Eemeli Neuvonen

Kontaktien jäljityssovelluksiin liittyvät yksityisyyshuolet

Tietotekniikan kandidaatintutkielma

15. toukokuuta 2023

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Eemeli Neuvonen

Yhteystiedot: eemeli.j.neuvonen@student.jyu.fi

Ohjaaja: Timo Tiihonen

Työn nimi: Kontaktien jäljityssovelluksiin liittyvät yksityisyyshuolet

Title in English: Privacy Concerns in App-Based Contact Tracing

Työ: Kandidaatintutkielma

Opintosuunta: Tietotekniikka

Sivumäärä: 20+0

Tiivistelmä: COVID-19-pandemian aikana yleistyneet kontaktien jäljityssovellukset ovat luonnollisesti herättäneet huolta erityisesti käyttäjän yksityisyyden kannalta. Tässä tutkielmassa kartoitettiin havaittuja yksityisyysongelmia ja -huolia kirjallisuuskatsauksen muodossa. Havainnoista pääteltiin, mitkä huolista voivat olla aiheellisia. Lisäksi pohdittiin mahdollisia keinoja ongelmien ratkaisemiseen ja huolien vähentämiseen. Aiheellisiksi todettiin huolet datan jakamisesta kolmansille osapuolille sekä tietoturva-aukoista sovellusten teknisissä toteutuksissa. Keinoiksi huolien vähentämiseen ehdotettiin esimerkiksi parempaa viestintää ja yksityisyyskeskeisiä ratkaisuja sovellusten kehityksessä. Vaikka osalle huolista löytyi aihetta sovellusten kontekstissa, todettiin myös, ettei sovellusten vaikutus laajempaan digitaaliseen jalanjälkeen ole niin merkittävä.

Avainsanat: COVID-19, Kontaktien jäljitys, Yksityisyys

Abstract: Contact tracing applications popularized during the COVID-19 pandemic have naturally led to privacy concerns among users. This study reviews problems and concerns related to privacy in these applications. The results show which of the concerns are relevant based on the problems detected. In addition, possible solutions for resolving these problems and lowering the concerns are presented. The concerns about data being shared with third parties and security weaknesses in the app designs were confirmed to be relevant. Possible solutions discussed were better communication with the public and privacy-focused app de-

velopment. Although some of the concerns were confirmed to be relevant in the context of app-based contact tracing, the impact on the digital footprint of a user as a whole isn't as significant.

Keywords: COVID-19, Contact tracing, Privacy

Sisällys

1 Johdanto

COVID-19-pandemian aikana kontaktien jäljityssovellukset yleistyivät lähes globaalisti työkaluksi kontrolloida viruksen leviämistä populaatiossa. Lähtökohtaisesti sovelluksia on hankala vertailla keskenään, sillä käytännössä lähes jokaisella valtiolla on oma toteutuksensa. Niitä voidaan kuitenkin jäsennellä jonkin verran teknologia-arkkitehtuurien perusteella. Kontaktien jäljityssovellusten kaltaiseen teknologiaan liittyy luonnollisesti paljon huolenaiheita erityisesti käyttäjän yksityisyyden kannalta, ja niitä onkin viimeisten kolmen vuoden aikana tutkittu jo paljon.

Tämän tutkielman tarkoitus on kirjallisuuskatsauksen muodossa käydä läpi kontaktien jäljityssovelluksiin liittyvää tutkimusta käyttäjien yksityisyyshuolien osalta, verraten sitä tutkimukseen, jota on tehty kyseisten sovellusten yksityisyysongelmista. Lopulta päädytään johtopäätöksiin siitä, miltä osin käyttäjien huolet voivat nykyisen tutkimuksen valossa olla perusteltuja. Tämän lisäksi pohditaan myös mahdollisia keinoja huolien vähentämiseen sekä sovellusten aiheuttamien yksityisyysuhkien vaikutusta laajemman digitaalisen jalanjäljen kontekstissa.

Tutkielman toisessa luvussa perehdytään kontaktien jäljitykseen ja yksityisyyteen aihealueina. Ensin määritellään yksityisyys kontaktien jäljityssovellusten kontekstissa ja vertaillaan, miten erilaiset kulttuurierot voivat vaikuttaa siihen suhtautumiseen. Sen jälkeen esitellään sovelluspohjaisen kontaktien jäljityksen toimintaperiaate ja erilaiset teknologia-arkkitehtuurit tarkemmin. Kolmannessa luvussa perehdytään itse yksityisyyshuoliin ja -uhkiin. Ensin jäsennellään lähdekirjallisuudessa havaittuja yksityisyysongelmia ja -huolia. Sen jälkeen analysoidaan huolien aiheellisuutta ja mahdollisia uhkanäkymiä kerättyjen havaintojen pohjalta. Neljännessä luvussa pohditaan, miten sovelluksiin liittyviä yksityisyyshuolia voitaisiin vähentää ja mikä on sovellusten aiheuttamien yksityisyysuhkien vaikutus koko yksilön digitaaliseen jalanjälkeen. Viides luku on tutkielman yhteenveto.

