LAUSUNTO

Eduskunnan liikenne- ja viestintävaliokunnalle
Asia: E 44/2020 vp Valtioneuvoston selvitys: Komission suositus unionin yhteisestä työkalupakista liittyen mobiilisovellusten ja anonymisoidun liikkuvuusdatan käyttöön covid-19-kriisin torjumiseksi ja siitä ulospääsemiseksi

Teknologia-avusteisen kontaktijäljityksen käytöstä COVID-19 -pandemian taltuttamisessa

Electronic Frontier Finland – Effi ry kiittää mahdollisuudesta tulla kuulluksi asiassa.

Effi on vuonna 2001 perustettu kansalais- ja asiantuntijajärjestö, joka puolustaa perus- ja ihmisoikeuksia digitaalisessa toimintaympäristössä. Näkökulmamme on erityisesti sähköisiä palveluja käyttävän kansalaisen tietosuojaa ja perusoikeuksia painottava.

Effi pitää matkapuhelinsovelluksella ja siihen liitetyllä taustajärjestelmällä toteutettavaa teknistä kontaktijäljitystä (engl. Contact Tracing) mahdollisesti hyvinkin toimivana lisätyökaluna manuaalisesti tehtävän perinteisen tartuntaketjujen jäljittämisen aputyökaluna. Huonosti toteutettuna tällainen teknologia johtaa kuitenkin massavalvontaan, rikkoo oikeutta yksityisyyteen ja kerätty data on tietoturvariski.

Effin näkökulmasta on tärkeää on ymmärtää mistä teknologia-avusteisessa kontaktijäljityksessä on kyse. Kyse ei ole ihmisyksilöiden jäljittämisestä vaan kontaktien jäljittämisestä. Kun kahden ihmisen välillä tapahtuu kontakti, jossa virus voi tarttua, tartunnan toteamiseen saakka on epäolennaista keitä nämä ihmiset ovat. Tartunta todennetaan terveydenhuollon ammattihenkilön toimesta ja tässä prosessissa tulee ilmi testatun ja tartunnan saaneen henkilön henkilöllisyys. Tämän jälkeen henkilölle annettava neuvonta ja häneen kohdistettavat hoito- ja karanteenitoimenpiteet tapahtuvat voimassa olevan tartuntatautien torjuntaa koskevan lainsäädännön mukaisesti. Jos henkilö on käyttänyt kontaktijäljityssovellusta, mahdollisesti tartunnan saaneille voidaan lähettää sovelluksen kautta varoitus mahdollisesta tartunnasta. On tärkeää huomata että tämä voidaan tehdä ja se tulee tehdä anonyymisti.

Effi pitää tärkeänä että teknologia-avusteisen kontaktijäljityksen mahdollisia hyötyjä arvioidaan ja seurataan tehtyjen kokeilujen perusteella ja että

päätökset käyttöönotosta perustuvat näihin kokemuksiin. Euroopan laajuisen yhteentoimivuuden kannalta on valitettavaa että toteutustapoja on monia erilaisia ja osassa, kuten Norjan ja Iso-Britannian tietoturvasta ja tietosuojasta on tingitty kestämättömällä tavalla kajoten näin kansalaisten perusoikeuksiin. Tällainen kehitys tulisi pyrkiä pysäyttämään mahdollisimman pian.

Toisaalta esimerkiksi Itävalta ja Saksa, jotka lähtivät alkuun liikkeelle mallilla, jossa oli keskitetty taustajärjestelmä, johon kännykkäsovelluksen lähettämiä tietoja lähetettiin jatkuvasti, ovat joutuneet muuttamaan toimintatapaansa runsaan ja perustellun julkisen kriitikin takia. Olennaisinta asiassa on se, että näissäkin maissa on muutoksen jälkeen huomattu että yksityisyyden, tietosuojan ja tietoturvan kannalta huomattavasti parempi hajautettu malli ajaa tehtävänsä kontaktien jäljittämisessä aivan yhtä hyvin.

