Radioviestinnän luottamuksellisuutta koskevien säännösten soveltaminen alusten ja ilma-alusten tunnistamiseen ja seurantaan tarkoitettuihin AIS-, ADS-B- ja RID-radiolähetteisiin

Sisällys

1 Tausta

1.1 Merenkulun AIS-järjestelmä

AIS (Automatic Identification System) on alusten automaattiseen tunnistamiseen käytettävä järjestelmä. Se perustuu aluksiin asennettuihin radiolaitteisiin, jotka jatkuvasti ja automaattisesti lähettävät tähän tarkoitukseen maailmanlaajuisesti varatuilla radiotaajuuksilla aluksen sijainti- ja tunnistetietoja.[1] AIS-lähettimen käyttö Suomessa edellyttää radiolupaa.

Merenkulun AIS-järjestelmän käytön pakollisuudesta säädetään EU:n ns. seurantadirektiivissä.[2] AIS-laitteiden käyttö on kansainvälisen merenkulkujärjestön IMO:n päätöksellä pakollista kaupallisessa liikenteessä olevilla aluksilla. AIS-järjestelmien käyttö perustuu IMO:n SOLAS-yleissopimuksen V luvun 19 sääntöön ja sen nojalla annettuihin määräyksiin. IMO:n mukaan AIS:n tavoitteena on lisätä merenkäynnin ja navigoinnin turvallisuutta sekä suojella merellistä ympäristöä. IMO on kuvannut AIS:n tarkoituksen seuraavasti: "*the purpose of AIS is to help identify ships, assist in target tracking, assist in search and rescue operation, simplify information exchange (e.g. reduce verbal mandatory ship reporting) and provide additional information to assist situation awareness.*"[3]

AIS-yleislähetteiden tiedot tavanomaisesti sisältävät: 1) aluksen dynaamiset tiedot, kuten aluksen paikan, nopeuden, kulkusuunnan ja asetetun statuksen, 2) aluksen staattiset tiedot, kuten aluksen nimen, tunnuksen, meriradionumeron, IMO-numeron ammattialuksissa ja aluksen mitat sekä 3) aluksen matkakohtaiset tiedot, kuten lähtösataman, määräsataman, arvioidun saapumisajan ja aluksen syväyksen. AIS-tiedot jaotellaan A- ja B-laitteiden tietoihin siten, että yksinkertaistetusti A-luokan laitteiden tiedot ovat ammattialusten välittämiä tietoja[4] ja vapaaehtoisten B-luokan laitteiden tiedot pienten alusten ja huviveneiden välittämiä tietoja[5].

Seurantadirektiivillä on perustettu alusliikennettä koskeva unionin seuranta- ja tietojärjestelmä. Direktiivin nojalla kansalliset tiedonhallintajärjestelmät on liitetty yhteisön merenkulun tiedonvaihtojärjestelmään (SafeSeaNet-järjestelmä). Järjestelmä mahdollistaa meriturvallisuuteen, satamien ja merenkulun turvatoimiin, meriympäristön suojeluun sekä meriliikenteen ja merikuljetusten tehokkuuteen liittyvien tietojen vastaanottamisen, tallentamisen, hakemisen ja vaihtamisen. Seurantadirektiivin muutetussa 24(1) artiklassa säädetään, että jäsenvaltion on yhteisön tai kansallisen lainsäädännön mukaisesti toteutettava tarvittavat toimenpiteet niille tämän direktiivin nojalla lähetettyjen tietojen luottamuksellisuuden varmistamiseksi, ja ne saavat käyttää kyseisiä tietoja ainoastaan tätä direktiiviä noudattaen. Direktiivin liitteessä III tarkennetaan, että SafeSeaNet-keskusjärjestelmän ja kansallisten SafeSeaNet-järjestelmien on noudatettava direktiivin vaatimuksia, jotka koskevat tietojen luottamuksellisuutta, sekä IFCD:ssä kuvattuja turvallisuusperiaatteita ja eritelmiä, erityisesti käyttöoikeuksien osalta. IFCD-asiakirjaan sisältyy tietoturvaan liittyviä määräyksiä järjestelmän kyvystä säilyttää tietojen luottamuksellisuus. Asiakirjan mukaan SafeSeaNet-järjestelmän tulee käsitellä tietoa sen luottamuksellisuuden

[1] https://www.digitraffic.fi/meriliikenne/ais/.
[2] Euroopan parlamentin ja neuvoston direktiivi 2002/59/EY alusliikennettä koskevan yhteisön seuranta- ja tietojärjestelmän perustamisesta sekä neuvoston asetuksen 93/75/ETY kumoamisesta.
[3] IMO, Resolution A.1106(29) Adopted on 2 December 2015, Revised guidelines for the onboard operational use of shipborne automatic identification systems (AIS), k. 4.
[4] A-luokan AIS-laite on pakollinen kaikilla kaupallisen liikenteen aluksissa lukuun ottamatta kotimaanliikenteen alle 24 metrisiä matkustaja-aluksia sekä bruttovetoisuudeltaan alle 300 GT lastialuksia.
[5] B-luokan AIS-laitteita on pienemmillä kaupallisen liikenteen aluksilla sekä huviveneillä. A- ja B-luokkien tietosisällöt eroavat toisistaan.

tason mukaisesti.[6] – Seurantadirektiiviin tai IFCD:hen ei kutenkaan sisälly säännöksiä tai määräyksiä AIS-tietojen luottamuksellisuudesta sinänsä tilanteessa, jossa sivulliset ottavat AIS-lähetyksiä vastaan.

Suomessa osa viranomaisten keräämistä AIS-tiedoista on saatavissa avoimena tietoaineistona.[7] Koska AIS-laitteiden lähettämää radioviestintää ei ole salattu, kuka tahansa sopivan laitteen haltija voi vastaanottaa AIS-tietoja selväkielisenä. AIS-tietoja hyödynnetään myös muissa kuin viranomaisten tarjoamissa laivaliikenteen seurantaan ja analysointiin perustuvissa palveluissa. Näissä palveluissa käsiteltävien AIS-tietojen pääasiallisena lähteenä ovat vapaaehtoiset ympäri maailmaa, jotka AIS-signaalien kantaman puitteissa vastaanottavat laivojen ja alusten AIS-viestejä radiovastaanottimilla ja välittävät niitä palveluntarjoajille. Tunnetuin AIS-tietoa hyödyntävä julkinen ja avoin palvelu on MarineTraffic,[8] joka on meriliikennettä lähes reaaliaikaisesti seuraava verkkopalvelu. AIS-tietoja hyödyntävät palvelut MarineTraffic mukaan lukien keräävät tiedot aluksissa olevien AIS-laitteiden lähettämistä viesteistä ja tavanomaisesti näyttävät tiedot omilla lähes reaaliaikaisilla kartoillaan. Esimerkiksi MarineTraffic tallentaa myös historiatietoa alusten liikkeistä, jota voi hakea palvelusta muun muassa aluksen nimellä. AIS-tietoja on mahdollista kerätä myös satelliittien avulla.

1.2 Ilma-alusten ADS-B-järjestelmä

ADS-B (Automatic Dependent Surveillance - Broadcast) on ilma-alusten tunnistamiseen ja niiden sijainnin määrittämiseen käytettävä järjestelmä. Kyseessä on radiolähetin, joka lähettää automaattisesti ilma-aluksen tietoja lyhyin aikavälein. ADS-B-lähetin hyödyntää toisiotutkajärjestelmää (transponderia). ADS-B-transponderin lähete sisältää esimerkiksi ilma-aluksen tunnistustiedon sekä tietoja aluksen korkeudesta ja sijainnista sekä nopeudesta. ADS-B-lähetteitä voi vastaanottaa laitteella, jossa on ADS-B IN -ominaisuus, kuten maa-asema tai toisessa ilma-aluksessa oleva laite. Koska ADS-B-lähetyksiä ei ole salattu, kuka tahansa voi vastaanottaa niiden lähettämiä tietoja selväkielisenä myös yksinkertaisella ohjelmistoradiolla.

Järjestelmä on ensisijaisesti suunniteltu ilmatilan valvojien ja muiden ilmatilan käyttäjien käyttöön. Tietoa hyödynnetään lennonvarmistuksessa ilma-alusten sijainnin määrittämiseen ja ilmaliikennepalvelun antamiseen. Myös kaupallisessa lentotoiminnassa käytettävä ACAS-törmäysvaroitin (Airborne Collision Avoidance System) pohjautuu ADS-B-lähetteisiin. ADS-B-transponderin käyttäminen on pakollista tietyissä tilanteissa, kuten kaupallisessa ilmailutoiminnassa ja eräissä ilmatilan osissa.[9]

ADS-B-tietoja hyödynnetään myös muissa kuin viranomaisten tarjoamissa palveluissa. Tunnetuin tällainen palvelu lienee Flightradar24.[10] ADS-B-tietoja hyödyntävät palvelut keräävät tietoja, joita vapaaehtoiset välittävät palveluun vastaanottamistaan ilma-alusten ADS-B-out-laitteiden lähettämistä radioviesteistä. Palveluista on saatavissa ilma-alusten lentohistoriatietoja.