2 Kontaktien jäljitys ja yksityisyys

Jotta kontaktien jäljitystä voidaan tehdä, täytyy sovellusten väistämättä kerätä ja käsitellä arkaluontoista dataa (Abuhammad, Khabour ja Alzoubi 2020). Sovellukset ovat siis luonnollisesti herättäneet paljon yksityisyyteen liittyviä huolia, joiden onkin tutkittu olevan yksi tärkeimmistä käyttöön vaikuttavista tekijöistä (Chan ja Saqib 2021; Trkman, Popovič ja Trkman 2023). Koska korkea käyttöaste on sovellusten toiminnan kannalta kriittistä (Altmann ym. 2020; Barriga ym. 2020), on myös yksityisyyshuolien tutkiminen tärkeää. Seuraavissa alaluvuissa määritellään ensin, mitä yksityisyys tarkoittaa kontaktien jäljityssovellusten kontekstissa, ja miten erilaiset kulttuurierot voivat vaikuttaa siihen suhtautumiseen. Sen jälkeen esitellään sovellusten yleinen toimintaperiaate ja jäsennellään sovelluskenttää tarkemmin yksityisyyteen vaikuttavien ominaisuuksien pohjalta.

2.1 Yksityisyys ja kulttuurierot

Yksityisyys kontaktien jäljityssovellusten kontekstissa tarkoittaa sitä, että yksilö voi hallita, mitä tietoja hänestä kerätään, ja mihin tarkoituksiin näitä tietoja käytetään (Abuhammad, Khabour ja Alzoubi 2020). Tämä pitää sisällään myös sen, että jokaiseen erilliseen käyttötarkoitukseen vaaditaan käyttäjän erillinen suostumus (Mello ja Wang 2020). Toisin sanoen ei voida olettaa käyttäjän suostumusta, jos käytettävät tiedot tai käyttötarkoitus muuttuvat millään tapaa.

Suhtautuminen yksityisyyteen voi vaihdella eri ihmisryhmien välillä esimerkiksi ikäluokan tai kansalaisuuden perusteella. Etenkin demokraattisissa yhteiskunnissa ihmiset ovat tottuneet kontrolloimaan dataa, jota heistä kerätään (Trkman, Popovič ja Trkman 2023). On myös tutkittu, että mitä kollektiivisempi yhteiskunta on, sitä todennäköisemmin ihmiset ovat valmiita uhraamaan omaa yksityisyyttään yhteisön edun puolesta (Sharma ym. 2020). Esimerkkeinä kollektiivisista yhteiskunnista voisivat toimia monet Aasian valtiot. Individualistisia ja yksilön vapauksia painottavia yhteiskuntia taas löytyy paljon länsimaista.

Kontaktien jäljityssovellusten yhteydessä tärkeäksi tekijäksi on noussut myös luottamus hallintoa kohtaan (Akinbi, Forshaw ja Blinkhorn 2021; Trkman, Popovič ja Trkman 2023). Tä-

mä johtuu siitä, että suurimmassa osassa kontaktien jäljityssovelluksia, sovellusta hallinnoiva taho on nimenomaan maan hallinto. Luottamus voi näkyä niin yksilön kuin koko yhteiskunnan tasolla. Yksilön tasolla sosiaalisesti konservatiiviset henkilöt painottavat perinteisesti henkilökohtaista yksityisyyttä ja mahdollisimman vähäistä kansalaisten valvontaa (Chan ja Saqib 2021). Yhteiskunnan tasolla voidaan todeta, että valtioissa, joissa ollaan valveutuneempia yksityisyysasioista, kannatetaan myös suhteellisesti vähemmän sovelluspohjaista kontaktien jäljitystä. Esimerkkejä tämänkaltaisista valtioista ovat Saksa ja Yhdysvallat. (Altmann ym. 2020)

2.2 Toimintaperiaate

Kontaktien jäljitys ei suinkaan ole uusi keksintö, vaan perinteisesti sitä on tehty manuaalisesti (Leslie 2020). Esimerkiksi lääkäri on voinut kysellä sairastuneelta henkilöltä, keiden kanssa hän on viime aikoina ollut tekemisissä. Sovellusten avulla toiminta on muuttunut kuitenkin huomattavasti tehokkaammaksi. Ei pelkästään osittaisen automaation, vaan myös systemaattisuuden takia, sillä ihminen ei yleensä voi täydellisesti muistaa, missä tai keiden seurassa hän on ollut.

Sovellusten idea on se, että ihmisten kontakteja seuraamalla ja testituloksia keräämällä voidaan luoda lähes reaaliaikainen kuva viruksen leviämisestä. Näin ollen ihmisiä voidaan varoittaa mahdollisesta tartunnasta jo ennen potentiaalisia ensioireita. Kuten jo aikaisemmin todettiin, vaatii tämänkaltaisen toimintamallin tehokas hyödyntäminen tarpeeksi korkeaa käyttöastetta (Altmann ym. 2020; Barriga ym. 2020), ja tästä syystä kaikkien sovellusten käyttöä laskevien huolien tutkiminen ja vähentäminen on erityisen tärkeää. Pelkkä sovellusten lataaminen ei kuitenkaan riitä, vaan käyttäjien pitää myös ilmoittaa tartunnoistaan aktiivisesti (Barriga ym. 2020).

