

Puolustusministeriö

Lausuntopyyntöne 9.2.2015 FI.PLM.2015-218

TIEDONHANKINTALAKITYÖRYHMÄN MIETINTÖ

Puolustusministeriö on pyytänyt oikeusministeriöltä lausunnon tiedonhankintalakitöryhmän mietinnöstä. Oikeusministeriö toteaa lausuntoon seuraavan.

1. Lähtökohdista

Työryhmän mietinnössä tarkastellaan kansalliseen turvallisuuteen liittyvää tiedonhankintaa yhtäältä Suomessa tapahtuvan tietoliikennetiedustelun ja toisaalta ulkomaan tiedustelun (ml. henkilötiedustelu ja tietojärjestelmätiedustelu) kannalta.

Kansalliseen turvallisuuteen kohdistuvia uhkia torjuvien viranomaisten tiedustelutoimivallasta ja sen jakautumisesta siviili- ja sotilasviranomais-ten välillä ei ole nykyisin lainsäädäntöä. Nykyiset säännökset viranomais-ten tiedonhankintavaltuuksista perustuvat yksinomaan rikostorjuntaan. Myös ulkomaan henkilötiedustelulta ja ulkomaan tietojärjestelmätiedus- telulta puuttuu nykyisin sääntelypohja.

Oikeusministeriö keskittyy lausunnossaan arvioimaan työryhmän mietin- töä erityisesti Suomessa tapahtuvan, rajat ylittävään tietoliikenteeseen kohdistuvan tiedustelun osalta. Työryhmän johtopäätökset ulkomaan tie- dustelua koskevista sääntelytarpeista ovat alustavia eikä oikeusministeri- öllä ole niistä tässä vaiheessa lausuttavaa.

2. Tietoliikennetiedustelun suhde perustuslakiin

Työryhmän mietinnössä on asianmukaisesti selvitetty tietoliikennetiedustelun oikeudellisia reunaehdoja niin perustuslain kuin Euroopan unionin oikeusjärjestyksen ja kansainvälisten ihmisoikeussopimusten sekä näitä koskevan tulkintakäytännön kannalta.

Perustuslain 10 §:n 3 momentin mukaan lailla voidaan säätää välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä ja turvallisuustarkastuksessa sekä vapaudenmenetyksen aikana. Nämä perustuslaissa säädetyt perusteet luottamuksellisen viestin suojan rajoittamiselle on tarkoitettu tyhjentäviksi (HE 309/1993 vp, s. 54). Perustuslaki ei siten tunnista viestin salaisuuden mahdollisena rajoitusperusteena kansallista turvallisuutta, ellei rajoitusperuste kytkeydy vähintään konkreettiseen ja yksilöityyn rikosepäilyyn perustuslakivaliokunnan tähänastisen tulkintakäytännön edellyttämällä tavalla.

Kuten mietinnössä todetaan (s. 59-60), perustuslain asettamat reunaehdot muodostuvat kansainvälisiin ihmisoikeusvelvoitteisiin verrattuna tiukemmiksi, sillä esimerkiksi Euroopan ihmisoikeussopimuksen 8 artikla sallii kansallisen turvallisuuden mahdollisena rajoitusperusteena.

Työryhmä on johtopäätöksissään päätenyt siihen, että tiedustelutarkoituksessa toteutettava tietoliikennetiedustelu näyttäisi edellyttävän perustuslain muuttamista. Työryhmän mukaan jatkotyössä voitaisiin pohtia, olisiko tehokasta tietoliikennetiedustelua mahdollista toteuttaa ensi vaiheessa rajoitetummin esimerkiksi kohdentamalla se tunnistamistietoihin (s. 80).

Oikeusministeriö yhtyy työryhmän oikeudelliseen arviointiin siitä, että tietoliikennetiedustelun mahdollistaminen Suomessa edellyttäisi perustuslain muuttamista. Oikeusministeriö kiinnittää tässä yhteydessä huomiota perustuslakivaliokunnan linjauksiin perustuslain muutostarpeiden arvioinnin yleisistä lähtökohdista. Valiokunnan mukaan perustuslain mahdollisia muutostarpeita tulee arvioida huolellisesti ja välttämättömiksi arvioidut muutokset tehdä perusteellisen valmistelun sekä siihen liittyvän laajapohjaisen keskustelun ja yhteisymmärryksen pohjalta (PeVM 9/2010 vp, s. 3/II, PeVM 10/2006 vp, s. 2-3, PeVM 5/2005 vp, s. 2/I).

