Liikenne- ja viestintäministeriö

Oikeudenmukaista ja älykästä liikennettä

Tietoturva ja yksityisyyden suoja -alatyöryhmä

Julkaisuja 40/2013

Liikenne- ja viestintäministeriön

visio
Hyvinvointia ja kilpailukykyä hyvillä yhteyksillä

toiminta-ajatus
Liikenne- ja viestintäministeriö edistää väestön hyvinvointia ja elinkeinoelämän kilpailukykyä. Huolehdimme toimivista, turvallisista ja edullisista yhteyksistä.

arvot
Rohkeus
Oikeudenmukaisuus
Yhteistyö

Liikenne- ja viestintäministeriö

Julkaisun päivämäärä 16.12.2013	
Julkaisun nimi Oikeudenmukaista ja älykästä liikennettä. Tietoturva ja yksityisyyden suoja -alatyöryhmä	
Tekijät Traficon Oy ja RappTrans AG	
Toimeksiantaja ja asettamispäivämäärä	
Julkaisusarjan nimi ja numero Liikenne- ja viestintäministeriön julkaisuja 40/2013	ISSN (verkkojulkaisu) 1795-4045 ISBN (verkkojulkaisu) 978-952-243-375-6 URN http://urn.fi/URN:ISBN:978-952-243-375-6 HARE-numero
Asiasanat Tiemaksut, tietosuoja	
Yhteyshenkilö Tuomo Suvanto	
Muut tiedot	

Tiivistelmä

Oikeudenmukaista ja älykästä liikennettä -työryhmä on selvittänyt tienkäyttömaksujen käyttöönottoa, motiiveja ja vaikutuksia Suomessa. Osana työtä on laadittu taustaraportti tietoturvasta ja yksityisyyden suojasta erilaisissa tiemaksujärjestelmissä. Tienkäyttömaksujärjestelmiä käsiteltäessä nousevat tietoturva ja yksityisyyden suoja yhdeksi tärkeimmistä selvitettävistä asioista. Taustaraportissa käydään läpi tiemaksujen tietoturvaan liittyviä lainsäädännöllisiä säädöksiä niin Suomen kuin Euroopan unioninkin tasolla, sekä käydään läpi tienkäyttömaksujen teknisiä ratkaisuja yksityisyyden suojan kannalta.

Taustaraportissa todetaan, että paikannukseen perustuvaan tiemaksujärjestelmään on mahdollista luoda sellainen yksityisyyden suoja, joka pystyy takaamaan käyttäjän yksityisyyden mahdollisimman tarkasti ja luotettavasti. Tällaisen järjestelmän suunnittelun pitäisi perustua ”privacy by design” -periaatteelle, ja järjestelmän luonnissa pitäisi noudattaa ”älykäs ajoneuvolaite” -konseptia, jossa ajoneuvoista kerätty data säilytetään hajautetusti ja jossa yksityiskohtainen reittitieto tuhotaan heti, kun sitä ei enää tarvita.

Kerätty tieto pitäisi olla mahdollisuuksien mukaan käyttäjän hallinnassa, ja tietojen käyttäminen muihin tarkoituksiin (esim. "pay-as-you-drive” vakuutukseen) tulisi olla mahdollista vain käyttäjän selkeällä ja yksiselitteisellä suostumuksella. Ratkaisuna tällaiseksi järjestelmäksi voisi olla ns. pilvipalveluna toimiva kansalaistili, johon ajoneuvolaite lähettäisi tiedot ajoneuvon liikkeistä, ja josta sitten määräajoin lähetettäisiin laskutusta hoitavalle viranomaiselle kooste ajetuista kilometreistä laskutusta varten. Myös järjestelmän valvonnassa käyttäjän henkilöllisyyttä tulisi selvittää vain silloin, jos väärinkäytöksistä on todisteita. Kaikkien käyttäjälaitteen rajapintojen tulisi perustua avoimiin rajapintamäärittelyihin ja rajapintojen ajurien tulisi perustua avoimeen lähdekoodiin.

Yhteenveto

Tarkoittaako sähköisten tiemaksujen tuleminen anonyymin ajamisen loppumista? Eikö tiemaksuissa ole kyse siitä, että tiedetään, kuka oli missä milläkin hetkellä ja laskuttaa siitä?

Ajanmukaisissa maksujärjestelmissä, jotka perustuvat maantieteelliseen paikantamiseen satelliittien avulla, ajoneuvojen etenemistä seurataan periaatteessa metri metriltä. Miten voi olla varma siitä, että tätä yksityiskohtaista tietoa käytetään ainoastaan hyväksyttävään tarkoitukseen ja edelleen, miten tienkäyttäjä voi varmistua siitä, että hänen päivittäistä matkaa koskeva arkaluontoinen informaatio, kuten sairaalakäynti, lääkärissä käynti, poliittiseen kokoukseen osallistuminen tai ostoskäyttäytyminen, jää yksityiseksi?

Tiedon suojaamisessa on ensi kädessä kysymys käyttäjän suojaamisesta ei-toivotun käytön aiheuttamia negatiivisia seuraamuksia vastaan, mutta myös yleisemmin jokaisen ihmisen intimiteetin ja yksityisen lähialueen turvaamisesta. Tietosuojatoimet turvaavat intimiteettisuojan IT-maailmassa paljolti samalla tavalla kuin vaatteet, seinät, kylpyhuoneen verhot ja wc-ovet suojaavat ihmisen intimiteettiä reaalimaailmassa. Reittitietoa on käsiteltävä henkilökohtaisena informaationa jopa nimettömänä. Kun tunnetaan päivittäinen reitti, henkilö on helposti tunnistettavissa kuten myös missä hän asuu, työpaikka, mieluinen ostoskeskus, mahdolliset vierailut sairaalassa, kirkossa, poliittisessa kokouksessa jne. Tällaista tietoa on kaikissa tilanteissa suojattava, eikä vähiten sen takia, että yksityisyyden rikkominen tai edes kuviteltu rikkominen julkisuushälyn seuraamana on vahvasti myötävaikuttanut hankkeiden kaatumiseen, kuten esimerkit osoittavat.

On siten suositeltavaa suunnitella tiemaksujärjestelmää alusta alkaen yksityisyyden turvaamista silmälläpitäen. Tämä suositus ei ole tietonörtin, vaan sen tulisi olla normaalisti noudatettava hyvä käytäntö (good practice). Yksityisyyden suojanäkökulmat eivät johda monimutkaisiin ratkaisuihin, jos ne alun perin otetaan mukaan suunniteluun integroituna elementtinä.

Voidaan antaa seuraavat suositukset:

- Tulisi noudattaa ”älykäs ajoneuvolaite” (smart client) -konseptia, jossa data säilytetään hajautetusti ja pysyy käyttäjän hallinnassa
- Yksityiskohtainen reittitieto tulee tuhota heti, kun sitä ei enää tarvita
- Tietojen käyttäminen muihin tarkoituksiin (esim. "pay-as-you-drive” vakuutukseen), tulisi olla mahdollista vain käyttäjän selkeällä ja yksiselitteisellä suostumuksella
- Valvonnassa käyttäjän henkilöllisyyttä tulisi selvittää vain, jos on todisteita väärinkäytöksestä
- Kaikkien käyttäjälaitteen rajapintojen tulisi perustua avoimiin rajapintamäärittelyihin ja rajapintojen ajurien tulisi perustua avoimeen lähdekoodiin.

Henkilötietojen suojaamisen perusperiaatteet pyrkivät säilyttämään käyttäjän nimettömyyden ja teknologiaa tulisi ja voidaan soveltaa siten, että kuljettajan nimettömyys säilyy. Jokainen poikkeama tästä periaatteesta merkitsisi taas uutta loukkausta informaatioyhteiskunnan jo heikentämää yksityisyyttä kohtaan.

Työstettäessä jatkossa järjestelmäarkkitehtuuria noudattaen ”Yksityisyys suunnittelemalla” (Privacy by Design) paradigmaa, huomio tulisi olla kohdistettuna siihen, missä tiedot säilytetään ja käsitellään ja kenen toimesta, rajapintojen tunnistamiseen, tietovirtojen määrittelyyn sekä tiedon suojaamiseen.

Esipuhe

Oikeudenmukaista ja älykästä liikennettä selvittävän työryhmän selvitystyön tarkoituksena on muodostaa kokonaiskuva siitä, kuinka Suomen kannattaisi edetä tiemaksujen käyttöönotossa pitkällä aikavälillä. Selvityksessä tulee tarkastella tiemaksujen teknisiä, liikenteellisiä, taloudellisia ja lainsäädännöllisiä kysymyksiä.

Yksityisyyden suoja ja sitä myöten myös tietoturva ovat keskeisimpiä kysymyksiä tiemaksu/verojärjestelmää valmisteltaessa. Käyttäjää tunnistavat ja paikantavat järjestelmät luovat uusia haasteita yksityisyyden suojaamiselle. Ottamalla asia huomioon suunnittelun kaikissa vaiheissa sekä tekemällä asiat oikein alusta alkaen, yksityisyyden suoja ja tietoturva voidaan kuitenkin hoitaa.

Ministeriö on kiinnittänyt Traficon Oy:n ja RappTrans AG:n laatimaan muistion yksityisyyden suojaan ja tieturvaan liittyvistä kysymyksistä ja näkemyksistä sekä siihen liittyvistä kansainvälisistä kokemuksista.

Bernhard Oehry RappTrans AG:stä on pääosin vastannut muistion laadinnasta. Kristian Appel Traficon Oy:stä on osallistunut tehtävän sisällön määrittelyyn sekä vastannut työn laadunvalvonnasta. Ministeriön edustajana työssä on ollut Tuomo Suvanto.

Sisällysluettelo

Yhteenveto 1
Esipuhe 2
1. Selvityksen tarkoitus ja kohde 4
2. Periaatteet 4
2.1 Yksityisyyden käsite 4
2.2 Yksityisen tiedon lajeja 5
2.3 Käsitteet 6
3. Lainsäädäntö ja ohjeet 7
3.1 Perusoikeudet 7
3.2 Tietosuojadirektiivi 8
3.3 Direktiivit yksityisyydestä viestinnässä ja tiedon säilyttämisessä 9
3.4 Tietosuojaan liittyvät kansalliset oikeuspäätökset 9
4. Yksityisyys tiemaksujen yhteydessä 11
4.1 Veloitustekniikoiden kehittyminen 11
4.2 Tiemaksujen arkaluonteisuus 12
4.3 Yksityisyys avoimissa ympäristöissä 14
5. Kokemuksia eri maista 16
5.1 Sveitsi 16
5.2 Itävalta 16
5.3 Saksa 17
5.4 Yhdistyneet kuningaskunnat 18
5.5 Alankomaat 18
6. Yksityisyyden sisällyttäminen arkkitehtuurin suunnitteluun 20
6.1 Henkilötiedon lajit tiemaksujärjestelmissä 20
6.2 Yksityisyyteen kohdistuvat uhat 21
6.3 Toimenpiteet käyttäjän yksityisyyden suojaamiseksi 22
6.4 Veloitusprosessin yksityisyyden suoja 25
6.5 Yksityisyyden suunnitteleminen valvontaprosessiin 28
6.6 Yksityisyyden suojan suunnitteleminen avoimiin palvelumarkkinoihin 30
7. Suositukset 32
7.1 Sofia Memorandumin suositukset koskien tiemaksuja ja yksityisyyttä 32
7.2 Suositukset koskien avoimen palveluympäristön arkkitehtuuria 32
7.3 Johtopäätökset 33
8. Lyhenteet 34
9. Lähteet 35

1. Selvityksen tarkoitus ja kohde

Tämän selvityksen tarkoituksena on tuoda esiin näkökulmia ja suosituksia yksityisyyden huomioonottamiseksi riittävässä määrin mahdollisessa henkilöautoja koskevassa koko tieverkon kattavassa km-maksujärjestelmässä Suomessa. Tässä yhteydessä on tunnistettava tiemaksujärjestelmien erityinen herkkyys liittyen yksityisyyden suojaan ja otettava huomioon, että on vain rajoitetusti käytettävissä kokemuksia tämänkaltaisista järjestelmistä, erityisesti koskien henkilöautoja ja yhdistettynä satelliittipaikannusteknologiaan.

Selvitys selkiyttää ensin käsitteitä: Mitä yksityisyys oikeastaan on? Mitä yksityisiä tietoja on olemassa? Selvitys luo myös katsauksen asiaan liittyvään lainsäädäntöön Euroopassa erityisesti pureutuen asiaan tiemaksujen näkökulmasta. Tämän jälkeen kerrotaan muutaman maan kokemuksista, joista voidaan ottaa oppia, sekä onnistuneista että epäonnistuneista projekteista. Raportin keskeisin osa käsittelee yksityisyyden uhkia, uhkien torjuntamahdollisuuksia sekä erityisesti nk. hyviä suunnittelukäytäntöjä. Näistä johdetaan lopulta joukko suosituksia järjestelmäsuunnittelulle, joissa tietosuoja on otettu huomioon.

2. Periaatteet

2.1 Yksityisyyden käsite

Oikeus yksityisyyteen on käsite, jonka mieltäminen riippuu voimakkaasti kulttuurillisesta taustasta ja johon sosiaalinen, taloudellinen ja teknologinen kehitys ovat vaikuttaneet. Alun perin yksityisyys on nähty suhteessa itsensä paljastamiseen toisille. Tämä kattaa sekä ”oikeuden saada olla rauhassa” että henkilön omaan vartaloon liittyvän yksityisyyden.

Fyysinen yksityisyys voidaan määritellä oikeudella torjua sivullisten tunkeutuminen henkilön omalle alueelle tai arvoasemaan sekä oikeudella fyysiseen koskemattomuuteen. Fyysinen yksityisyys voidaan saavuttaa suojelevilla toimenpiteillä, kuten vaatteita käyttämällä, seinien ja aitojen sisäpuolella asumalla, estämällä ihmisiä ottamasta luvatta kuvia tai videoita, estämällä luvaton tunkeutuminen ja kajoamisen kotiin, autoon tai muuhun omaisuuteen sekä estämällä pääsy henkilön terveyttä koskeviin tietoihin.

Informaatioaikakauden myötä informaatio- tai tietosuoja (information privacy, data privacy) on tullut keskeiseksi yksityisyyteen liittyväksi huoleksi. Näille käsitteille ei ole yleistä, yksiselitteistä määritelmää. Asiayhteydestä riippuen informaatio- ja tietosuojalla voidaan tarkoittaa suojautumista loukkaavan tiedon käsittelyltä, henkilön oikeutta päättää itseään koskevan tiedon käytöstä sekä henkilön yksityisen vaikutuspiirin suojaamista. Yleisesti tietosuojalla tarkoitetaan periaatetta, että kaikilla tulee olla oikeus päättää vapaasti, mitä tietoa haluaa jakaa kenenkin kanssa ja milloin.

Tietojen suojaamisella (data protection) oli alun perin erilainen merkitys kuin nykyään. Sillä tarkoitettiin kirjaimellisesti itse tiedon suojaamista häviämistä, muokkaamista ja varastamista vastaan. Nykyään tietojen suojaamisesta on tullut synonyymi tietosuojan (data privacy) kanssa.

Itse datan suojaamisesta käytetään nykyään termiä informaatioturvallisuus (information security / InfoSec) tai tietoturva (data security). Informaatioturvallisuudella tarkoitetaan informaation suojaamista luvatonta pääsyä, käyttöä, levittämistä, muokkaamista, tarkastelua, tallennusta, vaurioittamista tai tuhoamista vastaan. Informaatioturvallisuus ja tietoturva tällaisenaan eivät ole keskeisiä tässä raportissa, paitsi siltä osin kuin ne liittyvät tietosuojaan (data privacy) ja ennen kaikkea henkilötietojen suojaamiseen.

2.2 Yksityisen tiedon lajeja

Yksityisyysongelmia esiintyy aina, kun kerätään ja varastoidaan tai tallennetaan henkilöihin liittyvää, tunnistettavaa dataa. Henkilökohtaisen tiedon, kuten uskontoon, seksuaaliseen suuntautumiseen, poliittisiin yhteyksiin tai muuhun henkilön toimintaan liittyvän informaation paljastumista vastustetaan useista syistä. Tällaisia voivat ovat esimerkiksi syrjintä, nolostuminen tai henkilön ammatilliselle maineelle aiheutuva vahinko. Monentyyppiseen henkilökohtaiseen informaatioon liittyy siis yksityisyysongelmia.

Esimerkkejä:

Poliittinen yksityisyys on ollut huolenaihe äänestysjärjestelmien kehittymisestä lähtien ja sitä pidetään kansalaisen perusoikeutena. Äänestyskoppi ja anonyymi äänestyslipuke mahdollistavat yksityisen ja turvallisen äänestyksen ilman äänestäjään kohdistuvaa painostusmahdollisuutta.

Taloudellinen yksityisyys tarkoittaa henkilön transaktioihin liittyvien tietojen suojelemista. Henkilön ostoksiin liittyvä informaatio paljastaa paljon asioita henkilön vierailemista paikoista, mieltymyksistä, yhteyksistä, tavoista ja henkilön käyttämistä tuotteista, kuten lääkkeistä. Taloudellinen yksityisyys on tärkeää petosten ja identiteettivarkauksien välttämiseksi.