2.3 Teknologia-arkkitehtuurit

Kuten johdantoluvussa mainittiin, voidaan kontaktien jäljityssovellukset jakaa muutamaan eri kategoriaan niissä käytettyjen teknologiaratkaisujen perusteella. Ensimmäinen jako voidaan tehdä kontaktien tunnistamisen kannalta. Noin kolmannes sovelluksista käyttää kontak-

tien tunnistamiseen GPS-sijaintia, kolmannes Bluetoothia, ja kolmannes molempia (Surber 2021). Bluetoothin etu yksityisyyden kannalta on se, ettei käyttäjän sijaintia tarvitse suoranaisesti tallentaa. Sen sijaan kerätään dataa vain siitä, keistä muista käyttäjistä käyttäjä on ollut tietyn etäisyyden päässä tiettynä aikavälinä. (Leslie 2020)

Toinen jako voidaan tehdä kerätyn datan säilytyksen kannalta, eli tallennetaanko data keskitetysti vai hajautetusti. Hajautettu ratkaisu on yksityisyyden kannalta turvallisempi. (Barriga ym. 2020) Keskitetyssä ratkaisussa data tallennetaan keskitetylle palvelimelle, jossa sovelluksen toiminta tapahtuu. Sen etuna voidaan pitää koko datamassan helppoa käsittelyä esimerkiksi sitä analysoidessa. (Azad ym. 2021) Keskitetyt sovellukset ovat herättäneet pelkoja väärinkäytöksistä sekä datavuodoista, ja nämä yksityisyyshuolet ovatkin vaikuttaneet monien eri maiden ratkaisuihin sovellusten kehityksessä. Keskitettyyn ratkaisuun päädyttiin kuitenkin muun muassa Australiassa, Islannissa, Ranskassa ja Singaporessa. (Leslie 2020) Hajautetussa ratkaisussa keskitetylle palvelimelle tallennetaan ainoastaan anonyymejä tunnisteita tartunnan saaneista henkilöistä, tai tarkemmin ottaen heidän laitteistaan. Samalla sovellus käyttäjän puhelimessa kerää tunnisteita laitteista, joiden kanssa on ollut tartuntaetäisyydellä. Näitä tunnisteita vertailemalla sovellus voi varoittaa käyttäjää mahdollisesta tartunnasta. (Azad ym. 2021) Hajautetut sovellukset eivät kerää yksityiskohtaista tietoa käyttäjistä, mutta jotkut sovellukset saattavat kerätä dataa esimerkiksi kontakti-ilmoituksen saaneiden käyttäjien määrästä (Leslie 2020). Tästä huolimatta yksityisyyshuolia on kuitenkin todettu myös hajautettujen sovellusten yhteydessä (Trkman, Popovič ja Trkman 2023). Hajautettuun ratkaisuun päädyttiin muun muassa Saksassa ja Sveitsissä (Leslie 2020).

Näiden päätekijöiden lisäksi sovellusten yksityisyyssuunnittelu voi vaihdella myös kerätyn datan määrän ja laadun sekä datan organisaation sisäisten käyttöoikeuksien (*data access control*) osalta (Abuhammad, Khabour ja Alzoubi 2020). Keväällä 2020 Applen ja Googlen yhteistyössä kehittämä sovelluspohja on toteutettu Bluetoothin avulla (Leslie 2020), ja se tallentaa datan hajautetusti. Se on ollut suosittu ratkaisu varsinkin eurooppalaisissa sovelluksissa. Ehtona sovelluspohjan käytölle on se, että siihen pääsee käsiksi vain yksi sovellus valtiota kohden. Lisäksi sovelluksen pitää olla valtion hallinnon tai terveysviranomaisten hallinnoima. (Barriga ym. 2020)

3 Yksityisyyshuolet ja -uhkat

Kun tutkitaan yksityisyysongelmia näin laajassa sovelluskentässä, on järkevintä keskittyä pääasiassa yleisiin trendeihin. Kaikkiin sovelluskohtaisiin ongelmiin ei edes kannata tarttua, sillä usein ne saatetaan korjata hyvinkin pienellä viiveellä. Sama pätee myös yksityisyyshuolien osalta. Ei ole järkevää keskittyä yksittäisiin huoliin, sillä erilaisia huolia voi olla yhtä monta kuin on uniikkeja käyttäjiä. Huolienkin osalta keskitytään siis laajempiin kokonaisuuksiin. Seuraavissa alaluvuissa käydään ensin läpi lähdekirjallisuudessa havaitut yksityisyysongelmat ja -huolet. Sen jälkeen analysoidaan näitä havaintoja ja määritellään, miltä osin huolet voivat olla perusteltuja.

3.1 Yksityisyysongelmat

Ennen kuin ryhdytään käsittelemään sovelluksissa havaittuja yksityisyysongelmia, on syytä huomioida, että kontaktien jäljityssovellusten kaltainen seurantateknologia luo aina jo lähtökohtaisesti jonkin tasoisen riskin yksityisyydelle (Barriga ym. 2020). Tämä johtuu sovellusten perimmäisestä luonteesta sekä käsiteltävän datan arkaluonteisuudesta. Vaikka sovellusten kehityksessä tehtäisiin kaikki oikeat päätökset, tulee niihin siis aina sisältymään jonkin tasoinen riski (Li ym. 2021). Yleensä kun otetaan käyttöön uutta teknologiaa, tapahtuu niin sanottu normalisaatio, jolloin siitä harvoin enää luovutaan ainakaan kokonaan. Esimerkiksi Edward Snowdenin mukaan syyskuun 11. päivän terrori-iskujen jälkeisestä kansalaisten vakoilusta, kuten puheluiden salakuuntelusta, ei koskaan luovuttu kokonaan. (Barriga ym. 2020) Jo näistä perimmäisistä riskitekijöistä johtuen olisi hyvä, että sovellusten kehitystä valvottaisiin useammankin tahon toimesta. Tämä ei kuitenkaan ole monissa tapauksissa toteutunut. Esimerkiksi keväällä 2020 Yhdysvalloissa tilanne ei ollut ideaali, vaan sovelluksia kehittäville teknologiayrityksille ei näyttänyt olevan minkäänlaista valvontamekanismia. (Mello ja Wang 2020)

