Turun yliopisto

Lausunto

05.05.2020

Asia: VN/10058/2020, STM053:00/2020

Lausuntopyyntö esityksestä kontaktien jäljityssovelluksen käyttöönotosta Covid-19-epidemian hallinnan tueksi

Kysymykset

1. Muistiossa esitellään mobiilisovellus tukemaan tartuntatautien jäljitystyötä ja tartuntaketjujen katkaisemista. Onko tämä tarkoituksenmukainen tapa jäljittää tartuntaketjuja?

ei pääosin

Avoimet huomiot koskien kysymystä 1

Lausuntopyynnön materiaaleissa ei kuvata sovellusta tai sen toimintaa tarkasti. Materiaalien perusteella ei voi saada tarkkaa kuvaa itse sovelluksesta tai sen toiminnasta. Tästä syystä huomiot voivat olla vain suuntaa antavia ja osin spekulatiivisia.

Keskeisiä oikeudellisia kysymyksenasetteluja on näkemyksemme mukaan joka tapauksessa kaksi.

1. Sovelluksella voidaan puuttua ja merkittävästi rajoittaa sen käyttäjien perusoikeuksia. Sovellus on suunniteltava siten, että tällaiset rajoitukset ovat hyväksyttäviä ja täyttävät perusoikeuksien rajoitusedellytykset.

2. Sovelluksella kerätään henkilötietoja. Sovellusta suunniteltaessa on otettava huomioon tietosuojaperiaatteet, erityisesti datan minimoinnin periaate.

Tämän kysymyksen osalta on on tärkeää tarkastella sovelluksen perusoikeusulottuvuutta.

Sovelluksessa kerätään väistämättä tietoa sen käyttäjien kontakteista toisiin käyttäjiin. Sovellus voi myös antaa julkiselle vallalle mahdollisuuden ryhtyä toimenpiteisiin, joilla konkreettisesti rajoitetaan henkilöiden perusoikeuksia. Terveysviranomaiset voisivat esimerkiksi määrätä käyttäjän, jonka on syytä epäillä saaneen tartunnan, eritykseen. Sovelluksen tieto- ja sen ympärille luotavan

viranomaistoimintojen arkkitehtuuri vaikuttaa merkittävästi siihen, miten sovelluksen avulla voidaan rajoittaa sen käyttäjien perusoikeuksia.

Tietoarkkitehtuurille on kaksi päävaihtoehtoa. Keskitetyssä arkkitehtuurissa tiedot, joita sovelluksella kerätään sen käyttäjien kontakteista, kerätään keskitettyyn tietokantaan. Karkeimmillaan tämä voisi tapahtua reaaliaikaisesti: sovellus tallentaa tiedot sen käyttäjien kontakteista keskitettyyn tietokantaan sitä mukaa kuin niitä kertyy.

Hajautetussa vaihtoehdossa kontaktitietoja ei kerätä keskitettyyn tietokantaan. Kun henkilöllä todetaan virustartunta, terveysviranomaiset saavat tämän suostumuksella käyttöönsä tiedot henkilön laitteen lähettämistä tunnistetiedoista esimerkiksi 14 päivän ajalta. Terveysviranomainen ei en sijaan saa käyttöönsä tietoja henkilön kontakteista. Kontaktit saavat tiedon altistuksestaan, kun terveysviranomaiset julkaisevat sairastuneen laitteen lähettämistä tunnistetiedoista ja sovellus havaitsee, että altistuneen laitteelle on tallentunut sairastuneen tunnistetieto. Näin toimii esimerkiksi 300 eurooppalaisen tutkijan muodostaman konsortion kehittämä DP-3T-protokolla.

Lausuntopyynnön taustamateriaalin perusteella näyttää siltä, että Suomeen kaavaillaan ns. hybridimallia. Kontaktitiedot pysyvät käyttäjien laitteilla, kunnes käyttäjä sairastuu. Diagnoosin jälkeen terveysviranomaiset saavat käyttöönsä tiedot sairastuneen laitteen rekisteröimistä kontakteista. Sovellus ohjaa tämän jälkeen virukselle altistuneet eristäytymään muista ihmisistä ja testeihin.

Lausunnon taustamateriaaleissa viitataan siihen, että terveysviranomaiset voisivat ylläpitää tietokantaa sovelluksen käyttäjien yhteistiedoista. Jos terveysviranomaisilla on tällainen tietokanta käytössään, he voivat kohdistaa aktiivisia toimenpiteitä sovelluksen käyttäjiin. Jos tällaista tietokantaa ei ole, terveysviranomaiset eivät voi tunnistaa altistuneita. Tietosuojalainsäädännön näkökulmasta tunnistamismahdollisuus on merkittävä. Bluetooth-laitteiden lähettämät tunnisteet eivät ole henkilötietoa, jos niitä ei voida liittää johonkin luonnolliseen henkilöön suoraan tai epäsuorasti.

