Finanssiala ry

Lausunto

22.01.2026

Asia: VN/26633/2024

Lausuntopyyntö perustuslain 10 §:n tarkistamista valmistelleen työryhmän mietinnöstä

Lausunnonantajan lausunto

1. Mietinnössä ehdotetaan, että perustuslain 10 §:n 2 momentissa säädettäisiin yleisesti kaiken luottamuksellisen viestin salaisuuden loukkaamattomuudesta. Nimenomaiset viittaukset kirjeen ja puhelun luottamuksellisuuteen poistettaisiin säännöstekstistä.
Pidättekö kyseistä muutosta perusteltuna? Miten arvioitte ehdotettua säännöstekstiä ja sen perusteluja?

FA katsoo, että esitetty muutos teknologianeutraaliudessaan on perusteltu ja mahdollistaa teknologioiden kehittyessä soveltamisen myös mahdollisiin uusiin viestintäteknologian muotoihin. Sääntelyn soveltaminen yhdenmukaisesti kaikkiin viestinnän muotoihin selkeyttää oikeustilaa eikä heikennä perusoikeussuojaa.

FA yhtyy Elinkeinoelämän keskusliiton (EK) lausuntoon siitä, että teknologianeutraali tulkinta ei saa kuitenkaan johtaa velvoitteisiin, jotka tosiasiallisesti heikentävät viestinnän tietoturvallisuutta tai nykyaikaisten viestintäpalvelujen suojaustasoa. Digitaalisissa palveluissa salaus ja korkea tietoturvan taso turvaavat viestinnän luottamuksellisuuden suojaa.

2. Perustuslain 10 §:n 3 ja 4 momentteihin lisättäisiin rajoitusperuste, joka mahdollistaisi kotirauhan suojan ja luottamuksellisen viestin salaisuuden suojan rajoittamisen tiedon hankkimiseksi yksilön tai yhteiskunnan turvallisuutta vakavasti uhkaavan vakavan rikollisuuden torjumiseksi (ns. uhkaperusteinen rikostiedustelu).

Pidättekö kyseistä muutosta perusteltuna? Miten arvioitte ehdotettua säännöstekstiä ja sen perusteluja?

FA haluaa nostaa esille olevan tärkeää varmistaa, etteivät lakivaraukset aiheuta sähköisen viestinnän palveluista annetun lain (SVPL) jo valmiiksi tiukan tulkinnan kaventumista erityisesti huomioiden nykypäivän uhkaympäristö ja yhteiskunnan kriittiset toimialat. Perustuslain 10 §:n ei tule muodostua esteeksi mahdollisille työelämän tietosuojalainsäädäntöä koskeville uudistuksille, joilla mahdollistettaisiin modernien tietoturvaratkaisujen käyttöönotto (esim. data loss prevention -ohjelmistot). Sidosryhmät ovat nostaneet asiaa esiin esimerkiksi lausunnossaan työ- ja

elinkeinoministeriön työryhmälle (TEM055:00/2025), joka on arvioinut työelämän tietosuojalain muutostarpeita. Tämä olisi tärkeää myös siksi, ettei PL 10 §:n 4 momentin (viestin salaisuus) sisältämä lakivaraus huomioi perusoikeuksien, muun muassa elinkeinovapauden, turvaamista rajoitusperusteena.

Edelleen FA huomauttaa, että PL 10 §:n muutoksilla voi olla suoria vaikutuksia mahdollisiin SVPL:n muutoksiin. Laissa sähköisen viestinnän palveluista tulee mahdollistaa kriittisten toimialojen työnantajille (eli laissa mainituille ”yhteisötilaajille” siltä osin kuin ne ovat DORA-asetuksen ja kyberturvallisuusdirektiivin piirissä) sähköisen viestinnän sisällön ja välitystietojen valvonta käyttäjien väärinkäytösten ja tahallisten ja tahattomien tietovuotojen ehkäisemiseksi, havaitsemiseksi ja selvittämiseksi sekä muiden oikeutettujen etujen turvaamiseksi. On huomioitava, että finanssiyhteisöjen osalta suora velvoite ehkäistä tietovuotoja on kodifioitu nimenomaisesti EU:n komission delegoidun asetuksen (2024/1774) 14 artiklaan. Laissa mainitut keinot eivät vastaa nykyisiä tarpeita, sillä voimassa olevan sääntelyn keinojen pääpaino on viestinnän luottamuksellisuuden ja yksityisyyden suojan varmistamisessa (esimerkkinä lain 272 §, jossa velvoite ottaa käyttöön toimenpiteitä tietoturvan toteuttamiseksi on mahdollista vain tiettyihin tarkoituksiin kuten viestin vastaanottajan ja lähettäjän viestintämahdollisuuksien turvaamiseksi).

3. Mietinnössä ehdotetaan tiedustelutoimivaltuuksien käyttämisen mahdollistamista kotirauhan suojaamissa tiloissa. Perustuslain 10 §:n 3 momenttiin lisättäisiin nykyistä 4 momenttia vastaava rajoitusperuste, joka mahdollistaisi kotirauhan suojan rajoittamisen tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta.

Pidättekö kyseistä muutosta perusteluna? Miten arvioitte ehdotettua säännöstekstiä ja sen perusteluja?

Ei lausuttavaa.

