OIKEUSMINISTERIÖ **MUISTIO**
Lainvalmisteluosasto 9.6.2006
Anna-Riitta Wallin

TYÖMARKKINAOSAPUOLTEN EHDOTUS SÄHKÖISEN VIESTINNÄN TIETOSUOJALAIN 13 §:N MUUTTAMISESTA; EHDOTUKSEN OIKEUDELLISTA ARVIOINTIA

1. Ehdotus ja sen tausta

Tässä muistiossa tarkastellaan liikenne- ja viestintäministeriölle toimitettua työmarkkinaosapuolten[1] ehdotusta, joka koskee sähköisen viestinnän tietosuojalakiin (516/2004; jäljempänä tietosuojalaki) 13 §:ään otettavia säännöksiä yhteisötilaajan oikeudesta käsitellä viestinnän tunnistamistietoja tiettyjen rikosten paljastamiseksi ja selvittämiseksi.

Ehdotus on tullut esiin tietosuojalain osittaistarkistuksen loppuvaiheissa muutama viikko sitten ja se ei siten ollut mukana esitysluonnoksessa, joka on ollut lausuntokierroksella. Liikenne- ja viestintäministeriöstä saatujen tietojen mukaan hallituksen esitys on tarkoitus antaa 15.6.2006 ja ministeriön virkamiehet on ohjeistettu ottamaan työmarkkinaosapuolten laatima ehdotus annettavaan esitykseen.

Työmarkkinajärjestöjen esittämä ehdotus kuuluu:

> Yhteisötilaaja voi käsitellä tunnistamistietoja rikoslain 30 luvun 4-6 §:ssä tarkoitetun yritysvakoilun, yrityssalaisuuden rikkomisen ja yrityssalaisuuden väärinkäytön havaitsemiseksi, estämiseksi ja selvittämiseksi sekä esitutkintaan saattamiseksi, jos mainitut rikokset saattavat vahingoittaa yksityisen huomattavan arvokasta liike- tai ammattisalaisuutta tai muuta tähän rinnastettavaa erittäin merkittävää yksityistä taloudellista etua.
>
> Yhteisötilaajan tulee tehdä kirjallinen ilmoitus tietosuojavaltuutetulle ennen edellä 3 momentissa tarkoitetun tunnistamistietojen käsittelyn aloittamista. Ilmoituksessa tulee yksilöidä mahdollisimman tarkasti tunnistamistietojen käsittelyn tarkoitus ja käsittelyn tarkoituksen toteutumisen kannalta välttämättömät toimenpiteet. Lisäksi yhteisötilaajan on laadittava kirjallinen ohje, jossa määritellään ne perusteet, joiden nojalla tunnistamistietoja 3 momentin perusteella voidaan käsitellä.
>
> Tunnistamistietoja saavat käsitellä edellä 2 ja 3 momentissa mainituilla perusteilla vain ne yhteisötilaajan viestintäverkon ylläpidosta ja tietoturvasta sekä yhteisötilaajan turvallisuudesta huolehtivat henkilöt, joiden tehtäviin tunnistamistietojen käsittely asiallisesti ja perustellusti kuuluu. Yhteisötilaajan on nimettävä nämä henkilöt tai määriteltävä edellä mainitut tehtävät. Tunnistamistietoja käsittelevät henkilöt eivät saa ilmaista näitä tietoja sivulliselle.
>
> Jos yksittäisen käyttäjän tunnistamistietoja on käsitelty edellä 2 ja 3 momentissa mainituilla perusteilla ja jos käsittelyn perusteella on tarkoitus ryhtyä hänen oikeus-

[1] Tätä kirjoitettaessa Akava ei saatujen tietojen mukaan ole allekirjoittanut esitystä.

> asemaansa vaikuttaviin toimiin, tunnistamistietojen käsittelystä on tiedotettava hänelle heti, kun se voi tapahtua käsittelyn tarkoitusta vaarantamatta. Tunnistamistietojen käsittely ja ohje sekä niistä tiedottaminen kuuluvat työnantajan ja työntekijöiden välisen yhteistoiminnan ja tiedottamisen piiriin siten, kuin siitä säädetään yksityisyyden suojasta työelämässä annetun lain (759/2004) 21 §:ssä.
>
> Viestin ja tunnistamistietojen käsittelemisestä tietoturvasta huolehtimiseksi säädetään 5 luvussa.
>
> Viestintävirasto voi antaa tarkempia määräyksiä edellä 1 momentissa tarkoitetun tunnistamistietojen käsittelyn teknisestä toteuttamisesta.

Edellä oleva ehdotus on tiettävästi syntynyt työmarkkinaosapuolten välisissä neuvotteluissa, joissa paikalla ei ole ollut ketään lainvalmistelutehtävissä valtionhallinnossa toimivaa. Kysymys ei siten ole ns. kolmikantaisesta valmistelusta. Tämä myös näkyy ehdotuksesta.

Ehdotusta on myöhemmin täydennetty liikenne- ja viestintäministeriössä siten, että yhteisötilaajan oikeus tunnistetietojen käsittelyyn olisi sovellettavissa myös vakoilun, turvallisuussalaisuuden paljastamisen ja luvattoman tiedustelutoiminnan paljastamiseksi.

> Yhteisötilaaja voi käsitellä tunnistamistietoja rikoslain 12 luvun 5-9 §:ssä tarkoitetun vakoilun, turvallisuussalaisuuden paljastamisen ja luvattoman tiedustelutoiminnan sekä rikoslain 30 luvun 4-6 §:ssä tarkoitetun yritysvakoilun, yrityssalaisuuden rikkomisen ja yrityssalaisuuden väärinkäytön havaitsemiseksi, estämiseksi ja selvittämiseksi sekä esitutkintaan saattamiseksi, jos mainitut rikokset saattavat vahingoittaa Suomen sisäistä tai ulkoista turvallisuutta, maanpuolustusta tai poikkeusoloihin varautumista, Suomen suhteita toiseen valtioon tai kansainväliseen järjestöön, julkistaloutta taikka yksityisen huomattavan arvokasta liike- tai ammattisalaisuutta tai muuta tähän rinnastettavaa erittäin merkittävää yksityistä taloudellista etua.

Tässä muistiossa arvioidaan ehdotusta jälkimmäisen, laajennetun ehdotuksen pohjalta.[2] Tarkastelussa on päällekkäisyyksiä. Tämä on jotensakin väistämätön seuraus valitusta tarkastelutavasta: voimassa oleva lainsäädäntö osoittaa johdonmukaisuutta ja on kaikilta keskeisiltä osiltaan ollut perustuslakivaliokunnan arvioinnin kohteena. Toisaalta arvioinnin lopputulokset eri näkökulmista käsin osoittavat sen moniongelmaisiin säädösehdotuksiin säännönmukaisesti liittyvän seikan, että samat sääntelyehdotuksen puutteellisuudet nousevat esiin säännösehdotusta eri näkökulmista tarkasteltaessa.

