FiCom ry

Lausunto

18.06.2026

Asia: VN/10660/2026

Lausuntopyyntö yhteisötilaajasääntelystä ja muista sähköisen viestinnän tietosuojadirektiivin kansallisista laajennuksista

1 Yleisiä kysymyksiä SVPL:n yhteisötilaajia ja sijaintitietojen käsittelyä koskevasta sääntelystä

1.1 Pidättekö SVPL:n yhteisötilaajia ja muita viestinnän välittäjiä sekä sijaintitietojen suojaa koskeva sääntelyä yleisesti ottaen sisällöltään ja soveltamisalaltaan asianmukaisena, kun otetaan huomioon nykyinen toimintaympäristö ja muu soveltuva kansallinen ja EU-lainsäädäntö?

FiCom ei pidä sääntelyä kaikilta osin asianmukaisena. Sääntelyn tavoite eli viestinnän luottamuksellisuuden suoja on edelleen tärkeä ja perusteltu, eikä FiCom esitä tämän suojan heikentämistä.

Ongelma ei ole yksittäisessä säännöksessä, vaan siinä, että kokonaisuus on rakentunut aikana, jolloin organisaatioiden teknologinen ja sääntely-ympäristö oli nykyistä yksinkertaisempi. Sittemmin sääntely-ympäristö on muuttunut olennaisesti muun muassa yleisen tietosuoja-asetuksen ja uudemman kyberturvallisuutta koskevan sääntelyn myötä.

Tähän nähden kansallinen erityissääntely on paikoin päällekkäistä, tulkinnanvaraista ja nykyisiin toimintamalleihin nähden jäykkää. Kansallista lisäsääntelyä tulee keventää ja päällekkäisyyksiä karsia siten, että viestinnän luottamuksellisuuden ja henkilötietojen suojan korkea taso säilyy.

1.2 Liittyykö SVPL:n ePrivacy-direktiiviä täydentävään sääntelyyn mielestänne piirteitä, jotka eivät asianmukaisesti huomioi nykyistä kyberturvallisuuden toimintaympäristöä, uusien digitaalisten palveluiden käytön ja tarjonnan muotoja tai uudempaa muuta kansallista ja EU-sääntelyä?

Kyllä. Sääntely on suurelta osin laadittu ennen nykyistä pilvi-, ohjelmisto- ja kyberturvallisuusympäristöä sekä ennen yleisen tietosuoja-asetuksen ja uudemman kyberturvallisuussääntelyn voimaantuloa.

Käytännössä sääntely soveltuu huonosti tilanteisiin, joissa viestintä-, tietoturva- ja hallintaratkaisut tuotetaan keskitetysti pilvi- tai konserniympäristössä ja samoja järjestelmiä käytetään useissa maissa.

1.3 Millaisia vaikutuksia SVPL:n ePrivacy-direktiiviä täydentävällä sääntelyllä on käsityksenne mukaan ollut käyttäjien yksityisyyden suojalle? Onko sääntely toteuttanut yksityisyyden ja henkilötietojen suojaa mielestänne tarkoituksenmukaisella tavalla?

Yleinen tietosuoja-asetus muodostaa nykyisin henkilötietojen käsittelyä koskevan yleisen sääntelykehyksen koko EU:ssa. Se ei kuitenkaan poista tarvetta suojata viestinnän luottamuksellisuutta. Kansallisen erityissääntelyn tulisi kohdistua vain tilanteisiin, joissa ePrivacy-sääntelyn ja perusoikeuksien näkökulmasta on aidosti tarpeen säätää täydentävistä erityisvaatimuksista.

Nykyisen kansallisen erityiskerroksen tuottama lisähyöty yksityisyyden suojalle jää monilta osin epäselväksi suhteessa sen aiheuttamaan tulkinnanvaraan ja hallinnolliseen monimutkaisuuteen. Käyttäjien suoja toteutuu parhaiten silloin, kun sääntely on ymmärrettävää, teknisesti toteuttamiskelpoista ja yhteensopivaa muun sovellettavan lainsäädännön kanssa.

2 Kyberturvallisuuden riskienhallinta ja viestinnän ja välitystietojen käsittely

2.1 Pidättekö SVPL:n ePrivacy-direktiiviä täydentävää sääntelyä tarkoituksenmukaisena siltä osin kuin se sääntelee sellaista välitystietojen ja viestien käsittelyä, joka liittyy erilaisilta kyberuhkilta suojautumiseen? Millaisia vaikutuksia tällä sääntelyllä on ollut organisaatioiden ja käyttäjien kyberturvallisuuteen? Onko sääntely mielestänne mahdollistanut kyberturvallisuuden riskienhallinnan tarkoituksenmukaisella tavalla vai aiheuttanut sille rajoituksia?