[6] SAFESEANET Interface and Functionalities Control Document SSN IFCD, versio 1.1.2, 7.7.2016, k. 7.2.2.5.
[7] https://www.digitraffic.fi/meriliikenne/ais/.
[8] https://www.marinetraffic.com/.
[9] Ks. https://www.easa.europa.eu/newsroom-and-events/news/amendment-airspace-requirements-ads-b-and-mode-s ja https://ais.fi/ais/eaip/ge/EF_GEN_1_5_EN.pdf. Vaatimuksista säädetään komission täytäntöönpanoasetuksessa (EU) N:o 1207/2011 yhtenäisen eurooppalaisen ilmatilan valvonnan suorituskykyä ja yhteentoimivuutta koskevista vaatimuksista.
[10] https://www.flightradar24.com/.

1.3 RID-järjestelmä miehittämättömässä ilmailussa

Miehittämättömien ilma-alusten (esim. drone) osalta on tietyissä tilanteissa tulossa pakolliseksi suoran etätunnistuksen järjestelmä (direct remote identification), jolla "varmistetaan toiminnassa olevan miehittämättömän ilma-aluksen tietojen paikallinen lähettäminen, mukaan lukien tieto miehittämättömän ilma-aluksen merkinnästä, jotta nämä tiedot voidaan saada ilman fyysistä kontaktia miehittämättömään ilma-alukseen" (RID-lähete).[11] Kyse on droneen kuuluvasta järjestelmästä, joka lähettää radioluvasta vapailla taajuuksilla tietoja lennätyksestä.

Euroopan unionissa vaatimusta suoran etätunnistuksen järjestelmistä sovelletaan vuoden 2024 alusta.[12] Tämän jälkeen edellytetään yli 250 g painavien laitteiden varustamista RID-järjestelmällä. RID-lähetteeseen sisältyy mm. dronen operaattorin rekisteritunnus, sarjanumero, aikaleima, sijainti, korkeus, kulkusuunta, kauko-ohjaajan sijainti sekä ilmoitus dronen hätätilasta.[13]

Lainsäädännössä ei tarkemmin määritellä tai rajoiteta RID-lähetteen käyttötarkoitusta. Yleisesti ottaen järjestelmä mahdollistaa tietojen käytön erilaisia turvallisuuteen liittyviä tarkoituksia varten. Järjestelmää ei ole suunniteltu erityisesti valvontajärjestelmiä varten, mutta käytetty tekniikka mahdollistaa lähetysten tietojen käytön myös valvontajärjestelmissä. RID:n käyttö lisää yleisön hyväksyntää miehittämättömälle ilmailulle. Toiset dronet eivät juurikaan hyödy toisten RID-lähetteestä. RID-lähetteitä tulee olla mahdollista vastaanottaa erityisten valvontajärjestelmien lisäksi esimerkiksi tavanomaisella matkapuhelimella.[14]

Liikenne- ja viestintävirasto Traficomilla ei ole aiempaa tulkintaa siitä, miten RID-lähetteitä olisi arvioitava suhteessa radioviestinnän luottamuksellisuuteen. Kuitenkin ilmailulakiin (864/2014) lisätyn miehittämättömien ilma-alusten havainnointitoimivaltaa koskevan säännöksen (169 a §, laissa 1327/2021) esitöissä on huomautettu, että vaatimus miehittämättömien ilma-alusten etätunnistusjärjestelmästä tuo osan miehittämättömän ilma-aluksen lennättämisen radioviestinnästä yleisesti vastaanotettavaksi.[15] Sen sijaan dronen *kauko-ohjaukseen* liittyvä radioviestintä on SVPL:n mukaan luottamuksellista.[16] Esimerkiksi aluksen havainnointi ohjausliikennettä käsittelemällä edellyttää erikseen laissa säädettyä toimivaltuutta.[17]

1.4 Nykytilanne ja uudelleenarvioinnin tarve

Traficom on aiemmin lainsäädännön soveltamista koskevassa neuvonnassaan tehnyt tulkinnan, että ADS-B-lähetettä tulee pitää luottamuksellisena ilmailuradioviestintänä. Tulkinta on perustunut siihen, että sähköisen viestinnän palveluista annetun lain mukaan luottamuksellista on sellainen radioviestintä, jota ei ole tarkoitettu yleisesti vastaanotettavaksi (917/2014, SVPL, 136.2 §). ADS-B-lähete ei kuulu mihin-

[11] Komission täytäntöönpanoasetus (EU) 2019/947 säännöistä ja menetelmistä miehittämättömien ilma-alusten käytössä, 2 art. 13 kohta (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02019R0947-20220404).
[12] Komission täytäntöönpanoasetus (EU) 2019/947 20, 22 ja 23 art. muutoksineen.
[13] Ks. tarkemmin komission delegoitu asetus (EU) 2019/945 40(5) art. ja EASA Easy Access Rules for Unmanned Aircraft Systems, syyskuu 2022, k. 12 (b) (https://www.easa.europa.eu/en/downloads/110913/en#page=419).
[14] Komission delegoitu asetus (EU) 2019/945 40(5)(b) artikla.
[15] HE 197/2021 vp, s. 12.
[16] Miehittämättömän aluksen kauko-ohjaukseen liittyvän radioviestinnän tilastollisesta käsittelystä säädetään väliaikaisesti voimassa olevassa SVPL 136.5 §:ssä.
[17] Ilmailulain ohella tällaisia säännöksiä sisältyy esimerkiksi ydinenergialain 7 v §:ään ja vankeuslakin 16 luvun 2 a §:ään.

kään laissa erikseen yleisesti vastaanottavaksi määritettyyn radioviestinnän tyyppiin. Lähetteiden on arvioitu olevan tarkoitettu pikemminkin ilmatilan valvojien ja muiden ilmatilan käyttäjien käyttöön kuin kenen tahansa vapaasti hyödynnettäväksi.

Merenkulun AIS-yleislähetysten käyttötarkoitusta on pidetty siinä määrin samankaltaisena kuin ilmailun ADS-B-lähetettä, että myös niitä on pidetty luottamuksellisena radioviestintänä. Kyseisen radioviestinnän ensisijaisena tarkoituksena on katsottu olevan varmistaa lento- ja meriliikenteen turvallisuus ja mahdollistaa sen valvonta. Lähetteiden tietojen välittäminen kaupallisiin palveluihin ei ole katsottu olevan järjestelmien alkuperäisen, meri- ja ilma-alusten navigointia ja turvallisuutta tukevan tarkoituksen mukaista toimintaa.

Se, joka on saanut tiedon luottamuksellisesta radioviestinnästä, jota ei ole hänelle tarkoitettu, ei lähtökohtaisesti saa ilman viestinnän osapuolen suostumusta ilmaista tai käyttää hyväksi viestin sisältöä, välitystietoa tai tietoa viestin olemassaolosta (SVPL 136.4 §). Tästä seuraa, että AIS- ja ADS-B-lähetysten tietojen välittäminen kaupallisiin palveluihin sivullisten, eli käytännössä muiden kuin toisten ilma- tai merialueen käyttäjien sekä liikennettä valvovien tahojen toimesta on Traficomin neuvontakäytännössä katsottu voimassa olevan lainsäädännön vastaiseksi, kun tällainen käyttö ei ole ollut lähetteiden alkuperäisen käyttötarkoituksen mukaista.

Merkittävää osaa ilma- ja meriliikenteestä koskee edellä todetusti alun perin kansainvälisistä sopimuksista tai EU-sääntelystä peräisin oleva velvollisuus AIS- ja ADS-B-tietoja välittävien radiolaitteiden käyttämiseen. Näiden laitteiden käytön tarkoituksena on parantaa merenkulun ja ilmailun turvallisuutta mm. ehkäisemällä yhteentörmäyksiä, kun muiden alusten ja ilma-alusten reaaliaikainen sijainti on AIS- ja ADS-B-lähetteiden perusteella käytettävissä.

Traficomin näkemyksen mukaan AIS- ja ADS-B-lähetteiden asemaa luottamuksellisena radioviestintänä on syytä arvioida uudelleen näiden tietojen käsittelyyn liittyvän toimintaympäristön nykytilaa vasten. AIS- ja ADS-B-tietoja käsitellään tosiasiassa hyvin laajasti. Tiedot ovat saatavilla myös kaupallisista palveluista. Näitä ovat esimerkiksi AIS-tietojen osalta MarineTraffic sekä ADS-B-tietojen osalta FlightRadar24. Nämä palvelut saavat tietoja esimerkiksi yksityishenkilöiltä, jotka vapaaehtoisesti välittävät vastaanottimillaan keräämänsä tiedot kyseisille palveluille ilmailun ja merenkulun turvallisuuden edistämiseksi. AIS- ja ADS-B-radiolähetteiden vastaanotto ja käsittely on teknisesti yksinkertaista, kun taas vastaanoton ja välittämisen valvominen on erittäin vaikeaa. Tämä johtuu siitä, että kuka tahansa pystyy radiolaitteella kuuntelemaan salaamatonta radioviestintää, eikä tätä voi radioteknisistä johtuvista syistä estää. AIS- ja ADS-B-lähetteiden vastaanottaminen on mahdollista myös satelliitilla, johon on asennettu sopiva vastaanotin.

