3.4.2020 LOPULLINEN

Digitaalinen kontaktiketjujen jäljitys virusepidemian hallinnassa – eettisiä ja perusoikeudellisia lähtökohtia

---

Tämä on eduskuntapuolueiden tietopolitiikan toimijoiden yhteistyöryhmän jäsenten kiireellisesti kirjoittama “non-paper”, joka **ei edusta puolueiden kantaa**, sitä ei ole käsitelty minkään puolueen päätöselimissä. Kirjoittajien nimet löytyvät paperin lopusta.

Miksi tämä asia on tärkeä selvittää juuri nyt?

Vapaaehtoinen digitaalinen kontaktiketjujen jäljityssovellus voidaan nähdä lupaavimpana ja perusoikeuksien näkökulmasta vähiten yksityisyyteen puuttuvana ratkaisuna epidemian hallintaan. Mikäli tällainen sovellus halutaan sovittaa Suomen oloihin, tulisi se lanseerata ennen sulkutilojen purkamista (toukokuu 2020). Sovellus voisi auttaa sulkutilan hallitussa ja asteittaisessa purkamisessa.

Suomella tulee olla nyt ja jatkossa kansallinen kyky nopeaan reagointiin epidemioiden eri vaiheissa, jotta voimme tarvittaessa joustavasti lisätä tai vähentää rajoitustoimia. Kontaktiketjujen jäljityssovellusta hyödynnettäessä voivat valitut rajoitukset olla vähäisempiä haitoiltaan.

Koronavirusepidemian hallitsemisen näkökohtia

Koronavirusepidemian hallitsemisessa tavoitteena on vähentää kuolemia ja tartuntoja. Samalla laajojen toimenpiteiden, kuten sulkujen ja karanteenien, hinta on niin taloudellisesti, kuin yhteiskunnallisesti ja ihmisten perusoikeuksien kannalta korkea. Toiveena on, että teknologian avulla rajoitustoimia voitaisiin kohdentaa paremmin niin, että koronavirus pysyisi hallinnassa sulkutiloja purettaessa ja että purkamiseen päästäisiin mahdollisimman nopeasti. Tässä muistiossa on tarkasteltu:

1. Niin sanottua **“Singaporen mallia” eli mobiilisovelluksiin pohjautuvaa digitaalista kontaktiketjujen jäljitystä**, joka on noussut esille yhtenä lupaavana keinona virusepidemian hallintaan. [1] [2]

2. Digitaalisen kontaktiketjujen jäljitys **perusoikeuksien näkökulmasta** sekä **yleisiä oikeudellisia lähtökohtia yksityisyyden suojan kannalta**.

Muistiossa keskitytään nimenomaan kontaktiketjujen jäljitykseen. Myös muita henkilötietoihin pohjautuvia keinoja, kuten teletunnistetietojen hyödyntämistä karanteenivalvontaan,

[1] **Quantifying dynamics of SARS-CoV-2 transmission suggests that epidemic control and avoidance is feasible through instantaneous digital contact tracing**
https://github.com/BDI-pathogens/covid-19_instant_tracing/blob/master/Manuscript%20-%20Modelling%20instantaneous%20digital%20contact%20tracing.pdf

[2] **Data koronaa vastaan, mutta miten?** https://www.linkedin.com/pulse/data-koronaa-vastaan-mutta-miten-antti-jogi-poikola

immuniteettipasseja ja niin edelleen on ehdotettu maailmalla, mutta tässä niihin ei syvällisemmin paneuduta [3] (liite 1).