4. Mietinnössä ehdotetaan perustuslain 10 §:n 3 ja 4 momenttien sanamuotojen muuttamista vastaamaan perustuslakivaliokunnan tulkintakäytännössä tapahtunutta kehitystä. Molemmissa momenteissa käytettäisiin ilmaisua ”rikosten estämiseksi ja selvittämiseksi”.

Pidättekö kyseistä muutosta perusteltuna? Miten arvioitte ehdotettua säännöstekstiä ja sen perusteluja?

FA pitää esitettyä muutosta järkevänä ja perusteltuna lähestymistapana, joka mahdollistaa paremmin ennakoivan lähestymistavan kuin nykyinen sanamuoto.

5. Pidättekö perusteltuina mietinnön liitteessä esitettyä arviointia ja johtopäätöksiä kotirauhan suojan rajoittamista koskevan lakivarauksen ja Euroopan unionin lainsäädännön suhteesta?

Ei lausuttavaa.

6. Muut huomionne työryhmän mietinnöstä

FA pitää lähtökohtaisesti perusteltuna, että perustuslakiin lisätään mahdollisuus rajoittaa kotirauhan ja viestinnän suojaa silloin, kun kyse on yksilön tai yhteiskunnan turvallisuutta vakavasti uhkaavien rikosten torjunnasta. Samalla FA korostaa, että kyberuhkat kohdistuvat laajasti myös yksityisen sektorin toimijoihin, eivätkä vain viranomaisiin.

FA haluaa kiinnittää huomiota siihen, että yhteiskunnan toiminnan kannalta kriittisiä toimijoita on julkisen sektorin lisäksi yksityisellä sektorilla, joista osalla on merkittävä rooli osana yhteiskunnan huoltovarmuuden turvaamista. Kriittinen toiminta on yhä laajemmin siirtynyt myös yksityisen sektorin toimijoiden vastuulle ja on ehdottoman tärkeää, että yksityisellä sektorilla on riittävät mahdollisuudet ja keinot tunnistaa sekä hallita tähän liittyviä riskejä. Kriittisiin yksityisen sektorin toimijoihin kohdistuvat kyberturvallisuuteen liittyvät uhat ja poikkeamat eivät ole vain ulkoisia, vaan niitä voi ilmetä myös organisaation omien palomuurien ja turvakehikon (security paerimeter) sisältä. Sisäpiirissä ilmenevät turvallisuusuhat ovat vaikeasti hallittava ilmiö, jonka haasteisiin vastaamisen aikaikkuna kaventuu teknologian kehittymisen myötä.

Tämän vuoksi lainsäädännön tulisikin tarjota kriittisille toimijoille nykyistä selvästi tehokkaampia keinoja varmistaa tietojärjestelmiensä, käyttöympäristöjensä ja tietoverkkojensa sekä niitä hyödyntävien prosessien ja palvelujen turvallisuus myös sisäisten virheiden, vahinkojen ja väärinkäytösten varalta. FA painottaa, että DORA asetuksen velvoitteet eivät ole yhteensovitettavissa sääntelymallin kanssa, jossa viestinnän luottamuksellisuus muodostuu esteeksi välttämättömien tietoturvatoimien toteuttamiselle.

Perustuslakiin ehdotettu muutos on sinänsä kannatettava, ja FA katsoo ehdotetun sanamuodon mahdollistavan myös sellaisen tulevan lainsäädännön, jossa vakavan rikollisuuden ehkäisemiseksi välttämättömät toimenpiteet sallittaisiin viestinnän lähtökohtaisesta luottamuksellisuudesta huolimatta myös yksityisellä sektorilla. Mietinnön perustelut viittaavat siihen, että mahdollisuutta poiketa viestinnän luottamuksellisuudesta voitaisiin hyödyntää lähinnä vain viranomaissektorilla. Poikkeusmahdollisuuden soveltumista yksityiseen sektoriin ei ole erikseen käsitelty, mikä saattaa antaa virheellisesti sen käsityksen, että yksityiselle toimijalle ei voida laissa koskaan antaa mahdollisuutta käsitellä luottamuksellista viestiä esimerkiksi vakavan rikoksen torjumiseksi, vaikka ehdotetun uuden sanamuodon edellytykset muutoin täyttyisivät. Tähän liittyen vähintään esimerkinomainen viittaus yksityiseen sektoriin olisi tärkeä esimerkiksi kohdan 4.2 kolmannessa kappaleessa.

Lisäksi esimerkiksi kohdassa 2.5 Uhkaperusteinen rikostiedostelu (alkaen s. 22) nostetaan esiin kriittiseen infrastruktuuriin kohdistuvat uhat, mutta ei huomioida tämän erinäisissä laeissa (esim. NIS2-direktiivi ja finanssialaan kohdistuva lex specialis DORA-asetus) toimijoille asetettuja velvoitteita torjua ja estää muun muassa kyberuhkia. Olisi siis perusteltua, että perustuslain muutosta säädettäessä huomioitaisiin myös muut tahot kuin julkinen valta. FA painottaa, että DORA asetuksen velvoitteet eivät ole yhteensovitettavissa sääntelymallin kanssa, jossa viestinnän luottamuksellisuus muodostuu esteeksi välttämättömien tietoturvatoimien toteuttamiselle.

Karvinen Tuulia
Finanssiala ry