FiCom ei pidä sääntelyä kaikilta osin tarkoituksenmukaisena. Välitystietojen ja viestien käsittelyä koskevat kansalliset rajoitukset vaikeuttavat perusteltujen kyberturvallisuustoimenpiteiden suunnittelua ja käyttöönottoa erityisesti silloin, kun samoja ratkaisuja käytetään konserni- tai pilviympäristössä useissa maissa. Samaan aikaan NIS2-sääntely ja muu uudempi sääntely edellyttävät organisaatioilta tehokkaita kyberturvallisuuden riskienhallintatoimenpiteitä.

Sääntelyn tulisi tukea kyberturvallisuuden riskienhallintaa eikä asettaa sille kansallisia lisäesteitä. Tarpeelliset, oikeasuhtaiset ja dokumentoidut tietoturvatoimet pitäisi voida toteuttaa selkeän sääntelykehyksen puitteissa. Sama koskee viestintäpalveluihin, verkkoihin ja käyttäjiin kohdistuvien petosten, väärinkäytösten ja huijausviestinnän ehkäisyä, havaitsemista ja torjuntaa silloin, kun toimenpiteet edellyttävät välitystietojen käsittelyä.

Tämä ei ole vain organisaatioiden hallinnollinen kysymys. Jos kyberuhkien havaitsemista, torjuntaa ja selvittämistä koskeva oikeustila on epäselvä, myös käyttäjien suoja voi käytännössä heikentyä tai ainakin jäädä hitaammin kehittyvien suojatoimien varaan.

2.2 SVPL 18 luvun (ns. Lex Nokia) mukaisia toimenpiteitä on käytetty vähemmän, kuin sääntelyn valmistelussa aikanaan ennakoitiin. Millaisia syitä arvioitte olevan sen taustalla, ettei toimenpiteitä ole

otettu käyttöön? (SVPL 18 luvussa säädetään yhteisötilaajan oikeudesta käsitellä tietyin edellytyksin välitystietoja maksullisen tietoyhteiskunnan palvelun, viestintäverkon tai viestintäpalvelun luvattoman käytön taikka liikesalaisuuksien paljastamisen ehkäisemiseksi ja selvittämiseksi.)

Keskeinen syy on menettelyn raskaus ja epävarmuus. Käsittelyn edellytykset ovat tiukat, ja menettelyyn liittyy useita ennakollisia velvoitteita, kuten käsittelystä päättäminen, käytäntöjen määrittely, henkilöstön informointi ja yhteistoimintamenettely sekä ennakkoilmoitus ja vuosittainen selvitys tietosuojavaltuutetulle.

Lisäksi 18 luvun suhde yleiseen tietosuoja-asetukseen ja työelämän tietosuojalakiin on tulkinnanvarainen. Organisaatio voi joutua arvioimaan erikseen yleisen tietosuoja-asetuksen käsittelyperusteet, työelämän tietosuojalain vaatimukset ja SVPL:n 18 luvun erityisedellytykset. Tämä selittää osaltaan, miksi menettelyä on käytetty vähän: jos sääntelyn hyöty jää epäselväksi, mutta sen käyttöönotto edellyttää raskaita ennakkotoimia, organisaatioilla ei ole käytännössä vahvaa kannustinta turvautua menettelyyn.

2.3 Voiko SVPL:n tietoturvatoimenpiteistä säätävän 272 §:n ja SVPL 18 luvun muun muassa liikesalaisuuksien paljastamisen selvittämistä koskevan sääntelyn (Lex Nokia) suhde aiheuttaa mielestänne soveltamishaasteita? Millaisia?

Tietoturvatoimenpiteistä säätävän 272 §:n ja 18 luvun mukaisen menettelyn suhde voi aiheuttaa soveltamishaasteita, sillä niiden soveltamisalat ovat osin lähellä toisiaan, mutta niiden edellytykset poikkeavat toisistaan. Rajanveto siitä, milloin kyse on sallitusta tietoturvatoimenpiteestä ja milloin 18 luvun mukaisesta välitystietojen käsittelystä, on epäselvä.