Ensimmäinen yksityisyysongelma on ylimääräisten oikeuksien vaatiminen, ylimääräisen datan kerääminen tai muu ylimääräinen toiminta. Tämä ei monestikaan aseta käyttäjän tietoja suoraan vaaraan, mutta nostaa riskitasoa, ja usein vielä täysin turhaan, jos vaaditut oikeudet

tai kerätty data eivät ole sovelluksen toiminnan kannalta olennaisia. Osa sovelluksista vaatii esimerkiksi pääsyä laitteen puhelu- ja tekstiviestitietoihin, kameraan, mikrofoniin, tiedostojärjestelmään tai mediaan (Azad ym. 2021). Osa sovelluksista kerää myös ylimääräistä dataa. Esimerkiksi Dubain valtion kehittämä sovellus kerää käyttäjän nimen, syntymäpäivän, sähköpostiosoitteen sekä puhelinnumeron (Azad ym. 2021), ja Etelä-Afrikan vastaava sovellus kerää käyttäjän nimen, passin numeron sekä osoitteen (Letsebe 2023).

Toinen yksityisyysongelma on datan jakaminen kolmansille osapuolille. Lukuisat sovellukset kertovat tekevänsä tätä, mutta monesti tietosuojalausekkeesta jää kuitenkin epäselväksi, keitä nämä osapuolet ovat, mitä dataa heille jaetaan, tai miten he sitä käyttävät. Tämä on yksityisyyden kannalta ongelmallista, sillä jos datan jakamisen tarkoitus ei ole selkeä, ei käyttäjä voi tietää, mihin hänen tietojaan käytetään. (Azad ym. 2021) Lähdekirjallisuudesta löytyy useita mainintoja datan jakamisesta niin luvallisesti kuin luvattomastikin. Esimerkiksi saksalainen Corona-Datenspende-sovellus vaati yhteyden kolmannen osapuolen kuntoilusovellukseen toimiakseen (Azad ym. 2021). Toukokuussa 2020 myös paljastui, että Pohjois-Dakotan osavaltion virallinen Care19-sovellus lähetti sijaintitietoja ilman käyttäjien lupaa Googlelle sekä eräälle sijaintitietoja mainostajille myyvälle yhtiölle (Akinbi, Forshaw ja Blinkhorn 2021; Leslie 2020). Hieman humoristisempiakin tapauksia löytyy. Esimerkiksi Bahrainissa BeAware Bahrain -sovellus jakoi dataa paikalliselle “Are You at Home?” -TV-ohjelmalle, joka palkitsee niitä, jotka pysyvät ramadanin aikaan kotona (Akinbi, Forshaw ja Blinkhorn 2021).

Kolmas yksityisyysongelma on sovellusten suunnitteluun ja toteutukseen liittyvät tietoturva-aukot. Esimerkiksi osassa kehitysmaissa tehdyistä sovelluksista ei käytetty lainkaan TLS- tai edes SSL-protokollaa tietoliikenteen suojaamiseen (Azad ym. 2021). Useissa sovelluksissa, kuten Qatarin EHTERAZ:issa, Intian Aarogya Setu:ssa ja Pakistanin COVID-19 Gov PK:ssa, havaittiin myös heikkouksia, jotka saattaisivat antaa hakkereille pääsyn käyttäjän arkaluontoisiin tietoihin, kuten nimeen, henkilötunnukseen, terveydentilaan tai sijaintiin (Akinbi, Forshaw ja Blinkhorn 2021). Lisäksi esimerkiksi Bluetooth-teknologiasta paljastuvat heikkoudet vaikuttavat epäsuorasti niiden sovellusten tietoturvallisuuteen, jotka toimivat Bluetoothin kautta, sillä sovellusten toiminta vaatii tietenkin Bluetoothin päällä oloa. Vaikka Bluetoothista löydetyt heikkoudet korjataan yleensä nopeasti, on monissa puhelimissa käy-

tössä niin vanha käyttöjärjestelmä, ettei tietoturvapäivityksiä ole enää saatavilla. Sovellusten oikeaoppinen käyttö vaatisi näiltä käyttäjiltä siis haavoittuvaisen Bluetooth-version jatkuvaa päällä pitämistä. (Akinbi, Forshaw ja Blinkhorn 2021)

3.2 Yksityisyyshuolet

Kontaktien jäljityssovellusten käyttäjäarvioiden ja -palautteen pohjalta vaikuttaa siltä, että suuri osa sovellusten käyttäjistä on tietoisia myös niitä koskevista yksityisyyskysymyksistä (Azad ym. 2021). Yksi huolta aiheuttavista tekijöistä on puutteellinen informaatio esimerkiksi sovellusten tavoitteista, toimintaperiaatteista, kehittäjistä tai muista taustalla olevista tahoista, käytön mahdollisista eduista ja haitoista sekä käytön vapaaehtoisuudesta. Näiden lisäksi myös epäselvät käyttöehdot ja tietosuojalausekkeet ovat omiaan nostamaan huolta. (Abuhammad, Khabour ja Alzoubi 2020) Lähdekirjallisuudessa havaitut yksityisyyshuolet voidaan jakaa kahteen kategoriaan: luotto sovellusta hallinnoivaan organisaatioon (esim. valtio, terveysviranomaiset, yksityinen kehittäjä) ja luotto itse sovelluksen teknologiaan. Organisaatioon liittyvät huolet voidaan niin ikään jakaa karkeasti kolmeen eri kategoriaan.

