Henkilötietojen käsittelyn läpinäkyvyys ja joukkoliikenteen mobiilisovellukset

Mickelsson, Sini, OTM, Turun yliopisto, Oikeustieteellinen tiedekunta.
Carlsson, Robin, tekniikan ylioppilas, Heino, Timi, tekniikan kandidaatti, Rauti, Sampsa, diplomi-insinööri Leppänen, Ville, filosofian tohtori, Turun yliopisto, Teknillinen tiedekunta

Tiivistelmä

Joukkoliikenteen käyttäminen on monelle kansalaiselle välttämättömyys, joten joukkoliikenteen mobiilisovelluksien toiminnan tulee olla avointa ja luotettavaa. Tässä artikkelissa tutkimme henkilötietojen käsittelyn läpinäkyvyyden toteutumista suomalaisissa joukkoliikenteen mobiilisovelluksissa havainnoimalla empiirisesti sovellusten tietosuojaselosteiden saatavuutta ja sisältöjä sekä analysoimalla teknisillä työvälineillä sovellusten tekemiä tietojen siirtoja. Henkilötietojen käsittelyn läpinäkyvyydessä vaikuttaisi tutkimuksemme perusteella olevan selkeitä puutteita: yli kolmella neljäsosalla tutkituista neljästätoista sovelluksesta ei ollut helposti saatavilla sellaista tietosuojaselostetta, joka kuvaisi henkilötietojen käsittelyä kyseisessä sovelluksessa. Havaitsimme myös, että osa sovelluksista lähetti henkilötietoja kolmansille osapuolille ja Euroopan talousalueen ulkopuolelle, vaikka sovellusten tietosuojaselosteissa ei tiedotettu tästä selkeästi käyttäjälle.

1. Johdanto

Kuntalainen hyödyntää joukkoliikennettä päästäkseen lääkärin vastaanotolle paikalliselle terveysasemalle. Hän huomaa ostaessaan lipun joukkoliikenteen mobiilisovelluksen kautta, että kyseisen sovelluksen käyttöehdot ovat pituudeltaan useita A4-arkkeja tiivistä tekstiä. Tottuneesti henkilö navigoi ostamaan lippua lukematta

ehtoja. Kyseessähän on julkinen, luotettava toimija eikä hänellä ole varaa muuhun kuljetukseen kuin paikallisbussiin. Jos kyseinen sovelluksen käyttäjä olisi lukenut käyttöehtojen henkilötietojen käsittelyä koskevan osion, hän olisi huomannut, ettei niiden sisältö oikeastaan lainkaan selvennä sitä, miten henkilötietoja käsitellään sovelluksessa. Joukkoliikenteen mobiilisovellus voi lähettää käyttäjää koskevia tietoja useille eri tahoille ja maantieteellisiin sijainteihin ilman, että käyttäjällä on siitä selkeää tietoa tai ymmärrystä.

Henkilötietojen käsittelyn läpinäkyvyydestä säädetään Euroopan unionin yleisessä tietosuoja-asetuksessa (TSA). Tässä artikkelissa tutkimme, onko joukkoliikenteen mobiilisovelluksissa tietosuojalainsäädännön edellyttämällä tavalla helposti saatavilla tietoa henkilötietojen käsittelystä. Tarkastelemme myös, lähettävätkö mobiilisovellukset käyttäjää koskevia tietoja kolmansille osapuolille ja Euroopan talousalueen ulkopuolelle ja arvioimme, tiedotetaanko näistä siirroista tietosuojalainsäädännön edellyttämällä tavalla käyttäjää. Tarkastelun kohteena ovat erityisesti tietosuojaselosteiden helppo saatavuus sekä tiedonsiirroista ja tietojen vastaanottajista tiedottaminen. Saatavuus on ylipäätänsä koko henkilötietojen käsittelystä tiedottamisen toteutumisen edellytys. Tietojen siirtoihin on puolestaan kiinnitetty erityistä huomiota oikeuskäytännössä viime vuosina (C-311/18, Facebook Ireland and Schrems; Itävallan tietosuojaviranomaisen ratkaisu 22.12.2021; TSV 30.12.2021; TSV 27.4.2023; Irlannin tietosuojaviranomaisen ratkaisu 12.5.2023).

Metodologisesti artikkeli hyödyntää kahta, toisiaan täydentävää lähestymistapaa. Lainopillista lähestymistapaa hyödynnetään systemaattisen tulkinnan muodostamisessa siitä, mitä vaatimuksia lainsäädäntö, oikeuskäytäntö ja viranomaisohjeistukset asettavat henkilötietojen käsittelyn läpinäkyvyydelle. Empiirisessä tutkimuksessa läpinäkyvyysvaatimusten toteutumista arvioidaan sekä havainnoimalla sovellusten tietosuojaselosteiden saatavuutta ja sisältöjä että tutkimalla sovellusten tekemiä tietojen siirtoja verkkoliikenneanalyysin avulla.

Julkisten toimijat eivät aina kaikilta osin ole onnistuneet antamaan tietosuoja-asetuksen edellyttämällä tavalla läpinäkyvästi

tietoa verkkosivuillaan ja mobiilisovelluksissaan henkilötietojen käsittelystä (Heino ym. 2022; Carlsson ym. 2022; TSV 13.12.2022). Tutkittaviksi valittiin joukkoliikenteen mobiilisovellukset, sillä joukkoliikennepalvelut ovat osa kaikenikäisten ihmisten arkea, ja joukkoliikenteen käyttäjiin lukeutuu myös haavoittuvaan ihmisryhmään kuuluvia käyttäjiä kuten lapsia ja vanhuksia. (Traficomin tutkimuksia ja selvityksiä 1/2023, s. 70–71; Liikenneviraston valtakunnallinen henkilöliikennetutkimus 2016, s. 1.) Tulevaisuudessa matkamäärien ennustetaan myös entisestään kasvavan (Metsäranta – Weiste 2019, s. 12). Laajasti käytetyn julkisen palvelun tarjoajina joukkoliikenteen toimijoiden voisi myös olettaa hoitavan henkilötietojen käsittelyn ja sähköisten palvelujensa tietosuojan esimerkillisesti.

