Liikenne- ja viestintävirasto (Traficom)

Lausunto

18.06.2026

TRAFICOM/324907/04.04.05.03/2026

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?

Henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla annettu Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY (sähköisen viestinnän tietosuojadirektiivi) annettiin vuonna 2002 osana televiestintäpakettia ja tarkastettiin viimeksi vuonna 2009 direktiivillä 2009/136/EY. Toimeenpantaessa direktiiviä kansallisesti sähköisen viestinnän tietosuojalailla, sääntelyn soveltamisalaa laajennettiin yhteisötilaajiin. Tuolloin selkeä ja tarkoituksenmukainen yhteisötilaajan määritelmä on muuttunut vaikeaselkoisemmaksi etätyön ja pilvipalveluiden hallitsemassa nykyajassa. Välitystietojen ja viestien tietoturvaperusteiset käsittelyoikeudet ovat pysyneet pääosin samoina tästä alkaen.

SVPL 272 §:n kasuistinen ja lähinnä sähköpostia ajatellen kirjoitettu sanamuoto korostaa teknologian ja palveluiden käyttötapojen muuttumisen aiheuttamia soveltamishaasteita. Jos näin yksityiskohtainen sääntely on esimerkiksi valtiosääntöoikeudellisista syitä tarpeen, on tärkeää varmistaa sääntelyn ajantasaisuus riittävällä tiheydellä (Esim. perustuslakivaliokunta katsoi sen, että silloin ehdotettu sähköisen viestinnän tietosuojalaki salli tietoturvasta huolehtimiseksi yleisesti mitkä tahansa "muut välttämättömät toimenpiteet" oli esteenä lain säätämiselle tavallisessa lainsäätämisjärjestyksessä (ks. PeVL 9/2004 vp, s. 4–5).)

SVPL 2 §:ssä määritelty sääntelyn soveltamisala jättää monia asioita epäselväksi. Siinä esimerkiksi viitataan lähinnä vain eräisiin 17 luvun säännöksiin eikä lainkaan 18–20 lukuihin. Soveltamisala on epäselvä esimerkiksi kun yhteisötilaajalla on toimipaikkoja useassa jäsenvaltiossa.

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?

Yhteisötilaajasääntely nykymuodossaan hankaloittaa ja hidastaa Kyberturvallisuuskeskuksen tiettyjen kyberturvallisuuteen liittyvien palvelujen tarjoamista huoltovarmuuskriittisille organisaatioille, sillä sen myötä välitystietojen ja viestien tietoturvaperusteista käsittelyä koskevasta oikeudellisesta kehikosta on muodostunut erittäin monimutkainen ja vaikeaselkoinen kokonaisuus.

Kyberturvallisuuskeskuksen näkökulmasta erityisesti huoltovarmuuskriittisillä organisaatioilla tulisi olla käytössään parhaat mahdolliset työkalut kyberturvallisuuden riskienhallinnasta huolehtimiseksi. Nykytilanne on se, että Suomen muuta Eurooppaa tiukempi sääntely johtaa siihen muun muassa siihen, että suomalaiset yritykset voivat huolehtia kyberturvallisuuden riskienhallinnastaan paremmilla työkaluilla Suomen ulkopuolella. Tilannetta ei voida pitää millään tapaa tarkoituksenmukaisena.

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?

SVPL 17 luvun säännökset konkretisoivat mm. perustuslain 10 §:n 2 momentissa, perusoikeuskirjan 7 artiklassa ja ihmisoikeuksien ja perusvapauksien suojaamiseksi tehdyn yleissopimuksen (Euroopan ihmisoikeussopimus) 8 artiklassa turvattuja oikeuksia määrittelemällä täsmällisesti sähköisten viestien ja välitystietojen käsittelyn edellytykset.