Tulkintahaaste voi ilmetä esimerkiksi tilanteessa, jossa sama lokitieto tai välitystieto on merkityksellinen sekä tietoturvapoikkeaman selvittämiseksi että väärinkäytöksen tai liikesalaisuuden paljastamisen arvioimiseksi. Tällöin organisaation on vaikea ennakoida, mitä menettelyä sen tulisi noudattaa ja missä vaiheessa käsittely siirtyy 272 §:n mukaisesta tietoturvatoimesta 18 luvun erityismenettelyn piiriin. Tämä tekee oikeustilasta ennakoimattoman.

2.4 Voiko SVPL:n ePrivacy-direktiiviä täydentävä sääntely estää organisaatioita käyttämästä viestinnän tai välitystietojen käsittelyä edellyttäviä riskienhallintatoimenpiteitä, jotka olisivat käsityksenne mukaan perusteltuja ja muun soveltuvan lainsäädännön mukaisia, tai rajoittaa niiden käyttöä? Mitä toimenpiteitä? Mistä SVPL:n vaatimuksesta tämä johtuu? Onko SVPL:n sääntely asettanut teille esteitä tai rajoituksia tällaisten toimenpiteiden käyttöön?

Sääntely voi estää tai rajoittaa perusteltuja ja muun lainsäädännön mukaisia riskienhallintatoimenpiteitä. Käytännössä kyse voi olla esimerkiksi keskitetystä lokienhallinnasta, haitallisen liikenteen tunnistamisesta, tietovuotojen estämisestä, petosten ja huijausviestien estämisestä tai siitä, että konsernin yhteistä sähköposti- ja päätelaiteturvaa ei voida ottaa Suomessa käyttöön samalla tavalla kuin muissa toimintamaissa.

Ongelma konkretisoituu esimerkiksi silloin, kun konsernissa on käytössä yhteinen lokienhallinta- tai tietovuotojen estämisratkaisu, joka on rakennettu yleisen tietosuoja-asetuksen ja tavanomaisten kyberturvallisuusvaatimusten pohjalta. Suomessa sama ratkaisu voi edellyttää erillistä SVPL-

arviointia, vaikka sen käyttötarkoitus olisi perusteltu ja muualla konsernissa jo hyväksytty. Esteet ja rajoitukset johtuvat ennen kaikkea välitystietojen ja viestien käsittelyä koskevista käyttötarkoitus- ja menettelyvaatimuksista sekä siitä, että sallitut käsittelytilanteet on määritelty kansallisessa sääntelyssä kapeasti.

3 Muu kuin kyberturvallisuuden riskienhallintaan liittyvä välitystietojen ja viestinnän käsittely

3.1 Pidättekö SVPL:n ePrivacy-direktiiviä täydentävää välitystietojen ja viestinnän käsittelyn sääntelyä tarkoituksenmukaisena siltä osin kuin tietojen käsittely liittyy muuhun kuin erilaisilta kyberuhkilta suojautumiseen? Onko sääntelyn mahdollistamat käsittelytilanteet määritelty tarkoituksenmukaisesti?

Sääntelyn mahdollistamat käsittelytilanteet on määritelty kapeasti ja osin epäselvästi, eikä sääntely jousta nykyisten käyttötarpeiden mukaan. Esimerkiksi viestintäjärjestelmien käytön valvonnan osalta sääntely on jäykkää ja limittyy työelämän tietosuojalain ja yleisen tietosuoja-asetuksen kanssa.

Sääntelyä tulisi arvioida niin, etteivät organisaatioiden tavanomainen järjestelmien hallinta, väärinkäytösten ehkäisy ja käytön valvonta tarpeettomasti esty, kun käsittely on yleisen tietosuoja-asetuksen ja työelämän tietosuojalain mukaista. Nykyinen epäselvyys heikentää oikeusvarmuutta.

3.2 Onko ja millä tavoin SVPL:n sääntely edistänyt tai tukenut sellaisten muiden viestinnän tai välitystietojen käsittelyä edellyttävien toimenpiteiden käyttöönottoa, jotka eivät liity kyberuhkien torjumiseen? Millaisten toimenpiteiden?

FiComin tiedossa ei ole, että kansallinen erityissääntely olisi edistänyt tällaisten toimenpiteiden käyttöönottoa. Käytännössä sääntely on pikemminkin lisännyt epävarmuutta siitä, milloin organisaatio voi toteuttaa perusteltuja ja muuhun lainsäädäntöön perustuvia valvonta- tai selvittämistoimia. Sääntelyn lisähyöty jää tältä osin epäselväksi suhteessa sen aiheuttamaan hallinnolliseen taakkaan ja tulkinnanvaraan.

