

Asia: VN/36541/2024

## **Lausuntopyyntö luonnoksesta hallituksen esitykseksi poliisilain 5 a luvun (siviilitiedustelu) muuttamiseksi ja siihen liittyviksi laeiksi**

### Lausunnonantajan lausunto

#### **Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään**

Poliisihallituksen lausunto Sisäministeriölle luonnoksesta hallituksen esitykseksi poliisilain 5 a luvun (siviilitiedustelu) muuttamiseksi

Sisäministeriö on pyytänyt Poliisihallitukselta lausuntoa luonnoksesta hallituksen esitykseksi poliisilain 5 a luvun (siviilitiedustelu) muuttamiseksi.

Esityksessä ehdotetaan muutettavaksi poliisilain lisäksi lakia tietoliikennetiedustelusta siviilitiedustelussa, rajavartiolakia, henkilötietojen käsittelystä rajavartiolaitoksessa annettua lakia ja rikoslakia. Edelleen ehdotetaan muutettavaksi viranomaisten toiminnan julkisuudesta annettua lakia.

#### 1 Lausunto

##### 1.1 Yleistä

Poliisihallitus on tutustunut lausuttavana olevaan luonnokseen hallituksen esitykseksi ja Poliisihallituksen näkemyksen mukaan on välttämätöntä, että Suojelupoliisilla on ajantasaiset ja riittävät siviilitiedustelun toimivaltuudet toteuttaa tiedustelua; hankkia ja käsitellä tietoa kansallista turvallisuutta uhkaavasta toiminnasta.

Siviilitiedustelulainsäädäntö tuli voimaan 1. kesäkuuta 2019. Siviilitiedustelutoimintaa koskevat keskeiset säännökset sisältyvät poliisilain (872/2011) 5 a lukuun ja tietoliikennetiedustelusta siviilitiedustelussa annettuun lakiin (582/2019).

Lain voimaantulon jälkeisenä aikana ja käytännön soveltamisen kautta on tehty havaintoja lain uudistamisen tarpeista. Uudistamista puoltavat myös vaikeutunut turvallisuustilanne ja tekninen kehitys, joka jatkuvasti haastaa viranomaisten kyvykkyyttä vastata uhkiin.

Edellä mainituin perustein Poliisihallitus pitää esitystä kokonaisuutena kannatettavana.

Poliisihallitus kiinnittää huomiota siihen, että siviilitiedustelun kohteena olevan valtiollisen toimijan toiminta Suomessa voi samanaikaisesti täyttää myös jonkin rikoslain rikoksen tunnusmerkistön (esimerkiksi vakoilurikokset). Myös erilaiset hybridiuhkat ilmenevät poliisin tehtäväkentässä usein monimuotoisena rikollisuutena, jonka taustalla olevista tekijöistä ja motiiveista voi olla kuitenkin vaikeaa saada selvitystä. Tiedonhankinnan alkuvaiheessa toiminnan taustalla olevaa valtiollista toimijaa voi olla vaikeaa tunnistaa. Tämän vuoksi on tärkeää, että siviilitiedusteluviranomaiset huolehtivat riittävästä koordinaatiosta

poliisin ja muiden toimivaltaisten viranomaisten kesken päällekkäisten toimien havaitsemiseksi sekä operaatioturvallisuuden varmistamiseksi.

Koordinaatiovelvoite on kirjattu jo voimassa olevaan poliisilain 5a luvun 56 §:ään. Vastaavanlainen koordinaatiovelvoite on kirjattu myös rikostiedustelua koskevaan hallituksen esitysluonnokseen.

Koordinaatiovelvoitteen lisäksi on tärkeää, että tieto mahdollisesta vakavasta rikosepäilystä luovutetaan niin kutsutun palomuurisääntelyn mukaisesti Keskusrikospoliisille tai muulle toimivaltaiselle viranomaiselle. Poliisilain 5 a luvun 44 §:n mukaan suojelupoliisin on ilman aiheetonta viivytystä ilmoitettava Keskusrikospoliisille, jos tiedustelumenetelmän käytön aikana ilmenee, että voidaan olettaa tehdyksi sellainen rikos, josta säädetty ankarin rangaistus on vähintään kuusi vuotta vankeutta. Ilmoitusta saadaan suojelupoliisin päällikön päätöksellä siirtää enintään vuodeksi kerrallaan, jos se on välttämätöntä

kansallisen turvallisuuden varmistamiseksi tai hengen tai terveyden suojaamiseksi. Arvioinnissa on otettava huomioon rikoksen selvittämisen tai sen estämisen merkitys yleisen ja yksityisen edun kannalta. 44 § 2 momentin mukaan Suojelupoliisin on viipymättä ilmoitettava rikoksen estämiseksi toimivaltaiselle viranomaiselle, jos tiedustelumenetelmän avulla saadusta tiedosta ilmenee, että hankkeilla on sellainen rikos, josta säädetty ankarin rangaistus on vähintään kuusi vuotta vankeutta ja rikos on vielä estettävissä.