Aiemman tulkintalinjauksen kriittinen tarkastelu on tarpeen myös sen johdosta, että droneissa ollaan ottamassa käyttöön RID-lähetteitä. Traficomilla ei ole ollut aiemmin tulkintaa siitä, miten RID-lähetteitä on arvioitava suhteessa viestinnän luottamuksellisuuteen. Koska RID-lähete on jossain määrin piirteiltään samankaltainen suhteessa AIS- ja ADS-B-lähetteisiin, on viimeksi mainittuja koskevalla tulkinnalla merkitystä myös RID-lähetteiden osalta. Toisaalta RID-lähetteistä on edellä todetusti lain esitöissä omaksuttu käsitys, että ne olisivat yleisesti vastaanotettavaksi tarkoitettua radioviestintää, mikä alustavasti puoltaisi vastaavaa tulkintaa myös AIS- ja ADS-B-lähetteiden osalta.

Viestinnän luottamuksellisuutta koskeva tiukka tulkinta Suomessa voi muodostua perusteettomaksi esteeksi liiketoiminnalle, tutkimustoiminnalle tai sellaisille keskeistä infrastruktuuria suojaavien valvontajärjestelmien käytölle, joissa yllä mainittuja lähetteitä voitaisiin käyttää toiminnan turvallisuudesta huolehtimiseen.

Selvyyden vuoksi on syytä todeta, että tämä arviomuistio ei koske miehittämättömien ilma-alusten *kauko-ohjausliikenteen* luottamuksellisuutta. Kauko-ohjaukseen liittyvä radioviestintä on luottamuksellista, ja sen käsittely on mahdollista vain laissa säädetyin perustein. Lisäksi on huomattava, että AIS-lähetteiden osalta tässä muistiossa tarkastellaan ainoastaan yleislähetteitä (broadcast) erotuksena kohdennetuista lähetteistä (addressed), joille on määritelty viestin vastaanottaja.

Tämän arviomuistion luonnos oli lausuntopalvelussa lausuttavana maaliskuussa 2023.[18] Lausunnon antoivat Rajavartiolaitos, Suojelupoliisi ja Väylävirasto sekä Liikenteenohjausyhtiö Fintraffic Oy, ICEYE Oy ja Sensofusion Oy. Lausunnon antaneet tahot pitivät arviomuistiossa esitettyä kantaa joko kannatettavana tai eivät lausuneet muistion johtopäätöksistä.

2 Keskeinen viestinnän luottamuksellisuutta koskeva lainsäädäntö

2.1 Euroopan unionin oikeus ja Euroopan ihmisoikeussopimus

Euroopan unionin perusoikeuskirja

Euroopan unionin perusoikeuskirjan (jäljempänä myös perusoikeuskirja) 7 artiklassa säädetään yksityis- ja perhe-elämän kunnioittamisesta. Sen mukaan jokaisella on oikeus siihen, että hänen yksityis- ja perhe-elämäänsä, kotiaan sekä viestejään kunnioitetaan.

Perusoikeuskirjan 8 artiklassa säädetään puolestaan henkilötietojen suojasta. Sen 1 kohdan mukaan jokaisella on oikeus henkilötietojensa suojaan ja 2 kohdan mukaan tietojen käsittelyn on oltava asianmukaista ja sen on tapahduttava tiettyä tarkoitusta varten ja asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla. Jokaisella on oikeus tutustua niihin tietoihin, joita hänestä on kerätty, ja saada ne oikaistuksi. Lisäksi 8 artiklan 3 kohdan mukaan riippumaton viranomainen valvoo näiden sääntöjen noudattamista.

Lisäksi perusoikeuskirjan 52(3) artiklan mukaan siltä osin kuin perusoikeuskirjan oikeudet vastaavat ihmisoikeuksien ja perusvapauksien suojaamiseksi tehdyssä yleissopimuksessa taattuja oikeuksia, niiden merkitys ja ulottuvuus ovat samat kuin mainitussa yleissopimuksessa. Tämä määräys ei estä unionia myöntämästä tätä laajempaa suojaa.

Sopimus Euroopan unionin toiminnasta

Euroopan unionin toiminnasta annetun sopimuksen 16 artiklassa säädetään henkilötietojen suojasta ja sen 1 kohdan mukaan jokaisella on oikeus henkilötietojensa suojaan.

Sähköisen viestinnän tietosuojadirektiivi

Sähköisen viestinnän tietosuojadirektiivin[19] 3 artiklan mukaan kyseistä direktiiviä sovelletaan henkilötietojen käsittelyyn, joka liittyy yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoamiseen yleisissä viestintäverkoissa yhteisössä, mukaan luettuina tiedonkeruu- ja tunnistuslaitteita tukevat yleiset viestintäverkot.

[18] https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=a7833512-8509-4d9a-bd2b-4845b011c37a.
[19] Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla.

Direktiivin 5 artiklassa säädetään viestinnän luottamuksellisuudesta. Sen 1 kohdan mukaan jäsenvaltioiden on kansallisella lainsäädännöllä varmistettava yleisen viestintäverkon ja yleisesti saatavilla olevien sähköisten viestintäpalvelujen välityksellä tapahtuvan viestinnän ja siihen liittyvien liikennetietojen luottamuksellisuus. Niiden on erityisesti kiellettävä se, että muut henkilöt kuin käyttäjät ilman kyseisten käyttäjien nimenomaista suostumusta kuuntelevat, salakuuntelevat, tallentavat tai muulla tavalla sieppaavat tai valvovat viestintää ja siihen liittyviä liikennetietoja, jollei se ole laillisesti sallittua 15 artiklan 1 kohdan mukaisesti. Mitä tässä kohdassa säädetään, ei estä teknistä tallentamista, joka on tarpeen viestinnän välittämiselle, tämän rajoittamatta luottamuksellisuuden periaatteen soveltamista.

Yleinen tietosuoja-asetus

EU:n yleinen tietosuoja-asetus[20] (TSA) sääntelee yleisesti henkilötietojen käsittelyä EU:n alueella. TSA 2 artiklan 1 kohdan mukaan tietosuoja-asetusta sovelletaan henkilötietojen käsittelyyn, joka on osittain tai kokonaan automaattista, sekä sellaisten henkilötietojen käsittelyyn muussa kuin automaattisessa muodossa, jotka muodostavat rekisterin osan tai joiden on tarkoitus muodostaa rekisterin osa. Saman 2 artiklan 2 kohdan c alakohdan mukaan tietosuoja-asetusta ei sovelleta henkilötietojen käsittelyyn, jonka luonnollinen henkilö suorittaa yksinomaan henkilökohtaisessa tai kotitalouttaan koskevassa toiminnassa.

TSA 4(1) artiklan mukaan henkilötiedoilla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja.

TSA 5 artiklassa säädetään henkilötietojen käsittelyä koskevista periaatteista. Kyseisen artiklan 1 kohdassa säädetään muun muassa vaatimuksesta käsitellä henkilötietoja lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi.

Henkilötietojen käsittely edellyttää TSA 6 artiklan mukaista henkilötietojen käsittelyn oikeusperustetta.

Euroopan ihmisoikeussopimus

Euroopan ihmisoikeussopimuksen 8 artiklassa säädetään oikeudesta nauttia yksityis- ja perhe-elämän kunnioitusta. Sen 1 kohdan mukaan jokaisella on oikeus nauttia yksityis- ja perhe-elämäänsä, kotiinsa ja kirjeenvaihtonsa kohdistuvaa kunnioitusta. Lisäksi 2 kohdan mukaan viranomaiset eivät saa puuttua tämän oikeuden käyttämiseen, paitsi silloin kun laki sen sallii ja se on demokraattisessa yhteiskunnassa välttämätöntä kansallisen ja yleisen turvallisuuden tai maan taloudellisen hyvinvoinnin vuoksi, tai epäjärjestyksen ja rikollisuuden estämiseksi, terveyden tai moraalin suojaamiseksi, tai muiden henkilöiden oikeuksien ja vapauksien turvaamiseksi.

2.2 Suomen kansallinen lainsäädäntö

Perustuslaki

Perustuslain 10 §:ssä säädetään yksityiselämän suojasta ja sen 1 momentin mukaan jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla.

Perustuslain 10 §:n 2 momentin mukaan kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton.

[20] Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta.

Pykälän 4 momentin nojalla lailla voidaan säätää välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä, turvallisuustarkastuksessa ja vapaudenmenetyksen aikana sekä tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta.

Laki sähköisen viestinnän palveluista

Sähköisen viestinnän palveluista annetun lain (917/2014, SVPL) 3 §:n 17 kohdan mukaan radioviestinnällä tarkoitetaan viestintää radioaaltojen avulla ja radiomäärityksellä esineen sijainnin, nopeuden tai muun luonteenomaisen piirteen määrittämistä radiomäärityksellä taikka näihin parametreihin liittyvien tietojen hankkimista radioaaltojen etenemisominaisuuksien avulla.

