Kaikkien eduskuntapuolueiden tietopolitiikan toimijoiden yhteistyöryhmä

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?

kyllä pääosin

Avoimet huomiot koskien kysymystä 1

Tietopolitiikan yhteistyöryhmän näkemys on, että jäljityssovellus kannattaa ottaa nopeasti käyttöön. Olemme julkaisseet digitaalisten kontaktiketjujen eettisistä ja perusoikeudellisista kysymyksistä non-paperin 3.4.2020. Tarkoituksenmukaisuuden arviointi on keskeinen seikka arvioitaessa sovelluksen oikeudellista perustaa. Nähdäksemme käsillä olevassa kriisitilanteessa toiminnan nopeus vaikuttaa merkittävästi toimien hyödyllisyyteen, eikä kattavaa ennakkokokemusta digitaalisen kontaktiketjujen jäljityksen tarkoituksenmukaisuudesta ole saatavilla. Kattavan ennakkoarvioinnin sijaan joudutaan nojaamaan toiminnan aikaiseen arviointiin. Olennaista on etukäteen kuvata toiminnan päämäärät ja oletetut vaikutukset, joiden toteutumista ja siten myös suhteellisuusperiaatteen toteutumista voidaan arvioida toiminnan aikana.

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

ei kantaa

Avoimet huomiot koskien kysymystä 2

Esityksessä ilmenee epäselvyyttä hajautetun ja keskitetyn mallin suhteen. Esimerkiksi kappaleessa 3 Tavoitetilan kuvaus todetaan, että “mobiiliratkaisu perustuu henkilöiden vapaaehtoisesti käyttöön ottamaan sovellukseen, joka tallentaa vahvasti salatut kontaktitiedot hajautetusti käyttäjien mobiililaitteisiin. Jäljityssovellus ei tallenna tunnisteellista henkilötietoa, vaan yksilöllisiä pseudonymisoituja tunnisteita, jolloin yksittäiset, lähikontaktissa olleet henkilöt eivät ole tunnistettavissa”. Tämä ei ole hajautetun mallin mukainen kuvaus, sillä sovelluksen ei tulisi ladata kontaktitietoja suoraan, vaan ns. kättelytietoja. Kontaktitiedot hajautetussa järjestelmässä muodostuvat myöhemmin, kun tartunnan saanut on ladannut kättelytietonsa keskitettyyn

tietokantaan. Myös sivulla 5 todetaan, että toimitetaan "tallentuneet kontaktitiedot taustajärjestelmälle", joka viittaa mallin mukailevan keskitettyä järjestelmää. Olennaista tässä olisi toimitta kohtaamisavaimet taustajärjestelmälle, ei kontaktitietoja sinänsä.

Hajautetussa mallissa on olennaista seuraavat kaksi asiaa:

1: uniikit tunnisteet (token) pysyvät sovelluksen sisällä (käyttäjän matkapuhelin) ellei käyttäjä erikseen anna lupaa niiden lataamiseen. Käytännössä vain tartunnan saaneet lataavat uniikit tunnisteet (token) itse keskitettyyn tietokantaan saatuaan terveydenhuollon ammattihenkilöltä tarvittavan koodin.

2: Käyttäjäjien yhdistäminen (tartuttaja ja mahdollinen tartunnan saanut) tapahtuu mahdollisesti tartunnan saaneen sovelluksessa, ei taustajärjestelmässä. Taustajärjestelmään ei tallenneta virukselle altistuneiden kättelytietoja, vaan ainoastaan tartunnan saaneiden.

Esityksen kohdassa 3.1 Jäljityssovelluksen toiminnalliset periaatteet on yhdeksi periaatteeksi kirjattu, että jäljityssovelluksen käyttö ja sillä kerätty tieto on yhteentoimivaa kansallinen ja kansainvälinen tiedonvaihto huomioiden. Kuten ylempänä todettiin, esityksen prosessi mukailee keskitettyä jäljityssovelluksen mallia, joka tekee yhteentoimivuudesta muiden maiden järjestelmien kannalta haastavan jatkossa. Esimerkiksi tarpeellinen matkustaminen Viroon voi vaikeutua, elleivät Viron ja Suomen jäljityssovellukset pysty keskustelustelemaan keskenään tietoturvallisesti.