Perustuslain 10 §:n 2 momentin "ensisijaisena tarkoituksena on suojata luottamukselliseksi tarkoitetun viestin sisältö ulkopuolisilta". Säännös lisäksi edellyttää "lainsäädäntöä, joka käytännössä tehokkaasti turvaa luottamuksellista viestintää sekä viranomaisten että muiden ulkopuolisten loukkauksilta" (HE 309/1993 vp, s. 53). SVPL:n esitöiden mukaan "perinteinen [esimerkki] osapuolten välisestä viestinnästä on kahden luonnollisen henkilön toisilleen lähettämät yksityisasioita koskevat viestit. Viestinnän osapuolia ovat tällöin sekä viestin lähettäjä että sen vastaanottaja. Tilanne ei muutu, vaikka yksityisasioita koskeva viesti lähetettäisiin viestin vastaanottajalle työnantajan tarjoamaan viestintäpalveluun." (HE 221/2013 vp, s. 152).

Kuten tietosuojatyöryhmä on huomauttanut, "se seikka, että työnantaja omistaa sähköiset välineet, ei sulje pois työntekijöiden oikeutta viestintäsalaisuuteen, sijaintitietojen salaisuuteen ja kirjesalaisuuteen" (Tietosuojatyöryhmä, Lausunto 2/2017 tietojenkäsittelystä työpaikalla, WP 249, 8.6.2017. kohta 6.1, s. 23).

SVPL VI osan säännöksiä sovelletaan kaikkiin viestinnän välittäjiin. Esitöiden mukaan määritelmällä kuvataan ne tahot, jotka ovat luottamuksellisen viestinnän suojan kannalta kriittisessä asemassa (HE 221/2013 vp s. 92). Sääntelyn myötä esimerkiksi VPN-palvelut kuuluvat viestinnän luottamuksellisuutta turvaavan sääntelyn piiriin, vaikka niitä ei pidettäisi teleyrityksinä (ks. esim. KKO 2022:23).

Näiden toimijoiden keskeisen aseman vuoksi niillä on myös erityiset mahdollisuudet vaarantaa viestinnän luottamuksellisuutta, jolloin erityiset suojatoimenpiteet ovat perusteltuja väärinkäytösten ehkäisemiseksi. Vaikka sääntely kohdistuu luottamuksellisen viestinnän suojan kannalta kriittisessä asemassa oleviin toimijoihin, sääntelyn on silti oltava tasapainossa suhteessa toimijoiden tarpeeseen huolehtia tietoturvasta. Viestinnän välittäjillä on oltava riittävän joustavat keinot huolehtia tietoturvasta myös huolehtiakseen sen käsittelemien henkilötietojen tietoturvasta.

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?

Liikenne- ja viestintävirasto katsoo, että sähköisen viestinnän tietosuojadirektiiviä täydentävää sääntelyä ei voida kaikilta osin pitää täysin tarkoituksenmukaisena siltä osin kuin se sääntelee sellaista välitystietojen ja viestien käsittelyä, joka liittyy erilaisilta kyberuhkilta suojautumiseen. Sääntely voisi mahdollistaa joustavammin viestinnän välittäjille erilaiset tietoturvatoimenpiteet. Nykyisin voimassa oleva sääntely on varsin kasuistisista eikä käsittelyperusteita ole päivitetty vastaamaan nykyistä uhkaympäristöä. Tämä rajoittaa tarpeettomasti kyberturvallisuuden riskienhallintaa.

Nykyaikana tekoäly mahdollistaa merkittävästi aiempaa helpommin uusien ohjelmistohaavoittuvuuksien tunnistamisen. Yksittäisen organisaation onkin erittäin vaikeaa, ellei jopa mahdotonta estää kehittyneen nollapäivähaavoittuvuutta hyödyntävän kyberhyökkäyksen ensimmäistä vaihetta eli organisaation tietojärjestelmiin murtautumista. Tässä teknisessä todellisuudessa käynnissä olevien hyökkäysten havaitseminen nousee kyberturvallisuuden riskienhallinnan keskiöön: se on välttämättömyys vahinkojen pienentämiselle ja mahdollistaa esimerkiksi organisaation luottamuksellisten tietojen vuotamisen estämisen tai kiristyshaittaohjelmahyökkäyksen pysäyttämisen ennen tietojen salaamista.