Seuraavassa luvussa taustoitetaan henkilötietojen käsittelyn läpinäkyvyyden merkitystä lainsäädännön ja aiemman tutkimuksen avulla. Tämän jälkeen esitellään tutkimusaineisto ja -menetelmät sekä tulokset. Lopuksi käydään läpi johtopäätelmät.

2. Tausta

Henkilötietona pidetään kaikkia tunnistettuun tai tunnistettavissa olevaan henkilöön eli rekisteröityyn liittyviä tietoja (TSA 4(1) artikla). Henkilötiedon käsitettä tulkitaan lähtökohtaisesti laajasti, joten monenlaiset yksilöön yhdistettävissä olevat tietotyypit katsotaan henkilötiedoksi (WP 136, s. 4–5; Korpisaari ym. 2018, s. 52–53, 61–62; Bygrave – Tosoni 2020, s. 113–114). Tietosuoja-asetus edellyttää, että rekisteröidyille on oltava läpinäkyvää, miten ja missä laajuudessa heitä koskevia henkilötietoja käsitellään. Henkilötietojen käsittelyyn liittyvien tietojen ja viestinnän on oltava helposti saatavilla ja ymmärrettävissä ja niissä on käytettävä selkeää ja yksinkertaista kieltä (TSA 5(1) artikla; TSA:n johdannon resitaali 39).

Henkilötietojen käsittelyn läpinäkyvyys on perinteisesti nähty keskeisenä edellytyksenä yksilön mahdollisuudelle valvoa ja vaikuttaa

henkilötietojensa käsittelyyn (WP 260 rev.01, s. 5; COM(2010) 609 final, s. 6.). Läpinäkyvyyteen liittyvä oikeustieteellinen keskustelu on linkittynyt erityisesti tiedollisen itsemääräämisoikeuden ja suostumuksen käsitteisiin. Tiedollisella itsemääräämisoikeudella tarkoitetaan rekisteröidyn valtaa päättää siitä, miten ja mitä tietoa hänestä annetaan muille (Westin 1967, s. 7; Saarenpää 2011, s. 508; Voutilainen 2019, s. 33–36). Oikeustieteellisessä keskustelussa on kuitenkin epäilty rekisteröityjen tosiasiallista kiinnostusta ja kykyä ymmärtää monimutkaisista käsittelytoimenpiteistä annettuja tietoja ja eri käsittelytoimiin myöntymisen seurauksia (Blume 2012, s. 31; Buitelaar 2012, s. 178–179; Koops 2014, s. 252; Van Alsenoy ym. 2014, s. 189–190; van de Waerd 2020, s.13–14; Graef – van der Sloot 2022, s. 519–521). Erityisen ongelmallisena läpinäkyvyyden toteutuminen on nähty verkkoympäristöissä (Edwards 2014, s. 190–191). Ongelmia on pyritty ratkaisemaan muun muassa oikeudellisen muotoilun keinoin (Koolen 2021, s. 178–183).

Toisaalta läpinäkyvyydellä on nähty olevan sekä tärkeä rooli tiedollisen asymmetrian tasoittamisessa eri osapuolten välillä (Koillinen 2012, s. 186–187; van de Waerdt 2020, s. 14) että legitimiteettiä luova vaikutus erityisesti julkisen hallinnon kontekstissa (Koivisto 2021, s. 342). Henkilötietojen käsittelyn läpinäkyvyys voi lisätä luottamusta ja mahdollistaa rekisteröidyn sekä ulkoisten tahojen kontrollin (WP 260 rev.01, s. 4–5). Tietojen antaminen tietosuojaselosteen muodossa on ollut alan vallitseva käytäntö. Tietosuojaselosteet voivat muodostaa toimivan tiedonlähteen käyttäjän päätöksenteon tueksi, mikäli ne ovat helposti saatavilla ja antavat ymmärrettävää tietoa henkilötietojen käsittelystä.

3. Tutkimusaineisto ja -menetelmät

Tutkimukseen valittiin mukaan Suomen 15 suurimman kaupungin joukkoliikenteen mobiilisovellukset. Kunkin kaupungin joukkoliikennesovelluksen nimi selvitettiin, sovellukset etsittiin

Google Play -kaupasta ja asennettiin testipuhelimelle. Tutkittaviksi valittiin 14 sovellusta. Joillakin alueilla käytössä oli useampi sovellus, ja esimerkiksi pääkaupunkiseudulla käytetään samaa sovellusta useammassa suuressa kaupungissa. Google Play -kaupassa latausmäärät vaihtelivat yli 1 000 000 latauksesta yli 500 lataukseen. Latausmäärien mediaanina oli yli 50 000 latausta.

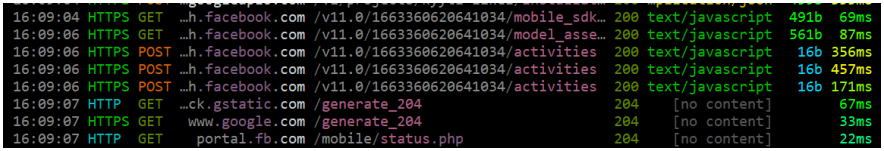
Tutkimuksessa arvioitiin mobiilisovellusten vaatimustenmukaisuutta tietosuoja-asetuksesta, Euroopan tietosuojaneuvoston ja sen edeltäjän tietosuojaryhmän ohjeistuksista ja tietosuojaviranomaisten oikeuskäytännöstä tunnistettuja vaatimuksia vasten. Arvioidut vaatimukset edustavat subjektiivista tulkintaamme siitä, millaisia vaatimuksia eri oikeuslähteissä on esitetty henkilötietojen käsittelyn läpinäkyvyydelle eivätkä tulokset näin ollen välttämättä edusta absoluuttista totuutta tutkittujen tietosuojaselosteiden ja käytäntöjen lainmukaisuudesta. Vaatimusten täyttymistä arvioitiin dikotomisella asteikolla (täyttyy / ei täyty). Vaatimukset avataan yksityiskohtaisesti tuloksien yhteydessä.