Kontaktiketjujen jäljittäminen on klassinen toimenpide epidemioiden hallinnassa. Siinä tartunnan saaneen liikkeet ja kontaktit muiden henkilöiden kanssa pyritään selvittämään ja altistuneita asetetaan karanteeniin. Manuaalisesti tehtynä kontaktiketjujen jäljittäminen on kuitenkin mahdollista vain rajatulle määrälle tapauksia ja nykyisessä tilanteessa se työllistää entuudestaan kuormitettua terveydenhuollon henkilöstöä. Näin ollen henkilötietoon ja erityisesti sijainti- ja oiretietojen keruuseen nojautuvia keinoja koronaepidemian hallitsemiseen kehitetään valtavallanopeudella. Tilannekuva näistä keinoista ja arviot niiden hyödyllisyydestä, toteuttamis kelpoisuudesta ja oikeudellisista edellytyksistä sekä vaikutuksista muuttuvat päivittäin. Tilanne on uusi kaikille ja tuoreen ja luotettavan tiedon saamisessa ei voi nojautua pelkästään virallisiin organisaatioihin. Nopeaa ja laadukasta päätöksentekoa varten tarvitaan useiden tahojen aktiivisuutta ja yhteistyötä.

Vapaaehtoinen digitaalinen kontaktiketjujen jäljityssovellus nähdään lupaavimpana ja perusoikeuksien näkökulmasta vähiten yksityisyyteen puuttuvana ratkaisuna epidemian hallintaan. Toimet sen käyttöönottoon Suomen oloissa tulisi aloittaa välittömästi, koska tarve on akuutti.

Toteutus vaatii selkeän omistajuuden sovellukselle ja sen taustaprosesseille, sekä mahdollisesti uutta lainsäädäntöä, joka mahdollistaa terveysviranomaisille kontaktiketjuja kuvaavan henkilötiedon käsittelyn. Kaikki edellä mainittu edellyttää huolellista valmistelua perusoikeuksien näkökulmasta. Yksityisyyden suojan varmistaminen on ennakkoedellytys myös sille, että sovellus otetaan hyväksyen vastaan kansalaisten keskuudessa ja se saavuttaa riittävän laajan käyttäjäjoukon. Nähdäksemme avoimella valmistelulla tämä kaikki on tehtävissä. On myös huomioitava se, että toteuttaminen tuo mukanaan riskejä, jotka vaativat teknologisen kehittämisen ohella eettistä tarkastelua.

1. Mobiilisovelluksiin pohjautuva digitaalinen kontaktiketjujen jäljitys

Mobiililaitteiden avulla kontaktien jäljittäminen ja altistuneiden varoittaminen voidaan pitkälti automatisoida. Digitaaliset kontaktiketjujen jäljitysjärjestelmät nojautuvat jäljityssovelluksiin, jotka keräävät tietoa siitä, minkä muiden mobiililaitteiden läheisyydessä jäljitystä tekevä puhelin on ollut. Yhdistelmä laajaa testausta, digitaalista kontaktiketjujen jäljitystä sekä altistuneiden ohjaamista kotikaranteeniin on tutkimusten valossa nähtävissä lupaavana keinoyhdistelmänä epidemian taltuttamiseen ja tilanteen ylläpitoon sitten, kun sulkutiloja puretaan.[4] [5]

Esimerkiksi Singaporen TraceTogether-sovellus[6] toimii niin, että kun kaksi sovelluksen käyttäjää ovat fyysisesti riittävän lähellä (noin 2 m) toisiaan, puhelimet vaihtavat bluetoothin välityksellä keskenään uniikit tunnisteet (token), jotka jäävät muistoksi kohtaamisesta.

---

[3] **Projects using personal data to combat SARS-CoV-2**
https://gdprhub.eu/index.php?title=Projects_using_personal_data_to_combat_SARS-CoV-2

[4] **Contact tracing and disease control** https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1691540/pdf/14728778.pdf.

[5] **Response to COVID-19 in Taiwan: Big Data Analytics** https://jamanetwork.com/journals/jama/fullarticle/2762689..

