Tietosuojavaltuutetun toimisto

Lausunto

02.06.2017 1408/03/2017

Asia: SMDno-2015-1509; SM047:00/2015

Ehdotus siviilitiedustelua koskevaksi lainsäädännöksi; työryhmän mietintö 8/2017

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

Sisäministeriölle

Lausunto mietinnöstä ”Siviilitiedustelulainsäädäntö”

SM047:00/2015

Esitän lausuntonani seuraavan.

Yleisiä huomioita

Siviilitiedustelulainsäädäntö liittyy oikeusministeriössä valmisteltavaan perustuslain 10 §:n muutokseen. OM:n työryhmämietinnön (41/2016) mukaan nykyisen perustuslain tulkintakäytännön valossa, ei ole mahdollista säätää perustuslain 10 §:n 3 momentin nojalla sellaisista rajoituksista viestin salaisuuteen, joiden tarkoituksena ei olisi yksilöidyn rikoksen torjuminen tai selvittäminen. Kun ehdotetut tiedustelumenetelmät eivät ole rikossidonnaisia siten kuin voimassa olevat poliisilain 5 luvun salaiset pakkokeinot, on sääntelyn edellytyksenä perustus-lain 10 §:n 3 momentin muuttaminen.

Henkilötietojen perustuslailliseen suojaan ei ehdoteta muutosta, mutta henkilötietojen suojan kysymyksiä ei voida sivuuttaa tässä hankkeessa, vaikka ensisijaisesti ehdotetuilla toimenpiteillä kajotaan luottamuksellisen viestin salaisuuteen. Ensinnäkin vaikka tiedustelulla saatava infor-maatio ei ole kaikilta osin henkilötietoa eikä ole kyse tietyn henkilöityvän rikoksen tutkinnasta tai ennalta estämisestä voidaan katsoa, että tietoliikennetiedostelulla pyritään ja väistämättä joudutaan käsittelemään myös henkilötietoja, oli ne sitten tiettyä henkilöä koskevia välitystie-toja tai viestien sisällöistä ilmeneviä henkilötietoja. Tietoverkoista saatava informaatio ei ole vain perinteisiä

henkilöä kuvaavia tai häneen liitettyjä tietoja vaan yhä enemmän tietoa henki-lön ”toiminnasta” tietoverkossa ja sen välityksellä ja tällaisen toiminnan seurauksista, jotka voivat ilmetä tietoverkossa ja siihen kytketyissä tietojärjestelmissä ja päätelaitteissa sekä ns. reaalimaailmassa. Toinen henkilötietojen suojaan liittyvä näkökulma on se, että viime kädessä tietoliikennetiedustelulla saadun datan analysoinnilla hankitun henkilötiedon käsittelyä koske-van sääntelyn perusteella voitaisiin osaltaan vahvistaa sellaisia henkilötiedon elinkaaren koh-tia, joissa muun muassa virheellisen tiedon riskit ja hankitun tiedon käytön seuraukset olisivat paremmin hallittavissa ja siten myös ennakoitavissa.

Vaikka kansallisen turvallisuuden kysymykset eivät kuulu unionin toimivaltaan eikä EU:n yleistä tietosuoja-asetusta (2016/679) tai tietosuojadirektiiviä (2016/680) sovelletakaan, edustavat säännökset viimeisimpiä kansainvälisiä säännöksiä henkilötietojen suojan alalla. Kumpikin inst-rumentti perustuu kuuteen tietosuojaperiaatteeseen, joita voi pitää koko henkilötietojen suo-jan oikeudellisen sääntelyn systematisoivana perusteena ja joilla pyritään kattamaan henkilö-tietojen käsittelyn elinkaari tietojen hankinnasta, jalostamisesta, käytöstä sekä niiden suojauk-sesta hävittämiseen saakka. Periaatepohjainen sääntely ei ole kansainvälisesti kovin uutta sillä niin EU:n tietosuojadirektiivi vuodelta 1995 ja Euroopan neuvoston tietosuojasopimus (nro 108/1981) perustuvat kumpikin saman tyyppisiin tietosuojaperiaatteisiin. Toinen ehkä merkit-tävämpi muutos liittyy siihen, että henkilötietojen käsittelyyn liittyviä riskejä ei tulisi arvioida vain suhteessa yksityiselämän suojaan vaan yleisemmin suhteessa perusoikeuksiin ja – vapauk-siin. Tämän mukaan henkilötietojen suoja voi liittyä yksityiselämän suojaan, mutta myös mui-hin perusoikeuksiin ja -vapauksiin kuten kiellettyyn syrjintään tai sananvapauteen.