Jatkopohdinnoissa on lisäksi otettava huomioon se, että perustuslakivaliokunnan tulkinta viestin tunnistamistietojen perusoikeussuojasta on Euroopan unionin oikeusjärjestyksen vaikutuksesta tarkentunut aikaisempaan verrattuna.

Valiokunnan aikaisemmassa tulkintakäytännössä viestin tunnistamistietojen katsottiin jäävän luottamuksellisen viestin salaisuutta suojaavan pe-

rusoikeuden ydinalueen ulkopuolelle, jolloin tunnistamistietoihin kohdistuvia rajoitustoimia ei arvioitu samanlaisin tiukoin kriteerein kuin oikeuden ydinalueeseen puuttuvia rajoituksia. Sitten perustuslakivaliokunta on katsonut — arvioidessaan Euroopan unionin tuomioistuimen ratkaisun (ns. Data Retention –direktiivin pätevyys, EUT:n tuomio yhdistetyissä asioissa C-293/12 ja C-594/12) merkitystä tietoyhteiskuntakaaren säännösten kannalta —, että ”käytännössä sähköisen viestinnän käyttöön liittyvät tunnistamistiedot sekä mahdollisuus niiden kokoamiseen ja yhdistämiseen voivat kuitenkin olla yksityiselämän suojan näkökulmasta siinä määrin ongelmallisia, että kategorinen erottelu suojan reuna- ja ydinalueeseen ei aina ole perusteltua, vaan huomiota on yleisemmin kiinnitettävä myös rajoitusten merkittävyyteen” (PeVL 18/2014 vp, s. 6/II).

Työryhmän hahmottelemat alustavat suuntaviivat tietoliikennetiedustelun edellyttämästä lupamenettelystä, tiedon käsittelyn menettelytapasääntelystä ja tarpeellisista oikeussuojakeinoista sekä oikeudellisen ja parlamentaarisen valvonnan järjestämisestä ovat oikeusministeriön mielestä oikeansuuntaisia.

3. Tietoliikennetiedustelun suhde rikostorjuntaan ja poliisin salaisiin tiedonhankintakeinoihin

Nykytilanteen arvioinnin ja mahdollisesti tarvittavien toimenpiteiden arvioinnin kannalta keskeistä on sen määrittäminen, mitä ”uhalla” tarkoitetaan. Mietinnön johdantojaksossa sivulla 13 todetaan, että kysymys ei ole tavanomaisena pidettävästä verkkorikollisuuden torjunnasta vaan kansalliseen turvallisuuteen kohdistuvien vakavien uhkien havaitsemisesta ja tunnistamisesta sekä niiden torjunnan mahdollistamisesta. Toisaalta sivulla 21 tietoverkkouhkia koskevassa jaksossa nostetaan esimerkkeinä esiin kybervakoilu ja kyberhyökkäykset, joilla tässä yhteydessä ilmeisesti tarkoitetaan tekoja, jotka ovat Suomen rikoslainsäädännön mukaan rangaistavia tekoja. Myöhemmin tiedonhankintatoimivaltuuksien käsittelyn yhteydessä (sivu 47) todetaan, ettei salaisia tiedonhankintakeinoja voida nykyisin käyttää pelkän tiedustelutiedon hankkimiseen sellaisesta esimerkiksi kansallista turvallisuutta uhkaavasta toiminnasta, joka ei ole edennyt rikoksen valmistelun asteelle tai ei ole säädetty rangaistavaksi.

Mainittujen viittausten ja muiden uhkaa käsittelevien mietinnön osien perusteella jossakin määrin epäselväksi jää se, mihin uhkiin tietoliikennetiedustelulla puututtaisiin. Selvänä voidaan kuitenkin pitää sitä, että mahdollisella tietoliikennetiedustelulla saatujen tietojen avulla tulisi ainakin puuttua toimintaan, joka jo tiedustelun siihen kohdistuessa on rikos tai joka ainakin jatkuessaan esteettömästi tulisi olemaan rikos. Rikoksella tässä yhteydessä tarkoitetaan paitsi täyttynyttä rikosta, rikoksen täyttymistä edeltävää rangaistavaksi säädettyä valmistelua tai rangaistavaksi säädettyä

yritystä. Kriminalisoinneilla määritetään vahingolliset ja vaaralliset, yhteiskunnan puuttumista edellyttävät teot.