Ensimmäinen olennainen oikeudellinen kysymys nousee esille, kun tarkastellaan, olisiko sovellus oikeudellisesti hyväksyttävä, jos se antaa terveysviranomaisille mahdollisuuden puuttua aktiivisesti käyttäjien perusoikeuksiin, esimerkiksi määräämällä heidät eristyksiin tartuntaepäilyn perusteella.

Tartuntatautilain 50 §:n mukaan virkasuhteinen kunnan tartuntataudeista vastaava lääkäri tai virkasuhteinen sairaanhoitopiirin kuntayhtymän tartuntataudeista vastaava lääkäri voi määrätä henkilön karanteeniin yhden kuukauden ajaksi. Päätös edellyttää, että henkilöllä on todettu yleisvaarallinen tartuntatauti yleisvaaralliselle tartuntataudille tai hänen on perustellusti epäilty altistuneen sille.

Kyse on osin suoraan laintulkintakysymyksestä. Jos kontaktirekisterisssä on merkintä, että sairastunut ja sovelluksen käyttäjä ovat tavanneet, onko käsillä perusteltu epäily siitä, että henkilö on altistunut tartuntataudille? Voidaanko hänet määrätä karanteeniin?

Kysymys on sovelluksen tehokkuudesta. Lausuntopyynnön taustamateriaaleissa ei ole tietoa siitä, voiko sovellus tuottaa luotettavaa tietoa siitä, ketkä ovat tosi asiassa altistuneita virukselle. Sovellus perustuu Bluetooth LE -teknologialle. Teknologialla on rajoitteensa. Laitteet rekisteröivät kontaktin, jos Bluetooth-signaali on riittävän voimakas. Signaalin voimakkuuteen vaikuttavat paitsi lähettimien etäisyys toisistaan myös niiden välissä olevat aineet. Teknologian rajoitteista johtuu, että sovelluksessa on merkittävä vaara sekä virheellisiin positiivisiin tartuntaepäilyihin että siihen, että todennäköisiä altistuksia jää huomaamatta.

On selvää, että kontakti rekisteröityy, jos käyttäjät ovat samassa tilassa riittävän pitkän ajan. Järjestelmä voi kuitenkin osoittaa, että henkilö on altistunut virukselle, vaikka tällaista mahdollisuutta ei tosi asiassa olisi. Esimerkiksi seinät tai lasi eivät aina estä Bluetooth-signaalin kulkua. Tästä seuraa, että kontakti voi kirjautua, vaikka henkilöt olisivat olleet eri tiloissa, esimerkiksi eri huoneistoissa tai autoissa pysäköintialueella.

Jos sovellus tuottaa merkittävän määrän perusteettomia tautiepäilyjä, on epäselvää, onko tartuntatautilääkäreillä oikeus tartuntatautilain perusteella määrätä epäiltyjä karanteenin pelkästään sovelluksen tuottaman tartuntaepäilyn perusteella. Karanteenimääräys rajoittaa merkittävästi yksilön perusoikeuksia. Jotta karanteenimääräykset ja perusoikeusrajoitukset olisivat perusteltuja, altistusepäilyn on oltava vahva. Tästä syystä tieto siitä, kuinka luotettavia sovelluksen antamat tiedot ovat, on tärkeä osa sovelluksen oikeudellisen hyväksyttävyyden arviointia. Jos sovellus tuottaa merkittävän määrän perusteettomia tautiepäilyjä, sitä ei voitane käyttää karanteenimääräysten perusteena.

Tutkimusnäytön perusteella näyttää siltä, että yksilöt ovat vuorokaudessa yhteydessä noin 13 toisen yksilön kanssa tavalla, jossa koronavirus voisi tarttua. Tutkimukset osoittavat kuitenkin, että ilman rajoitustoimenpiteitä koronaviruksen tarttuvuusluku korkeimmillaankin vain kolme koko sairauden ajalta. Näin on ilmeistä, että enin osa kontakteista ei saa tartuntaa, mutta heidät voitaisiin määrätä karanteeniin. Tämä oletettavasti johtaisi tilanteeseen, jossa sovelluksen lähettämän muutaman ensimmäisen mahdollisesti väärän hälytyksen jälkeen luottamus sovellukseen vähenisi ja samalla halukkuus hakeutua testeihin heikkenisi.

Kokemukset ulkomailta osoittavat, että sovellusten tehottomuus on vaikuttanut myös hallitusten päätöksiin. Belgian hallitus päätti luopua seurantasovelluksen kehittämisestä. Keskeisenä perusteluna toimi sovelluksen tehottomuus. Samanlaisia puheenvuoroja on esitetty myös Alankomaissa, joissa ensimmäisen vaiheen kaikki seitsemän sovellusta arvioitiin tietosuojan näkökulmasta riittämättömiksi.