Kyberturvallisuuden riskienhallinta perustuu nykyaikana enenevissä määrin käyttäytymisperusteiseen poikkeamienhallintaan. Esimerkiksi viime vuosien aikana yleistyneet Living off the Land -hyökkäykset perustuvat pelkästään kohdeympäristössä valmiiksi olevien hyväksyttyjen ohjelmistojen ja tavanomaisten järjestelmäkomponenttien hyödyntämiseen hyökkäyksissä. Tällaisten työkalujen käyttö ei johda tietoturvahälytyksiin uhriorganisaatiossa. Kyseisten hyökkäysten havaitseminen perustuu organisaation tieto- ja viestintäjärjestelmien poikkeavan käyttäytymisen tunnistamiseen.

Tähän liittyen on olennaista huomata, että Onnettomuustutkintakeskuksen Helsingin kaupungin tietomurtoa koskevan tutkintaselostuksen 4. johtopäätös on, että "Julkisen sektorin kyky vastata tietoverkkorikosten aiheuttamiin uhkiin on tällä hetkellä puutteellinen, koska hyökkäysten ja haavoittuvuuksien havainnointimenetelmiä ei ole käytössä kattavasti. Hyökkäysten ja haavoittuvuuksien tunnistamisella ja korjaamisella on mahdollista estää tietomurtoja ja suojata tietoja." (Onnettomuustutkintakeskus, Helsingin kaupungin tietomurto 2024, Tutkintaselostus 3/2025, Tutkinnan tunnus: P2024-01, s. 79)

Julkisen tutkintaselostuksen mukaan Helsingin kaupungin tietomurrossa oli kyse LOTL-hyökkäyksestä. Tämän kannalta on olennaista tunnistaa, että nykyinen välitystietojen ja sähköisten viestien tietoturvaperusteisesta käsittelyä koskeva sääntely voi monissa organisaatioissa osoittautua esteeksi tällaisten hyökkäysten tunnistamiseksi. Tähän vaikuttaa osaltaan ainakin sääntelyn monimutkaisuus ja -tulkintaisuus, jonka myötä suomalaiset organisaatiot ovat varovaisia aidosti tarpeellisten tietoturvatyökalujen käyttöönotossa.

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.)

SVPL 18 luvun säännökset, jotka koskevat viestintäverkon tai viestintäpalvelun luvattoman käytön torjuntaa ovat potentiaaliselta soveltamisalaltaan jokseenkin suppeita (ks. Veikko Vauhkonen ja Jesse Heiskanen, Kyberturvallisuussääntely - tulkinta ja soveltaminen, 2025 Alma Insights, s. 468). On epäselvää, että kuinka tehokkaasti SVPL 18 luvun mukaisen välitystietojen käsittelyn avulla on mahdollista ehkäistä liikesalaisuuksien paljastamista.

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?

SVPL:n tietoturvatoimenpiteistä säätävän 272 §:n ja SVPL 18 luvun soveltaminen on aiheuttanut huomattavasti yhteydenottoja yrityksiltä, jotka harkitsevat erilaisten data loss prevention (DLP) -ohjelmistojen käyttöä. SVPL 18 luvun on tarkoitus määritellä tyhjentävästi välitystietojen ja viestien käsittelyoikeudet, joita yhteisötilaaja voi käyttää liikesalaisuuksien paljastamisen ehkäisemiseksi. Tämä sulkee pois viestin sisältöön puuttuvat toimenpiteet liikesalaisuuksien paljastamisen ehkäisemiseksi. DLP-ohjelmistojen käyttömahdollisuudet muiden luottamuksellisten tietojen kuin liikesalaisuuksien paljastamisen estämiseksi jäävät tarpeettoman epäselviksi.