2. Arvioinnin perusteet

Tehtyä ehdotusta on oikeudellisesti arvioitava useammasta eri näkökulmasta niin kuin lainvalmisteluhankkeita yleensäkin. Ehdotetun sääntelyn tulisi olla muuhun lainsäädäntöön sopeutuva siten, että oikeusjärjestys pysyy johdonmukaisena, ristiriidattoma-

[2] Jäljempänä ei siten arvioida tietosuojalain 13 §:n 1 momenttiin suunniteltua muutosta, johon siihenkin näyttäisi liittyvän ongelmia.

na ja selkeänä (*konsistenssi- ja koherenssivaatimus*). Sääntelyssä tulee ottaa huomioon asiaa koskeva yleislainsäädäntö ja järjestää ehdotetun sääntelyn suhteet muuhun lainsäädäntöön asianmukaisesti. Ehdotetun sääntelyn tulee olla sopusoinnussa Suomen perustuslain (731/1999) ja Suomea sitovien kansainvälisten velvoitteiden kanssa; ehdotetussa sääntelyssä tulisi siis ottaa huomioon *lainsäätäjän harkintamarginaalit.*

Ehdotetun sääntelyn varsin pintapuolinenkin tarkastelu tuo esiin monia ongelmia edellä olevien yleisten lainvalmistelua sitovien ja ohjaavien tekijöiden kannalta. Seuraavassa tarkastellaan niistä keskeisempiä.

3. Ehdotus ja lainsäädännön johdonmukaisuus

Seuraavassa kuvataan yksityiskohtaisemmin ehdotuksen sisältöä sekä konkretisoidaan sen merkitystä sekä selostetaan voimassa olevia poliisille säädettyjä oikeuksia tunnistamistietojen käsittelyssä. Luvun tarkoituksena on antaa mahdollisuudet suhteuttaa tehty ehdotus muuhun lainsäädäntöön sekä siinä omaksuttuihin ratkaisuihin sen arvioimiseksi, miten ehdotus täyttää oikeusjärjestyksen johdonmukaisuudelle asetetut vaatimukset.

3.1. Ehdotuksen sisällön konkretisointi

Ehdotus antaisi oikeuden sähköisen viestinnän *tunnistamistietojen* käsittelyyn. Tunnistamistiedolla tarkoitetaan tietosuojalaissa tilaajaan tai käyttäjään yhdistettävissä olevaa tietoa, jota viestintäverkoissa käsitellään viestien siirtämiseksi, jakelemiseksi tai tarjolla pitämiseksi. Tietoa viestin tai sen liitteen tallennusmuodosta (esim. mp3, .doc, .exe tai .pdf) on pidetty tunnistamistietona (HE 125/2003 vp). Tunnistamistiedoissa on siten kysymys tiedoista, joista ilmenee viestinnän osapuolet ja yhteyden tapahtuma-aika. Niiden käsittelyn käyttötarkoituksena on viestinnän toteuttaminen. Tunnistamistietojen käsittelyn rajoittaminen on keskeinen keino tietosuojan turvaamisessa sähköisessä viestinnässä (HE 125/2003 vp).

Oikeus koskisi tunnistamistietojen *käsittelyä,* jolla tietosuojalaissa tarkoitetaan keräämistä, tallentamista, järjestämistä, käyttöä, siirtämistä, luovuttamista, säilyttämistä, muuttamista, yhdistämistä, suojaamista, poistamista, tuhoamista sekä muita vastaavia toimenpiteitä. Käsite on laaja, ja oikeuttaisi muun ohella tietojen yhdistämiseen ja luovuttamiseen.[3] Ehdotus merkitsee *yhteisötilaajalle annettua oikeutta televalvontaan rinnastettavissa olevaan toimivaltaan, joka puuttuu perustuslain mukaiseen viestinnän luottamuksellisuuteen, yksityisyyden ja henkilötietojen suojaan.*

> Pakkokeinolain 5 a luvun 1 §:ssä (646/2003) ja poliisilain 28 §:ssä (525/2005) televalvonta on määritelty asiallisesti samansisältöisesti. Televalvonnalla tarkoitetaan salassa pidettävien tunnistamistietojen hankkimista televiesteistä, jotka on lähetetty yleiseen viestintäverkkoon tai siihen liitettyyn viestintä-

[3] Perustuslakivaliokunta on kiinnittänyt huomiota käsitteen ongelmallisuuteen perustuslain kannalta, ks. jäljempänä s. 10.

> verkkoon kytketystä teleliittymästä, teleosoitteesta tai telepäätelaitteesta taikka vastaanotettu tällaiseen teleliittymään, teleosoitteeseen tai telepäätelaitteeseen, sekä matkaviestimen sijaintitiedon hankkimista ja tällaisen teleliittymän tai telepäätelaitteen tilapäistä sulkemista.

Käsittelytoimiin olisi oikeutettu *yhteisötilaaja*, jolla tietosuojalaissa tarkoitetaan viestintäpalvelun tai lisäarvopalvelun tilaajana olevaa yritystä tai yhteisöä, joka käsittelee viestintäverkossaan käyttäjien luottamuksellisia viestejä, tunnistamistietoja tai paikkatietoja. Yhteisötilaaja on siis mikä tahansa yhteisö, jolla on yleiseen viestintäverkkoon liitetty sisäinen viestintäverkko, kuten yritys, virasto, sairaala, eduskunta, hotelli, valtioneuvosto tai oppilaitos. *Yhteisötilaaja on viestinnän osapuolten kannalta tarkasteltuna sivullinen* (HE 125/2003 vp).

Yhteisötilaajan käsitteestä johtuu, että ehdotetut säännökset eivät ilmeisesti ole sovellettavissa tietoihin, jotka syntyvät matkapuhelimen käytössä ilman yhteyttä sisäiseen verkkoon. [4]

Käsittelyyn olisivat oikeutetut ne yhteisötilaajan viestintäverkon ylläpidosta ja tietoturvasta sekä yhteisötilaajan turvallisuudesta huolehtivat henkilöt, joiden tehtäviin tunnistamistietojen käsittely asiallisesti ja perustellusti kuuluu.[5] Näillä kullakin, ts. *jokaisella yksinään, olisi kontrolloimaton oikeus tietojen käsittelyyn*. Kontrolloimattomuus johtuu siitä, että säännösehdotuksessa *ei ole mitään velvoitteita käsittelytoimien tallentamisesta*.

> Vertailun vuoksi on todettava, että tietosuojalain 15 §:ssä on säännökset teleyrityksen velvollisuudesta tallettaa tunnistamistietojen käsittelystä yksityiskohtaiset tapahtumatiedot. Tapahtumatiedoista on käytävä ilmi käsittelyn ajankohta, kesto ja käsittelijä. Tapahtumatiedot on säilytettävä kaksi vuotta niiden tallentamisesta.
>
> Huomiota voidaan kiinnittää myös yksityisyyden suojasta työelämässä annettuun lakiin, jonka mukaan työntekijälle lähetetyn työnantajalle tarkoitetun viestin esille hakemisesta ja avaamisesta on laadittava siihen osallistuneiden henkilöiden allekirjoittama selvitys, josta ilmenee, miksi viestiä on haettu, hakemisen ja avaamisen ajankohta ja sen suorittajat. Lain sanamuodon mukaan toimenpiteisiin on osallistuttava useamman henkilön.

