



Lausunto

01.06.2020

2630/2020 §57

Asia: VN/10579/2020

Lausuntopyyntö: Luonnos hallituksen esityksestä laiksi tartuntatautilain väliaikaisesta muuttamisesta: koronavirusepidemian tartuntaketjujen jäljittämistä ja katkaisua tehostava altistuneiden tunnistusjärjestelmä

Lausunnonantajan lausunto

Vastaajatahon virallinen nimi

Espoon kaupunki

Vastauksen kirjanneen henkilön nimi

-

Vastauksen vastuuhenkilön yhteystiedot

-

Onko vastaaja

kunta

Kysymyksiä esityksen tavoitteista ja vaikutuksista

Voidaanko ehdotetulla altistuneiden tunnistusjärjestelmällä mielestänne tehostaa koronavirusepidemian tartuntaketjujen jäljittämistä ja katkaisua?

Kyllä pääosin [Lausunnossa todetaan, että tunnistusjärjestelmä muodostuu kahdesta komponentista: mobiilisovelluksesta ja taustajärjestelmästä. Tunnistusjärjestelmällä, erityisesti mobiilisovelluksella, ei kyetä yksinään nujertamaan epidemiaa vaan sen käyttö on osa hallituksen hybridistrategiaa, jonka pohjana on testaa, jäljitä, eristä ja hoida -malli. Mikäli mallin muut palaset

eivät toimi, ei tunnistusjärjestelmästä ole merkittävää hyötyä. Kyse on kokonaisuudesta. Lausunnossa mainitaan, että tunnistusjärjestelmän käyttöönottoa kiirehditään. Tämä on ymmärrettävää vallitsevassa tilanteessa, mutta nopeuteen liittyy riskejä: Osataanko varmasti arvioida tunnistusjärjestelmän pidemmän aikavälin vaikutukset tietosuojan ja ihmisten sosiaaliseen käyttäytymiseen? Samanaikaisesti todetaan, että tunnistusjärjestelmästä on todennäköisesti hyötyä tartuntaketjujen jäljittämässä. Sovellus ei korvaa nykyistä jäljitystyötä, vaan täydentää sitä. Merkittävä varaus tarkoituksenmukaisuuteen liittyy sovelluksen käytön kattavuuteen: Kun kyse on vapaaehtoisesti, proaktiivisesti etukäteen ladattavasta älypuhelinsovelluksesta, kysymykseksi nousee, saadaanko vaadittava käyttäjämäärä kasaan, että sovelluksesta olisi tosiasiallisesti hyötyä. Koska sovelluksen käyttö perustuu vapaaehtoisuuteen, sen käyttöastetta ja sovelluksen käyttäjien halukkuutta jakaa tietojan viranomaiselle on vaikea arvioida. On tärkeää pohtia kriittisesti kalliin mobiilisovellusratkaisun tehokkuutta. Tämä on erityisen tärkeää ottaen huomioon sovelluksen avulla kerätty hyvinkin sensitiivinen data. Kyse on apuvälineestä, jonka toimivuus edellyttää laajaa testausta. On huolellisesti arvioitava, voidaanko sovelluksella saavuttaa merkittäviä hyötyjä, vaikka käyttöaste jäisi selvästi esityksessä arvioitua matalammaksi. Sovelluksen käyttöönotossa olisi panostettava viestintään, jotta se otettaisiin laajamittaisesti käyttöön ja sen avulla saavuttaisiin asetetut tavoitteet. Selvitystyön yhteydessä tulisi miettiä, millaisin keinoin ihmisiä voitaisiin kannustaa sovelluksen käyttöön. Henkilötietojen käsittelystä on aina kerrottava mahdollisimman läpinäkyvästi ja ymmärrettävästi kansalaisten luottamuksen takaamiseksi. Bluetooth-teknoologiaan liittyy myös epävarmuutta. Ilmeisesti yhteys kahden puhelimen välillä toimii vain muutaman metrin tarkkuudella. Bluetooth -teknoologiaan perustuva jäljitys ei ole täysin luotettavaa. Virheellistä tietoa syntyy esimerkiksi tilanteissa, joissa puhelinta käyttää on muu kuin sen ilmoitettu omistaja tai henkilöiden välissä on seinä tai muu este. Merkittävä riski on, että sovelluksen antama tieto olisi ainoa selvitys sovelluksen käyttäjistä, jota käytettäisiin tartunnan jäljitykseen ja jonka perusteella karanteenipäätökset tehtäisiin.]