3.3 Voiko SVPL:n sääntely mielestänne estää ottamasta käyttöön viestinnän tai välitystietojen käsittelyä edellyttäviä toimenpiteitä, jotka eivät liity kyberuhkien torjumiseen mutta olisivat käsityksenne perusteltuja ja muun soveltuvan lainsäädännön mukaisia, tai rajoittaa niiden käyttöä? Mitä toimenpiteitä? Mikä lainsäädännön vaatimus voi muodostua esteeksi? Onko SVPL:n sääntely estänyt teitä ottamasta jotakin tällaista toimenpidettä käyttöön?

Sääntely voi estää tai rajoittaa myös perusteltuja ja muun lainsäädännön mukaisia toimenpiteitä, jotka eivät liity kyberuhkien torjuntaan. Sama välitystietojen ja viestien käsittelyä koskeva kansallinen erityissääntely, joka rajoittaa kyberturvallisuustoimenpiteitä, voi rajoittaa myös esimerkiksi viestintäjärjestelmien asianmukaisen käytön valvontaa.

Esteeksi muodostuvat ennen kaikkea käsittelytilanteiden suppea määrittely ja menettelyvaatimukset. Tämä voi tehdä toimenpiteen toteuttamisesta epävarmaa tai suhteettoman raskasta myös silloin, kun sille olisi yleisen tietosuoja-asetuksen mukainen oikeusperuste ja hyväksyttävä tarkoitus.

FiComilla ei ole käytettävissään kattavaa organisaatiokohtaista selvitystä yksittäisistä käyttöönottotilanteista. Toimialan näkökulmasta sääntelyn ongelma on kuitenkin juuri se, että epäselvä oikeustila voi johtaa perusteltujenkin toimenpiteiden lykkäämiseen, rajaamiseen tai toteuttamatta jättämiseen.

4 Hallinnollinen taakka ja lisäkustannukset sekä rajat ylittävät tilanteet

4.1 Millaisia hallinnollisia vaikutuksia SVPL:n ePrivacy-direktiiviä täydentävällä sääntelyllä on ollut organisaatioiden ja käyttäjien kannalta? Pidättekö sääntelyä tarkoituksenmukaisena tältä kannalta vai onko sääntely aiheuttanut mielestänne tarpeetonta hallinnollista taakkaa?

Sääntely aiheuttaa tarpeetonta hallinnollista taakkaa. Yhteisötilaajien on noudatettava yleisen tietosuoja-asetuksen velvoitteiden lisäksi kansallisia erityisvaatimuksia, jotka voivat edellyttää erillistä dokumentaatiota, ennakollisia menettelyjä ja tietyissä tilanteissa myös ilmoituksia viranomaiselle. Päällekkäisyys lisää työtä ja oikeudellisen arvioinnin tarvetta ilman vastaavaa lisähyötyä.

Käytännössä taakka näkyy esimerkiksi siinä, että samoista järjestelmistä ja menettelyistä joudutaan laatimaan erillisiä Suomen-arviointeja, vaikka ratkaisut olisi jo suunniteltu yleisen tietosuoja-asetuksen ja konsernin yhteisten tietoturvavaatimusten mukaisesti.

Käyttäjien kannalta hallinnollinen lisäkerros ei välttämättä näy parempana suojana, vaan voi pikemminkin vaikeuttaa selkeiden ja tehokkaiden tietoturva- ja riskienhallintakäytäntöjen toteuttamista.

4.2 Poikkeaako SVPL:n sääntely käsityksenne mukaan merkittävästi muiden EU-maiden sääntelystä? Millä tavoin?

FiComin käsityksen mukaan Suomen malli näyttäytyy EU-vertailussa kansallisena erityisratkaisuna. Ongelma korostuu monikansallisessa toiminnassa, jossa samoja viestintä-, tietoturva- ja hallintaratkaisuja pyritään käyttämään useissa jäsenvaltioissa. Suomen sääntely tuo tähän erillisen kansallisen arviointikerroksen yleisen tietosuoja-asetuksen ja ePrivacy-sääntelyn rinnalle.

4.3 Millaisia vaikutuksia mahdollisilla eroilla sääntelyssä voi olla tai on ollut organisaatioiden toiminnan kannalta tai sijoittautumis- ja investointipäätöksiä tehtäessä?

Erot vaikeuttavat monikansallista toimintaa ja yhtenäisten järjestelmien käyttöä. Organisaatiot joutuvat rakentamaan Suomea varten erillisiä määrityksiä ja menettelyjä, mikä lisää kustannuksia ja voi heikentää Suomen asemaa toiminnan ja investointien sijaintipaikkana.