Ensimmäinen organisaatioon liittyvä huoli on kerätyn datan päätyminen kolmansille osapuolille. Vaikka organisaatio kieltäisi jakavansa dataa, on huoli silti ymmärrettävä, sillä varsinkin sijaintitiedoille löytyy paljon kaupallista käyttöä (Barriga ym. 2020). Myös esimerkiksi vakuutusyhtiöt olisivat varmasti kiinnostuneita henkilökohtaisista terveystiedoista. Tarkemmin ottaen huolta aiheuttavia kysymyksiä ovat muun muassa mihin data tallennetaan, kuka siihen pääsee käsiksi, miten sitä jaetaan ja käytetään (Akinbi, Forshaw ja Blinkhorn 2021), sekä ketkä siitä hyötyvät (Abuhammad, Khabour ja Alzoubi 2020). Joidenkin käyttäjien keskuudessa on herännyt myös epäilys siitä, että dataa jaettaisiin mainostoimistoille, jotka voisivat käyttää sitä kohdennettuun mainontaan (Azad ym. 2021).

Toinen organisaatioon liittyvä huoli on kaikki sovellusten tai kerätyn datan muu väärinkäyttö. Toisin sanoen se, että sovellus valjastettaisiin kansalaisten perusteettomaan syrjintään, seurantaan, käyttäytymisen profilointiin tai muuhun alkuperäisestä poikkeavaan tarkoitukseen (Akinbi, Forshaw ja Blinkhorn 2021). Sovellusten luonteen takia niissä käytetty teknologia voisi olla sovellettavissa myös esimerkiksi poliittisten vastustajien tunnistamiseen ja

seuraamiseen (Mello ja Wang 2020). Varsinkin jos kerätty data yhdistettäisiin muuhun väestötieteelliseen ja sosioekonomiseen dataan, voitaisiin helposti toteuttaa valikoivaa politiikkaa tietyllä tavalla käyttäytyvää väestönosaa kohtaan. Esimerkiksi yleisempi riskien ottaminen ja korkeammat tartuntaluvut voisivat näkyä tulevissa rajoituksissa sekä terveydenhuollon resurssien jakamisessa ja rahoituksessa. (Akinbi, Forshaw ja Blinkhorn 2021)

Kolmas ja viimeinen organisaatioon liittyvä huoli sisältyy varmasti myös kahteen edelliseen, mutta nousee lähdekirjallisuudessa tarpeeksi monta kertaa esille ansaitakseen oman kategoriansa. Kyseessä on huoli sovellusten tai kerätyn datan kohtalosta pandemian jälkeen. Useammassa lähdeartikkelissa mainitaan huoli siitä, että pandemian jälkeen sovelluksia ryhdyttäisiin käyttämään muihin tarkoituksiin, kuten kansalaisten kasvavaan tarkkailuun (Abuhammad, Khabour ja Alzoubi 2020; Altmann ym. 2020). Tämä voisi olla potentiaalinen uhka yksityisyydelle, kansalaisoikeuksille ja poliittisille oikeuksille (Barriga ym. 2020). Lisäksi jo pandemian aikana kerätyn datan kohtalo herättää huolta. Keskeisimpiä ovat kysymykset siitä, miten data tuhotaan, tai aiotaanko se ylipäätään tuhota (Akinbi, Forshaw ja Blinkhorn 2021). Jos kerättyä dataa ei tuhota, voi siitä hyötyä monetkin tahot, kuten suuret teknologiayritykset tai valtiolliset toimijat (Barriga ym. 2020).

Teknologiaan liittyvät huolet ovat epäilyksiä siitä, että sovellukset saattaisivat luoda uhkan tietoturvallisuudelle tahattomasti huonon suunnittelun tai kehitysvirheiden seurauksena. Esimerkiksi huoli siitä, että sovellus sisältäisi tietoturva-aukkoja (Akinbi, Forshaw ja Blinkhorn 2021) tai asettaisi koko puhelimen alttiiksi pahantahtoisille toimijoille (Altmann ym. 2020). Näihin huoliin johtaa todennäköisesti sovellusten nopea kehityskaari sekä käsiteltävien tietojen arkaluonteisuus.

3.3 Uhkanäkymien analyysi

Yksityisyyshuolien aiheellisuutta analysoidessa törmätään ongelmaan, ettei täysin varmasti voida sanoa jonkin realistisen huolen olevan aiheeton, vaikka siitä ei tällä hetkellä löytyisikään näyttöä. Sen sijaan hieman varmempaa on todeta jokin huoli aiheelliseksi, jos siitä löytyy tutkittua näyttöä. Tästä syystä tässä tutkielmassa todetaan yksityisyyshuolia vain aiheellisiksi. Jos huolen aiheellisuudelle ei löydy perusteita, ei siis suoraan hypätä johtopää-

tökseen, että huoli olisi aiheeton. Sen sijaan todetaan, ettei huolta voitu todeta aiheelliseksi.

Lähdekirjallisuudessa havaittiin neljä laajempaa huolenaihetta, jotka ovat datan jakaminen kolmansille osapuolille, sovellusten tai kerätyn datan muu väärinkäyttö, sovellusten tai kerätyn datan kohtalo pandemian jälkeen sekä tietoturva-aukot sovellusten teknisissä toteutuksissa. Lähdekirjallisuudessa havaittujen ongelmien perusteella voidaan suoraan todeta huolet datan jakamisesta kolmansille osapuolille sekä tietoturva-aukoista sovellusten teknisissä toteutuksissa aiheellisiksi, sillä molemmista ongelmista löytyi runsaasti havaintoja useissa eri sovelluksissa. Teknologiaan liittyviä huolia tarkastellessa on kuitenkin syytä huomioida, että suuri osa tietoturva-aukoista esiintyi esimerkiksi kehitysmaissa (Azad ym. 2021), joissa teknologinen osaaminen ei välttämättä ole yhtä korkealla tasolla kuin länsimaissa. Maantieteellinen sijainti voi siis vaikuttaa paljonkin siihen, kuinka perusteltu on huoli sovelluksen teknisestä toteutuksesta.