[6] https://bluetrace.io

Singaporen sovelluksen kehitys aloitettiin jo vuoden 2008 SARS-epidemian jälkeen. Singapore on luvannut avata sovelluksen lähdekoodin avoimeksi näillä näkymin 14.4.2020. Myös Euroopassa on Saksan johdolla oma hanke[7], jossa on toteutettu vastaava Bluetooth-pohjainen ratkaisu. Yhteistyössä on mukana useita Euroopan maita. Saksassa sovellus on jo testikäytössä kasarmeilla ja julkistus kansalaisille tapahtuu näillä näkymin 17.4.2020. Sekä Singaporen mallia että Eurooppalaista mallia ja lähdekoodia ollaan parhaillaan evaluoimassa myös Suomessa.

Operaattoreilta mahdollisesti saatava sijaintitieto tai GPS-paikannus pandemian torjunnassa eivät ole riittävän tarkkoja tietolähteitä määrittämään sellaisia kohtaamisia, joissa pisaratartuntana leviävä virustartunta olisi mahdollinen. Tämä johtuu siitä, että esimerkiksi GPS-sijainti voi olla sama henkilöillä, jotka ovat samassa rakennuksessa, mutta eri huoneissa tai eri kerroksissa. Pandemian torjunnassa paremmin toimivat kontaktiketjusovellukset nojautuvakin sijaintitiedon tai paikannuksen sijaan käyttäjien mobiililaitteiden fyysisen läheisyyden tunnistamiseen bluetoothin avulla.

Automaattinen kontaktien jäljitys ei missään oloissa ole aukotonta. Se on yksi keino muiden joukossa, joka tuottaa lisäarvoa, jos sovellusta käyttää merkittävä osa väestöstä.[8] Sovelluksen käytön laajuuden vaikutus sen tuottamaan hyötyyn tulee arvioida (mallintaa). Tämän pohjalta voidaan asettaa tavoitteet sille, kuinka suuri osa väestöstä tulisi saada sovelluksen käyttäjiksi. Tämä on myös vaikuttava seikka suhteellisuusperiaatteen toteutumisen arvioinnissa, mikäli sovelluksen käyttöönotto edellyttää uutta lainsäädäntöä.

2. Digitaalisen kontaktiketjujen jäljitys perusoikeuksien näkökulmasta

Kontaktiketjujen jäljityksen kehitys tulisi tehdä ihmiskeskeisesti, jolloin vahvistetaan ihmisten omaa kykyä ja mahdollisuuksia toimia.

Suurin yksittäinen perusoikeuksiin kohdistuva riski on siinä, että pakkokeinot avaavat tietä pakkokeinojen käyttöön myöhemminkin. Tällaisia näennäisesti legitiimejä intressejä kontakiketjujen jäljitykselle voi olla esim. rikostorjunnassa. On tärkeää täten korostaa sitä, että jäljitys on tehty mahdolliseksi vain pandemian mukanaan tuoman poikkeustilan takia, ei muihin tarkoituksiin. Tämän yhteydessä tunnistettavien pysyvien lainsäädäntömuutosten tarve kartoitetaan kriisitilanteen lauettua ja tarvittaessa käynnistetään tavanomainen lainsäädäntöprosessi.

Myös suorat riskit yksityisyyden vakaviinkin loukkauksiin ovat olemassa kun väestöä koskevien henkilötietojen poikkeuksellisen käsittelyn toimia tehdään kiireessä ja paineen alaisena. Tahattomien virheiden mahdollisuus kasvaa tällaisissa tilanteissa. Oikeudenmukaisuutta ja vahinkojen välttämistä tulee täten tavoitella sekä määritellä selkeästi vastuut. Yhteiskuntamme on rakennettu ajatukselle autonomisista yksilöistä, joten perusoikeuksien toteutuminen tulee ottaa huomioon koko sovelluksen suunnittelun ja käytön elinkaaren aikana niin hyvin kuin mahdollista. Sovelluksen kehityksessä on myös otettava huomioon yksilön mahdollisuus saada selville mihin omia tietoja on käytetty.

