

Lausunto

16.06.2017

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

Ehdotus siviilitiedustelua koskevaksi lainsäädännöksi; työryhmän mietintö 8/2017

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

Lausunto siviilitiedustelulainsäädäntöön

1. Yleistä

Tiedustelutiedon hankkimisen ja käyttämisen pelisäännöt ovat nousseet kansainväliseen keskusteluun kesän 2013 jälkeen ja kiihtyneet uusien tiedustelutapausten julkitulon myötä sekä myös turvallisuusympäristön muutosten myötä. SIY ry pitää kannatettavana, että oikeusvaltion periaatteita noudattaen luodaan myös Suomeen lakiin perustuva sääntely tiedustelusta, sen oikeutuksesta yleensä, sekä toimijoiden oikeuksista ja velvoitteista.

Siviilitiedustelulakityöryhmän mietintö ja lakiehdotuksen perustelut ovat osittain epätarkkoja ja jopa harhaanjohtavia. Ryhmässä ei ollut edustettuna varsinaisia tietoliikenne- ja internet –toimialan asiantuntijoita joita olisi ollut käytettävissä koko valmistelun ajan. Lainvalmistelun laatu ei välttämättä näin vastaa sitä tasoa jota voisi odottaa perusoikeuksia ja viranomaisten salassa pidettävää toimintaa käsittelevässä ehdotuksessa. Vastuun ja vallan tasapaino on jäänyt epäsuhtaiseksi ja pitkälti ehdotetun uuden valvontaelimen varaan (tiedusteluvaltuutettu).

Tuomioistuimen kyky arvioida tiedustelutoiminnan oikeasuhtaisuutta, tarpeellisuutta ja lainmukaisuutta tulee olemaan koetuksella mikäli lakiehdotuksen laatua ei kohenneta. Tuomioistuimen tulisi lainmukaisuuden lisäksi kyetä arvioimaan onko pyydetty toimi perusteltu ja tehokas sekä riittävän tarkkarajainen ettei perusoikeuksia loukattaisi tarpeettomasti. Tehtävä on haasteellinen vaatien sekä juridisen osaamisen laista että ymmärryksen tietoverkkojen ja

järjestelmien rakenteesta. Harkinta sen suhteen onko sovellettavissa muita tiedonhankintakeinoja vaatii jo kokemusta teleyritys tai yhdysliikennetoiminnasta tai ulkopuolista asiantuntijaosaamista.

Tiedonhankinta tietoliikenteestä, sekä tiedon tallennus, vaatii laitteistoja ja ohjelmia toteutukseen. Näiden laitteiden ja ohjelmistojen turvallisuutta Suomi ei kykene varmuudella varmistamaan mikäli niitä ei alisteta kansallisen tieto-turvasertifioinnin alaiseksi. Laissa tulisi edellyttää tiedusteluun käytettäviltä laitteistoilta ja ohjelmistoilta sellaista turvatasoa jotka VAHTI –ohjeet ja suositukset asettavat yleisesti henkilötietojen ja salassa pidettävien tietojen käytölle, tallennukselle ja hävittämiselle.

2. SIY ry:n keskeiset huomiot ja viestit

Poliisilaki

Muutokset poliisilakiin ja eräisiin muihin lakeihin ovat pitkälti teknisiä ja liittyvät Suojelupoliisin tehtävien ja oikeuksien tarkempaan rinnastamiseen esitutkintaviranomaisiin. Lakiehdotuksissa ei ole säädetty rajoituksista salaukseen, salausavaimiin tai ohjelmistojen tai laitteiden ns. takaporteista jota voidaan pitää hyvänä linjauksena. Salauksen tai luottamuksen murtaminen tai purkaminen olisi tuhoisaa modernille digitaaliselle yhteiskunnalle ja uhkaksi myös yritystoimintaa vakavasti.

Ehdotetut muutokset ovat sinänsä mittavia mutta keskeisten uusien oikeuksien osalta tuomioistuinkäsittelyn alaisia ja määräaikaista joka ohjaa harkittuun oikeuksien soveltamiseen. SIY ry pitää hyvänä, että toiminnan valvontaan on kiinnitetty erityistä huomiota lakiehdotuksen muodossa tiedusteluvaltuutetun toimesta kantelu-oikeuksineen.

Poliisilain 15 §:n mukaan suojelupoliisille tulisi oikeus sijoittaa ja poistaa tekniseen tarkkailuun käytettävälaite, menetelmä tai ohjelmisto tietojärjestelmään menemällä salaa kohteeseen kaipa tarkennusta. Lain perusteissa tulisi määritellä miltä tahoilta toimenpide voidaan salata jotta tuomioistuin kykenee arvioimaan luvan perusteet. Salaa tietojärjestelmään asetettu ohjelmisto sisältää aina riskin järjestelmän toiminnalle ja on omiaan heikentämään sen turvallisuutta. Toimenpidelupa-anomuksen tulisi sisältää analyysi mitä vahinkoa tarkkailuohjelma voi aiheuttaa tietojärjestelmälle tai sen ohjaamalle prosessille, sekä myös uskottava kuvaus miten ohjelmisto poistetaan vaaraa aiheuttamatta. Tietojärjestelmän toimimattomuus tällaisen toimenpiteen seurauksena voi johtaa tilanteeseen jossa keskeisiä yhteiskunnan palveluita keskeytyy, esimerkiksi lentoliikenne tai keskeinen elintarvike- tai energiantuotanto.