SVPL:n esitöiden mukaan radioviestinnällä tarkoitetaan tiedon siirtoa, lähettämistä ja vastaanottoa käyttäen hyväksi radiotaajuuksia. Radioviestintää ovat muun muassa televisio- ja radiolähetykset, matkaviestintä, meriradioviestintä, turvallisuusradioviestintä, radioamatööriviestintä ja lyhytaaltoradioviestintä.[21] Lisäksi SVPL:n radioviestinnän määritelmän säädöskohtaisissa perusteluissa todetaan, että määritelmä vastaa radiolain 4 §:n 2 kohdan määritelmää (HE 80/2001 vp, HE 119/1987 vp). Kyseisessä jo kumotussa radiolaissa (1015/2001) radioviestinnällä tarkoitettiin tiedon siirtoa, lähettämistä tai vastaanottamista käyttäen hyväksi radiotaajuuksia.[22]

SVPL 3 §:n 40 kohdassa säädetään välitystietojen määritelmästä, jonka mukaan välitystiedoilla tarkoitetaan oikeus- tai luonnolliseen henkilöön yhdistettävissä olevaa tietoa, jota käsitellään viestinnän välittämiseksi sekä tietoa radioaseman tunnisteesta ja radiolähettimen käyttäjästä sekä tietoa radiolähetyksen alkamisajankohdasta, kestosta tai lähetyspaikasta.

SVPL 17 luvussa säädetään sähköisen viestin, välitystietojen ja rikoksia koskevien tietojen käsittelystä. Radioviestinnän luottamuksellisuutta koskeva sääntely on sisällytetty SVPL 136 §:ään, jossa säädetään viestin ja välitystietojen luottamuksellisuudesta. Sen 1 momentin mukaan viestinnän osapuoli voi käsitellä omia sähköisiä viestejään ja niihin liittyviä välitystietoja, jollei laissa toisin säädetä. Viestinnän luottamuksellisuus kohdistuu sähköisen viestinnän ohella myös radioviestintään ja sen välitystietoihin, jotka kuuluvat perusoikeutena turvatun luottamuksellisen viestin salaisuuden piiriin.

SVPL 136 §:n 2 momentin mukaan yleisesti vastaanotettavaksi tarkoitettua radioviestintää ja sen välitystietoja saa käsitellä, jollei laissa toisin säädetä. Tällaisena radioviestintänä pidetään:

1) televisio- ja radio-ohjelmistojen lähetyksiä;

2) hätäkutsuja;

3) yleisellä kutsukanavalla harjoitettavaa radioviestintää;

4) radioamatööriviestintää;

[21] HE 221/2013 vp, s. 87.
[22] Vastaavasti radiolain esitöissä HE 80/2001 vp, s. 19-20, jossa todetaan, että pykälän 2 ja 4 kohtien mukaiset radioviestinnän ja turvallisuusradioviestinnän määritelmät vastaisivat sisällöltään voimassa olevan radiolain määritelmiä. Tuolloin oli vielä voimassa vuoden 1987 radiolaki, jonka 3 §:n 1 momentin mukaan radioviestinnällä tarkoitettiin kaikkea merkin, merkinannon, kirjoituksen, kuvan, äänen tai muussa muodossa olevan tiedon siirtoa, lähettämistä tai vastaanottamista käyttäen hyväksi radioaaltoja.

5) lyhytaaltoradioviestintää 27 megahertsin taajuusalueella;

6) muuta kuin 1–5 kohdassa tarkoitettua radioviestintää, joka on tarkoitettu yleisesti vastaanotettavaksi.

SVPL 136 §:n 3 momentin mukaan muita sähköisiä viestejä ja välitystietoja saa käsitellä viestinnän osapuolen suostumuksella tai jos laissa niin säädetään.

SVPL 136 §:n 4 momentin mukaan se, joka on ottanut vastaan tai muutoin saanut tiedon sähköisestä viestistä, radioviestinnästä tai välitystiedosta, jota ei ole hänelle tarkoitettu, ei saa ilman viestinnän osapuolen suostumusta ilmaista tai käyttää hyväksi viestin sisältöä, välitystietoa tai tietoa viestin olemassaolosta, ellei laissa toisin säädetä. Näin ollen viestinnän luottamuksellisuutta koskevassa säännöksessä otetaan huomioon myös vahingossa vastaanotettua radioviestintää koskeva hyväksikäyttökielto ja vaitiolovelvollisuus.

SVPL 349 §:ssä säädetään sähköisen viestinnän tietosuojarikkomuksesta. Sen 1 momentin 4 kohdan mukaan, joka tahallaan käsittelee välitystietoja 136–144 §:ssä säädetyn vastaisesti tai laiminlyö käsittelyyn liittyvän tiedonantovelvollisuuden tai viranomaisen antamat määräykset, on tuomittava sähköisen viestinnän tietosuojarikkomuksesta sakkoon, jollei teosta muualla laissa säädetä ankarampaa rangaistusta.

SVPL 350 §:n 2 momentissa on informatiivinen säännös vaitiolovelvollisuuden ja hyväksikäyttökiellon rikkomisen rangaistavuudesta. Sen mukaan rangaistus lain 136 §:n 4 momentissa ja 160 §:n 5 momentissa säädetyn salassapitovelvollisuuden rikkomisesta tuomitaan rikoslain 38 luvun 1 tai 2 §:n mukaan, jollei teko ole rangaistava rikoslain 40 luvun 5 §:n mukaan tai siitä muualla laissa säädetä ankarampaa rangaistusta.

3 Arviointi ja ratkaisuvaihtoehdot

3.1 Tulkintavaihtoehdot

AIS-, ADS-B- ja RID-lähetteiden suhde radioviestinnän luottamuksellisuutta koskevaan sääntelyyn on periaatteessa ratkaistavissa kahdella tavalla:

1. Ensimmäinen ratkaisuvaihto: Ei muuteta Traficomin aiempaa tulkintaa, jonka mukaan AIS- ja ADS-B-lähetteet ovat luottamuksellista radioviestintää ja niitä saa käsitellä vain SVPL:n tai jonkin erityislain mukaisella perusteella. Tulkintalinjausta sovellettaisiin jatkossa myös RID-lähetteisiin.

2. Toinen ratkaisuvaihtoehto: AIS-, ADS-B- ja RID-lähetteet eivät ole luottamuksellista radioviestintää, vaan kyse on yleisesti vastaanotettavaksi tarkoitetusta radioviestinnästä (SVPL 136 §:n 2 momentin 6 kohta), jolloin niiden käsittely olisi mahdollista muun lainsäädännön asettamissa rajoissa.

Ensimmäisestä vaihtoehdosta seuraisi, että lähetteitä vastaanottavat ja palveluntarjoajille välittävät vapaaehtoiset sekä kyseiset palveluntarjoajat käsittelisivät lähetteiden tietoja viestintätapahtumaan nähden sivullisina. Tällainen käsittely olisi SVPL 136.4 §:n vastaista. Toisessa vaihtoehtoehdossa edellä mainitut tahot voisivat käsitellä lähetteiden tietoja SVPL:n sääntelyn estämättä. Käsittelyn tulisi kuitenkin tapahtua muun soveltuvan lainsäädännön, kuten EU:n yleisen tietosuoja-asetuksen puitteissa.

3.2 Lähetteet SVPL:n systematiikassa ja suhteessa ePrivacy-direktiiviin

AIS-, ADS-B- ja RID-tunnistusjärjestelmien lähetteet tietoineen ovat alusten ja ilmaalusten radiolaitteiden lähettämää automaattista radioviestintää. Näin ollen kyseiset tiedot ovat SVPL:n mukaista radioviestintää ja lähetteiden tiedot viestinnän sisältöä. Kyseiset lähetteet sisältävät edellä todetusti mm. aluksen yksilöivät tiedot ja sen reaaliaikaisen sijainnin, ja nimenomaan kyseisten lähetteiden tietoja käytetään erilaisissa palveluissa.[23]

Lähetteiden välittämiseen ei käytetä yleisiä viestintäverkkoja. Tästä syystä tässä muistiossa tarkastellussa radioviestinnässä ei ole kyse sähköisen viestinnän tietosuojadirektiivin 3 artiklassa tarkoitetusta sellaisesta henkilötietojen käsittelystä, joka liittyy *yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoamiseen yleisissä viestintäverkoissa*. Näin ollen direktiiviä ei sovelleta kyseisten järjestelmien radioviestintään ja sen luottamuksellisuuteen, eikä sen tulkintavaikutus edellytä lähetteiden käsittelyn lukemista luottamuksellisen radioviestinnän piiriin.

3.3 Yleisesti vastaanotettavaksi tarkoitettu radioviestintä

SVPL 136 §:stä ilmenevä sääntelyn lähtökohta on, että radioviestintä on luottamuksellista, jollei sitä ole tarkoitettu yleisesti vastaanotettavaksi. Muuta kuin yleisesti vastaanotettavaksi tarkoitettua radioviestintää käsiteltäessä tulee ottaa huomioon pääsääntö, jonka mukaan sivullinen saa käsitellä luottamuksellista viestintää tai sen välitystietoja ainoastaan laissa säädetyllä perusteella.