Läpinäkyvyysvaatimusten täyttymistä arvioitiin kahta eri lähestymistapaa hyödyntäen. Ensinnäkin havainnoitiin Google Play -sovelluskaupassa saatavilla olevia tietosuojaselosteita, sovelluksen käyttöönoton yhteydessä henkilötietojen käsittelystä annettuja tietoja sekä sovelluksen käyttöliittymän kautta saatavilla olevia tietosuojaselosteita. Tietosuojaselosteet kerättiin tammikuussa 2022. Toiseksi mobiilisovelluksen verkkoliikennettä tallennettiin ja tarkasteltiin sen havainnoimiseksi, mitä henkilötietoja mobiilisovellus lähettää ja minne, ja näitä tietoja vertailtiin tietosuojaselosteissa esitettyihin tietoihin. Näin läpinäkyvyysvaatimusten toteutumista päästiin arvioimaan syväluotaavasti, monipuolisen aineiston valossa.

Ohjelmistotekniikan alalla mobiilisovellusten liikenteen tallentamista on käsitelty useissa tutkimuksissa, joita myös tässä käytetty menetelmä mukailee. Esimerkiksi Conti ym. (2018, s. 2658–2713) tarkastelevat erilaisia tapoja tallentaa mobiililaitteiden

verkkoliikennettä ja Liu ym. (2015, s. 59–70) tutkivat keinoja tunnistaa henkilötietoja verkkoliikenteestä. Verkkoliikenteen sisältämien henkilötietojen ja niitä vastaanottavien kolmansien osapuolien selvittämiseksi toteutetussa koeasetelmassa älypuhelin yhdistettiin internetiin WiFi-tukiasemana toimivan Linux-tietokoneen kautta. Tukiasema säädettiin tallentamaan puhelimen verkkoliikennettä. Koska puhelimen käyttöjärjestelmän mukana on esiasennettuja sovelluksia, jotka tuottavat verkkoliikennettä, ja koska koeympäristö ei salli liikenteen aiheuttaneen sovelluksen tunnistamista tarkasti, käyttöjärjestelmän tyypillistä liikennettä eli taustakohinaa tallennettiin, ja tämä kohina poistettiin kaikista tallenteista. Kokeissa käytettiin Samsung Galaxy J5 SM-J530F-älypuhelinta, jonka käyttöjärjestelmänä oli Android 9.

Verkkoliikennettä tallennettiin mitmproxy- ja tcpdump-työkaluilla. Mitmproxy on avoimen lähdekoodin työkalu, jota voidaan käyttää verkkoliikenteen tarkasteluun, muokkaamiseen ja toistamiseen. Tcpdump puolestaan on verkkoliikenteen pakettien analysointiin soveltuva työkalu, joka lukee ja näyttää verkkoliikenteen pakettien sisällöt käyttäjälle. Mitmproxylla tallennetusta verkkoliikenteestä tutkittiin sekä verkkopyyntöjen sisältöä että vastaanottajaa. Jos pyyntö lähti analytiikkapalvelun osoitteeseen, pyynnössä välitetyt mahdolliset henkilötiedot kirjattiin ylös. Laitteen taustakohinasta eroteltiin ne pyynnöt, jotka ilmenivät ainoastaan sovellusten ollessa asennettuna ja käytössä. Lisäksi monissa pyynnöissä oli jokin muu selvä yhteys testattuun sovellukseen, esimerkiksi sovelluksen nimi osana lokitietoja tai pyynnön User-Agent-otsikkoa. Lisäksi laadittiin lista analytiikkapalveluista (kuten Google ja Facebook), joihin sovellukset välittivät henkilötietoja. Kuvassa 1 on esimerkkiote tallennetusta verkkoliikenteestä. Verkkoliikennettä tallennettaessa kutakin sovellusta käytettiin aktiivisesti noin 5–10 minuuttia, ja käytön aikana käytiin läpi sovelluksen keskeinen toiminnallisuus.



Kuva 1: Esimerkki tutkituista sovelluksista tallennetusta verkkoliikenteestä. Liikenteessä näkyy yhteydenottoja Facebookin ja Googlen palvelimille.

4. Tulokset

4.1 Helppo saatavuus

Tässä alaluvussa tarkastellaan tietosuojaselosteiden ja muiden henkilötietojen käsittelystä annettujen tietojen valossa läpinäkyvyysvaatimusten toteutumista tiedon helpon saatavuuden osalta. Tietosuoja-asetus edellyttää, että henkilötietojen käsittelystä on tiedotettava rekisteröidylle *"helposti ymmärrettävässä ja saatavilla olevassa muodossa"* (TSA 12(1) artikla; TSA:n johdannon 39 kohta). Mobiilisovellusten osalta rekisteröidyn tietojensaanti tulee varmistaa monella eri tasolla. Ensinnäkin tietosuojaselosteen tulee olla löydettävissä sovelluskaupasta jo ennen sovelluksen lataamista (vaatimus 1.1) (WP 260 rev.01, s. 8; WP 202, s. 23). Jotta henkilö voisi tehdä harkitun päätöksen sovelluksen lataamisesta hänen tulisi saada ennakkoon tietoa siitä, miten henkilötietoja käsitellään sovelluksessa. Toiseksi sovelluksen asentamisen jälkeen on henkilötietojen keräämisen yhteydessä annettava linkki tietosuojaselosteeseen tai vaihtoehtoisesti annettava henkilötietoja koskevat tiedot samalla sivulla, jolla henkilötietoja kerätään (vaatimus 1.2) (WP 260 rev.01, s. 8). Käytännössä tämä tarkoittaa, että tietosuojaseloste tulisi tuoda käyttäjän tietoon, kun sovellus otetaan käyttöön ja esimerkiksi käyttäjätilin luomisen yhteydessä. Kolmanneksi tietosuojaselosteen on oltava sovellusta käytettäessä löydettävissä viimeistään kahden napautuksen päästä (WP 260 rev. 01, s. 8). Tässä tutkimuksessa on edellytetty, että tiedot ovat aina

enintään kahden napautuksen päässä pääsivulta niin, että napautusten jälkeen avautuvalta sivulta löytyy suora viittaus henkilötietojen käsittelyyn tai tietosuojaselosteeseen (vaatimus 1.3).

