SOK – Suomen Osuuskauppojen Keskuskunta

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?

SVPL:n viestintäsalaisuutta koskeva sääntely on kansainvälisesti poikkeuksellisen tiukkaa. Useimmissa EU:n jäsenvaltioissa työnantajan oikeudet valvoa yrityksen viestintäjärjestelmien käyttöä on toteutettu joustavammin, esimerkiksi oikeutetun edun tai työnantajan omai-suuden suojan perusteella, tietosuojasääntelyn ja työoikeuden yleisten periaatteiden nojalla. Suomessa sen sijaan viestintäsalaisuuden suoja on ulotettu perustuslain 10 §:n 2 momentin tasolla koskemaan myös työnantajan omistaman viestintäjärjestelmän kautta lähetettyjä viestejä.

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?

SVPL:n rajoitukset johtavat käytännön haasteisiin kansainvälisesti suosittujen ja alansa joh-tavien tietoturva- ja viestintätyökalujen perusominaisuuksien hyödyntämisessä. Modernien tietoturvaratkaisujen vakio-ominaisuuksiin kuuluu esimerkiksi Data Loss Prevention (DLP) -järjestelmät, jotka estävät arkaluonteisten tietojen lähettämisen sähköpostitse, sähköpostilii-kenteen automaattinen suodatus ja valvonta tietoturvauhkien tunnistamiseksi sekä tiedosto-jen latauksen valvonta ja esto kielletyille verkkosivustoille. Kansainväliset palveluntarjoajat eivät kustomoi tuotteitaan Suomen kokoisen markkinan takia, mikä asettaa suoraan suoma-laiset yritykset epäedulliseen asemaan suhteessa muiden EU-maiden yrityksiin, jotka voivat hyödyntää samojen työkalujen täyttä toiminnallisuutta ilman vastaavia oikeudellisia esteitä. Tämä on myös kilpailukykyhaitta suomalaisille yrityksille unionin sisämarkkinoilla. Tekoälyn teollisen skaalan hyödyntäminen edellyttää tekoälyn tehokasta valvontaa, jolloin laajamittais-ta ja kiihtyvän tahdin kehitystä voidaan tehdä valvonnan (ns. turvakaiteet) suojassa turvallisesti. Lisäksi on huomionarvoista, että nykyisissä olosuhteissa kyberturvallisuuskyvyk-kyyksien täysimittainen hyödyntäminen on laajemmankin turvallisuuden ja valmiuden kannalta ensiarvoisen tärkeätä.

Yleisellä tasolla olisi toivottavaa, että lainsäädäntöä mukautettaisiin huomioomaan myös kansallisen tason huoltovarmuustarpeet.

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?

EU:n yleinen tietosuoja-asetus (GDPR) asettaa rekisterinpitäjälle velvollisuuden toteuttaa asianmukaiset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi (32 ar-tikla) sekä velvollisuuden ilmoittaa tietoturvaloukkauksista (33–34 artiklat). Työnantaja on rekisterinpitäjänä vastuussa siitä, ettei henkilötietoja päädy asiattomille tahoille. SVPL:n kansallinen sääntely kuitenkin rajoittaa merkittävästi työnantajan mahdollisuuksia rakentaa teknisiä kontrolleja, joilla voitaisiin estää työntekijöitä lähettämästä vahingossa tai tarkoituksella henkilötietoja sähköpostitse väärälle vastaanottajalle, havaita henkilötietojen tietosuojalouk-kauksia viestintäjärjestelmissä tai selvittää toteutuneita poikkeamia.

