|  |  |  |
| --- | --- | --- |
|  | **Lausunto** |  |
|  |  |  |
| Tieto-osasto / Turvallisuusyksikkö |  | LVM/1936/02/2016 |
| Maija Rönkä | 13.1.2016 |  |
|  |  |  |
|  |
|  |
|  |
|  |
|  |

Luottamuksellisen viestin salaisuus – perustuslakisääntelyn tarkistaminen

Oikeusministeriö on antanut 11.10.2016 mietinnön perustuslakisääntelyn tarkistamisesta koskien luottamuksellisen viestin salaisuutta. Mietintö liittyy laajempaan sotilas- ja siviilitiedustelua sekä tiedustelun viranomaisvalvontaa koskevien lakien valmistelun kokonaisuuteen. Liikenne- ja viestintäministeriö on nimennyt oikeusministeriön perustuslakityöryhmän lisäksi pysyvät asiantuntijat puolustusministeriön sekä sisäministeriön työryhmiin.

Liikenne- ja viestintäministeriö on tiedustelulainsäädäntöä valmisteltaessa pitänyt tärkeänä, että lainsäädännön valmistelun yhteydessä tarkasteltaisiin erilaisia vaihtoehtoisia keinoja, joilla viranomaisille voitaisiin turvata sellaiset tehokkaat ja oikeasuhtaiset toimivaltuudet lakisääteisten tehtäviensä suorittamiseen, joista aiheutuisi kuitenkin mahdollisimman vähän haittaa suhteessa tavoiteltavaan päämäärään.

Perustuslain 10 §:n mukaan luottamuksellisen viestin salaisuuden suoja on loukkaamaton. Pykälään sisältyy lakivaraus, jonka oikeuttaa viranomaisen rajoittamaan suojaa vain perustuslaissa määritellyillä edellytyksillä. Oikeusministeriön työryhmä ehdottaa, että perustuslain 10 §:n kvalifioitua lakivarausta muutettaisiin siten, että

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

**Liikenne- ja viestintäministeriö on antanut asiantuntijanäkemyksensä työryhmälle. Ministeriö on kiinnittänyt valmistelussa huomion seuraaviin seikkoihin:**

Perustuslain 10 §:ssä turvattu luottamuksellisen viestin salaisuuden suoja on yksi keskeinen yksityiselämän suojan osa. Luottamuksellisen viestin salaisuuden suojan merkitys kasvaa yhä merkittävämmäksi tekijäksi jokaisen yksityiselämän suojan toteutumisen kannalta, kun lähes kaikki kansalaisten ja yritysten käyttämistä arkisista palveluista digitalisoituvat ja kun valtaosa palveluiden toteuttamisesta perustuu sähköisessä muodossa olevan tiedon välittämiseen tieto- ja viestintäverkoissa – internetissä.

Perustuslain esitöiden mukaan yksityiselämän suojan lähtökohtana on, että yksilöllä on oikeus elää omaa elämäänsä ilman viranomaisten tai muiden ulkopuolisten tahojen mielivaltaista tai aiheetonta puuttumista hänen yksityiselämäänsä (HE 309/1993 vp). Perustuslain 22 §:n nojalla julkisen vallan on turvattava perus- ja ihmisoikeuksien toteutuminen. Perustuslain 10 §:n säännös edellyttääkin yhdessä 22 §:n kanssa lainsäädäntöä, joka käytännössä tehokkaasti turvaa luottamuksellista viestintää sekä viranomaisten että muiden ulkopuolisten loukkauksilta (HE 309/1993 vp). Mietinnön mukaan perusoikeussuoja koskee luonnollisten henkilöiden lisäksi välillisesti myös oikeushenkilöitä eli esimerkiksi Suomessa toimivia yrityksiä.

Tietoyhteiskuntakaaressa on säädetty keskeisistä oikeuksista ja velvollisuuksista, joilla turvataan yksityiselämän ja luottamuksellisen viestin salaisuuden suojan toteutuminen sähköisissä viestintäverkoissa ja viestintäpalveluissa. Eduskunta on tietoyhteiskuntakaaren säätämisen yhteydessä antanut lausuman, jonka mukaan palvelujen käyttäjien oikeuksien, kuten yksityisyyden suojan ja luottamuksellisen viestin suojan säilymisestä sähköisissä palveluissa ja verkkoympäristössä huolehditaan kaikin keinoin ja mm. kyberturvallisuuden kehittämistyössä pyritään erityisesti ottamaan näiden oikeuksien toteutuminen huomioon (EV 106/2013 vp – HE 221/2013 vp).