Google ja Apple ovat ilmoittaneet tuovansa käyttöjärjestelmätasolle toteutettuna tiukkojen yksityisyysvaatimusten mukaisen hajautetun ratkaisun altistumisilmoitusten tekemiseen. Eri maiden kontaktijäljityssovellukset voivat tukeutua tähän käyttöjärjestelmätason ratkaisuun. Applen puhelimissa ainoastaan tätä Applen ja Googlen yhteistä teknologiaa hyödyntävät sovellukset toimivat myös niin sanotusti tausta-ajossa, eli silloinkin, kun kyseinen sovellus ei ole päällimmäisenä aktiivisessa käytössä.

Keskitettyä mallia aiemmin ajanut Saksalaislähtöinen PEPP-PT konsortio purkaantui ja myös Saksa päätti hiljattain toteuttaa oman sovelluksensa hajautetun mallin mukaisesti.

Euroopan komission suositukset eivät poissulje keskitettyä mallia, mutta puoltavat hajautettua mallia, koska se on linjassa datan minimoinnin tietosuojaperiaatteen kanssa.

3. Onko muistiossa tunnistetut lainsäädäntömuutokset riittävät?

ei pääosin

Avoimet huomiot koskien kysymystä 3

Tietopolitiikan yhteistyöryhmän näkemys on, että paljon vähäisemmät lainsäädäntömuutokset ovat mahdollisia, mikäli sovellus toteutetaan hajautetusti, siten että taustajärjestelmään ei tallenneta altistuneiden uniikkeja tunnisteita, vaan ainoastaan infektoituneiden tunnisteet, kuten yllä esitimme. Toisin sanoen hajautettu malli vaatii vähäisempiä muutoksia, mikä voi nopeuttaa sen käyttöönottoa.

4. Mahdolliset yksilöidyt säädösmuutosehdotukset

-

5. Mitä hyötyjä arvioitte sovelluksella olevan ja mille tahoille?

Tietopolitiikan yhteistyöryhmä uskoo, että hyvin toteutettuna sovelluksesta on hyötyä liikkumisrajoitusten nopeammassa ja hallitussa purkamisessa, mikä on kaikkien tahojen edun mukaisesta.

6. Millaisia riskejä valmisteluun tai sovelluksen käyttöön voi kohdistua?

Avoimen vuoropuhelun puute: Liian suljettu valmistelu on riski sovellukseen kohdistuvan luottamuksen ja julkisen mielipiteen kannalta. Tarvitaan vahvaa keskinäistä luottamusta. Kansalaisten ja kansalaisjärjestöjen on pystyttävä varmistamaan, että luottamuksellisten tietojen suoja pitää myös jatkossa. Viranomaisten on luotettava, että yrityksillä on kyky varmistaa tietoturva ja käyttäjän yksityisyys, joita auditoidaan säännöllisesti. Yritysten on luotettava viranomaisten linjausten pitävyyteen. Kokonaisuutta edesauttaa se, että sovelluksesta ja sen taustajärjestelmästä kerrotaan avoimesti. Julkishallinnon on ehdottomasti avattava ja tiedotettava sovelluksen kehityksestä merkittävästi tähän mennessä tapahtunutta avoimemmin.

Sovelluksen viivästyminen: Järjestelmäintegraatioita esimerkiksi Kelan ylläpitämiin taustajärjestelmiin ja pysyviä lainsäädäntömuutoksia esimerkiksi tartuntatautilakiin tulisi mahdollisuuksien mukaan välttää, jotta väliaikaiseksi tarkoitettu sovellus saadaan otettua käyttöön mahdollisimman ketterästi. Julkisuudessa olleet tiedot projektin huomattavista kustannuksista ja niiden jakautumisesta eri toimijoille kiinnittävät huomiomme siihen, onko tämän kokoluokan projektia mahdollista tehdä sen vaatimassa kiireellisessä aikataulussa. Kriisitilanteen aikana tulee välttää pysyviä muutoksia lainsäädäntöön. Tarvittaessa voidaan säätää datan käsittelyn mahdollistava määräaikainen erityislaki. Kiire ja paineenalainen tilanne tekevät riittävän harkinnan vaikeaksi, mitä pysyvä lainsäädäntö edellyttäisi.