Ennakoitavuus ja yhteensopivuus muun EU-sääntelyn kanssa ovat tärkeitä erityisesti pilvipalvelujen, tietoturvapalvelujen, konsernitason hallintaratkaisujen ja digitaalisten palvelujen sijoittumista arvioitaessa. Kansalliset erityisratkaisut voivat vähentää Suomen houkuttelevuutta, jos ne edellyttävät erillisiä teknisiä ratkaisuja tai poikkeavia sisäisiä prosesseja ilman selkeää lisähyötyä.

4.4 Voiko SVPL:n sääntely aiheuttaa lisäkustannuksia otettaessa käyttöön viestinnän tai välitystietojen käsittelyä edellyttäviä riskienhallintatoimenpiteitä tai muita toimenpiteitä (esim. tietojärjestelmien tai prosessien muuttaminen Suomen lainsäädännön mukaiseksi)? Mistä syystä? Onko SVPL:n sääntely aiheuttanut teille tällaisia lisäkustannuksia?

Sääntely voi aiheuttaa lisäkustannuksia riskienhallinta- tai muiden toimenpiteiden käyttöönotossa. Lisäkustannuksia syntyy erityisesti silloin, kun valmisohjelmistoja, pilvipalveluja tai konsernin yhteisiä järjestelmiä on muokattava tai konfiguroitava Suomen erityisvaatimusten mukaisiksi.

Kustannuksia voi syntyä myös erillisestä oikeudellisesta arvioinnista, sisäisten prosessien rakentamisesta, henkilöstön kouluttamisesta sekä ilmoitus- ja dokumentointivelvoitteiden täyttämisestä. Taustalla on kansallisen sääntelyn poikkeaminen ePrivacy-direktiivin ja yleisen tietosuoja-asetuksen perustasosta.

FiCom ei arvioi kysymystä yksittäisenä järjestelmähankkeena, vaan toimialan näkökulmasta. Jäsenyritysten kannalta kustannusriski syntyy erityisesti siitä, että Suomen erityissääntely voi edellyttää erillisiä oikeudellisia ja teknisiä arviointeja muuten yhtenäisiin eurooppalaisiin tai globaaleihin ratkaisuihin.

4.5 Voiko SVPL:n sääntely mielestänne estää tai rajoittaa muissa EU-maissa hyödylliseksi havaittujen järjestelmien, niiden toimintojen tai menettelyjen käyttöä Suomessa? Voiko sääntely edellyttää niiden merkittävää muokkaamista Suomen lainsäädännön mukaiseksi toimittaessa monikansallisessa toimintaympäristössä? (Esim. valmisohjelmistot, pilvipalvelut ja monikansallisen konsernin yhteiset viestintäjärjestelmät.) Mistä vaatimuksesta tämä voi johtua? Onko näin tapahtunut kohdallanne ja miten ratkaisitte tilanteen?

Sääntely voi estää tai rajoittaa muissa EU-maissa hyödyllisten järjestelmien tai menettelyjen käyttöä Suomessa taikka edellyttää niiden merkittävää muokkaamista. Valmisohjelmistot, pilvipalvelut ja monikansallisen konsernin yhteiset viestintä- ja tietoturvajärjestelmät on suunniteltu pääsääntöisesti yleisen tietosuoja-asetuksen ja ePrivacy-direktiivin perustason mukaisiksi.

Suomen kansallinen erityissääntely voi edellyttää järjestelmien muokkaamista tai rajoittaa niiden käyttöä esimerkiksi lokienhallinnassa, haitallisen liikenteen havaitsemisessa, tietovuotojen estämisessä, sähköposti- ja päätelaiteturvassa, identiteetin- ja pääsynhallinnassa sekä konsernin sisäisissä väärinkäytösten selvittämismenettelyissä. Tämä johtuu erityisesti SVPL:n kansallisista käyttötarkoitus- ja menettelyvaatimuksista sekä niiden epäselvästä suhteesta yleisen tietosuoja-asetuksen mukaiseen käsittelyyn.

Toimialan kannalta ongelma syntyy jo siitä, että Suomea varten tarvitaan erillinen oikeudellinen ja tekninen arviointi. Tämä lisää kustannuksia, hidastaa käyttöönottoja ja voi johtaa siihen, että Suomessa otetaan käyttöön suppeampi tai teknisesti poikkeava ratkaisu kuin muissa maissa.

5 Välitystietoja ja viestintää koskevien säännösten suhde yleiseen tietosuoja-asetukseen

5.1 Oletteko havainnut erityisiä haasteita SVPL:n välitystietoja ja viestintää koskevan sääntelyn soveltamisessa yhdessä yleisen tietosuoja-asetuksen kanssa? Millaisia?