Onko esityksessä asianmukaisesti otettu huomioon henkilötietojen ja yksityisyyden suojaan liittyvät näkökohdat?

Kyllä pääosin [Lausunnossa mainitaan, että mobiilisovelluksen käyttö on kansalaiselle vapaaehtoista ja maksutonta. Aitoon vapaaehtoisuuteen saattaa liittyä kysymyksiä mahdollisten lieveilmiöiden kohdalla, jos esimerkiksi työnantaja tai ravintola edellyttää sovelluksen asentamista. Käsiteltävien henkilötietojen tulee olla välttämättömiä käyttötarkoituksen saavuttamiseksi. Tietosuojan näkökulmasta tulisi pohtia minimointiperiaatteen mukaisesti, päästäisiinkö haluttuun lopputulokseen vähemmällä henkilötietojen käsittelyllä ja vähemmän yksityisyyden suojaan puuttuvalla tavalla. Kuten lausunnossa todetaan, tunnistusjärjestelmän tuottama lisähyöty riippuu siitä, miten usein henkilö ilmoittaisi altistumisestaan terveydenhuoltoon. Lisäksi sovelluksen käyttöasteen tulisi olla väestötasolla merkittävä. Haasteita liittyy myös teknoologiaan, sillä kaikilla ei ole riittävän modernia älypuhelinia, ja Bluetooth-signaali saattaa aiheuttaa virheellisiä positiivisia ja negatiivisia tuloksia. Jos kaikki riskit realisoituvat, lopputuloksena on puutteellinen tunnistusjärjestelmä ja samanaikaisesti todennäköisesti runsaasti sensitiivistä dataa kansalaisista keskitetyssä viranomaisjärjestelmässä. Henkilötietojen käsittelyperuste on avattu selkeästi luonnoksessa. Lisäksi luonnoksessa on arvioitu kattavasti rekisteröityihin kohdistuvia mahdollisia tunnistettuja riskejä ja miten niitä on kyetty minimoimaan.]

Onko esityksestä aiheutuvat taloudelliset vaikutukset arvioitu asianmukaisesti?

Kyllä pääosin [Keskitettyyn taustajärjestelmään tallennettaisiin runsaasti sensitiivistä dataa kansalaisista. Datan käsittelyyn liittyisi merkittäviä riskejä, joiden minimointi ja monitorointi vaatisi

jatkuvasti resursseja. Kyse ei olisi kertaluonteisesta investoinnista, sillä datan elinkaaren hallinnasta pitäisi huolehtia pidempään. Toisaalta lausunnossa mainitaan, että pseudonyymia tietoja säilytettäisiin taustajärjestelmässä ainoastaan 14 vuorokautta.]

Onko esityksestä aiheutuvat muut vaikutukset arvioitu asianmukaisesti?

Kyllä pääosin

Mahdolliset yksilöidyt pykälämuutosehdotukset

Ehdotuksenne 43 a §:n muutoksiksi (Terveiden ja hyvinvoinnin laitoksen tehtävät)

Katso lausuntopyyntöä kohta "Mahdolliset muut näkemyksenne esityksestä"

Ehdotuksenne 43 b §:n muutoksiksi (Kansaneläkelaitoksen tehtävät)

Katso lausuntopyyntöä kohta "Mahdolliset muut näkemyksenne esityksestä"

Ehdotuksenne 43 c §:n muutoksiksi (Altistuneiden tunnistusjärjestelmän yhteydessä tapahtuva tietojen käsittely)

Katso lausuntopyyntöä kohta "Mahdolliset muut näkemyksenne esityksestä"

Ehdotuksenne 43 d §:n muutoksiksi (Suhde 22 §:ssä säädettyyn ilmoitusvelvollisuuteen)

Katso lausuntopyyntöä kohta "Mahdolliset muut näkemyksenne esityksestä"

Ehdotuksenne 43 e §:n muutoksiksi (Altistuneiden tunnistusjärjestelmästä saadun altistumistiedon käsitteleminen)

Katso lausuntopyyntöä kohta "Mahdolliset muut näkemyksenne esityksestä"