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?

Yhteisötilaajasääntely rajoittaa epätarkoituksenmukaisesti viestinnän tai välitystietojen käsittelyä edellyttävien perusteltujen riskienhallintatoimenpiteiden käyttämistä.

Liikenne- ja viestintävirasto katsoo, että välitystietojen ja viestinnän käsittelyä koskevaa sääntelyä tulisi kehittää siten, että se mahdollistaa joustavasti kehittyviltä kyberuhilta suojautumisen. SVPL 272 §:n mukaiset tietoturvaperusteiset viestien ja välitystietojen käsittelyperusteet ovat säilyneet pääosin samoina vuoden 2004 sähköisen viestinnän tietosuojalaista lähtien.

Esimerkiksi SVPL 272 §:n 1 momentin 3 kohdan mukainen käsittelyoikeus rajoittuu vain rikoslain 37 luvun 11 §:ssä tarkoitettujen maksuvälinepetosten valmistelun ehkäisemiseen, joka aiheuttaa tarpeetonta epäselvyyttä esimerkiksi ns. spearfishingin tai toimitusjohtajahuijauksilta suojautumisen suhteen sillä tätä voidaan pitää pikemminkin petoksena.

Sähköisen viestinnän tietosuojadirektiivin kansallinen laajennus vaikeuttaa myös kyberuhkatietojen jakamista. Jos tietty uhkatieto, kuten hyökkääjän käyttämä IP-osoite, on kerätty viestinnän välittämisen yhteydessä, se on herkästi välitystieto, jolloin sen käsittely ja luovuttaminen muille organisaatioille, jotta nämä voivat suojautua kyseiseltä kyberuhalta, hankaloituu merkittävästi. Kyberturvallisuuslain 3 lukuun on kehitelty epätarkoituksenmukaisia ratkaisuja ongelman kiertämiseksi kansallisen CSIRT-yksikön orkestroimissa luottamusverkostoissa, mutta ne ovat pelkästään keinoja yrittää tilkitä jo perustuksiltaan kyberturvallisuuden riskienhallinnan kannalta ongelmallisen sääntelyn aiheuttamia haasteita.

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?

SVPL 17 luvun säännökset koskevat myös radioviestinnän ja sen välitystietojen käsittelyä. Radioviestintä ei kuulu sähköisen viestinnän tietosuojadirektiivin soveltamisalaan, vaan kyse on tältä osin täysin kansallisesta laajennuksesta. Luvun käsittelysäännökset eivät sovellu luontevasti radioviestintään ja sen välitystietoihin.

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?

Vertailukohta jää kysymyksestä epäselväksi. Sääntely, joka määrittelee edellytykset jonkin toimenpiteiden toteuttamiselle, ei luonnollisesti voi edistää toimenpiteiden käyttöä verrattuna tilanteeseen, jossa lainsäädäntö ei lainkaan rajoita toimintaa.

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?

Voi aiheuttaa epäselvyyksiä liittyen esim. järjestelmiin, joihin kerätään automaattisesti työntekijän edustajana toimivan työntekijän ja asiakkaan välistä yhteydenpitoa.

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?

On epäselvää, missä määrin SVPL:n yhteisötilaajasääntely on mahdollisesti hallinnollisesti raskaampaa yleisen tietosuoja-asetuksen 88 artiklan puitteissa annettuun erityisesti työntekijöiden suojelua koskevaan sääntelyyn verrattuna.

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

Useissa muissa jäsenvaltioissa sen sijaan, että telesääntelyn laajennetaan sovellettavaksi yhteisötilaajiin, sääntely perustuu yleiseen tietosuoja-asetukseen ja mahdollisesti myös sen 88 artiklan puitteissa annettuun erityisesti työntekijöiden suojelua koskevaan kansalliseen sääntelyyn.