Myöskään EU:n perusoikeuskirjan 8 artikla, jossa säädetään kansallista perusoikeutta yksityis-kohtaisemmin henkilötietojen suojan perusoikeuden sisällöstä, ei tule sellaisenaan sovelletta-vaksi SEU 4.2 ja SEUT 16.2 artikloiden perusteella. Sen sijaan Euroopan ihmisoikeussopimus (EIS) tulee Suomea sitovana kansainvälisenä velvoitteena ottaa huomioon. OM:n työryhmä-mietinnön liitteenä on Jukka Viljasen selvitys EIT:n oikeuskäytännöstä perustuslain 10 §:n kan-nalta relevanteissa tilanteissa. Kuten selvityksestä ilmenee nykyaikaisten tiedonhankintakei-nojen arvioinnin kannalta keskeiset valitukset ovat vireillä EIT:ssä. Näitä ovat muun muassa Big Brother Watch ja muut v. Yhdistynyt Kuningaskunta (58170/13), 10 ihmisoikeusorganisaatiota ja muut v. Yhdistynyt Kuningaskunta (24960/15).

Vireillä näyttäisi edelleenkin olevan Ruotsin signaalitiedustelua koskeva hakemus Centrum För Rättvisa v. Sweden (35252/08), jonka käsittelyssä näkyy tällaisen tuomioistuinkontrollin haas-teet, kun hakijalla ei ole juurikaan mahdollisuuksia saa tietoa salaisista ja salassa pidettävistä tiedonhankintakeinoista ja niiden yksityiskohdista tai edes sitä onko niitä kohdistettu häneen vai ei. Tähän haasteeseen EIT on vastannut tapauksessa Kennedy v. Yhdistynyt Kuningaskunta hyväksymällä hakemuksen, joka perustui hakijan esittämiin epäilyksiin päätyen arvioimaan ta-pausta sääntelyn ja erityisten suojaustoimien perusteella yleisesti siten, että mahdollista tie-donhankintaa viestinnästä saatettiin pitää oikeutettuna suhteessa EIS:n 8 artiklaan eli yksityis-elämän suojaan.

Tietoliikennedatan talteen otto, analysointi ja henkilötiedon elinkaari

Seuraavassa pyrin tarkastelemaan yksityiskohtaisemmin työryhmän lakiehdotusta tietoliikennetiedustelusta siviilitiedustelussa. Henkilötietojen suojaan ja käsittelyyn liittyviä kysymyksiä on perusteltua käsitellä henkilötiedon elinkaarimallin mukaan lähtien laillisesta hankinnasta ja käsittelystä päätyen niiden hävittämiseen.

Lakiehdotuksen mukaan tietoliikennetiedustelu siviilitiedustelutarkoituksissa käynnistyisi siten, että suojelupoliisi pyytäisi ehdotuksen 7 §:n mukaisen tuomioistuimen luvan perusteella tai 9 §:n mukaisessa kiireellisessä menettelyssä päättäisi itse pyytää puolustusvoimien tiedustelulai-tokselta yksilöidyn viestintäverkon osan läpi kulkevan ”tietoliikennevirran peilaamista kulke-maan myös tiedustelujärjestelmän kautta”. Tähän ns. tiedustelujärjestelmään peilattua tieto-liikennettä verrattaisiin ehdotuksen 4 §:ssä tarkoitetuilla hakuehdoilla, jotka perustuvat ehdo-tuksen 7 ja 9 §:ien mukaiseen lupaan tai päätökseen. Ehdotuksen 10 §:n 3 momentin mukaan suojelupoliisi toimittaa luvan tai päätöksen puolustusvoimien tiedustelulaitokselle, joka suorit-taisi 4 §:ssä tarkoitetut toimet suojelupoliisin puolesta. Tällainen toimeksiantosuhde tarkoit-taa tavallisesti sitä, että toimeksisaajan oikeus ryhtyä käsittelemään tarkoituksena hankkia myös henkilötietoja tulee johtaa toimeksiantajan oikeuksista. Ehdotuksesta puuttuu selkeä säännös, jossa suojelupoliisi oikeutetaan siviilitiedustelussa peilaamaan tai ottamaan talteen kohteeksi valitun viestintäverkon osa läpi kulkeva tietoliikennedata sen erottelemiseksi ehdo-tuksen 4 §:n mukaan. Mielestäni 4 §:n tarkoittama erottelu ei ole mahdollista ”lennossa” vaan tietoliikennetiedustelun liityntäpisteessä on otettava tietoliikennedata talteen, jotta siihen voitaisiin kohdistaa 4 §:ssä tarkoitettuja hakuja ja erityisesti toimittaa mahdolliset hakutulokset suojelupoliisille. Kun erottelun kohteena olevaa aineistoa ei ehdoteta rajattavaksi (esim. 7 §:n 2 momentin 5 kohta), on erottelun kohteena kaikki kyseisen viestintäverkon osan kautta kulke-va tietoliikennedata.