Oikeuteen asettaa valvontaohjelmistoja tietojärjestelmiin tulisi asettaa myös korvausvelvollisuus vahingon varalta. Asiattomien ohjelmistojen poisto ja turvallisuusjärjestelmien tarkistus aiheuttavat kustannuksia ja liiketoiminnan haittaa. Olisi kohtuutonta edellyttää, että näiden aiheuttaja ei olisi korvausvelvollinen johtuen virka-asemastaan.

Poliisilaki §16 ja §22 Peitetoimintaa sekä tietolähteen ohjattua käyttöä koskevat esitykset ja suunnitelmat tulisivat sisältää myös peitetoiminnan tai tietolähteen ohjatun käytön purkamisen suunnitelman. Tietoverkossa toteutettava peitetoiminta tai ohjattu käyttö voi vaarantaa tietoverkon asiallisen käytön tai kriittisen viestinnän ja siksi sen lopettamiseen tai purkamiseen pitäisi olla velvoite sekä tosiasiallinen mahdollisuus.

Poliisilaki §52 tietojen käytöstä tulisi olla tarkkarajaisempi. Tietojen käyttö tulisi liittää Suojelupoliisin tehtävien toteuttamiseen ja tietojen luovutuksesta oltava erillinen sääntely. Kansainvälistä käyttöä (§54) ei ole rajattu viranomaisiin tai yleensäkkään vieraan valtion lukuun toimiviin tahoihin joten niitä voitaisiin käyttää myös tietojen tai hyödykkeiden ostamiseen rikollisista tai vihamielisistä lähteistä. Kansainvälisen käytön ja luovuttamisen voisi tarkemmin rajata tai asettaa luvanvaraiseksi (valvontaviranomainen).

3. Laki tietoliikennetiedustelusta siviilitiedustelussa

Lakiehdotuksessa rajataan tiedustelu Suomen rajat ylittävään tietoliikenteeseen ja perusteluissa todetaan, että Internetin luonteesta johtuen Suomen sisäinen liikenne voi sattumanvaraisesti kiertää ulkomaisen viestintäverkon kautta. Tosiasiallisesti osa Suomen sisäisestä liikenteestä välittyy ulkomaisten viestintäverkkojen kautta pääasiallisesti ja jatkuvasti. Perustelu on tosiasiallisesti virheellinen väittäjä ja se tulisi korjata.

Verkkoliikenteen ml. sähköpostit välitetään valtaosin salattuna. Mietinnössä useasti mainittu tuloksellisuus ja tuloksellisuusodotus ovat siten lähtökohtaisesti erittäin huonoja koska kykyä salauksen murtamiseen ei liene olemassa. [Viite salauksen yleisyyteen: "A forecast that 70% of global Internet traffic will be encrypted in 2016, with many networks exceeding 80%" (<https://www.sandvine.com/trends/encryption.html>)].

Mietinnössä mainitut muut tunnistetiedot ovat niin ikään kyseenalaisia, koska mitään järkevää tunnistetietoa ei ole saatavissa edes Facebookin, Googlen, TOR:n tai VPN-palveluiden tapauksissa.

Lakiehdotuksessa tietoliikennetiedustelusta siviilitiedustelussa ei riittävän tarkkarajaisesti määritellä tiedustelun kohdentamisesta, ainoastaan seikasta että toiminnan tulee kohdistua Suomen rajat ylittävään liikenteeseen. Määrittelyn epätarkkuus on omiaan rinnastamaan toiminnan massatiedusteluun jonka kansainvälinen standardointijärjestö IETF on dokumentissään RFC7258 määrittellyt, ja yhteisö hyväksynyt, tekniseksi hyökkäykseksi yksityisyyttä vastaan (<https://tools.ietf.org/html/rfc7258>).

Jotta riittävä tarkkarajaisuus saavutettaisiin tulisi laissa määritellä, että luvassa jolla tiedusteluoikeutta haetaan tulee määritellä yhteysväli tai -välit josta tiedustelu toteutetaan. Valvontaviranomaiselle jäisi valvontavelvollisuus ja harkinta siitä täyttääkö haettu ja saatu lupa

massavalvonnan tunnusmerkit vai voidaanko sitä perustellusti pitää riittävän kohdennettuna siihen uhkaan joka lupa-anomuksessa on kuvattu.

Mellin Jorma
Suomen Internet-yhdistys, SIY ry