SVPL 136 §:n 2 momentissa määritellään yleisesti vastaanotettavaksi tarkoitettu radioviestintä. AIS-, ADS-B- tai RID-lähetteitä ei voida pitää minään momentin 1–5 kohdissa lueteltuna radioviestinnän lajina. Momentin 6 kohdan mukaan yleisesti vastaanotettavaa radioviestintää on kuitenkin myös muu kuin 1–5 kohdassa tarkoitettu radioviestintä, joka on *tarkoitettu* yleisesti vastaanotettavaksi. Näin ollen arvioinnin tulkintakysymys tiivistyy siihen, ovatko lähetteet katsottavissa SVPL 136 §:n 2 momentin 6 kohdan mukaiseksi muuksi radioviestinnäksi, joka on tarkoitettu yleisesti vastaanotettavaksi. Jos kyse on yleisesti vastaanotettavaksi tarkoitetusta radioviestinnästä, sitä ei pidetä luottamuksellisena, vaan sitä saa käsitellä SVPL:n viestinnän luottamuksellisuutta koskevan sääntelyn estämättä.

Yleisesti vastaanotettavaksi tarkoitettua radioviestintää ei ole tyhjentävästi määritelty, joten arvioinnissa korostuu tapauskohtaisuus. Tästä johtuen on tulkinnanvaraista, mitä yleisesti vastaanotettavaksi tarkoitetulla radioviestinnällä tarkoitetaan. Asiaa ei ole tarkennettu aihetta koskevissa hallituksen esityksissä.[24] Tämän arvioinnin tekeminen voi edellyttää teknistä asiantuntemusta radiotekniikasta ja kyseiseen viestintätilanteeseen liittyvistä käytännöistä.

Tulkinnan kohteena voi olla lähinnä sen arviointi, onko käyttäjä (radioviestinnän lähettäjä) tarkoittanut radioviestin yleisesti vastaanotettavaksi tai onko radioviesti

[23] Tällaista lähetystä kuvaavat tiedot voivat lisäksi olla SVPL 3 §:n 40 kohdan mukaisia radioviestinnän välitystietoja. Tässä muistiossa ei ole kuitenkaan tarpeen tarkastella erikseen radioviestinnän välitystietojen käsittelyä, sillä ne ovat samoin perustein luottamuksellisia kuin varsinainen radiolähetyksen sisältökin.
[24] Ks. HE 221/2013 vp, s. 153 ja HE 75/2004 vp, s. 6 ja 15. Nykyinen SVPL 136 §:n 2 momentin esimerkinomainen luettelo lisättiin alun perin radiolakiin ja se on laadittu erityisesti radiolaitteiden käyttäjien näkökulmasta. Esimerkkiluettelo lisättiin lakiin, koska sillä haluttiin selventää radioviestinnän luottamuksellisuutta koskevaa sääntelyä.

käyttötarkoitukseltaan sellainen, että se on yleisesti vastaanotettavaksi tarkoitettua.[25] Tyypillisesti arvioinnissa korostuu (olosuhteista pääteltävä) lähettäjän tarkoitus. Aina ei ole mahdollista etukäteen tietää, onko radiolähetys luottamuksellinen vai tarkoitettu yleisesti vastaanotettavaksi SVPL 136 §:n 2 momentin mukaisessa merkityksessä. SVPL 136 §:n 2 momentin 6 kohtaa sovellettaessa keskeistä on, onko viestin lähettäjä (oletettavasti) tarkoittanut viestin yleisesti vastaanotettavaksi. Jos viestin lähettäjä ei ole tarkoittanut sitä yleisesti vastaanotettavaksi radioviestinnäksi, sen käsittelyyn soveltuu SVPL 136 §:n 4 momentin mukainen sivullisen vastaanottamaan viestiin liittyvä vaitiolovelvollisuus ja hyväksikäyttökielto, jonka mukaan se, joka on ottanut vastaan tai muutoin saanut tiedon sähköisestä viestistä, radioviestinnästä tai välitystiedosta, jota ei ole hänelle tarkoitettu, ei saa ilman viestinnän osapuolen suostumusta ilmaista tai käyttää hyväksi viestin sisältöä, välitystietoa tai tietoa viestin olemassaolosta, ellei laissa toisin säädetä.

3.4 Lähetteiden käyttötarkoitus ja toimialalla noudatettavat käytännöt

Asian arvioinnin kannalta ongelmallista on, että useille toimijoille AIS- ja ADS-B-järjestelmien käyttö ei ole harkinnanvaraista, vaan niiden käyttö on kansainvälisissä merenkulun ja ilmailun sopimuksissa sekä EU-oikeudessa säädetty pakolliseksi. Tämä pakollisuus johtuu nimenomaisesti kyseisten reaaliaikaisten sijaintitietojen turvallisuutta parantavasta vaikutuksesta, joka perustelee sitä, että kyseisten tietojen on tarkoitettu tulevan mahdollisimman laajan joukon tietoon alusten ja ilmaalusten yhteentörmäysten välttämiseksi sekä hädässä olevan aluksen löytämiseksi. Tämän johdosta lähettäjän henkilökohtainen tarkoitus soveltuu käsitteenä huonosti sen arvioimiseen, onko kyseessä yleisesti vastaanotettavaksi tarkoitettu radioviestintä.[26] SVPL 136 §:n 2 momentin 6 kohta on kuitenkin kirjoitettu passiivimuotoon: yleisesti vastaanotettavaa on radioviestintä, joka *on tarkoitettu* yleisesti vastaanotettavaksi. Tämä mahdollistaa yleisemmin järjestelmien käyttötarkoituksen ottamisen huomioon sen sijasta, että tarkasteltaisiin yksittäisen lähettimen haltijan oletettua käsitystä radioviestinnän luottamuksellisuudesta.

Vaikuttaa mahdolliselta katsoa AIS- ja ADS-B-tiedot käyttötarkoituksensa puolesta sellaiseksi radioviestinnäksi, joka on tarkoitettu yleisesti vastaanotettavaksi. Tämä johtuu kyseisten tietojen viestimisen pääasiallisesta tarkoituksesta, joka on aluksen sijaintitiedon välittäminen toisille merenkulkijoille tai ilmailijoille alusten yhteentörmäysten estämiseksi. Liikenteen turvallisuuden näkökulmasta kyseisten tietojen mahdollisimman laaja käytettävyys ja avoimuus olisi perusteltua. Lähetys palvelee ennen kaikkea niitä vastaanottajia, jotka tarvitsevat tietoa meri- ja ilmaliikenteen turvallisuuden varmistamiseksi, kuten toisia meri- tai ilma-alueen käyttäjiä ja niiden turvallisuudesta vastaavia tahoja. *Olennaista on, että lähetyksiä ei ole osoitettu millekään tietylle vastaanottajalle*, vaan lähetteiden tarkoituksena on yleisesti turvallisuuden ja tilannetietoisuuden parantaminen. Vaikka lähetysten katsottaisiin olevan tarkoitettu ensisijaisesti ilmatilan tai merialueen valvojien ja muiden ilmatilan tai merialueen käyttäjien käyttöön, ei näitäkään tahoja ole ennalta määrätty siten, kuin luottamuksellisessa radioviestinnässä normaalisti edellytetään olevan.

EU-lainsäädäntö vaikuttaisi suhtautuvan ADS-B-tietoihin vapaasti hyödynnettävinä tietoina. Ns. droneasetuksen ohjemateriaalissa on yhtenä DAA (Detect and Avoid) -keinoista mainittu "Use of (web-based) real-time aircraft tracking services, jollainen muun muassa ADS-B-tietoja laajasti hyödyntävä Flightradar24 on.[27]

[25] Eija Alavesa – Erika Leinonen: Yksityisyyden suoja, radioviestinnän luottamuksellisuus ja lennokkeja hyödyntävät uudet palvelut. Viestinnän muuttuva sääntely – Viestintäoikeuden vuosikirja 2016, s. 154.
[26] Säännökset toisaalta mahdollistavat sen, että poikkeuksellisissa olosuhteissa AIS voidaan kytkeä pois päältä, ks. esim. seurantadirektiivin 6a(2) artikla.
[27] EASA Easy Access Rules for Unmanned Aircraft Systems, s. 100.

AIS-lähetteiden tietoihin näyttäisi EU-oikeudessakin suhtaudutun sellaisina julkisina tietoina,[28] joita voi käsitellä henkilötietojen käsittelyä koskevien säännösten puitteissa.[29] Lisäksi myös suomalaiset viranomaiset keräävät ja jakavat ainakin AIS-tietoja.[30] Kyseisten radiolähetysten luottamuksellisuutta suhteessa sivullisiin koskevia erityisiä säännöksiä ei ole.

Ruotsissa tämänkaltaisten radiolähetysten mahdollinen luottamuksellisuus tulisi todennäköisesti arvioitavaksi Ruotsin sähköisestä viestinnästä annetun lain (2022:482) 9 luvun 34 §:n perusteella, mutta Ruotsin PTS:ltä[31] saatujen tietojen mukaan tällaista arviointia ei ole toistaiseksi tehty. Pykälässä säädetään kiellosta välittää oikeudettomasti edelleen radiovastaanottimella vastaanotettua, radioteitse viestintäverkossa siirrettyä viestiä, jota ei ole tarkoitettu tälle viestin vastaanottaneelle tai yleisesti vastaanotettavaksi.