Terveydellinen yksityisyys tarkoittaa henkilön oikeutta salata terveystietonsa ja muu tähän liittyvä informaatio ulkopuolisilta. Terveydellisen informaation paljastuminen voi vaikuttaa henkilön vakuutuksiin, työllisyyteen ja aiheuttaa kiusallisia tilanteita. Terveystiedot voivat myös kertoa paljon henkilön yksityiselämästä, kuten seksuaalisista preferensseistä.

Yksityisyyden suoja internetissä tarkoittaa henkilön oikeutta päättää itse, mitä informaatiota jakaa itsestään verkossa, kenellä on pääsy kyseiseen tietoon ja mihin tarkoitukseen tietoa saa käyttää.
Internetin käyttäjiä saattaa huolettaa tietää, kuinka monet heidän vierailemistaan internetsivuista keräävät, tallentavat ja mahdollisesti jakavat tunnistettavaa tietoa heistä. Vastaavasti sähköpostin käyttäjät yleensä pitävät sähköpostejaan yksityisinä ja olisivat huolestuneita, jos heidän sähköpostejaan luettaisiin, tallennettaisiin ja välitettäisiin kolmansille osapuolille ilman omaa suostumusta.

Paikannustiedon yksityisyys. Mobiililaitteiden paikannusominaisuudet ovat parantuneet huimasti viime aikoina, joten paikannustietoon liittyvästä yksityisyydestä on tullut ajankohtaista. Paikannustieto on kiistatta yksi arkaluonteisimmista tällä hetkellä kerättävistä tiedoista. Henkilön matkapuhelimen sijainnin perusteella voidaan päätellä potentiaalisesti arkaluontoista henkilöön liittyvää informaatiota, kuten kuuluminen tiettyyn kirkkoon tai henkilön käynti motellissa tai aborttiklinikalla. Vastikään julkaistu tutkimus (MIT Location Privacy Study) osoitti, että tieto neljästä päivän aikana vieraillusta paikasta ja ajankohdista riittää yksilöimään jopa 95 % ihmisistä, vaikka tiedon laatu on suhteellisen matala. Siksi karkeakin paikannustieto vie helposti henkilön anonymiteetin.

Paikannustiedon yksityisyys on kriittisen tärkeä osa tätä selvitystä. Paikannustiedon yksityisyys on melko uusi näkökulma tietosuojaan (data privacy) ja on tullut esille vain viimeaikaisen teknologisen kehityksen vuoksi, pääasiassa GSM-verkon matkapuhelinpuhelinpaikannuksen sekä GNSS:n, pääasiassa GPS:n, laajamittaisen käytön vuoksi. Edulliset GNSS -vastaanottimet ovat mahdollistaneet lukuisia uusia sovelluksia ja palveluita. Yleistyminen on ollut suunnattoman nopeaa, erityisesti älypuhelimissa. Käyttäjät nauttivat paikkatietoon perustuvista palveluista, kuten navigoinnista, paikallisista säätiedoista ja uutisista, kohdistetuista joukkoliikenteen

aikatauluista, lähimmän ravintolan tai elokuvateatterin etsimisestä ja paljosta muusta, ilman suurempaa tietoisuutta potentiaalisista yksityisyysseurauksista. Paikannustietoa ei kuitenkaan käytetä ainoastaan kohdennettuun kaupalliseen tietoon ja mainontaan, jonka useimmat ihmiset hyväksyvät pakollisena kiusana. Tiedot paljastavat paljon enemmän ihmisen yksityisestä alueesta, erityisesti yhdistettynä muihin tietolähteisiin ja rekistereihin.

2.3 Käsitteet

Yksityisyydestä ja tietosuojasta puhuttaessa käytetään erityiskäsitteitä. Seuraavat käsitteet ovat Euroopan tietosuojadirektiivin määrittelemiä.

Henkilötiedoilla tarkoitetaan kaikenlaisia tunnistettua tai tunnistettavissa olevaa luonnollista henkilöä ("rekisteröity") koskevia tietoja; tunnistettavissa olevana pidetään henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa, erityisesti henkilönumeron taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.

Rekisteröidyn suostumuksella tarkoitetaan kaikenlaista vapaaehtoista, yksilöityä ja tietoista tahdon ilmaisua, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn.

Henkilötietojen käsittelyllä tarkoitetaan kaikenlaisia sellaisia toimintoja tai toimintojen kokonaisuuksia, joita kohdistetaan henkilötietoihin joko automaattisen tietojenkäsittelyn avulla tai manuaalisesti, kuten tietojen kerääminen, tallentaminen, järjestäminen, säilyttäminen, muokkaaminen tai muuttaminen, tiedon haku, kysely, käyttö, luovuttaminen siirtämällä, levittämällä tai asettamalla muutoin saataville, yhteensovittaminen tai yhdistäminen sekä suojaaminen, poistaminen tai tuhoaminen.

Henkilötietojen käsittelijällä tarkoitetaan luonnollista tai oikeushenkilöä, julkista viranomaista, virastoa tai muuta toimielintä, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.

Rekisterinpitäjällä tarkoitetaan luonnollista tai oikeushenkilöä, julkista viranomaista, virastoa tai muuta toimielintä, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoituksen ja keinot; jos käsittelyn tarkoitus ja keinot määritellään kansallisilla tai yhteisön laeilla tai asetuksilla, rekisterinpitäjä tai erityiset perusteet rekisterinpitäjän nimeämiseksi voidaan vahvistaa kansallisten tai yhteisön säännösten mukaisesti.

Lisäksi edellä mainittuihin ydinkäsitteisiin, seuraavat kaksi toimeenpanoon liittyvää käsitettä ovat keskeisiä (lähde Wikipedia):

Privacy by Design / Data Protection by Design -termillä tarkoitetaan periaatteetta, jossa yksityisyys ja tietosuoja ovat mukana teknologioiden koko elinkaaressa varhaisesta suunnittelutasosta käyttöönottoon, käyttöön ja lopulliseen hävitykseen.

Private Enhancing Technology (PET) on yleinen termi tietokoneohjelmille, sovelluksille ja mekanismeille, jotka integroituna verkossa oleviin palveluihin ja sovelluksiin tai käytettynä yhdessä tällaisten palveluiden kanssa, mahdollistavat käyttäjien suojata palveluille tai sovelluksiin lähetettävästä tiedosta henkilöön viittaavan, tunnistettavan osan.

3. Lainsäädäntö ja ohjeet

3.1 Perusoikeudet

Oikeus henkilötietojen suojaamisesta ihmisen perusoikeutena säädettiin Euroopan talousliiton perustamissopimuksessa vuonna 1957 ja muunnettiin myöhemmin artiklaksi 16 Euroopan Unionin perustamissopimuksessa (TFEU). Samankaltaiset ehdot sisältyivät myös EU:n perusoikeuksien asiakirjaan (ks. artikla 8 EU:n perusoikeuksien asiakirjassa).

Operatiiviset toimenpiteet yksityisyysoikeuden täytäntöönpanosta jätettiin valtioille. Suuren mittakaavan automaattisten tiedonkäsittelyjärjestelmien kehityttyä tarve määritellä henkilötietojen käsittely kyseisissä järjestelmissä tuli kuitenkin ilmeiseksi. OECD toteutti ensimmäisen onnistuneen yrityksen yhdenmukaistaa kansainvälistä yksityisyyslainsäädäntöä. Organisaatio julkaisi vuonna 1980 ohjeistuksen yksityisyyden suojaamisesta ja henkilötietojen liikkumisesta rajojen yli. Tässä dokumentissa säädettiin perusteet henkilötietojen suojaamiseksi seitsemän periaatteen muodossa.

Tiedon keräämisen rajoittaminen: Henkilötietojen keräämisen on oltava rajallista. Rekisterinpitäjän on saatava tiedot laillisilla ja rehellisillä keinoilla. Henkilön on tiedettävä tietojen keräämisestä ja
tarvittaessa annettava siihen suostumuksensa.

Tietojen laatu: Henkilötietojen on oltava käyttötarkoitukseensa nähden asianmukaisia. Näihin tarkoituksiin välttämättömien tietojen on oltava täsmällisiä, täydellisiä ja ajan tasalla.

Käyttötarkoituksen määrittely: Henkilötietojen keräämisen tarkoitukset on määriteltävä etukäteen. Tietojen käyttäminen myöhemmin on rajattava alkuperäisiin tarkoituksiin tai sellaisiin tarkoituksiin, jotka eivät ole yhteen sopimattomia niiden kanssa. Jälkimmäisessä tapauksessa uusi käyttötarkoitus on aina määriteltävä erikseen.

Käytön rajoittaminen: Henkilötietoja ei saa paljastaa, jättää saataville tai käyttää muihin kuin edellisessä kohdassa määriteltyihin tarkoituksiin muutoin kuin rekisteröidyn suostumuksella tai lain valtuuttamana.

Turvallisuuden varmistaminen: Henkilötiedot on suojattava kohtuullisilla turvajärjestelyillä erilaisilta riskeiltä. Tällaisia riskejä ovat tietojen häviäminen, luvaton pääsy tietoihin sekä tietojen tuhoaminen, käyttö, muuttaminen ja luovuttaminen ilman lupaa.

Avoimuus: Henkilötietojen käsittelyssä on noudatettava yleistä avoimuutta. Tietojen rekisteröinnistä, ominaisuuksista, käyttötarkoituksista sekä rekisterinpitäjästä ja sen sijainnista on oltava saatavilla informaatioita.

Yksilön osallistuminen: Yksilölle on taattava oikeus:

- saada tarkastaa rekisterinpitäjältä, onko rekisterissä tietoja hänestä itsestään vai ei
- saada nämä tiedot kohtuullisella viiveellä, hinnalla ja tavalla sekä ymmärrettävässä muodossa
- saada perustelut päätökseen ja mahdollisuus valittaa asiasta, jos rekisterinpitäjä torjuu tietojen tarkastuspyynnön
- kiistää itseään koskevat tiedot ja pyytää rekisterinpitäjää tuhoamaan, korjaamaan, täydentämään tai muuttamaan virheelliset tiedot.

OECD:n ohjeet eivät kuitenkaan ole sitovia. Euroopan neuvosto laati vuonna 1981 “sopimuksen yksilöiden suojaamisesta henkilötietojen automaattisessa käsittelyssä”.

Tämä sopimus velvoitti allekirjoittajia säätämään lain koskien henkilötietojen automaattista käsittelyä. Useat maat toteuttivat tämän.

3.2 Tietosuojadirektiivi

Euroopan komissio ymmärsi, että poikkeava tietosuojalainsäädäntö eri jäsenmaiden välillä haittaisi vapaata tiedonsiirtoa EU:n sisällä ja myöhemmin esitti tietosuojadirektiivin, joka hyväksyttiin vuonna 1995. Direktiivi on otettu käyttöön kansallisissa laeissa EU:n jäsenmaissa. Tämä takaa, että kaikki keskeisimmät elementit ja vaatimukset henkilötietojen suojauksesta ovat samat eri puolilla Eurooppaa.

Tietosuojadirektiivi rakentuu OECD:n yksityisyyden suojauksen seitsemän periaatteen pohjalle. Mikä tärkeintä, se vahvistaa, että henkilötietojen käsittely on sallittua vain rekisteröidyn luvalla tai laillisen velvoitteen / yleisen edun vuoksi. Henkilötietoja ei tule käsitellä ollenkaan, paitsi tiettyjen edellytysten täyttyessä. Nämä edellytykset voidaan jakaa kolmeen ryhmään: avoimuuteen, laillisuuteen ja suhteellisuuteen.

Avoimuusperiaate: Rekisteröidyllä on oikeus saada tietää, kun hänen henkilötietojaan käsitellään. Rekisterinpitäjän on ilmoitettava oma nimensä ja osoitteensa, käsittelyn tarkoitus, tietojen vastaanottajat sekä kaikki muut tiedot, joita asianmukaisen käsittelyn varmistaminen edellyttää.

Tietoja voidaan käsitellä vain seuraavissa tapauksissa:
- jos rekisteröity on yksiselitteisesti antanut suostumuksensa
- jos käsittely on tarpeen käyttäjäsopimuksen solmimiseksi tai sen täytäntöön panemiseksi
- jos käsittely on tarpeen laillisen velvoitteen noudattamiseksi
- jos käsittely on tarpeen rekisteröidyn keskeisen edun suojaamiseksi

Laillisuuden periaate: Henkilötietojen käsittelyn on tapahduttava tiettyä nimenomaista ja laillista tarkoitusta varten, eikä tietoja myöhemmin saa käsitellä näiden tarkoitusten kanssa yhteensopimattomalla tavalla.

Suhteellisuusperiaate: Käsiteltyjen tietojen on oltava asianmukaisia, olennaisia eikä liian laajoja siihen tarkoitukseen, mihin ne on kerätty ja/tai missä niitä myöhemmin käsitellään. Tietojen on oltava paikkansapitäviä ja ne on pidettävä ajan tasalla. On toteutettava kaikki aiheelliset toimenpiteet sen varmistamiseksi, että tietokannasta poistetaan tai siinä oikaistaan tiedot, jotka ovat virheellisiä tai puutteellisia niihin tarkoituksiin nähden, joita varten ne kerättiin tai joita varten niitä käsitellään. Henkilötietoja voidaan säilyttää muodossa, josta rekisteröidyt ovat tunnistettavissa, ainoastaan sen ajan, mikä on tarpeen niihin tarkoituksiin, joihin tiedot on kerätty tai joita varten niitä käsiteltiin.

Kunkin jäsenvaltion tulee asettaa valvontaviranomainen seuraamaan tietosuojan tasoa jäsenvaltiossa. Valvontaviranomainen neuvoo hallitusta lainsäädännöllisissä ja hallinnollisissa toimenpiteissä sekä käynnistää oikeustoimet, mikäli tietosuojasäädöstä on rikottu. Rekisterinpitäjän tulee ilmoittaa valvontaviranomaiselle ennen kuin aloittaa tiedonkäsittelyn. Suomessa tämä valvontaviranomainen on Tietosuojavaltuutetun toimisto.

Direktiivin artikla 29 on perustanut tietosuojatyöryhmän. Työryhmä neuvoo tietosuojan tasosta yhteisössä ja kolmansissa maissa.

Uusi tietosuojasäädös on esitelty tammikuussa 2012. Laajojen nykyistä tietosuojadirektiiviä koskevien neuvotteluiden jälkeen EY teki johtopäätöksen, että vaikka nykyisen direktiivin päämäärät ja periaatteet ovat tyydyttäviä, ovat henkilötietosuojan toimeenpanon käytännöt hajanaisia eri puolilla unionia. Ehdotettu uusi lainsäädäntö ei

siksi muuta päämääriä tai periaatteita, mutta pyrkii poistamaan nykyisten menettelyjen epäjohdonmukaisuudet ja tehottomuudet tietosuojan toteutuksen suhteen. Uuden lain keskeiset päämäärät ovat:

- selkeyttää järjestelmien operoijia ja kansalaisia koskevia lakipykäliä
- yhdenmukaistaa henkilötietosuojan valvontaa Euroopan unionissa
- vahvistaa kuluttajien luottamusta verkossa oleviin palveluihin

Uusi säädös poistaisi myös hallinnollisia vaatimuksia. Säädöksen tarkoitus on keskittää resursseja suuri-riskisiin tiedonkäsittelytilanteisiin ja helpottaa tavanomaisia, matalariskisiä tilanteita. Säädös poistaa nykyisen direktiivin ilmoitusvelvollisuuden (artiklat 18 ja 19). Etukäteisvaltuutus on edelleen tarpeen, jos operoija ei sovella standardoituja sopimusehtoja tai laillisesti pitäviä varmuustoimia, kun on kyse henkilötietojen välittämisestä kolmansiin maihin tai kansainväliselle organisaatiolle. Säädös ulottaisi EU:n tietosuojalain myös kaikkiin ulkomaisiin yrityksiin, jotka käsittelevät Euroopan unionin kansalaisten tietoja.

Vuoden 2013 lopussa säädöksen lainsäädäntöprosessi on vielä kesken.

3.3 Direktiivit yksityisyydestä viestinnässä ja tiedon säilyttämisessä

Direktiivi 2002/58/EC henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (sähköisen viestinnän tietosuojadirektiivi) käsittelee sähköisen viestinnän yksityisyyttä ja sitä voidaan pitää erikoistuneempana kehitelmänä tietosuojadirektiivistä 95/46/EC. Direktiivi 2002/58/EC sisältää ehdot verkkojen ja palveluiden turvallisuuteen, viestinnän salassapitoon, päätelaitteilla säilytettävään tietoon pääsyyn, liikenne- ja paikannustiedon käsittelyyn, kutsuvan tilaajan tunnistukseen, tilaajaluetteloihin sekä ei-toivottuun kaupalliseen viestintään. Direktiivi liittyy liikennetelematiikan sovelluksiin erityisesti käytettäessä matkapuhelinverkkoa paikannukseen.

Direktiivi tiedon säilyttämisestä muuttaa sähköisen viestinnän tietosuojadirektiiviä. Direktiivin mukaan jäsenvaltioiden tulee säätää laki, joka velvoittaa puhelinoperaattoreita ja internetpalvelujen tarjoajia säilyttämään kansalaisten tietoliikennetiedot 6 - 24 kuukauteen. Direktiivin mukaan poliisi ja turvallisuusviranomaiset voivat pyytää pääsyä tietoihin, kuten IP-osoitteisiin ja ajankohtaan kustakin lähetetystä tai vastaanotetusta sähköpostista, puhelusta tai tekstiviestistä. Lupa informaatioon pääsyyn voidaan myöntää vain tuomioistuinkäsittelyssä.