Tutkituista 14 sovelluksesta kaikissa paitsi yhdessä oli Google Play sovelluskauppaan linkattu jonkinlainen tietosuojaseloste tai kuvaus henkilötietojen käsittelystä. Syynä puuttuvaan tietosuojaselosteeseen ilmeisesti oli, että sovelluksen kehittäjän mukaan sovellus ei kerää henkilötietoja (Applen App Storesta oli kuitenkin löydettävissä asiaa koskeva lyhyt seloste). Koska kyseisen sovelluksen käytön yhteydessä käsitellään ainakin jossain määrin muun muassa käyttäjän sijaintitietoa, tässä tutkimuksessa tulkittiin, että sovellukseen liittyy henkilötietojen käsittelyä.

Pelkästään saatavuutta tarkastelemalla ei saada totuudenmukaista kuvaa tilanteesta käyttäjän näkökulmasta. Rekisteröidyn näkökulmasta olennaista on, että tietojen tulee koskea nimenomaan kyseistä sovellusta: tiedoksi ei tulisi antaa esimerkiksi pelkästään sovelluksen omistavan tai julkaisevan organisaation yleistä tietosuojaselostetta, jos se ei anna täsmällistä kuvaa juuri sovelluksen piirissä tapahtuvasta henkilötietojen käsittelystä (WP 260 rev. 01, s. 8). Lisäksi henkilötietojen käsittelyä koskevat tiedot tulisi aina esittää selkeästi erillään muusta kuin tietosuojaan liittyvästä tiedosta kuten sopimusmääräyksistä tai yleisistä käyttöehdoista (vaatimus 1.4), jotta rekisteröity huomaa tiedot tehokkaasti (WP 260 rev. 01, s. 7). Taulukossa 1 on arvioitu tietosuojaselosteiden saatavuutta läpinäkyvyysvaatimuksia vasten huomioiden sen, kuvaako tietosuojaseloste kyseisessä sovelluksessa tapahtuvaa henkilötietojen käsittelyä ja onko tiedot annettu selkeästi erikseen muusta tiedosta.

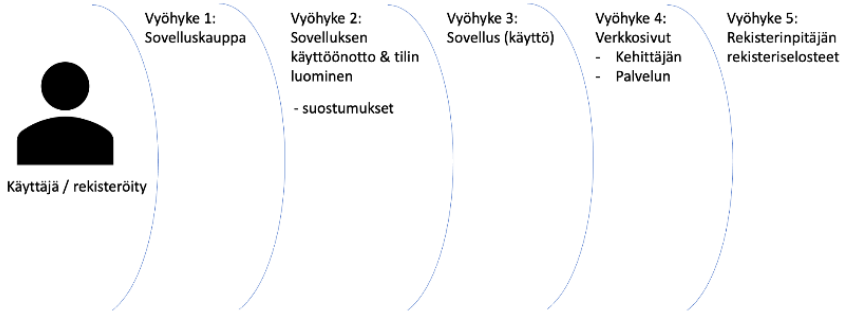
Tietosuojaselostetta koskeva vaatimus / mobiilisovellus	Sovellusta koskeva tietosuoja-seloste on saatavilla mobiilikaupassa (1.1 ja 1.4)	Käyttöönoton yhteydessä annetaan selkeästi tiedoksi sovellusta koskeva tietosuoja-seloste (1.2 ja 1.4)	Käytettäessä on helposti löydettävissä sovellusta koskeva tietosuoja-seloste (1.3 ja 1.4)	Tiedot esitetään erillään muusta kuin tietosuojaan liittyvästä tiedosta (1.4 erikseen)
1.	täyttyy	täyttyy	täyttyy	täyttyy
2.	täyttyy	ei täyty	ei täyty	täyttyy
3.	ei täyty	ei täyty	ei täyty	ei täyty
4.	ei täyty	ei täyty	ei täyty	ei täyty
5.	täyttyy	täyttyy	täyttyy	täyttyy
6.	ei täyty	ei täyty	ei täyty	ei täyty
7.	ei täyty	ei täyty	ei täyty	ei täyty
8.	ei täyty	ei täyty	ei täyty	ei täyty
9.	täyttyy	täyttyy	täyttyy	täyttyy
10.	täyttyy	ei täyty	ei täyty	täyttyy
11.	ei täyty	ei täyty	ei täyty	ei täyty
12.	ei täyty	ei täyty	ei täyty	täyttyy

Tietosuojaselostetta koskeva vaatimus / mobiilisovellus	Sovellusta koskeva tietosuoja-seloste on saatavilla mobiilikaupassa (1.1 ja 1.4)	Käyttöönoton yhteydessä annetaan selkeästi tiedoksi sovellusta koskeva tietosuoja-seloste (1.2 ja 1.4)	Käytettäessä on helposti löydettävissä sovellusta koskeva tietosuoja-seloste (1.3 ja 1.4)	Tiedot esitetään erillään muusta kuin tietosuojaan liittyvästä tiedosta (1.4 erikseen)
13.	täyttyy	ei täyty	ei täyty	ei täyty
14.	ei täyty	ei täyty	ei täyty	ei täyty

Taulukko 1: Läpinäkyyysvaatimusten toteutuminen tietosuojaselosteen saatavuuden, soveltumisalan ja esittämistavan osalta.

Tutkittujen joukkoliikennesovellusten perusteella helpossa saatavuudessa olisi paljon parannettavaa: sovellusta koskeva tietosuojaseloste löytyi sovelluskaupasta kuudessa tapauksessa, sovelluksen käyttöönoton yhteydessä kolmessa tapauksessa ja sovellusta käytettäessä käyttöliittymän kautta vain kolmessa tapauksessa neljästätoista tutkitusta sovelluksesta. Sovelluskaupan osalta seitsemän sovelluksen osalta oli sovelluskauppaan linkitetty vain kehittäjän yleinen tietosuojaseloste, joka ei koske kyseistä mobiilisovellusta, ja yhdessä tapauksessa seloste puuttui kokonaan. Käyttöönoton ja käytön yhteydessä 8/14 sovelluksista tarjosi henkilötietojen käsittelyä koskevat tiedot käyttöehtojen osana, mutta nämä eivät tietosisällöiltään vastanneet tietosuoja-asetuksen vaatimuksia. Kolmesta sovelluksesta tietosuojaselostetta ei ollut löydettävissä lainkaan käyttöönoton ja käytön yhteydessä.