Edellä sanottujen tavoitteiden toteutuminen edellyttäisi, että viranomaisten tiedusteluvaltuuksien tulisi olla tehokkaita tavoiteltavaan päämäärään nähden eikä niistä tulisi aiheutua tarpeetonta vahinkoa sivullisille henkilöille taikka Suomessa toimiville yrityksille.

Tiedusteluvaltuuksien tehokkuutta, välttämättömyyttä ja oikeasuhtaisuutta arvioitaessa olennaisinta on se, miten tiedusteluvaltuuksien käyttö kohdennetaan ja keiden viestinnän luottamuksellisuutta viranomaisten voidaan antaa lain nojalla rajoittaa. **Liikenne- ja viestintäministeriö katsoo, että olennaista on ratkaista se, kohdennetaanko tiedustelutoimintaa vain tiettyjen kohdehenkilöiden (esim. sotilasorganisaatiot tai rikoksia tekevät ja valmistelevat tahot) harjoittamaan viestintään vai kaikkeen jossakin tietyssä viestintäverkossa kulkevaan tietoliikenteeseen. Kohdentamattomat valtuudet rajoittaisivat suomalaisten perusoikeussuojaa huomattavasti laajemmalla tavalla kuin yksinomaan kohdehenkilöiden viestintään kohdennetut tiedusteluvaltuudet. Oikeus puuttua tiedustelutoiminnassa sivullisten henkilöiden luottamukselliseen viestintään olisi omiaan heikentämään ihmisten edellytyksiä luottaa viranomaisiin sekä Suomessa digitaalista liiketoimintaa harjoittaviin yrityksiin ja niiden palveluihin.**

**Tiedustelutoiminnan kohdentaminen**

Kohdentamiskysymys on ratkaiseva myös sen suhteen, onko perustuslakia tarpeen muuttaa ja miten, jotta tiedusteluvaltuuksista voitaisiin säätää.

*Sotilaallinen toiminta*

Työryhmän mietinnössä todetaan, ettei ”*vieraan valtion sotilas- tai muun viranomaisorganisaation*

*viestintä ei nauti luottamuksellisen viestin salaisuuden suojaa, eikä pelkästään tällaisten organisaatioiden viesteihin kohdistuvista toimivaltuuksista säätäminen muodostuisi perustuslain 10 §:n 3 momentin kannalta ongelmalliseksi.”* Mietinnön mukaan ”*tiedustelutoimivaltuuksia ei kuitenkaan arvioida olevan mahdollista kohdistaa kaikissa tapauksissa niin täsmällisesti, ettei olisi vaaraa viranomaisten tilapäisestä pääsystä yksittäisten, tiedustelutehtävään liittymättömien henkilöiden viestintää koskeviin tietoihin.”*

Tiedustelutoiminnan luonteen kannalta lienee aina mahdollista, että viranomaisilla on vaara tilapäiseen pääsyyn tiedustelutehtävään liittymättömien henkilöiden viestintää koskeviin tietoihin. Tätä vaaraa ei kuitenkaan voida pitää perusteena oikeuttaa tiedustelua silloin, kun henkilöillä ei ole liityntää tiedustelutehtävään, vaan tämän vaaran vuoksi tiedustelua koskevaan kansalliseen lainsäädäntöön sisältyy esimerkiksi tiedustelun päättämistä sekä tiedustelulla saatujen tietojen hävittämistä koskevia säännöksiä.