FiCom on havainnut erityisiä haasteita SVPL:n sääntelyn soveltamisessa yhdessä yleisen tietosuoja-asetuksen kanssa. Keskeisin haaste on päällekkäinen ja osin rinnakkainen sääntely, jonka keskinäinen suhde ja etusijajärjestys ovat tulkinnanvaraisia. Käsittelyn oikeusperusteiden ja kansallisten erityisedellytysten yhteensovittaminen on epäselvää. Kun SVPL nimenomaisesti sääntelee viestinnän välittäjän oikeutta käsitellä välitystietoja, käsittely perustuu tähän erityissääntelyyn. Tämä lähtökohta tuottaa oikeusvarmuutta ja vähentää tarvetta arvioida tapauskohtaisesti, mihin yleisen tietosuoja-asetuksen käsittelyperusteeseen käsittely nojautuu.

Myös ilmoitusvelvollisuuksien päällekkäisyys on ongelmallista: samasta tietoturvaloukkauksesta voidaan joutua arvioimaan sekä Liikenne- ja viestintävirastolle että tietosuojavaltuutetun toimistolle tehtäviä ilmoituksia. Epäselvässä oikeustilassa organisaation turvallisin vaihtoehto voi olla jättää myös perusteltu käsittely tekemättä tai toteuttaa se tarpeettoman suppeasti. Tämä ei ole välttämättä käyttäjienkään edun mukaista, jos kyse on esimerkiksi tietoturvapoikkeamien havaitsemisesta tai selvittämisestä.

Samalla FiCom pitää tärkeänä, ettei yleisen tietosuoja-asetuksen ja SVPL:n suhdetta selkeytettäessä horjuteta niitä tilanteita, joissa SVPL:ssä on nimenomaisesti säädetty viestinnän välitystietojen käsittelystä erityissääntelynä. Erityissääntelyn tarkoituksena on ollut luoda tarkkarajaiset ja ennakoitavat puitteet viestinnän luottamuksellisuuden suojaa koskevalle käsittelylle.

6. Sijaintitietojen käsittely

6.1 Onko SVPL:n ePrivacy-direktiiviä täydentävä sääntely edistänyt tai tukenut sijaintitietojen käsittelyä edellyttävien toimenpiteiden käyttöönottoa? Onko sääntely toteuttanut yksityisyyden ja henkilötietojen suojaa mielestänne tarkoituksenmukaisella tavalla? Millä tavoin?

Sijaintitiedon kansallinen määritelmä kattaa myös päätelaitteesta saatavan paikannustiedon, kuten satelliittipaikannustiedon. Tämä ulottaa soveltamisalaa ePrivacy-direktiivin lähtökohtaa laajemmalle ja limittyy yleisen tietosuoja-asetuksen kanssa.

Sijaintitiedot voivat olla yksityisyyden suojan kannalta hyvin arkaluonteisia, ja niiden käsittely edellyttää jatkossakin selkeitä suojakeinoja. Nykyinen laajennettu ja tulkinnanvarainen soveltamisala on kuitenkin lisännyt epävarmuutta siitä, milloin sovelletaan SVPL:n erityissääntelyä ja milloin käsittelyä arvioidaan ensisijaisesti yleisen tietosuoja-asetuksen nojalla.

FiComin tiedossa ei ole, että SVPL:n kansallinen erityissääntely olisi erityisesti edistänyt tai tukenut sijaintitietojen käsittelyä edellyttävien palvelujen tai toimintojen käyttöönottoa. Käytännössä

epävarmuutta syntyy siitä, milloin kyse on SVPL 20 luvun mukaisesta sijaintitiedosta ja milloin käsittelyä tulisi arvioida ensisijaisesti yleisen tietosuoja-asetuksen perusteella. Tämä ei tue uusien palvelujen suunnittelua eikä lisää sääntelyn ennakoitavuutta.

6.2 Pidättekö SVPL 20 luvun sijaintitietojen käsittelyä koskevan lainsäädännön soveltamisalaa selvänä suhteessa esimerkiksi työnantajien toteuttamaan työntekijöiden tai ajoneuvojen paikantamiseen? Minkälaisia haasteita sääntelyn soveltamisalan tulkintaan voi liittyä?