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

Liikenne- ja viestintävirastolla ei ole lausuttavaa sääntelyn eroavaisuuksien vaikutuksista organisaatioiden toiminnan kannalta tai sijoittautumis- ja investointipäätöksiä tehtäessä.

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?

Sisämarkkinoilla saatavilla olevien tietojärjestelmien tai toisessa jäsenvaltiossa hyödylliseksi havaittujen prosessien muuttaminen Suomen lainsäädännön mukaiseksi aiheuttanee väistämättä jossain määrin kustannuksia.

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?

Erilaisten valmisratkaisujen oletusasetusten mukaiset tietoturvatoimenpiteet eivät ole välttämättä helposti yhteensovitettavissa kansallisen lainsäädännön vaatimusten kanssa.

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?

Sähköisen viestinnän palveluista annettu laki tarjoaa erityistä suojelua tietyille sellaisten tietojen luokille, jotka saattavat olla myös henkilötietoja kuten käyttäjän sähköiselle viestinnälle ja välitystiedoille.

Sääntelyn yhteensovittamiseen liittyy ajoittain haasteita. Esimerkiksi välitystietojen ja viestien tietoturvaperusteisen havainnoinnin reunaehdot herättävät ymmärrettävästi kysymyksiä Kyberturvallisuuskeskuksen kyberturvallisuuteen liittyvien palvelujen mahdollisissa asiakasorganisaatioissa. Nykymuotoinen yhteisötilaajasääntely tekee tällaisten palvelujen tarjoamista koskevista sopimuksista tarpeettoman monimutkaisia. Yleisen tietosuoja-asetuksen ja SVPL:n yhteensovittaminen on osoittautunut käytännön elämässä ajoittain haasteelliseksi.

Kysymyksiä kun rekisteröity haluaa käyttää yleisen tietosuoja-asetuksen 15 artiklassa säädettyä oikeutta saada tutustua tietoihin, mutta pyyntö kohdistuu esimerkiksi rekisterinpitäjän palveluksessa olevien henkilöiden välisiin sähköposteihin, joissa rekisterinpitäjää itseään ei voida pitää viestinnän osapuolena.

Silloin kun sähköisen viestinnän palveluista annetun lain vaatimukset ovat päällekkäisiä yleisen tietosuoja-asetuksen kanssa, sovelletaan teleyritysten osalta vain ensiksi mainittuja yleisen tietosuoja-asetuksen säännösten sijaan asetuksen 95 artiklan nojalla. Tämä ei kuitenkaan koske muita viestinnän välittäjiä kuin teleyrityksiä, joiden on noudatettava rinnakkain kumpaakin sääntelykokonaisuutta. Toimijoihin kohdistuu myös rinnakkaista valvontaa Liikenne- ja viestintäviraston ja tietosuojavaltuutetun taholta (valvontaviranomaisen toimivallasta ks. Euroopan tietosuojaneuvosto, Lausunto 5/2019 sähköisen viestinnän tietosuojadirektiivin ja yleisen tietosuoja-asetuksen vuorovaikutuksesta erityisesti tietosuojaviranomaisten toimivallan, tehtävien ja valtuuksien osalta, 12.3.2019, kohta 68). Muun viestinnän välittäjän kuin teleyrityksen on

osoitettava henkilötiedoiksi luokiteltavien sähköisten viestien ja välitystietojen käsittelylle rinnakkainen peruste myös yleisestä tietosuoja-asetuksesta.

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?

