

Lausunto

13.01.2017

Asia: OM 27/41/2015

Mietintö ”Luottamuksellisen viestin salaisuus”

Lausunto

Lausuntonne mietinnöstä ”Luottamuksellisen viestin salaisuus”

Tietosuojavaltuutetun toimisto

Dnro 3248/03/2016

13.1.2017

Oikeusministeriölle

Lausunto mietinnöstä ”Luottamuksellisen viestin salaisuus”

OM 27/41/2015

Esitän lausuntonani seuraavan.

Työryhmä esittää perustuslain 10 §:n 3 momentin muutosta ja uutta 4 momenttia, joiden perusteella voitaisiin tavallisessa lainsäätämisyjärjestyksessä rajoittaa luottamuksellisen viestin salaisuuden suoja. Keskeiset muutokset liittyvät siihen, että nykyisinkin yksilöityjä oikeushyviä (yksilön tai yhteiskunnan turvallisuus tai kotirauha) vaarantavien rikosten - ei vain tutkinnassa vaan jo torjuntavaiheessa olisi mahdollista murtaa luottamuksellisen viestinnän salaisuus siten kuin siitä laissa tarkemmin säädetään. Lisäksi uutena rajoitusperusteena olisi tiedon hankkiminen sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Muulla toiminnalla tarkoitetaan perustelujen mukaan valtiojärjestystä tai yhteiskunnan perustoimintoja uhkaavaa toimintaa kuten terrorismiin liittyvää toimintaa tai väkivaltaista radikalisoitumista taikka ulkomaisten tiedustelupalvelujen toimintaa.

Perusoikeuskirjaus vastaamaan sen tulkintaa

Mietinnön mukaan rikosten tutkinnan muuttaminen rikoksen torjunnaksi vastaa säännöksen sanamuodon tulkinnan muutosta, joka tapahtui perustuslakivaliokunnan myötävaikutuksella jo varsin pian perusoikeusuudistuksen jälkeen. Tässä mielessä muutoksella saatetaan perusoikeus ja sen rajoittamisperusteet vastaamaan jo pitkä aikaista tulkintakäytäntöä, jolloin perusoikeuskirjaus perustuslaissa vastaisi sen tulkintaa, mitä voidaan pitää jo sellaisenaan perusteltuna oikeusinformatiivisista syistä.

Niihin oikeushyviin, joita vaarantavien rikosten torjuntaan varten voitaisiin säätää keinoista, joilla puututaan luottamuksen viestinnän salaisuuteen, ei ehdoteta muutosta. Perusoikeusuudistuksen esitöissä (HE 309/1993 vp) yksilön tai yhteiskunnan turvallisuutta vaarantavia rikoksia olisivat esimerkiksi huumausainerikokset, törkeät väkivaltarikokset sekä maan- ja valtiopetosrikokset. Lisäksi voimassaolevassa ja ehdotetussa säännöksessä mainitaan erityisesti kotirauha suojattavana oikeushyvinä - ei sen takia, että kyse olisi törkeästä rikoksesta tai sen tekemuodosta vaan sen takia, että rikos tehdään viestintävälinettä hyödyntämällä. Perusoikeusuudistuksen aikoihin kyse oli puhelimitse tehdyistä häirintäsoitoista ja niiden tekijän selvittämisestä. Nykyisin tämä rikostunnusmerkistö tunnetaan paikkariippumattomana viestintärauhan rikkomisena (879/2013) eikä niinkään kotirauhan rikkomisena. Näiltä osin olisi mielestäni yleisemminkin arvioitava, olisiko tällainen rajaus (tiedyt törkeät rikokset ja häirintäsoitot) päivitettävissä siten, että se vastaisi paremmin erityisesti pakkokeinolain 10 luvun telekuuntelun ja -valvonnan kriteereitä, joissa on laajemmin tunnistettu tarve saada tietoja nimenomaan viestintävälineiden avulla tietoverkossa tehdyistä tai siellä tapahtuvista rikoksista.