Ehdotus johtaisi esim. siihen, että eduskunnan turvallisuuspäällikkö saisi käsitellä eduskunnan keskuksen kautta tapahtuvan viestinnän osapuolten tunnistamistietoja ja vastaavasti valtioneuvoston turvallisuuspäällikkö kaikkia valtioneuvoston sisäisen verkon kautta tapahtuvaa viestintää esim. turvallisuussalaisuuden rikkomisen paljastamiseksi ja ilman, että viestinnän seurannan laajuus ja siinä toteutetut menettelyt olisivat jälkeenpäin todennettavissa. Esimerkki osoittaa yhtä ulottuvuutta ehdotuksen vaikutuksista – tässä tapauksessa vaikutuksia poliittisen päätöksentekojärjestelmän kannalta.

---

[4] Tällä seikalla voi olla merkitystä arvioitaessa sääntelyn tehokkuutta ja sääntelyn välttämättömyyttä.

[5] Ehdotus merkitsisi näiltä osin ilmeisesti poikkeusta sähköisen viestinnän tietosuojadirektiivin 6 artiklasta. Direktiivistä tarkemmin s. 7.

Ehdotus oikeuttaisi viestinnän luottamuksellisuuden suojaa rajoittaviin käsittelytoimiin tiettyjen *rikosten havaitsemiseksi, estämiseksi ja selvittämiseksi sekä esitutkintaan saattamiseksi*. Säännöksessä sallittu käsittelyoikeus olisi siten hyvin laaja, koska se voisi koskea jo rikosten havaitsemista. Ehdotetun sääntelyn arvioinnin kannalta tärkeä havainto on, että ehdotuksessa *ei ole mitään muita edellytyksiä* (esim. edellytystä rikosepäilystä tai edellytystä käsittelyn kestolle) *tunnistamistietojen käsittelylle*.

Ehdotetuissa säännöksissä *ei ole määritelty, kenen viestintää koskevia tunnistamistietoja käsittelyoikeus koskisi*. Ehdotuksen tausta huomioon ottaen tarkoituksena on saattanut olla, että kysymys on työnantajan sisäisiin verkkoihin tallentuvista työntekijän viestintää koskevista tiedoista, mutta tämä ei lainkaan näy säännösehdotuksesta. Käsittelyoikeus kohdistuisi siten kaikkiin yhteisötilaajan yleiseen verkkoon liitetyn sisäisen verkon välityksellä tapahtuvaan viestintään.

3.2. Viranomaisen valtuudet ja niiden sääntely

Televalvonnan edellytyksistä säädetään pakkokeinolain 5 a luvussa 3 §:ssä (646/2003) sekä poliisilain 31 c §:ssä (525/2005). Poliisilain 32 b – 32 d ja 33 §:ssä säädetään erilaisista televalvonnan muista edellytyksistä ja siihen liittyvistä menettelyistä. Televalvonnan edellytykset on säädetty varsin tarkkarajaisesti toimintaan liittyvän perusoikeuskytkennän vuoksi.

Televalvonta voidaan pakkokeinolain 5 a luvun 3 §:n mukaan sallia, jos televalvonnalla saatavilla tiedoilla *voidaan olettaa olevan erittäin tärkeä merkitys rikoksen selvittämiselle*. Poliisilain mukaan televalvonta on sallittua rikoksen *estämiseksi tai paljastamiseksi*. Kummassakin tapauksessa on kysymys *yksilöidystä rikosepäilystä*.

Televalvonta voidaan pakkokeinolain mukaan *kohdistaa henkilöön, jota on syytä epäillä rikoksesta*. Poliisilain 28 §:n mukainen pääsääntö on, että televalvonnan piiriin tulevan henkilön voidaan hänen lausumiensa, uhkausten tai käyttäytymisen perusteella taikka muutoin *voidaan perustellusti olettaa syyllistyvän rikokseen.* Televalvonta voidaan voimassa olevan lainsäädännön mukaan kohdistaa *vain epäillyn henkilön hallussa olevaan liittymään* sekä, milloin kysymys on rikoksen selvittämisestä, asianomistajan suostumuksella myös asianomistajan teleliittymään.

Televalvontaan ei ole oikeutta minkä tahansa rikosepäilyn perusteella; säännöksissä edellytetään, että kysymys on rikoksesta, josta säädetty ankarin *rangaistus on vähintään neljä vuotta vankeutta.* Näiden tilanteiden lisäksi televalvontaa voidaan kohdistaa *tiettyihin laissa määriteltyjen rikosten* selvittämiseen (automaattiseen tietojenkäsittelyjärjestelmään kohdistunut rikos, joka on tehty telepäätelaitetta käyttäen, paritus, oikeudenkäytössä kuultavan uhkaaminen, laiton uhmaaminen, huumausainerikos) samoin kuin laissa mainittujen rikosten rangaistavasta yrityksestä tai terroristisessa tarkoituksessa tehtävän rikoksen valmistelusta. Näissä ei edellytetä, että edellä mainittu rangaistusasteikkovaatimus täyttyisi.

Tietojenkäsittelyjärjestelmiin kohdistuneista rikoksista mainittiin hallituksen esityksessä (HE 22/1994 vp) esimerkkeinä tietokoneen luvaton käyttö (rikoslain 28 luvun 7 §), yritysvakoilun (rikoslain 30 luvun 4 §) eräät muodot,[6] tietokonevahingonteko (rikoslain 35 luvun 1 §:n 2 mom.), eräät väärennyksen muodot (rikoslain 33 luvun 1 ja 6 §:n 1 mom.) ja tietokonepetos (rikoslain 36 luvun 1 §:n 2 mom.).

Pakkokeinolaissa ja poliisilaissa on säännökset erilaisista *oikeusturvatakeista ja televalvonnan valvonnasta*. Oikeuksien asianmukaista käyttöä ennakolta varmistaa se, että televalvonta on mahdollista pääsäännön mukaan *vain tuomioistuimen luvalla*. Pakkokeinolain 5 a luvun 5 §:n ja poliisilain 32 b ja d §:n mukaan kiireellisessä tapauksessa päällystöön kuuluva poliisimies voi päättää tilapäisesti televalvonnasta.

Televalvonta ei voi olla jatkuvaa. Televalvontaa koskeva lupa voidaan antaa kerrallaan enintään yhdeksi kuukaudeksi. Luvassa on määriteltävä toimenpiteen kohteena oleva teleliittymä, teleosoite tai telepäätelaite ja henkilöt. Televalvontaa koskeva lupa voidaan myöntää koskemaan myös päätöstä edeltänyttä tiettyä aikaa, joka voi olla kuukautta pidempi. Televalvonta on lopetettava, kun sen tarkoitus on saavutettu (pakkokeinolain 5 a luku 11 § 1 mom., poliisilain 32 b § 3 mom.).