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

Mitä tarkoitetaan hajautetulla mallilla (komission suositus ja Googlen/ Applen tukema)

Täysin hajautettu järjestelmä, missä ei olisi lainkaan keskitettyä taustajärjestelmää ei ole realistinen sovelluksella tavoiteltujen hyötyjen kannalta. Käytännössä tarvitaan joka tapauksessa jokin viranomaisten ylläpitämä taustajärjestelmä, mihin pseudonymisoituja testattujen covid19-positiivisten päätelaitteden käyttämiä kättelyavaimia kerätään.

Olennainen kysymys on, että onko viranomaisilla teknisesti mahdollisuus taustajärjestelmään kerättyjen tietojen pohjalta myös tunnistaa altistuneet ja ottaa heihin yhteyttä (keskitetty/tunnistettu) vai toteutetaanko järjestelmä niin päin, että käyttäjien päätelaitteet tarkistavat säännöllisesti tietokannasta, ovat sovelluksesta altistumisviestin saaneet ottavat yhteyttä terveydenhuoltoon (hajautettu/anonyymi).

Tietopolitiikan yhteistyöryhmä kannattaa jälkimmäistä ratkaisua, koska se on:

A: Parempi yksityisyydensuojan kannalta

B: Kevyempi lainsäädännön muutostarpeiden osalta

C: Euroopan komission suositusten mukainen

D: Googlen ja Applen tukema käyttöjärjestelmien tasolta

E: Uskomme, että hyvällä suunnittelulla lähes kaikki altistumisviestin saaneista ovat yhteydessä terveydenhuoltoon, jolloin sen hyödyllisyys on yhtä hyvä, kuin toisessa mallissa.

Hajautetussa/anonyymissa mallissa sovelluksen hyöty viranomaisten näkökulmasta riippuu siitä miten yhteydenotto käytännössä tapahtuu. Siitä ei ole mitään hyötyä, jos jokainen altistunut ihminen itse hakeutuu terveydenhuollon piiriin. Tämä kuormittaa terveydenhuollon ammattihenkilöitä, ja vaatii paljon kansalaisilta omaa aktiviisuutta sekä tiedonhankintaa.

Yhteydenotto tulisi tehdään niin, että altistumistiedon saaneelta henkilöltä kysytään sovelluksessa, haluaako hän olla yhteydessä terveydenhuoltoon. Mikäli vastaus on kyllä, hän klikkaa sovelluksesta helposti hyväksynnän. Tämä aktivoisi taustajärjestelmässä kyseisen altistuneen niin, että viranomaiset saavat tiedon henkilöllisyydestä, ja voivat olla yhteydessä häneen ennen kaikkea automatisoiduin viestein, mutta tarvittaessa myös henkilökohtaisesti.

On myös mahdollista, että käyttäjä antaa sovellukselle ennakoivasti luvan olla automaattisesti yhteydessä terveydenhuoltoon, kun sovellus on saanut altistumisesta tiedon. Tämä niin sanottu hybridimalli on perusteiltaan hajautettu/yksityinen, mutta toiminnalisuudeltaan vastaa terveydenhuollon ammattihenkilöiden näkökulmasta keskitetty/tunnistettu -tyyppiä.

Kuvattuna prosessiksi on hajautettu/yksityinen tiivistetysti seuraavanlainen:

Käyttäjä A lataa sovelluksen ja antaa luvan kerätä kättelytietoa.

Käyttäjä A sairastuu, uniikit tunnisteet (token) ladataan tietokantaan.

Käyttäjä B lataa tietokannasta sairastuneiden uniikit tunnisteet (token) ja vertaa niitä oman sovelluksensa kättelytietoihin.

Käyttäjä B:n sovelluksessa paljastuu, että hän on altistunut ja sovellus antaa käyttäjälle altistumisviestin

Käyttäjä B reagoi altistumisviestiin. Käyttäjä B:n tietoja ei missään vaiheessa eikä missään muodossa päädy tietokantaan, ellei häntä lopulta todeta sairastuneeksi.

Hybridimalli edellyttää lisäksi seuraavaa:

Käyttäjä B:n asentaessa sovellusta hän hyväksyy oletusarvona, että altistuttuaan hänen tiedot ladataan automaattisesti viranomaisille, jotta he voivat ottaa yhteyttä. Valinnan on oltava vapaaehtoinen. Mikäli tämä valinta on tehty sovelluksen sisällä, korvaa tämä kohdan 5.

Harju Juhana
Kaikkien eduskuntapuolueiden tietopolitiikan toimijoiden yhteistyöryhmä