---

[7] **Pan-European Privacy-Preserving Proximity Tracing**-hanke https://www.pepp-pt.org

[8] **620,000 people installed TraceTogether in 3 days, S'pore's open source contact tracing app.** 11% Singaporen 5.6 miljoonasta asukasta otti sovelluksen siellä käyttöönsä ensimmäisen kolmen päivän aikana https://mothership.sg/2020/03/tracetogether-installed-open-source

Digitaalisten kontaktiketjujen jäljityksen on oltava teknisesti luotettavaa. Hyödynnettäessä henkilötietoja, on oltava erityisen huolellinen tietoturvasta, tiedostettava käsiteltävien tietojen arkaluonteisuus ja varmistettava yksityisyyden suoja niin hyvin kuin mahdollista. Tietosuojaan tulee myös kiinnittää erityistä huomiota.

Kansalaisilla on oltava luottamus siihen, että tiedetään miten ja millä periaatteilla sovellus toimii. Oikeudenmukaisuus rakentuu luottamukselle ja luottamuspääomassa korkealla olevan Suomen on pidettävä tästä kiinni myös poikkeuksellisissa oloissa. Automatisointi ei saa vähentää läpinäkyvyyttä.

3. Yleiset oikeudelliset lähtökohdat yksityisyyden suojan kannalta

Alla esitettyjen yleisten lähtökohtien pohjana on yksityisyyden suoja sekä henkilötietojen suoja siten, kun siitä on säädetty ja perustuslaissa, tietosuoja-asetuksessa sekä laissa sähköisen viestinnän palveluista (sähköisen viestinnän tunnistamistietojen osalta).

Kaikki tietosuojan heikennykset ovat perusoikeuksien heikennyksiä. Henkilötietojen suoja on yksityisyyden suojaa ja oikeus yksityisyyteen on perustuslain 10 § takaama perusoikeus. EU:n yleinen tietosuoja-asetus nojaa Euroopan ihmisoikeussopimukseen ja sen 8 artiklaan.

Koronaepidemia on poikkeustilanne, joka edellyttää poikkeuksellisia toimia. Lupaaviin henkilötietoja hyödyntäviin menetelmiin epidemian hallitsemiseksi tulee viipymättä tarttua. Tietosuoja ei ole este toiminnalle,[9] toimimatta jättäminen tietosuojaan vedoten voisi olla pitkässä juoksussa haitallisempaa tietosuojalle sen poliittisten seurausten myötä. Kerättävien henkilötietojen käsittelyn on tapahduttava EU:n tietosuoja-asetuksen puitteissa. Asetuksessa on huomioitu rajat ylittäviltä terveysuhkilta suojautuminen yhtenä käsittelyperusteena.[10] Tietojen kerääminen saattaa kuitenkin edellyttää, että tällaisesta toimivaltuudesta säädetään laissa.

Vaikeassakin tilanteessa on pidettävä kiinni yleisistä rajoitusperusteista henkilötietojen käytölle. Tietojen käytölle tulee olla **lakiperuste** (tarvittaessa väliaikaiseen lakiin perustuva) ja käytön tulee olla, **täsmällistä**, **tarkkarajaista** ja **hyväksyttävää**, sekä noudattaa **suhteellisuusperiaatetta**. Lisäksi on varmistettava perusoikeuden ydinalueen koskemattomuus, oikeusturvajärjestelyiden riittävyys ja ihmisoikeusvelvoitteiden noudattaminen. Valmiuslaki (1152/2011) ei sisällä säännöksiä, joilla yksityisyyden suojaan voidaan suoraan puuttua[11].

Kriisitilanteen aikana tulee välttää pysyviä muutoksia lainsäädäntöön. Tarvittaessa voidaan säätää datan käsittelyn mahdollistava määräaikainen erityislaki. Kiire ja paineenalainen tilanne eivät mahdollista riittävää harkintaa, mitä perusoikeuksiin kajoava pysyvä lainsäädäntö edellyttäisi. Historia on täynnä huonoja esimerkkejä poikkeustilanteiden aikana tehdyistä muutoksista, jotka ovat pysyvästi heikentäneet ihmisten perusoikeuksia. Nopeimmillaan erityislainsäädäntö on tehtävissä muutamassa päivässä, kuten on jo toimittu muun muassa ravintoloiden sulkemisen

[9] EDPS lausunto "data protection rules currently in force in Europe are flexible enough to allow for various measures taken in the fight against pandemics"

[10] Käsittelyperusteena saattaisi soveltua tietosuoja-asetuksen 6 artiklan 1 kohdan a, d, e tai f alakohta ja erityisten henkilötietoryhmien osalta 9 artiklan 2 kohdan a tai i alakohta.