Ehdotuksenne 43 f §:n muutoksiksi (Altistuneiden tunnistusjärjestelmän toteutuksen ohjaus)

Katso lausuntopyyntöä kohta "Mahdolliset muut näkemyksenne esityksestä"

Ehdotuksenne 43 g §:n muutoksiksi (Altistuneiden tunnistusjärjestelmän tietoturvallisuuden arvioiminen)

Katso lausuntopyyntöä kohta "Mahdolliset muut näkemyksenne esityksestä"

Ehdotuksenne 43 h §:n muutoksiksi (Valvonta)

Katso lausuntopyyntöä kohta "Mahdolliset muut näkemyksenne esityksestä"

Voimaantulosäännös: Ovatko esityksen voimaantulo- ja voimassaoloajat perusteltuja esityksen tavoitteiden saavuttamiseksi?

-

Muut huomiot esityksestä

Mahdolliset muut näkemyksenne esityksestä?

Tietojen välittäminen kunnan ja sairaanhoitopiirin terveydenhuollon toimintayksiköihin:

Lakiluonnoksen 43 b §:ssä on todettu ”Kansaneläkelaitos voi toteuttaa teknisen menetelmän, jolla altistumistiedot voidaan välittää kunnan tai sairaanhoitopiirin terveydenhuollon toimintayksikköön.” Hallituksen esityksen perusteella jää epäselväksi, kuinka tiedot käytännössä luovutetaan kuntien ja sairaanhoitopiirien terveydenhuollon toimintayksiköille, sillä teknistä menetelmää ei ole avattu hallituksen esityksessä enempää. Tämä on olennainen asia, sillä sujuva ja tietosuojalainsäädännön mukainen tietojen luovutus on edellytyksenä sille, että altistuneiden tunnistusjärjestelmästä saadaan olennaista hyötyä.

Hallituksen esityksen luvun kaksi mukaan kuntien ja sairaanhoitopiirien välinen työnjako vaihtelee alueittain ja tapauskohtaisesti mm. todetusta tapauksesta ja altistusten luonteesta johtuen. Teknisessä ratkaisussa on pystyttävä rajaamaan tiedonsaantioikeudet riittävän täsmällisesti niin, että tiedonsaantioikeudet kohdistuvat oikein.

Henkilötietojen käsittelytarkoitukset:

Hallituksen esityksen 43 c §:ää koskevissa perusteluissa on todettu ”Pykälän 1 momentissa säädettäisiin henkilötietojen käyttötarkoituksesta. Ehdotetun säännöksen mukaan altistuneiden tunnistusjärjestelmän yhteydessä voitaisiin käsitellä henkilötietoja koronavirusepidemian tartuntaketjujen jäljittämistä ja katkaisua varten siten kuin ehdotetussa luvussa säädetään. Henkilötietoja saisi käyttää ainoastaan ehdotetun luvun mukaisiin tarkoituksiin. Käyttötarkoitus rajattaisiin näin ollen ainoastaan säännöksessä mainittuun tarkoituksiin, eikä henkilötietoja saisi myöhemmin käyttää muihin tarkoituksiin. Altistuneiden tunnistusjärjestelmän avulla kerättyjä henkilötietoja ei siten voisi käyttää esimerkiksi kaupallisissa tai lainvalvonnallisissa tarkoituksissa.” Hallituksen esityksen perusteella jää vielä hieman epäselväksi, onko säännösehdotuksen tarkoituksena, että altistuneiden tunnistusjärjestelmässä käsiteltävien henkilötietojen toisiokäyttö ei olisi mahdollista muun lainsäädännön nojalla. Tätä tulisi selkeyttää.

Käsiteltävät henkilötiedot ja henkilötietojen luovutus:

