Defensor Legis N:o 4 /2008

# YRITYSSALAISUUKSIEN SUOJAAMINEN JA OMA HENKILÖSTÖ

(*Der Schutz von Betriebsgeheimnissen und eigenes Personal*)

## 1 Johdanto

Yrityssalaisuuksien suojaamisessa asettaa elinkeinonharjoittajalle suurimman haasteen oma henkilöstö. Syynä tähän on se, että elinkeinonharjoittaja säännönmukaisesti joutuu luovuttamaan salassa pidettävää tietoaan työntekijöidensä haltuun ja saataville, jotta nämä voivat suorittaa työtehtäviään. Suuri osa työnantajan yrityssalaisuuksikseen katsomista tiedoista lisäksi syntyy suoraan omien työntekijöiden työsuoritusten pohjalta. Yritystoiminnan tuloksellisuus usein myös edellyttää työyhteisön sisällä tiedon aktiivista jakamista eikä niinkään tietoon pääsemisen rajoittamista.

Useissa tuomioistuinkäsittelyyn edenneissä yrityssalaisuuden suojaa koskeneissa tapauksissa asetelma on ollut se, että vastakkain ovat olleet nimenomaan työnantaja ja yrityksen oma työntekijä – ja tyypillisesti siten, että kysymys on ollut työntekijän menettelystä *työsuhteen päättymisen jälkeisenä ajanjaksona* ja ehkä osittain myös *työsuhteen loppuvaiheissa*. Tämä selittyy sillä, että työntekijän näkökulmasta merkittävin tarve hyödyntää työssä opittua tietoa jonkun muun kuin oman työnantajan hyväksi ja lukuun syntyy herkimmin juuri työpaikkaa vaihdettaessa tai omaa yritystoimintaa työsuhteen jälkeen käynnistettäessä.

Työsuhteen päättymisen jälkeen tuleekin usein ajankohtaiseksi tehdä eroa sen suhteen, mikä tieto on aikaisemmalle työnantajalle kuuluvaa yrityssalaisuutta ja mikä sellaista, josta työsuhteen kestäessä on tullut osa työntekijän omaa ammattitietoa tai -taitoa. Lain säännösten tulkinnan vaikeutta lisää se, että useissa tapauksissa voidaan esittää hyviä perusteluja – näkökulmasta riippuen – sekä tiedon yrityssalaisuudeksi katsomiselle että sille, että tieto on muodostunut osaksi työntekijän omaa ammattitaitoa. Tietojen erottelemisen vaikeus korostuu asiantuntijatehtävissä ja pitkälle erikoistuneissa toimenkuvissa sekä myös tehtävissä, joissa työnteko suoritetaan lähellä asiakasrajapintaa.[1]

Vielä 2000-luvun alkupuolelle saakka lähdettiin lainsäädännössä siitä, että työntekijän salas-

[1] Asiakasrajapinnan osalta keskeinen merkitys on ollut erityisesti *asiakasrekistereillä*. Oikeustapauksista, joissa arvioitavana on ollut tällaisen rekisterin luonne yrityssalaisuutena ks. *Klaus Nyblin*, Yrityssalaisuusrikokset, teoksessa Talousrikokset, toim. Raimo Lahti ja Pekka Koponen, Suomalaisen Lakimiesyhdistyksen julkaisuja E-16, 2., uudistettu painos, Helsinki 2007, s. 240. Asiakaskontaktien merkityksestä tilanteessa, jossa työntekijä ryhtyy työsuhteen jälkeen harjoittamaan kilpailevaa liiketoimintaa, ks. myös KKO 2003:19, jossa arvioitavana oli liike- ja ammattisalaisuuksien suojaamiseksi tehdyn kilpailukieltosopimuksen pätevyys työsopimuslain säännösten pohjalta.

sapitovelvollisuus ja tietojen oikeudettoman hyväksi käyttämisen kielto on aiheellista rajoittaa *työsuhteen kestoaikaan*. Yhtenä perusteluna tälle oli juuri se, työnantajan yrityssalaisuuksia ja työntekijän omaa ammattitaitoa on toisinaan vaikea erotella toisistaan.[2] Yrityssalaisuuden rikkomista koskevan rikoslain (RL) 30:5:n muuttamisella vuonna 2003 säädettiin kuitenkin rangaistavaksi yrityssalaisuuksien oikeudeton ilmaiseminen ja käyttäminen vielä *kahden vuoden ajan palvelussuhteen päätyttyäkin*.[3] Keskeisenä taustaperusteluna oli tarve puuttua sellaisiin moitittaviin tekoihin, joilla aikaisemmalle työnantajalle kuuluvia yrityssalaisuuksia suoraan siirretään toisen työnantajan tai työntekijän perustaman uuden yrityksen toimintaan.[4]

Yrityssalaisuuden rikkomista koskevan rangaistussäännöksen muuttamisen seurauksena RL:n sääntelystä tuli työsopimuslain (55/2001, TSL) ja sopimattomasta menettelystä elinkeinotoiminnassa annetun lain (1061/1978, SopMenL) sääntelystä poikkeava. Sekä TSL 3:4:n että SopMenL 4.2 §:n mukaisesti työnantajan ammatti- ja liikesalaisuuden (tai ”liikesalaisuuden”, kuten suojan kohde on SopMenL:ssa määritelty) lakisääteinen suoja nimittäin päättyy työntekijän työsuhteen (palvelusajan) päättyessä. RL 30:5:n mukaisesti rangaistusvastuu sen sijaan säilyy vielä kaksi vuotta tämän jälkeenkin. Eri lakien eripituisia aikarajauksia ei voida pitää lainsäädännön informatiivisuuden näkökulmasta hyvänä asiaintilana, mutta käytännössä tämä ei kuitenkaan näytä aiheuttaneen erityisempiä tulkintaongelmia.[5]

RL 30:4–6:een sisältyvät yrityssalaisuusrikossäännökset (yritysvakoilu, yrityssalaisuuden rikkominen ja yrityssalaisuuden väärinkäyttö) ovat olleet olennaisilta osiltaan nykyisensisältöisinä – mainittu RL 30:5:n ajallisen soveltamisalan pidennys pois lukien – voimassa jo runsaat 17 vuotta. Tänä aikana säännösten soveltamisesta on jo ehtinyt kertyä melko paljon oikeuskäytäntöä myös hovioikeustasolta, noin 20 tapausta tähän mennessä. Toistaiseksi yrityssalaisuusrikoksista ei ole ollut annettuna yhtään RL 30:4–6:een perustuvaa korkeimman oikeuden ratkaisua. Yksi valituslupa on vuoden 2008 puolella kuitenkin jo myönnetty[6], joten lähitulevaisuudessa on yrityssalaisuusrikossäännöksistä käytettävissä myös KKO:n ratkaisu.[7]

KKO:n myöntämä valituslupa koskee tapausta, jossa sovellettava säännös on yrityssalaisuuden rikkomista koskeva RL 30:5 – ja nimenomaan työntekijän työsuhteen päättymien jälkeisen ajanjakson osalta. Valitusluvan myöntämisestä julkaistun selosteen mukaan tapauksessa ”A oli ryhtynyt harjoittamaan liiketoimintaa samalla alalla kuin millä hänen entinen työnantajansa oli toiminut. Kysymys siitä, oliko A syyllistynyt yrityssalaisuuden rikkomiseen”. On odotettavissa, että KKO:n asiassa antama ratkaisu tulee keskeisesti linjaamaan sitä, millaisin ”pelisäännöin” uudessa yritystoiminnassa tulee menetellä – tai on sallittua menetellä – suhteessa aikaisemman työnantajan (väitettyihin) yrityssalaisuuksiin.

Yrityssalaisuuksien suojan osalta on paraikaa valmisteilla myös yksi sellainen kiinnostava lainmuutos, joka ei suoraan liity RL 30:4–6:n tunnusmerkistöjen ulottuvuuteen mutta jolla kuitenkin voi olla keskeistäkin merkitystä yrityssalaisuuksia koskevan oikeussuojan *käytännön toteuttamises-*

---

[2] Ks. RL 30:4–6:n säännöksiä koskenut ensimmäinen HE 66/1988 vp, s. 86 sekä työsopimuslakia (55/2001) koskeva HE 157/2000 vp, s. 81.

[3] L 61/2003 – HE 53/2002 vp ja LaVM 18/2002 vp.

[4] Sääntelyn taustaperusteluista – viittauksin HE:een 53/2002 vp – ks. *Nyblin*, Yrityssalaisuuden suoja ja entiset työntekijät, DL 2003, s. 231–232.

[5] Ks. yksityiskohtaisemmin *Nyblin*, DL 2003, s. 240–241.

[6] VL 2008-33. – Olen viitannut Kouvolan hovioikeuden asiassa antamaan tuomioon aikaisemmassa artikkelissani *Nyblin* 2007, s. 234 (viite 12), 236 (viite 16), 239, 277 ja 279 (viite 128).

[7] Huomaa, että KKO:n ratkaisuja on liikesalaisuuden suojaa koskevista rikosasioista kuitenkin aikaisemman lainsäädännön ajalta: KKO 1984 II 177 ja 1991:11. Ks. myös KKO 1984 II 43 ja 1989:39.