Vuokraus- ja kiertotalousliiketoiminnan yleistyminen tuo esiin lisäulottuvuuden SVPL:n rajoitusten ongelmallisuudesta. Kun yritykset vuokraavat kalustoa, ajoneuvoja tai muuta omai-suutta, omaisuuteen liitettyjen paikannuslaitteiden tuottama data on tyypillisesti SVPL:n 20 luvussa (160–162 §) tarkoitettua sijaintitietoa, ei välitystietoa, sillä sijainnin ilmaisevaa tietoa käytetään muuhun tarkoitukseen kuin viestintäpalvelun toteuttamiseen. Vuokrausliiketoimin-nassa omaisuuden omistajalla on perusteltu tarve seurata vuokrakalustonsa sijaintia ja käyt-töä rikoksen estämiseksi tai omaisuuden takaisinsaamiseksi. SVPL:n sijaintitietoja koskevat säännökset rajoittavat kuitenkin tätä mahdollisuutta, sillä sijaintitietojen käsittely edellyttää luonnollisen henkilön suostumusta siltä osin kuin sijaintitieto on yhdistettävissä luonnolliseen henkilöön. Käytännössä vuokrausliiketoiminnassa laitteen tai ajoneuvon sijaintitieto on lähes aina yhdistettävissä vuokraajaan, jolloin suostumusvaatimus soveltuu. GDPR:n mukaisen pätevän suostumuksen edellytykset ovat kuitenkin yritykselle raskaita, ja suostumuksen peruuttamismahdollisuus tekee seurannasta haastavaa huomioiden yrityksen tarpeen var-mistaa vuokrauskaluston sijainti rikoksien ja väärinkäytöksien estämiseksi tai omaisuuden takaisinsaamiseksi.

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?

SVPL 272 §:n mukainen tietoturvaoikeus kattaa nykymuodossaan ainoastaan viestintäverk-kojen tai niihin liitettyjen palvelujen sekä tietojärjestelmien tietoturvalle haittaa aiheuttavien häiriöiden havaitsemisen, estämisen ja selvittämisen. Tämä rajaus on ongelmallinen erityisesti EU:n finanssialan digitaalista häiriönsietokykyä koskevan asetuksen (EU) 2022/2554 (DORA) valossa.

DORA-asetus edellyttää finanssiyhteisöiltä kattavaa TVT (eli ICT) -riskienhallintaa, johon kuuluu muun muassa tietojen vuotamisen estäminen ja datan suojaaminen tiedonhallinnan riskeiltä, kuten esimerkiksi inhimillisiltä virheiltä (DORA 9 artikla, DLP-kyvykkyydet) sekä toimintatavat poikkeamien havaitsemiseen, reagointiin ja hallintaan (DORA 10-11 artiklat ja III luku). DORA-asetuksen velvoitteiden tehokas täyttäminen edellyttää sekä ennaltaehkäiseviä toimenpiteitä, kuten luottamuksellisen tiedon jakamisen rajoitukset, että tapahtuneiden poik-keamien ja tietovuotojen nopeaa havaitsemista ja hallintaa. Kattava tiedon luottamuksellisuu-den varmistaminen ja tiedon menettämisen estäminen edellyttää myös juuri sellaisia automaattisia sähköisen viestinnän valvonta- ja estomekanismeja, joiden käyttö SVPL:n säännösten puitteissa on oikeudellisesti haastavaa. Tilanne on erityisen ongelmallinen, koska DORA on suoraan sovellettava EU-asetus, joka asettaa finanssialan toimijoille NIS2-direktiivin velvoitteita pidemmälle menevän velvoitteen kyberuhkiin varautumiseen. Kansalli-nen lainsäädäntö voi siten olla suorassa ristiriidassa EU:n asetustason sääntelyn kanssa erityisesti finanssialan toimijoiden osalta.¨

SVPL:n nykyiset yhteisötilaajan käsittelyoikeudet (146–156 §) sallivat välitystietojen käsitte-lyn vain viestintäverkon luvattoman käytön tai liikesalaisuuksien paljastamisen ehkäise-miseksi ja selvittämiseksi. Henkilötietojen suojaaminen ei ole itsenäinen käsittelyperuste.

Tämä johtaa tilanteeseen, jossa poikkeamien havaitseminen jää lähinnä työntekijän oman rehellisyyden/toiminnan varaan, koska työnantaja ei voi rakentaa automaattisia järjestelmiä, jotka havaitsisivat henkilötietoja sisältävien viestien lähettämisen organisaation ulkopuolelle. Poikkeaman selvittäminen voi lisäksi edellyttää työntekijän suostumusta, koska SVPL 136 §:n 3 momentin mukaan muita sähköisiä viestejä ja välitystietoja saa käsitellä viestinnän osapuolen suostumuksella tai jos laissa niin säädetään. Jos kyse on väärinkäytöksestä, on sisäisesti ristiriitaista, että selvittäminen edellyttäisi epäillyn omaa suostumusta. Toisaalta työnantaja ei myöskään kykene suojaamaan työntekijää vahingossa tapahtuvilta poikkeamil-ta, vaikka inhimilliset virheet ovat yleisiä ja tekninen esto olisi sekä työnantajan että työntekijän edun mukainen.

