmen 2030-ohjelma.*

EU 2024/1689. *EU:n tekoälyasetus.*

EU 2024/2218*. Euroopan neuvoston tekoälysopimus.*

EUT C-203/15. *Tele2 Sverige AB ym. (Tele2/Watson).*

EUT C-293/12 ja C-594/12. *Digital Rights Ireland (tietojen säilyttämisdirektiivi).*