[11] ValmL 62–63 §§ koskevat tietoturvaa, mutta täsmällisesti vain verkko-, tieto- ja viestintäjärjestelmien toimivuuden turvaamiseksi.

mahdollistamisessa. Lainsäädännön näkökulmasta anonymisointiin tai suostumukseen perustuvat ratkaisut ovat helpompia kuin esimerkiksi sovelluksen käyttöön liittyvät pakot ja velvoitteet.

Kerättävät tiedot ja käyttötarkoitukset tulee määritellä täsmällisesti ja niiden käsittelyn tulee olla ajallisesti, henkilöllisesti, maantieteellisesti ja tilanteeseen sitoen tarkkarajaista ja rajattu vain välttämättömään. Yleisluontoisia heikennyksiä henkilötietojen suojaan tai yksityisyyden suojaan ei tule hyväksyä, eivätkä ne luultavasti menisi läpi eduskunnan perustuslakivaliokunnassa. Datan kerääminen pelkästään louhittavaksi tai muutoin epämääräisten toiveiden perusteella ei ole mahdollista, koska keräämiselle ja käsittelylle täytyy olla tietosuoja-asetuksessa mainittu peruste. Käsittelyoikeus olisi laissa sidottava tämän epidemian torjumiseen, mutta siten että käsittelyn rajaus on voimassa tietyn ajan kerrallaan ja tietyllä maantieteellisellä rajauksella (ei voi olla ei-tarkkarajaisesti esimerkiksi “koronaviruspandemian ajan”).

Suhteellisuusperiaatteen mukaisesti valittujen keinojen tulee olla oikeassa suhteessa niillä tavoiteltuihin päämääriin nähden. Tämä edellyttää valittujen keinojen hyödyllisyyden ja käyttökelpoisuuden arvioimista. Käsillä olevassa kriisitilanteessa toiminnan nopeus vaikuttaa merkittävästi toimien hyödyllisyyteen, eikä ennakkokokemusta eri keinojen hyödyllisyydestä ole. 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.

Etukäteen on tehtävä suunnitelma tietojen keruun ja käsittelyn lopettamiseksi. Jotta yleisön luottamus säilytetään, on tehtävä selväksi että tietoja käytetään vain tartuntatautilain kuvaamiin tarkoituksiin ja tiedot hävitetään kun kyseinen lakiperuste on lakannut olemasta ja tietojen hävittämisestä informoidaan avoimesti. Myös mikäli toiminnan aikainen arvio ei osoita keinojen hyötyjä riittäviksi suhteessa suhteessa asetettuihin tavoitteisiin tulee tietojen käsittely ja keruu lopettaa.

Toteutuksessa tulee välttää luonnollisen henkilön tunnistamista ja pyrkiä mahdollisuuksien mukaan tekemään altistumisvaroitukset automaattisesti järjestelmän kautta ilman loppukäyttäjien tunnistamista. On tärkeämpää saada kansalaisten luottamus ja mahdollisimman suuri käyttäjämassa. Tällaisen järjestelmän kautta altistumisvaroituksen viranomaiselta saava kansalainen jatkaa lähes poikkeuksetta yhteydenpitoa terveydenhuoltoon ja hakeutuu hoidon piiriin.

Auditoitavuuden ja luotettavuuden takaamiseksi avoimen lähdekoodin sovellus on suositeltavin.