Tekoälytyökalujen nopea yleistyminen työympäristöissä on lisännyt riskiä tietojen tahattomasta vuotamisesta. Työntekijät voivat syöttää luottamuksellisia tietoja tai henkilötietoja tekoälypalveluihin tiedostamatta seurauksia, ja tiedot voivat päätyä kolmansille osapuolille esimerkiksi sähköpostiviestin liitteenä, kopioimalla verkkolomakkeelle tai lataamalla tiedostoja ulkoisiin palveluihin. Valvonnan näkökulmasta tekoälyn ja työntekijän oman toiminnan erot-taminen toisistaan on haastavaa, sillä tekoälyavusteiset työkalut voivat generoida ja lähettää viestejä työntekijän puolesta, ja rajankäynti sen suhteen, mikä on "työntekijän viesti" ja mikä "automaattisesti generoitu viesti", muuttuu epäselväksi.

Työnantajan pitää voida valvoa ja estää työnantajan tiedostojen lataaminen verkkosivustoille, mukaan lukien kielletyt tekoälytyökalut, ilman pelkoa siitä, että rikotaan viestintäsalaisuutta. Nykyinen SVPL ei tarjoa tähän riittävää oikeusperustaa, vaikka kyse on työnantajan omaisuuden, liikesalaisuuksien ja henkilötietojen suojaamisesta.

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.)

-

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?

-

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?

SVPL:n sääntely perustuu rakenteeltaan vuoden 2004 sähköisen viestinnän tietosuojalakiin ja sitä edeltäneeseen sääntelyyn. Tuolloin sähköisen viestinnän valvonta tarkoitti käytännössä manuaalista viestien lukemista. Nykyinen teknologia mahdollistaa sähköisen viestinnän tehokkaan valvonnan myös ilman manuaalista puuttumista viestien sisältöön. Automaattiset DLP-järjestelmät tunnistavat henkilötietoja ja estävät niiden lähettämisen ilman, että kenen-kään tarvitsee lukea viestiä. Tekoälypohjaiset luokittelujärjestelmät tunnistavat arkaluonteisen sisällön metatietojen ja mallien perusteella, ja koneoppimiseen perustuvat poikkeamien havaitsemisjärjestelmät tunnistavat epätavallisen viestintäkäyttäytymisen tilastollisesti.

Näillä järjestelmillä voidaan toteuttaa tehokasta valvontaa tavalla, joka puuttuu viestintäsalaisuuteen huomattavasti vähemmän kuin manuaalinen käsittely. SVPL ei kuitenkaan nykymuodossaan erota automaattista teknistä valvontaa manuaalisesta viestien lukemisesta riittävästi.

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?

-

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?

-

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?

-

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?

-

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

-

4.3 Millaisia vaikutuksia mahdollisilla eroilla sääntelyssä voi olla tai on ollut 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?

-

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?

-

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?

-

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?

-

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?

-

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?

-

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?

-

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

-

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?

8. Ehdotukset sääntelyn muuttamiseksi

8.1 SVPL 146 §:n muuttaminen – Yhteisötilaajan käsittelyoikeuksien laajentaminen

Nykyinen 146 § 1 momentti:

Yhteisötilaajalla on oikeus käsitellä välitystietoja maksullisen tietoyhteiskunnan palvelun, viestintäverkon tai viestintäpalvelun luvattoman käytön taikka rikoslain 30 luvun 11 §:ssä tarkoitettujen liikesalaisuuksien paljastamisen ehkäisemiseksi ja selvittämiseksi siten kuin tämän lain 147–156 §:ssä säädetään.

Ehdotettu 146 § 1 momentti:

Yhteisötilaajalla on oikeus käsitellä välitystietoja seuraavien tarkoitusten toteuttamiseksi siten kuin tämän lain 147–156 §:ssä säädetään:

1. tietoyhteiskunnan palvelun, viestintäverkon tai viestintäpalvelun luvattoman käytön taikka muun viestintäverkon tai viestintäpalvelun käyttöä koskevan ohjeen vastaisen menettelyn ehkäisemiseksi ja selvittämiseksi;

2. rikoslain 30 luvun 11 §:ssä tarkoitettujen liikesalaisuuksien paljastamisen ehkäisemiseksi ja selvittämiseksi;

3. luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679 (yleinen tietosuoja-asetus) 4 artiklan 12 kohdassa tarkoitettujen henkilötietojen tietoturvaloukkausten ehkäisemiseksi ja selvittämiseksi; sekä

4. yhteisötilaajan viestintäverkon tai viestintäpalvelun avulla tapahtuvien muiden väärinkäytösten tai vahinkojen ehkäisemiseksi ja selvittämiseksi.