3.4 Tietosuojaan liittyvät kansalliset oikeuspäätökset

Keoliksen tapauksessa (Keolis Case) useat käyttäjät jättivät valituksen Ranskan tietosuojaviranomaiselle koskien anonyymia joukkoliikennelippua ”Korrigoa” Rennesin kaupungissa. Tietosuojaviranomainen määräsi seuraavat epäkohdat korjattaviksi: Anonyymi lippu oli 2.5 – 4 kertaa verrannollista personoitua lippua kalliimpi. Anonyymejä lippuja tarjottiin vain yksittäisille matkoille (kausilippuja ei tarjolla). Anonyymien lippujen käyttömahdollisuuksista oli tarjolla vain vähän tietoa.

Tapaus toimii esimerkkinä ja vahvistuksena periaatteelle, että yksityisyys on luonnollisten henkilöiden perusoikeus. Niin pitkään kuin on järkevästi mahdollista, palvelun anonyymistä käytöstä ei tule pyytää korkeampaa hintaa, eikä palvelusta tule tehdä asiakkaalle epämiellyttävää heikommalla toimivuudella tai saatavuudella.

TomTomin tapauksessa (TomTom Case) Hollannissa kansallinen tietosuojan valvontaviranomainen tutki TomTomin keräämän yksityishenkilöiden navigaattoreiden reaaliaikaisen ja historiallisen paikannustiedon käsittelyä. Tutkinnan tuloksena todettiin, että TomTom rikkoi yksityisyyslainsäädäntöä ja yhtiön tuli korjata toimintatapansa.

Havaittu rikkomus koski puutteellista informaatiota koskien TomTomin keräämää historiallista paikannustietoa ja puutteita rekisteröidyiltä pyydetyissä suostumuksissa koskien paikannustiedon käsittelyä. Vaikka TomTom ilmoittaa tietosuojalausunnossaan, mitä tietoa kerätään ja mihin tarkoitukseen, ei tätä voida valvontaviranomaisen mukaan pitää rekisteröidyn suostumuksena.
Tarkasteltaessa TomTomin tapaa käsitellä paikkatietoa tehdään kiinnostava huomio. Tietosuojan valvontaviranomainen arvosti TomTomin tapaa poistaa tiettyyn käyttäjään viittaavat tunnisteet tallennettavasta tiedosta ja yritys on nähnyt vaivaa välttääkseen mahdollisuuden yhdistää tietoja kehenkään käyttäjään. Valvontaviranomainen katsoi kuitenkin, että tietoja oli mahdollista joissakin tapauksissa kohdistaa suurella todennäköisyydellä tiettyihin henkilöihin esimerkiksi vertaamalla paikkatietoja muuhun informaatioon. Siksi anonyymiksi tehtyjä paikkatietoja tulee pitää henkilötietoina ja rekisteröidyn suostumus tietojen käsittelyyn vaaditaan.

4. Yksityisyys tiemaksujen yhteydessä

4.1 Veloitustekniikoiden kehittyminen

Ensimmäiset yhden kaistan sähköiset maksunperintäjärjestelmät esiteltiin 1980-luvulla. Tekniikka mahdollisti autoilijoiden ajaa maksuasemien läpi pysähtymättä, vaikkakin alennetulla nopeudella ja automaattisesti ohjautuva puomi sääteli yhä maksulliselle tieosuudelle pääsyä. Radiotaajuisen etätunnistuksen (RFID), lyhyen kantaman tiedonsiirtotekniikoiden (DSRC) sekä automaattisen rekisterikilven tunnistuksen (ANPR) kehitykset ovat mahdollistaneet vapaan liikennevirran sähköiset maksunperintäjärjestelmät (EFC). Ajoneuvot voivat kulkea maksullisen tieosuuden läpi pysähtymättä edellyttäen, että ne on varustettu tunnisteella, jossa on voimassaoleva sopimus. Sisäänajo- ja poistumispisteillä tai tieosuuden keskellä sijaitsevat tienvarsijärjestelmät lukevat tunnisteeseen tallennetun sopimustunnisteen ja tallentavat informaation, joka sisältää paikan, päivämäärän ja kellonajan ja joskus ajoneuvon luokkatiedon käyttäjän laskuttamiseksi tai maksun vähentämiseksi käyttäjän pre-paid -tililtä.

Euroopassa vapaan liikennevirran EFC on otettu käyttöön useissa maissa raskaiden ajoneuvojen tiemaksujen perintään koko päätieverkolla. Tietosuojan näkökulmasta askel sekalaisista manuaali-elektronisista tekniikoista täysin elektroniseen oli merkittävä muutos, sillä vaihtoehtoa maksullisen tien anonyymille käytölle ei enää tarjota.

Viimeisen vuosikymmenen aikana nousi esiin uusi lähestymistapa, itsenäisiin ajoneuvolaitteisiin (OBE) perustuva tienkäyttömaksu. Tässä konseptissa ei tarvita tienvarsi-infrastruktuuria rekisteröimään tunnisteita tai havainnoimaan ajoneuvoja, sillä ajoneuvolaitteet keräävät itse maksun laskemiseen tarvittavan tiedon. Laite käyttää GNSS –tekniikkaa (tavanomaisesti GPS) paikannukseen ja matkapuhelinverkkoa tienkäyttötiedon lähettämiseen keskukselle. Esimerkkeinä tällaisista järjestelmistä toimivat raskaiden ajoneuvojen tietullijärjestelmät Saksassa ja Slovakiassa.

Vapaan liikennevirran maksunperintäjärjestelmien (EFC) edut ovat ilmeiset. Tienkäyttäjälle ei aiheudu ylimääräistä viivettä maksulliselle tieverkolle pääsystä, tilaa vieville maksuasemille ei ole tarvetta ja järjestelmän operointikustannukset tienkäyttömaksujen kerääjälle ovat yleensä huomattavasti alhaisemmat.
EFC:n haittapuoli on, että järjestelmä ilman käteismaksumahdollisuutta kerää tietoa, joka on yleensä jäljitettävissä ajoneuvon omistajaan tai käyttäjään ja sisältää informaatiota hänen liikkeistään (aika ja paikka). Riippuen maksullisen tieverkon laajuudesta ja veloituskonseptista, voidaan kyseisestä informaatiosta muodostaa liikkumismalleja. Monet kokevat tällaiset tiedot arkaluonteisiksi. On havaittu, että ammattiliikenteen (raskaan tavaraliikenteen) keskuudessa tällaista yksityisyyskysymystä ei yleensä nähdä ongelmaksi.

Monissa maissa on selvitetään tai on selvitetty, joissain maissa myös suunniteltu vakavasti, tienkäyttömaksuja, jotka perustuvat henkilöautojen liikennesuoritteeseen päätieverkolla tai koko tieverkolla (Hollanti, Tanska, Belgia, Slovenia, Yhdysvallat). Etäisyysperusteinen maksujärjestelmä laajennetulla tieverkolla nähdään yleisesti oikeudenmukaisempana kustannustenjakona kuin yleinen aikaperusteinen tai kiinteä maksu ja se on potentiaalisesti tehokas väline ruuhkautumisen ja ajoneuvon käytön aiheuttamien haitallisten ympäristövaikutusten vähentämiseksi. Kyseisten konseptien toteuttaminen on kuitenkin osoittautunut vaikeaksi sekä teknisten, lainsäädännöllisten että poliittisten vaikeuksien vuoksi. Tienkäyttäjien yksityisyydensuoja on jatkuvasti merkittävä asia. Niin pitkään kuin kuljettajat näkevät sähköiset maksunperintäjärjestelmät viranomaisten keinona seurata heidän yksityiselämäänsä entistä enemmän, on järjestelmille vaikea saada julkista yleistä tukea. Asenteiden muuttamiseksi tienkäyttäjät täytyisi saada vakuuttumaan, että heidän ei tarvitse pelätä “big brother” -tyylistä seurantaa heidän jokaisesta liikkeestään.

Tähän asti veloitusjärjestelmät ovat olleet täysin kansallisessa hallinnassa, oli tienkäyttömaksujen kerääjä sitten julkinen tai yksityinen taho. Maksuja keräävät yritykset ovat olleet yhteen toimintaan erikoistuvia yrityksiä, joissa tiemaksut ovat olleet ainoa liikennetoiminta. Tämä on muuttumassa kahdesta syystä:

Yhteentoimivuus kansallisten järjestelmien välillä on noussut tärkeäksi tekijäksi. Yhteentoimivuusdirektiivi 2004/52/EC ja tähän liittyvä EETS-päätös 2009/750/EC edellyttävät, että sähköiset maksunperintäjärjestelmät tulevat yhteensopiviksi koko Euroopassa, jotta yhdellä ajoneuvolaitteella (OBE) ja yhdellä sopimuksella voidaan käyttää kaikkia järjestelmiä. Tätä varten tulee luoda avoimet markkinat palveluntarjoajille. Siten järjestelmän hallinta tulee tulevaisuudesta siirtymään yksittäisiltä kansallisilta tahoilta kansainväliseen palveluntarjoajajärjestelyyn, jossa ei ole lähes ollenkaan keskushallintoa.

Myös kansalliset liikennetelematiikkapalveluiden markkinat avautuvat. Monissa maissa suunnitellaan konseptia, jossa kustannukset ja tiemaksujärjestelmän rakentaminen sekä siihen sisältyvät riskit jaetaan useiden yksityisen sektorin toimijoiden kesken. Toiveena on, että sähköisten maksunperintäjärjestelmien laajentumista kaikkiin kevyisiin ajoneuvoihin kannustetaan sallimalla yksityisten toimijoiden tarjota tiemaksujen kerääminen yhtenä palveluna muiden joukossa, kuten ”maksa-kuten-ajat ” -vakuutusten, pysäköintiopastuksen ja muiden lisäarvoa tuottavien palveluiden joukossa.

Tämä kehitys, joka ei koske vain teknologiakonsepteja vaan myös liiketoimintamallin laajentamista pelkästä EFC:stä laajempiin liikennetelematiikan sovelluksiin, on tehnyt tietosuojakysymyksistä ja tiedon arkaluontoisuudesta yhä suuremman asian viime vuosina. Kerätyn tiedon arkaluontoisuutta ja modernin monipalveluliiketoimintaympäristön vaikutuksia tarkastellaan tarkemmin kahdessa seuraavassa kappaleessa.

4.2 Tiemaksujen arkaluonteisuus

Kansainvälinen telekommunikaatiokysymysten tietosuojaryhmä, IWGDPT, on kansainvälisen tietosuojavaltuutettujen konferenssin komitea. Ryhmä on vuodesta 1983 lähtien hyväksynyt lukuisia suosituksia (yhteiset kannat ja työversiot), jotka tähtäävät telekommunikaation yksityisyyden parantamiseen. Ryhmän jäseniin kuuluu edustajia tietosuojavaltuutetuista ja muista kansallisista hallintoelimistä, kansainvälisistä organisaatioista ja tiedemiehistä eri puolilta maailmaa.

Maaliskuussa 2009 IWGDPT hyväksyi tärkeän johdatusraportin tiemaksuihin, (Sofia Memorandum). Se toteaa tietojen arkaluontoisuudesta: “Syy miksi tiemaksut ovat niin tunteita herättävä asia on se, että ne tuovat yhteen paikkatiedon, tunnistettavan henkilödatan ja veloitustiedot: toisin sanoen, ne tietävät, kuka oli missä ja milloin, ja laskuttaa heitä siitä. “Pay as you go” -periaatteen (ja yhteentoimivan järjestelmän) mahdollistamiseksi vapaassa liikennevirrassa on selvää, että tällaiset tiemaksujärjestelmät voivat tuoda mukanaan suuren määrän yksilöiden liikkumisen valvontaa (sekä ajoneuvojen omistajien että kuljettajien). Siksi vaikutukset asianomaisten yksityisyyteen tulee selvittää huolellisesti. Ei ole vaikea kuvitella, kuinka arvokas tietokanta kuljettajien liikkumistiedoista ja muista oheistiedoista olisi. Tietoja voitaisiin kuvitella käytettävän hyväksi monin tavoin aivan eri tarkoituksiin, kuin mihin ne alun perin oli kerätty (tienkäyttömaksuihin). Yksityisyyden suojaan liittyviä väärinkäsityksiä pidetään usein tärkeimpinä esteinä laajojen tiemaksujärjestelmien toteuttamiselle.

Sofia Memorandum tuo esiin myös kaksi yleistä yksityisyyttä koskevaa väärinymmärrystä, jotka tulee vankasti oikaista. Ensiksi, työryhmä korostaa “ei ole huolta että GPS-pohjaiset ratkaisut tarkoittaisivat suuren kaiken kattavan

tietokannan rakentamista ajoneuvojen sijainneista “big brother taivaalla” -tyyliin. On todellakin yleinen väärinkäsitys, että GNSS-järjestelmien satelliitit tietäisivät, missä henkilö tai ajoneuvo on. Todellisuudessa GNSS-satelliitit lähettävät vain tietyn aikainformaation ajoneuvossa oleville vastaanottimille. Tämän perusteella vastaanottimet laskevat oman sijaintinsa, mitä satelliitit eivät voi tietää. Vastaanottimilla ei edes ole teknistä mahdollisuutta lähettää informaatiota takaisin satelliiteille. Tulee kuitenkin huomata, että – riippuen järjestelmän konseptista – käytettäessä ajoneuvolaitetta (OBE) tienkäyttömaksuihin laite lähettää enemmän tai vähemmän yksityiskohtaista sijainti- ja reittitietoa veloituskeskukseen tai muuhun tukitoimintoon langattoman verkon (yleensä GSM) kautta.

Toiseksi, Sofia Memorandumissa todetaan, että “vertailua tehdään usein mobiilien puhelinpalveluiden ja luottokorttien kanssa, joissa yksityisiä tietoja jäljitetään tai voidaan jäljittää. Työryhmä korostaa, että sellaiset yksioikoiset vertailut eivät ole asianmukaisia, ensinnäkin koska tiemaksulaitteiden tulee olla jatkuvassa operoinnissa (ainakin maksullisilla teillä), toisin kuin matkapuhelimien tapauksessa, jossa käyttö on täysin vapaaehtoista. Mahdollisuus kytkeä laite pois päältä maksullisilla teillä johtaisi maksujen kiertoon, ja siksi tiemaksuhankkeiden yksityisyysasiat ovat tulleet sitäkin olennaisemmiksi.

Sofia Memorandum korostaa oikeaoppisesti, että tienkäyttömaksujen herkkä luonne yksityisyydestä puhuttaessa johtuu paljolti sen luonteesta veloittaa käyttäjää tietämällä, missä kukin oli ja mihin aikaan. Siten yksi ajatus parantaa käyttäjän yksityisyyttä olisi tehdä veloituksesta anonyymiä. Kuten tässä raportissa myöhemmin todetaan, anonymiteettiä veloituksessa ei ole helppoa saavuttaa, etenkin kun kyseessä ovat kevyet ajoneuvot. Vaikka kuljettajan identiteetti yritettäisiin peittää, jo tietyn auton tunnistus tietyssä paikassa rekisteritunnuksen perusteella rikkoo anonymiteetin useimmissa tapauksissa, koska henkilöautoissa – nimensä mukaisesti - auton yksilöinti riittää usein tietoon kuljettajasta. Jos asioita halutaan vielä mutkistaa, eikä haluta tiedettävän autoa eikä kuljettajaa, niin silti jo minimaalinenkin tieto kuljetuista reiteistä riittää poistamaan anonymiteetin.

Kuten MIT:n tietosuojatutkimuksessa todettiin edellisessä luvussa ja kuten TomTomin oikeustapauksessa korostettiin, jo tietämällä tiettyjä yksityiskohtia päivittäisestä liikkumisesta henkilö voidaan tunnistaa. Yksityiskohtaisempi liikkumismalli puolestaan sivuaa myös terveydellistä yksityisyyttä (vierailut lääkärille, sairaalaan, aborttiklinikoille) ja siitä voidaan tehdä päätelmiä henkilön poliittisesta suuntautumisesta (vierailut poliittisiin kokoontumisiin, ammattiliiton tapaamisiin, kansalaisjärjestöjen toimistoihin), seksuaalisista tavoista (vierailut bordelleihin, klubeille, elokuvateattereihin) ja monista muita tiettyihin paikkoihin kytköksissä olevista aktiviteeteistä. Jopa alkoholi- ja peliriippuvuus voidaan päätellä karkeista liikkumismalleista.

Ymmärrys paikannustiedon yksityisyydestä on vielä lapsenkengissä ja suuren yleisön tietoisuus on vielä matalalla tasolla. Tulee myös huomioida, että “yksityisyys” ei tarkoita vain suojautumista tiedon väärinkäytöltä asianomaisen (rekisteröidyn) etujen vastaisesti, vaan myös paljon vahvempaa konseptia liittyen henkilön oikeuteen intiimisyyteen ja itseä koskevan tiedon hallintaan. Tunnustaen teknologisen kehityksen nopeus ja ennen kaikkea voima yhdistää toisiinsa liittymättömät tiedonkappaleet toisiinsa, joka nykyään tunnetaan käsitteenä “big data”, on erittäin suositeltavaa olla todella konservatiivinen ja suojeleva koskien yksilön oikeuksia.