Perustuslain tarjoama suoja ei ylety vieraan valtion sotilas- tai muun viranomaisorganisaation

viestintään. Yksityiskohtaisissa perusteluissa on todettu, että ehdotettu perustuslainmuutos kattaisi myös jatkuvan tiedonhankinnan esimerkiksi muiden maiden sotilaallisen suorituskyyn kehittymisestä. **Liikenne- ja viestintäministeriö katsoo, että mikäli tällaisesta toiminnasta hankittaisiin tietoa vieraan valtion sotilas- tai muun viranomaisorganisaation tai siihen liittyvästä viestinnästä, ei tällainen viestintä nykysääntelynkään valossa nauttisi perustuslain suojaa, eikä tarvetta tällöin perustuslain muutokselle olisi.**

*Kansallista turvallisuutta vakavasti vaarantava toiminta*

Työryhmän mietinnössä on esitetty, että viestinnän luottamuksellisuuden suojan rajoittamiseen oikeuttava *muu kansallista turvallisuutta vakavasti vaarantava toiminta* voi olla sellaista, joka konkretisoituessaan olisi rikos, mutta jota ei vielä voida pitää konkreettisena ja yksilöitynä rikosepäilynä. Samoin kyse voi mietinnön mukaan olla toiminnasta, joka ei ole Suomen lain mukaan rikos.

Työryhmän mietinnöstä ei käy ilmi keiden henkilöiden viestinnän luottamuksellisuutta näissä tapauksissa olisi oikeutettua rajoittaa. Mietinnössä tiedustelutoiminnan kohteena on aina toiminta, eikä kukaan yksilö, esimerkiksi toimintaa harjoittava henkilö. Viestinnän luottamuksellisuuden suoja kuitenkin turvaa yksilön oikeutta.

Mietinnöstä ei myöskään käy ilmi, tulisiko henkilön harjoittaman muun kuin rikollisen toiminnan olla erikseen lainsäädännössä määriteltyä tai jollain tavoin moitittavaa, jotta hänen viestinnän luottamuksellisuuttaan voitaisiin rajoittaa.

Työryhmän mietinnön perusteella ei ole selvää, voitaisiinko ehdotetun säännöksen nojalla tiedusteluviranomainen periaatteessa oikeuttaa rajoittamaan kenen hyvänsä viestinnän luottamuksellisuuden suojaa riippumatta siitä, onko tämä syyllistynyt mihinkään moitittavaan toimintaan - esimerkiksi rikoksen suunnitteluun tai valmisteluun taikka sotilaalliseen toimintaan. Mietinnöstä ei myöskään selviä millainen yhteys henkilöllä, jonka viestinnän luottamuksellisuuteen puututaan, on oltava kansallista turvallisuutta vakavasti vaarantavaan toimintaan.

Euroopan ihmisoikeusistuimen (EIT) oikeuskäytännössä tiedustelun kohdentaminen on noussut esille osana tiedustelutoiminnan välttämättömyyskriteerin tarkastelua. Kuten perusteluissa on todettu, Euroopan ihmisoikeustuomioistuin on oikeuskäytännössään katsonut, että tiedusteluviranomaisten on pystyttävä näyttämään, että tiedustelutoimet ovat välttämättömiä.

EIT on Unkarin poliisin salaisia tiedonhankintakeinoja koskevassa Szabo & Vissy v. Unkari -tapauksessa ehdottoman välttämättömyyden (”strict necessity”) -kriteerin osalta todennut, että tiedustelua valvovan elimen on pystyttävä tosiasiallisesti arvioimaan välttämättömyys-kriteerin toteutumista. Välttämättömyyskriteerin arviointiin sisältyy myös henkilön tai henkilöiden ryhmän liittyminen tiedustelun oikeuttavaan uhkaan:

… For the Court, the category is overly broad, because there is no requirement of any kind for the authorities to demonstrate the actual or presumed relation between the persons or range of persons “concerned” and the prevention of any terrorist threat – let alone in a manner enabling an analysis by the authoriser which would go to the question of strict necessity (Szabó And Vissy V. Hungary para 67)

…There is no legal safeguard requiring TEK to produce supportive materials or, in particular, a sufficient factual basis for the application of secret intelligence gathering measures which would enable the evaluation of necessity of the proposed measure and this on the basis of an individual suspicion regarding the target person (see Roman Zakharov, cited above, §§ 259 and 261). For the Court, only such information would allow the authorising authority to perform an appropriate proportionality test. (ibid. para 71)

Viranomaisten on siis pystyttävä perustelemaan tiedustelutoimien välttämättömyys ja oikeasuhtaisuus. Tähän sisältyy vaatimus osoittaa yhteys tiedustelutoimet oikeuttavan uhkan ja tiedustelun kohteena olevan henkilön tai henkilöiden ryhmän välillä. Vaatimus liittyi Szabo & Vissy -tapauksessa poliisin kohdennettuihin tiedonhankintakeinoihin. Luottamuksellisen viestin salaisuuteen puuttuvat tiedustelumenetelmät puuttuvat kuitenkin lopulta aina tiettyjen yksittäisten henkilöiden viestintään. Siksi tiedustelutoimen oikeuttavan uhkan ja tiedustelun kohteena olevan henkilön välinen yhteys on merkityksellinen.