Sääntelyn välineriippumattomuus ja -riippuvuus

Perusoikeussuojan välineriippumattomuus on hyvä lainsäädännöllinen lähtökohta, mutta se voi aiheuttaa vaikeuksia soveltamisessa, kun lainsäädännölliset käsitteet ja ratkaisut ovat kehittyneet tietyssä teknisessä ympäristössä ja ympäristö, jossa perusoikeuksien tulisi toteutua, muuttuu olennaisesti. Perusoikeusuudistuksen aikaan 1990-luvun alussa puhelinverkot oli saatu digitalisoitua, mikä tarkoitti muun muassa sitä, että sykäysperusteisesta laskutuksesta voitiin siirtyä viestintätapahtumasta kerättyihin tietoihin eli tunnistamistietoihin perustuvaan laskutukseen. Perustuslakivaliokunta omaksui tuolloin tulkinnan, jonka mukaan tunnistamistiedot kuuluvat viestintäsalaisuuden suojan piiriin, mutta ne eivät ole perusoikeuden ydinaluetta, jonka muodosti viestinnän sisällön suoja. Erottelu tunnistetietoihin ja sisältöihin oli siinä mielessä helppo, että ns. piirikytkentäistä puhelua ei tallennettu, ellei taltiointia oltu erikseen järjestetty ja teleoperaattoreille jäi puhelutapahtumasta vain nämä tunnistetiedot, joita ensisijaisesti käytettiin laskutukseen. Tietoverkossa viestintä ei perustu em. piirikytkentäiseen yhteyteen vaan pakettikytkentäiseen datan siirtoon tcp/ip -protokollan perusteella. Kyseessä on yleinen datan siirtoon perustuva protokolla, jota ei voi pitää kategorisesti luottamuksellisen viestinnän välineenä vaan dataa siirretään milloin missäkin tarkoituksessa ja vasta sovellustasolla voidaan jotain päätellä datan siirron tarkoituksesta (kuten SMTP, VoIP). Olennaisena erona voidaan pitää myös sitä, että tunnistetiedot (ns. header-tiedot) ja viestin sisällöt siirretään samassa paketissa ja tallennetaan siirron eri vaiheissa sellaisenaan, jollei niitä ole erikseen salattu. Toinen olennainen piirre nimenomaan sähköpostien osalta on se, että ne lähetetään tai vastaanotetaan sekä usein säilytetään palvelimelle, jonka henkilökohtaiseen osaan tulisi olla pääsy vain kyseisellä viestinnän osapuolella. Se, mikä myös poikkeaa perinteisestä puhelinverkosta, on se, etteivät yksittäiset viestintätapahtumat ole laskutusperusteita, jolloin teleyrityksillä ei ole sellaista omista tarpeista johtuvaa käsittelyperustetta

kuin aikaisemmin. Tämän voi nähdä keskeisenä perusteena sille, että EU antoi ns. data retention -direktiivin (2006/24/EY), joka sittemmin EUT:n tuomiolla (Digital Rights Ireland C-293/2012) todettiin pätemättömäksi.

Perustuslakivaliokunta on tarkastellut kyseistä EUT:n tuomiota todeten muun muassa, että se antaa perusteita arvioida uudelleen perustuslakivakiokunnan vakiintunutta tulkintaa, jonka mukaan viestin tunnistamistietojen on katsottu jäävän luottamuksellisen viestin salaisuutta suojaavan perusoikeuden ydinalueen ulkopuolelle (PeVL 18/2014 vp). Vaikka tunnistetiedot jäävät ydinalueen ulkopuolelle, on niiden perustuslaillista suojaa pidetty lähtökohtaisesti henkilötietojen suojaa vahvempana ja siten EUT:n tuomio näyttäisi johtavan ainakin siihen, että yksityiselämän suojan perusoikeuksien kesken joudutaan tilannekohtaisemmin punnitsemaan tunnistamistietojen ja henkilötietojen suojan suhdetta yksityiselämän suojan kannalta.