Soveltamisala ei ole selvä. Tämä on ongelmallista erityisesti työntekijöiden, ajoneuvojen ja työvälineiden paikantamisessa. Epäselvää on muun muassa, milloin paikantaminen kuuluu 20 luvun mukaisen erityissääntelyn piiriin ja milloin sitä arvioidaan ensisijaisesti työelämän tietosuojalain ja yleisen tietosuoja-asetuksen nojalla. Tulkinnanvaraisuus voi koskea esimerkiksi sitä, paikannetaanko työntekijää, työnantajan ajoneuvoa, työvälinettä vai palvelun käyttöä teknisesti mahdollistavaa päätelaitetta.

6.3 Voiko sijaintitietojen käsittelyä koskeva SVPL:n ePrivacy-direktiiviä täydentävä sääntely (kuten siihen liittyvä käyttäjän suostumuksen vaatimus) estää tai rajoittaa työpaikoilla toimenpiteitä, jotka olisivat käsityksenne mukaan perusteltuja ja muun soveltuvan lainsäädännön mukaisia? Mitä toimenpiteitä?

Sijaintitietojen sääntely voi estää tai rajoittaa perusteltuja ja muun lainsäädännön mukaisia toimenpiteitä työpaikoilla. SVPL:n suostumukseen perustuva lähtökohta sopii huonosti yhteen työsuhteen kanssa, koska suostumusta ei työnantajan ja työntekijän välisen epätasapainon vuoksi yleensä voida pitää yleisen tietosuoja-asetuksen tarkoittamalla tavalla aidosti vapaaehtoisena käsittelyperusteena.

Tämä voi estää tai rajoittaa esimerkiksi ajoneuvojen ja työvälineiden paikantamista työturvallisuus-, logistiikka- tai omaisuudensuojatarkoituksissa, vaikka käsittely olisi muutoin yleisen tietosuoja-asetuksen ja työelämän tietosuojalain mukaista.

6.4 Voiko sijaintitietojen käsittelyä koskevan sääntelyn soveltamisala ja tulkinta aiheuttaa haasteita paikannettaessa muita kuin työntekijöitä, esimerkiksi tarjottaessa mobiililaitteen paikannusta hyödyntäviä palveluita yleisölle? Millaisia haasteita? Onko sääntelyn suhde evästeiden ja muiden päätelaitteiden tietojen käyttöä sääntelevään SVPL 205 §:ään mielestänne selvä?

Soveltamisala ja tulkinta voivat aiheuttaa haasteita myös paikannettaessa muita kuin työntekijöitä. Yleisölle tarjottavissa, mobiililaitteen paikannusta hyödyntävissä palveluissa soveltamisala ja suostumusedellytysten tulkinta ovat epäselviä.

Sääntelyn suhde päätelaitteelle tallennettujen tietojen käyttöä koskevaan 205 §:ään ei ole selvä. Sama palvelu voi edellyttää sekä päätelaitteella olevan tiedon käyttöä että sijaintitiedon käsittelyä, jolloin 20 luvun, 205 §:n ja yleisen tietosuoja-asetuksen välinen suhde jää epävarmaksi.

6.5 Oletteko havainnut erityisiä haasteita SVPL:n sijaintitietoja koskevan sääntelyn soveltamisessa yhdessä yleisen tietosuoja-asetuksen kanssa? Millaisia?

FiCom on havainnut erityisiä haasteita sijaintitietojen sääntelyn soveltamisessa yhdessä yleisen tietosuoja-asetuksen kanssa. Haasteet liittyvät päällekkäisiin suostumus- ja käsittelyperustevaatimuksiin sekä siihen, ettei sääntelyjen keskinäinen suhde ole selvä.

Yleisen tietosuoja-asetuksen mukainen käsittelyperuste ei välttämättä riitä, jos SVPL:n erityissääntelyä tulkitaan niin, että käsittely edellyttää erillistä suostumusta. Tämä on ongelmallista erityisesti silloin, kun suostumus ei ole toimiva käsittelyperuste mutta käsittely olisi muutoin tarpeellista, oikeasuhtaista ja riittävin suojatoimin toteutettavissa.

7 Sääntelyn kehittämistä koskevat ehdotukset

7.1 Pidättekö SVPL:n ePrivacy-direktiiviä täydentävää välitystietojen, viestinnän ja sijaintitietojen käsittelyä koskevien sääntelyn kehittämistä tarpeellisena? Jos kyllä, millä tavoin havaitsemanne haasteet SVPL:n säännösten soveltamisessa tulisi mielestänne ratkaista? Tulisiko sääntelyn soveltamisala määrittää toisin kuin nykyisin tai sääntelyä muuttaa jollakin muulla tavoin? Mitkä arvioitte ehdotuksenne merkittävimmiksi vaikutuksiksi?