*sa*. Eduskunnan käsiteltäväksi on keväällä 2008 tullut hallituksen esitys 48/2008 vp, joka koskee (muun ohella) sähköisen viestinnän tietosuojalain (516/2004) muuttamista siten, että työnantajat saisivat rajoitetun oikeuden käsitellä työntekijöidensä sähköpostiviestinnän tunnistamistietoja sen selvittämiseksi, ovatko työntekijät oikeudettomasti paljastaneet yrityssalaisuuksia.[8]

Käsittelen seuraavassa työnantajan yrityssalaisuuksien suojaa paitsi eräiden käytännön tyyppitapausten näkökulmasta myös erikseen suhteessa siihen, *millä tavoin* työnantajat käytännössä voivat *selvittää*, ovatko työntekijät menetelleet yrityssalaisuuksien suhteen moitittavalla tavalla. Keskityn erityisesti sellaisiin kysymyksenasetteluihin, jotka yrityssalaisuuden suojaa käytännössä toteutettaessa ovat osoittautuneet haasteellisiksi. Työnantajan, joka tehokkaasti pyrkii suojaamaan yrityssalaisuuksiaan, on aiheellista tiedostaa, millaiset toimintatavat väärinkäytösten selvittämiseksi ovat sallittuja. Kovin suoraviivaiset toimintatavat voivat nimittäin johtaa työntekijöiden oikeuksien loukkaamiseen – ja myös siihen, että työnantajan edustajien oma toiminta tulee arvioitavaksi rikossäännösten pohjalta.

## 2 Yrityssalaisuusrikokset

### *2.1 Yleistä*

Liike- ja ammattisalaisuuden suojasta on RL:n ulkopuolella säädetty erityisesti TSL:ssa ja SopMenL:ssa. TSL 3:4:n mukaan työntekijä ei saa työsuhteen kestäessä käyttää hyödykseen tai ilmaista työnantajan ammatti- ja liikesalaisuuksia. Säännöksen mukaan jos työntekijä on saanut tiedot oikeudettomasti, kielto jatkuu myös työsuhteen päättymisen jälkeen.

TSL 3:4:ään nähden sisällöltään olennaisesti samanlainen säännös on myös SopMenL:ssa, jossa säädetään liikesalaisuuden suojasta paitsi työnantajan ja työntekijän välisessä suhteessa myös muissa relaatioissa. SopMenL 4.1 §:n mukaan kukaan ei saa oikeudettomasti hankkia tai yrittää hankkia tietoa liikesalaisuudesta eikä käyttää tai ilmaista näin hankkimaansa tietoa. Säännöstä on mahdollista soveltaa myös yrityksen omiin työntekijöihin.[9] SopMenL 4.2 §:n mukaisesti se, joka elinkeinonharjoittajan palveluksessa ollessaan on saanut tiedon liikesalaisuudesta, ei saa sitä palvelusaikanaan oikeudettomasti käyttää eikä ilmaista hankkiakseen itselleen tai toiselle etua tai toista vahingoittaakseen.

SopMenL 4.3 §:ssä säädetään elinkeinonharjoittajan puolesta tehtävää suorittavan velvollisuudesta pitää luottamuksellisesti tietoon saatu liikesalaisuus salassa sekä velvollisuudesta pidättäytyä käyttämästä tällaista tietoa oikeudettomasti hyväksi. Momentissa säädetään erikseen myös *teknisten esikuvien ja ohjeiden* suojasta: se, jolle työn tai tehtävän suorittamista varten tai muuten liiketarkoituksessa on uskottu tekninen esikuva tai tekninen ohje, ei saa sitä oikeudettomasti käyttää eikä ilmaista. Kielto koskee myös työntekijäasemassa olevia[10], eikä kiellon voimassaoloa ole ajallisesti rajoitettu. SopMenL 4.4 §:ssä on lisäksi säännös kolmannen henkilön vastuuasemasta oikeudettomasti hankittujen tai ilmaistujen liikesalaisuuksien sekä teknisten esikuvien ja ohjeiden suhteen.[11]

Vaikka TSL 3:4:ssä ja SopMenL 4.2 §:ssä on rajattu työntekijöiden lakisääteinen salassapitovelvollisuus koskemaan vain työsuhteen kestoaikaa, lainvalmistelussa ja oikeuskirjallisuudessa on yleisesti katsottu, että työntekijän sidonnaisuutta voidaan pidentää sellaisella salassapitoso-

[8] Hallituksen esitys Eduskunnalle sähköisen viestinnän tietosuojalain ja eräiden siihen liittyvien lakien muuttamisesta.
[9] Oikeuskäytännöstä ennen RL 30:4–6:n voimaantuloa ks. edellä viitatut KKO 1984 II 177 ja 1991:11.
[10] HE 114/1978 vp, s. 15.
[11] SopMenL 4 §:n kielloista yksityiskohtaisemmin ks. *Tom Vapaavuori*, Yrityssalaisuudet ja salassapitosopimukset, Helsinki 2005, s. 114–119.

pimuksella, jossa salassapitovelvollisuus määrätään koskemaan koko työsuhteen jälkeistä aikaa tai tiettyä, lyhyempää aikaa työsuhteen päättymisen jälkeen.[12] Tyypillistä on ollut käytännössä se, että jos sidonnaisuus on sopimuksella ulotettu myös työsuhteen päättymisen jälkeiseen aikaan, sopimusehtoon ei ole sisällytetty erityistä määräaikaa. Tältä osin käytäntö on poikennut yritysten välisistä salassapitosopimuksista, joille on tunnusomaista, että salassapidolle on yleensä jokin nimenomainen määräaika, esimerkiksi viisi vuotta (pää)sopimussuhteen päättymisestä.[13]

RL 30:4–6:een sisältyvät yrityssalaisuusrikossäännökset rakentuvat systematiikaltaan samalle pohjalle kuin SopMenL 4 §:n kieltosäännökset: erikseen on säännelty oikeudetonta tiedonhankintaa (*yritysvakoilu*, RL 30:4) ja erikseen luottamusasemassa olevien salassapitovelvollisuutta (*yrityssalaisuuden rikkominen*, RL 30:5) sekä kolmannen henkilön vastuuasemaa (*yrityssalaisuuden väärinkäyttö*, RL 30:6).[14] RL 30:4:n ja 30:6:n mukaisten rikosten tekijänä voi olla lähtökohtaisesti kuka tahansa, mutta RL 30:5:n tunnusmerkistön soveltaminen edellyttää, että tekijä kuuluu johonkin sellaiseen ryhmään, joka säännöksessä on nimenomaisesti määritelty. Yksi tällainen ryhmä on *toisen palveluksessa olevat henkilöt*.

### *2.2 Lähtevä työntekijä potentiaalisena yrityssalaisuusrikoksen tekijänä?*

Yrityssalaisuuden rikkomista koskevan RL 30:5:n mukaisesti toisen palveluksessa olevalla (käytännössä yleensä työsopimussuhteessa olevalla henkilöllä) ei ole oikeutta paljastaa toiselle (omalle työnantajalle tai tämän yhteistyökumppanille) kuuluvaa yrityssalaisuutta tai käyttää tällaista salaisuutta luvattomasti itsensä tai jonkun muun hyväksi. Kielto on voimassa sekä palvelussuhteen aikana että kaksi vuotta sen jälkeen. RL 30:5 on kirjoitettu siten, että yrityssalaisuuden rikosoikeudellinen suoja on lähtökohtaisesti yhtä vahva sekä palvelussuhteen kestäessä että sen jälkeen; eroa ei ole myöskään sen suhteen, onko teossa kysymys yrityssalaisuuden ilmaisemisesta vai käyttämisestä.

Kun RL 30:5:n ajallista soveltamisalaa vuonna 2003 toisen palveluksessa olevien osalta laajennettiin, otettiin kantaa samalla myös siihen, millä tavoin käytännössä voidaan tehdä eroa sen suhteen, millainen tieto on (aikaisemmalle) työnantajalle kuuluvaa yrityssalaisuutta ja millainen tieto sitä vastoin työntekijän omaa ammattitaitoa, jota työntekijällä on oikeus vapaasti hyödyntää. Tuossa yhteydessä nostettiin esille erottelu *kirjallisesti tai sähköisesti tallennettuun tietoon* ja *työntekijän muistissa siirtyvään tietoon*.[15] Tällä erottelulla pyrittiin esittämään ainakin jonkinasteinen tulkintasääntö, jonka mukaan tallennettu tieto lähtökohtaisesti olisi työnantajalle kuuluvaa yrityssalaisuutta ja muistin varassa kulkeva tieto puolestaan työntekijän omaa ammattitaitoa.[16]

Vaikka tallenneliityntään perustuvaa tulkintasääntöä ei ole tarkoitettu sovellettavaksi ehdottomana, sen taustalla oleva ajatuskulku on sinänsä perusteltu ja myös vastaa melko pitkälle sitä, miten työelämässä ja yritystoiminnassa on yleisesti arvioitu niitä pelisääntöjä, joiden pohjalta työpaikkaa vaihdetaan tai omaa yritystoimintaa aloitetaan; kunkin työntekijän tulisi lähteä ”vanhalta työpaikaltaan” vain se tieto ja osaaminen

---

[12] Ks. *Nyblin*, DL 2003, s. 241 ja siinä viitattu kirjallisuus sekä *Seppo Koskinen – Kimmo Nieminen – Mika Valkonen*, Työhönotto ja työsopimuksen ehdot, Helsinki 2008, s. 472.