Ehdotuksen 4 §:n mukaisella erottelulla pyritään kohdistamaan tietoliikennetiedustelua. Näiltä osin olennaista on se, mitä hakuehtoja käytetään. Yleisesti ottaen voitaneen todeta, että mitä yleisempiä hakuehdot ovat, sitä enemmän löytyy hakuehtoja täyttäviä tuloksia, jotka päätyvät tarkempaa 5 §:ssä tarkoitettuun jatkokäsittelyyn. Ehdotuksen 4 §:n 2 momentin mukaan vies-tin sisältöä koskevaa hakuehtoa ei saisi käyttää ja 3 momentin mukaan hakuehtona ei saisi käyttää Suomessa olevan henkilön hallussa olevan telepäätelaitteen tai teleosoitteen yksilöiviä tietoja. Tällaiset sisällölliset hakuehtoja koskevat rajoitukset olisivat omintakeinen suomalai-nen ratkaisu, joka näyttäisi kuitenkin toimivan kohdistamistarkoitusta vastaan ja kannustaisi pikemminkin yleisempien hakuehtojen kehittämiseen ja tietoliikennedatan laajempaan pääty-miseen ehdotuksen 5 §:n mukaiseen jatkokäsittelyyn. Mikäli siviilitiedusteluviranomaisella olisi yksilöiviä tietoja olisi kyse enemmänkin ehdotuksen 6 §:n 2 momentissa säädetystä välttämät-tömyysarvioinnista eli tietoliikennetiedustelu olisi viime kätinen tiedonhankintakeino esimerkiksi suhteessa ehdotetun poliisilain 5 a luvussa säädetyille tiedustelumenetelmille.

Ehdotuksen 5 §:n perusteella suojelupoliisi saisi oikeuden käsitellä edellä mainitun erottelun perusteella sille toimittua aineistoa automaattisesti ja manuaalisesti. Automatisoidulla käsitte-lyllä pyritään edelleen kohdentamaan tiedonhankintaa siten, että voitaisiin supistaa manuaali-sen käsittelyn kohteeksi tulevan tiedon määrää. Näiltä osin rajoitukset eivät koske luottamuk-sellisen

viestinnän sisältöä tai muita luottamuksellisia tietoja vaan ehdotuksen 12 §:n mukaisia rajoituksia, joiden mukaan tietoliikennetiedustelua ei saa kohdistaa viestiin, jonka lähettäjä ja vastaanottaja ovat viestinnän tapahtuessa Suomessa (ks. 15 §:n 1 momentin 1 kohta). Tällai-sen tosiseikan eli sen, että niin lähettäjä kuin vastaanottaja ovat Suomessa viestinnän tapahtu-essa, ei selviä hetkellisen tietoliikennedataotoksen perusteella esim. sähköpostityyppisissä viestintäpalveluissa, koska viestien lähettäminen ja vastaanottaminen eivät tapahdu samanai-kaisesti tai aina samasta paikasta. Lisäksi yleisimmin käytössä olevien sähköpostipalvelujen (hotmail ja gmail) palvelimet ovat muualla kuin Suomessa ja siten tällainen liikenne ohittaa tietoliikennetiedustelun liityntäpisteen, jolloin on todennäköistä, että tällaista aineistoa myös kertyy. Todistamiskieltoa koskevien seikkojen selvittäminen edellyttäisi vielä yksityiskohtaisem-paa tutkintaa, joka ei todennäköisesti onnistu automaattisesti ja tällöin ei voida puhua enää vain tietoliikennetiedustelun kohdentamisesta vaan siitä, että on hankittu muun muassa henki-lötietoja, joihin ei ole käsittelyoikeutta. Tällaiset tapaukset tulisi ehdotuksen 13 ja 14 §:ien mukaisesti tutkia ja tarkastaa ja viranpuolesta hävittää ehdotuksen 15 §:n nojalla.