Oikeusturvaa varmistavat myös *kirjaamisvelvoitteet sekä vastuusuhteiden määrittely*. Pakkokeinolain 5 a luvun 8 §:n mukaan televalvonnasta on laadittava pöytäkirja. Syntyneet tallenteet on pikaisesti tarkastettava ja niihin sisältyvien tietojen tutkimisesta on soveltuvin osin voimassa, mitä pakkokeinolain 4 luvun 8 §:ssä säädetään takavarikoidun yksityisen asiakirjan tutkimisesta (pakkokeinolaki 12 §, poliisilaki 32 b § 3 mom.). Luvassa ja päätöksessä on mainittava tutkinnanjohtaja, joka johtaa ja valvoo toimenpiteiden suorittamista ja vastaa siitä, että niiden yhteydessä noudatetaan, mitä laissa säädetään.

Sille, jonka viestintää on seurattu, on ilmoitettava tietyin rajoituksin jälkeenpäin tunnistamistietojen hankkimisesta.

3.3. Johtopäätöksiä ehdotuksesta lainsäädännön johdonmukaisuuden kannalta

Voimassa olevan oikeuden lähtökohtana on, että *rikosten ehkäisy ja selvittäminen puuttumalla toisen henkilön perustuslailla suojattuihin oikeuksiin kuuluu poliisin ja muiden esitutkintaviranomaisten toimivaltaan laissa varsin tarkasti määritellyin edellytyksin*. Yksityisellä taholla ei tällaista oikeutta lähtökohtaisesti ole. Jokaisella on toki oikeus suojautua sellaisia rikollisia tekoja vastaan, jotka kohdistuvat esimerkiksi yritykseen tai yhteisöön itseensä, kunhan se voi tapahtua puuttumatta toisen henkilön perustuslain turvaamiin oikeuksiin. Hätävarjelusäännökset sallivat tietyin laissa säädetyin edellytyksin puolustautumisen aloitettua tai välittömästi uhkaavaa oikeudetonta hyökkäystä vastaan puuttumalla hyökkääjän etuihin. Yksityisellä henkilöllä ja yhtei-

[6] Nykyinen lainsäädäntö näyttäisi mahdollistavan poliisin televalvonnan ainakin joissakin sellaisissa tilanteissa, joissa on kysymys on yrityksen kannalta arvokkaiden etujen suojaamisesta. Ehdotusta koskevassa käytettävissä olevassa aineistossa näitä tilanteita ei ole arvioitu. Tällä on merkitystä arvioitaessa ehdotetun sääntelyn välttämättömyyttä ja hyväksyttävyyttä (ks. tarkemmin s. 9 ss.).

söllä on myös oikeus ilmoittaa poliisille epäillyistä yhteisöön kohdistuneista rikoksista, jotta poliisi voisi ryhtyä selvittämään epäiltyä rikosta tarvittaessa käyttäen laissa tarkoin säädettyä toimivaltaansa puuttua toisen henkilön oikeuksiin.

Ehdotuksessa *yhteisötilaajalle ehdotetaan lähtökohtaisesti viranomaiselle kuuluvaa toimivaltaa puuttua toisen henkilön oikeuksiin rikoksen ehkäisemiseksi ja selvittämiseksi*. Tähän arviointiin ei oikeudellisesti vaikuta se, että tunnistamistiedot on saatavissa yhteisötilaajan verkosta, koska tunnistamistiedot tallentuvat viestinnän toteuttamiseksi. Tunnistamistietojen käyttötarkoituksena on sähköisen viestinnän tietosuojadirektiivin, henkilötietodirektiivin ja näitä vastaavien kansallisten säädösten mukaan ensisijaisesti viestinnän toteuttaminen.

Ehdotus merkitsisi peruslähtökohdiltaan *huomattavaa poikkeusta nykyiseen järjestelmään*, joka koskee viranomaisten ja yksityisten tahojen toimivaltaa ehkäistä, tutkia ja selvittää rikoksia.

Voimassa olevan lainsäädännön mukaan *poliisin ja esitutkintaviranomaisen* tunnistamistietojen käsittelyn oikeuden yleisenä edellytyksenä, että tunnistamistiedoilla voidaan olettaa olevan erittäin tärkeä merkitys rikoksen selvittämiselle tai että tunnistamistiedot palvelevat rikoksen estämisestä tai paljastamista. Kummassakin tapauksessa on kysymys *tietyn liittymän tunnistamistietojen käsittelystä yksilöidyn rikosepäilyn vuoksi*. *Ehdotuksen* mukaan kynnys televalvontaan olisi epätavallisen alhainen, oikeus käsittelyyn olisi jo ”rikosten paljastamiseksi”. *Tunnistamistietojen käsittely kohdistuisi kaikkeen viestintään ja viestinnän osapuoliin ilman konkreettista rikosepäilyä*. Tällaisenaan ehdotus merkitsee huomattavaa poikkeusta lainsäädännön johdonmukaisuudesta.

Poliisilla ja muilla esitutkintaviranomaisilla toimivalta tunnistamistietojen hakemiseen liittyy tietyn vakavasta rikoksesta epäillyn henkilön teleliittymään *tuomioistuimen luvalla.* Käsittelyyn oikeutettu olisi ehdotuksen mukaan mikä tahansa yhteisötilaaja ja riippumatta siitä, mikä hänen ja viestinnän osapuolen välinen oikeudellisen suhde olisi. Ehdotuksen mukaan tunnistamistietojen käsittelyn perustaksi ja sen aloittamiseksi riittäisi *yhteisötilaajan oma arvio* siitä, että joku yhteisötilaajan verkossa oleva saattaa välittää tietoa, joka vahingoittaa esim. yksityisen huomattavan arvokasta liike- tai ammattisalaisuutta tai muuta tähän rinnastettavaa erittäin merkittävää yksityistä taloudellista etua. Ehdotuksen mukainen toimivalta merkitsisi yhteisötilaajalle *avointa ja yleistä toimivaltaa seurata ja kontrolloida kaikkea viestintäverkon ja viestintäpalvelun tapahtumia*.