[13] Yritysten välisten salassapitosopimusten aikarajausta koskevista tyypillisistä ehdoista ks. *Vapaavuori*, s. 234–237.

[14] Systematiikasta yksityiskohtaisemmin ks. *Nyblin* 2007, s. 246–249.

[15] HE 53/2002 vp, s. 16 ja 32.

[16] Asiasta yksityiskohtaisemmin ks. *Nyblin*, Yrityssalaisuuksille dokumenttisuoja?, DL 2001 (”Nyblin 2001a”), s. 77–79 ja 93–94, *Nyblin*, Edelleen yritysvakoilusta ja yrityssalaisuuden rikkomisesta, DL 2001 (”Nyblin 2001b”), s. 924–925 ja *Nyblin*, DL 2003, s. 244–247; vrt. *Pekka Viljanen*, Vielä yritysvakoilusta ja yrityssalaisuuden rikkomisesta, DL 2001, s. 431 ja 434 (viite 36).

mukanaan, mikä muistissa kulkee – ja vielä tarkemmin ilmaistuna: vain se tieto mukanaan, joka on muodostunut osaksi työntekijän omaa ammattiosaamista.[17] Tämän lähtökohdan ovat monet työnantajat myös pyrkineet varmistamaan joko nimenomaisin sopimusehdoin tai erillisin tietoturvallisuusmääräyksin.[18]

Käytännössä saattaa kuitenkin olla jopa jossain määrin yleistä, että työntekijät eivät vaihda työpaikkaa aivan ”tyhjin käsin”. Näyttäisi siltä, että osa työntekijöistä mieltää oikeudekseen ottaa työpaikkaa vaihtaessaan mukaansa kopioita ainakin sellaisista asiakirjoista, jotka työntekijä on itse laatinut. Tällaiset asiakirjat saatetaan mieltää jonkinlaiseksi omaksi ”osaamispääomaksi” tai ”portfolioksi”, jonka mukana vieminen ei tunnu ainakaan erityisen väärältä. Toisaalta mainitunlaisia ”omia dokumenttejakin” kopioitaessa työntekijä ei tyypillisesti tee tätä avoimesti, vaan jättää asiasta työnantajalle kertomatta. Useissa tapauksissa kopioiminen ja dokumenttien siirtäminen myös suoritetaan *ennen* irtisanoutumista – ehkä juuri sitä silmällä pitäen, että työpaikan vaihdoksen tullessa työnantajan tietoon työnantaja saattaa erilaisilla käyttöoikeuksien poistamisilla ym. rajoittaa mahdollisuuksia tietojen kokoamiseen.

Yritysvakoilua koskeva RL 30:4 kieltää *oikeudettoman tiedonhankinnan* toiselle kuuluvista yrityssalaisuuksista esimerkiksi tallenteita jäljentämällä, niitä haltuun hankkimalla tai muulla tällaiseen rinnastettavalla tavalla. Keskeinen tulkintakysymys RL 30:4:n osalta on kuitenkin se, voidaanko säännöstä soveltaa myös edellä kuvatunlaiseen toimintaan – toisin sanoen sellaiseen aktiiviseen, muistinvahvistamistarkoituksessa suorittavaan tiedonhankintaan, joka kohdistuu tallenteisiin, joiden käsittelemiseen ja tutkimiseen työntekijällä sinänsä – osana työtehtäviään – on ollut lupa. Yrityssalaisuuden rikkomista koskevan RL 30:5:n kohdalla ei ole vastaavanlaisia tulkintaongelmia, mutta sen soveltamisessa nousee keskeiseen osaan tyypillisesti kysymys siitä, onko yrityssalaisuuksia sittemmin tosiasiallisesti *käytetty* tai *ilmaistu*; itse kopioimistoimenpidehän ei ole vielä yrityssalaisuuden käyttämistä tai ilmaisemista.

Useissa esitutkintaan päätyneissä yrityssalaisuuden suojaa koskeneissa tapauksissa on ollut työnantajan puolelta keskeisenä oikeustoimien käynnistämiseen vaikuttaneena syynä havainto siitä, että työntekijä on työsuhteen päättymisvaiheessa tavalla tai toisella kopioinut itselleen mukaansa asiakirjoja, esimerkiksi teknisiä piirustuksia tai asiakasluetteloita. Näissä tapauksissa on ollut työnantajan puolelta myös ilmeisenä oletuksena, että työntekijällä on ollut tarkoitus ryhtyä käyttämään tai ilmaisemaan kopioimiaan tietoja kilpailevassa liiketoiminnassa. Esitutkinnassa on useissa tapauksissa myös saatu varsin mittavaa näyttöä aineiston kopioimisesta. Tutkittavana olevaksi rikokseksi on kuitenkin yleensä kirjattu *yrityssalaisuuden rikkominen*, ei tietojen oikeudetonta hankkimista koskeva *yritysvakoilu*. Kysymys siitä, onko työntekijä lopulta *käyttänyt tai ilmaissut* hankkimiaan tietoja, on saattanut nousta esitutkinnassa perusteellisemmin esille vasta sen loppupuolella.

Edellä selostamani näkökohdat koskevat sellaisia käytännön haasteita, joita havaintojeni mukaan on useassa yrityssalaisuusrikosta koskevassa esitutkinnassa noussut esille. Alkuvaiheessa moni ”selvältä tapaukselta” vaikuttanut asia on sittemmin monimutkaistunut ja tapaus ei ehkä ole lopulta edennyt syyksi lukevaan tuomioon – tai edes syytteeseen – asti. Syynä RL 30:5:n mukaisen yrityssalaisuuden rikkomisen täyttymättä jäämiseen on saattanut olla joko se, että riittävää näyttöä tietojen käyttämisestä tai ilmaisemisesta ei ole esitutkinnassa onnistuttu hankkimaan, tai sitten vain yksinkertaisemmin se, että työntekijän menettelyä ei ole lopulta voitu

[17] Ks. *Nyblin*, DL 2001a, s. 89–90.
[18] Esimerkkinä mallisopimusehdosta ks. *Vapaavuori*, s. 279.

pitää sellaisena, mitä RL 30:5:n tunnusmerkistössä tarkoitetaan. Käsittelen tähän liittyviä tulkintaongelmia – myös yritysvakoilua koskeva RL 30:4:n tunnusmerkistö huomioon ottaen – jäljempänä erityisesti kohdassa 4.1.

### *2.3 Yrityssalaisuuksien suojaaminen ja RL 30:11*

Yrityssalaisuuden käsite on määritelty RL 30:11:ssä: yrityssalaisuudella tarkoitetaan ”liike- tai ammattisalaisuutta taikka muuta vastaavaa elinkeinotoimintaa koskevaa tietoa, jonka elinkeinonharjoittaja pitää salassa ja jonka ilmaiseminen olisi omiaan aiheuttamaan taloudellista vahinkoa joko hänelle tai toiselle elinkeinonharjoittajalle, joka on uskonut tiedon hänelle.”[19] Yrityssalaisuuden lakisääteisen määritelmän yksi tunnusmerkki siis on, että elinkeinonharjoittaja ”pitää tiedon salassa” – toisin sanoen, on ryhtynyt asianmukaisiin tietoturvallisuustoimenpiteisiin siitä huolehtimiseksi, että tieto ei päädy ulkopuolisten haltuun tai saataville.[20]

RL 30:11:n perusteluissa on hallituksen esityksessä todettu, että tiedon salassapitoa koskeva kriteeri merkitsee sitä, että ”tiedon tulee olla tosiasiallisesti suojattu ulkopuolisilta”.[21] Muissa yhteyksissä on lainvalmistelussa ja oikeuskirjallisuudessa viitattu työ- ja muihin sopimuksiin sisällytettäviin vaitiolovelvollisuuslausekkeisiin, oman henkilöstön ohjeistamiseen, teknisiin ja fyysisiin suojautumistoimenpiteisiin sekä yrityksessä suoritettaviin valvontatoimenpiteisiin.[22]

Jos elinkeinonharjoittaja laiminlyö RL 30:11:ssä edellytetyn tietojen suojaamisen, seurauksena RL 30:4–6:n tunnusmerkistöjen näkökulmasta on se, että väitetyssä yrityssalaisuutta loukanneessa menettelyssä jää täyttymättä se, että kyse ylipäänsä olisi *yrityssalaisuuteen* kohdistuneesta teosta.[23] Lisäksi tietoturvallisuustoimenpiteiden laiminlyönti merkitsee käytännössä sitä, että riski tietojen joutumisesta ulkopuolisten haltuun on huomattavasti suurempi kuin siinä tapauksessa, että tietoturvallisuudesta olisi huolehdittu. Toisaalta korkeatasoinenkaan tietoturva ei varmista sitä, etteivätkö sellaiset yrityksen omat työntekijät, joilla työtehtäviensä puolesta on laajalti pääsy yrityssalaisuuksia sisältäviin tallenteisiin, voisi sinänsä varsin helposti – niin halutessaan – ryhtyä yrityssalaisuuksien suojaa loukkaaviin tekoihin.