## 2 Säännöskohtaiset huomiot

### 2.1 14 § Teknisestä laitetarkkailusta siviilitiedustelussa päättäminen

Teknistä laitetarkkailua koskevan 14 §:n 3 momentin 2 kohtaan lisättäisiin viittaus teknistä laitetta tai ohjelmistoa käyttävästä henkilöstä. Teknisen laitetarkkailun lupa olisi mahdollista myöntää jatkossa joko laite- tai ohjelmistokohtaisesti taikka henkilöperusteisesti. Poliisihallitus pitää esitettyä muutosta kannatettavana. Vastaava muutos henkilöperusteisesta laitetarkkailusta tulisi tehdä myös poliisilain 5 lukuun sekä pakkokeinolain 10 lukuun.

Poliisihallitus kiinnittää huomioita määritelmien eroavaisuuksiin laite-etsinnän ja teknisen laitetarkkailun osalta. Laite-etsinnän yhteydessä käytetään sanaa tietojärjestelmä, mutta teknisen laitetarkkailun yhteydessä on sen sijaan käytetty ohjelmiston -käsitettä. Olisikin arvioitava, onko laitetarkkailun kohteen määritelmä riittävän täsmällinen ja kattava sekä tietoverkkoympäristön ja tietojärjestelmien erityispiirteet huomioiva. Poliisissa on tunnistettu laitetarkkailun määritelmästä johtuvat kohteen yksilöintiin liittyvät haasteet. Yksittäisen fyysisten laitteen osalta yksilöinti on yksiselitteisemmin tehtävissä, kuin tietojärjestelmien/ohjelmistojen osalta. Laitetarkkailun nykyinen terminologia olisi tarkoituksenmukaisempaa korvata käsitteillä tietojärjestelmä tai sen osa.

## 2.2 16 § Laitteen, menetelmän tai ohjelmiston asentaminen ja poisottaminen siviilitiedustelussa

Poliisilain 5a luvun 16 §:ään lisättäisiin uusi 2 momentti, jonka mukaisesti tiedusteluviranomainen voisi pyytää viranomaisen ulkopuolisen henkilön tekemään yksittäisen tiedustelumenetelmän käytön edellyttämän asennus- tai poistamistoimenpiteen. Ulkopuolista asennusapua tarvitaan erityisesti, kun kyse olisi laitteen, menetelmän tai ohjelmiston sijoittamisesta sellaisiin teknisesti hyvin suojattuihin tietojärjestelmiin, joita hyödynnetään kansallista turvallisuutta vakavasti uhkaavaan toimintaan tai jotka sisältävät sellaista uhkaa koskevaa tärkeää tietoa. Tällaisten tietojärjestelmien suojauksen kiertäminen tai purkaminen ulkopuolelta tapahtuvien toimenpiteiden avulla voi olla erittäin vaikeaa tai mahdotonta. Perusteluissa korostetaan ulkopuolisen avun viimesijaisuutta, mutta tämä ei käy ilmi itse säännöksestä.

Viranomaisen ulkopuolisen henkilön toteuttamaan asennus- tai poistotoimenpiteeseen saattaa liittyä niin juridisia, kuin myös operatiivisia riskejä. Jatkovalmistelussa olisikin perusteltua kiinnittää huomiota seuraaviin seikkoihin: Suojelupoliisin päällystöön kuuluvan poliisimiehen valvonta, minkälaista välittömyyttä valvonnalta edellytetään ja onko Suojelupoliisilla velvollisuus huolehtia ulkopuolisen henkilön turvallisuudesta tehtävän aikana?