4. Suositukset

1. **Annetaan toimivaltaiselle viranomaiselle tehtäväksi tarkemman oikeudellisen arvion tekeminen digitaalisesta kontaktiketjujen jäljittämisestä.**

   Arvion pohjana voi hyödyntää Max Schremsin / NOYB paperia, joka käsittelee kontaktienjäljityssovelluksia tietosuoja-asetuksen näkökulmasta[12]. Kontaktiketjujen jäljittämisprosessi jakautuu ainakin kahteen vaiheeseen: (A) jatkuva kontaktien “tokenien” tallentaminen paikallisesti käyttäjän puhelimeen sovelluksen käytön aikana (“tallennusvaihe”) sekä (B) tallennetun tiedon välittäminen viranomaiselle ja käyttö

[12] **Max Schrems / NOYB Ad hoc Paper (V0.2) SARS-CoV-2 Tracking under GDPR**
https://noyb.eu/sites/default/files/2020-03/ad_hoc_paper_corona_tracking_v0.2_5.pdf

altistumisvaroitusten tekemiseen. Erilliset oikeudelliset analyysit ja eri käsittelyperusteet saattavat päteä eri vaiheissa.

Suomessa nähdäksemme suoraviivaisen ja samalla perusoikeuksia mahdollisimman vähän ja vain väliaikaisesti heikentävä lakiperusta saadaan oikeuttamalla tietojen kerääminen ja käsittely 1) suostumuksella ja 2) tartuntatautilailla.

Suostumus on todennäköisesti soveltuva käsittelyperuste otettaessa sovellusta käyttöön ja tallennusvaiheessa, kun viranomainen ei vielä osallistu tiedon käsittelyyn.

Tartuntatautilaki (1227/2016) antaa THL:lle mahdollisuuden epidemian uhatessa käyttää ja yhdistellä tietoja tietyistä kansallisista rekistereistä[13], mutta lakia saattaa olla tarpeen muuttaa, että voitaisiin käsitellä tietoja sairastuneen kohtaamisista muiden henkilöiden kanssa ja toteuttaa altistuneiden kontaktointi.

2. **Annetaan epidemiologiaa ja matemaattista mallinnusta osaavalle taholle tehtäväksi arvio kontaktiketjusovelluksen käyttöönoton laajuuden vaikutuksista sovelluksen hyötyihin epidemian hallinnassa.**

3. **Evaluoidaan Singaporen malli ja muut jo käytössä olevat kontaktiketjujen jäljityssovellukset (ks. GDPRhub) siitä näkökulmasta, että onko jossain saatavilla laadukasta ja käyttökelpoista avoimen lähdekoodin pohjaa.**

4. **Arvioidaan eri alueille suunniteltujen ja käytössä olevien ratkaisujen sovellettavuus Suomessa perus- ja ihmisoikeuksien sekä itsemääräämisoikeuden näkökulmasta.**

5. **Kootaan projektitiimi, jolla on kyvykkyydet ja resurssit sekä tekniseen toteutukseen, että palvelumuotoiluun ja ketterään projektijohtamiseen konseptin toteuttamiseksi.**

6. **Sovelluksen kehittäminen ja käyttöönotto tulee tehdä laajassa kansallisessa yhteistyössä, sillä nopeaa ja laadukasta päätöksentekoa varten tarvitaan useiden tahojen aktiivisuutta ja yhteistyötä.**

7. **Hankkeen julkistamisen viestintä laaditaan niin, että se kannustaa kansalaisia omaehtoiseen käyttöönottoon ja synnyttää luottamusta.**

8. **Suomi tekee tiivistä kansainvälistä yhteistyötä asiaan liittyvien tutkimuslaitosten, valtioiden ja yksityisten toimijoiden kanssa.**

[13] Tiedonsaantioikeudesta vakavan epidemian torjumiseksi säädetään tartuntatautilain 25 §:ssä.

Lisätietoja

Tämän dokumentin laatimiseen ovat osallistuneet kaikkien eduskuntapuolueiden tietopolitiikan toimijoiden yhteistyöryhmän jäsenet. Lisätietoja voi kysyä puolueiden yhteyshenkilöiltä.