Ehdotuksen 15 §:ssä säädetään hankitun tiedon hävittämisestä, jossa yksilöllisiä poistokritee-reitä edustavat edellä mainitut ehdotuksen 12 §:ssä tarkoitetut tiedustelukieltoa koskevat sei-kat. Näiden osalta kyse on siitä, miten paljon tiedusteluviranomaisen tulisi näitä poistoperus-teita tutkia, koska salaisen tiedonhankinnan osalta henkilöllä itsellään ei ole mahdollisuuksia esittää näistä poistoperusteista selvitystä. Yleisenä poistokriteerinä on tiedustelutarkoituksiin viittaava kriteeri eli tietoa ei enää tarvita kansallisen turvallisuuden suojaamiseksi. Ehdotuksen 15 §:n 2 momentin mukaan tietoa, jota ei enää tarvita tiedustelutarkoituksessa ja olisi siten tämän pääsäännön mukaan hävitettävä, voitaisiin luovuttaa rikostorjuntaan ehdotetun poliisi-lain 5 a luvun 43 §:n edellytyksin. Tästä avautuu tiedustelutiedon toissijaiselle käytölle sana-muodon perusteella erityinen käyttötarkoitus eli rikostorjunta, mikä viittaisi poliisilain 5 a lu-vun 43 §:n 1 momenttiin (rikostorjunta) eikä niinkään 2 momenttiin (selvittäminen) vaikka 43 §:n otsikkona on rikostorjunta. Se, saako tiedustelutietoa luovuttaa myös rikosten selvittämi-seen, tulisi selventää jatkovalmistelussa. Kun tällaisia rajoituksia arvioidaan tulisi muun ohella ottaa huomioon se, että rikosprosessi voi tuottaa EIS:n 6 artiklan oikeudenmukaisen oikeuden-käynnin periaatteiden perusteella tiedonhankintakeinoista sellaista asianosaisjulkisuutta, joita ehdotuksen 18 §:n asianosaisjulkisuuden rajoittamisella ja 20 §:n käytöstä ilmoittamisella ei saavuteta. Lisäksi rikosprosessi johtaa tuomioistuimen arviointiin hankitusta tiedosta ja viime kädessä tuomioon, jossa EIS:n 6 artiklan 2 kohdan syyttömyysolettama tulee vahvistetuksi tai kumotuksi.

Toinen toissijaisen käytön mahdollisuus avautuu ehdotuksen 15 §:n 3 momentin viittauksesta ehdotetun poliisilain 5 a luvun 44 §:n 2 momenttiin. Säännöksessä ei puhuta ”tiedustelumene-telmän aikana ilmenneestä rikosepäilystä” toisin kuin poliisilain 5 a luvun 43 §:ssä vaan oikeu-tetaan ehdotuksen 15 §:n 1 momentin 3 kohdan mukaan hävitettävän tiedon säilyttäminen ja tallentaminen poliisin rekisterilaissa (PoreL 761/2004) tarkoitettuun rekisteriin. Käyttötarkoi-tuksina olisivat rikoslain 15 luvun 10 §:ssä tarkoitettujen rikosten estäminen tai syyttömyyttä tukeva selvitys. Kun PoreL:n säännöstä ei ole yksilöity jää säännöksen perusteella epäselväksi tällä perusteella edelleenkin säilytettävien henkilötietojen käyttötarkoitus. Kun lopullinen säi-lyttämisaika on kuitenkin määritelty suhteessa asian lainvoimaiseen ratkaisuun tai sillensä jät-tämiseen, voi säilyttämisaika venyä suhteettoman pitkäksi, jos ei ole takeita siitä, että tämän tyyppisen tiedon perusteella ryhdytään esitutkintatoimenpiteisiin.