## 3 Työnantajan valvonta- ja selvittelyoikeudet

### *3.1 Yleistä näytön hankkimisesta ja esitutkintakynnyksen ylittymisestä*

RL 30:4–6:n mukaiset yrityssalaisuusrikokset ovat *asianomistajarikoksia*: virallinen syyttäjä ei saa nostaa syytettä niistä, ellei asianomistaja ilmoita rikosta syytteeseen pantavaksi taikka ellei erittäin tärkeä yleinen etu vaadi syytteen nostamista. Käytännössä esitutkinnan aloittamisen ja syytteen nostamisen perustana on aina ollut asianomistajan tutkinta- ja syyttämispyyntö – tiedossani ei ole yhtään sellaista tapausta, jossa virallinen syyttäjä olisi päätynyt esitutkinnan toimittamisen pyytämiseen tai syytteen nostamiseen ”erittäin tärkeän yleisen edun” perusteella. Yrityssalaisuusrikosta koskevan esitutkinnan alkaminen edellyttää siten aina asianomistajayritykseltä aktiivista toimintaa.

Esitutkintalain (449/1987) 2 §:n mukaisesti poliisin on toimitettava esitutkinta, kun sille teh-

[19] Ks. yksityiskohtaisemmin HE 66/1988 vp, s. 92–93, *Vapaavuori*, s. 27–77 ja *Nyblin* 2007, s. 233–246.

[20] Oikeuskäytännössä on tietoturvallisuustoimenpiteiltä vaadittavaa tasoa arvioitu Turun hovioikeuden tuomiossa 30.4.2007, dnro R 06/199.

[21] HE 66/1988 vp, s. 92.

[22] Ks. esim. HE 114/1978 vp, s. 14 ja *Vapaavuori*, s. 46–47.

[23] Ks. myös *Vapaavuori*, s. 44.

dyn ilmoituksen perusteella *on syytä epäillä, että rikos on tehty*. Jäljempänä kohdassa 3.3 tarkemmin esiteltävän sähköisen viestinnän tietosuojalain muuttamista koskevan hallituksen esityksen 48/2008 vp perusteluissa on viitattu epäkohtana siihen, että yrityksillä on puutteelliset mahdollisuudet saattaa poliisin tutkittavaksi yrityssalaisuuksien luvattomia luovuttamisia, *jos luovutus on tehty sähköisessä muodossa*.[24] Nykyisin voimassa oleva sähköisen viestinnän tietosuojalaki ei salli sähköpostiviestinnän tunnistamistietojen käsittelyä yrityssalaisuuksien oikeudettoman paljastamisen selvittämiseksi.[25] Elinkeinoelämän piirissä onkin ollut tyytymättömyyttä yrityksillä oleviin puutteellisiin mahdollisuuksiin hankkia riittävää näyttöä yrityssalaisuusrikoksista sitä silmällä pitäen, että poliisille tehtävä tutkintapyyntö myös johtaisi ”on syytä epäillä” -kynnyksen ylittymiseen ja siten esitutkinnan aloittamiseen. Kuten jäljempänä kohdassa 3.3 tarkemmin kuvataan, ehdotetut muutokset sähköisen viestinnän tietosuojalakiin johtavat toteutuessaan siihen, että yrityksillä on aikaisempaa paremmat mahdollisuudet väärinkäytösten selvittämiseen ennen tutkintapyynnön tekemistä poliisille.

Yleisesti on kuitenkin syytä edelleen kiinnittää huomiota siihen, että esitutkintakynnyksen ylittyminen edellyttää lähtökohtaisesti aina sitä, että on riittävästi selvitystä jonkin nimenomaisen rikoksen *tekemisestä*. Jos käytettävissä oleva selvitys viittaa vain sellaiseen mahdollisuuteen, että joku *saattaa tehdä* rikoksen, esitutkintakynnyksen ei lähtökohtaisesti tulisi ylittyä.

Juuri todettua peruslähtökohtaa ei ole havaintojeni mukaan aivan loppuun saakka mielletty kaikissa niissä esitutkinnoissa, jotka ovat koskeneet RL 30:5:n mukaista *yrityssalaisuuden rikkomista*. Useissa tapauksissa mainittua rikosta koskenut tutkintapyyntö on perustunut vain näyttöön siitä, että yrityksen työntekijä on kopioinut itselleen mukaansa yrityssalaisuuksia sisältävää aineistoa. Selvitys ei ole kaikissa tapauksissa sisältänyt näyttöä siitä, että epäilty työntekijä olisi myös ryhtynyt käyttämään tai ilmaisemaan hankkimaansa ja mukaan ottamaansa tietoa. Tällaisissa tapauksissa tulisikin aina erikseen arvioida, onko esitutkintakynnyksen ylittymiselle riittävä peruste nimenomaan *yrityssalaisuuden rikkomisen* osalta – vai olisiko asiassa ehkä syytä epäillä RL 30:4:n mukaista *yritysvakoilua*.[26] Viittaan tähän kysymyksenasetteluun tarkemmin jäljempänä kohdassa 4.1.

### *3.2 Näytön hankkiminen henkilötietojen käsittelynä*

Työnantaja käsittelee omia työntekijöitään koskevia *henkilötietoja* jatkuvasti osana työsopimussuhteeseen liittyvien oikeuksien ja velvollisuuksien hoitamista. Henkilötietojen käsittelyn henkilötietolain (523/1999) mukaisena perusteena on tällöin lain 8.1 §:n 5 kohdan mukainen palvelussuhde. Henkilötietolain säännösten lisäksi sovellettaviksi tulevat muun muassa yksityisyyden suojasta työelämässä annetun lain (759/2004, työelämän tietosuojalaki) säännökset. Yhtenä työnantajalla rekisterinpitäjänä olevana velvollisuutena on laatia *rekisteriselosteet* ylläpitämistään henkilörekistereistä. Rekisteriselosteissa tulee muun muassa kuvata se, mikä on henkilötietojen käsittelyn *tarkoitus* asianomaisen rekisterin osalta.[27]

Työnantajalla on osana työntekijöihin kohdistuvan työnjohto ja -valvontaoikeuden toteut-

[24] HE 48/2008 vp, s. 11.

[25] HE 48/2008 vp, s. 4. Ks. myös *Nyblin*, Työelämän sähköposti, 2., uudistettu painos, Helsinki 2004, s. 228–231.

[26] Ks. asiaa koskevasta aikaisemmasta keskustelusta *Nyblin*, DL 2001a, s. 93 ja *Nyblin*, DL 2001b, s. 928 (viite 51); vrt. *Viljanen*, s. 432.

[27] Henkilötietojen käsittelystä työelämässä ks. yleisesti *Ari Raatikainen*, Yksityisyyden suoja työelämässä, Helsinki 2002 ja *Mikko Nyyssölä*, Yksityisyyden suoja työsuhteessa, 3., uudistettu painos, Porvoo 2004.

tamista oikeus suorittaa myös *teknisin menetelmin toteutettua valvontaa*[28]. Tällaisen valvonnan muotoja ovat muun muassa kameravalvonta, kulunvalvonta, tietojärjestelmiin kirjautumisten ja tietojärjestelmissä toteutettujen käsittelytoimenpiteiden valvonta sekä sen valvonta, millaisia tietokoneohjelmia työntekijöiden käyttöön annetuille työasemille on tallennettuna. Mainituista valvonnan muodoista on työelämän tietosuojalaissa erityissäännöksiä vain kameravalvonnasta (lain 5 luvun 16 ja 17 §) – muiden valvonnan muotojen osalta yksittäisten toimenpiteiden oikeutus arvioidaan etupäässä kyseisen lain 3 §:n yleissäännöksen nojalla. Sen mukaan työnantaja saa käsitellä vain välittömästi työntekijän työsuhteen kannalta tarpeellisia henkilötietoja, jotka liittyvät työsuhteen osapuolten oikeuksien ja velvollisuuksien hoitamiseen tai työnantajan työntekijöille tarjoamiin etuuksiin taikka johtuvat työtehtävien erityisluonteesta.

Sähköisen viestinnän tietosuojalain muuttamista koskevassa tuoreessa hallituksen esityksessä 48/2008 vp on todettu teknisin menetelmin toteutettujen valvontatoimenpiteiden oikeutuksesta yrityssalaisuuksiin kohdistuneiden väärinkäytösten selvittämisessä seuraavaa[29]:

> ”… yrityssalaisuuksien oikeudettoman paljastamisen selvittämisessä ovat käytettävissä tietohallinnolliset keinot, kuten käyttäjälokien tarkastaminen, pääsyä rajoittaviin järjestelmiin kirjautuvien tietojen tarkastaminen sekä järjestelmien teknisessä ylläpidossa kerätyt tiedot. Näiden tietojen käsittelylle ei sähköisen viestinnän tietosuojalaissa aseteta rajoituksia…
>
> Toisin sanoen tietojärjestelmiä voidaan seurata vapaasti muun muassa väärinkäytöksiä selvitettäessä erilaisten käyttäjä-, tallennus- ja muiden sellaisten lokitietojen avulla.”

Täydennyksenä hallituksen esityksessä todettuun on aiheellista tuoda esille, että mainitut toimenpiteetkin työnantajan on kuitenkin tullut *etukäteen suunnitella* henkilötietolain 6 §:n tarkoittamalla tavalla, ja niiden toteuttamisessa työnantajan tulee myös muilta osin menetellä henkilötietolaissa ja työelämän tietosuojalaissa säädetyn mukaisesti. Yksi teknisin menetelmin toteutettavaa valvontaa koskeva keskeinen ennakollinen edellytys on se, että asiaa käsitellään yhteistoimintamenettelyssä siten kuin työelämän tietosuojalain 21 §:ssä on säädetty.