Mikael Jungner (Liik)
Jonna Ijäs (PS)
Jouni Markkanen ja Miia Lindell (KOK)
Niko Eskelinen ja Juhana Harju (SDP), +358 44 010 1004, jyharju@gmail.com
Kristo Lehtonen (KESK)
Mikko Pöri (VAS)
Asmo Maanselkä (KD)
Atte Harjanne ja Antti 'Jogi' Poikola (VIHR), +358 44 337 5439, antti.poikola@iki.fi
Anders Adlercreutz (RKP)

LIITE 1. Henkilötietoa hyödyntäviä keinoja virusepidemian hallitsemiseksi

Tyypillisiä henkilötietoa hyödyntäviä keinoja virusepidemian hallintaan. Luokittelu on muokattu versio GDPRhub-sivuston luokittelusta[14].

Digitaalinen kontaktiketjujen jäljitys (contact tracing apps and systems)	Sairastuneen henkilön kontaktien jäljittäminen mobiililaitteiden avulla, jotta altistuneita voidaan varoittaa ja määrätä kotikaranteeniin. Singaporen TraceTogether-sovellus on tunnetuin esimerkki, mutta maailmalla on lukuisia muitakin vastaavia kehitteillä ja käytössä.
Immuniteettitodistukset (immunity certificates)	Rokotuskorttia vastaava sertifikaatti, jolla taudin jo sairastaneet voisivat osoittaa (todennäköisen) immuniteettinsa. Tämä helpottaisi epidemian hallintaa siinä vaiheessa, kun liikkumisrajoituksista aletaan asteittain luopumaan. Esimerkiksi saksalainen tutkimusryhmä on ehdottanut tällaista lähestymistapaa[15].
Oireiden tilannekyselijät (self-assessment apps)	Suomalainen Oiretutka, Applen sovellus ja muut vastaavat oireiden tilannekyselysovellukset pyrkivät toisaalta auttamaan ihmisiä itsediagnosoinnissa ja toisaalta kerryttämään populaatiotason tilannekuvaa siitä, missä oirehtivia ihmisiä on. Myös keinoja jatkuvaan seurantaan itsemittauslaitteiden kuten Oura-sormuksen avulla on kehitteillä[16].
Digitaalinen karanteenivalvonta (enforcement of individual quarantine)	Yksilötasolla eristykseen määrätyn valvonta mobiililaitteen tai teletunnistetietojen avulla.
Liikkumistilastot (movement statistics)	Teletunnistetietojen käyttäminen pseudonymisoituina tilastollisen yleiskuvan saamiseksi ihmisten liikkumisesta[17]. Tällainen tilastollinen tieto voi auttaa ulkonaliikkumisrajoitteiden yms. tehokkuuden arvioinnissa ja epidemiamallinnuksessa. Euroopan komissio on lähestynyt teleoperaattoreita kehotuksella luovuttaa dataa viranomaisille[18].

[14] GDPRHub on avoin wikisivusto, johon kootaan ja päivitetään luetteloa henkilötietoratkaisuista koronaepidemiassa https://gdprhub.eu/index.php?title=Projects_using_personal_data_to_combat_SARS-CoV-2

[15] Guardian "'Immunity passports' could speed up return to work after Covid-19" https://www.theguardian.com/world/2020/mar/30/immunity-passports-could-speed-up-return-to-work-after-covid-19

[16] Suomalainen Oura yrittää kehittää älysormustaan niin, että se voi auttaa tunnistamaan koronan oireet https://www.iltalehti.fi/digiuutiset/a/f80888a9-f67a-4ca4-98b9-d8697bdae1aa

[17] VIENNA – Telecom operator sends citizens' movement data to the government https://www.euractiv.com/section/all/short_news/vienna-telecom-operator-sends-citizens-movement-data-to-the-government

[18] Commission tells carriers to hand over mobile data in coronavirus fight https://www.politico.eu/article/european-commission-mobile-phone-data-thierry-breton-coronavirus-covid19