Samat tehottomuusnäkökohdat tulevat esille, kun pohditaan, onko sovellus ylipäätään hyväksyttävä. Oikeus yksityisyyteen on perusoikeus. On selvää, että yksilöt menettävät osan yksityisyydestään, jos sovellus otetaan käyttöön. Tällainen perusoikeusrajoitus on mahdollinen vain, jos rajoitusperuste on hyväksyttävä. Tässä tapauksessa rajoitusperusteena on, että toimenpiteillä pyritään suojaamaan väestön terveyden suojaaminen. Jos toimenpiteet ovat tehottomia eikä niillä pystytä riittävässä määrin suojaamaan väestön terveyttä, ne eivät ole hyväksyttäviä. Perusteettomien tartuntaepäilyjen lisäksi arvioinnissa on otettava huomioon myös sovelluksen yleiset terveysvaikutukset. Sovelluksen tehokkuus riippuu ennen kaikkea siitä, kuinka laajalti se on käytössä. On esitetty, että sovellus tuottaisi merkittävää hyötyä vain, jos noin 40–60 prosenttia väestöstä käyttäisi sitä.

Samaan arvioon vaikuttavat myös ne altistukset, jotka jäävät huomaamatta. On esitetty, että virus voisi tarttua myös pinnoilta tai jopa aerosolitartuntana ilmasta, ainakin jonkin ajan sen jälkeen, kun kantaja on jo poistunut tilasta. Bluetooth-jäljitys ei voi havaita tällaisia altistuksia. Jos Bluetooth-jäljityksellä ei voida havaita merkittävää osaa tartuntaketjuista, yksilön perusoikeuksien rajoittaminen ei ole perusteltua.

GPS-perusteisella altistuksella voitaisiin tietenkin jäljittää myös tällaisia tartuntaketjuja. GPS-jäljitys tuottaa kuitenkin Bluetooth-jäljitystä sensitiivisempää henkilötietoa. On myös oletettavaa, että GPS-jäljitys tuottaisi myös Bluetooth-jäljitystä enemmän perusteettomia tartuntaepäilyjä erityisesti sisätiloissa, joissa GPS-paikannus on epätarkkaa.

Jos tartuntatautilääkärit käyttävät sovellustietoa karanteenimääräysten perusteena, yksilöiden yhdenvertaisuus voi niin ikään vaarantua. Perusoikeuksien rajoitukset kohdistuvat yksilöihin epätasavertaisesti. Yhdenvertaisuusnäkökohdan merkitys voi olla vähäinen, jos yksilöt voivat valita, käyttävätkö sovellusta vai eivät. Jos sovellus sen sijaan "pakkoasennettaisiin” puhelimiin, joihin se voidaan asentaa, tilanne olisi toinen. Jos sovelluksen keräämää tietoa käytettäisiin tällöin pakkotoimenpiteiden kohdistamiseen, yksilöiden yhdenvertaisuus vaarantuisi tavalla, joka ei todennäköisesti ole hyväksyttävä.

Kokoavasti voidaan todeta, että sovelluksen tehokkuus epidemian hallinnassa on keskeinen tekijä, kun arvioidaan perusoikeusrajoitusten hyväksyttävyyttä. Jotta yksilö voitaisiin määrätä karanteeniin ja siten rajoittaa hänen perusoikeuksiaan, tartuntaepäilyn on oltava jo olemassa olevan lain mukaan perusteltu. Jos sovellus tuottaa suuren määrän perusteettomia tartuntaepäilyjä, näin ei näyttäisi olevan. Jotta yksityisyysperusoikeuden rajoitukset eli se, että viranomaiset saavat tietoa yksilöiden kontakteista, olisivat hyväksyttäviä, rajoitustoimenpiteiden on oltava tehokkaita epidemian hallinnasta ja siten tuotettava merkittävää terveyshyötyä.

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

ei

Avoimet huomiot koskien kysymystä 2

Perusoikeusrajoitusten ohella myös tietosuojakysymykset nousevat esille. Yleisen tietosuoja-asetuksen näkökulmasta ongelmat eivät ole sinällään ole erityisen polttavia. Euroopan tietosuojaneuvoston antama ohjeistus sovelluksista toteaa sovelluksien sinänsä olevan sallittuja tietosuojan näkökulmasta, mikäli yleisistä tietosuojaperiaatteista pidetään huolta. Yleinen tietosuoja-asetus antaa lisäksi jäsenvaltioille asetuksen 6 artiklan 1 pykälän e) ja 9 artiklan 2 pykälän g) kohdissa laajan harkintamarginaalin säätää henkilötietojen käsittelystä yleisen edun toteuttamiseksi. Sovelluksen nykyinen kuvaus ei anna erityistä aihetta epäillä, etteivätkö sovellusta suunniteltaisi myös Suomessa siten, että tietosuoja-asetuksen vaatimukset teknisesti täyttyvät. Muutoinkin luonnoksessa kuvailtu malli puuttuu oikeuksiin osin vähemmän kuin Ranskassa vastikään omaksuttu sovellus, jonka Ranskan tietosuojaviranomainen katsoi lähtökohtaisesti lailliseksi.