Kolmas vanhanajan rekisterisäännös ilmenee ehdotuksen 1 §:n 3 momentista, joka viittaa Po-reL:iin, jota ollaan parhaillaan muuttamassa tai uusimassa ennen kaikkea EU:n tietosuojadirek-tiivin (2016/680) perusteella. Näiltä osin PoreL:iin ehdotetaan sanallista täsmennystä siitä, että suojelupoliisin toiminnalliseen tietojärjestelmään voi sisältää tietoja, jotka on hankittu tietolii-kennetiedustelulla. Ehdotuksessa ei ole otettu esille tätä kautta avautuvia henkilötietojen jatkokäsittelytilanteita, joista yhtenä merkittävimpänä voidaan pitää henkilöturvallisuusselvi-tyksiä turvallisuusselvityslain (726/2014) perusteella. Turvallisuusselvityslain 25 §:n 1 momentin 4 kohdan mukaan selvitys voi perustua muun muassa suojelupoliisin toiminnalliseen tietojär-jestelmään, jolloin myös tietoverkkotiedustelulla hankittu tieto voi tulla käytettäväksi, jollei turvallisuusselvityslain 32 §:n käyttörajoitukset tule sovellettavaksi. Tällaiset vaikutukset tulisi tarkemmin arvioida ottaen erityisesti huomioon se, ettei henkilöturvallisuusselvityksen koh-teena olevalla henkilöllä ole juurikaan keinoja saada tietää tiedustelutiedon keräämisestä, joll-ei tietoliikennetiedustelun käytöstä ole ehdotuksen 20 §:n perusteella erityisesti ilmoitettu.

Tietoliikennetiedustelulla saadun henkilötietojen käsittelyn avoimuus suhteessa tiedonkohteeseen on asianosaisjulkisuussäännösten ja tarkastusoikeuden osalta suljettu pois ehdotuksen 18 §:n mukaan. Toisin kuin poliisilain 5 luvun salaisissa pakkokeinoissa, tiedustelutieto ei tulisi myöskään rikosprosessin kautta asianosaisen tietoon ja tuomioistuimen arvioitavaksi, jollei sitä toissijaisesti käytetä rikosten torjuntaan tai selvittämiseen. Ehdotuksen 20 §:n mukainen tieto-liikennetiedustelun käytöstä ilmoittaminen tulee kyseeseen vain silloin kun Suomessa olevan henkilön luottamuksellisen viestin tai tallentaman tiedon sisältö on manuaalisesti selvitetty. Pelkästään automatisoitua käsittelyä ilmoitusvelvollisuus ei koskisi, mikä voi kannustaa pelkäs-tään tällaisten keinojen käyttöön ja kehittämiseen jopa henkilötietojen täsmällisyyden ja virheettömyyden kustannuksella.

Toinen tietoliikennetiedustelun avoimuuteen liittyvä kysymys on se, että tietoliikennetiedustelun edellytyksenä on ehdotuksen 6 §:n mukaan se, että sen avulla ”voidaan olettaa” saatavan tietoja kansallista turvallisuutta vakavasti uhkaavasta toiminnasta ja tietoliikennetiedustelun ”voidaan olettaa” olevan välttämätön keino tällaisen tiedon saamiseksi. Se, osoittautuvatko nämä oletukset oikeiksi, selviää käyttökokemuksien kautta. Jotta tällainen uusi ja massiivinen tiedonhankinta täyttäisi sille asetetut yhteiskunnan perustellut turvallisuusodotukset, tulisi tällaisten odotusten täyttymisestä kyetä myöskin kertomaan ja ainakin pyrkiä riippumattomasti varmistamaan se, että tällaiset ns. tuloksellisuusodotukset täyttyvät riittävissä määrin eikä kyse ole perusteettomasta puuttumisesta yksilön perusoikeuksiin ja -vapauksiin.

Tietosuojavaltuutettu Reijo Aarnio

Ylitarkastaja Heikki Partanen

Partanen Heikki
Tietosuojavaltuutetun toimisto