Sovellusten tai kerätyn datan muusta väärinkäytöstä ei löytynyt tarpeeksi näyttöä, jotta voitaisiin todeta huolen olevan aiheellinen. Vaikka väärinkäytöksiä ei havaittu, huomattiin lähdekirjallisuudessa kuitenkin sellaista ylimääräistä toimintaa, joka voisi altistaa väärinkäytöksille. Ylimääräiset oikeudet tai ylimääräinen data antavat organisaatiolle avaimet ylimääräiseen toimintaan, jolloin toiminnan toteuttaminen riippuu enää organisaation tai sen sisäisten yksittäisten henkilöiden hyväntahtoisuudesta. Jos sovellus saa esimerkiksi oikeudet laitteen mikrofoniin, on organisaatiolla teoreettinen mahdollisuus kuunnella käyttäjää. Tästä näkökulmasta myös sovellusten tai kerätyn datan muu väärinkäyttö voitaisiin siis nähdä relevanttina huolenaiheena. Kun huomioidaan vielä, etteivät kaikki maailman hallinnot ole demokraattisia tai yhtä hyväntahtoisia, voidaan vetää johtopäätös, että maantieteellinen sijainti voi vaikuttaa myös siihen, kuinka perusteltu on huoli sovelluksen tai kerätyn datan muusta väärinkäytöstä. Useissa valtioissa pandemiaa ja siihen liittyviä toimia käytettiin demokratian vastaisesti (Barriga ym. 2020), eikä sovellukset tai niiden lähdekoodit saa missään nimessä luoda apuvälineitä tämänkaltaiseen toimintaan.

Tutkielman kirjoitushetkellä (keväällä 2023) tiedetään, että sovellusten käyttö on jo pääosin lopetettu. Huolta sovellusten käytöstä pandemian jälkeen ei siis voida todeta aiheelliseksi. Kaiken kerätyn datan kohtalosta ei tietenkään voida olla varmoja, mutta koska suurempia väärinkäytöksiä ei ole tullut ilmi, ei myöskään huolta datan kohtalosta voida todeta aiheelli-

seksi. Helmikuussa 2023 Etelä-Afrikassa nousi kohu, kun valvova elin väitti, etteivät maan terveysviranomaiset olisi de-identifioineet ja tuhonneet kerättyä dataa säännösten mukaisesti. Terveysviranomaisten mukaan kyseessä oli kuitenkin vain väärinkäsitys ja datan kanssa oli toimittu asianmukaisesti. (Letsebe 2023) Vaikka sovellusten käytöstä on jo pääosin luovuttu, on syytä huomioida, että seuraavalla kerralla kynnys vastaavaan tai jopa astetta intiimimpään seurantaan lienee alhaisempi jo aikaisemmin mainitun normalisaation takia.

4 Johtopäätökset ja pohdinta

Edellisessä luvussa tultiin siihen johtopäätökseen, että huolet datan jakamisesta kolmansille osapuolille sekä tietoturva-aukoista sovellusten teknisissä toteutuksissa ovat aiheellisia. Sen sijaan huolia sovellusten ja kerätyn datan muusta väärinkäytöstä tai kohtalosta pandemian jälkeen ei voitu todeta aiheellisiksi, vaikka tehtiin myös huomio, että ylimääräisten oikeuksien vaatiminen ja ylimääräisen datan kerääminen voisivat mahdollistaa tämänkaltaista toimintaa. Seuraavissa alaluvuissa pohditaan ensin, miten tutkielmassa havaittuja ongelmia voitaisiin ratkaista ja millä muilla keinoilla yksityisyyshuolia voitaisiin vähentää. Lopuksi verrataan kontaktien jäljityssovellusten aiheuttamia yksityisyysuhkia muuhun yksilöstä kerättävään dataan, ja näin voidaan pohtia yksityisyyshuolien aiheellisuutta vielä koko digitaalisen jalanjäljen kontekstissa.

4.1 Ratkaisut

Aiheellisten huolien vähentämisessä ensisijaisena keinona täytyy olla havaittujen ongelmien ratkaiseminen, eli niitä on mahdollista hallita sovelluksen tai toimintamallin tasolla. Organisaatioon liittyvissä huolissa tämä voi tarkoittaa esimerkiksi sitä, että sovelluksen toimintamalli on muutettava sellaiseksi, ettei dataa enää jaeta kolmansille osapuolille. Jos dataa kuitenkin päätetään jakaa kolmansille osapuolille, tulee käyttäjiä informoida asiasta selkeästi. Koska ensisijaisena tavoitteena on maksimoida sovellusten käyttöaste, lienee toimintamallin muuttaminen parempi vaihtoehto. Aiheettomista huolista eroon pääseminen on haastavampaa, sillä usein ne voivat johtua huonoista mielikuvista tai ennakkoluuloista.