Liikenne- ja viestintävirasto kiinnittää huomiota siihen, että kuten unionin tuomioistuimen vakiintuneessa oikeuskäytännössä korostetaan, "liikenne- ja paikkatiedot voivat paljastaa tietoja huomattavasta määrästä asianomaisten henkilöiden yksityiselämään liittyviä seikkoja, ja myös arkaluonteisia tietoja, kuten seksuaalista suuntautumista, poliittisia mielipiteitä, uskonnollista, filosofista, yhteiskunnallista tai muuta vakaumusta sekä terveydentilaa koskevia tietoja, vaikka tällaiset tiedot saavat unionin oikeudessa lisäksi erityistä suojaa. Näiden tietojen kokonaisuus voi mahdollistaa hyvin tarkkojen päätelmien tekemisen niiden henkilöiden, joiden tietoja on säilytetty, yksityiselämästä, kuten elämäntavoista, vakituisista tai tilapäisistä oleskelupaikoista, päivittäisestä tai muusta liikkumisesta, toiminnasta sekä näiden henkilöiden sosiaalisista suhteista ja heidän sosiaalisesta ympäristöstään. Niiden perusteella voidaan erityisesti laatia rekisteröityjen profiili, joka on yksityiselämän kunnioittamista koskevan oikeuden kannalta aivan yhtä arkaluonteista tietoa kuin itse viestinnän sisältö" (yhdistetyt asiat C-511/18, C-512/18 ja C-520/18 La Quadrature du Net ym., tuomio 6.10.2020, EU:C:2020:791, kohta 117 viittauksineen).

Nykyiset yleisesti kuluttajien käytössä olevat satelliittipaikannusjärjestelmät mahdollistavat paikannuksen muutamaan metrin tarkkuudella. Sähköisen viestinnän tietosuojadirektiivi on annettu vuonna 2002, jolloin tällaiset toiminnot eivät olleet vielä yleistyneet päätelaitteissa. On myös huomattava, että myös viestintäverkkojen on mahdollista saada päätelaitteesta myös satelliittipaikannustietoja mm. hätäkeskuksen tarpeisiin esimerkiksi LPP:n (LTE Positioning Protocol) avulla. Vaikutukset yksityisyyteen ovat kuitenkin jokseenkin samanlaisia riippumatta sijaintitiedon teknisestä hankkimistavasta.

Lisäksi on syytä huomata, että direktiivillä 2009/136/EY laajennettiin paikkatiedon määritelmää kattamaan myös sellaiset päätelaitteen maantieteellisen sijainnin ilmaisevat tiedot, joita käsitellään sähköisen viestintäpalvelun avulla. Mainitun direktiivin johdanto-osan 56 kappaleesta ilmenee sääntelyn laaja soveltamisala ja tarkoitus vastata uusien tiedonkeruu- ja tunnistuslaitteisiin perustuvien sovellusten kehittämiseen.

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?

Liikenne- ja viestintävirastolla ei ole lausuttavaa kohdasta 6.2.

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?

Liikenne- ja viestintävirastolla ei ole lausuttavaa kohdasta 6.3.

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?

Evästeiden ja muiden päätelaitteiden tietojen käyttöä sääntelevä SVPL 205 § eroaa tarpeettomasti sanamuodoltaan sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdan sanamuodosta, vaikka direktiivin säännös ei jätä säännöksen toimeenpanossa juuri liikkumavaraa, muuten kuin 15 artiklan 1 kohdan mukaisesti. Toisin kuin SVPL 205 §:ssä direktiivissä 2002/58/EY viitataan käyttäjän päätelaitteen ohella myös tilaajan päätelaitteeseen ja tilaajan suostumukseen. Em. direktiivissä tarkoitettu tilaaja, toisin kuin käyttäjä, voi olla myös oikeushenkilö (ks. em. direktiivin johdanto-osan kappaleet 12 ja 17).

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

Liikenne- ja viestintävirastolla ei ole lausuttavaa kohdasta 6.5.

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?

7.1.1 RIITTÄVÄN JOUSTAVIEN TIETOTURVATOIMENPITEIDEN MAHDOLLISTAMINEN

Liikenne- ja viestintävirasto pitää perusteltuna varmistaa, että SVPL:n tietoturvaperusteiset välitystietojen käsittelyoikeudet ovat riittävän joustavia mahdollistamaan kehittyviin kyberuhkiin vastaamisen. Erityisesti yhteisötilaajien osalta olisi kiinnitettävä huomiota siihen, että niiden tarpeet eroavat huomattavasti muista viestinnän välittäjistä.