Työnantajan, joka teknisin menetelmin toteutettavan valvonnan keinoin seuraa yrityssalaisuuksien käsittelyä koskevien määräystensä ja ohjeittensa noudattamista, on siis *etukäteen* suunniteltava toimenpiteensä. Valvonta ei voi olla sillä tavoin salaista, että työntekijät olisivat tietämättömiä siitä, millaisia valvonnan muotoja on käytössä ja mihin työnantajalla oleviin tarpeisiin ne perustuvat. Kaikista teknisin menetelmin toteutetussa valvonnassa kertyvistä henkilörekistereistä tulee lisäksi laatia rekisteriselosteet, joista muun ohella ilmenee, millaista tietoa kerätään ja mikä on kerättävien tietojen käyttötarkoitus. Rekisteriselosteiden tulee myös olla työpaikalla jokaisen saatavilla, esimerkiksi intranetistä.

Jos työnantajan tietoon tulee nimenomainen epäilys siitä, että joku työntekijä tai jotkut työntekijät ovat syyllistyneet yrityssalaisuuksien suhteen väärinkäytöksiin, työnantajalla on huomattavasti paremmat valmiudet tehdä asiaa koskevia selvityksiä teknisin menetelmin toteutettavan valvonnan keinoin, jos työnantaja on jo etukäteen huolehtinut henkilötietolaissa ja työelämän tietosuojalaissa säädetyistä velvoitteistaan ja muutenkin pitänyt huolta siitä, että asiaan liittyvät prosessit ovat lain edellyttämällä tasolla. Työnantajalla, joka ”herää” vasta nimenomaisten väärinkäytösepäilyjen tullessa esille, toimintavalmius voi olla heikompi. Työnantajan on syytä

[28] Työelämän tietosuojalaissa (ks. 21 §) käytetään ilmaisua ”teknisin menetelmin toteutettu valvonta” erotuksena ”teknisestä valvonnasta”, joka pakkokeinolain (450/1987) säännösten mukaisesti on poliisille kuuluva oikeus. Käytetystä terminologiasta ks. PeVL 10/2004 vp, s. 6.

[29] HE 48/2008 vp, s. 3–4. Ks. myös HE:n s. 20 ja 39.

ottaa huomioon, että myös hankittaessa näyttöä epäillyistä yrityssalaisuuksiin kohdistuneista väärinkäytöksistä henkilötietojen käsittelyssä tulee täysimääräisesti noudattaa henkilötietolain ja työelämän tietosuojalain säännöksiä.

### *3.3 Sähköpostiviestinnän tunnistamistietojen käsittely*

Hallituksen esityksessä 48/2008 vp sähköisen viestinnän tietosuojalain muuttamiseksi on ehdotettu säädettäväksi työnantajille rajoitettu oikeus käsitellä työntekijöiden sähköpostiviestinnän tunnistamistietoja sen selvittämiseksi, ovatko työntekijät luvattomasti paljastaneet yrityssalaisuuksia. Esittelen seuraavassa pääkohdat tästä sääntelystä siten, että käyn läpi työnantajalle tulevia velvoitteita ja oikeuksia niiden käytännön toteuttamisjärjestyksen pohjalta. Tätä kirjoitettaessa käytettävissäni on hallituksen esityksen lisäksi siitä annettu eduskunnan työelämä- ja tasa-arvovaliokunnan lausunto[30], mutta ei vielä muiden valiokuntien kannanottoja, jotka valmistunevat syksyn 2008 kuluessa. Hallituksen esityksessä on ehdotettu lainmuutosten voimaantuloajankohdaksi vuoden 2009 alkua.

Sähköpostiviestinnän tunnistamistietojen käsittelyä *ei* ole ehdotetussa lainsäädännössä tarkoitettu *ensisijaiseksi tavaksi* selvittää yrityssalaisuuksiin kohdistuvia loukkauksia – itse asiassa edellytys lakiehdotuksen mukaisten selvittelyoikeuksien käyttämiselle on, että työnantaja on ensin huolehtinut *muilla keinoilla* yrityssalaisuuksien riittävästä suojaamisesta. Edellä jaksossa 3.2 olen jo viitannut työnantajan käytettävissä oleviin *tietohallinnollisiin valvontatapoihin*. Ehdotetussa sähköisen viestinnän tietosuojalain 13 b §:ssä säädettäisiin erikseen työnantajan eräistä nimenomaisista huolehtimisvelvollisuuksista. Säännöksen mukaan yhteisötilaajan (työnantajan) tulisi ennen tunnistamistietojen käsittelyn aloittamista yrityssalaisuuksien paljastamisen ehkäisemiseksi:

- rajoittaa pääsyä yrityssalaisuuksiin ja ryhtyä muihin toimenpiteisiin tietojen asianmukaiseksi suojaamiseksi; ja
- määritellä, miten yrityssalaisuuksia saa viestintäverkossa siirtää, luovuttaa tai muutoin käsitellä ja minkälaisiin kohdeosoitteisiin yrityssalaisuuksia käsittelemään oikeutetut henkilöt eivät ole oikeutettuja lähettämään viestejä.

Tässä mainituista asioista työnantajan tulisi antaa *kirjalliset ohjeet* viestintäverkon tai viestintäpalvelun käyttäjille, siis käytännössä erityisesti työntekijöilleen. Hallituksen esityksessä todetun mukaisesti noudattamalla näitä ohjeita työntekijä voisi välttyä siltä, että hänen viestintäänsä koskevat tunnistamistiedot tulevat työnantajan tietoon.[31]

Hallituksen esityksessä on korostettu työnantajan velvollisuutta tietoturvallisuusjärjestelyin huolehtia siitä, että työyhteisössä vain tiettyjä tehtäviä hoitavat työntekijät pääsevät yrityssalaisuuksiin käsiksi (ns. *need to know* -lähtökohta). Tämä edellyttää tietojärjestelmien käyttäjähallinnolta asianmukaista suunnittelua ja toteuttamista. Näiden toimenpiteiden – ja yleisemminkin työpaikalla annettavan yrityssalaisuuksien käsittelyohjeistuksen – seurauksena yrityssalaisuuksien kanssa tekemisiin joutuvat työntekijät voivat selkeämmin mieltää, että heidän käsittelemänsä tieto on tarkoitettu luottamukselliseksi eikä sitä saa jakaa vapaasti myöskään työyhteisön sisällä.[32] On ilmeistä, että ehdotettujen sähköisen viestinnän tietosuojalain 13 b §:n mukaisten velvoitteiden huolellinen toteuttaminen tulee useassa yrityksessä johtamaan tietoturvan tason tosiasialliseen parantumiseen.

Työnantajille ei olla säätämässä oikeutta seurata *kaikkien* työntekijöiden sähköpostiviestinnän tunnistamistietoja. Käsittely on sallittua

[30] TyVL 14/2008 vp.
[31] HE 48/2008 vp, s. 21.
[32] Ks. HE 48/2008 vp, s. 22.

kohdistaa vain sellaisten työntekijöiden sähköpostien tunnistamistietoihin, joilla työtehtäviensä puolesta on oikeus käsitellä yrityssalaisuuksia sisältäviä aineistoja (ks. ehdotettu sähköisen viestinnän tietosuojalain 13 e §:n 2 momentti). Tällaisia työntekijöitä ovat tyypillisesti asiantuntija- ja kehitystehtävissä työskentelevät henkilöt. Lisäksi hallituksen esityksessä on viitattu erilaisissa avustavissa tehtävissä työskenteleviin sekä tietojärjestelmien ylläpidosta ja huollosta vastaaviin.[33] Tässä mainittujen työntekijöidenkään sähköpostiviestinnän tunnistamistietoja ei ole kuitenkaan sallittua käsitellä aivan kaikenlaisten yrityssalaisuuksien suojaamisen tarkoituksessa, vaan kysymys tulisi olla ”työnantajan tai sen yhteistyökumppanin elinkeinotoiminnan kannalta keskeisistä yrityssalaisuuksista tai teknologisen tai muun kehittämistoiminnan tuloksista, jotka todennäköisesti ovat merkittäviä elinkeinotoiminnan tai sen harjoittamisen kannalta” (ks. ehdotettu 13 d §:n 3 momentin 2 kohta). Lisäksi on huomattava, että kysymys on vain *tunnistamistietojen* käsittelyoikeudesta – ei oikeudesta avata itse viestejä tai muullakaan tavoin selvittää niiden sisältöä.

Tunnistamistietojen käsittelyoikeus on hallituksen esityksessä ehdotettu jaettavaksi *automaattisen* ja *manuaalisen* käsittelyn oikeuteen. Automaattinen käsittely olisi sallittua suorittaa sellaisen hakutoiminnon avulla, joka perustuu viestien kokoon, yhteenlaskettuun kokoon, tyyppiin, määrään, yhteystapaan tai kohdeosoitteisiin. Automaattista hakutoimintoa käytettäessä tunnistamistiedot eivät tulisi kenenkään ”ihmissilmin” katsottaviksi. Manuaaliseen käsittelyyn työnantajalla olisi oikeus turvautua vasta, jos jokin laissa erikseen määritelty edellytys täyttyy. Sähköisen viestinnän tietosuojalain ehdotetun 13 d §:n 2 momentissa on mainittu viisi tällaista edellytystä (neljä tarkemmin määriteltyä ja yksi yleislauseketyyppinen). Kyseeseen tulisivat lähinnä ”automaattisen hakutoiminnon avulla havaittu poikkeama viestinnässä” (1 kohta) tai olosuhteet, joissa ”yrityssalaisuus julkaistaan tai sitä käytetään luvatta” (4 kohta). Erityisedellytyksen täyttymisen lisäksi vaaditaan, että työnantajalla on perusteltu syy epäillä, että yrityssalaisuus on luvattomasti annettu ulkopuoliselle.