Asian käsittely työnantajan ja työntekijöiden välisessä yhteistoimintamenettelyssä ja tietosuojavaltuutetulle tehty ilmoitus ehdotuksen mukaisen laajan tunnistamistietojen käsittelyn aloittamisesta mahdollistaisi käsittelyn aloittamisen ja keskeytymättömän jatkamisen vailla velvollisuutta lopettaa tai tarkistaa tietojen laatua. Tietosuojavaltuutetulle tehtävälle ilmoitukselle ja tietosuojavaltuutetun valvonnalla ei kirjaamisvelvoitteen puuttumisen vuoksi olisi tosiasiallisia edellytyksiä. Käsittelyoikeuden käyttö ei olisi tosiasiallisesti asianmukaisen kontrollin piirissä. Ne, joiden viestintään tunnistamistietojen käsittely kohdistuu, eivät koskaan saisi tietää niistä konkreettisista tilanteista, joissa heidän viestintäänsä on seurattu, lukuun ottamatta sitä, jota kohtaan on

tarkoitus ryhtyä oikeustoimiin. *Ehdotus poikkeaa näiltä osin merkittävästi niistä ratkaisuista, joilla lainsäädännössä taattu oikeusturvaa tunnistamistietojen käsittelyssä.*

Kuten aikaisemmasta on käynyt ilmi, ehdotus poikkeaa myös työelämän tietosuojalaissa omaksutusta sääntelytavasta ja sen mukaisista menettelytavoista.

Ehdotus merkitsee, että

> *yhteisötilaajalle ehdotetaan radikaalisti uutta toimivaltaa televalvonnassa, joka ylittäisi tuntuvasti poliisin ja muiden esitutkintaviranomaisten toimivallan puuttua yksityisyyden suojaan ja viestinnän salaisuuteen rikoksen havaitsemiseksi, ehkäisemiseksi ja selvittämiseksi. Ehdotetut säännökset poikkeavat myös merkittävällä tavalla yksityisyyden suojasta työelämässä annetun lain sääntelyjärjestelmästä. Ilmeiseltä näyttää, että ehdotus ei täytä oikeusjärjestyksen johdonmukaisuudelle asetettuja vaatimuksia.*

4. Lainsäätäjän harkintamarginaalit

Ehdotettua sääntelyä ei ilmeisestikään ole tarkasteltu lainsäätäjän harkintamarginaalien kannalta. Ennen esityksen antamista olisikin välttämätöntä arvioida, onko ehdotus sopusoinnussa perustuslain ja Suomea sitovien kansainvälisten velvoitteiden kanssa. Tässä yhteydessä merkityksellisimpiä kansainvälisiä velvoitteita ovat EU:n *henkilötietodirektiivi* 95/46/EY, *sähköisen viestinnän tietosuojadirektiivi* 2002/58/EY sekä Euroopan *neuvoston tietosuojasuojasopimus* (yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä koskevan Euroopan neuvoston yleissopimus, SopS 36/1992).

4.1. Arviointi kansainvälisten velvoitteiden kannalta

Henkilötietodirektiivissä, sähköisen viestinnän tietosuojadirektiivissä sekä Euroopan neuvoston tietosuojasopimuksessa on rajoitettu kansallisen lainsäätäjän mahdollisuuksia poiketa sopimusvelvoitteista.

Sähköisen viestinnän tietosuojasopimuksen 5 artiklassa on määräykset viestinnän luottamuksellisuudesta, mikä kattaa myös tunnustamistietojen luottamuksellisuuden. Direktiivissä on erikseen säädetty tietyistä sallitusta tunnistamistietojen käsittelystä. Artiklan 5 määräyksistä voidaan muutoin poiketa vain direktiivin 15 artiklan osoittamissa tapauksissa.

Jäsenvaltiot voivat 15 artiklan mukaan toteuttaa lainsäädännöllisiä toimenpiteitä, joilla rajoitetaan mm. direktiivin 5 artiklassa säädettyjen oikeuksien ja velvollisuuksien soveltamisalaa, jos tällaiset rajoitukset ovat välttämättömiä, asianmukaisia ja oikeasuhteisia demokraattisen yhteiskunnan toimenpiteitä kansallisen turvallisuuden (valtion turvallisuus) sekä puolustuksen, yleisen turvallisuuden tai rikosten tai sähköisen viestintäjärjestelmän luvattoman käytön torjunnan, tutkinnan, selvittämisen ja syyteharkinnan varmistamiseksi direktiivin 95/46/EY 13 artiklan 1 kohdan mukaisesti. Kaikkien toimenpiteiden on oltava yhteisön oikeuden yleisten periaatteiden mukaisia, mu-

kaan lukien Euroopan unionista tehdyn sopimuksen 6 artiklan 1 ja 2 kohdassa tarkoitetut periaatteet.

Ehdotettu sääntely merkitsisi poikkeusta tarkoitussidonnaisuuden vaatimuksesta, josta on määräykset sekä henkilötietodirektiivissä että Euroopan neuvoston tietosuojasopimuksessa. Tarkoitussidonnaisuuden vaatimuksesta voidaan poiketa vain ao. instrumenttien osoittamissa tapauksissa. Henkilötietodirektiivin ja Euroopan neuvoston poikkeuksia ja rajoituksia koskeva artikla on sisällöltään pitkälti sähköisen viestinnän tietosuojadirektiiviä vastaava.

Kansainvälisistä velvoitteista johtuvat rajoitukset kansalliselle lainsäädännölle vastaavat kansallisia perusoikeuksien rajoittamista koskevia vaatimuksia, minkä vuoksi ehdotusta tarkastellaan lainsäätäjän harkintamarginaalien kannalta kaikilta osin yksityiskohtaisemmin seuraavassa jaksossa.

4.2. Arviointi perustuslain kannalta

Ehdotusta on arvioitava perustuslain 10 §:ssä säädetyn yksityiselämän suojan, henkilötietojen suojan ja viestinnän luottamuksellisuuden kannalta. Julkiselle vallalle perustuslain 22 §:ssä säädetty perus- ja ihmisoikeuksien turvaamisvelvollisuus koskee oikeuksien toteutumista myös yksityisten keskinäisissä suhteissa. Velvollisuus kohdistuu säännöksen esitöiden mukaan käytännössä lähinnä lainsäätäjään, jonka tehtävänä on täsmentää perustuslaissa yleisellä tasolla ilmaistuja perusoikeuksia niin, että niiden vaikutus ulottuu myös yksityisiin suhteisiin (HE 309/1993 vp, s. 75).

Perustuslain 10 §:n 2 momentin mukaan kirjeen, puhelun ja muun *luottamuksellisen viestin salaisuus on loukkaamaton*. Pykälän 3 momentin nojalla lailla voidaan säätää välttämättömistä rajoituksista viestin salaisuuteen muun muassa yksilön tai yhteiskunnan turvallisuutta vaarantavien rikosten tutkinnassa.

Viestin tunnistamistiedot jäävät perustuslakivaliokunnan lausuntokäytännön mukaan luottamuksellisen viestin salaisuutta koskevan perusoikeuden ydinalueen ulkopuolelle, Sääntelyn on kuitenkin *yksityiselämän ja henkilötietojen suojan* vuoksi muutoin täytettävä perusoikeuksien yleiset rajoitusedellytykset (PeVL 7/1997 vp, s. 2/I, PeVL 26/2001 vp, s. 3/II, PeVL 7/1997 vp).