”Big data” on nouseva teknologia, joka kiitos IT-alan viimeaikaisen edistyksen käsittelykapasiteetissa, tiedon säilytyksessä ja ohjelmistoteknologiassa sallii analysoida ja yhdistää erillisistä lähteistä ennennäkemättömän kokoisia tietopaketteja toisiinsa. Maailmanlaajuinen datan määrä kaksinkertaistuu joka toinen vuosi. Tämä johtuu lähinnä automaattisesta tiedonkeruusta, esimerkiksi tietoliikenneyhteyksistä, verkon lokitiedoista, myyntikirjanpidosta, tilisiirroista, energiamittareista,

geneettisistä analyyseistä jne. Vaikka useimpien käyttötarkoitusten ei pitäisi heikentää käyttäjien anonymiteettiä, on näin kuitenkin houkutus tapahtua, sillä kaupalliset edut olisivat suuret kohdennetussa markkinoinnissa, lainanannon riskienhallinnassa, käyttäjän terveysarvioissa ja työsuhdetiedoissa, mutta myös kriisien hallinnassa ja terrorisminvastaisessa taistelussa. Liikkumistiedot ovat haluttuja tässä yhteydessä, sillä liikkumismallit kertovat paljon ihmisestä nykyajan mobiilissa yhteiskunnassa, kuten yllä tuli ilmi, esim. tiedot työtavoista, taloudellisesta tilanteesta, terveystilanteesta jne.

Näistä syistä tiemaksujen yhteydessä on suositeltavaa ottaa hyvin varovainen asenne koskien paikannustietoa. Jopa näennäisesti anonyymi tieto voidaan melko helposti yhdistää tiettyyn henkilöön yhdistettynä muualta saatavaan erilliseltä vaikuttavaan tietoon. Tähän liittyviä riskejä ei täysin ymmärretä ja siksi konservatiivinen ja suojeleva lähestymistapa on paras suojamuuri. Tietoturvallisuusasiat nähdään usein harmina projekteissa. Monet asiantuntijat ja myös raportin laatijat ovat havainneet, että kun älyliikenteen hankkeiden yhteydessä otetaan puheeksi tietoturvallisuusasiat, keskustelu vaiennetaan pikaisesti ja asian esille ottajan on riski leimautua “tietoaktivistiksi”. Luultavasti tämä havainto pitäisi nähdä merkkinä siitä, että aiheesta on vähän ymmärrystä ja se yritetään jättää huomioitta, luultavasti (tarpeettomien) vaikeuksien välttämiseksi. Tässä selvityksessä pyritään tuomaan esiin tiemaksujärjestelmille suunnitteluvaihtoehtoja, joissa yksityisyysnäkökohdat on otettu tarkasti huomioon ilman järjestelmän kohtuutonta raskauttamista.

4.3 Yksityisyys avoimissa ympäristöissä

Kuluttajat haluavat hyviä tuotteita ja palveluita edullisesti. Tämä toteutuu vain kilpailun avulla avoimilla markkinoilla. Avoimet markkinat takaavat jatkuvan kehityksen ja hintapaineen. Tästä syystä toimialoja, jotka aiemmin on mielletty valtion monopoleiksi, ollaan avaamassa, esimerkkeinä telekommunikaatio, joukkoliikenne, terveyspalvelut ja energiahuolto.

Myös liikennetelematiikan alalla tulisi olla yhteistyötä yksityisen ja julkisen sektorin välillä. Lisäksi ajatusmallit ovat muuttuneet ja tuotteita ei enää toimiteta erillisinä laitteina tai “laatikoina” vaan palvelukonseptina. Käyttäjä ei enää osta yhden käyttötarkoituksen laitetta, kuten radiota, puhelinta tai navigaattoria, vaan tilaa palveluita. Tämä nähdään parhaiten älypuhelinmarkkinoilla: Käyttöjärjestelmien avoimet ympäristöt ovat laukaisseet kehityksen ja markkinoinnin miljoonille sovelluksille, jotka tarjoavat monenlaisia palveluita yhdessä laitteessa (viestintä, internet, mediasoitin, paikallissääennuste, pankkipalvelut, uutiset, aikataulut, hintatiedot, pelit, lipunmyynti ym.). Tässä kuluttaja todella nauttii päivittäisestä kehityksestä ja hintakilpailusta. Edellytys tällaiselle kilpaillulle ympäristölle on avoimuus, toisin sanoen avoimet määrittelyt, rajapinnat ja mukaanpääsy.

Tässä uudessa ajatusmallissa tiemaksut tai EFC toimitettaisiin yhtenä palveluna monien muiden joukossa avoimessa laitteistossa ja ohjelmistoalustoilla. Tämä kehitys tuo mukanaan uusia riskejä. Esimerkkinä, miten voidaan välttää, että arkaluontoinen tienkäyttömaksutieto, toisin sanoen yksityiskohtainen tieto henkilön tietyn päivän reitistä, siirtyy vakuutusyhtiön maksa-kuten-ajat -sovellukseen samalla teknisellä alustalla? Vakuutuksenantaja on varmasti kiinnostunut käyttäjän liikkumisesta, ei vain koskien yksin ajoneuvon vakuutusta, vaan myös yleiseen riskinarviointiin käyttäjän sairausvakuutuksen tai henkivakuutuksen avulla.

Vaikuttaa lähes mahdottomalta suojata datan liikkumista sovellusten välillä samalla alustalla. Vaikka EFC -ohjelmisto testattaisiin ja sertifioitaisiin yksityisen tiukimpia tietosuojasääntöjä noudattavan laboratorion toimesta, jo seuraava ohjelmistopäivitys muuttaisi tilanteen täysin.

Keskustelu useiden palveluntarjoajien avoimen ympäristön riskeistä ei tarkoita, että sellaista ympäristöä tulisi välttää. Päinvastoin, tiettyjä ehtoja, joiden yksityiskohtiin palataan myöhemmin, noudattamalla avoimet ympäristöt takaavat parhaan läpinäkyvyyden tiedon käsittelyyn ja antavat käyttäjälle parhaan mahdollisuuden vaikuttaa itseään koskevaan tietojalanjälkeen.

Tienkäyttömaksujen kohdalla valinta avoimen palveluympäristön puolesta on joka tapauksessa jo tehty. EETS -direktiivi edellyttää sellaista ympäristöä lain nojalla. Eräs toinen hankaluus EETS:ssä on, että palveluntarjoajat tulevat olemaan kansainvälisiä. Tämä tulee johtamaan tilanteeseen, jossa kansallisia veroja kerää ulkomainen yritys. Tällöin kansallisella viranomaisella on vain vähän mahdollisuuksia valvoa tarkkaan palvelun luonnetta. Lisäksi EETS:ssä palveluntarjoajat eivät ole minkään kansallisen viranomaisen hyväksymiä. Kaikki prosessit pohjautuvat palveluntarjoajien ja niiden laitetoimittajien itse-sertifiointiin. Operointivaiheessa on vähän mahdollisuuksia vaikutta tietovirtaan.

5. Kokemuksia eri maista

Viime vuosina on useassa maassa toteutettu laajoja tiemaksujärjestelmiä, mutta vain raskaalle liikenteelle. Kaikki yritykset toteuttaa valtakunnanlaajuisia tiemaksujärjestelmiä henkilöautoille ovat epäonnistuneet. Mutta sekä toteutetuista raskaan liikenteen maksuhankkeista että henkilöautomaksuja kohdanneista epäonnistumisista voidaan saada paljon hyödyllisiä oppeja.

5.1 Sveitsi

Maailman ensimmäinen koko tieverkon kattava ajosuoriteperusteinen maksujärjestelmä LSVA toteutettiin Sveitsissä v. 2001 raskaalle liikenteelle. Kaikkien ajoneuvojen, joiden paino on yli 3,5 tonnia, tulee maksaa jokaisesta ajetusta kilometristä millä tahansa tiellä maan alueella. Yksityisyyden suoja ei esittänyt suurta roolia toteutuksessa. Hankkeessa verotuskohteeksi katsottiin ajoneuvo ja maksuvelvolliseksi ajoneuvon omistaja. Järjestelmässä rekisteröidään ajoneuvo ja omistaja. Kuljettajalla ei ole mitään osuutta asiassa eikä hänen henkilöllisyyttänsä saada tietoon, paitsi esimerkiksi valvontatapauksissa.

Tämän lisäksi LSVA:n ajoneuvolaite (OBU) ei tallenna matkareittiä, vaan ainoastaan ajosuoritteen ilman erittelyjä missä suorite syntyy. Ajoneuvolaitteessa on tosin GPS -vastaanotin, mutta sitä käytetään lähinnä vain varmistamaan, että suoritetieto, joka otetaan ajopiirturista, on oikea. Ajoneuvolaitteeseen tallentuu paikkatietoja vain erityistapauksissa, kuten valtakunnanrajan ylityspisteissä tai kohdissa, joissa tiettyjä virheitä saattaa syntyä.

Sveitsiläiset ovat keskimäärin aika levollisia niin kauan kuin valtio hallitsee järjestelmää. Saattaa olla niin, että kiitos maassa noudatetun suorademokratian kansalaiset katsovat, että he ovat valtio ja he luottavat yleensä viranomaisiin.

Jälkiviisautena voidaan todeta, että on ollut varsin otollista, ettei LSVA -järjestelmässä sovellettu paikkasidonnaista tariffia esim. tietyypin tai alueen mukaan. Yksityisyyden suoja on ollut esillä vain yhdenlaisessa tilanteessa, kun ajoneuvo vaihtaa omistajaa. Vanha omistaja ei halua, että ajoneuvolaitteessa säilytettäviä laskutustietoja missään olosuhteissa siirtyy toiselle kilpailevalle yritykselle oston seurauksena. Tämän välttämiseksi edellinen omistaja voi poistaa kaikki tiedot ajoneuvolaitteesta, tai itse asiassa tiedot kryptataan, jotta ne olisivat edelleen tallessa mahdollisia myöhempiä viranomaistarkastuksia varten.

5.2 Itävalta

Kuten Sveitsissä, Itävallassakaan ei ole koko maan kattavia maksuja henkilöautoille. Käytössä on moottoritievinjetti paperilipun muodossa, joka ei aiheuta ongelmia yksityisyyteen nähden. Joillakin erityisillä tieosuuksilla, kuten alppiteillä tai tunneleissa, on tiemaksuja myös henkilöautoille. Nämä maksetaan paikan päällä tavanomaisin maksuvälinein. Ajoneuvolaite ei ole käytössä eikä mitään reittitietoja tallenneta. Vuonna 2004 otettiin käyttöön maanlaajuinen tiemaksu raskaille ajoneuvoille moottoriteillä. Teknisenä ratkaisuna on DSRC (mikroaaltolaite). Jokaisella moottoritieosuudella on ajoneuvolaitteiden tunnistuslaitteet portaalissa tien yläpuolella.

Ajoneuvolaite on periaatteessa tunnistuslaite, joka kommunikoi DSRC tienvarsilaitteelle tunnistetietonsa kuten sopimuksen tunnus, ajoneuvon rekisterinumero sekä joukon ajoneuvoluokan luokittelutietoja kuten akselimäärä. Kaikki nämä tiedot toimitetaan keskusjärjestelmään. Kuten Sveitsissä, kuljettajan henkilöllisyys jää periaatteessa avoimeksi. Tästä huolimatta yksityisyysasia nousi järjestelmän jo toimiessa esille odottamattomasta syystä: Moottoritieyhtiö tarjosi kuljetusliikkeille web-palvelun, josta yhtiö pystyi keräämään yksityiskohtaisia tietoja omien ajoneuvojensa reiteistä. Tiedot tallentuivat palveluun pian tievarsilaitteen ohituksen jälkeen. Tämä tarkoitti, että

kuljetusliikkeet pystyivät seuraamaan ajoneuvojensa ja käytännössä kuljettajiensa liikkeitä lähes tosiajassa. He pystyivät seuraamaan, miten kuljettajat ottivat matkan aikana taukoja WC:ssä käyntiä, lounasta ym. varten. Asiasta seurasi kovat riidat kuljettajien ja ammattiliittojen kanssa.

Liikennöitsijöiden mielestä heillä oli täysi oikeus seurata, miten heidän arvokkaat ajoneuvonsa lasteineen liikkuivat tieverkolla. Kuljetusliikehän vastaa ajoneuvon hankinnasta, käyttökuluista, kuljettajan palkasta ja myös tietulleista. Kuljettaja ei päätä, missä tai milloin hän ajaa. Kuljettajat katsoivat, ettei heitä saisi koko ajan seurata. Vireillä oli jo oikeustapauksia, jossa pyrittiin kieltämään tietojen keräämistä siitä, kuinka usein kuljettajat kävivät ja kuinka pitkään he viipyivät WC:ssä. Kuljettajat katsoivat, että web-palvelu loukkasi heidän yksityisyyttään. Moottoritieyhtiö päättikin tarjota kyseiset tiedot vasta viiveen jälkeen.

On todettava, että vastaava konflikti nousee esiin useissa kaupallisen liikenteen ITS -sovelluksissa: yrityksen tarve seurat ajoneuvojensa toimintaa vs. kuljettajan oikeus tietynlaiseen yksityisyyteen ja vapauteen. Tämä koskee kaikkia kalustonhallintasovelluksia eikä se ole helposti ratkaistavissa. Lopullinen ratkaisu ei voi perustua kuljettajan hyväksyntään, koska kuljettaja on riippuvainen työantajastaan eikä hän siten voi tehdä päätöstä vapaasti.

5.3 Saksa

Saksassa on otettu vuoden 2005 alusta käyttöön yli 12 tonnia painavien ajoneuvojen tiemaksujärjestelmä. Alun perin järjestelmä koski moottoriteitä ja joitakin muita tieosuuksia, joille liikenne muutoin olisi saattanut siirtyä. Vuonna 2011 järjestelmä laajeni 1100 km:lle 4-kaistaisia teitä, joilla ajosuunnat on erotettu keskikorokkeella tms. Maksujärjestelmää operoi yksityinen Toll Collect -yhtiö. Järjestelmä on maailmassa ensimmäinen, joka perustuu ns. autonomiseen konseptiin käyttäen hyväksi satelliittipaikannusta ja langattomia solupuhelinverkkoja.

Kuten Itävallassa, kuljettajien yksityisyyden suoja ei saanut suurta huomiota osakseen järjestelmän suunnitteluvaiheessa. Ajoneuvolaite vertailee jatkuvasti satelliittipaikannustietoja digitaaliseen karttaan maksun piiriin kuuluvasta verkosta ja pitää kirjaa kaikista maksullisista tieosuuksista, joita ajoneuvo käyttää. Maksettavan tiemaksun suuruus näkyy heti kuljettajalle. Reittitiedot (ainoastaan maksullisen verkon osalta) siirretään GSM-verkon kautta useita kertoja vuorokaudessa TollCollectin keskusjärjestelmään.

Täten sekä TollCollect:lla että valtiolla on täysi tietämys kunkin ajoneuvon sijainnista ja vastaavasta ajankohdasta päätieverkon osalta. Ei ole syntynyt mitään yleistä keskustelua kuljettajan yksityisyyden suojasta; päinvastoin kuljetusliikkeet vaativat, että laskuihin sisältyisi reittikuvaus. Yritykset tarvitset yksityiskohtaisen erittelyn laskun oikeellisuuden tarkistamiseksi ja voidakseen kohdistaa kustannukset oikein eri kuljetuksille.

Joitakin yksityisyyden suojaan liittyviä kysymyksiä on tullut yllättäen esille liittyen valvontaan, jota operoi BAG (Federal Office for Goods Transport). Yksi valvonnan muoto koostuu liikenteessä liikkuvista partioautoista, jotka tarkistavat vieressä liikkuvien raskaiden ajoneuvojen ajoneuvolaitteen tilan ja toimivuuden DSRC -linkin välityksellä. Voidakseen kerätä täydellistä valvontatiedostoa, myös valvonta-autossa on ajoneuvolaite, joka jatkuvasti kerää paikkatietoa. Valvontahenkilöstön ammattiyhdistys on valittanut työantajan ”vakoilumahdollisuudesta” henkilökunnan suhteen, koska työpäivän lähes jokaisen hetken osalta tallennetaan työntekijän paikka ja siihen liittyvä aika. Lopulta asia sovittiin niin, että vain aidosti tärkeät paikkatiedot säilytetään ja niitäkin käytetään BAG:n erityisen lupauksen mukaisesti vain valvonnan tarkoituksiin, mutta ei missään tapauksessa henkilökunnan suorituskyvyn arvioimiseen.

5.4 Yhdistyneet kuningaskunnat

Vuonna 2005 suoritettiin laajoja selvityksiä liittyen kansalliseen tiemaksujärjestelmään tavoitteena toteutus aikaisintaan 2013. Lokakuussa 2005 hallitus ehdotti, että tiemaksut hyödyntäisivät yksityisen sektorin ratkaisuja, kuten käyttöön perustuvia vakuutusmaksuja (usage based insurance; tunnetaan myös nimellä myös pay-as-you-drive, PAYD). Lähestymistavan avulla voitaisiin välttää laaja julkisen sektorin hankintamenettely, mutta oli avoinna, onnistuuko PAYD saavuttamaan laajat massamarkkinat. Suunnitelman mukaan maksu olisi kilometripohjainen, riippuisi tien ja ajoneuvon laadusta ja matkan ajankohdasta. Jokaiseen ajoneuvoon tulisi asentaa laite, joka satelliittipaikannuksen perusteella laskisi maksettavat tiemaksut. Vuonna 2007 eräs yksityishenkilö, Mr. Peter Roberts, julkaisi pääministerin sivuilla pääministerille kirjeen, jossa hän ehdotti ”ajoneuvojen seuranta- ja tiemaksusuunnitelman” romuttamista. Hän sanoi maksujen olevan epäoikeudenmukaisia köyhiä kohtaan ja niille, jotka joutuvat asumaan erillään perheistään. Hän myös esitti, että ainoa tapa saada tiemaksujärjestelmä toimimaan olisi seurata jokaisen kansalaisen jokaista liikettä. ”That is an invasion of your privacy and I think it is a very sad day when a democratic government wants to track your movements. It is time for the government to listen to the people rather than dictate to the people.”