Lakiluonnoksen 43 e §:n mukaan terveyden- ja hyvinvoinnin laitoksella on salassapitosäännösten estämättä oikeus luovuttaa kunnan tai sairaanhoitopiirin kuntayhtymän terveydenhuollon toimintayksikölle sellaiset 43 c §:n 2 momentin 5 kohdassa tarkoitettuun yhteydenottopyyntöön sisältyvät tiedot, jotka ovat tarpeellisia niille laissa säädettyjen tehtävien suorittamiseksi koronavirusepidemian yhteydessä. Riittävätkö ainoastaan yhteydenottopyyntöön sisältyvät tiedot terveydenhuollon toimintayksiköille, jotta toimintayksiköt pystyvät arvioimaan altistumista? Terveydenhuollon toimintayksiköillä ei olisi säännösehdotuksen perusteella oikeutta saada esim. tietoja kohtaamisen kestosta, ajankohdasta ja signaalin voimakkuudesta. Tiedonsaantioikeuksien riittävyttä tulisi arvioida huomioimalla hallintolaisissa säädetty selvitysvelvollisuus, sillä altistuneiden tunnistusjärjestelmässä käsiteltäviä henkilötietoja käytetään karanteenia koskevassa päätöksenteossa.

Hallituksen esityksen luvussa 3.1 on todettu, että terveydenhuolto antaa A:lle avauskoodin, jonka avulla hän itse voi luovuttaa oman tunnisteensa taustajärjestelmälle. Hallituksen esityksessä ei ole

tuotu esiin sitä, onko avauskoodi henkilötietoa ja mistä terveydenhuolto saa avauskoodin. Hallituksen esityksessä ei ole myöskään tuotu esiin pohdintaa siitä, tulisiko laissa säätää terveydenhuollolle oikeudet tähän avauskoodiin. Lakiluonnoksen 43 e §:ään kirjatut terveydenhuollon tiedonsaantioikeudet eivät sisällä oikeutta avauskoodiin.

Lakiluonnoksen 43 c §:ssä on lueteltu altistuneiden tunnistusjärjestelmän yhteydessä käsiteltävät henkilötiedot. Hallituksen esityksestä ei käy ilmi, onko listauksen tarkoitus olla tyhjentävä. Mm. lokitiedot puuttuvat lakiluonnoksen 43 c §:ssä luetelluista henkilötiedoista.

Tietoturvallisuus

Hallituksen esityksen 43 g §:ää koskevissa perusteluissa on todettu ”Tietoturvallisuuden arvioimisessa Kyberturvallisuuskeskus voisi hyödyntää tarkempia Terveyden ja hyvinvoinnin laitoksen altistuneiden tunnistusjärjestelmälle asettamia tietoturva vaatimuksia sekä arviointityössä yleisesti käytettyjä tietoturva vaatimuksia.” Altistuneiden tunnistusjärjestelmässä käsitellään terveydentilaa koskevia henkilötietoja. Mm. kansalaisten luottamuksen turvaamiseksi olisi asianmukaista, että lailla säädettäisiin keskeisistä tietoturva vaatimuksista taikka valvovalle viranomaiselle annettaisiin laissa oikeus antaa määräys tietoturva vaatimuksista.

Nykyaikaisen sovelluksen tai tietojärjestelmän kehittäminen tapahtuu jatkuvalla syklillä, ja on oletettavaa, että myös tämän seurantasovelluksen osalta kehittämistä tapahtuu myös käyttöönoton jälkeen. Perustelumateriaalissa esitetty Kyberturvallisuuskeskuksen aika ja kustannusarvio antaa oletuksen, että heidän tuottama arvio on kattava ja syväluotaava. Se koskee kuitenkin vain tiettyä ajanhetkeä. Jatkuvan tietoturvallisuuden valvonnan ja arvioinnin vastuu on esityksen mukaan Valviralla. Näin vaikuttavan ja huomiota herättävän sovelluksen tietoturvan varmistamiskäytäntönä ei voida pitää kertaluontoista arviointia, vaan sen tulee olla jatkuvaa.

On tärkeää, että julkisuuteen saatetaan tietoa tarpeeksi sovelluksen tietoturvasta ja sen valvonnasta. Tämä todennäköisesti edistäisi sovelluksenlaajaa käyttöönottoa ja toisi julkiseen, avoimeen keskusteluun sovelluksen tietosuojan – ja turvallisuuden oikeilla ja riittäväillä tiedoilla. Tähän liittyen tulisi harkita, että sovelluksen lähdekoodi julkaistaan mahdollisuuksien mukaan avoimena lähdekoodina, jolloin ulkopuoliset ja riippumattomat tahot, kuten tietoturvatutkijat, voivat tarkastella sitä vapaasti ja koodin mahdolliset haavoittuvuudet yms. tulisivat todennäköisesti nopeammin ilmi. Tämä avoimuus mahdollistaisi myös sovelluksen kriitikoille sen toimintaan tutustumisen, hälventäisi tietoturvaan liittyviä epäluuloja sekä kasvattaisi luottamusta sovellusta tuottavaan tahoon.