Jotta teknologia-avusteisesta kontaktijäljityksestä olisi merkittävää hyötyä, sen tulee täyttää kaksi vaatimusta:

1. Järjestelmän on toimittava saumattomasti maarajojen yli liikuttaessa. Keski-Euroopassa on monin paikoin sama tilanne kuin Suomen ja Ruotsin rajalla: Ruotsin puolella Länsi-Pohjan alueella olevat sairaalat eivät toimisi ilman Suomen puolella asuvaa työvoimaa. Viron ja Ruotsin rajat ylittävä henkilö- ja rahtiliikenne on merkittävä riskitekijä koronaviruksen kurissa pitämisen näkökulmasta. Suomen kannalta olisi erinomaista jos Ruotsi Viron tavoin[1] ottaisi käyttöön saman, teknisesti yksityisyysominaisuuksiltaan parhaan teknologian, DP-3T:n[2]
2. Kun on selvää, että länsimaisessa oikeusvaltiossa kontaktijäljityssovelluksen käyttämisen tulee olla vapaaehtoista, sovelluksen käytön yleistymisen edellytyksenä on läpinäkyvyys, väliaikaisuus ja sitä kautta lainsäädännöllinen sidos tartuntatautilainsäädäntöön sekä mahdollisimman vähäinen yksityisyyden rikkominen. Kansalaisten luottamusta ei voi saavuttaa jos näistä periaatteista tingitään. Näistä periaatteista kiinni pitäminen edistää myös edellisen kohdan tavoitetta.

Tarkemmin eriteltynä kännykkäsovelluksen ja sen taustajärjestelmän muodostamalle kokonaisuudelle sekä niiden käytölle tulee esittää seuraavat vaatimukset:[3]

1. Sovelluksia ja dataa käytetään vain ja ainoastaan SARS-CoV-2 -tartuntaketjujen jäljittämiseen. Muu käyttö on kielletty.
2. Sovelluksen käytön on oltava vapaaehtoista ja kieltäytymisestä ei saa seurata sanktioita.
3. Yksityisyydestä ei tingitä.
4. Läpinäkyvyyden ja toiminnallisuuden verifioitavuuden vuoksi sovelluksen

1 https://e-estonia.com/trace-covid-19-while-respecting-privacy/
2 https://github.com/DP-3T
3 Listaus noudattaa erään Euroopan johtavan tietotekniikka-asiantuntijakerhon CCC:n tietosuojaryhmän suosituksia: https://www.ccc.de/en/updates/2020/contact-tracing-requirements Myös muut tietosuojasuuntautuneet kansalaisjärjestöt kautta Euroopan ovat joko ilmoittaneet kannattavansa näitä vaatimuksia tai julkaisseet hyvin samansuuntaisia kantoja.

ja taustaohjelmistojen on oltava vapaasti saatavilla joko avoimena lähdekoodina tai ainakin julkisesti luettavissa.
5. Ei keskusorganisaatiota, johon on pakko luottaa.
6. Dataa kerätään vain tarkoituksen kannalta välttämätön minimimäärä. Esimerkiksi käyttäjien IP-osoitteita ei tule kerätä.
7. Anonyymiys: käytetty teknologia ei saa mahdollistaa sitä käyttävien yksilöiden tunnistamista.
8. Järjestelmä ei saa mahdollistaa keskitettyä liikkumisen tai kontaktien tallennusta.
9. Linkittämättömyys: käyttäjän kontaktijäljityksessä käytettävää yksilöivää tunnistetta (ID) ei saa johtaa mistään muusta tiedosta tai linkittää sellaiseen, esimerkiksi käyttäjätileihin muissa palveluissa.
10. Tiedonsiirron salaaminen: sovelluksesta siirrettävästä tiedosta ei ulkopuolinen saa pystyä päättelemään mitään terveydentilasta tai muustakaan sovelluksen tallentamista tiedoista.