On kuitenkin syytä huomata, että tietosuoja-asetus rakentuu ns. datan minimoisen periaatteen varaan. Tietoa on kerättävä mahdollisimman vähän. Vaikka periaate ei käsityksemme mukaan estä nyt kaavaillun sovelluksen käyttöönottoa, sille tulisi kuitenkin antaa merkitystä, kun valitaan minkälainen perusarkkitehtuuri olisi valittava. Teholtaan samanarvoisista vaihtoehdoista pitäisi valita se, jossa tietoa kertyy mahdollisimman vähän.

Tästä syystä olisi tärkeää harkita, onko nyt kaavailtu ratkaisu optimaalinen ja perustella. miksi esimerkiksi DP-3T-hankkeessa hahmoteltu kontaktinjäljitysratkaisu ei ole riittävän tehokas ja miksi ja miten nyt hahmoteltu keskitetty ratkaisu on sitä tehokkaampi.

On myös huomattava, että tietosuojaviranomaiset useissa muissa unionivaltioissa ovat päätyneet tukemaan täysin hajautettua ratkaisua, joka parhaiten toteuttaa tietosuoja-asetuksen vaatimukset tietojen minimisoinnista. Esimerkiksi Saksassa hylättiin kansallisesti kehitetty PEPP-PT-protokolla ja päädyttiin tukemaan hajautettua DP-3T-protokollaa. Myös Isossa-Britanniassa NHSX:n kehittämää sovellusta on viime päivinä kritisoitu voimakkaasti valitusta keskitetystä ratkaisusta. Samoin olisi tarpeen selventää täsmällisemmin, mitä tarkoitetaan eurooppalaisella tietojenvaihdolla ja yhteensopivuudella.

Toiseksi on tärkeää huomata, että suostumuksella voi olla vain rajoitettua merkitystä tietojenkäsittelyn perusteena. Lausuntomateriaaleissa korostetaan kuitenkin usein sitä, että tietojen kerääminen ja siirtäminen perustuu suostumukselle. Samalla huomautetaan, että tietojenkäsittelyn perusteesta on kuitenkin säädettävä lailla, koska yksilö ei voi yksilö-viranomainen -asetelmassa antaa aidon vapaaehtoista suostumustaan asetelman epätasapainoisuuden vuoksi. Kaksi seikkaa on syytä huomata. Ajatellaan tapausta, jossa sovelluksessa terveysviranomaisille luovutetaan tiedot käyttäjien kontakteista ja tunnistetiedot ovat henkilötietoja. Lausuntomateriaaleissa todetaan, että käyttäjä antaa suostumuksensa siirtoon. Nyt on syytä huomata, että kontaktitiedot ovat kahden yksilön henkilötietoja: käyttäjän ja kunkin kontaktin. Kun käyttäjä antaa suostumuksen, hän antaa suostumuksen toisen yksilön henkilötietojen siirtämiseen. Kontaktilta tätä suostumusta ei voida tässä saada. Se voidaan tietenkin konstruoida taustalle. Kun kontakti on ottanut sovelluksen käyttöön, hän on antanut suostumuksensa siihen, että häntä koskeva henkilötieto voidaan luovuttaa viranomaiselle. Jos henkilö on kuitenkin tällä välin tullut toisiin aatoksiin ja peruuttanut suostumuksensa, siirretään henkilötietoa vastoin kontaktin tahtoa.

3. Onko muistiossa tunnistetut lainsäädäntömuutokset riittävät?

kyllä

Avoimet huomiot koskien kysymystä 3

-

4. Mahdolliset yksilöidyt säädösmuutosehdotukset

-

5. Mitä hyötyjä arvioitte sovelluksella olevan ja mille tahoille?

-

6. Millaisia riskejä valmisteluun tai sovelluksen käyttöön voi kohdistua?

-

7. Muut huomiot muistiosta ja liitteestä. Voit esittää myös näkemyksiä jäljitysprosessissa tarvittavaan tiedonhallinnan ja tietojärjestelmien kehitykseen.

-

Viljanen Mika
Turun yliopisto - Suomen akatemian rahoittamat AALAW (315007) - ja ETAIROS (327357) -projektit