Viestinnän välittäjillä tulee olla riittävät työkalut, jotta ne kykenevät vastaamaan kyberuhkaympäristön perustavanlaatuiseen muutokseen. Tätä muutosta ja olemassa olevan sääntelyn haasteita on kuvattu asianmukaisesti liikenne- ja viestintäministeriön julkaisussa taustamuistio: sähköisen viestinnän tietosuojasäännösten ajantasaisuuden tarkastelu (25.5.2026, VN/10660/2026).

7.1.2 RADIOVIESTINTÄ

SVPL 17 luvun säännökset koskevat myös radioviestinnän ja sen välitystietojen käsittelyä. Radioviestintä ei kuulu sähköisen viestinnän tietosuojadirektiivin soveltamisalaan, vaan kyse on tältä osin täysin kansallisesta laajennuksesta. Luvun käsittelysäännökset eivät sovellu luontevasti radioviestintään ja sen välitystietoihin.

Liikenne- ja viestintävirasto pitää perusteltuna, että samalla tarkasteltaisiin yleisesti vastaanotettavaksi tarkoitetun radioviestinnän esimerkkiluetteloa ottaen huomioon mm. perustuslakivaliokunnan lausuntokäytännön kehittymisen koskien perustuslain 10 §:n 2 momentin suojan alaa. Lisäksi "luottamuksellisuuden kannalta on merkitystä sillä, että periaatteessa kuka tahansa voi kuunnella radiolähetyksiä" (LiVM 6/2001 vp).

8 Muut huomiot

8.1 Tässä voitte esittää mahdolliset muut huomionne selvitystä varten.

8.1.1 LUOTTAMUKSELLISEEN VIESTINNÄN SUOJAAMINEN TYÖNTEKIJÄN JA TYÖNANTAJAN VÄLISESSÄ SUHTEESSA

Kaikkien lainsäädäntömuutosten valmistelussa on huomioitava perustuslain 10 §:n 2 momentin reunaehdot, joka ensisijaisena tarkoituksena esitöiden mukaan on suojata luottamukselliseksi tarkoitetun viestin sisältö ulkopuolisilta, joka toisaalta antaa turvaa muillekin tällaista viestiä koskeville tiedoille, joilla voi olla merkitystä viestin säilymiselle luottamuksellisena. Säännös edellyttää "lainsäädäntöä, joka käytännössä tehokkaasti turvaa luottamuksellista viestintää sekä viranomaisten että muiden ulkopuolisten loukkauksilta". (ks. HE 309/1993 vp, s. 53)

On tärkeää, että lainsäädännöllä turvataan työntekijöiden oikeus luottamukselliseen viestintään myös työnantajan taholta tulevalta puuttumiselta. On tyypillistä, että työnantajan käyttöön antamia laitteita käytetään täysin luvallisesti yksityisasioihin. Työnantajat antavat usein työntekijöidensä käyttöön puhelimia puhelinetuna. On tärkeää, että työnantajalla ei ole oikeutta puuttua työntekijän yksityiseen viestintään.

Mahdollisessa sääntelyn muutoksessa on huomioitava, että sähköisen viestinnän tietosuojadirektiivin 5 artiklan 1 kohdan mukaisesti jäsenvaltioiden on kansallisella lainsäädännöllä varmistettava yleisen viestintäverkon ja yleisesti saatavilla olevien sähköisten viestintäpalvelujen välityksellä tapahtuvan viestinnän ja siihen liittyvien liikennetietojen luottamuksellisuus. Niiden on erityisesti kiellettävä se, että muut henkilöt kuin käyttäjät ilman kyseisten käyttäjien nimenomaista suostumusta kuuntelevat, salakuuntelevat, tallentavat tai muulla tavalla sieppaavat tai valvovat viestintää ja siihen liittyviä liikennetietoja, jollei se ole laillisesti sallittua 15 artiklan 1 kohdan mukaisesti. On selvää, että henkilöiden välisten viestintäpalveluiden kautta tapahtuva työntekijöiden yksityinen viestintä kuuluu selkeästi tämän suojan piiriin riippumatta viestintään käytetyn laitteen omistajasta.