Myös tunnistamistietojen käsittelyä yrityssalaisuuksien suojaamiseksi on tarkoitettu koskemaan sähköisen viestinnän tietosuojalain jo nykyisin voimassa oleva 8 §:n 3 momentti, jossa säädetyn mukaisesti käsittely on sallittua ainoastaan käsittelyn tarkoituksen vaatimassa laajuudessa ja käsittelyllä ei saa rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä. Tarkoitus siis on, että sekä automaattisen että manuaalisen tunnistamistietojen käsittelyn edellytykset tulee harkita työnantajan puolelta aina huolellisesti ja tapauskohtaisesti.[34] Lisäksi sovellettavaksi tulisi ehdotettu sähköisen viestinnän tietosuojalain 13 d §:n 4 momentti, jonka mukaan tunnistamistietojen käsittelyn edellytyksenä on aina, että käsittelyn avulla saatavat tiedot ovat välttämättömiä väärinkäytöksen ja siitä vastuussa olevien selvittämiseksi.

Työntekijöiden oikeussuoja on hallituksen esityksessä ehdotettu turvattavaksi muun muassa työnantajan varsin yksityiskohtaisilla ja laajoilla *menettelyvelvoitteilla*. Ennen tunnistamistietojen käsittelyn aloittamista työnantajan tulisi käsitellä asiaa työelämän tietosuojalain 21 §:n mukaisesti *yhteistoimintamenettelyssä* (ks. ehdotettu sähköisen viestinnän tietosuojalain 13 c §:n 2 momentti). Lisäksi työnantajan tulisi tehdä ryhtymisestään tunnistamistietojen käsittelyyn *ennakollinen ilmoitus tietosuojavaltuutetulle* (ks. ehdotettu lain 13 h §:n 1 momentti). Käytännössä ne asiat, joita yhteistoimintamenettelyssä tulisi käsitellä ja jotka ennakollisesti tulisi ilmoittaa tietosuojavaltuutetulle, ovat hyvin pitkälle samoja. Tietosuojavaltuutetulle tehtävän ennakkoilmoituksen

[33] HE 48/2008 vp, s. 26.
[34] Ks. HE 48/2008 vp, s. 19–20 ja 25–26.

tarkoituksena on osaltaan varmistaa se, että tunnistamistietojen käsittelyyn ei ryhdytä puutteellisen harkinnan tai vaillinaisen suunnittelun pohjalta. Lisäksi ennakollisen ilmoituksen saamisen välityksin tietosuojavaltuutetun mahdollisuudet käytännössä suorittaa hänelle säädettävää valvontatehtävää paranevat.

Jos työnantaja on ottanut työntekijöiden sähköpostiviestinnän tunnistamistietoja manuaalisesti käsiteltäväksi, työnantajan tulisi ehdotetun sähköisen viestinnän tietosuojalain 13 f §:n mukaisesti laatia tästä erillinen *selvitys*, jonka sisällöstä säännöksessä tarkemmin määrätään. Selvityksen tarkoituksena on turvata menettelyn läpinäkyvyys suhteessa työntekijään, jonka sähköpostiviestinnän tunnistamistietoja on manuaalisesti käsitelty. Lisäksi työnantajan tulisi ehdotetun 13 g §:n mukaan antaa *työntekijöiden edustajille vuosittain ilmoitus* tunnistamistietojen manuaalisesta käsittelystä. Vuosittainen ilmoitus työnantajan tulisi ehdotetun 13 h §:n 2 momentin mukaan antaa *myös tietosuojavaltuutetulle*. Kokonaisuutena tunnistamistietojen käsittelyyn liittyvät menettelylliset vaatimukset ovat niin laajat ja yksityiskohtaiset, että ne todennäköisesti varsin hyvin turvaavat työntekijöiden oikeussuojan toteutumisen.

## 4 Keskeisiä tulkintakysymyksiä

### *4.1 Yritysvakoilu vai yrityssalaisuuden rikkominen?*

Edellä jaksossa 1 todetun mukaisesti työntekijälle syntyy tyypillisesti herkimmin tarve työnantajan (tai tämän yhteistyökumppanin) yrityssalaisuuksien luvattomaan hyödyntämiseen tai paljastamiseen nimenomaan silloin, kun työntekijä on siirtymässä tai jo siirtynyt muun työnantajan palvelukseen – tai vaihtoehtoisesti perustamassa tai perustanut oman yrityksen. Sellaiset tapaukset, joissa työntekijä muissa olosuhteissa työsuhteensa aikana luvattomasti paljastaa työnantajansa (tai tämän yhteistyökumppanin) yrityssalaisuuksia *jonkin ulkopuolisen tahon hyödyttämisen tarkoituksessa*, lienevät harvinaisempia. Tällaisissa tapauksissa väärinkäytöksen houkuttimena lienee yleensä se, että yrityssalaisuuksia paljastava työntekijä saa jonkin taloudellisen korvauksen lainvastaisesta toiminnastaan.

Kun yrityssalaisuuden rikkomista koskevan RL 30:5:n soveltamisala vuonna 2003 laajennettiin koskemaan myös työntekijän palvelussuhteen jälkeistä aikaa, tarkoituksena oli puuttua erityisesti työnantajan (tai tämän yhteistyökumppanin) yrityssalaisuuksien ”suoraan” siirtymiseen pois lähtevän työntekijän uudelle työnantajalle tai työntekijän itsensä perustamalle uudelle yritykselle. Keskeisenä tavoitteena oli rangaistavuuden ulottaminen sellaisiin tekoihin, joissa työntekijä järjestelmällisesti työsuhteensa loppuvaiheissa kokoaa yrityssalaisuuksia, ottaa ne mukaansa (paperikopioina tai sähköisessä muodossa) ja sitten siirtää ne tavalla tai toisella kilpailevassa liiketoiminnassa käytettäviksi.[35] Yhtenä esimerkkitapauksena oli esillä menettely, jossa työntekijä työsuhteensa loppuvaiheissa ensin lähettää yrityssalaisuuksia sisältäviä tiedostoja *sähköpostitse itselleen* yksityiseen sähköpostiosoitteeseensa ja sitten, työsuhteensa päätyttyä, ottaa näin hankkimansa tiedostot kilpailevassa liiketoiminnassa käyttöön.[36]

Nykyisin voimassa olevan RL 30:5:n pohjalta on selvää, että jos kuvatunlaisesta menettelystä kertyy näyttöä kaikilta osin – siis myös tietojen myöhemmän *käyttämisen tai ilmaisemisen* osalta – edellytykset teon rangaistavuudelle ovat käsillä. Ongelmia kuitenkin aiheutuu – aikaisemman työnantajan näkökulmasta –, jos näyttö yrityssalaisuuksien käyttämisestä tai ilmaisemisesta jää joko puuttumaan kokonaan tai ainakin huomattavan niukaksi. Kun sovellettavana on yrityssalai-

[35] Ks. HE 53/2002 vp, s. 16 ja 32.
[36] Ks. *Viljanen*, s. 432.

suuden oikeudetonta ilmaisemista tai käyttämistä koskeva RL 30:5, ei tältä osin puutteelliseksi jäävää näyttöä voida korvata esittämällä näyttöä siitä, miten laajalti työntekijä on *kopioinut* luottamuksellista aineistoa mukaansa. Tästä kertyvä näyttö voi toki olla osoitus teon suunnitelmallisuudesta ja myös siitä, että tiedoissa on kysymys toiselle kuuluvista yrityssalaisuuksista eikä työntekijän omasta ammattitaidosta, mutta se ei kuitenkaan vähennä näyttövelvollisuutta itse tietojen käyttämisestä tai ilmaisemisesta.[37]

Asetelma on tulkinnallisesti erilainen, jos kuvatunlainen menettely voidaan katsoa RL 30:4:n mukaiseksi *yritysvakoiluksi* – toisin sanoen, jos työntekijän aktiivinen, muistinvahvistamistarkoituksessa suorittama systemaattinen *tiedonhankinta* voidaan jo sellaisenaan katsoa rangaistavaksi. Epävarmuutta ei ole sen suhteen, etteikö kuvatunlaisessa menettelyssä ilman muuta täyttyisi yritysvakoilusäännöksen *tekotapaa* koskeva tunnusmerkki (= yrityssalaisuuden hankkiminen tietoon ”hankkimalla haltuun tai jäljentämällä asiakirja tai muu tallenne taikka muulla siihen rinnastettavalla tavalla”). Keskeinen kysymys on kuitenkin se, onko teko RL 30:4:n tarkoittamalla tavalla *oikeudeton* – ottaen huomioon sen, että asianomaisella työntekijällä on ollut osana työtehtäviään oikeus käsitellä kyseisiä yrityssalaisuuksia. Koska tämän kysymyksenasettelun osalta on oikeuskirjallisuudessa jo käyty yksityiskohtaista keskustelua, en tässä artikkelissa arvioi asiaa erikseen.[38]