Ei ole kuitenkaan itsestään selvää, että AIS- ja ADS-B-laitteita ja jatkossa RID-toiminnon sisältäviä droneja käyttävien tahojen perusteltuja odotuksia yksityisyydestään vastaa se, että näiden radiolähetyksien tietoja julkaistaan myös kaupallisissa palveluissa tai että niitä saatetaan muutoin vapaasti saataville. Tällainen käsittely voisi periaatteessa olla kyseisille henkilöille yllättävää, mikä voisi viitata kyseisten tietojen olevan muuta kuin yleisesti vastaanotettavaksi tarkoitettua radioviestintää. Kyseisen viestinnän luottamuksellisuuden puolesta puhuisi sinänsä se, että muu ilmailu- ja meriradioviestintä katsotaan luottamukselliseksi viestinnäksi samoin kuin dronen kauko-ohjaukseen liittyvä radioviestintä.[32] Jos lähetteet katsottaisiin luottamukselliseksi radioviestinnäksi, tarkoittaisi tämä sitä, että niitä vastaanottaneeseen sivulliseen, jolle lähetystä ei ole tarkoitettu, sovellettaisiin SVPL 136 §:n 4 momentin mukaista vaitiolovelvollisuutta ja hyväksikäyttökieltoa. Tällöin lähetteiden käsittely ja välittäminen tietoja hyödyntäville palveluntarjoajille, kuten MarineTraffic ja Flightradar24, olisi Suomessa tuon vaitiolovelvollisuuden vastaista. Tällöin vapaaehtoisten tietojen välittäjien toimintaa voisi olla mahdollista tarkastella myös rikosoikeudelliselta kannalta.[33]

AIS- ja ADS-B-tietojen käsittelyn nykytilanne on kuitenkin se, että näitä tietoja käsitellään sekä maailmanlaajuisesti että Suomessa laajasti tunnistamatta, että kyseiset tiedot katsottaisiin Traficomin aiemman tulkinnan mukaan Suomessa luottamukselliseksi radioviestinnäksi. Tietojen saatavuus kaupallisista palveluista arvioidaan myös olevan tosiasiallisesti hyvin laitteiden käyttäjien tiedossa. Tietoja hyödyntävät niin viranomaiset kuin yksityiset toimijat, ja ne koetaan hyödyllisiksi ja tarpeellisiksi etenkin merenkulun ja ilmailun turvallisuuden näkökulmasta. Kun tietoja joka tapauksessa käsitellään laajasti, ko. radioviestinnän katsominen luottamukselliseksi ei näyttäisi vastaavan lähettimien ja tietojen käyttäjien käsitystä tietojen luonteesta.

Tällaisten, kaupallisista palveluista tosiasiallisesti maailmanlaajuisesti saatavilla olevien tietojen luottamuksellisuuden arvioinnissa on lisäksi perusteltua ottaa huomi-

[28] Euroopan parlamentin ja neuvoston direktiivi 2002/59/EY, annettu 27 päivänä kesäkuuta 2002, alusliikennettä koskevan yhteisön seuranta- ja tietojärjestelmän perustamisesta sekä neuvoston asetuksen 93/75/ETY kumoamisesta luettuna yhdessä IFCD:n kanssa.
[29] AIS-lähetteiden käsittelyn osalta Euroopan tietosuojavaltuutetun lausunto komission täytäntöönpanoasetuksesta (EU) N:o 404/2011 (2012/C 37/01), k. 10.
[30] https://www.digitraffic.fi/meriliikenne/ais/.
[31] Post- och telestyrelsen (https://www.pts.se/).
[32] Viimeksi mainittu ilmenee SVPL 136.5 §:stä, jossa poikkeuksellisesti sallitaan tämän radioviestinnän käsittely eräin edellytyksin.
[33] SVPL 350.2 §:n mukaan rangaistus lain 136 §:n 4 momentissa säädetyn salassapitovelvollisuuden rikkomisesta tuomitaan rikoslain 38 luvun 1 tai 2 §:n mukaan, jollei teko ole rangaistava rikoslain 40 luvun 5 §:n mukaan tai siitä muualla laissa säädetä ankarampaa rangaistusta.

oon se, ettei kyseisten tietojen tulkitseminen Suomessa kansallisesti luottamuksellisiksi estä ulkomaisen lainsäädännön perusteella tapahtuvaa, Suomen lainkäyttövaltaan kuulumatonta käsittelyä. Arvioinnissa on perusteltua myös ottaa huomioon se, että valvontaviranomaisella ei ole tehokkaita keinoja puuttua AIS- ja ADS-B-tietojen välittämiseen palveluntarjoajille. Näin ollen kyseisten tietojen tulkitseminen myös Suomessa yleisesti vastaanotettavaksi tarkoitetuksi radioviestinnäksi ei käytännössä muuttaisi nykytilannetta. Kyseisiä tietoja hyödynnetään nykyisin hyvin laajasti, ja MarineTrafficin ja FlightRadar24:n kaltaisia palveluja pidetään yleisesti hyödyllisinä merenkulun ja ilmailun toimijoiden piirissä. Näiden tietojen käsittelyn perusteena nähdään merenkulun ja ilmailun turvallisuuden parantaminen, eikä niiden saatavuutta julkisista palveluista ole yleisesti koettu ongelmana, joskin kriittisempiäkin näkemyksiä on esitetty.

3.5 AIS- ja ADS-B-radiolähetteiden käsittelyn turvallisuusvaikutukset

Tietojen asemaa arvioitaessa on merkityksellistä arvioida myös niiden väärinkäytösmahdollisuuksia, sillä AIS- ja ADS-B-tiedot mahdollistavat lähes reaaliaikaisen alusten seuraamisen julkisesti saatavilla olevista palveluista. Sivullisten mahdollisuus käyttää ja jakaa tietoja onkin aiheuttanut keskustelua siitä, miten ADS-B-järjestelmä sovitetaan yhteen yksityisyydensuojan ja turvallisuuden kannalta.[34] Ehdotuksia on myös tehty siitä, miten tietoturva ja yksityisyyden suoja voitaisiin varmistaa salausta käyttämällä.[35] Toisaalta B-luokan laitteita käyttävät henkilöt ovat tavanomaisesti hyvin tietoisia MarineTrafficin kaltaisista palveluista ja mahdollisesti itsekin hyödyntävät kyseisiä palveluja. Lisäksi B-luokan laitteiden käyttö on edellä todetusti vapaaehtoista, joten huviveneilijät voivat halutessaan myös kytkeä radiolaitteensa väliaikaisesti pois päältä. Eräissä muissakin poikkeuksellisissa olosuhteissa AIS voidaan kytkeä pois päältä, jos se on tarpeen aluksen turvallisuuden kannalta.[36] Vaikka AIS- ja ADS-B-tietojen katsottaisiin olevan yleisesti vastaanotettavaksi tarkoitettua radioviestintää, jolloin viestinnän luottamuksellisuutta koskevat säännökset eivät soveltuisi kyseisiin tietoihin, kyseisten tietojen käyttöä sääntelisi kuitenkin mahdollisten henkilötietojen käsittelyn osalta yleinen tietosuoja-asetus, mitä käsitellään jäljempänä.

Aiemmin on selvitetty eri yhteyksissä viranomaisten AIS-tietojen julkaisemista, jolloin AIS- ja ADS-B-radiolähetteiden tietojen saatavuuden itsessään ei yleisellä tasolla ole katsottu aiheuttavan erityisiä turvallisuusriskejä etenkään, kun tietoja tosiasiassa on ollut jo pitkään vapaasti saatavilla. Tietoja voidaan pitää julkiseksi suunniteltuina ja ne ovat ulkopuolisten vastaanotettavissa, joten kyseisten tietojen käytön kaupallisiin tarkoituksiin ei ole sellaisenaan katsottu aiheuttavan erityisiä turvallisuusriskejä, vaikka tietoja voitaisiin periaatteessa käyttää myös turvallisuutta vaarantaviin laittomiin tarkoituksiin.[37] Näiden radiolähetteiden käsittelyyn kaupallisissa tarkoituksissa ei siten liity sellaisia erityisiä turvallisuusriskejä, jotka perustelisivat kyseisten lähetteiden tulkitsemista luottamukselliseksi radioviestinnäksi.

[34] Ks. esim. https://www.flightglobal.com/safety/use-of-ads-b-by-flight-tracking-websites-spurs-proposition-to-protect-privacy/150391.article ja https://www.planeandpilotmag.com/article/privacy-lost-in-the-age-of-ads-b/.
[35] Ks. esim. E. Hableel – J. Baek – Y.-J. Byon – D. S. Wong: How to protect ADS-B: Confidentiality framework for future air traffic communication, https://ieeexplore.ieee.org/abstract/document/7179377.
[36] Tällaisesta mahdollisuudesta säädetään ainakin seurantadirektiivin 6a artiklassa.
[37] AIS-lähetteiden osalta Liikenteen turvallisuusviraston lausunto 4.3.2016 Liikennevirastolle merenkulun AIS-tietojen julkaisemisen rajoittamisesta sekä Suojelupoliisin lausunto 28.2.2007 Merenkulkulaitokselle: Merenkulkulaitoksen keräämän AIS-tiedon luovuttaminen muiden kuin merenkulkulaitoksen käyttöön.

3.6 Radiolähetteet ja henkilötietojen käsittely

Lähetteiden tiedot voivat tietyissä tapauksissa olla EU:n yleisen tietosuoja-asetuksen 4 artiklan 1 kohdan mukaisia henkilötietoja, kun ne liittyvät tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön.[38] Suomessa henkilötietojen käsittelyä valvoo tietosuojavaltuutettu.