Perustuslakivaliokunnan käytännössä korostuu lähtökohtana se, että kulloinkin tarkasteltavana olevaa säädösehdotusta arvioidaan kokonaisuutena perustuslain kannalta. Nyt käsiteltävänä olevan ehdotuksen vuoksi onkin aihetta kiinnittää huomiota siihen, että käsitellessään poliisin oikeutta tunnistamistietojen saamiseen, valiokunta antoi *arvioinnissaan erityistä merkitystä sille, että tunnistamistietojen saaminen vaatisi aina tuomioistuimen luvan ja asianomistajan suostumuksen.*

Perusoikeuksien yleiset rajoittamisedellytykset ovat muokkautuneet perustuslakivaliokunnan lausuntokäytännössä. Yleisiin rajoittamisedellytyksiin kuuluu se, että ***rajoitusperusteet ovat hyväksyttäviä ja painavan yhteiskunnallisen tarpeen vaatimia***. Hyväksyttävyyden arvioinnissa merkitystä voi olla esim. Euroopan ihmisoikeussopimuk-

sen määräyksillä. Rajoitukset eivät saa olla ristiriidassa Suomen kansainvälisten ihmisoikeusvelvoitteiden kanssa (PeVM 25/1994 vp, s. 5/I).

Rikoksen selvittäminen on perustuslakivaliokunnan käytännössä todettu hyväksyttäväksi ja painavaksi perusteeksi perusoikeuksien rajoittamiselle. Näissä tapauksissa on kuitenkin ollut kysymys *poliisin oikeudesta* saada tietoja mainittuja tarkoituksia varten. Myös kansainvälisissä säädöksissä todetaan rikosten selvittäminen perusteena oikeuksien rajoittamiselle. Näissäkin on kuitenkin kysymys julkisen vallan organisaation tehtävistä. Voidaan myös todeta, että valtion toimet rikosoikeuden alalla ovat sähköisen viestinnän tietosuojadirektiivin soveltamisalan ulkopuolella (1 artikla).

Perustuslakivaliokunnan käytännön mukaan perusoikeuksien rajoitusten tulee olla ***tarkkarajaisia ja riittävän täsmällisesti määriteltyjä*** (PeVM 25/1994 vp, s. 5/I). Tarkkarajaisuusvaatimuksen suhteen ehdotus on ongelmallinen useammassa eri suhteessa. Tarkoituksena on turvata yrityssalaisuuksien ja keskeisten yleisten etujen suoja. Ehdotetussa sääntelyssä ei, kuten edellä jo on todettu, aseteta mitään rajoituksia sille, minkälaiset yhteisötilaajat voivat tietoja käsitellä, millaisiin viestinnän osapuolten tunnistamistietoihin käsittelyoikeus kohdistuu, missä tilanteissa käsittelyoikeus on ja kuinka kauan käsittely voi jatkua. Siten kenenkä tahansa yhteisötilaajan palveluksessa tai palveltavana olevan (esim. hotelli) viestinnän yhteystiedot olisivat käsittelyoikeuden piirissä milloin tahansa ja vaikka jatkuvasti.

Ehdotuksen *tarkkarajaisuutta heikentää jo käytetty käsitteistö*: "käsittely" on määritelty hyvin laaja-alaiseksi. Valiokunta on henkilötietolain arvioinnin yhteydessä huomauttanut tällaisen käsitteen käyttöön perustuvan tekniikan "yleisesti heikentävän sääntelyn selkeyttä ja samalla myös vähentävän sääntelyn täsmällisyyttä, mikä ei ole merkityksetön seikka sääntelyn perusoikeuskytkennän vuoksi" (PeVL 25/1998 vp, s. 3/I).

Käsittelyyn oikeutettu olisi lisäksi mikä tahansa yhteisötilaaja ja riippumatta siitä, mikä hänen ja viestinnän osapuolen välinen oikeudellisen suhde olisi. Ehdotettujen säännösten tarkkarajaisuuteen ei näyttäisi kovin merkittävästi vaikuttavan tietosuojalain 8 §:n yleissäännös, jonka mukaan lain 9–14 §:ssä tarkoitettu käsittely on sallittua ainoastaan käsittelyn tarkoituksen vaatimassa laajuudessa ja sillä ei saa rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä. Tämä johtuu siitä jo aikaisemmin todetusta seikasta, että *kynnys olisi epätavallisen alhainen*, oikeus käsittelyyn olisi jo ”*rikosten havaitsemiseksi ja paljastamiseksi*”. Säännöksissä ei siten – toisin kuin pakkokeinolaissa – olisi lainkaan edellytystä siitä, että toimenpide on tarpeen yksilöidyn rikosepäilyn johdosta.

Käsittelyn käsitteen piiriin kuuluu muun ohella tietojen luovuttaminen. Tunnistamistietoja voidaan tietosuojalain 8 §:n mukaan luovuttaa niille tahoille, joilla on oikeus käsitellä tietoja asianomaisessa tilanteessa. Tästä, samoin kuin ehdotuksen sanamuodosta seuraa, että ehdotuksen on ilmeisesti tarkoitettu mahdollistavan sen, että yhteisötilaajan käsittelyoikeuden piiriin kuuluvat tiedot voitaisiin aina luovuttaa poliisille. Tässä yhteydessä tulee jälleen esiin käsitteen ”käsitellä” ongelmallisuus, joka on johtanut siihen, ettei luovutus – vakiintuneesta lainsäädäntökäytännöstä poiketen – lainkaan näy vaitiolovelvollisuussäännöksestä.

Mikä tahansa yhteisötilaaja voisi käsitellä tietoja säännösehdotuksessa mainittujen rikosten paljastamiseksi ja selvittämiseksi. Voidaankin siis kysyä, voisiko poliisi pyytää yhteisötilaajalta tunnistamistietojen käsittelyä.[7] Kun näin ilmeisesti on, lakiehdotus *merkitsisi pakkokeinolain tunnistamistietojen luovuttamista koskevan sääntelyn tulemista turhaksi niiltä osin kuin kysymys on ehdotuksessa tarkoitetuista rikoksista. Samalla tunnistamistietojen käsittelyssä merkitystä ei olisi enää lainkaan rangaistusasteikolla. Tästäkin näkökulmasta tarkasteltuna säännösehdotus ei täytä lainsäädännön tarkkarajaisuudelle ja johdonmukaisuudelle asetettavia vaatimuksia.*

Tarkkarajaisuuteen liittyy myös *kysymys ajasta, jossa käsittely olisi sallittua*. Säännösehdotuksissa eikä sen perusteluissa ole asiaa lainkaan käsitelty. Jotkin perustelujen lausumat viittaavat enemmänkin siihen, että kysymys on jatkuvasta toiminnasta (mainin ta tietosuojavaltuutetulle tehdystä kertailmoituksesta). Perustuslakivaliokunnan käytännössä on useissa eri yhteyksissä todettu, että vaatimus perusoikeuksia rajoittavan toimenpiteen välttämättömyydestä rajaa myös sen kestoa, mutta siitä huolimatta on usein edellytetty jonkinasteista määräaikaa. Tietosuojalain 8 §:ssä on säädetty yleinen edellytys siitä, että käsittelyllä ei saa rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä. Tämän merkitys jää kuitenkin varsin ohueksi ehdotetussa sääntelymallissa, koska mikään ei velvoita yhteisötilaajaa edes esittämään asiasta selvitystä tietosuojavaltuutetulle annettavassa ilmoituksessa.