Nettikirjoitus sai 1,8 miljoona allekirjoittajaa, mikä vastaa 6 % ajokortin haltijoista. Pääministeri vastasi tekemällä selkoa suunnitelman tarkoituksesta kiistäen, että oli tarkoitus viedä kansalaisten varoja tai lisätä kansalaisten valvontaa ja luvaten, että ennen päätöstä kansallisesta suunnitelmasta käydään ”keskustelu”. Hallitus järkyttyi vastustuksen ennenäkemättömästä laajuudesta ja median laajasta kiinnostuksesta asiaan. Lopulta suunnitelmista luovuttiin ja keskityttiin paikallisiin hankkeisiin, kuten Lontoon ruuhkamaksu.

5.5 Alankomaat

Alankomailla on pitkät perinteet yrittää toteuttaa tiemaksuja ruuhkien taltuttamiseksi. Jo 1980-luvun lopulla valmisteltiin suunnitelmia ylikuormittuneiden moottoriteiden puomittomista sähköisistä tiemaksuista (free-flow EFC) hankkeessa ”Rekening rijden”. Liikenneongelmat pahenivat edelleen eikä tieverkkoa pystytty kehittämään tarvetta vastaavasti, vaan ruuhkat vain lisääntyivät. Eräät poliitikot uskoivat tiemaksujen olevan oleellinen osa kehittämisstrategiaa ongelmien ratkaisemiseksi. Koska yleisön ja politikkojen laaja tuki olisi vaikeasti saavutettavissa, perustettiin laaja foorumi, jossa oli edustajia työnantajista, ammattiyhdistysliikkeestä, liikennesektorista, auto-organisaatioista, ympäristöorganisaatiosta jne. tarkoituksena etsiä yleisesti hyväksyttävä ratkaisu. Vuonna 2005 saavutettiin yhteisymmärrys, että kilometrimaksut sidottuna aikaan, paikkaan ja ajoneuvon ominaisuuksiin olisi paras ratkaisu ja tulisi toteuttaa mahdollisimman nopeasti. Yleisen hyväksyttävyyden saavuttamiseksi uudistuksen tulisi olla veroneutraali.

Hallitus noudatti ehdotusta ja ryhtyi valmistelemaan verotusjärjestelmän täysuudistusta. Tieverosta ja ajoneuvon hankintaverosta luovuttaisiin ja autoilijoiden tulisi maksaa ajetuista kilometreistä, ”Kilometerheffing”.

Kilometrimaksulla oli kolme tavoitetta. Ensinnäkin tie- ja ajoneuvokustannukset jaettaisiin käyttäjien kesken oikeudenmukaisemmalla tavalla. Vaikka tämä ei yksinään perustele monimutkaista ja kallista järjestelmää, se on tarpeen yleisen hyväksyttävyyden saavuttamiseksi. Toiseksi suunnitelman uskottiin vähentävän ruuhkia merkittävästi, etenkin jos maksut riippuisivat ajasta ja paikasta. Kolmanneksi olisi saavutettu ympäristöhyötyjä. Oli päätetty, että maksut koskisivat kaikkia ajettuja kilometrejä riippumatta siitä, ajetaanko julkisella vai yksityisellä alueella. Etuna on tällöin, ettei tarvita tietoa kaikkien teiden sijainnista tai yksityisten alueiden rajoista, jotka sitä paitsi alati muuttuvat.

Yksityisyyden suojan turvaamiseksi konsepti perustui mahdollisimman vähäiseen henkilökohtaisen tiedon käsittelyyn (ns. ”älykäs ajoneuvolaite”). Ajoneuvolaitteen tuli summata ajosuoritteet pidemmän aikajakson kuluessa eri tariffiluokkiin. Vain nämä tiedot sekä joitain järjestelmän hallintaan liittyviä tietoja siirrettäisiin ajoneuvolaitteesta keskusjärjestelmään, mutta ei mitään sijaintitietoa.

Yksityiset toimijat voisivat toimia eri konseptilla, esim. koskien muissa palveluissa käytettäviä seurantatietoja. Käyttäjän suostumuksella voitaisiin ohittaa huolet yksityisyydestä.

Valittiin hybridimalli, jossa tehtävät jaettiin julkisen tahon ja yksityisten toimijoiden välille. Viranomainen olisi ylläpitänyt keskusjärjestelmää. Oletettiin, että yksityisen sektorin puolella syntyisi avoimet markkinat, jotka antaisivat autoilijoille mahdollisuuden valita joukosta sertifioituja ajoneuvolaitteita haluamansa palvelukirjon. Oletettiin, että avoimet markkinat johtaisivat jatkuviin innovaatioihin ja alhaisiin hintoihin.

Hankkeessa panostettiin paljon suhdetoimintaan ja julkisuuteen, koska kaikki aikaisemmat vastaavat hankkeet olivat kohdanneet kansalaisten epäluuloa ja kaatuneet. Tietyssä vaiheessa intressiryhmät, jotka edustivat 75 % äänestäjistä, tukivat hanketta, kuten autoilijaklubit, kauppa, ammattiliitot, autokauppiaat, jne. Mielipidetiedustelujen mukaan kansalaiset kannattivat laajasti hanketta, jota pidettiin tarpeellisena ja hyvänä tapana ratkaista ruuhkaongelmaa varsinkin, kun luvattiin, että esitys on veroneutraali. Käyttäjät toivoivat yksinkertaista, täysin automaattista ”hands-off, plug-and-play” -järjestelmää. Edelleen toivottiin yksityisyyden suojaa, tasapuolista kohtelua (ei mitään poikkeuksia), siistiä ajoneuvolaitetta ja vahvaa valvontaa. Selvää oli myös, että kansalaiset halusivat valtion olevan järjestelmän isäntä.

Hankkeen alamäki alkoi hitaasti, kun eräät puolueet arvelivat saavansa ääniä vastustamalla hanketta. Kannatuksen eroosio ei kuitenkaan vaarantanut hanketta tässä vaiheessa. Hankkeen pysäytti sen sijaan maan hallituksen kaatuminen Afganistanin politiikkaansa. Pitkittyneen väliaikaishallituksen aikana, jolloin hallitus ei halunnut tarttua arkoihin asioihin, hanke oli jäissä, innostus laski ja kannatus hupeni. Uusi hallitus ei käynnistänyt hanketta uudelleen, vaan käynnisti ohjelman alueellisten liikkuvuusprojektien käynnistämiseksi.

Alankomaiden tiemaksuprojektihistoria – ainakin viimeisin hanke – osoittaa, että kansalaisten huolet yksityisyyden suojasta voitiin hoitaa avoimen ja vastuuntuntoisen valmistelun avulla. Yksityisyyden hoidon vaatimukset olivat ohjaavia järjestelmän pääarkkitehtuuria määriteltäessä. Tässä mielessä ”Kilometerheffing” -hanke on ollut edelläkävijä, kun on kyse yksityisyyden hoidosta suunnittelemalla (Privacy by Design) tiemaksualalla. Keskeisenä arkkitehtuuriratkaisuna oli, että yksityiskohtaisen reittitiedon tulee jäädä ajoneuvolaitteeseen ja käyttäjän täydelliseen hallintaan ja vain jalostettu tieto siirtyy keskusjärjestelmään.

Mielenkiintoista on, että hanke ei kaatunut puuttuvaan kansalaisten hyväksyntään, vaan poliittisen tuen pettämiseen pitkittyneen prosessin aikana vaaleineen ja uusine hallituksineen. Yksityisyys on tärkeä asia Alankomaissa, jossa kansalaisilla on taipumus epäillä valtiollisia laitoksia. ”Kilometerheffing” hankkeen arkkitehtuuri, sen tiedotuskonsepti ja yhteistoiminta kansalaisten ja toimijoiden kanssa oli suunniteltu siten, että kyseiset huolet voitiin ottaa huomioon avoimella tavalla ja ”suunnittelemalla”.

Lopuksi on todettava, että valittu arkkitehtuuri oli teknisesti varsin haastava ja sen toteutuskelpoisuus on edelleen näyttämättä.

6. Yksityisyyden sisällyttäminen arkkitehtuurin suunnitteluun

Alankomaiden hanke kilometriperusteisesta veloitusjärjestelmästä (”Kilometreheffing”) toimii hyvänä esimerkkinä tiemaksujärjestelmästä, jossa käsitellään ”kuka oli missä ja milloin” luonteista tietoa, mutta joka voidaan suunnitella käyttäjän yksityisyyttä kunnioittaen. Yksityisyys tulee huomioida järjestelmän suunnittelussa alusta alkaen. Erityisen tärkeä on vaihe, jossa suunnitellaan järjestelmäarkkitehtuurin perusratkaisut ja päätetään, mitä tietoa kerätään, missä tietoa säilytetään ja käsitellään ja kenellä on pääsy tietoon. Tällaisesta lähestymistavasta, jossa tietosuoja on olennainen osa järjestelmän suunnittelua, käytetään termiä ”Privacy by Design”.

”Privacy by Design” tarkoittaa siis periaatetta, jossa yksityisyys ja tietosuoja ovat mukana teknologioiden koko elinkaaressa varhaisesta suunnitteluvaiheesta käyttöönottoon, käyttöön ja lopulliseen hävitykseen.” (Wikipedia)

Tämä luku esittelee systemaattisesti mahdollisia suunnitteluvaihtoehtoja. Aluksi kerrataan lyhyesti, mitä kaikkea dataa tiemaksujärjestelmiin liittyy, sen jälkeen käsitellään yksityisyyteen kohdistuvia uhkia ja lopuksi esitellään seikkaperäisesti soveltuvia yksityisyyden mahdollistavia tekniikoita.

6.1 Henkilötiedon lajit tiemaksujärjestelmissä

Tietosuojadirektiivin mukaan erityisen arkaluonteiseen tietoryhmään kuuluvat “henkilötiedot, jotka koskevat rotua tai etnistä alkuperää, poliittisia mielipiteitä, uskonnollista tai filosofista vakaumusta tai ammattiliittoon kuulumista, sekä terveyteen ja seksuaaliseen käyttäytymiseen liittyvät tiedot”. Sellaisia tietoja ei normaalisti käsitellä tiemaksujärjestelmissä eikä liikennetelematiikassa yleensäkään. Yleensä liikennetelematiikan palveluissa käytettävät paikannus- ja liikkumistiedot eivät kuulu kaikkein arkaluonteisimpiin tietoryhmiin.

Useimmat ihmiset eivät kuitenkaan pidä tienkäyttöön liittyvän tiedon päätymistä asiattomille tahoille suinkaan harmittomana. On myös jokseenkin ilmeistä, että mitä kattavampaa ja tarkempaa data on, sitä arkaluontoisemmaksi se muuttuu. Tulee myös huomata, että yksityiskohtainen paikannustieto saattaa paljastaa arkaluontoiseksi luokiteltavaa informaatiota. Kuten jo aiemmin on mainittu, paikannustieto saattaa esimerkiksi paljastaa säännölliset vierailut tiettyyn kirkkoon tai sairaalaan, joten jo itse paikannustietoa tulee pitää arkaluontoisena. Tämä arvioidaan seuraavaksi tapaus tapaukselta. On kuitenkin selvää, että riskit ovat suuremmat, jos paikannustieto on yksityiskohtaista ja kattavaa.

Tienkäyttöön liittyvän tiedon arkaluontoisuuden arvioimiseksi tässä selvityksessä käytetään seuraavaa yksinkertaista luokittelua:

Ryhmä	A	Matkatiedot ilman sijaintitietoa, esimerkiksi etäisyys ja aika
	A1	Satunnaisotokset
	A2	(Lähes) täydellinen tieto kaikesta liikkumisesta
Ryhmä	B	Paikkatieto
	B1	Satunnaiset yksittäiset otokset sisältäen paikan ja ajan
	B2	Yhdistetyt näytteet, jotka mahdollistavat matkojen / reittien jäljittämisen, mutta osittain hajanainen tieto; ei täydelliset tiedot sijainnista tai ajasta
	B3	Täydelliset ajoneuvon tai henkilön reittitiedot
Ryhmä	C	Yksityiskohtaiset tiedot ajokäyttäytymisestä (esim. nopeus, kiihdytykset, jarrutukset, ajotunnit)

Viimeiseen ryhmään kuuluvasta ajokäyttäytymisestä voidaan tehdä päätelmiä henkilön terveydellisestä tilasta (esim. tapahtunut onnettomuus) tai tapahtuneesta rikoksesta (esim. raju ylinopeus). Tällaiset tiedot ovat erityisasemassa ja niitä pidetään tietosuojadirektiivin mukaan arkaluontoisina. Joissakin maissa tietyt tietosuojan valvontaviranomaiset (esim. CNIL Ranskassa) eivät salli lainkaan rikkomukseen tai rikokseen liittyvän tiedon käsittelyä (pois lukien rikossyyte, kansallinen turvallisuus ja muut tietosuojadirektiivin ulkopuolella olevat tiedon käyttötarkoitukset).

Jo edellä kuvatun yksinkertaisen luokittelun perusteella nähdään, että tienkäyttöön liittyvien tietojen arkaluontoisuus riippuu voimakkaasti käytettävästä veloituskonseptista. Jos kerätään tietoa vain kuljetusta etäisyydestä, mutta ei sijainnista, on tietosuoja paljon pienempi kysymys kuin käytettäessä täydellistä ajan, etäisyyden ja paikan huomioivaa veloitusta. Seuraavassa pohdinnassa oletetaan käytettävän kokonaisvaltaista aikaan, etäisyyteen ja sijaintiin perustuvaa veloitusta, joka edellyttää tienkäyttömaksun laskemiseksi täydellisen reitti-informaation.

6.2 Yksityisyyteen kohdistuvat uhat

Euroopan komissiolle tehdyssä raportissa (ITS & Personal Data Protection) tunnistettiin kolmentyyppisiä liikennetelematiikan sovelluksiin liittyviä käyttäjän yksityisyyteen kohdistuvia uhkia. Ne liittyvät kaikki myös tienkäyttömaksuihin:

Luvaton pääsy henkilötietoihin salakuuntelemalla, henkilökunnan luvattomilla toimilla, hakkeroinnilla jne.

Tiemaksujärjestelmissä käyttäjän henkilöllisyyteen liittyvää tietoa, kuten hänen nimeään ja osoitettaan, säilytetään yleensä keskitetysti laskutuksen helpottamiseksi. On kuitenkin olemassa myös anonyymin käytön sallivia järjestelmiä, joihin käyttäjien ei tarvitse rekisteröityä. Käyttäjät maksavat ajoistaan ajoneuvolaitteeseen (OBE) ladatun pre-paid –tilin avulla. Ajoneuvolaite veloittaa tiliä reaaliaikaisesti. Tällainen ratkaisu vaikuttaa houkuttelevalta, mutta siinä on kuitenkin monia käytännön ongelmia: Tilille ladattu arvo voidaan varastaa tai tuhota, eikä sitä voida enää myöhemmin palauttaa sen anonyymiyden vuoksi. Myös rahanpesu on anonyymien tilien yleinen ongelma. Käyttäjän anonyymiys tienkäyttömaksujen yhteydessä on juridiselta kannalta vaikea asia. Riski luokitellaan tältä osin vain keskinkertaiseksi, sillä laskutuksen vuoksi keskitetysti tarvitsee säilyttää ainoastaan tietoa henkilöllisyydestä ja yhdistettyä tietoa tienkäytöstä, jonka ei tarvitse olla kovin yksityiskohtaista.

Laillisesti määritellyn tarkoituksen tai rekisteröidyn suostumuksen ylittävä henkilötietojen uudelleenkäyttö

Tämä uhka koskee erityisesti satelliittipaikannukseen (GNSS) perustuvia ratkaisuja, jotka tuottavat kaupallisesti kiinnostavaa oheistietoa, kuten tietoa ajonopeuksista ja matka-ajoista. Tienkäyttötiedot saattavat valua muihin sovelluksiin, kuten vakuutusyhtiön ilman kuljettajan lupaa tekemässä riskiprofiloinnissa.

Tarkoituksenmukaisen käytön ylittävä henkilötietojen käsittely

Tämä koskee erityisesti satelliittipaikannukseen (GNSS) perustuvia ratkaisuja, jotka tuottavat hyvin yksityiskohtaista paikannustietoa. Riski nähdään pienemmäksi automaattiseen rekisteritunnusten tunnistukseen (ANPR) ja lyhyen kantaman tiedonsiirtoon (DSRC) pohjautuvissa tekniikoissa, joista on saatavana dataa vain tietyistä havaintopisteistä. Jos maksu esimerkiksi on etäisyysperusteinen ja maksuvyöhykkeitä on vähän, ei keskusjärjestelmän tarvitse käsitellä yksityiskohtaisia reittitietoja.