Lakiluonnoksen 43 a §:n mukaan Terveyden ja hyvinvoinnin laitos ylläpitää altistuneiden tunnistusjärjestelmää ja vastaa sen toiminnasta sekä tietoturvallisuuden hyväksymisestä ja voi asettaa altistuneiden tunnistusjärjestelmälle tarkempia toiminnallisia, teknisiä ja tietoturva vaatimuksia” Kansalaisluottamuksen kannalta ei ole perusteltua, että sama taho vastaa tunnistusjärjestelmän toiminnasta, asettaa sille tarkempia tietoturva vaatimuksia ja vastaa

tietoturvallisuuden hyväksymisestä. Perusteluissa tai lakitekstissä ei ollut mainintaa tai määritelmää sille, mitä tässä yhteydessä tarkoitetaan ”tietoturvallisuuden hyväksymisellä”, joten se jää epäselväksi.

Ilmoitusvelvollisuus

Hallituksen esityksen 43 d §:ää koskevissa perusteluissa on todettu ”Tartuntatautilain 22 §:ssä säädetty velvollisuus sairastuneen ja sairastuneeksi epäillyn henkilön ilmoitusvelvollisuudesta asiaa selvittävälle lääkärille tartuntataudin leviämisen estämiseksi ei koski altistuneiden tunnistusjärjestelmän kautta saatuja tietoja. Näiden tietojen ilmoittaminen, kuten mobiilisovelluksen käyttö muutoinkin, olisi vapaaehtoista ja perustuisi mobiilisovelluksen käyttäjän omaan päätökseen käyttää sovellusta ja toimittaa siitä saamansa altistumistiedot niin halutessaan kunnan tai sairaanhoitopiirin kuntayhtymän terveydenhuollon toimintayksikköön.” Ilmoitusvelvollisuuden näkökulmasta on tärkeää, että kansalaiset saavat sovelluksen käyttöönoton yhteydessä selkeää informaatiota siitä, miksi ilmoitusvelvollisuutta ei sovelleta sovelluksen käyttöön ja milloin kansalaisilla on normaalisti ilmoitusvelvollisuus. Muutoin ilmoitusvelvollisuusasia voi olla vaikeasti ymmärrettävä ja pahimmillaan johtaa siihen, että ilmoitusvelvollisuutta ei osata noudattaa silloin, kun sitä tulisi tartuntatautilain nojalla noudattaa.

THL:n ohjaus

Hallituksen esityksen luvun 4.2 mukaan ”Pilotointivaiheessa THL:n tulee myös arvioida ehdotetun altistuneiden tunnistusjärjestelmän avulla saatujen altistustietojen käsittelyyn liittyvän kansallisen ohjeistuksen tarvetta kunnille ja kuntayhtymille.” Lisäksi luvussa on todettu ”Suuri osa tunnistetuista voi olla sellaisia, joista ei jäljittämisen yhteydessä tehtävien yhteydenottojen perusteella selviä muita altistumiseen tai tartuntaan viittaavaa kuin mobiilisovelluksen avulla tapahtunut tunnistaminen. Tällöin tartuntataudeista vastaavalla lääkärillä tai muulla jäljitystyötä tekevällä terveydenhuollon ammattihenkilöllä ei ole lääketieteelliseen arvioon perustuvan päätöksenteon tueksi muuta tietoa kuin se, että käyttäjän mobiilisovellus on antanut tiedon henkilön altistumisesta. Erityisesti näiden henkilöiden osalta voi ilmetä tarvetta linjata kansallisesti, mitä jatkotoimia terveydenhuollon toimintayksiköltä taikka tartuntataudeista vastaavilta lääkäreiltä heidän suhteensa edellytetään.” Kansalliset linjaukset ja ohjeistukset altistuneiden tunnistusjärjestelmän keräämien henkilötietojen tulkinnasta ovat kannatettavia, sillä linjauksilla parannetaan kansalaisten yhdenvertaisuutta karanteenia koskevassa päätöksenteossa.

Ylikoski Elina
Espoon kaupunki - Kaupunginjohtaja Jukka Mäkelä