Perusoikeuksia rajoitettaessa on otettava huomioon ***sääntelyn oikeasuhteisuus*** (suhteellisuusperiaate). Tältä kannalta merkityksellistä muun ohella on, että *ehdotuksessa käsittelyoikeuksien sääntelyyn ei ole liitetty minkäänlaisia yhteisötilaajan toimintavelvoitteisiin liittyviä edellytyksiä*. Asian konkretisoimiseksi voidaan viitata yksityisyyden suojasta työelämässä annetun lain työnantajalle tarkoitetun ja työntekijän sähköpostiosoitteeseen lähetetyn viestin esille hakemista ja avaamista koskeviin säännöksiin, joissa työnantajalla on oikeus toimenpiteisiin vain, jos se on suorittanut tietyt laissa säädetyt toimenpiteet (17 ja 18 §).

Ehdotusta on perusteltu tällä hetkellä käytössä olevassa aineistossa yrityssalaisuuksien merkityksellä elinkeinotoiminnalle. Rikoslain yrityssalaisuutta koskevien säännösten selkeänä lähtökohtana – ja yleisemminkin koko liike- ja ammattisalaisuuden olemassaolon kannalta – on yrityksen oma salassapitotahto ja sen mukaan mitoitetut toimenpiteet. Yrityssalaisuuden rikkomisena ei voida pitää tilannetta, jossa yritys itse laiminlyö valvoa pääsyä yritykselle sensitiivisiin tietoihin. *Siten mikään viestinnän osapuolten tunnistetietojen suojan rajoittaminen ei voi olla riippumaton siitä, onko kyseisillä henkilöillä pääsy yrityssalaisuuksiin vai ei.*

Sääntelyn oikeasuhteisuuteen kuuluu, että lainsäätäjä ei voi antaa oikeutta rajoittaa perusoikeutta laajasti ja ilman, että *asianomainen itse* hyödyntää täysimääräisesti käytettävissään olevat eri keinot. Osana tietoturvallisuustoimenpiteitä voidaan valvoa sensitiivisiä tietoja sisältävien tiedostojen käsittelyä erilaisten logitiedostojen avulla, joihin kirjaantuu vaikkapa tieto siitä, että tietoja on talletettu erilliseen tiedostoon. Esimerkiksi yritysvakoilun tunnusmerkkeihin kuuluu muun ohella tunkeutuminen ulkopuoli-

[7] Eri asia on, ettei poliisilla välttämättä ole tiedonsaantioikeutta. Tietovirtojen kannalta olennaista kuitenkin on, että yhteisötilaajalla olisi oikeus tietojen luovuttamiseen.

silta suojattuun paikkaan tai tietojärjestelmään sekä tallenteen jäljentäminen (RL 12: 4). Nämä toimenpiteet ovat havaittavissa huolellisten ja asianmukaisten tietoturvallisuustoimenpiteiden avulla.

Mitä edellä on todettu, koskee myös *viranomaistyönantajaa*. Viranomaisilla on viranomaisten toiminnan julkisuudesta annetun lain (621/1999) mukaan velvollisuus noudattaa hyvää tiedonhallintatapaa, mihin kuuluu myös tietoturvallisuudesta huolehtiminen. *Sensitiiviset tietoaineistot on asianmukaisesti luokiteltava sekä rajoitettava pääsy niihin vain nimetyille henkilöille. Tietoturvallisuusvaatimuksiin kuuluu myös käsittelyn dokumentointi,* ja osaa tietoaineistoista – etenkin kansainvälisistä tietoturvallisuusvelvoitteista annetun lain (588/2004) soveltamisalan piiriin kuuluvia aineistoja – ei saa edes käsitellä sähköisessä ympäristössä. [8] Voidaankin todeta, että esim. turvallisuussalaisuuden paljastamisen (RL 12:7) tunnusmerkkejä vastaavat tietoaineistot kuuluvat valtionhallinnon tietoturvallisuusvaatimusten mukaan korkeimpiin turvallisuus- tai käsittelyluokkiin, joihin on sovellettava erittäin tiukkoja käsittelyvaatimuksia (esim. logi kaikkine käsittelytietoineen; käsittely vain erillisessä työasemassa). Ehdotettua sääntelyä ei käytettävissä olevan aineiston perusteella näytetä lainkaan arvioidun valtionhallinnon tietoturvallisuuden kannalta. *Kontrolloimaton ja tosiasiallisesti rajoittamaton oikeus tunnistamistietojen käsittelyyn voi sisältää merkittävän tietoturvallisuusriskin; ts. ehdotus vaikuttaisi vastoin niitä etuja, joiden suojan tehostamisella ehdotusta perustellaan.*

Perusoikeuksia rajoitettaessa *on* ***huolehdittava riittävistä oikeusturvajärjestelyistä*** (ks. esim. PeVM 25/1994 vp). Ehdotuksessa on säännös yhteisötilaajan velvoittamisesta ilmoittaa seurannan toteuttamisesta sille, jonka tunnistamistietojen käsittelyn perusteella on tarkoitus ryhtyä toimenpiteisiin. Ehdotuksessa ei ole muita laintasoisia oikeusturvajärjestelyjä koskevia säännöksiä, jollei sellaisiksi haluttaisi katsoa tietosuojavaltuutetulle tehtävää ilmoitusta.

Ehdotuksen mukaan se, miten ja milloin ja kuinka kauan tunnistamistietoja käsiteltäisiin, jäisi käytännössä ja tosiasiassa yksinomaan yhteisötilaajan omaan harkintaan ja tietoisuuteen. Tietoja käsittelystä ei olisi velvollisuutta tallettaa. Päinvastoin: tietosuojalain 8 §:ssä velvoitetaan, että tunnistamistiedot on hävitettävä tai tehtävä sellaisiksi, ettei niitä voi yhdistää tilaajaan tai käyttäjään, ellei laissa toisin säädetä. Ainoa ulkopuolista valvontaa ja tietyssä määrin oikeusturvajärjestelyjä koskeva ehdotus tietosuojavaltuutetulle tehtävästä ilmoituksesta jää sekin varsin tyhjäksi, koska käsittelyn kirjaamisvelvoitetta ja käsittelytietojen säilyttämisvelvoitetta ei ole. Tietosuojalaissa ei ole säädetty tietosuojavaltuutetulle oikeutta valvonnalliseen tarkastukseen eikä selvyyttä myöskään ole, voidaanko tässä yhteydessä soveltaa henkilötietolain (523/1999) 39 §:ää.

