Liikenne- ja viestintävaliokunta
Eduskunta

Lausunto
4.5.2020

Viite: Lausunto; E 44/2020 vp Valtioneuvoston selvitys; Komission suositus unionin yhteisestä työkalupakista liittyen mobiilisovellusten ja anonymisoidun liikkuvuusdatan käyttöön covid-19-kriisin torjumiseksi ja siitä ulospääsemiseksi

F-Secure kiittää mahdollisuudesta lausua valtioneuvoston selvityksestä koskien komission suositusta unionin yhteisestä työkalupakista liittyen mobiilisovellusten ja anonymisoidun liikkuvuusdatan käyttöön covid-19-kriisin torjumiseksi ja siitä ulospääsemiseksi.

F-Secure pitää hyvänä, että Euroopan unionin tasolla on lähdetty liikkeelle yksityisyyttä ja tietosuojaa korostavista lähtökohdista. Tämä on erityisen tärkeää, sillä nyt valitut toimintatavat tulevat määrittämään toimintaa myös tulevissa kriisitilanteissa. Yksityisyyden suojaa rajaavista toimista saatujen hyötyjen tulee olla tarkkaan perustellut ja aiheutettua haittaa suuremmat.

Yksityisyyden ja tietosuojan näkökulmasta pidämme tärkeänä sitä, että jäljityssovellukset ja niiden keräämät tiedot rajataan vain yhteen selkeästi määriteltyyn ja ajallisesti rajattuun käyttötarkoitukseen, kuten Suomessa on kaavailtu. Vaikka lisäominaisuudet voisivat olla terveysviranomaisten kannalta hyödyllisiä ja kannustaa sovelluksen käyttöönottoon, voivat ne myös hämärtää sovelluksen käyttötarkoitusta ja käyttöä kansalaisten mielissä ja laajentaa väärinkäytösten mahdollisuutta. Vaarana voi myös olla, että jäljitettävyysominaisuutta käytettäisiin jatkossa myös muissa yksityisyyden suojaa rajaavissa tilanteissa. Tästä näkökulmasta, houkutuksia kerätä ylimääräistä, sinänsä varmasti hyödyllistä massadataa, tulee välttää.

Euroopan unionin tasolla on hyvä hakea ratkaisuja, joissa jäljitettävyys toimii myös rajat ylittävissä kohtaamisissa. Näin ollen tulisi välttää ratkaisuja, jotka ovat puhtaasti kansallisia ja keskenään teknisesti yhteensopimattomia. Käytännössä tämä tarkoittaa, että esimerkiksi käytettäessä Applen ja Googlen 'Exposure Notification' rajapintaa, tunnisteiden jakaminen kansallisten terveysviranomaisten välillä tulisi miettiä ja mahdollistaa.

Euroopan unionin tietosuojaneuvosto on ansiokkaasti selkeyttänyt sitä, mitä yksityisyyttä ja tietosuojaa koskevat periaatteet voivat tarkoittaa jäljityssovelluksia kehitettäessä. Tärkeänä lähtökohta on yksilölähtöisyys (vastakohtana valtiolliselle valvonnalle). Kansallisen sovelluksen tulisi perustua avoimeen lähdekoodiin, mikä lisää sovelluksen läpinäkyvyyttä ja helpottaa mahdollisuuksia arvioida sen ominaisuuksia. Positiivisten testitulosten määrittäminen ja sitä kautta jäljitystoiminnon aktivointikoodin antaminen tulee jättää terveysviranomaisten tehtäväksi, mikä rajaa väärinkäytöksiä ja väärien viestien levittämistä.

F-Secure

Liikenne- ja viestintävaliokunta
Eduskunta

Lausunto
4.5.2020

Yksityisyyden näkökulmasta on kannatettavaa, että jäljitettävyys perustuu nimenomaan mobiililaitteiden läheisyyteen perustuvaan teknologiaan (Bluetooth) eikä vaikka teleoperaattoreiden keräämiin yleisiin paikkatietoihin. Tartuntatietojen käsittelyn anonymisointi on ensiarvoisen tärkeää epäsuotuisien vaikutusten välttämiseksi. Kerättävän tiedon ja sen säilyttämisen osalta tulee huolehtia siitä, että sovelluksen keräämät tunnistetiedot rajataan vain kontaktien jäljityksen kannalta välttämättömiin tietoihin. Esimerkiksi maantieteellistä paikkatietoa, nimiä, puhelinnumeroita tai muuttumattomia laitetunnisteita (kuten IMEI-tunniste) ei tulisi kerätä. Tietojen säilyttämisaika tulee olla ennalta määritelty ja automatisoitu sovelluksessa. Lisäksi sovellus ja sen toimintakyky tulisi viranomaisten toimesta kytkeä pois päältä, kun epidemia on ohi.

On tärkeää pohtia sitä, miten jäljitettävyyssovelluksen käyttöönottoa voidaan tehostaa, jotta siitä saadaan tavoiteltu hyöty. Kansalaisia tulee kannustaa ja rohkaista ottamaan käyttöön sovellus. Luotettavuutta lisää, jos sovellus perustuu eurooppalaisiin ja kansallisiin ratkaisuihin. Sovelluksen käyttötarkoitus tulee rajata nyt käsillä olevaan epidemiaan. Eri terveydenhuollon toimijoiden yhtenäinen, kaikille saatavissa oleva kyvykkyys antaa jäljitystoiminnon aktivointikoodi on haaste, joka on ratkaistavissa. Tämän aktivointikoodin tulee olla satunnainen ja kertakäyttöinen väärinkäytösten estämiseksi. Henkilökohtainen aktivointikoodi olisi jaettavissa esimerkiksi Omakannan kautta QR-koodina tai terveydenhuollon henkilöstön toimesta puhelimitse. Ko. koodeilla tulisi olla rajattu voimassaoloaika.

On ensiarvoisen tärkeää, että jäljityssovellusten tietoturvasta huolehditaan parhaalla mahdollisella tavalla ja että tietoturvatestauksen asiantuntijat voivat testata sovelluksen ja siihen mahdollisesti tehtävät päivitykset. Jäljityssovelluksen suunnittelussa ja käyttöönotossa tulisi tarkastella laajemmin sovelluksen lisäksi kehitys- ja jäljitysprosessia ja tietoturva-arkkitehtuuria kokonaisuutena. Tällöin esimerkiksi sovellusta ja sen käyttämiä taustajärjestelmiä ja käyttötapauksia arvioitaisiin yhdessä ja samanaikaisesti, ei erillisinä osina.

F-Secure on mielellään käytettävissä ja tuomassa tietoturva-asiantuntemustamme kotimaisten ja eurooppalaisten ratkaisujen suunnitteluun ja käyttöönottoon.



Samu Konttinen
toimitusjohtaja
F-Secure Oyj