Yhteenvetona ainoastaan kolme neljästätoista sovelluksesta täytti kaikki tässä tarkastellut saatavuutta koskevat vaatimukset eli sovelluskaupasta (vyöhyke 1), sovelluksesta käyttöönoton yhteydessä (vyöhyke 2) sekä sovellusta käyttäessä (vyöhyke 3) löytyi helposti kyseistä sovellusta koskeva tietosuojaseloste (vyöhyke ei tässä viittaa joukkoliikennelippujen maantietellisiin kelpoisuusalueisiin, vaan rekisteriselosteen digitaaliseen saatavuuteen, toim.huom.) Tuloksiin vaikutti numeerisesti se, että sama palveluntarjoaja toimi seitsemän sovelluksen osalta sovelluskehittäjänä.



Kuva 2: Kuvaus vyöhykkeistä, joissa rekisteröityjä informoidaan.

Kun tiedonhaku ulotettiin myös sovelluksen ulkopuolelle eli sovelluksen kehittäjän ja palvelun verkkosivuille (vyöhyke 4) jonkinlainen sovellusta sisällöllisesti kuvaava tietosuojaseloste löydettiin kaikkien sovellusten osalta. Kahdeksassa sovelluksessa käyttäjän tuli siis käytännössä suorittaa Google-haku sovellusta koskevan tietosuojaselosteen löytämiseksi. Huomiona myös, että yhden sovelluksen osalta selosteen keskeinen sisältö oli väite siitä, ettei henkilötietoja kerätä. Kaupunkien verkkosivuilta (vyöhyke 5) oli myös tyypillisesti löydettävissä vielä erillisenä jonkinlainen joukkoliikennettä koskeva asiakasrekisteriseloste.

4.2 Tietojen vastaanottajat ja siirrot

Seuraavaksi tarkastelun kohteena ovat mobiilisovellusten tekemät tietojen siirrot ja niistä tiedottaminen tietosuojaselosteissa. Käsittelyn asianmukaisuuden arviointi edellyttää ymmärrystä siitä, millä toimijoilla on pääsy tietoihin sekä kenelle niitä siirretään. Tietojen maantieteelliset sijainnit ja siirrot vaikuttavat myös siihen, miten riskialttiiksi käsittely mielletään. Tietosuoja-asetus edellyttää, että rekisteröidylle on kerrottava henkilötietojen vastaanottajat (vaatimus 2.1) (TSA 13(1)(a) artikla ja 14(1)(a) artikla). Käytännössä vastaanottajilla tarkoitetaan kaikkia tietojen käsittelyyn osallistuvia tahoja kuten käsittelystä päättävää osapuolta tai osapuolia (rekisterinpitäjät), palveluntarjoajia sekä luovutuksensaajia (TSA 4(1)(9) artikla; WP 260 rev.01, s. 37).

Lähtökohtaisesti henkilötietojen vastaanottajat tulee nimetä. Jos ilmoitetaan nimeämisen sijaan pelkästään vastaanottajien ryhmät, tiedot tulee antaa mahdollisimman tarkasti kertomalla vastaanottajan toiminnasta, toimialasta ja sen alaluokista sekä sijainnista (vaatimus 2.2). (WP 260 rev.01, s. 37.) Oikeuskäytännössä tiedonsiirtojen osalta on määritetty vielä lisävaatimuksena, että rekisteröidyille tulee kertoa esimerkiksi palveluntarjoajista niin, että hän ymmärtää, mitä henkilötietoja on siirretty ja mitä tarkoituksia varten (vaatimus 2.3) (Irlannin tietosuojaviranomaisen ratkaisu 20.8.2021, kohta 427).

Tutkimuksessa havaittiin, että tietojen vastaanottajia käsitellään tietosuojaselosteissa joko yleisellä tasolla (13/14) tai ei lainkaan (1/14). Vain yhdessä selosteessa mainittiin nimeltä yksi palveluntarjoaja, muissa tiedottaminen tapahtui mainitsemalla palveluntarjoajan tai luovutuksen tyyppi (esimerkiksi 10/14 tietosuojaselosteesta mainitsi luovutukset maksupalveluntarjoajille ja 12/14 viranomaisille). Erityisesti käytettyjen järjestelmä- ja analytiikkapalveluntarjoajien erittely ja kuvaukset jäivät tietosuojaselosteissa niin yleiselle tasolle, ettei käyttäjä saa selkeää kuvaa käsittelyyn osallistuvista osapuolista. Tutkituissa sovelluksissa

13/14 tietosuojaselosteesta avasi ainakin jollain tasolla tietojen vastaanottajia (vaatimus 2.1).

Verkkoliikennettä tarkastelemalla todettiin, että tutkituista 14 sovelluksesta puolet (7) lähetti henkilötietoja kolmansille osapuolelle. Tietoa vastaanottavia tahoja olivat virheenjäljitystyökalu Sentry (3 sovelluksessa), Meta (2 sovelluksessa), Microsoftin App Center (1 sovelluksessa) ja Amplitude-analytiikkapalvelu (1 sovelluksessa). Yhdessäkään tietosuojaselosteessa ei nimetty näitä vastaanottajia suoraan. Kahdessa tietosuojaselosteessa mainittiin "sopimuskumppanit", neljässä "järjestelmäpalvelujen tuottajat" tai "järjestelmätoimittajat" ja yhdessä mainittiin, että kerätään analytiikkatietoa sovelluksen kaatumisen yhteydessä, mutta ei eritelty, mikä taho sen vastaanottaa. Verkkoliikenneanalyysissä tunnistettujen vastaanottajien osalta ei annettu tietoa vastaanottajan toiminnasta, toimialasta ja sen alaluokista tai sijainnista (vaatimus 2.2) eikä siitä, mitä tietoja lähetetään ja mitä tarkoituksia varten (vaatimus 2.3).