Organisaatioon liittyvien aiheettomien huolien vähentämiseen on lähdekirjallisuudessakin annettu monia keinoja, jotka perustuvat pääosin avoimuuteen ja parempaan viestintään. Koska organisaation maine ja aikaisempi toiminta vaikuttavat varmasti myös luottamukseen, on syytä jo lähtökohtaisesti harkita tarkkaan, minkä organisaation hallintaan sovellus annetaan. Eräässä lähdeartikkelissa onkin tultu esimerkiksi sellaiseen tulokseen, että ihmiset luottavat enemmän terveysviranomaisiin kuin muuhun hallintoon (Li ym. 2021). Muita keinoja luottamuksen nostattamiseen ovat muun muassa selkeä ja kattava tietosuojalauseke (Azad

ym. 2021; Sharma ym. 2020), puolueettoman komitean käyttö sovelluksen kehityksen ja käytön valvonnassa sekä avoin lähdekoodi, joka mahdollistaisi sovelluksen julkisen analyysin (Akinbi, Forshaw ja Blinkhorn 2021).

Sovellusteknologian kannalta huolia voidaan vähentää suunnittelemalla sovellukset alusta lähtien yksityisyyttä korostaen. Sovellukset tulisi siis suunnitella niin sanottua sisäänrakennettua yksityisyyden suojaa (*privacy by design*) mukaillen. Tällöin sovelluksen kehityksessä on suosittu yksityisyyskeskeisiä ratkaisuja ja mahdollisimman pieni osa väärinkäyttömahdollisuuksista riippuu sovellusta hallinnoivan tahon hyväntahtoisuudesta (Cavoukian 2010). Kontaktien jäljityssovellusten kontekstissa tätä voidaan toteuttaa esimerkiksi siten, ettei sovellus vaadi ylimääräisiä oikeuksia tai kerää ylimääräistä dataa. Kerätty data pitäisi siis minimoida siihen, mitä sovellus vaatii toimiakseen. Tämän lisäksi data olisi hyvä anonymisoida ja poistaa heti, kun sitä ei enää tarvita. Minimaalisen datan keräämisestäkin voi kuitenkin nousta tiettyjä ongelmia, kuten valekäyttäjät, joiden avulla voitaisiin toteuttaa palvelunestohyökkäyksiä tai ilmoittaa vääriä tartuntoja. Voi siis olla hyödyllistäkin, että käyttäjä tarvitsee esimerkiksi uniikin puhelinnumeron käyttääkseen sovellusta.

Suositeltavaa olisi myös käyttää jo aikaisemmin yksityisyyden kannalta turvallisemmiksi todettuja teknologiaratkaisuja, kuten kontaktien tunnistamisessa Bluetoothia ja datan käsittelyssä hajautettua mallia. Lisäksi tulisi noudattaa muita yleisesti hyväksi todettuja käytänteitä, kuten asiaankuuluvaa tietoliikenteen suojausta. Sovelluksiin voi tietenkin aina jäädä tietoturva-aukkoja myös vahingossa, mutta niiden määrään vaikuttaa varmasti osaltaan sovellusten nopea kehityskaari. Ratkaisuna voitaisiin sovelluksia siis kehittää jo valmiiksi ennen seuraavaa pandemiaa, jolloin niiden testaamiseen jäisi enemmän aikaa ja virheet voitaisiin minimoida.

4.2 Vaikutus digitaaliseen jalanjälkeen

Digitaalisella jalanjäljellä tarkoitetaan kaikkea dataa, jonka yksilö jättää jälkeensä tarkoituksellisesti tai tarkoituksettomasti käyttäessään Internetiä (Christensson 2014). Myös kontaktien jäljityssovellusten keräämä data on siis osa sitä. Digitaalista jalanjälkeä hyödyntävät pääosin yritykset kaupallisiin tarkoituksiin, eikä rikosoikeudellisia tarkoituksia lukuun otta-

matta dataa yleensä käytetä siihen, että hallinto jäljittäisi kansalaisia tai asettaisi seuraamuksia (Mello ja Wang 2020).

Lähdekirjallisuudessa on mainintoja myös kontaktien jäljityssovellusten ulkopuolella tapahtuneista yksityisyysloukkauksista pandemian aikana. Yhdysvalloissa maan tautikeskus keräsi dataa kymmenien miljoonien ihmisten puhelimista seuratakseen sulkutoimien, ulkonaliikkumiskieltojen ja rokoteohjelman toteutumista (Trkman, Popovič ja Trkman 2023). Israelissa maan hallitus käytti luvattomasti tartunnan saaneiden henkilöiden puhelimien sijaintitietoja ja lähetti niiden perusteella karanteenikäskyjä mahdollisesti tartunnan saaneille henkilöille. Etelä-Koreassa luvaton seuranta vietiin vielä astetta pidemmälle. Tartunnan saaneiden henkilöiden liikkeet tartuntaa edeltävinä päivinä ilmoitettiin julkisesti muun muassa puhelimien sijaintitietojen, luottokorttitietojen ja valvontakameranauhojen perusteella. Henkilöllisyyksiä ei tietenkään paljastettu, mutta ilmoitukseen kuului henkilön ikä, kansalaisuus ja sukupuoli. (Mello ja Wang 2020)

Muun paljastuneen toiminnan perusteella vaikuttaa siis siltä, ettei tosipaikan tullen suostumuksia lopulta edes kysellä, ja hallinnollinen taho pystyy seuraamaan ihmisten liikkumista hyvinkin tarkasti jo muualta saatavien tietojen perusteella. Eräässä lähdeartikkelissa on päädytty johtopäätökseen, ettei sovelluspohjainen kontaktien jäljitys vaaranna yksityisyyttä sen enempää kuin monet kaupallisetkaan tarkoitukset. Sovelluksiin liittyvät yksityisyyshuolet voivatkin johtua osittain siitä, että datan jakaminen hallinnolle herättää joissain ihmisissä enemmän epäilyksiä kuin datan jakaminen kaupallisille yrityksille. (Mello ja Wang 2020)