Myös Euroopan unionin tuomioistuimen (EUT) hiljattaisessa teletietojen yleistä säilytysvelvollisuutta koskevassa ratkaisussa Tele2 Sverige ja Watson - (C-203/15 ja C-698/15) EUT on todennut, että viranomaisen pääsy kohdennetun tallennusvelvoitteen alaisiin tallennettuihin tietoihin tulee perustua joko rikosepäilyyn tai tietoihin, joihin pääsy voi tapauskohtaisen objektiivisen näytön perusteella olla tarpeellista esimerkiksi kansallista turvallisuutta vaarantavien tekojen estämiseksi.

--- In that regard, access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime (see, by analogy, ECtHR, 4 December 2015, *Zakharov v.* *Russia*, CE:ECHR:2015:1204JUD004714306, § 260). However, in particular situations, where for example vital national security, defence or public security interests are threatened by terrorist activities, access to the data of other persons might also be granted where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating such activities. (Tele2 Sverige ja Watson para 119)

On myös hyvä huomioida, että perustuslain 10.3 §:n nykyiset rajoitusperusteet rajoittavat huomattavasti suppeammaksi sitä joukkoa, johon tiedustelutoiminta voi kohdistua. Rikosten tutkinta, oikeudenkäynti, turvallisuustarkastus, sekä vapaudenmenetys kohdistuvat kaikki hyvinkin rajattuun ihmisjoukkoon.

Periaatteessa sotilaallinen toiminta ja kansallista turvallisuutta vaarantava toiminta voisivat mahdollisesti rajata ihmisjoukkoa suhteellisen tarkasti silloin, kun tällaiselle toiminnalle on asetettu tiettyjä konkreettisuuden kriteereitä. Nyt yksityiskohtaisissa perusteluissa on päädyttä vastakohtaiseen ratkaisuun ja niiden mukaan:

”*Perustuslain 10 §:n 4 momentissa käytettäväksi ehdotettu ilmaisu ”uhkaa” laajentaa säännöksen soveltamisalaa tilanteisiin, joissa kansallinen turvallisuus ei välittömästi ole vaarantumassa. Näin ollen säännöksessä tarkoitettu tiedonhankinta voisi koskea myös toimintaa, joka jatkuessaan saattaisi vaarantaa kansallista turvallisuutta. Tiedon hankintaa ei ole rajoitettu ajallisesti, sillä kansallista turvallisuutta vakavasti uhkaavaa toimintaa on usein tarpeen seurata pitkäjänteisesti ja systemaattisesti.”*

On helppo ymmärtää, että toiminta, joka jatkuessaan saattaisi vaarantaa kansallista turvallisuutta, voisi periaatteessa tarkoittaa lähes millaista toimintaa tahansa, vaikka tämä ei ole luonnollisestikaan ollut esityksen tarkoitus. Kuitenkin esityksen valossa näyttäisi siltä, että viranomainen voitaisiin säännöksen nojalla oikeuttaa rajoittamaan lähes rajoittamattoman joukon viestinnän luottamuksellisuutta, jos se on välttämätöntä tiedon hankkimiseksi muusta kansallista turvallisuutta uhkaavasta toiminnasta. Tiedon tarpeellisuus voi työryhmän mietinnön mukaan liittyä esimerkiksi tilannekuvan tuottamiseen poliittiselle päätöksentekijälle.

Vaikka perusoikeuksien yleiset rajoittamisedellytykset vaikuttavat kaventavasti mahdollisuuksiin säätää tiedustelutoimivaltuuksista tavallisen lain tasolla, myös perustuslain perusteluilla voi olla merkittävä vaikutus perustuslain tulkintaan jatkossa.