Mikäli henkilötietoja siirretään ETA:n ulkopuolelle, tietosuoja-asetus edellyttää, että rekisteröidylle kerrotaan asiasta (vaatimus 2.4) (TSA artiklat 13 (1)(f) ja 14 (1)(f); WP 260 rev.01, s. 37–38). Lähtökohtaisesti siirtojen kohteena olevat kolmannet maat tulisi mainita nimeltä (WP 260 rev.01, s. 37–38) (vaatimus 2.5). Lisäksi rekisteröidylle on kerrottava tieto niistä perusteista ja toimenpiteistä, joilla varmistetaan siirretyille henkilötiedoille vastaava suojan taso kuin Euroopan talousalueella (vaatimus 2.6) (TSA 13 (1)(f) ja 14 (1)(f) artiklat; TSA 46–47 artiklat). Oikeuskäytännössä on tarkennettu edelleen, että henkilötietojen siirtoja koskevat tiedot on lisäksi annettava yhdistettynä henkilötietokategorioihin (vaatimus 2.7) (Irlannin tietosuojaviranomaisen ratkaisu 20.8.2021, kohta 427.)

Tarkastelluista 14 joukkoliikennesovelluksesta neljä lähetti hyvin suurella todennäköisyydellä henkilötietoja Euroopan talousalueen ulkopuolelle. Tietojen vastaanottajia olivat aiemmin mainitut Sentry ja Amplitude, joiden palvelimet paikantuivat Yhdysvaltoihin.

Pilvipalvelujen aikakaudella on usein haastavaa paikantaa datan vastaanottajaa täysin varmasti. Käytimme henkilötietojen vastaanottajien paikannukseen iplocation.net-palvelua, joka puolestaan tarkasti palvelimien sijainnit kahdeksalta eri paikannuspalvelulta. Sekä Sentryn että Amplituden tapauksessa kaikki kahdeksan palvelua paikansivat tietojen vastaanottajan Yhdysvaltoihin. Yhdessäkään tietosuojaselosteessa ei kuitenkaan ollut mainintaa tiedonsiirroista ETA:n ulkopuolelle. Yhdessä tosin tehtiin varauma, että ETA:n ulkopuolisia siirtoja voidaan tehdä, mutta siirroista ei kerrottu vaatimuksien 2.5–2.7 edellyttämiä tietoja.

Taulukko 2 listaa tutkittujen joukkoliikennesovellusten kolmansille osapuolille lähettämät henkilötiedot. IP-osoite on numerosarja, joiden avulla voidaan pääsääntöisesti yksilöidä verkkoon yhdistetty laite ja sen käyttäjä. Vaikka IP-osoitteet ovat useimmissa tapauksissa vaihtuvia, on hyvin tavallista, että sama osoite säilyy samalla laitteella ja käyttäjällä yli kuukaudenkin ajan (ks. esim. Mishra ym. 2020). Erityisesti suurilla globaaleilla analytiikkapalvelujen tarjoajilla voi olettaa olevan tehokkaita keinoja yhdistää dynaamisetkin IP-osoitteet tiettyyn käyttäjään. Vaihtuvakin IP-osoite voidaan tulkita tunnistettavissa olevaa henkilöä koskevaksi henkilötiedoksi, kun esimerkiksi verkkosivuston ylläpitäjä voi tarvittaessa laillisin keinoin saada viranomaisen hankkimaan internetyhteyden tarjoajalta sellaiset lisätiedot, jotka vaaditaan IP-osoitteen liittämiseksi yksilöön (C-582/14, Breyer, kohta 49). Käyttäjän tunnistamisessa voivat toisiinsa yhdistettynä kuitenkin auttaa sellaisetkin tiedot, jotka yksinään eivät kytkeydy tiettyyn käyttäjään. Näitä ovat esimerkiksi monet laitteeseen ja verkkoselaimeen liittyvät tiedot, kuten puhelimen merkki, käyttöjärjestelmä ja laitteen näytön koko. Koska kansainvälisiä tietojen siirtoja koskevat tiedot esitettiin tietosuojaselosteissa hyvin yleisellä tasolla, ei selosteista myöskään löytynyt erittelyä mahdollisesti siirrettävistä henkilötietojen kategorioista.

Sovelluksen analytiikassa lähettämä tieto	**Tiedon lähettäneiden sovellusten lukumäärä (max 14)**	**Prosenttiosuus sovelluksista (max 100%)**
IP-osoite	7	50,0
Puhelimen merkki	3	21,4
Puhelimen malli	3	21,4
Puhelimen käyttöjärjestelmä	5	35,7
Käyttöjärjestelmän versio	4	28,6
Näytön koko	2	14,3
Palveluntarjoaja (esim. Elisa)	1	7,1
Laitetunniste	1	7,1
Muu / tuntematon tunniste	2	14,3
Aikavyöhyke	1	7,1
Maa	2	14,3
Sijainti (kaupunki, alue)	1	7,1
Kieli	2	14,3

2: Sovelluksista kolmansille osapuolille lähetetyt henkilötiedot.

Tuloksien perusteella joukkoliikennesovellusten tietosuojaselosteiden kuvauksissa olisi tietojen vastaanottajien osalta selkeytettävää. Tutkituissa tietosuojaselosteissa käsitellään tietojen siirtojen vastaanottajia joko yleisellä tasolla tai ei lainkaan. Verkkoliikenteen analyysin perusteella puolet sovelluksista lähetti tietoja palveluntarjoajille tai kolmansille osapuolille, mutta näitä osapuolia ei nimetty tietosuojaselosteissa tai kuvattu tavalla, josta käyttäjä

ymmärtäisi niitä koskevat olennaiset tiedot. Tarkastelluista 14 joukkoliikennesovelluksesta neljä lähetti hyvin suurella todennäköisyydellä henkilötietoja ETA:n ulkopuolelle, mutta tietosuojaselosteissa ei kerrottu näiden tietojen siirtojen suojatoimenpiteistä tai siitä, mitä henkilötietotyyppejä siirrettiin ja mihin tarkoituksiin.