6.3 Toimenpiteet käyttäjän yksityisyyden suojaamiseksi

Käyttäjän yksityisyyteen kohdistuvia uhkia vastaan tehtävistä vastatoimista käytetään usein käsitettä PET (Privacy Enhancing Technology, Yksityisyyden suojaa parantavat tekniikat). Se on yleinen nimitys työvälineille ja mekanismeille, joilla parannetaan käyttäjän yksityisyydensuojaa erityisesti verkkopalveluissa. “PET tarkoittaa yhtenäistä tieto- ja viestintäteknisten toimenpiteiden järjestelmää, jolla suojataan yksityisyyttä poistamalla henkilötiedot kokonaan tai osittain tai ehkäisemällä tarpeeton ja/tai epätoivottu henkilötietojen käsittely heikentämättä kuitenkaan tietojärjestelmän toimivuutta” (PET Communication).

Edellä kuvattu PET:in määritelmä on lainattu Euroopan komission tiedonannosta, joka suosittelee PET:in käyttöä. Tätä raporttia varten kuvaamme “Privacy by Design” periaatteen toimenpiteinä, jotka voidaan luokitella seuraavasti (ITS & Personal Data Protection):

M1 Anonymisointi

Anonymisoinnilla tarkoitetaan tiedon käsittelyä siten, ettei tietoa pystytä enää jäljittämään luonnolliseen henkilöön tai tiettyyn ajoneuvoon. Tiemaksujen yhteydessä tämä on harvoin mahdollista, sillä vastuu maksujen suorittamisesta kuuluu yleensä henkilölle, joka on tunnistettava prosessissa. Kuten yllä selitettiin, anonyymit pre-pay-tilit ovat yksi varteenotettava käyttäjille tarjottava vaihtoehto. Sellaista järjestelmää käytetään esimerkiksi Itävallan raskaan liikenteen tienkäyttömaksujen keräämiseen. Käyttäjät voivat ostaa ajoneuvolaitteen (OBE) jakelupisteistä, kuten huoltoasemilta, ja ladata niihin samalla arvoa. Käyttäjien henkilöllisyys pysyy periaatteessa salassa. Käytännössä henkilöllisyys voitaisiin kuitenkin selvittää koska tahansa. Kuten aiemmin on todettu, käyttäjää on melko helppoa tunnistaa tämän reittitietojen perusteella. Itävaltalainen “Go-Maut” on lyhyen kantaman tiedonsiirtoon (DSRC) perustuva järjestelmä, jossa kaikki tapahtumatiedot lähetetään keskusjärjestelmään, joka tunnistaa täydellisesti ainakin moottoriteillä ajetut reitit.

Anonymisointi ei siis yleensä ole mahdollista, paitsi tietyissä erityisolosuhteissa. Erityisesti satelliittipaikannukseen (GNSS) pohjautuvissa järjestelmissä tiedon anonymisointi on vaikeaa.

M2 Pseudonymisointi

Tässä käyttäjän jäljitettävyys tehdään vaikeaksi käyttämällä tilapäisiä henkilöllisyyksiä. Anonymisoinnin tapaan se ei tavallisesti ole mahdollinen yksityisyyden suojaa parantava tekniikka tiemaksujen yhteydessä. Uhka yksityisyyttä kohtaan piilee ensisijaisesti reitti-informaatiossa, joka epäsuorasti sisältää henkilöllisyyden, koska reittitiedot paljastavat käyttäjän elinympäristöön (koti, työpaikka) ja elintapoihin liittyviä tekijöitä.

M3 Datan minimointi

Yleisenä tietosuojan periaatteena, tulisi kerättävä ja käsiteltävä data rajata ainoastaan käyttötarkoituksen vaatimiin tietoihin. Tämä toimenpide tulee aina huomioida. Esimerkiksi paikasta riippumattoman ajettuun etäisyyteen perustuvan hinnoittelun yhteydessä ei ole tarpeen käsitellä ajoneuvon sijaintiin liittyviä tietoja. Riittää että ajoneuvolaite (OBE) määrittää ajetun vyöhykekohtaisen matkan.

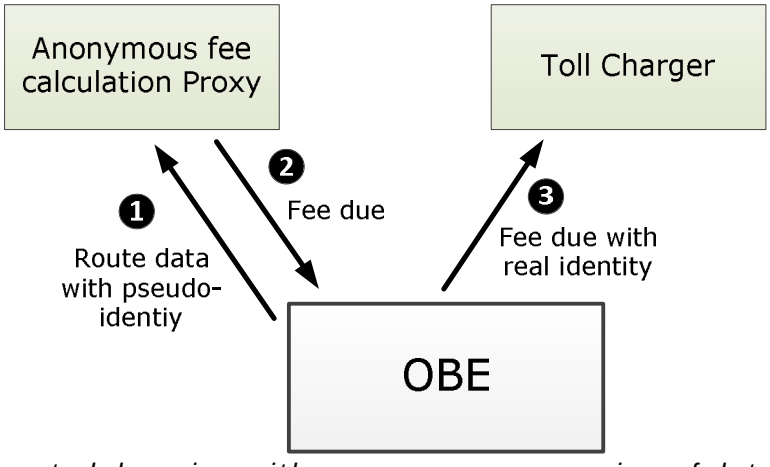
M4 Tiedonkäsittelyn hajauttaminen (Domain separation)

Tämä tarkoittaa tienkäyttöön ja ajokäyttäytymiseen liittyvän tiedon käsittelyä erillisessä keskuksessa, josta ei ole pääsyä käyttäjän henkilöllisyyteen liittyviin tietoihin (esim.

nimi, osoite, auton rekisteritunnus). Toinen keskus käsittelee henkilöllisyyteen liittyvän informaation ja saa ensimmäiseltä keskukselta vain laskutuksen kannalta välttämättömät, tiivistetyt tiedot tienkäytöstä.

Kansainvälisen telekommunikaatiokysymysten tietosuojaryhmän (IWGDPT) tekemässä tiemaksujen johdatusraportissa (Sofia Memorandum) tällaiseen ratkaisuun suhtaudutaan hyvin kriittisesti, sillä jo ensimmäinen keskus käsittelee reittitietoja, eli henkilötietoja. Vaikka tiedot anonymisoitaisiin tai pikemmin pseudonymisoitaisiin, niin reittitietoja täytyy pitää suojeltavina henkilötietoina, kuten on jo monesti todettu. Sofia Memorandumin mukaan, tiedonkäsittelyn hajauttamisesta huolimatta, suuria tietomääriä säilytetään keskitetysti, mikä saattaa johtaa tietojen alkuperäisestä käyttötarkoituksesta poikkeavaan hyödyntämiseen (function creep) (toinen luvussa 6.2. mainituista uhista). Hyvä esimerkki tästä tapahtui Sloveniassa, missä pankit saivat vakuutusyhtiöitä ostettuaan käsiinsä käyttäjien terveyttä ja maksukykyä koskevia tietoja. Monet pankkien asiakkaista kokivat yllätyksen, kun luottorajan korotuksesta tai asuntolainan myöntämisestä kieltäydyttiin ilman ilmeistä syytä.

Kansalliset informaatiovaltuutetut ovat useissa tilanteissa ilmaisseet huolensa siitä, että kun suuria tietomääriä säilytetään keskitetysti, ei tietoa voida pitkällä aikavälillä suojata. Olosuhteiden muuttuessa tieto päätyy muihin sovelluksiin ja instituutioihin. On huomionarvoista, että Sofia Memorandum näkee toisen hyvin samankaltaisen konseptin, anonyymin edelleen-lähettämisen ja anonyymien paluusilmukka välityspalvelimien (loop-back proxy) käytön paljon parempana vaihtoehtona. Tämä tekninen käsite tarkoittaa konseptia, jossa ajoneuvolaite (OBE) lähettää yksityiskohtaiset reittitiedot tekniselle laskentakeskukselle, joka laskee tietojen pohjalta veloitettavan tienkäyttömaksun. Käyttäjän ajoneuvolaite lähettää reittitiedot tilapäistä pseudo-henkilöllisyyttä käyttäen. Laskentakeskus lähettää takaisin ajoneuvolaitteelle salatulla allekirjoituksella varustetun vahvistuksen: “Minä, sertifioitu tiedonkäsittelykeskus, olen laskenut seuraavan tienkäyttömaksun seuraavaa pseudo-henkilöllisyyttä noudattavan käyttäjän toimittamiin reittitietoihin perustuen”. Käyttäjä lähettää lopuksi todellista henkilöllisyyttään käyttäen sertifioidut maksutiedot keskusjärjestelmälle laskutusta varten. Tällä tavalla käyttäjän anonymiteetti pysyy suojattuna.



Concept of separated domains with anonymous processing of detailed route information

Päinvastoin kuin Sofia Memorandum, tämä konsepti nähdään kriittisenä. Se on vain toinen tapa hajauttaa tiedonkäsittelyä (domain separation), missä henkilötiedot, eli reittitiedot, käsitellään keskitetysti. Konsepti saattaisi toimia vain, jos maksunlaskentakeskus olisi ehdottoman luotettava, eli reittitiedot poistettaisiin

välittömästi käsittelyn jälkeen eikä kellään ulkopuolisella olisi pääsyä tietoon. Käyttäjien luottamus järjestelyyn riippuu voimakkaasti mukana olevien toimijoiden maineesta.

Tiedonkäsittelyn hajauttaminen (domain separation) siis saattaa edistää tietosuojaa, mutta ei välttämättä ole lopullinen ratkaisu. Yksityiskohtaisia reittitietoja säilytetään ja käsitellään yhä keskitetysti ja reittitiedot ovat henkilötietoja, vaikka käyttäjän tunnistetiedot poistettaisiin. Mitään ei siis saavuteta, jollei tiedonkäsittelykeskukseen ole ehdotonta luottamusta. Jos luottamusta olisi, niin miksi tiedonkäsittelyä ylipäänsä hajautettaisiin? Jo hajautetun tiedonkäsittelyn soveltaminen viittaa pohjimmiltaan siihen, että täyttä luottamusta ei ole ja tunnistetietojen käsittely tulisi erottaa tienkäyttötietojen käsittelystä.

M5 Käyttäjän suostumus

Yleinen periaate on, että käyttäjien tulee antaa vapaasti suostumus tietojensa käsittelyyn, ellei laissa toisin määrätä. Tämä todetaan esimerkiksi tietosuojadirektiivissä. Tienkäytön hinnoitteluun liittyvien tietojen käyttöön ei käyttäjän suostumus päde, vaan tämä määritellään aina laissa. Ei ole mahdollista valita vapaasti osallistuuko tiemaksujärjestelmään vai ei, vaan tämä määritetään lainsäädännössä.

Käyttäjän suostumusmekanismit pätevät kuitenkin, jos tiemaksujen veloitus on yksi sovellus muiden joukossa monipalveluympäristössä. Tällöin käyttäjien tarvitsee luonnollisesti tehdä “vapaaehtoinen, yksilöity ja tietoinen tahdon ilmaisu, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn” (ks. ”rekisteröidyn suostumuksen” määritelmä luvussa 2.3).

M6 Tietojen poistaminen heti käsittelyn jälkeen

Tämä on hyvä yleisperiaate, jota tulisi aina noudattaa. Tiedot tulee poistaa heti, kun niitä ei enää tarvita. Valitettavasti tienkäyttömaksuihin liittyvää tietoa joudutaan säilyttämään melko pitkään. Käyttäjä saattaa esimerkiksi vaatia erittelyn tienkäyttölaskustaan, maksun oikeellisuuteen liittyviä kiistoja voidaan joutua selvittämään tai viranomainen voi tarvita reittitietoja pakkotoimenpiteenä rikosten selvittämiseksi. Mikäli tienkäyttömaksu määritellään veroksi, edellyttää lainsäädäntö yleensä veroihin ja verotusperusteisiin liittyvän tiedon säilyttämistä useiden vuosien ajan.

Lisäksi toimenpide tarvitsee käyttäjän luottamuksen siitä, että tiedot todella on poistettu. Monet ovat tietoisia, että nykyaikaisissa elektronisissa laitteissa, kuten tietokoneissa, matkapuhelimissa ja digitaalikameroissa tietojen “poistaminen” ei tarkoita tietojen lopullista hävittämistä. Ne vain merkitään poistetuiksi ja voivat tietyissä oloissa olla pitkän aikaa palautettavissa, ennen kuin ne tuhotaan päällekirjoittamalla.

M7 Jaettu tiedonkäsittely

Tässä kaikkein yksityiskohtaisimmat ja arkaluontoisimmat tienkäyttötiedot käsitellään paikallisesti, esimerkiksi mobiililaitteessa tai ajoneuvoon asennetussa laitteistossa. Keskusjärjestelmään lähetetään ainoastaan esimerkiksi laskutuksen kannalta oleellinen informaatio. Tämä konsepti on periaatteessa todella vahva, sillä kriittisiä henkilötietoja ei säilytetä tai käsitellä keskitetysti. Tulee kuitenkin tiedostaa, että vaikka yksityiskohtaista informaatiota käsitellään ajoneuvolaitteessa (OBE) eikä ladata keskusjärjestelmään, niin tiedonkäsittely tapahtuu kuitenkin rekisterinpitäjän vastuulla.

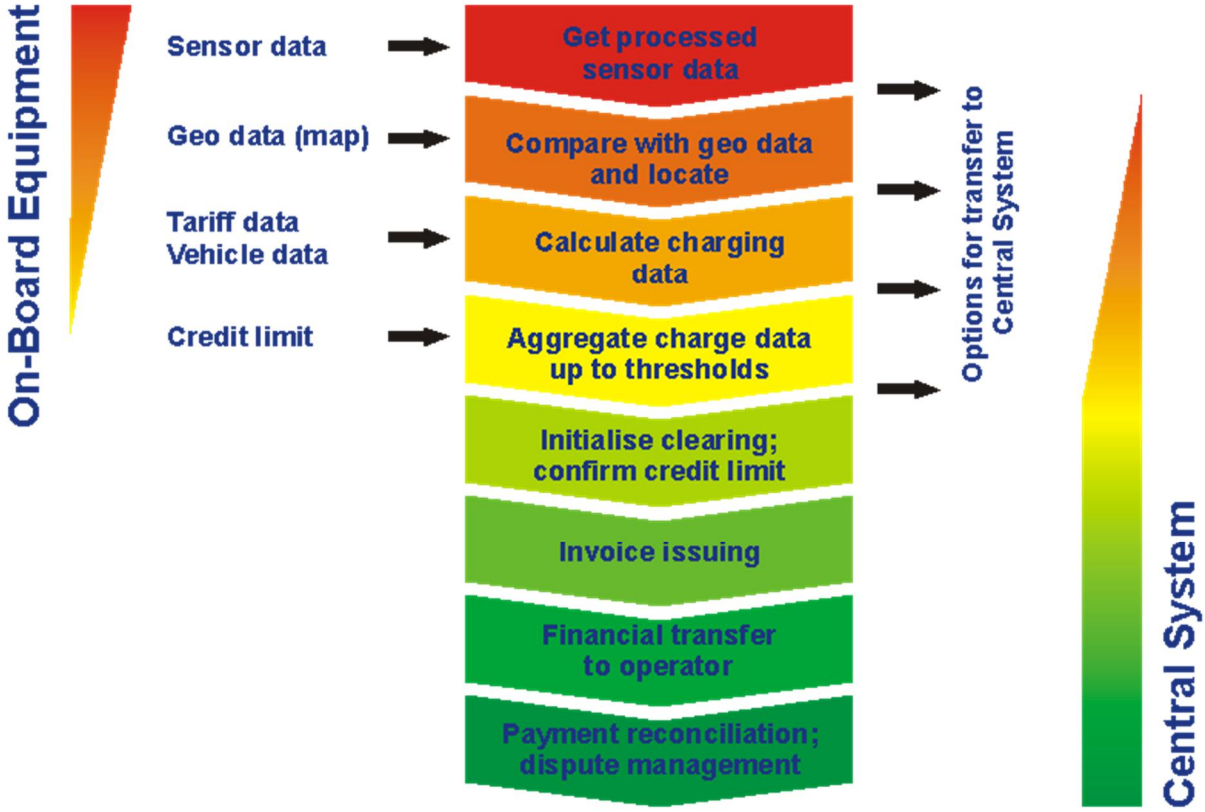
Tienkäytön hinnoittelussa konsepteja, joissa kriittinen tiedonkäsittely tapahtuu ajoneuvolaitteissa (OBE), kutsutaan “smart client” (tai “thick client”) – lähestymistavoiksi. Näitä käsitellään yksityiskohtaisemmin seuraavassa luvussa.

M8 Rekisteröidyn määräysvalta

Tässä toimenpiteessä yksityisyys suojataan käyttäjän mahdollisuudella hallita säilytettävää yksityiskohtaista henkilötietoa. Käyttäjä voi poistaa tai tuhota tiedot osittain tai kokonaan ja päättää, luovuttaako niitä esimerkiksi valituksen tekemiseksi. Tämä lähestymistapa on joskus käyttökelpoinen, jos yksityiskohtaisia tietoja ei tarvita ensisijaisessa prosessissa, vaan ainoastaan rekisteröidyn edun ja laillisen aseman turvaamisessa. Tienkäytön hinnoittelun yhteydessä konsepti ei yleensä ole käyttökelpoinen, paitsi lisäominaisuutena. Esimerkiksi “smart client” lähestymistavassa, jossa tietoa käsitellään ensisijaisesti ajoneuvolaitteessa (OBE) ja yksityiskohtaiset henkilötiedot pysyvät normaalisti paikallisina, käyttäjä voi päättää, avaako hän jotain tietoa saadakseen eritellyn raportin tai todistaakseen jotain riitatilanteessa.