Ulkopuolisen henkilön oikeudellinen asema asennus- tai poistamistoimenpiteen paljastuessa. Toimenpidettä suorittaessaan henkilö saattaa pahimmillaan syyllistyä jonkun rikoslain mukaisen rikoksen tunnusmerkistön mukaiseen tekoon (esim. yritysvakoilu tai tietojärjestelmän häirintä). Esityksessä ei ole tuotu esille, miten ulkopuolista asentajaa suojattaisiin tällaisilta väitteiltä, olisiko tältä osin säänneltävä vastaavanlaisesta syytevapaudesta kuin valtionrajarikoksen osalta esitetään Suomea avustaneen henkilön osalta. Avustaminen saattaa myös aiheuttaa henkilölle työpaikan menetyksen ja vahingonkorvausvastuun.

## 2.3 18 a § Yksinomaan tietoverkossa toteutettava peitetoiminta, 18 b § Yksinomaan tietoverkossa toteutettavasta peitetoiminnasta päättäminen

Uutena tiedustelumenetelmänä esitetään säädettäväksi tietoverkossa toteutettavasta peitetoiminnasta. Esityksen mukaisesti tietoverkossa toteutettavan peitetoiminnan kohdentaminen olisi varsin avointa. Voimasta olevan siviilitiedustelun peitetoimintaa koskevan lainsäädännön mukaisesti on yksilöitävä tiedonhankinnan kohteena oleva henkilö tai, jos tiettyä henkilöä ei voida yksilöidä, henkilöryhmä riittävästi yksilöitynä, sekä 3§:ssä tarkoitettu siviilitiedustelun kohteena oleva toiminta, esimerkiksi terrorismi (17 § ja 18 §).

Esityksen mukaisesti tietoverkossa toteutettavan peitetoiminnan osalta riittävää olisi kohdentaminen 3 § mukaisesti esimerkiksi terrorismiin, ilman nykyistä yksilöintiä tiedonhankinnan kohteesta (tiedonhankinnan kohteena oleva henkilö tai, jos tiettyä henkilöä ei voida yksilöidä, henkilöryhmä riittävästi yksilöitynä).

Poliisihallituksen näkemyksen mukaan tietoverkossa toteutettavan peitetoiminnan avoin kohdistaminen luo haasteita yhteensovittamiselle, koordinoinnille ja kohteiden tunnistamiselle tilanteessa, jossa Poliisihallituksen alaisella poliisilla olisi käynnissä peitetoimintaoperaatio samaan kohteeseen liittyen rikoksen estämiseksi (Poll 5) tai rikoksen selvittämiseksi (PKL 10).

## 2.4 28 a § Aineen, omaisuuden tai esineen tilapäinen haltuunotto

28 a § 2 momentissa todetaan: ”Jollei omaisuutta, esinettä tai ainetta voida vaaratta palauttaa, suojelupoliisin päällystöön kuuluva poliisimies voi määrätä omaisuuden, esineen tai aineen hävitettäväksi. Hävittämisestä on tehtävä merkintä paikkatiedustelusta laadittavaan pöytäkirjaan tai tehtävä vastaava merkintä muuhun asiakirjaan.”

Esityksen 28 a § perusteluissa mainitaan tilanne, jossa pykälän toimivaltuudella hankittu tieto esimerkiksi räjähteessä käytettävästä aineesta varmistuisi, tieto voitaisiin luovuttaa niin kutsutun palomuurisääntelyn mukaisesti rikostorjuntaviranomaiselle. Esityksessä ei oteta kantaa siihen voisiko Suojelupoliisi palomuri-ilmoituksen ohessa luovuttaa esineen, aineen tai omaisuuden rikostorjuntaviranomaiselle. Kyseessä voisi olla rikosasiaan liittyvä todiste, jota ei tulisi 2 momentin perusteella hävittää.

## 2.5 39 a § Tietojärjestelmän käytön estäminen tai sen toiminnan haittaaminen vakavan vaaran torjumiseksi

Poliisilakiin esitetään uutta toimivaltuutta, jonka mukaan suojelupoliisi voisi estää Suomen ulkopuolella olevan tietojärjestelmän käytön tai haitata sen toimintaa, jos tietojärjestelmällä tai sen kautta voidaan aiheuttaa kansalliselle turvallisuudelle vakavaa vaaraa.

Toimivaltuus ei varsinaisesti olisi niin sanottu tiedonhankinnallinen toimivaltuus, vaan ennemminkin niin sanottu vaikuttamistoimivaltuus. Nykyiset viranomaisten toimivaltuuksiin sisältyvät menetelmät rajautuvat pitkälti tiedonhankintaan, mutta eivät aiheutuvan haitan tai vahingon tai vaaran estämiseen. Esitettyä muutosta onkin pidettävä kannatettavana. Varsinkin rikollisten infrastruktuuri on usein nopeasti monistettavissa tai se on verkotettu

niin, ettei yhteen fyysiseen laitteeseen kajoaminen nyky menetelmin estä infrastruktuurin toimintaa.