Tiedonhankinta yhtenä henkilötietojen käsittelyn ja suojan osana

Se, mikä myös näyttäisi kyseisen EUT:n tuomion ja perustuslakivaliokunnan lausunnon osalta ilmeiseltä liittyä siihen, että ottaen huomioon viestintään kohdistuvat tiedonhankinnan tarkoitukset joudutaan ennen pitkään tai jo alusta alkaen (kun tarkoituksena on tunnistaa tietty henkilö) arvioimaan toimintaa henkilötietojen suojan perusoikeuden näkökulmasta. Vaikka kansallisesti henkilötietojen suoja on sellaisenaan vakiointunut tietyksi laissa säädettävien käsittelytoimien luetteloksi, on usein myös kyse siitä, ettei henkilötietojen suoja redusoidu pelkäksi henkilötiedon suojaksi vaan henkilötietojen käsittely voi viime kädessä liittyä muiden perusoikeuksien suojaan, jolloin henkilötietojen käsittelyyn liittyviä riskejä tulisi arvioida perusoikeusjärjestelmän kokonaisuuden kannalta. Vaikka EU:n tietosuoja-asetusta (2016/679) tai tietosuojadirektiiviä (2016/680) ei sellaisenaan sovelleta, kun on kyse kansallisesta turvallisuudesta, antaa asetuksen periaatepohjainen sääntelymalli mahdollisuuden kehittää ns. riskiperusteista lähestymistapaa, joka ottaisi paremmin huomioon tilannesidonnaiset riskit ja jonka perusteella vaadittavat suojaustoimenpiteet voitaisiin suhteuttaa näihin riskeihin. Tällaisessa yhteydessä yhtenä riskinä voidaan pitää henkilön tunnistamiseen liittyviä virheitä, jotka voivat johtaa huomattaviin seurauksiin ei niinkään henkilötietojen suojan (virheellinen tieto) vaan muiden perusoikeuksien (vapaus, omaisuus) osalta. Kun tällaisessa henkilötietojen käsittelyssä joudutaan ottamaan riskejä, on kyse siitä, minkälaista riskinottoa voidaan pitää oikeutettuna kussakin tarkoituksessa.

Sotilaallinen toiminta ja muu toiminta sekä tiedonhankinnan kohdistaminen

Työryhmän ehdottaa uusia rajoitusperusteita luottamuksellisen viestinnän salaisuuden suojaan. Näitä olisivat tiedonhankinta sotilaallisesta toiminnasta ja sellaisesta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Kun tässä tarkoitetaan vieraan valtion sotilaallista toimintaa, on ilmeistä, ettei luottamuksellisen viestinnän salaisuuden suoja voi ulottua vieraaseen valtioon, kun kyse on ensisijaisesti luonnollisten henkilöiden perusoikeuksista. Tämä mietinnössä selkeästi todetaankin (s. 42), mutta rajoitusperusteeksi sotilaallista toimintaa ehdotetaan siitä syystä, ettei tiedustelutoimivaltuuksia arvioida olevan mahdollista kohdistaa niin täsmällisesti, ettei olisi vaaraa viranomaisten tilapäisestä pääsystä yksittäisten, tiedustelutehtävään liittymättömien henkilöiden

viestintää koskeviin tietoihin. Tämän perusteella työryhmällä näyttäisi olevan jonkinlainen käsitys tai epäily siitä, ettei tiedonhankintaa voida tarkasti kohdistaa, mutta kyse olisi kuitenkin vain tilapäisesti tiedustelutehtäviin liittymättömistä henkilöistä. Tämän näkemyksen arviointi jää tehtäväksi varsinaisen lainsäädäntöesityksen perusteella, missä toivon mukaan avataan riittävästi tiedonhankinnan yksityiskohtia.

Kansallista turvallisuutta vakavasti uhkaavan muun toiminnan tekijöinä ja tiedonhankinnan kohteina voisivat olla luonnolliset henkilöt tai heidän ryhmänsä, kun on kyse terrorismiin liittyvästä toiminnasta tai väkivaltaisesta radikalisoitumisesta tai ulkomaisten tiedustelupalvelujen toiminnasta. Viimeksi mainitusta uhasta työryhmä katsoo perustellusti, ettei vieraan valtion viranomaisorganisaation viestintä nauti luottamuksellisen viestinnän salaisuuden suojaa. Terrorismiin liittyvä toiminta ja väkivaltainen radikalisoituminen voisivat olla konkretisoituessaan rikoksia, mutta niitä koskevia yksilöityä rikosepäilyä ei vielä ole. Se, ettei ole yksilöityä epäilyä rikoksen teon aikomuksista, on ilmeisesti kriteeri, joka erottaa tämän tiedonhankintaperusteen saman momentin alun tiedonhankinnasta rikosten torjunta tarkoituksissa. Kun kyse ei ole yksilöidyistä rikosepäilyistä, joudutaan näiltä osin arvioimaan sitä, miten tiedonhankintaa voidaan kohdistaa siten, että sitä voidaan pitää oikeasuhtaisena demokraattista yhteiskuntaa vakavasti uhkaavan toiminnan tunnistamiseksi ja torjumiseksi. Myös näiltä osin tiedonhankinnan kohdentaminen jää arvioitavaksi varsinaisen lainsäädäntöesityksen perusteella.

Tietosuojavaltuutettu

Reijo Aarnio

Ylitarkastaja

Heikki Partanen

Partanen Heikki
Tietosuojavaltuutetun toimisto