6.4 Veloitusprosessin yksityisyyden suoja

Veloitusprosessi voidaan jakaa useisiin vaiheisiin, mitä havainnollistetaan seuraavassa kaaviossa:

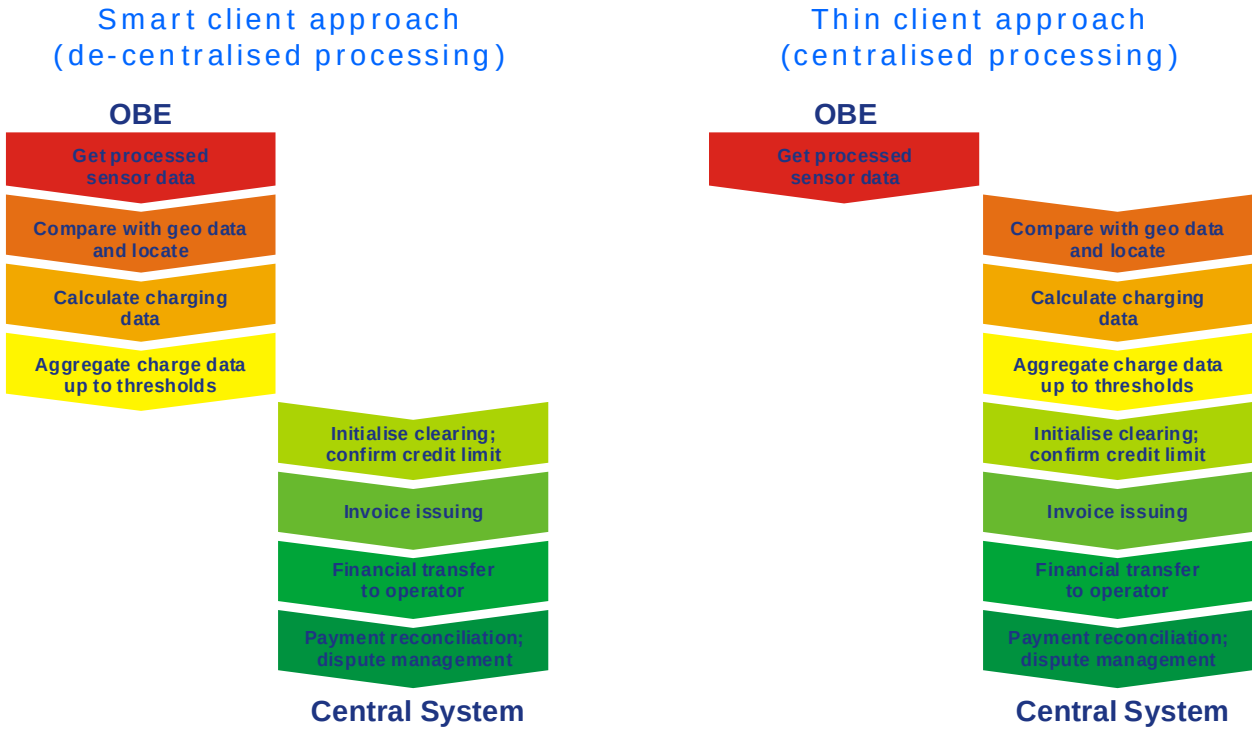


Autonomisen järjestelmän veloitusprosessin vaiheet (satelliittipaikannus / matkapuhelinverkko –järjestelmät)
(Lähde: Presentation by B. Oehry at Stockholm Group meeting, Vienna, 5 Oct. 2005)

Kaavio esittää ylhäältä alaspäin veloitusprosessiin kuuluvat vaiheet, kun käytössä on autonominen järjestelmä. Esimerkki tällaisesta on ajoneuvolaitetta (OBE), satelliittipaikannusta (GNSS) ja matkapuhelinverkkoa hyödyntävä järjestelmä. Ensimmäisessä vaiheessa ajoneuvolaite (OBE) kerää sensoritietoa sijainnista, kuljetusta etäisyydestä ja ajankohdasta. Sitten tätä tietoa, erityisesti sijaintitietoa, verrataan tiemaksujärjestelmän karttatietoihin ja määritetään, onko käyttäjä ajanut maksullista tieosuutta ja mikä tariffi pätee. Kolmas vaihe on laskea reaaliaikaisesti tienkäyttömaksu tämän informaation, ajankohdan ja ajoneuvoluokan perusteella. Kertyneet maksut voidaan laskea yhteen esimerkiksi yhden matkan, tietyn tuntimäärän tai tietyn kuljetun

etäisyyden välein. Veloitusprosessin loput vaiheet liittyvät laskutukseen. Järjestelmä varmistaa, ettei käyttäjällä ole erääntyneitä tienkäyttömaksuja ja laskuttaa käyttäjää. Käyttäjän maksettua laskun varmistetaan vielä maksun saapuminen operaattorille ja selvitetään mahdolliset epäselvyydet.

Veloitusprosessiin viimeiset vaiheet ovat sellaisia, että ne suoritetaan luonnostaan keskitetysti. Alkuvaiheen toimenpiteiden osalta voidaan puolestaan tehdä valinta, suoritetaanko ne ajoneuvolaiteessa (OBE)(“smart client” tai thick client”) vai keskitetysti (”thin client”).



Käsittelyn hajauttaminen ”smart client” ja ”thin client” -lähestymistavoissa
(Lähde: Presentation by B. Oehry at Stockholm Group meeting, Vienna, 5 Oct. 2005)

Kansainvälinen telekommunikaatiokysymysten tietosuojaryhmä (IWGDPT) on Sofia Memorandumissa ilmaissut voimakkaan mielipiteensä “thin client” ja “fat client” –arkkitehtuureista. “Thin client” –konsepteista todetaan seuraavaa:

“Yksityisyydensuojan kannalta vähiten suositeltava ratkaisu sähköisten tiemaksujen keräämiseksi on järjestelmä, jossa kaikki matka-aikoihin ja ajoneuvojen sijainteihin liittyvä informaatio päätyy valvontakeskuksena toimivalle yksittäiselle taholle tai instituutiolle. Niin kutsuttu “thin client” (tai ajoneuvolaite) ainoastaan kerää tiedon matkoista ja kaikki muut veloitusprosessin vaiheet suoritetaan valvontakeskuksessa, jossa on keskitetty tietokanta sijaintitiedoista, käyttäjän tunnistetiedoista sekä veloitustiedoista.

Työryhmä ilmaisee huolensa tällaisen ratkaisumallin käyttöönotosta, sillä se tarjoaa yksilöille selvästi vähiten yksityisyydensuojaa. Periaatteessa kysymyksessä “thin client” tai “smart client” –lähestymistapojen suosimisessa on kysymys valinnasta keskitetyn ja hajautetun tiedonkäsittelyn välillä. Tämä ongelma kohdataan usein yksityisyyden ja tietosuojan yhteydessä.

Keskitetyn tiedonkäsittelyn puolestapuhujien mukaan keskitetty tiedonsäilytys ja oikeanlaiset tietosuojamekanismit (esim. tarkoituksenmukainen pääsyn sääntely, lokitiedot henkilötietojen käsittelystä jne.) varmistaisivat paremman turvallisuustason, kuin mitä yksittäinen henkilö pystyisi takaamaan. Vastalauseena voidaan kuitenkin todeta, että mikäli data on vain yksittäisen henkilön hallinnassa, vain henkilön omat henkilötiedot ovat haavoittuvaisia (esim. jos ajoneuvo tai ajoneuvolaite (OBE) varastetaan). Keskitetyssä tiedonkäsittelyssä taas kaikki henkilötiedot, mahdollisesti paremmasta tietoturvasta huolimatta, ovat potentiaalisesti haavoittuvaisia. Tämän vuoksi ja yksityisyydensuojan näkökulmasta tulee suosia ratkaisuja, joissa henkilötietoja ei säilytetä keskitetysti, vaan ne ovat yksilön hallussa ja hallinnassa. Lisäksi yksityisyydensuojan yhteydessä joudutaan usein tekemisiin niin sanotun "function-creep" –ilmiön kanssa, missä alunperin tiettyyn tarkoitukseen (voi olla täysin laillinen tarkoitus) kerättyä tietoa käytetään muihin tarkoituksiin. Ennalta-arvaamattomalla kolmannella osapuolella saattaa olla mahdollisuus päästä tietoihin. "Function-creep" –ilmiöön liittyvät ongelmat käytännössä häviävät, kun käsiteltävä tieto on käyttäjän hallinnassa."

On hyvä huomata, että vaikka yksityiskohtaista informaatiota käsitellään vain ajoneuvolaitteessa (OBE), eikä lähetetä keskusjärjestelmään, niin tämä ei tarkoita, ettei tietoa käsiteltäisi rekisterinpitäjän vastuulla. Toisin sanoen, se ei merkitse datan minimointia, vaan hajautettua käsittelyä. "Smart client" –lähestymistavan käyttöönotossa oleellinen kysymys on, kuka oikeastaan hallitsee ajoneuvolaitetta (OBE). Alankomaissa vuosina 2009 ja 2010 käydyssä tiemaksuja koskevassa poliittisessa keskustelussa ehdotetun "smart client" –konseptin yksityisyydensuoja nähtiin yhä haavoittuvaksi, vaikka siinä noudatettiin tietosuojan valvontaviranomaisen suositusta. Merkittävä huolenaihe oli, että ajoneuvolaitetta (OBE) pystyvät ohjaamaan etäältä tahot, joille yksityisyydensuoja ei välttämättä ole muita liiketoiminnallisia intressejä tärkeämpi prioriteetti. Siten ei lopulta ole takeita siitä, ettei ajoneuvolaitteen asetuksia tai ohjelmistoa muutettaisi jossakin vaiheessa lähettämään sijaintia ja liikkumista koskevaa yksityiskohtaista informaatiota. Teoriassa ongelma voitaisiin ratkaista rajaamalla ajoneuvolaitteen (OBE) hallinta ainoastaan käyttäjälle ja keskusjärjestelmään lähetettäisiin vain sellaista informaatiota, johon käyttäjä on antanut suostumuksensa. Ohjelmistonhallinta, asiakaspalvelu, sääntöjen noudattaminen ja turvallisuusasiat vaikuttavat kuitenkin nykytekniikalla ylitsepääsemättömiltä vaikeuksilta.

Toinen asiaa mutkistava tekijä on se, että tiedot yhteenlasketuista tienkäyttömaksuista ja etäisyyksistä palvelevat ensisijaista prosessia ainoastaan, mikäli kaikki toimii odotusten mukaisesti.
Huomattava osa käyttäjistä vaatii tienkäyttömaksunsa hyväksyäkseen tarkasti eritellyn laskun. Ajoneuvolaitteen (OBE) oikeille mittaustuloksille (erityisesti satelliittipaikantimen toiminnalle) tai laskutusprosessin virheettömälle toiminnalle ei voida antaa absoluuttista takuuta. Käyttäjällä tulisi laskutusvirheiden varalta olla käytössään lisäinformaatiota. Tämän informaation tulisi olla koskematonta ja luotettavaa, jotta sitä voidaan käyttää todisteena valituksen tai muutoksenhaun yhteydessä. Tämä onnistuu käyttäjän käytössä olevan digitaalisesti allekirjoitetun "käyttäjälokin" avulla, jollaista esitettiin käytettäväksi myös Alankomaiden tiemaksuhankkeen yhteydessä. Konseptin ja käyttäjävalvontaa koskevan näkemyksen vahvistamiseksi, henkilötietojen käsittelijän ei tulisi koskaan päästä käsiksi näihin tietoihin ilman käyttäjän nimenomaista pyyntöä. Ajoneuvolaitteen (OBE) haltijalla tulisi myös olla mahdollisuus poistaa tiedot kokonaan tai osittain käyttäjälokissa.

Sofia Memorandumin toteamuksiin koskien “smart client” –lähestymistapaa ei ole paljoa lisättävää:

”Yksilöiden yksityisyyden varmistamisen kannalta selvästi tarkoituksenmukaisin järjestelmä olisi sellainen, missä tienkäyttömaksuihin liittyvää tietoa käsiteltäisiin ainoastaan käyttäjän valvonnassa. Tässä tapauksessa ajoneuvolaite (ns. älykäs laite) laskisi tienkäyttömaksun ja keskusjärjestelmälle toimitettaisiin vain tietoa loppusummasta. Ajoneuvolaite siis suorittaisi kaikki veloitusprosessin kannalta kriittiset vaiheet: ajoneuvon sijainnin määrityksen, tieosuuden ja sitä vastaavan kilometritaksan määrittämisen sekä tieosuudelta koituvan maksun ja kokonaissumman laskennat.

Kuljettajan anonymiteetti siis säilytettäisiin, sillä kaikki sijaintia ja matka-aikaa koskeva tieto pidettäisiin yksin käyttäjän hallinnassa. Käyttäjien henkilöllisyys paljastuisi ainoastaan eräissä poikkeustapauksissa, esimerkiksi kun käyttäjä ei ole maksanut oikein laskettua tienkäyttömaksua, ajoneuvo on varastettu, käyttäjän ajoneuvolaite on rikki tai siinä on toimintahäiriö (ajettaessa maksullisella tieosuudella). Keskusjärjestelmän tarvitsee ainoastaan varmistaa, että tienkäyttömaksun laskeva ajoneuvolaite toimii oikein maksullisilla tieosuuksilla.

Vaikka “smart client” –lähestymistapa näyttäisi olevan ns. “thin client” vaihtoehtoa kalliimpi ratkaisu, on siinä myös tiettyjä taloudellisia etuja: älykäs ajoneuvolaite ei ole altis yhteyshäiriöille (esim. matkapuhelinverkon ulkopuoliset alueet), ja vaikka keskusjärjestelmä olisi tilapäisesti pois toiminnasta, kyetään tienkäyttömaksu silti laskemaan. Toisaalta, jatkuvasti dataa keskusjärjestelmälle lähettävä ja keskusjärjestelmän laskentaan nojaava ajoneuvolaite (“thin client” –ratkaisu) ei voi laskea itse tienkäyttömaksuja , mikäli matkapuhelinverkon kuuluvuus on heikko tai keskusjärjestelmä on pois toiminnasta.

Työryhmän mielestä henkilötietojen keskitetty käsittely tienkäytön hinnoittelussa vapaassa liikennevirrassa ei ole tarpeellista, joten sitä ei voida suhteellisuusperiaatteen mukaan pitää oikeutettuna. Tämä edellyttää, että on olemassa todennettuja teknologisia ratkaisuja, jotka eivät vaadi henkilötietojen käsittelyä keskitetysti.”

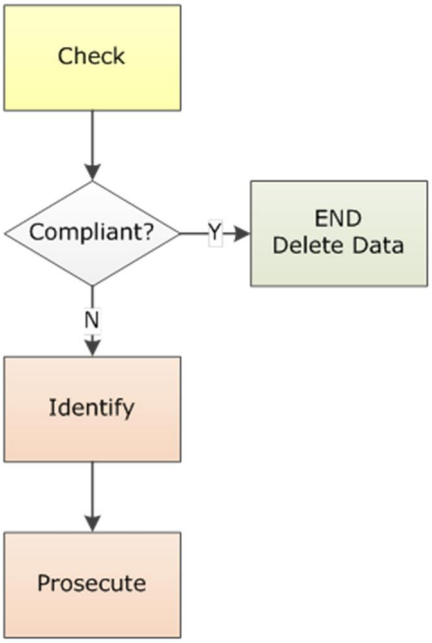
6.5 Yksityisyyden suunnitteleminen valvontaprosessiin

Traditionalisissa järjestelmissä on kori, johon tiemaksun voi maksaa kolikoilla. Jos oikea summa on maksettu, sulkupuomi avautuu. Jos puomia ei olisi, niin harva maksaisi.

Sähköisessä maksunperinnässä tämä kolikoiden käsittely on automatisoitu. Ajoneuvolaite (OBE) maksaa oikean summan virtuaalisesti käyttäjän puolesta – vain puomi puuttuu! Ajoneuvolaite (OBE) ei pysäytä ajoneuvoa, vaikka käyttäjän varat olisivat lopussa tai satelliittivastaanotin (GNSS) olisi kytketty pois toiminnasta. Kuvainnollinen puomi täytyy siis toteuttaa toisella tavalla – valvontajärjestelmän avulla.

Valvontaprosessi käsittää kolme vaihetta:

1. Valvo sääntöjen noudattamista
2. Tunnista ajoneuvo tai käyttäjä epäiltäessä rikkomusta
3. Nosta syyte ajoneuvon omistajaa tai käyttäjää vastaan rikkomuksen todentamisen ja käyttäjän tunnistamisen jälkeen



Tienkäytön hinnoittelun valvontaprosessi

Ensimmäinen vaihe ei edellytä käyttäjän tunnistamista. Sääntöjen noudattamisen tarkistamisessa tarkistetaan ensin ajoneuvolaitteen (OBE) toiminta ja sitten suoritetaan yksinkertainen vertausprosessi, jossa ajoneuvolaitteen tuottamaa dataa verrataan toisesta, itsenäisestä lähteestä saatuun havaintoon. Ajoneuvolaite esimerkiksi ilmoittaa tiedon tietystä ajoneuvoluokasta, sijainnista tai maksuvyöhykkeestä. Yleensä toinen, itsenäinen havainto saadaan tien päältä, joko automaattiselta valvonta-asemalta tai valvontapartiolta. On huomattava, että sääntöjen noudattamisen tarkistaminen ei edellytä käyttäjän tunnistamista. Ajoneuvon tunnistamisella on merkitystä vain tietyissä tapauksissa, kuten tarkistettaessa, että ajoneuvolaite on sijoitettu oikeaan ajoneuvoon. Jos ajoneuvolaitteen todetaan olevan toimintakuntoinen (esim. vastaa lyhyen kantaman tiedonsiirrolla (DSRC) tehtyyn yhteydenottoon), eikä vertailussa havaita poikkeamia laitteen antaman tiedon ja havainnon välillä, päättyy valvontaprosessi tähän. Prosessin toista vaihetta, eli ajoneuvon tai käyttäjän tunnistusta, tarvitaan vain epäiltäessä rikkomusta.