Esimerkiksi mietinnön tietoliikennetiedustelun toteuttamista koskevasta jaksosta 6.1.4 on pääteltävissä, että kyseinen tiedustelu olisi tiettyjen hakuehtojen perusteella tapahtuvaa seulontaa kaikesta tietoliikenteestä uhkien havaitsemiseksi. Mahdollista on, että tällaisella seulonnalla voisi myös löytyä tietoja, joilla on merkitystä rikosten estämisessä, paljastamisessa ja selvittämisessä. Mietinnön sivulta 64 kuitenkin ilmenee, että rajapinta tiedustelun ja torjuntatoimien välillä olisi järjestettävä (pohdittava) erikseen. Lisäksi samassa yhteydessä todetaan, että olisi pohdittava sitä, millä tavoin tieto jo tapahtuneesta rikoksesta voitaisiin antaa esitutkintaviranomaiselle.

Tiedustelulla saatavan tiedon hyödyntämisen kannalta on huomattava, että vuoden 2014 alusta voimaan tulleet pakkokeinolaki (806/2011) ja poliisilaki (872/2011) tarjoavat poliisille laajat toimivaltuudet esimerkiksi vakoi- ja terrorismirikosten estämiseen, paljastamiseen ja selvittämiseen. Tuossa yhteydessä kiinnitettiin huomiota myös tietoverkkojen kautta tehtäviin rikoksiin esimerkiksi säätämällä salaiseksi tiedonhankintakeinoksi tekninen laitetarkkailu.

Koska tiedusteluvaiheessa ollaan usein tilanteessa, jossa rikosta ei ole vielä tehty, merkityksellisiä ovat etenkin rikosten estämistä ja paljastamista koskevat poliisilain 5 luvussa säädetyt salaiset tiedonhankintakeinot. Sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa annetun lain (255/2014) 9 luvun säännösten mukaisesti puolustusvoimilla on rajatusti oikeus käyttää salaisia tiedonhankintakeinoja rikosten ennalta estämisessä ja paljastamisessa, mitä täydentää oikeus saada poliisilta virka-apua.

Liikenne- ja viestintäministeriön edustajan eriävässä mielipiteessä (sivu 117) kiinnitetään huomiota siihen, että työryhmä ei ole mietinnössään kattavasti arvioinut poliisilain ja pakkokeinolain salaisen tiedonhankinnan toimivaltuuksien käyttöä ja tehokkuutta sekä niiden riittävyttä tai riittämättömyyttä.

Samantapaisiin kysymyksiin kiinnittää huomiota poliisijohtaja Tomi Vuori lausumassaan. Hän toteaa (sivu 139) työryhmän työn kuluessa käyneen ilmeiseksi, että on yksityiskohtaisemmin selvitettävä, mihin poliisilain salaiset tiedonhankintakeinot tällä saralla riittävät ja mihin uusia tiedusteluvaltuuksia konkreettisesti tarvittaisiin.

Tältä osin on kuitenkin huomattava se, että mietinnössä tarkoitettu tiedustelu ilmeisesti aikajanalla pääsääntöisesti sijoittuisi salaisten tiedonhankintakeinojen käyttämistä edeltävään aikaan, jolloin tiedustelulla saadut tiedot saattaisivat olla hyödyllisiä kohdennettaessa salaisia tiedonhankintakeinoja tiedustelussa havaitussa konkreettisessa tapauksessa rikoksen estämiseen, paljastamiseen tai selvittämiseen. Kuten edellä jo todettiin, ja mihin myös Vuori viittaa, asiaa ei ole kuitenkaan arvioitu rikostorjunnan

kokonaisuutta silmällä pitäen. Vaikka kokonaisuus on sinällään tärkeä, asioita on myös analyyttisesti arvioitava erikseen vaihe vaiheelta.

Ylijohtaja



Asko Välimaa

Lainsäädäntöneuvos



Tuula Majuri