Oikeusturvajärjestelyjen kannalta voidaan tietysti pohtia sitä, mikä merkitys on sillä, että yhteisötilaajan on laadittava tunnistamistietojen käsittelyohje ja että tietojenkäsittely ja ohje sekä siitä tiedottaminen kuuluvat ns. yt-menettelyn piiriin. Ehdotus ei

[8] Tietoturvallisuuden varmistamisessa on käytössä myös henkilön taustojen selvittämismenettely turvallisuusselvityksistä annetun lain (177/2002) mukaisesti, minkä lisäksi henkilön luotettavuutta voidaan selvittää mm. huumetestien avulla yksityisyyden suojasta työelämässä annetun lain mukaisesti.

näiltä osin voi korvata laissa säädettyjä oikeusturvatakeita, minkä lisäksi ehdotettu menettely kattaa vain osan niistä tilanteista, joita ehdotetun sääntelyn johdosta syntyy – ehdotushan koskee kaikkia yhteisötilaajia.

Henkilötietolaki on henkilötietojen käsittelyä koskeva yleislaki, jota on noudatettava myös sähköisessä viestinnässä silloin, kun kysymys on henkilötietojen käsittelystä ja kun sähköisen viestinnän tietosuojalaissa ei ole toisin säädetty. Siten esim. henkilötietolain 24 §:n säännökset informointivelvoitteesta tulisivat ilmeisesti sovellettaviksi. Tietoja siitä, miten säännöstä sovellettaisiin ja miten informointivelvoite toteutettaisiin erilaisten toimintojen yhteydessä, ei ole ehdotuksesta tai sen perusteluista löydettävissä. Varsin erikoinen kuva Suomesta matkailumaana piirtyy, jos ja kun hotellivieraille ilmoitetaan, että heidän hotellin keskuksen kautta meneviä sähköisiä viestejään voidaan käsitellä lakiehdotuksessa tarkoitetulla tavalla.

Edellä olevan perusteella näyttää ilmeiseltä, että

> *tehty ehdotus ei täytä perustuslain ja sitä koskevan tulkintakäytännön mukaisia vaatimuksia perusoikeuksien rajoittamisesta eikä se näyttäisi olevan myöskään sopusoinnussa Suomea sitovien kansainvälisten velvoitteiden kanssa.*

Ehdotetun sääntelyn mukaan yhteisötilaajat voisivat käsitellä tunnistamistietoja rikosten paljastamiseksi, ehkäisemiseksi, selvittämiseksi ja esitutkintaan saattamiseksi.
Koska yhteisötilaajan oikeus olisi ehdotuksen mukaan riippumaton sen tehtävistä ja siitä, kenen viestintää koskevia tietoja käsittelyoikeus koskisi, herää myös kysymys *ehdotetun sääntelyn suhteesta perustuslain 124 §:ään*, jossa säännellään hallintotehtävän antamista muulle kuin viranomaiselle. Ehdotetusta säännöksestä saattaisi olla mahdollista tehdä se johtopäätös, että yhteisötilaajilla on oikeus toimialastaan riippumatta toimia ehdotuksessa tarkoitettujen rikosten paljastamiseksi ja ehkäisemiseksi. Perustuslain 124 §:n mukaan merkittävää julkisen vallan käyttöä sisältäviä tehtäviä voidaan kuitenkin antaa vain viranomaiselle. Merkittävänä julkisen vallan käyttämisenä on pidettävä esimerkiksi itsenäiseen harkintaan perustuvaa *oikeutta* käyttää voimakeinoja tai *puuttua muuten merkittävällä tavalla yksilön perusoikeuksiin.* Tällaisia valtuuksia ei siis saisi antaa muille kuin viranomaisille (HE 1/1998 vp).

5. Ehdotuksen suhteesta muuhun sääntelyyn

Kuten edellä on todettu, ehdotuksen perustelut ja sen valmistelusta vastaavat tahot viittaavat voimakkaasti ja jotensakin yksiselitteisesti siihen, että ehdotuksessa on kysymys työntekijän ja työnantajan välisiin suhteisiin liittyvistä kysymyksistä. Asia on ollut esillä viime aikoina myös eräissä esitutkinta- ja oikeusprosesseissa, joissa työnantaja on itse tai teleoperaattorin avustuksella seurannut työntekijöiden sähköpostiliikennettä. Säännöksen eräs vaikutus olisikin, että tällainen toiminta enemmän tai vähemmän laajasti deskriminalisoitaisiin, ts. tehtäisiin lailliseksi.

Jos ja kun yhteisötilaaja, jolla käsittelyoikeus olisi, määriteltäisiin ehdotuksen tarkoitusta vastaavalla tavalla työnantajaksi, nousee väistämättä esiin kysymys säännöksen

sijoituspaikasta. Työelämän tietosuojaa määrittelee *laki yksityisyyden suojasta työelämässä*. Lain luonne ja rooli oikeusjärjestyksessä on selvä: kysymys on laista, jossa tyhjentävästi näkyvät *kaikki ne tilanteet, joissa työnantaja käsittelee tai voi käsitellä henkilötietoja tai suorittaa työntekijän teknistä valvontaa.* Vaikka ehdotettu säännös poliittisista syistä otettaisiinkin sähköisen viestinnän tietosuojalakiin, yksityisyyden suojasta työelämässä annettua lakia olisi joka tapauksessa tarkistettava lainsäädännön ristiriidattomuuden varmistamiseksi. Tällaisia työelämän tietosuojalain säännöksiä ovat ainakin lain 2 ja 4 § sekä 6 luku. Toisin sanoen: *laki yksityisyyden suojasta työelämässä olisi avattava samassa yhteydessä*.

6. Tiivistelmäksi

Käsiteltävänä oleva *ehdotus on erittäin ongelmallinen*. Se ei täytä Suomea sitovien kansainvälisten velvoitteiden eikä perusoikeuksien rajoittamista koskevia vaatimuksia sääntelyn hyväksyttävyydestä, tarkkarajaisuudesta ja oikeasuhtaisuudesta sekä oikeusturvatakeista. Ehdotettu sääntely ei täytä oikeusjärjestyksen johdonmukaisuudelle asetettuja vaatimuksia ja säännösten suhdetta muuhun lainsäädäntöön ei ole toteutettu asianmukaisesti. Sääntelyn sijoituspaikka on väärä, jos tarkoituksena on lisätä työnantajan oikeuksia.

Ehdotettuja säännöksiä *ei tulisi sisällyttää kevään aikana annettavaan esitykseen*. Asia vaatii yksiselitteisen selvästi jatkovalmistelua, jossa tulisi noudattaa yleisiä lainvalmisteluperiaatteita.

Tässä yhteydessä ei voi olla kiinnittämättä huomiota tarpeeseen valtioneuvoston tasolla vakavasti miettiä, miten kolmas kanta, ts. valtio ja valtioneuvoston taso, ovat mukana kolmikantavalmistelussa vastaamassa siitä, että annettavat esitykset täyttävät laadukkaan lainvalmistelun vaatimukset, mitä sekä valtioneuvosto että eduskunta ovat toistuvasti korostaneet.