FiCom pitää sääntelyn kehittämistä tarpeellisena. Lausuntopyynnön kohteena olevaa ePrivacy-direktiiviä täydentävää kansallista erityissääntelyä tulisi arvioida kriittisesti ja keventää siltä osin kuin se on päällekkäistä, tulkinnanvaraista tai nykyiseen toimintaympäristöön nähden tarpeettoman raskasta. FiCom ei esitä viestinnän luottamuksellisuuden tai viestintäverkkojen tietoturvan suojatason heikentämistä, vaan kansallisen lisäsääntelyn kohdentamista nykyistä täsmällisemmin ja riskiperusteisemmin.

Sääntelyn tulisi olla nykyistä teknologianeutraalimpaa ja päämääräperusteisempaa siten, että se määrittää selkeästi suojattavat tavoitteet, mutta ei tarpeettomasti estä tarkoituksenmukaisia ja oikeasuhtaisia teknisiä toteutustapoja. Tämä on erityisen tärkeää kyberturvallisuuden, petosten ja huijausviestinnän torjunnan sekä monikansallisissa pilvi- ja konserniympäristöissä käytettävien ratkaisujen kannalta.

Kehittämisessä tulisi arvioida ainakin yhteisötilaajasääntelyn soveltamisalaa, 18 luvun menettelyjen tarpeellisuutta ja suhdetta yleiseen tietosuoja-asetukseen sekä työelämän tietosuojalakiin, 272 §:n mukaisten tietoturvatoimien ja 18 luvun erityismenettelyn rajanvetoa, sijaintitietosääntelyn soveltamisalaa sekä SVPL:n 20 luvun, 205 §:n ja yleisen tietosuoja-asetuksen välistä suhdetta. Tavoitteena tulee olla, etteivät tavanomaiset tieto- ja viestintäjärjestelmät tai perustellut kyberturvallisuus- ja riskienhallintatoimenpiteet tarpeettomasti esty.

Kehittäminen on luontevaa kytkeä hallitusohjelman mukaiseen kansallisen lisäsääntelyn purkamiseen, vireillä olevaan työelämän tietosuojalain muutostarpeiden selvittämiseen sekä tietosuojalainsäädännön kokonaisuudistukseen. Muutoksen tärkein vaikutus olisi oikeustilan selkeytyminen. Organisaatioiden olisi helpompi arvioida etukäteen, milloin viestinnän, välitystietojen tai sijaintitietojen käsittely on sallittua ja mitä menettelyjä se edellyttää. Se vähentäisi erillistä kansallista arviointia, helpottaisi yhteisten eurooppalaisten ja konsernitason ratkaisujen käyttöä sekä parantaisi edellytyksiä toteuttaa kyberturvallisuustoimia ilman, että viestinnän luottamuksellisuuden tai henkilötietojen suojan tasoa heikennetään.

Sääntelyn kehittämisessä on huolehdittava siitä, että mahdollinen kansallisen lisäsääntelyn keventäminen kohdistuu lausuntopyynnössä tarkoitettuihin tulkinnanvaraisiin ja päällekkäisiin sääntelykohtiin eikä johda viestinnän välittäjien vakiintuneiden ja tarkkarajaisten SVPL 17 luvun käsittelyperusteiden kaventumiseen. Nämä käsittelyperusteet tuottavat oikeusvarmuutta, ja niiden säilyttäminen on tärkeää.

8 Muut huomiot

8.1 Tässä voitte esittää mahdolliset muut huomionne selvitystä varten.

FiCom pitää hanketta tarpeellisena ja kannatettavana. SVPL:n kansallisia erityissäännöksiä on perusteltua arvioida kokonaisuutena suhteessa nykyiseen teknologiseen toimintaympäristöön, yleiseen tietosuoja-asetukseen, ePrivacy-sääntelyyn, työelämän tietosuojalakiin sekä uuteen kyberturvallisuus- ja datasääntelyyn.

Kansallisen erityissääntelyn keventäminen tulee perustaa huolelliseen vaikutusarviointiin, ja mahdollisessa myöhemmässä säädöshankkeessa on varmistettava, että viestinnän luottamuksellisuuden ja henkilötietojen suoja toteutuvat edelleen. Samalla on tärkeää varmistaa, ettei sääntely tarpeettomasti estä organisaatioiden vastuullista kyberturvallisuuden riskienhallintaa, tietoturvapoikkeamien selvittämistä tai digitaalisten palvelujen kehittämistä.

Hälinen Janne
FiCom ry