Perustelut: Nykyinen 146 § rajaa yhteisötilaajan käsittelyoikeuden yksinomaan tietoverkon luvattomaan käyttöön ja liikesalaisuuksien paljastamiseen. Ehdotetulla 3 kohdalla käsittelyoikeus laajenisi kattamaan henkilötietojen suojaamisen, mikä on välttämätöntä GDPR:n rekisterinpitäjälle asettamien velvoitteiden ja DORA-asetuksen edellyttämien TVT-riskienhallintatoimenpiteiden täyttämiseksi. Ehdotetulla 4 kohdalla katettaisiin myös muut väärinkäytös- ja vahinkotilanteet, mukaan lukien tahaton tietojen vuotaminen. Nykyisen 1 kohdan muotoilua laajennettaisiin kattamaan myös muu kuin tahallisesti luvaton käyttö.

SVPL 272 § 1 momentin muuttaminen

Nykyinen 272 § 1 momentti:

Viestinnän välittäjällä ja lisäarvopalvelun tarjoajalla sekä niiden lukuun toimivalla on oikeus ryhtyä 2 momentissa tarkoitettuihin välttämättömiin toimiin tietoturvasta huolehtimiseksi:

1. viestintäverkkojen tai niihin liitettyjen palvelujen sekä tietojärjestelmien tietoturvalle haittaa aiheuttavien häiriöiden havaitsemiseksi, estämiseksi, selvittämiseksi ja esitutkintaan saattamiseksi;

2. viestin lähettäjän tai viestin vastaanottajan viestintämahdollisuuksien turvaamiseksi; tai

3. viestintäpalvelujen kautta laajamittaisesti toteutettavien rikoslain 37 luvun 11 §:ssä tarkoitettujen maksuvälinepetosten valmistelun ehkäisemiseksi.

Ehdotettu 272 § 1 momentti:

Viestinnän välittäjällä ja lisäarvopalvelun tarjoajalla sekä niiden lukuun toimivalla on oikeus ryhtyä 2 momentissa tarkoitettuihin välttämättömiin toimiin tietoturvasta ja tietosuojasta huolehtimiseksi:

1. viestintäverkkojen tai niihin liitettyjen palvelujen sekä tietojärjestelmien tietoturvalle haittaa aiheuttavien häiriöiden havaitsemiseksi, estämiseksi, selvittämiseksi ja esitutkintaan saattamiseksi;

2. viestin lähettäjän tai viestin vastaanottajan viestintämahdollisuuksien turvaamiseksi;

3. viestintäpalvelujen kautta laajamittaisesti toteutettavien rikoslain 37 luvun 11 §:ssä tarkoitettujen maksuvälinepetosten valmistelun ehkäisemiseksi;

4. tietoturvaloukkausten ehkäisemiseksi ja havaitsemiseksi, mukaan lukien erityisiin henkilötietoryhmiin kuuluvien, laajamittaisten henkilötietojen, liikesalaisuuksien tai muun suojaamisen arvoisen tieto-omaisuuden oikeudettoman siirtämisen estäminen viestintäverkon tai viestintäpalvelun kautta; tai

5. tiedostojen ja tietojen oikeudettoman siirtämisen estämiseksi viestintäverkon kautta sellaisille verkkosivustoille tai palveluihin, jotka yhteisötilaaja on 147 §:n 3 momentissa tarkoitetuissa ohjeissa yksilöinyt kielletyiksi.

Perustelut: Nykyinen 272 § mahdollistaa tietoturvatoimenpiteet, mutta sen tarkoitusperusteet eivät kata henkilötietojen suojaamista eivätkä tiedostojen latauksen estoa kiellettyihin palveluihin. Ehdotetulla 4 kohdalla mahdollistettaisiin automaattiset DLP-järjestelmät henkilötietojen suojaamiseksi. Tämä on erityisen tärkeää DORA-asetuksen velvoittamille finanssialan toimijoille, joilta edellytetään kattavaa TVT-riskienhallintaa, joka ei rajoitu pelkästään henkilötietoihin vaan kattaa myös pankkisalaisuuden piiriin kuuluvat yritysasiakkaiden tiedot sekä yritysturvallisuuteen liittyvät tiedot, jotka eivät aina ole liikesalaisuuksia. Ehdotetulla 5 kohdalla mahdollistettaisiin tiedostojen latauksen esto kiellettyihin palveluihin, mukaan lukien kielletyt tekoälytyökalut, ilman viestintäsalaisuuden loukkauksen riskiä.