Työryhmän mietinnön mukaan

”*tiedustelutoimivaltuuksia ei kuitenkaan arvioida olevan mahdollista kohdistaa kaikissa tapauksissa niin täsmällisesti, ettei olisi vaaraa viranomaisten tilapäisestä pääsystä yksittäisten, tiedustelutehtävään liittymättömien henkilöiden viestintää koskeviin tietoihin*.”

Kuten edellä on mainittu, tiedustelutoiminnan luonteen kannalta lienee aina mahdollista, että viranomaisilla on vaara tilapäiseen pääsyyn tiedustelutehtävään liittymättömien henkilöiden viestintää koskeviin tietoihin. On kuitenkin tärkeää arvioida kuinka todennäköistä tämä on ja kuinka suureen joukkoon sivullisia tiedustelu voi kohdistua.

Nykyiset poliisilain-, pakkokeinolain ja sotilaskurinpitolain mukaiset salaiset telepakkokeinot mahdollistavat tiedonhankinnan hyvinkin kohdennetusti. Oikeusministeriön mietinnössä ei suoraan oteta kantaa siihen, perustuuko perustuslain säännöksen muuttamisen tarve siihen, ettei viranomaisille voida nykyisen perustuslain nojalla säätää oikeutta puuttua tiedustelutehtävään liittymättömien henkilöiden viestintään. Mietinnöstä ei myöskään ilmene, miten suureen sivullisten henkilöiden joukkoon tiedusteluviranomaisille voitaisiin sallia pääsy ehdotetun perustuslain säännöksen nojalla tai mitä tarkoitettaisiin tilapäisellä pääsyllä sivullisten henkilöiden viestintään.

**Liikenne- ja viestintäministeriö toteaa, ettei perustuslain muutoksella tulisi mahdollistaa kaiken tietoliikenteen seulontaa eikä viranomaisen pääsyä sellaisten henkilöiden luottamukselliseen viestintään, joilla ei ole yhteyttä sotilaalliseen toimintaan, vakavaan rikokseen tai jotka eivät muutenkaan ole tiedustelutehtävän kohdehenkilöitä. Liikenne- ja viestintäministeriö pitää tärkeänä selvittää vaihtoehtoisena, tehokkaampana ja oikeasuhtaisempana tiedustelutoimivaltuuksien mallina myös sitä, että poliisi-, pakkokeino- ja puolustusvoimien rikostorjuntalain mukaisten salaisten pakkokeinojen aineellista tai alueellista soveltamisalaa laajennettaisiin nykyisestään. Käytännössä telepakkokeinoja voitaisiin käyttää nykyistä useampien rikostunnusmerkistöjen perusteella epäiltyihin henkilöihin tai toisaalta sellaisiin henkilöihin tai organisaatioihin, joita ei epäillä rikoksesta, mutta jotka eivät nauti myöskään perustuslain suojaa. Tiedustelu voitaisiin tällöin kohdentaa tuomioistuimen antamalla luvalla vain tiettyjen määriteltyjen kohdehenkilöiden ja heidän hallussaan olevien liittymien tai laitteiden viestintään.**

**Tällainen vaihtoehtoinen malli vastaisi nykyistä vakavien rikosten torjunnassa omaksuttua salaisten tiedonhankintavaltuuksien kohdentamista rikosepäiltyihin tuomioistuimen luvalla. Viranomaisella ei olisi teknistä pääsyä kaikkeen viestiliikenteeseen eikä siten sellaisten ulkopuolisten henkilöiden luottamukselliseen viestintään, jotka eivät valmistele rikoksia, jotka eivät harjoita sotilaallista toimintaa tai jotka eivät muutenkaan ole tiedustelun kohdehenkilöitä.**

**EU-oikeuden ja EU:n perusoikeuksien soveltuminen**

Työryhmän mietinnössä on erittäin ansiokkaasti kuvattu EU-oikeuden sisältöä yksityiselämän suojan alueella. Työryhmän mietinnön antamisen jälkeen EU-tuomioistuin on antanut ratkaisun tapauksessa Tele2 Sverige ja Watson - (C-203/15 ja C-698/15), joka on merkityksellinen myös yksityiselämän suojan sekä EU-oikeuden soveltumisen kannalta ja joka tulisi huomioida myös esityksen jatkovalmistelussa.

Anne Berner

Liikenne- ja viestintäministeri

Laura Vilkkonen

Osastopäällikkö, ylijohtaja