8.1.2 YHTEENSOPIVUUS UNIONIN OIKEUDEN KANSSA

Vaikka suljettujen käyttäjäryhmien ja yritysverkkojen sääntely jätettiin toissijaisuusperiaatteen mukaisesti unionin sähköisen viestinnän tietosuojasääntelyn ulkopuolelle (ks. direktiivin 2009/136/EY johdanto-osan 55 kappale) ja siten jäsenvaltioille. Niin Liikenne- ja viestintävirasto pitää kuitenkin tärkeänä, että SVPL 17, 18, 19 ja 20 luku ovat täysin yhteensopivia unionin oikeuden kanssa ottaen huomioon yleistä ja sähköisen viestinnän tietosuojasääntelyä koskevan oikeuskäytännön.

8.1.3 ALUEELLINEN SOVELTAMISALA

SVPL 2 §:n soveltamisalasäännös rajoittaa tarpeettomasti Suomeen sijoittautuneiden toimijoiden mahdollisuuksia tarjota radiolähetteiden havainnointiin perustuvia palveluita esimerkiksi satelliittien avulla, vaikka ulkomaille sijoittautuneet palveluntarjoajat kykenevät tarjoamaan kyseisiä palveluita huomattavasti pienemmillä rajoituksilla.

SVPL 2 §:n soveltamisalasäännös on vaikeaselkoinen koska se on kirjoitettu vastaamaan sähköisten viestintäverkkojen ja -palvelujen yhteisestä sääntelyjärjestelmästä annetun Euroopan parlamentin ja

neuvoston direktiivi 2002/21/EY (puitedirektiivi) mukaisia viestintäpalveluita, jolloin määritelmä ei kattanut eurooppalaisesta sähköisen viestinnän säännöstöstä annetun Euroopan parlamentin ja neuvoston direktiivin (EU) 2018/1972 mukaisia henkilöiden välisiä viestintäpalveluita. Soveltamisalasäännös ei ole myös johdonmukainen kyberturvallisuuslain (124/2025) 6 §:n 2 momentin kanssa, jonka mukaan riippumatta valtiosta, johon toimija on sijoittautunut, kyberturvallisuuslakia sovelletaan yleisen sähköisen viestintäverkon tarjoajaan ja yleisesti saatavilla olevan sähköisen viestintäpalvelun tarjoajaan silloin kun se tarjoaa palvelujaan Suomessa. Lisäksi muutenkin "sähköisiä viestintäpalveluja koskevien valvontamenettelyjen toimittaminen kuuluu sen jäsenvaltion viranomaisille, jossa kyseisten palvelujen vastaanottajat asuvat" (asia C-475/12, UPC DTH, 30.4.2014, EU:C:2014:285, kohta 88). SVPL 2 §:n tulisi selkeästi ottaa kantaa kaiken sähköisen viestinnän tietosuojadirektiivin toimeenpanemiseksi annetun kansallisen lainsäädännön alueelliseen soveltamisalaan.

Arvioitaessa SVPL 17 luvun säännöksiä voitaisiin harkita selvitettävän, että voitaisiinko mahdollistaa teleyritysten oma-aloitteiset toimenpiteet viestintäverkkojen kautta ohjattujen miehittämättömien ilma-alusten ym. havaitsemiseksi ja seuraamiseksi viranomaisten tukemista varten.

Ilmarinen Tuure
Liikenne- ja viestintävirasto (Traficom) - Kyberturvallisuuskeskus