SVPL 272 § 2 momentin muuttaminen: Automaattisen valvonnan erityisasema

Nykyinen 272 § 2 momentti:

Edellä 1 momentissa tarkoitetut toimet voivat käsittää:

4. viestin sisältöä koskevan automaattisen selvittämisen;

5. viestien välittämisen ja vastaanottamisen automaattisen estämisen tai rajoittamisen;

6. tietoturvaa vaarantavien haitallisten tietokoneohjelmien automaattisen poistamisen viesteistä;

7. muut 1–3 kohdassa tarkoitettuihin rinnastettavat teknisluonteiset toimenpiteet.

Ehdotettu 272 § 2 momentti:

Edellä 1 momentissa tarkoitetut toimet voivat käsittää:

1. viestin sisältöä koskevan automaattisen selvittämisen;

2. viestien välittämisen ja vastaanottamisen automaattisen estämisen tai rajoittamisen;

3. tietoturvaa vaarantavien haitallisten tietokoneohjelmien automaattisen poistamisen viesteistä;

4. tiedostojen ja tietojen siirtämisen automaattisen estämisen tai rajoittamisen ennalta määriteltyjen sääntöjen perusteella;

5. muut 1–4 kohdassa tarkoitettuihin rinnastettavat teknisluonteiset toimenpiteet.

Edellä 1–5 kohdissa tarkoitetut automaattiset toimenpiteet, joissa yksittäisen viestin sisältö ei tule luonnollisen henkilön tietoon, puuttuvat luottamuksellisen viestin ja yksityisyyden suojaan vähemmän kuin manuaalinen käsittely. Tällaisten automaattisten toimenpiteiden käyttöönotto ei edellytä 3 momentissa tarkoitettua manuaalista käsittelyä koskevien edellytysten täyttymistä.

Perustelut: Nykyinen laki ei tee riittävää eroa automaattisen algoritmipohjaisen käsittelyn ja manuaalisen käsittelyn välillä niiden perusoikeusvaikutusten osalta. Perustuslakivaliokunta on johdonmukaisesti katsonut, että automaattinen tietojenkäsittely puuttuu yksityisyyden suojaan vähemmän kuin manuaalinen käsittely. Ehdotetulla lisäyksellä tunnustettaisiin tämä periaate nimenomaisesti lakitekstissä, mikä mahdollistaisi nykyaikaisten DLP- ja tietoturvatyökalujen käyttöönoton ilman tulkintaepävarmuutta.

8.4 SVPL 149 § 1 momentin muuttaminen: Automaattisen haun perusteet

Nykyinen 149 § 1 momentti:

Yhteisötilaaja saa käsitellä välitystietoja automaattisen hakutoiminnon avulla, joka voi perustua viestien kokoon, yhteenlaskettuun kokoon, tyyppiin, määrään, yhteystapaan tai kohdeosoitteisiin.

Ehdotettu 149 § 1 momentti:

Yhteisötilaaja saa käsitellä välitystietoja automaattisen hakutoiminnon avulla, joka voi perustua viestien kokoon, yhteenlaskettuun kokoon, tyyppiin, määrään, yhteystapaan, kohdeosoitteisiin,

liitetiedostojen metatietoihin tai muihin ennalta määriteltyihin viestinnän ominaisuuksiin, jotka ilmentävät 146 §:ssä tarkoitetun väärinkäytöksen tai vahingon riskiä.

Perustelut: Nykyinen automaattisen hakutoiminnon perusteiden luettelo on tyhjentävä ja heijastaa 2000-luvun alun teknologista ympäristöä. Ehdotettu muotoilu mahdollistaa nykyaikaisten tietoturvatyökalujen tehokkaamman käytön ilman, että työnantajan tarvitsee rajoittua vanhentuneisiin parametreihin.

8 Muut huomiot

8.1 Tässä voitte esittää mahdolliset muut huomionne selvitystä varten.

-

Salokangas Jussi
SOK – Suomen Osuuskauppojen Keskuskunta - Lakiosasto