5. Yhteenveto ja päätelmät

Joukkoliikenteen mobiilisovelluksia koskevan tutkimuksemme tulokset osoittavat, että läpinäkyvyysvaatimusten toteutumisessa on puutteita tarkastelemiemme osa-alueiden eli saatavuuden ja tietojen siirtojen läpinäkyvyyden osalta. Havaitsimme, että yli kolmella neljäsosalla tutkituista sovelluksista ei ollut helposti saatavilla sellaista tietosuojaselostetta, joka kuvaisi henkilötietojen käsittelyä kyseisessä sovelluksessa. Verkkoliikennettä tarkastelemalla todettiin, että tutkituista 14 sovelluksesta puolet (7) lähetti henkilötietoja kolmansille osapuolille. Lisäksi tarkastelluista sovelluksesta neljä lähetti hyvin suurella todennäköisyydellä henkilötietoja Euroopan talousalueen ulkopuolelle. Tietosuojaselosteissa oli tietojen siirtojen osalta selkeitä puutteita sekä tietojen vastaanottajista että maantieteellisistä sijainneista tiedottamisessa.

Tutkimuksemme tulokset antavat viitteitä, että joukkoliikenteen mobiilisovellusten rekisterinpitäjillä ja sovellusten kehittäjillä ei ole välttämättä selkeää kuvaa siitä, miten helppo saatavuus tulisi toteuttaa mobiilisovellusten osalta. Mobiilisovellusten kehittäjille suunnatun tiiviin ja selkokielisen vaatimuslistan julkaiseminen todennäköisesti ohjaisi mobiilisovellusten läpinäkyvyyskäytäntöjä oikeaan suuntaan. Läpinäkyvyyden toteuttamisessa on tärkeää, että rekisterinpitäjät tuntevat henkilötietoja koskevat käsittelytoimensa ja siirtonsa. Käytännössä tämä usein edellyttää ymmärrystä myös palkatun palveluntarjoajan teknisistä ratkaisuista ja alikäsittelijöistä.
Useissa tapauksissa havaitsimme, että joukkoliikenteen mobiilisovellusten saatavilla oleva tietosuojaseloste tai muu

tietosuojaa koskeva osio ei koskenut tutkittavaa sovellusta vaan esimerkiksi kehittäjätahon yleisten verkkosivujen tietosuojakäytäntöjä. Tietosuojaselosteiden tarkoituksen toteutumisen kannalta on tärkeää, että niiden sisältö koskee täsmällisesti juuri kyseistä mobiilisovellusta ja tarvittaessa erittelee sen suhteen mahdollisiin muihin tietosuoja- tai rekisteriselosteisiin. Esimerkiksi, jos kaupungilla on erikseen joukkoliikenteen mobiilisovellusta koskeva kuvaus ja joukkoliikenteen yleistä asiakasrekisteriä koskeva rekisteriseloste, tulisi selkeästi kuvata, mikä näiden kahden selosteen välinen suhde on. Tiedot tulisi antaa rekisteröidyn kannalta ymmärrettävällä tavalla (Voutilainen 2019, s. 99). Sovelluksen käyttäjän näkökulmasta selkeintä olisi käyttää yhtä palvelu- tai sovelluskohtaista tietosuojaselostetta.

Joukkoliikenteen mobiilisovellusten käyttäjäkunnalla ei usein käytännössä ole niiden käytölle markkinoilla tosiasiallista vaihtoehtoa. Käsittelyn piirissä on myös haavoittuvassa asemassa olevia ihmisryhmiä. Yhteiskunnan merkittävien palveluiden kuten joukkoliikenteen palveluiden yhteydessä tapahtuvan henkilötietojen käsittelyn tulisi olla avointa ja pitäytyä siinä, mikä on välttämätöntä. Tällaisten palveluiden kehittäjiltä tulisi edellyttää mahdollisimman tietosuojasensitiivisten ratkaisujen tekemistä, kuten esimerkiksi sellaisen analytiikkakehyksen valitsemista, missä analytiikkatietoa ei välitetä sovelluksesta kolmansille osapuolille tai Euroopan talousalueen ulkopuolelle. Läpinäkyvyydellä edistetään sekä yksilön tiedollisen itsemääräämisoikeuden toteutumista että lisätään palveluiden luotettavuutta kansalaisten silmissä.

Lähteet

Article 29 Data Protection Working Party. 2013. Opinion 02/2013 on apps on smart devices. WP 202. Adopted on 27 February 2013.

Blume, P. 2012. The inherent contradictions in data protection law. International Data Privacy Law. [Verkkolehti]. Vol. 2:1. S. 26–34. [Viitattu

3.3.2023]. ISSN 2044-4001 (sähköinen). https://doi.org/10.1093/idpl/ipr020

Buitelaar, J.C. 2012. Privacy: Back to the roots. German Law Journal. Cambridge University Press. [Verkkolehti]. Vol. 13:3. S. 171–202. [Viitattu 1.3.2023] ISSN 2071-8322 (sähköinen). https://doi.org/10.1017/S2071832200020460

Bygrave, L. A. & Tosoni, L. 2020. Article 4(1) Personal data. S. 103–115 teoksessa Kuner, C. & Bygrave, L. A. & Docksey, C. (toim.). The EU General Data Protection Regulation (GDPR): A Commentary. Oxford University Press. ISBN 9780198826491. https://doi.org/10.1093/oso/9780198826491.003.0007

Carlsson, R. & Heino, T. & Koivunen, L. & Rauti, S. & Leppänen, V. 2022. Where Does Your Data Go? Comparing Network Traffic and Privacy Policies of Public Sector Mobile Applications. S. 214–225 teoksessa Rocha, A. & Adeli, H. & Dzemyda, G. & Moreira, F. (toim.). Information Systems and Technologies. WorldCIST 2022. Lecture Notes in Networks and Systems, vol 468. Springer, Cham. ISBN 978-3-031-04826-5. https://doi.org/10.1007/978-3-031-04826-5_21

Conti, M. & Li, Q. & Maragno, A. & Spolaor, R. 2018. The dark side (-channel) of mobile devices: A survey on network traffic analysis. IEEE communications surveys & tutorials. [Verkkolehti]. Vol. 20:4. S. 2658–2713. [Viitattu 3.1.2023] ISSN 1553-877X (sähköinen). https://doi.org/10.48550/arXiv.1708.03766

Edwards, L. 2013. Privacy, law, code and social networking sites. S. 309–352 teoksessa Brown, Ian (toim.). Research Handbook on Governance of the Internet. Edward Elgar. ISBN 978 1 84980 502 5. https://doi.org/10.4337/9781849805025.00021

European Commission. 2010. Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of Regions: A comprehensive approach on personal data protection in the European Union. Brussels, 4.11.2010. COM (2010) 609 final.