Nostan sitä vastoin esille yhden näkökulman, joka olennaisesti liittyy jäljempänä jaksossa 4.2 tarkasteltavaan työntekijöiden sähköpostiviestinnän tunnistamistietojen käsittelemiseen yrityssalaisuuksien luvatonta paljastamista epäiltäessä. Ehdotetuissa sähköisen viestinnän tietosuojalain uusissa 13 a–13 j §:ssä tunnistamistietojen käsittelyoikeutta ei ole sinänsä sidottu nimenomaisiin RL 30 luvun (tai RL 38 luvun, jossa säädetään salassapitorikoksesta ja -rikkomuksesta) tunnusmerkistöihin, mutta niiden mukaisten oikeuksien käyttämisessä on kuitenkin syytä jäsentää se, millaiset teot ovat yrityssalaisuuksien *hankkimista* ja millaiset puolestaan yrityssalaisuuksien *ilmaisemista* – tai tällaisen teon *valmistelemista*. Se, että työntekijä kopioi itselleen yrityssalaisuuksia sisältäviä tallenteita tai *siirtää* niitä *itselleen*, esimerkiksi yksityiseen sähköpostiosoitteeseensa, ei vielä sellaisenaan ole yrityssalaisuuden *ilmaisemista toiselle*.

### *4.2 Millaisten yrityssalaisuuteen kohdistuvien loukkausten selvittämiseksi sähköpostien tunnistamistietoja saa käsitellä?*

Ehdotetun sähköisen viestinnän tietosuojalain 13 a §:n mukaisesti yhteisötilaajalle (työnantajalle) on tulossa oikeus käsitellä tunnistamistietoja *yrityssalaisuuksien paljastamisen selvittämiseksi* siten kuin lain 13 b–13 j §:ssä säädetään. Ehdotetun 13 b §:n mukaan yhteisötilaajan (työnantajan) etukäteinen huolehtimisvelvollisuus niin ikään koskee sellaisia tietoturvallisuustoimenpiteitä, joilla pyritään ehkäisemään yrityssalaisuuksien paljastamista. Myös ehdotetuissa 13 d ja 13 e §:ssä, joissa tarkemmin säädetään tunnistamistietojen käsittelyoikeuden edellytyksistä ja niiden rajoituksista, säännösten sanamuodot viittaavat tapauksiin, joissa yrityssalaisuus on ilmaistu ulkopuoliselle: ”perusteltu syy epäillä, että yrityssalaisuus on luvattomasti annettu ulkopuoliselle”, ”epäilty yrityssalaisuuden paljastaminen” ja ”yrityssalaisuuden paljastamisen selvittäminen”.

Toisaalta – kuten edellä on jo mainittu – ehdotettuja sähköisen viestinnän tietosuojalain 13 a–13 j §:n mukaisia käsittelyoikeuksia ei ole sidottu nimenomaisesti siihen, että epäillyn rikoksen tulisi olla juuri RL 30:5:n mukainen *yri-*

[37] Toisenlainen – ja samalla käsitykseni mukaan myös ilmeisen virheellinen – lähestymistapa on omaksuttu yhdessä Vaasan hovioikeuden ratkaisussa, 14.11.1996, dnro R 96/109. Ks. yksityiskohtaisemmin *Nyblin* 2007, s. 276.

[38] Käydystä keskustelusta ks. *Nyblin* 2007, s. 262–265 ja siinä viitattu kirjallisuus.

*tyssalaisuuden rikkominen*. On selvää, että tunnistamistietojen käsittelyoikeus voi tulla kysymykseen myös esimerkiksi silloin, kun se yrityssalaisuuksiin kohdistunut loukkaus, jota ollaan selvittämässä, täyttäisi (vain) RL 38 luvun 1 §:n mukaisen *salassapitorikoksen* tai saman luvun 2 §:n mukaisen *salassapitorikkomuksen* tunnusmerkistön.[39] Sen sijaan näyttäisi ilmeiseltä, että ehdotettu tunnistamistietojen käsittelyoikeus ei – ottaen huomioon edellä viitatut säännösten sanamuodot – tulisi kyseeseen silloin, kun epäillään, että yrityssalaisuuksia on *hankittu* oikeudettomasti. Tämä onkin siinä mielessä johdonmukaista, että tunnistamistietojen käsittelyoikeus on ylipäänsä tarkoitettu kohdistettavaksi vain sellaisten työntekijöiden sähköpostien tunnistamistietoihin, joille työnantaja on näiden työtehtävien perusteella antanut pääsyn yrityssalaisuuksia sisältäviin aineistoihin.

Käytännössä työnantajien näkökulmasta vahingollisimmat yrityssalaisuuksia sisältävien aineistojen luvattomat siirtämiset ovat kuitenkin yleensä liittyneet tapauksiin, joissa työpaikkaa vaihtava tai oman yrityksen perustanut työntekijä on kopioinut ja siirtänyt tällaisia aineistoja itselleen. Työntekijä on esimerkiksi lähettänyt yrityssalaisuuksia sisältäviä tiedostoja sähköpostitse itselleen omaan webmail-sähköpostiosoitteeseensa. Ehdotettuja uusia sähköisen viestinnän tietosuojalain säännöksiä tarkasteltaessa nouseekin esille kysymys siitä, ovatko työnantajat nyt saamassa sähköpostien tunnistamistietojen käsittelyoikeuden myös tällaisia tapauksia silmällä pitäen – epäselvyyttähän ei ole sen suhteen, etteivätkö työnantajat varsin laajalti mieltäisi, että kuvatunlaisessa toiminnassa on kysymys heidän yrityssalaisuuksiinsa kohdistuvasta *väärinkäytöksestä*.

Ehdotetun sähköisen viestinnän tietosuojalain 13 b §:n (*Yhteisötilaajan huolehtimisvelvollisuus väärinkäytöstapauksissa*) 2 momentin 2 kohdan mukaan työnantajien tulee ennen tunnistamistietojen käsittelyn aloittamista yrityssalaisuuksien paljastamisen ehkäisemiseksi ”määritellä, miten yrityssalaisuuksia saa viestintäverkossa siirtää, luovuttaa tai muutoin käsitellä ja *minkälaisiin kohdeosoitteisiin* yrityssalaisuuksia käsittelemään oikeutetut henkilöt *eivät ole oikeutettuja lähettämään viestejä*.” Hallituksen esityksessä on todettu kiellettyjen kohdeosoitteiden osalta, että nämä voitaisiin määritellä ”kohtuullisen yleisellä tasolla”.[40] On todennäköistä, että suuressa osassa yrityksiä, joissa ehdotetut tunnistamistietojen käsittelyoikeudet otetaan käyttöön, määritellään kielletyiksi kohdeosoitteiksi muun muassa kaikki ilmaiset webmail-osoitteet. Mielenkiintoinen asetelma saattaakin muodostua, jos ehdotetun sähköisen viestinnän tietosuojalain 13 d §:n mukaisen automaattisen hakutoiminnon käyttämisessä tulee käytännössä ilmi esimerkiksi sellainen tieto, että yrityksestä on tietyn päivän aikana lähetetty vaikkapa 100 sähköpostiviestiä johonkin tiettyyn ilmaiseen webmail-osoitteeseen.

Kuvatunlaisessa asetelmassa on selvää, että kysymyksessä olisi ehdotetun sähköisen viestinnän tietosuojalain 13 d §:n 2 momentin 1 kohdan mukainen ”automaattisen hakutoiminnon avulla havaittu poikkeama viestinnässä”. Poikkeamaa voisi ehkä vielä vahvistaa se, jos viestien liitetiedostot olisivat kooltaan suuria. Tällaisen poikkeaman perusteella voisikin perustellusti herätä kysymys, ovatko tunnistamistietojen *manuaalisen käsittelemisen* edellytykset siis syntyneet. Tulkinnanvaraiseksi asian tekee se, että yksinomaan poikkeaman havaitseminen ei ehdotetun säännöksen sanamuodon mukaan vielä riitä – tarvitaan *myös* se, että työnantajalle on syntynyt ”perusteltu syy epäillä, että yrityssalaisuus on luvattomasti annettu ulkopuoliselle”. Ongelmalliseksi arvioinnin tekee se, että mainitun ”yleisen edellytyksen” ja ”erityisen edellytyksen” (esimerkiksi poikkeama viestinnässä) välinen suhde on jäänyt hallituksen esityksen säännösehdotukses-

[39] Näistä tunnusmerkistöistä tarkemmin – suhteessa RL 30:5:een – ks. *Nyblin* 2007, s. 256.
[40] HE 48/2008 vp, s. 22.

sa hieman tulkinnanvaraiseksi. Mielestäni näyttää jäävän jossain määrin epäselväksi, tulisiko kyseisten edellytysten täyttyä *toisistaan erillään* vai voitaisiinko lähteä esimerkiksi siitä, että merkittävä poikkeama viestinnässä jo *sellaisenaan* luo perustellun epäilyn siitä, että yrityssalaisuus on annettu luvattomasti ulkopuoliselle.