5 Yhteenveto

Tutkielmassa havaittuja yksityisyyshuolia olivat datan jakaminen kolmansille osapuolille, sovellusten tai kerätyn datan muu väärinkäyttö, sovellusten tai kerätyn datan kohtalo pandemian jälkeen sekä tietoturva-aukot sovellusten teknisissä toteutuksissa. Huolet datan jakamisesta kolmansille osapuolille sekä tietoturva-aukoista sovellusten teknisissä toteutuksissa todettiin aiheellisiksi. Keinoiksi huolien vähentämiseen ehdotettiin esimerkiksi parempaa viestintää ja yksityisyyskeskeisiä ratkaisuja sovellusten kehityksessä. Vaikka osalle huolista löytyi aihetta sovellusten kontekstissa, todettiin myös, ettei sovellusten vaikutus laajempaan digitaaliseen jalanjälkeen ole niin merkittävä. Tutkimuksen tuloksia heikensi se, että tutkittava sovelluskenttä on hyvin laaja. Tämän takia tulokset jäivät melko suuntaa antaviksi. Tuloksista voi kuitenkin olla hyötyä, kun aletaan tutkia yksityisyyshuolia ja -uhkia yksittäisten sovellusten kontekstissa. Vaikka COVID-19-pandemia alkaa olla ohi, on kontaktien jäljityssovelluksiin liittyvää tutkimusta syytä jatkaa, jotta seuraavan pandemian iskiessä voidaan olla paremmissa asemissa ja hyödyntää sovelluksia vieläkin tehokkaammin.

Lähteet

Abuhammad, S., O. F. Khabour ja K. H. Alzoubi. 2020. “COVID-19 Contact-Tracing Technology: Acceptability and Ethical Issues of Use”. *Patient Preference and Adherence* 14:1639–1647. https://doi.org/10.2147/PPA.S276183.

Akinbi, A., M. Forshaw ja V. Blinkhorn. 2021. “Contact tracing apps for the COVID-19 pandemic: a systematic literature review of challenges and future directions for neo-liberal societies”. *Health Information Science and Systems* 9:18. https://doi.org/10.1007/s13755-021-00147-7.

Altmann, S., L. Milsom, H. Zillessen, R. Blasone, F. Gerdon, R. Bach, F. Kreuter, D. Nosenzo, S. Toussaert ja J. Abeler. 2020. “Acceptability of App-Based Contact Tracing for COVID-19: Cross-Country Survey Study”. *JMIR Mhealth and Uhealth* 8 (8): e19857. https://doi.org/10.2196/19857.

Azad, M. A., J. Arshad, S. M. A. Akmal, F. Riaz, S. Abdullah, M. Imran ja F. Ahmad. 2021. “A First Look at Privacy Analysis of COVID-19 Contact-Tracing Mobile Applications”. *IEEE Internet of Things Journal* 8 (21): 15796–15806. https://doi.org/10.1109/JIOT.2020.3024180.

Barriga, A., A. F. Martins, M. J. Simões ja D. Faustino. 2020. “The COVID-19 pandemic: Yet another catalyst for governmental mass surveillance?” *Social Sciences & Humanities Open* 2 (1): 100096. https://doi.org/10.1016/j.ssaho.2020.100096.

Cavoukian, A. 2010. “Privacy by Design”. *Information and Privacy Commissioner of Ontario,* https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf.

Chan, E. Y., ja N. U. Saqib. 2021. “Privacy concerns can explain unwillingness to download and use contact tracing apps when COVID-19 concerns are high”. *Computers in Human Behavior* 119:106718. https://doi.org/10.1016/j.chb.2021.106718.

Christensson, P. 2014. “Digital Footprint Definition”. *TechTerms.com,* https://techterms.com/definition/digital_footprint.

Leslie, M. 2020. “COVID-19 Fight Enlists Digital Technology: Contact Tracing Apps”. *Engineering* 6 (10): 1064–1066. https://doi.org/10.1016/j.eng.2020.09.001.

Letsebe, K. 2023. “Privacy watchdog raises concerns over Covid tracking data”. *Research Professional News,* https://www.researchprofessionalnews.com/rr-news-africa-south-2023-2-privacy-watchdog-raises-concerns-over-covid-tracking-data/.

Li, T., C. Cobb, J. Yang, S. Baviskar, Y. Agarwal, B. Li, L. Bauer ja J. I. Hong. 2021. “What makes people install a COVID-19 contact-tracing app? Understanding the influence of app design and individual difference on contact-tracing app adoption intention”. *Pervasive and Mobile Computing* 75:101439. https://doi.org/10.1016/j.pmcj.2021.101439.

Mello, M. M., ja C. J. Wang. 2020. “Ethics and governance for digital disease surveillance”. *Science* 368 (6494): 951–954. https://doi.org/10.1126/science.abb9045.

Sharma, S., G. Singh, R. Sharma, P. Jones, S. Kraus ja Y. K. Dwivedi. 2020. “Digital Health Innovation: Exploring Adoption of COVID-19 Digital Contact Tracing Apps”. *IEEE Transactions on Engineering Management,* 1–17. https://doi.org/10.1109/TEM.2020.3019033.

Surber, R. S. 2021. “Corona pan(dem)ic: Gateway to global surveillance”. *Ethics and Information Technology* 23 (3): 569–578. https://doi.org/10.1007/s10676-020-09569-5.

Trkman, M., A. Popovič ja P. Trkman. 2023. “The roles of privacy concerns and trust in voluntary use of governmental proximity tracing applications”. *Government Information Quarterly* 40 (1): 101787. https://doi.org/10.1016/j.giq.2022.101787.