Silloin, kun kyseiset tiedot katsotaan henkilötiedoiksi, niiden käsittelyyn sovelletaan tietosuoja-asetuksen säännöksiä. Tietoja hyödyntävien palveluntarjoajien tulee toimia tietoja käsitellessään tietosuoja-asetuksen mukaisesti siltä osin kuin käsiteltävissä tiedoissa on kyse henkilötiedoista. Kun tietosuoja-asetuksen mukainen rekisterinpitäjä käsittelee henkilötietoja, tulee tällä olla käsittelylleen TSA 6 artiklan 1 kohdan mukainen henkilötietojen käsittelyn oikeusperuste. Tietosuoja-asetuksen velvoitteet antavat osaltaan suojaa niiden henkilöiden yksityisyydelle ja henkilötiedoille, joihin lähetteiden tiedot ovat yhdistettävissä, vaikka kyseisiä radiolähetyksiä pidettäisiinkin sinänsä yleisesti saatavilla olevina. Koska tietosuoja-asetuksen valvonta ei kuulu Traficomin toimivaltaan, ei Traficom voi antaa ohjeistusta siitä, millä tavoin yleisesti vastaanotettavia lähetteitä käsittelemällä saatuja henkilötietoja on mahdollista käyttää.

Tietosuoja-asetusta ei kuitenkaan sen 2 artiklan 2 kohdan c alakohdan mukaisesti sovelleta ns. kotitalouskäyttöön, jota luonnollinen henkilö suorittaa yksinomaan henkilökohtaisessa tai kotitalouttaan koskevassa toiminnassa.

Vertailukohtana voidaan mainita, että aiemman lainsäädännön aikana toiminut tietosuojalautakunta myönsi yritykselle luvan kerätä ja käsitellä eräitä WiFi-liityntäpisteiden radiolähetteisiin sisältyviä tai niistä pääteltäviä tietoja.[39] Käsiteltäviin tietoihin näyttäisi sisältyneen myös ainakin radioviestinnän välitystietoja. Asiaa ei lupapäätöksessä arvioitu suhteessa radioviestinnän luottamuksellisuuteen, mutta kyseisten tietojen käsittely luvassa tarkoitetulla tavalla on ollut mahdollista vain, jos kyseiset radiolähetykset on katsottava yleisesti vastaanotettavaksi radioviestinnäksi. Tässä yhteydessä voidaan mainita Traficomin edeltäjän Viestintäviraston tulkinta WiFi-tukiasemien signaaleista. Tämän tulkinnan mukaan WiFi-verkon teknisestä toteutuksesta ja vakiintuneista käyttötavoista voitiin päätellä, että ainakin WiFi-tukiaseman hallintakehyksessä lähettämä niin kutsuttu beacon-signaali, tukiaseman nimi (SSID-tunniste) ja MAC-osoite oli tarkoitettu yleisesti vastaanotettavaksi. WiFi-tukiaseman tällaisia yleisesti vastaanotettavia radiosignaaleja voidaan sikäli verrata automaattisten valvontajärjestelmien lähetteisiin, että kyseessä ovat radiolaitteen automaattisesti kenelle tahansa kuuluvuusalueella olevalle lähettämät tiedot, joiden perusteella lähettäjä voidaan tunnistaa jollakin tasolla. Tukiaseman tiedot voidaan myös yhdistää sen sijaintiin, ja tiedot voivat olla yhdistettävissä myös luonnolliseen henkilöön. WiFi-verkoissa tapahtuva varsinainen viestintä sen sijaan on luottamuksellista.

3.7 Perus- ja ihmisoikeuksien toteutuminen

SVPL:n säännöksiä radioviestinnän luottamuksellisuudesta tulee tulkita perusoikeusmyönteisesti. SVPL 136 §:llä on tarkoitus toteuttaa perustuslain 10.2 §:ssä säädettyä luottamuksellisen viestin salaisuutta tavallisen lain tasolla ja yksityisten välillä.

[38] AIS-lähetteiden käsittelyn osalta Euroopan tietosuojavaltuutetun lausunto komission täytäntöönpanoasetuksesta (EU) N:o 404/2011 (2012/C 37/01), k. 10.
[39] Päätös 18.8.2015 t. 4/2015, https://finlex.fi/fi/viranomaiset/ftie/2015/20150004.

SVPL 136.2 §:ssä tarkoitetun yleisesti vastaanotettavaksi tarkoitetun radioviestinnän käsitteen piiriin ei tule katsoa perustuslaissa suojattua luottamuksellista viestintää.[40]

Perustuslain 10.2 §:n mukaan kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton. Säännös on sinänsä välineneutraali. Voitaneen kuitenkin katsoa, ettei tässä arvioitujen lähetteiden tyyppinen automaattinen ja määrämuotoinen yleislähete kuulu ainakaan säännöksen ydinalueelle. Lähetteitä ei ole osoitettu kenellekään tietylle taholle vaan ne on tarkoitettu kenen tahansa kuuluvuusalueella olevan käytettäväksi. Tämän johdosta on kyseenalaista, voidaanko niitä pitää sellaisina luottamuksellisina viesteinä, joiden osalta olisi ylipäänsä olemassa sellaisia ulkopuolisia tahoja, joille olisi oikeudetonta saada tieto viestistä.

Perustuslakivaliokunta on katsonut, että miehittämättömän ilma-aluksen kauko-ohjauksessa ydinvoimalan alueelle esimerkiksi matkapuhelimen tai tietokoneen avulla ei ole kysymys sellaisesta perustuslain 10 §:n 2 momentin tarkoittamasta luottamuksellisesta viestinnästä, jolle kyseisen perustuslain säännöksen kautta on ylipäänsä tarkoitettu antaa perustuslain suojaa.[41] Tällöin suuremmalla syyllä on katsottava, ettei myöskään RID-yleislähete saisi vastaavassa oikeudettoman lennätyksen tilanteessa perustuslain 10.2 §:n suojaa, sillä toisin kuin ohjausliikenne, se nimenomaan on tarkoitettu muuhun kuin dronen lennättäjän omaan käyttöön. Perustuslain kannalta ei vaikuta olevan syytä arvioida eri tavalla myöskään AIS- tai ADS-B-lähetteitä vastaavassa tilanteessa niiden samankaltaisten piirteiden takia.

Epäselvää kuitenkin on, missä määrin perustuslakivaliokunnan arvioon on vaikuttanut se, että arviointi rajautui ydinvoimalan alueelle tapahtuvaan lennätykseen, joka tyypillisesti on kiellettyä, ja voisiko arvion lopputulos olla yleisemmässä tarkastelussa mahdollisesti erilainen. Ilmailulakiin lisätyn miehittämättömien ilma-alusten havainnointitoimivaltaa koskevan säännöksen esitöissä onkin omaksuttu perustuslakivaliokunnan lausunnon pohjalta käsitys, että nimenomaan oikeudettomasti tapahtuvan lennätyksen yhteydessä tapahtuva radioviestintä ei nauti vastaavaa luottamuksellisuuden suojaa kuin asianmukaisen lennätyksen yhteydessä tapahtuva viestintä.[42] Samoissa esitöissä on kuitenkin todettu, että vaatimus miehittämättömien ilma-alusten etätunnistusjärjestelmästä toisi osan (eli RID-lähetteet) miehittämättömän ilma-aluksen lennättämisen radioviestinnästä yleisesti vastaanotettavaksi.[43] Mikäli tämä hyväksytään, tulisi ADS-B- ja AIS-lähetteitä arvioida lähtökohtaisesti samoin. Yleislähetteen osalta kaikkien kuuluvuusalueella olevien mahdollisuus kuunnella lähetystä ei ole ei-toivottu seuraus radiolähetysten luonteesta, vaan nimenomaan järjestelmään suunniteltu ja tavoiteltu piirre.

Viestinnän luottamuksellisuus turvataan myös Euroopan ihmisoikeussopimuksen (EIS) 8 artiklassa, joka antaa suojaa "kirjeenvaihdolle", jota Euroopan ihmisoikeustuomioistuin (EIT) on tulkinnut laajasti. EIT tyypillisesti selvittää suojan soveltumista arvioimalla, onko yksilöllä ollut perusteltu odotus siitä, että hänen yksityisyytensä on turvattu (reasonable expectation of privacy).[44] EIT:n ratkaisukäytännöstä on pääteltävissä, että sitä, onko odotus yksityisyydestä perusteltu, voidaan arvioida muun

[40] Perustuslakivaliokunta on aiemmin todennut, että nykyisin SVPL 136.2 §:ään sisältyvä sääntely luottamuksellisen radioviestinnän ulkopuolelle rajatuista viesteistä ja viestinnän muodoista ei kohdistunut perustuslailla suojattuun luottamukselliseen viestintään (PeVL 44/2004 vp - HE 75/2004 vp hallituksen esitys laiksi radiolain muuttamisesta).
[41] PeVL 22/2020 vp - HE 8/2020 vp Hallituksen esitys eduskunnalle laeiksi ydinenergialain, turvallisuusselvityslain 21 §:n ja kaivoslain muuttamisesta.
[42] HE 197/2021 vp, s. 88. Korkein oikeus on myös katsonut, että rikosten suunnittelua tai tekemistä koskeva viestintä jää yksityiselämän suojan ydinalueen ulkopuolelle (KKO 2023:14, k. 31).
[43] HE 197/2021 vp, s. 12.
[44] Bărbulescu v. Romania, asia 61496/08, ratkaistu 5.9.2017 (suuri jaosto), k. 73.