Graef, I. & van der Sloot, B. 2022. Collective Data Harms at the Crossroads of Data Protection and Competition Law: Moving Beyond Individual Empowerment. European Business Law Review. [Verkkolehti]. Vol. 33:4. S. 513–536. [Viitattu 3.1.2023] ISSN 1875-841X (sähköinen). https://doi.org/10.54648/eulr2022024

Heino, T. & Carlsson, R. & Rauti, S. & Leppänen, V. 2022. Assessing discrepancies
between network traffic and privacy policies of public sector web services. S. 1-6 teoksessa ARES 2022: Proceedings of the 17th International Conference on Availability, Reliability and Security. ISBN 978-1-4503-9670-7.
https://doi.org/10.1145/3538969.3539003

Koillinen, M. 2013. Henkilötietojen suoja itsenäisenä perusoikeutena. Oikeus 2/2013. [Verkkolehti]. S. 171–193. [Viitattu 1.2.2023] ISSN 0356-4037 (sähköinen).

Koivisto, I. 2021. Miksi läpinäkyvyyden ihanne globalisoituu? Lakimies 3–4/2021. [Verkkolehti]. S. 333–356. [Viitattu 1.2.2023] ISSN 2953-9919 (sähköinen).

Koolen, C. 2021. Transparency and Consent in Data-Driven Smart environments. European Data Protection Law Review. [Verkkolehti]. Vol. 7:2. S. 174–189. [Viitattu 3.5.2023] ISSN 2364-284X (sähköinen). https://doi.org/10.21552/edpl/2021/2/7

Liikenne- ja viestintävirasto. 2023. Henkilöliikennetutkimus 2021. Traficomin tutkimuksia ja selvityksiä 1/2023. [Viitattu 3.5.2023] ISSN 2669-8781 (sähköinen).

Liikennevirasto. 2018. Henkilöliikennetutkimus: Joukkoliikenne. Faktakortti - laadittu helmikuussa 2018. Saatavissa: https://www.traficom.fi/sites/default/files/media/file/Faktakortti-HLT2016-joukkoliikenne.pdf

Liu, Y. & Song, H. & Bermudez, I. & Mislove, A. & Baldi, M. & Tongaonkar, A. 2015. Identifying personal information in internet traffic. S. 59–70 teoksessa COSN 2015: Proceedings of the 2015 ACM on Conference on Online Social Networks. ISBN 978-1-4503-3951-3. https://doi.org/10.1145/2817946.2817947

Koops, B.-J. 2014. The trouble with the European data protection law. International Data Privacy Law. [Verkkolehti]. Vol. 4:4. S. 250–261. [Viitattu 1.3.2023]. ISSN 2044-4001 (sähköinen). https://doi.org/10.1093/idpl/ipu023

Korpisaari, P. & Pitkänen, O. & Warma-Lehtinen, E. 2018. Uusi tietosuojalainsäädäntö. Alma Talent. ISBN 978-952-14-3170-8

Metsäranta, H. & Weiste, H. 2019. Taustaselvitys joukkoliikenteen tilakuvasta ja tavoitteellisesta kehityssuunnasta. Traficomin julkaisuja 25/2019. [Viitattu 30.1.2023]. ISSN 1799-0157 (sähköinen).

Mishra, V. & Laperdrix, P. & Vastel, A. & Rudametkin, W. & Rouvoy, R. & Lopatka, M. 2020. Don't count me out: On the relevance of IP address in the tracking ecosystem. S. 808–815 teoksessa Proceedings of The Web Conference 2020. ISBN 978-1-4503-7023-3. https://doi.org/10.1145/3366423.3380161

Polčák, R. 2020. Article 12 Transparent Information, communication and modalities for the exercise of the rights of the data subject. S. 398-412 teoksessa Kuner, C. & Bygrave, L. A. & Docksey, C. (toim.). The EU General Data Protection Regulation (GDPR): A Commentary. Oxford University Press. ISBN 9780198826491. https://doi.org/10.1093/oso/9780198826491.003.0042

Saarenpää, A. 2011. Oikeusinformatiikka. Teoksessa Niskanen, Maarit (toim.) Oikeusjärjestys osa I. 7. Täydennetty painos. Lapin yliopiston oikeustieteellisiä julkaisuja, sarja C 56. Bookwell Oy. ISBN 978-952-484-408-6.

Tietosuojatyöryhmä. 2017. Asetuksen 2016/679 mukaista läpinäkyvyyttä koskevat suuntaviivat. WP260 rev.01. Annettu 29. Marraskuuta 2017. Viimeksi tarkistettu ja hyväksytty 11. huhtikuuta 2018.

Tietosuojatyöryhmä. 2007. Lausunto 4/2007 henkilötietojen käsitteestä. WP 136. Annettu 20. kesäkuuta 2007.

Van Alsenoy, B. & Kosta, E. & Dumortier, J. 2014. Privacy notices versus informational self-determination: Minding the gap. International Review of Law, Computers & Technology. [Verkkolehti]. Vol. 28:2. S. 185–203. [Viitattu 2.3.2023]. ISSN 1364-6885 (sähköinen). https://doi.org/10.1080/13600869.2013.812594

van de Waerdt, P. J. 2020. Information asymmetries: recognizing the limits of the GDPR on the data-driven market. Computer Law & Security Review 38. [Verkkolehti]. [Viitattu 2.1.2023]. ISSN 1873-6734 (sähköinen). https://doi.org/10.1016/j.clsr.2020.105436

van Hoboken, J. & Dathaigh, R. Ó. 2021. Smartphone platforms as privacy regulators. Computer Law & Security Review 41. [Verkkolehti]. [Viitattu 2.1.2023]. ISSN 1873-6734 (sähköinen). https://doi.org/10.1016/j.clsr.2021.105557

Voutilainen, T. 2019. Oikeus tietoon: Informaatio-oikeuden perusteet. Edita Publishing Oy. 2., uudistettu painos. ISBN 978-951-37-7431-8.

Westin, A. F. 1967. Privacy and Freedom. New York: Atheneum Press. ISBN 0689102895.