Riippumatta vastauksesta juuri kuvattuun kysymyksenasetteluun jää jäljelle kuitenkin myös toinen tulkintaongelma: Jos työnantaja katsoo, että edellytykset tunnistamistietojen manuaaliselle käsittelemiselle ovat tapauksessa syntyneet, on mahdollista, että tietojen myöhemmässä manuaalisessa käsittelemisessä tulee ilmi, että kaikki kiellettyyn webmail-osoitteeseen lähetetyt viestit ovat peräisin samalta työntekijältä – ja kyseinen webmail-osoite itse asiassa näyttäisi olevan juuri tämän saman työntekijän oma yksityinen osoite. Jos kysymys lisäksi on sellaisesta työntekijästä, joka samoihin aikoihin on ollut siirtymässä kilpailevan yrityksen palvelukseen, asetelma näyttäisi työnantajan puolelta varsin huolestuttavalta – olosuhteiden perusteella näyttäisi nimittäin varsin todennäköiseltä, että asianomainen työntekijä on ollut kokoamassa dokumentoidussa muodossa itselleen yrityssalaisuuksia siirrettäväksi mahdollisesti myöhemmin edelleen kyseiseen toiseen yritykseen siellä hyödynnettäviksi.

Kuvatunlaisessa asetelmassa on kuitenkin tulkinnanvaraista, onko työntekijä pelkästään lähettämällä yksityiseen sähköpostiosoitteeseensa 100 (mahdollisesti erittäin merkittäviä yrityssalaisuuksia sisältävää) sähköpostiviestiä vielä syyllistynyt mihinkään sellaiseen tekoon, joka olisi RL 30 luvun säännöksissä tarkoitettu yrityssalaisuusrikos. Ilmeistä kuitenkin on, että mainittu teko ei vielä sellaisenaan – siis siinä tapauksessa, että kyseinen sähköpostiosoite selvästikin on työntekijän oma osoite – ole vielä minkäänlainen osoitus siitä, että yrityssalaisuuksia olisi luvattomasti *annettu ulkopuoliselle*. Mahdollista toki on, että teon olosuhteiden perusteella voidaan katsoa todennäköiseksi, että työntekijä myöhemmin tulisi saattamaan (tai on ehkä jo saattanutkin) yrityssalaisuudet myös jonkun ulkopuolisen tietoon.

Ehdotetussa sähköisen viestinnän tietosuojalain 13 j §:ssä säädetään ”yhteisötilaajan oikeudesta tietojen luovuttamiseen väärinkäytöstapauksissa”. Ehdotetun säännöksen mukaan yhteisötilaajalla olisi sen estämättä, mitä lain 8 §:n 3 momentissa säädetään, oikeus luovuttaa asianomistajana tekemänsä rikosilmoituksen tai tutkintapyynnön yhteydessä poliisille käsiteltäviksi lain 13 a–13 i §:n mukaisesti saamaansa yhteisötilaajan viestintäverkon tai viestintäpalvelun käyttäjän viestejä koskevat tunnistamistiedot.[41] Säännöksessä ei ole rajattu sitä, *minkä epäilemänsä rikoksen* ilmoittamisen tueksi yhteisötilaaja (työnantaja) olisi oikeutettu viestejä koskevat tiedot poliisille luovuttamaan. Toisin sanoen, jos työnantaja olisi tunnistamistietojen manuaalisen käsittelemisen perusteella päätynyt epäilemään esimerkiksi *yritysvakoilua* tai vaihtoehtoisesti sitä, että *valmisteilla* näyttäisi olevan (myöhemmin ehkä toteutettava) *yrityssalaisuuden rikkominen*, olisiko työnantaja

[41] HE:ssä 48/2008 vp on todettu säännöksen yksityiskohtaisten perustelujen yhteydessä mm. seuraavaa (s. 28; kursivointi tässä): ”Säännösehdotuksen muotoilussa on otettu huomioon se, että se *oikeuttaisi myös poliisin* käsittelemään näin saamiaan tietoja.” Arvioni on, että tämä perustelulausuma enemmänkin aiheuttaa tulkintaongelmia kuin ratkaisee niitä. Käytännössä nimittäin näyttää siltä, että esitutkinnassa on varsin yleisesti jo omaksuttu lähtökohta, jonka mukaan poliisilla on oikeus – ilman, että laissa on tästä erityistä säännöstä – tutkia sellaisia sähköisiä viestejä, jotka se saa haltuunsa sille annettujen päätelaitteiden (matkapuhelimet, tietokoneet ym.) välityksin. Samaa lähtökohtaa on käsitykseni mukaan noudatettu myös tapauksissa, joissa poliisi on takavarikoinut päätelaitteita epäillyn hallusta – esimerkiksi sähköpostien ja puhelutietojen tällä tavoin tapahtuvaan selvittämiseen ei ole katsottu tarvittavan pakkokeinolain 5 a luvun mukaista tuomioistuimen lupaa. Kun siis HE:ssä 48/2008 vp nyt nimenomaisesti lausutaan, että ehdotetun sähköisen viestinnän tietosuojalain 13 j §:n nojalla poliisi *saa oikeuden* tutkia sähköisiä viestejä, vastattavaksi jää kysymys siitä, ovatko tutkimisoikeudet tähän asti siis puuttuneet – ja tulevatko ne *edelleen puuttumaan* muunlaisissa tapauksissa. Asiaan liittyvästä kysymyksenasettelusta ks. *Klaus Helminen – Kari Lehtola – Pertti Virolainen*, Esitutkinta ja pakkokeinot, 2., uudistettu painos, Helsinki 2005, s. 690.

oikeutettu luovuttamaan viestejä koskevat tiedot poliisille?

Ottaen huomioon sen, että ehdotetussa sähköisen viestinnän tietosuojalain 13 a §:ssä on määritelty 13 b–13 j §:n mukainen tunnistamistietojen käsittelyoikeus koskemaan vain sellaisia tarkoituksia, jotka liittyvät *yrityssalaisuuksien paljastamisen selvittämiseen*, vastaus kysymykseen näyttäisi olevan kielteinen. Kun ehdotetuissa säännöksissä mitä ilmeisimmin on tarkoitettu antaa työnantajille lisävälineitä vain yrityssalaisuuksien luvattomien *paljastamisten* (jotka tyypillisesti täyttävät joko RL 30:5:n mukaisen *yrityssalaisuuden rikkomisen* tai RL 38:1–2:n mukaisten *salassapitorikoksen tai -rikkomuksen* tunnusmerkistön) selvittämiseen, näyttäisi siltä, että oikeus epäiltyjen yritysvakoilutekojen ja myös yrityssalaisuuden paljastamista *valmistelevien* tekojen selvittämiseen on jäämässä säännösten soveltamisalan ulkopuolelle. Eri asia on luonnollisesti se, onko tällainen soveltamisalan rajaus sellainen, mitä säännöksiä valmisteltaessa on tavoiteltukin – vai onko kysymys siitä, että asiaa ei ole vain tarkemmin pohdittu.

## 5 Kokoavia näkökohtia

Hallituksen esitys 48/2008 vp sähköisen viestinnän tietosuojalain säännösten muuttamiseksi on herättänyt julkisuudessa suurta mielenkiintoa. Esillä olleissa puheenvuoroissa on muun ohella arvuuteltu sitä, miten merkittävässä osassa yrityssalaisuuksien vuotamisia työnantajien uusilla selvittelyvaltuuksilla tulisi käytännössä olemaan merkitystä. Kriittisissä puheenvuoroissa on korostettu sitä, että työntekijät, jotka haluavat paljastaa työnantajansa yrityssalaisuuksia, kyllä löytävät menettelylleen muitakin keinoja kuin sähköpostien lähettämisen. Käytännössä näyttäisi kuitenkin siltä, että melko monessa yrityssalaisuuksia loukanneessa teossa tekijät eivät ole kovin hyvin ”peittäneet jälkiään”. Työnantajille ehdotetut sähköpostin tunnistamistietojen käsittelyoikeudet siis todennäköisesti tulevat johtamaan siihen, että joitakin sellaisia yrityssalaisuuksien paljastamisia, jotka muuten eivät tulisi ilmi, saadaan esitutkintaan arvioitaviksi.

Poissuljettua ei ole sekään, että *myös työnantajien menettelyjä* yrityssalaisuusrikosepäilyjen selvittämisessä päätyy poliisin tutkittavaksi. Ehdotetut sähköisen viestinnän tietosuojalain uudet säännökset sisältävät varsin yksityiskohtaisia menettelyllisiä velvoitteita työnantajille – ja näiden velvoitteiden rikkominen ollaan myös säätämässä rangaistavaksi. Tapauksissa, joissa työnantaja käynnistää oikeudellisia toimenpiteitä työntekijäänsä kohtaan sähköpostien tunnistamistietojen manuaalisessa käsittelyssä esille tulleiden seikkojen perusteella, on hyvinkin mahdollista, että asianomainen työntekijä itse haluaa selvityttää myös sen, onko työnantaja menetellyt lainmukaisesti. Sellaisten työnantajien, jotka aikovat ottaa käyttöön uusien säännösten mahdollistaman sähköpostien tunnistamistietojen käsittelyoikeuden, on siten syytä huolellisesti varmistua siitä, että käyttöön otettavat prosessit ovat lain edellyttämällä tasolla ja myös prosesseihin osallistuvat henkilöt ovat perillä lain säännösten sisällöstä.

*Klaus Nyblin*