Effin mielestä nämä vaatimukset täyttävä kokonaisuus on hyväksyttävä väliaikaisena manuaalisen jäljityksen aputyökaluna taisteltaessa COVID-19 -epidemiaa vastaan.

Teknologiajätit Apple ja Google ovat hyvin pitkälle samoilla linjoilla yksityisyysvaatimusten suhteen. Suvereenin valtion ei tietenkään tarvitse ottaa huomioon yksittäisten liikeyritysten linjauksia. Tässä asiassa etu on kuitenkin yhteinen ja valtion etu on se, että edellä mainitut yritykset ylipäätään suostuvat ottamaan valtion jakeleman sovelluksen sovelluskauppaansa jakeluun. Lisäksi Applen tuotteiden kohdalla on käytännön tason ongelma: jotta Bluetooth Low Energy (BLE) -teknologiaan perustuva jäljityssovellus toimisi myös Applen laitteissa, sen tulee käyttää Applen ja Googlen tekemää teknologiaa jotta BLE-toiminto pysyy päällä tausta-ajossa. Tähän asiaan haetaan jo ratkaisua DP-3T -hankkeessa.

Arvioitaessa tarvittavia lainsäädäntömuutoksia Effi haluaa nostaa harkittavaksi sen, mitä tietoa teknisessä kontaktienjäljitysjärjestelmässä käsitellään. Jos pyritään edellä lueteltujen vaatimusten mukaiseen tilanteeseen ja vältetään kaikkien henkilötietojen käsittelyä, päästään lainsäädäntötyössä helpommalla. On syytä harkita, voitaisiinko koko tietojen käsittely perustaa sovellusta käyttävien suostumukseen. Tällä tavoin voitaisiin tarjota suostumuksen kautta halukkaille mahdollisuus luovuttaa kontaktitietojaan epidemologiseen tutkimukseenkin. Lainsäädäntöteitse moisen toteuttaminen on hidas ja kankea prosessi ja nyt nopeus on tärkeintä.

Jos järjestelmällä halutaan tehdä muuta kuin sen perustoiminnallisuus, kontaktien jäljittäminen, esimerkiksi kerätä tietoa epidemologiseen tai muuhun tieteelliseen tutkimukseen tietojen keruulle pitää asettaa tiukat vaatimukset. Tietoa ei tule kerätä käyttäjiltä ennen kuin tieteellinen tutkimussuunnitelma on valmis ja siihen liittyvä tieteellisen tutkimuksen informointiasiakirja on tehty. Tietoa ei tule missään tapauksessa kerätä avoimella mandaatilla vaan esitetyllä tavalla tarkkarajaisesti. Lisäksi tiedon tallentamisen ja käsittelyn tulee perustua suostumukseen ja sovelluksen käyttäjän on voitava valita erikseen osa-alueet, joihin suostuu ja joihin ei, siltä osin kuin eri käyttötarkoitukset voidaan erottaa

toisistaan. Esimerkiksi suostumuksen tietojen käsittelemiseksi notifikaation antamiseen tulee olla erillinen käyttäjätunnisteiden käyttöän muuhun analysointiin ja/tai pitempiaikaiseen tallennukseen pyydettävästä suostumuksesta. Lisäksi tietojen keruusta tulee tehdä EU:n yleisen tietosuoja-asetuksen mukainen vaikutustenarviointi kuten kontaktijäljitysjärjestelmästäkin.

Taustajärjestelmän teknisestä toteutuksesta toteamme että palvelinten on sijaittava Suomessa ja lisäksi sellaisen toimijan ylläpitämänä, jonka toiminta ei voi kompromettoitua toisen valtion lainsäädännön kautta, esimerkiksi Yhdysvaltain antiterrorismilakien kautta. Tämä koskee myös käytettävää teknologiaa.

Electronic Frontier Finland – Effi ry
Elias Aarnio
varapuheenjohtaja