Luonnoksessa on tunnistettu toimenpiteeseen mahdollisesti liittyvät ulko- ja turvallisuuspoliittiset herkkyydet. Vakavan vaaran torjumiseksi toimivaltuuden voi katsoa olevan välttämätön, koska ilman ehdotettua vaikuttamistyyppistä toimivaltuutta siviilitiedustelun toimintamahdollisuudeksi jäisi lähinnä vaaraa aiheuttavan järjestelmän toiminnan seuraaminen. Todettakoon, että myös poliisin toiminnassa on tunnistettu tilanteita, joissa vastaavantyyppisiä toimenpiteitä olisi tarpeen toteuttaa rikosten estämiseksi kyberympäristössä.

Toimivaltuuden toteuttamiseen saattaa liittyä myös tarve toiminnan koordinoimiseen poliisin kanssa. Kansallista turvallisuutta uhkaavat teot täyttävät usein myös jonkin rikoksen tunnusmerkistön. On siten mahdollista, että poliisilla on meneillään toimenpiteitä samaan kohdetietojärjestelmään esimerkiksi osana kansainvälistä operaatiota. Operaatioiden turvaamiseksi sekä paljastumisen estämiseksi on välttämätöntä, että siviilitiedustelutoimenpiteiden käyttö yhteensovitetaan poliisilain 5a luvun 56 §:n edellyttämällä tavalla. Toimivaltaisten viranomaisten keskinäisen koordinaation kautta kyetään lisäksi varmistamaan tavoitteen mahdollisimman tehokas toteuttaminen, hallitsemaan riskejä, kartoittamaan

laajemmin eri toimintavaihtoehtoja ja löytämään tarvittaessa matalariskisempiä toimintavaihtoehtoja.

## 2.6 55 a § Yhteistoiminta Rajavartiolaitoksen kanssa

Poliisilakiin esitetään uutta pykälää, jossa säädettäisiin Rajavartiolaitoksen mahdollisuudesta Suojelupoliisin pyynnöstä suorittaa itsenäisesti, ilman valvontaa, poliisilain 5 luvun 13 §:n 1 momentissa, poliisilain 5 a luvun 9, 11-16, 26 ja 28 §:ssä säädetyn yksittäisen toimenpiteen. Tiedustelumenetelmiä, joita säännökset koskevat ovat suunnitelmallinen tarkkailu, teknisen tarkkailun menetelmät (katselu, kuuntelu, seuranta, tekninen laitetarkkailu), telepäätelaitteen yksilöintitietojen hankkiminen, paikkatiedustelu ja jäljentäminen siviilitiedustelussa.

Jatkovalmistelussa olisi tarpeen kiinnittää huomioita 55 a § 1 momentin muotoiluun, jotta myös pykälästä ilmenisi perusteluissa todetun mukaisesti, että Suojelupoliisi vastaisi tiedustelumenetelmää koskevasta päätöksestä tai luvasta.

Jatkovalmistelussa olisi tarpeen myös tarkentaa ehdotetun 55 a §:n 4 momentin suhdetta niin sanottuun palomuurisääntöön. Poliisin toiminnan kannalta on tärkeää, että tiedustelumenetelmän käytön aikana saatu, vielä estettäviin tai tapahtuneisiin rikoksiin liittyvä tieto, luovutetaan palomuurisääntelyn mukaisesti.

## 3 Lopuksi

Lisäksi Poliisihallitus nostaa esiin poliisin rikostiedustelua koskevan lain, joka on lausunnon antamisen aikaan valmisteilla Sisäministeriössä. Puolustusvoimat käyttää sotilastiedustelulakia ulkoisen uhan torjuntaan ja Suojelupoliisi siviilitiedustelun toimivaltuuksia kansalliseen turvallisuuden uhkien torjuntaan. Kokonaistiedustelun ja sisäisen turvallisuuden näkökulmasta Poliisihallituksen alaisella poliisilla ei kuitenkaan ole toimivaltuuksia rikostiedusteluun, joilla torjuttaisiin yksilön tai yhteiskunnan turvallisuutta vakavasti uhkaavaa rikollisuutta. Poliisihallitus pitää erittäin tärkeänä, että rikostiedustelua koskeva

laki saadaan säädettyä.

Ylipelkonen Jari  
Poliisihallitus