muassa sillä perusteella, onko puuttumisesta yksityisyyteen informoitu henkilöä tai onko tällaisen puuttumisen mahdollisuudesta erityisiä viitteitä, sekä puuttumisen luonteen, pysyvyyden ja vaikutusten perusteella.[45]

EIT on vanhemmassa ratkaisukäytännössään arvioinut radioviestinnän luottamuksellisuutta. Tapauksessa *X ja Y v. Belgia* katsottiin, että yksityinen radioviestintä voi sinänsä kuulua EIS 8 artiklassa tarkoitetun kirjeenvaihdon käsitteen piiriin.[46] EIT on kuitenkin myöhemmin todennut tapauksessa *B.C v. Sveitsi*, ettei EIS 8 artiklan mukainen luottamuksellisen viestin suoja ulotu luvattomiin radiolähetyksiin taajuudella, joka oli varattu toiseen käyttöön, kuten kyseisessä tapauksessa ilmailulle. Viimeksi mainitussa tapauksessa viitattiin myös siihen, että keskustelu tällaisella taajuudella oli muiden saatavissa, jolloin sitä tuskin voitiin pitää "yksityisenä". Hakijan todettiin näin toimimalla altistaneen itsensä riskille, että keskustelu paljastuu sivullisille.[47] Toisaalta myöhemmän käytännön mukaan kirjeenvaihdon suojaa ei EIS 8 artiklassa kvalifioida lainkaan, vaan suojan piirissä on myös muu kuin yksityinen viestintä.[48]

EIT:n ratkaisukäytännöstä ei ole saatavilla selvää johtoa käsillä olevaan tulkintatilanteeseen, mutta huomiota voidaan kiinnittää ainakin seuraaviin seikkoihin. Kuten edellä todettiin, AIS- ja ADS-B-järjestelmien käyttäjien tiedossa voidaan nykyisin selkeästi olettaa tietojen avoin saatavilla olo eri palveluissa. Kun tietoja jo käsitellään laajasti, ko. radioviestinnän katsominen luottamukselliseksi ei näyttäisi vastaavan lähettimien ja tietojen käyttäjien käsitystä tietojen luonteesta, jolloin järjestelmien käyttäjillä ei välttämättä voida katsoa olevan perusteltuja odotuksia yksityisyydestä. Myös RID-lähetteiden osalta lennättäjän tiedossa tulee olemaan lähetteiden olemassaolo ja käyttötarkoitus, sillä lennättäjän velvollisuutena on käyttää RID-järjestelmää ja lennättäjän on syötettävä itse tietonsa järjestelmään, jolloin hänen tietoonsa viimeistään tulee järjestelmän olemassaolo. EIT:n oikeuskäytännössä on tosin katsottu, ettei viestinnän luottamuksellisuutta voida kokonaan poistaa edes tilanteessa, jossa perusteltua odotusta yksityisyydestä ei olisi. Tapauksessa *Bărbulescu v. Romania* jäi avoimeksi, oliko työntekijälle jäänyt tällaista perusteltua odotusta sen jälkeen, kun työnantaja oli antanut joitakin tietoja viestinnän valvonnasta työpaikalla.[49] Tällä tulkintaratkaisulla voidaan katsoa suojattavan oikeuden ydinaluetta myös tilanteissa, joissa viestinnän luottamuksellisuutta on rajoitettu. Tapaukseen *B.C v. Sveitsi* verrattavasti AIS-, ADS-B ja RID-järjestelmiä käyttävän voidaan sanoa ottavan riskin, että lähetteitä kuuntelemaan pystyvä taho voi hyödyntää lähetteiden sisältöä; tässä arvioitava kysymys on kuitenkin tuota EIT:n tapausta monimutkaisempi, sillä automaattisten tunnistusjärjestelmien käyttö on monissa tilanteissa pakollista, kun taas EIT:n tapauksessa arvioitu radiolaitteen käyttö oli nimenomaan kiellettyä. Kuten edellä mainittiin, näyttää kuitenkin olevan mahdollista tehdä päätelmä, ettei näiden lähetteiden katsottaisi kuuluvan lainkaan luottamuksellisen viestinnän perusoikeussuojan piiriin Suomessa, vaan kyse olisi yleisesti vastaanotettavasta radioviestinnästä. Yllä mainittu perustuslakivaliokunnan kannanotto jättää jossain määrin epäselväksi, olisiko nimenomaan toiminnan oikeudettomuus ratkaiseva tekijä sen suhteen, onko siihen liittyvä radioviestintä perusoikeussuojan piirissä vai ei.

Kaikki seikat huomioon ottaen vaikuttaa perustellulta katsoa, ettei RID-, AIS- tai ADS-B-järjestelmien käyttäjillä voi olla sellaista perusteltua odotusta yksityisyydestä näitä järjestelmiä käytettäessä ja siten näiden lähetysten luottamuksellisuudesta,

[45] Frank Hendrickx – Aline Van Bever: Article 8 ECHR: Judicial Patterns of Employment Privacy Protection, s. 189. Teoksessa Filip Dorssemont et al. (toim.): The European convention on human rights and the employment relation, 2013.
[46] X ja Y v. Belgia, asia 8962/80, ratkaistu 13.5.1982, k. 4.
[47] B.C v. Sveitsi, asia 21353/93, ratkaistu 27.2.1995, kohta 1.
[48] Bărbulescu v. Romania, k. 72.
[49] Bărbulescu v. Romania, k. 80.

jonka nojalla EIS 8 artikla soveltuisi kyseisten järjestelmien yleislähetteisiin. Lähetteet eivät ole luonteeltaan minkään tiettyjen osapuolten välistä viestintää, sillä niitä ei ole osoitettu kenellekään tietylle taholle.[50] Sen sijaan ne on nimenomaan suunniteltu mahdollistamaan alusten ja ilma-alusten tunnistaminen kaikille kuuluvuusalueella oleville tahoille. Järjestelmiä säätelevässä erityislainsäädännössä ei anneta takeita tietojen säilymisestä luottamuksellisina suhteessa niitä kuuntelemaan pystyviin sivullisiin.

Vaikuttaakin asianmukaiselta tarkastella näiden lähetteiden käsittelyä viestinnän luottamuksellisuuden sijasta yleisemmin siltä kannalta, miten lähetteiden tietojen käyttö vaikuttaa henkilön yksityisyyden suojaan esimerkiksi sisältämällä tietoja aluksesta ja sitä kautta alukseen yhdistettävissä olevista henkilöistä. Olennaista on ottaa huomioon, että perustuslaissa turvattu yksityiselämän suoja sekä henkilötietojen suoja voivat koskea myös tällaisten tietojen käsittelyä. Tämä tarkoittaa, että perusoikeusjärjestelmässä ja muutoin lainsäädännössä annetaan muilla kuin viestinnän luottamuksellisuuden keinoin suojaa näille eduille. Tämä puoltaa sitä, ettei luottamuksellisen radioviestinnän alan laaja tulkinta ole tarpeen perusoikeuksien toteutumisen turvaamiseksi.

Edellä sanotun perusteella voidaan todeta, ettei perusoikeusmyönteinen laintulkinta vaadi yleisesti vastaanotettavan radioviestinnän käsitteen suppeaa tulkintaa niin, että AIS-, ADS-B- ja RID-lähetteet tulisi katsoa luottamuksellisiksi.

4 Johtopäätökset

Tässä muistiossa arvioitujen automaattisten tunnistusjärjestelmien (AIS, ADS-B ja RID) lähetteet on syytä katsoa kokonaisarvion perusteella SVPL 136 §:n 2 momentin 6 kohdan mukaiseksi yleisesti vastaanotettavaksi tarkoitetuksi radioviestinnäksi. Tämä tarkoittaa samalla aiemman AIS- ja ADS-B-lähetteiden luottamuksellisuutta koskevan tulkinnan päivittämistä. Tässä muistiossa esitetyt arviointiperusteet voivat olla sovellettavissa myös muihin samankaltaisiin lähetteisiin.

Yllä mainittujen lähetteiden tulkitseminen yleisesti vastaanotettavaksi tarkoitetuksi radioviestinnäksi merkitsee sitä, että lähetteiden tietoja ei suojata radioviestinnän luottamuksellisuutta koskevan SVPL:n sääntelyn nojalla. Näin ollen näiden tietojen käsittelyyn ei sovellu SVPL 136 §:n 4 momentin mukainen vaitiolovelvollisuus ja hyväksikäyttökielto, vaan tietoja voidaan käsitellä SVPL:n viestinnän luottamuksellisuutta koskevien säännösten estämättä. Tämä ei kuitenkaan tarkoita sitä, että lähetteitä voisi käsitellä täysin vapaasti. Tietojen käsittelyyn voi yllä todetusti soveltua ainakin EU:n yleinen tietosuoja-asetus.

[50] Esimerkiksi sähköisen viestinnän tietosuojadirektiivissä viestinnällä tarkoitetaan ainoastaan viestintää *tiettyjen osapuolten kesken* (2 artikla).