Periaate käsiteltävän datan minimoinnista pätee: sääntöjen noudattamisen tarkistuksessa käyttäjää tai ajoneuvoa ei tulisi tunnistaa, paitsi maksujärjestelmän vaatimissa erityistapauksissa. Kaikki tiedot sääntöjä noudattavista käyttäjistä tulee poistaa välittömästi tarkastuksen jälkeen. Ennen kaikkea tietoja ei tule välittää keskukseen. Jos tietoja lähetetään keskuspalvelimelle esimerkiksi tilastointitarkoituksessa, tulee niiden olla täysin anonymisoituja.

Sofia Memorandum päätyy pääpiirteittäin samoihin päätelmiin:

“Kuljettajan henkilöllisyyttä ei saa selvittää, jollei ole todisteita, että hän olisi tehnyt jotain rikkomukseksi luokiteltavaa. Kyse voi olla tienkäyttömaksujen käyttöehtojen rikkomisesta tai jostakin muusta rikkeestä. Suhteellisuusperiaatetta tulee kunnioittaa, toisin sanoen ensiksi tulee näyttää toteen, että ajoneuvolaite on ajoneuvossa ja se toimii virheettömästi. Jos valvontajärjestelmä ei havaitse rikkeitä laitteen sijoittamisessa ajoneuvoon tai ongelmia sen toiminnassa, ei toimenpiteisiin laitteen tai kuljettajan tunnistamiseksi tule ryhtyä. Valvontatahon tulee ryhtyä suhteellisuusperiaatteen mukaan toimiin vain, jos valvontajärjestelmä toteaa laitteen puuttuvan, virheellisen toiminnan tai laitteeseen mahdollisesti tehdyn virheellisen asetuksen. Komission käyttämien asiantuntijaryhmien selontekojen mukaan rekisterikilven tunnistus ja sitä kautta yksittäisen kuljettajan tai omistajan tunnistaminen on tällöin hyväksyttävä

valvontamenetelmä. Huomioiden kaikki edellä mainittu, niiden kuljettajien, jotka eivät ole tehneet mitään rikkomuksia, henkilötietoja ei tule käsitellä millään tavalla, paitsi asianomaisen kuljettajan toimesta. Tämän lähestymistavan mukaan valvontakeskus tarkistaisi vain ajoneuvolaitteen oikean toiminnan, ja vain valtuutettu henkilö (ja ainoastaan siinä tarkoituksessa, mihin valtuutus henkilötietoihin pääsyyn on myönnetty) voi pyytää yksilön tunnistamista tai informaatiota ajoneuvon sijainnista. Tämä sallitaan vain etukäteen määritellyissä tilanteissa (esimerkiksi jos ajoneuvolaitetta on peukaloitu, jos laite ei toimi maksullista tietä käytettäessä tai jos ajoneuvo on varastettu). Jokainen valvontatarkoituksessa tehty sijaintia, matka-aikaa tai tietulleja koskevan informaation käyttö tulee tallentaa asianmukaisesti. Tallennetut lokitiedot tulee pystyä jäljittämään aitoina ja kokonaisuudessaan. Olisi epäsuotavaa sallia luvaton ja rekisteröimätön pääsy laitteessa oleviin tietoihin.”

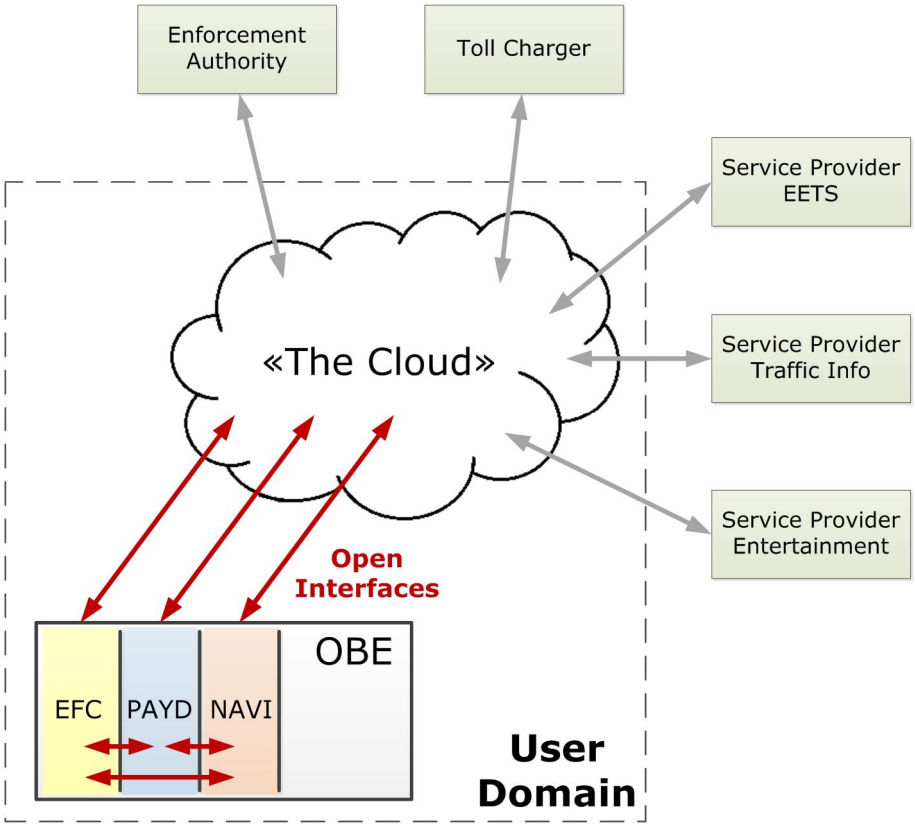
6.6 Yksityisyyden suojan suunnitteleminen avoimiin palvelumarkkinoihin

Asiat muuttuvat vähemmän suoraviivaisiksi, kun tiemaksupalvelu tarjotaan yhtenä palveluna monesta avoimessa palveluympäristössä. Ääritapauksessa käyttäjä saattaa hankkia kaikki laitteet ja sovellukset eri toimittajilta. On kuviteltavissa, että jotta ajoneuvojen telemaattisten laitteiden ja palveluiden markkinat syntyvät, tarvitaan jotain samankaltaista kuin älypuhelinmarkkinat. Älypuhelinten tapauksessa käyttäjä ostaa laitealustan, jonka jälkeen markkinoilla on tarjolla ohjelmistoja ja palveluita (apps). Tämä on ilmiselvästi nykyaikainen avoin palvelualusta, mutta siihen liittyvät yksityisyyden kysymykset ovat pitkälti ratkaisematta. Kun käyttäjät asentavat sovelluksia (appseja), he muodollisesti hyväksyvät sopimusehdot muutamalla klikkauksella yleensä lukematta niitä. Tämä tuskin täyttää tietosuojadirektiivin vaatimusta "rekisteröidyn suostumuksesta" eli kaikenlainen vapaaehtoinen, yksilöity ja tietoinen tahdon ilmaisu, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn. Ihmiset ovat itse asiassa hyvin tietoisia siitä, että heitä koskevia tietoja kerätään ja käytetään esim. suoramarkkinointiin. Esim. Google-haku näyttää eri ihmiselle eri tuloksia samalle haulle, riippuen käyttäjän aikaisemmasta käyttöhistoriasta ja kiinnostuksen kohteista. Ihmiset hyväksyvät tällaisen yksityisyyden loukkaamisen, koska palvelun hyödyt ovat suuremmat kuin tuo pieni kiusa tulla rekisteröidyksi joka internet-vierailun yhteydessä.

Tienkäyttömaksu ei ole sovellus, jonka käyttäjä voi valita vapaaehtoisesti. Se on pakollinen ja siksi käyttäjä on paljon kriittisempi suhteessa yksityisyytensä säilyttämiseen, kuten esimerkit Alankomaista ja Yhdistyneistä Kuningaskunnista ovat osoittaneet.

Siksi tieto, jota tarvitaan tienkäyttömaksujen perimiseen, erityisesti yksityiskohtainen reittitieto, tulee prosessoida käyttäjän valvonnassa. Ainoastaan koostettu tieto saisi jättää käyttäjän hallitseman alueen ja siirtyä keskusjärjestelmään. Tämä ei tarkoita, että kaiken tiedon tulisi jäädä ajoneuvolaitteeseen. Käyttäjän hallitsemaa aluetta voidaan hyvinkin laajentaa pilveen, jos se suojataan hyvin, esim. kryptaamalla.

Käyttäjä antaa pääsyn tietoonsa tai osaan siitä vain niille osapuolille ja niihin tarkoituksiin, joihin hän antaa suostumuksensa. Tietojen antamisen tarkoituksena voi olla esim. yksilöidyn laskun kirjoitus tai tietojen toimittaminen palveluntarjoajalle kalustonhallintasovellusta varten, tai koostetun tiedon lähettäminen, kuten päivittäinen ajosuorite, vakuutusyhtiölle pay-as-you-drive vakuutusta varten. Tämä kaikki on täysin mahdollista eikä ole syytä, miksi ei sovellettaisi tällaista laajennettua ”älykäs ajoneuvolaite” -konseptia, kun kyseessä on henkilöautot. Kaikki tähän asti toteutetut laajat satelliittipaikannuspohjaiset tienkäyttömaksujärjestelmät (jotka eivät kuitenkaan ole laajoja koko verkon maksuihin nähden) ovat koskeneet pelkästään raskaita ajoneuvoja, joiden kohdalla yksityisyydellä on aivan toisenlainen merkitys.



Data may remain under full user control, be they on-board or in the cloud

Älykkääseen ajoneuvolaitteeseen pohjautuvassa arkkitehtuurissa on keskeistä, että tieto säilyy käyttäjän hallinnassa. On siten varmistettava, ettei ajoneuvolaite lähetä herkkää tietoa jollekin taholle käyttäjän tietämättä. Periaatteessa ajoneuvolaite voitaisiin sertifioida käyttäjätiedon suojausominaisuuksien osalta, mutta ohjelmistopäivitykset voivat vaarantaa tätä. Avoimessa markkinaympäristössä sertifiointi käy epäkäytännölliseksi, koska jokainen pieni ohjelmistomuutos aiheuttaa uudelleensertifioinnin. Vaikka ohjelmisto jaettaisiin kriittiseen ja vähemmän kriittiseen osaan, niin päivitykset ovat toistuvia. Kuten tiedämme PC:stä ja älypuhelimesta, ohjelmistopäivitykset ovat pikemminkin sääntö kuin poikkeus.

Laitteiden sertifiointi ei siis tähän auta, mutta avoimet ja standardoidut rajapinnat kylläkin. Jos rajapinta ajoneuvolaitteen ja pilven välillä on avoimesti määritelty ja kuka tahansa asiantuntija voi tarkistaa rajapinnan turvallisuusmäärittelyt, käyttäjän tietoa voidaan välittää vain kyseisellä avoimella tavalla eikä takaovien kautta. Standardointi on tässä keskeisessä asemassa.

7. Suositukset

7.1 Sofia Memorandumin suositukset koskien tiemaksuja ja yksityisyyttä

Päällimmäisin suositus on seurata IWGDPT työryhmän nimenomaisia suuntaviivoja. IWGDTP on kansallisten tietosuojavaltuutettujen muodostama kansainvälinen työryhmä. Suositukset koskevat nimenomaan laajoja järjestelmiä, ja erityisesti kansallisia maksujärjestelmiä, jos ne liittyvät henkilöautoihin. Raportti on laajasti tunnettu ja arvossapidetty, koska se heijastaa hyvin tietosuojaviranomaisten näkemyksiä koskien tietosuojaa tiemaksujen yhteydessä:

Työryhmä suosittelee, että henkilötietoja käsitteleviä laajoja tiemaksujärjestelmiä valmisteltaessa tulisi noudattaa seuraavia suosituksia, jotka on suunniteltu suojaamaan kuljettajien ja ajoneuvojen omistajien yksityisyyttä:

- Kuljettajan anonymiteettiä pitää ja voidaan säilyttää soveltamalla ”älykäs ajoneuvolaite” -konseptia tai anonyymejä välityspalvelimia, jotka pitävät henkilökohtaiset tiedot käyttäjän hallinnassa ja jotka eivät edellytä paikannustietojen säilyttämistä muualla
- Tiemaksujärjestelmät tulisi suunnitella siten, että yksityiskohtainen matkatieto kokonaan ja lopullisesti hävitetään koko järjestelmästä, kun maksut on hoidettu, jotta estetään matkustusprofiilien luominen tai toimintojen liukuminen uusiin toiminnallisuuksiin
- Henkilökohtaisten tietojen käsittely muihin tarkoituksiin (kuten pay-as-you-drive vakuutukseen tai käyttäjäprofiiliin pohjautuvaan mainostamiseen) tulisi olla mahdollista vain käyttäjän selkeällä ja yksiselitteisellä suostumuksella.

Mitä tulee valvontaan, niin järjestelmän ei tulisi ottaa selville ajoneuvon kuljettajan tai omistajan henkilöllisyyttä, ellei ole todisteita siitä, että kuljettaja on tehnyt jotain, joka on määritelty rikkomukseksi tiemaksujärjestelmää kohtaan.

7.2 Suositukset koskien avoimen palveluympäristön arkkitehtuuria

Jos tiemaksujärjestelmä toteutetaan kokonaan viranomaisen hallinnassa, Sofia Memorandumin suositukset toimivat erinomaisina ohjeina järjestelmän suunnittelulle. Tekniset haasteet säilyvät, mutta ne voidaan hallita käytettävissä olevalla tekniikalla. Tässä ei ole tarkoitus käsitellä yksityiskohtaisia suunnitteluratkaisuja, mutta parhaita lähestymistapoja etsiessä Alankomaiden ”Kilometerheffing” -hanke on edelleen paras referenssi.
Ajanmukaisessa avoimessa palveluympäristössä prosessoinnin tulisi tapahtua ”älykäs ajoneuvolaite” paradigman mukaisesti kokonaan käyttäjän hallinnassa. Tämä ei tarkoita, että kaiken prosessoinnin tulisi tapahtua ajoneuvolaitteessa. Käyttäjän hallitsema alue voi hyvinkin ulottua pilveen, jos käyttäjän tietoja suojataan asianmukaisella kryptauksella. Tämä antaa käyttäjälle täyden vallan päättää, mihin tarkoituksiin hän antaa häntä koskevat tiedot käytettäväksi ja samalla tämä mahdollistaa ITS palvelumarkkinoiden synnyttämisen. Ehtona tällöin on, ettei ajoneuvolaitteeseen voida ohjelmoida ”takaovia”, joiden kautta tietoja voidaan ammentaa käyttäjän tietämättä. Tätä voidaan välttää sillä, että kaikki rajapinnat ohjelmoidaan avoimiksi, jolloin ne ovat kenen tahansa kiinnostuneen tutkisteltavissa. Samaa avoimuutta vaaditaan rajapintojen ohjelmistoilta eli ajureilta. Näiden tulee olla läpinäkyviä ja siksi perustua avoimeen lähdekoodiin – avointa tutkiskelua varten.

Avoimen palveluympäristön ollessa kyseessä, tarvitaan vain yksi lisäsuositus Sofia Memorandumiin nähden:

- Kaikkien käyttäjälaitteen rajapintojen tulisi perustua avoimiin rajapintamäärittelyihin ja rajapintojen ajurien tulisi perustua avoimeen lähdekoodiin.

7.3 Johtopäätökset

Tienkäyttömaksut ovat hyvin herkkiä tietosuojan suhteen. Yksinkertaisesti sanottuna tämä johtuu siitä, että tiemaksuissa on kyse siitä ”kuka oli missä milloin sekä siitä veloittamisesta”. Suuri yleisö on valppaana siitä, kuinka yksityiskohtaista reittitietoa käsitellään. Kukan ei halua tulla jäljitetyksi tai kuljettaa ”vakoojaa” ajoneuvossaan.

Reittitietoa on käsiteltävä henkilökohtaisena informaationa jopa nimettömänä. Kun tunnetaan päivittäinen reitti, henkilö on helposti tunnistettavissa kuten myös missä hän asuu, työpaikka, mieluinen ostoskeskus, mahdolliset vierailut sairaalassa, kirkossa, poliittisessa kokouksessa jne.

Tällaista tietoa on kaikissa tilanteissa suojattava, eikä vähiten sen takia, että yksityisyyden rikkominen tai edes kuviteltu rikkominen julkisuushälyn seuraamana on vahvasti myötävaikuttanut kaatamaan hankkeita, kuten esimerkit osoittavat.

On siten suositeltavaa suunnitella tiemaksujärjestelmää alusta alkaen yksityisyyden turvaamista silmälläpitäen. Tämä suositus ei ole tietonörtin, vaan sen tulisi olla normaalisti noudatettava hyvä käytäntö (good practice). Yksityisyyden suojanäkökulmat eivät johda monimutkaisiin ratkaisuihin, jos ne alun perin otetaan mukaan suunniteluun integroituna elementtinä.

Voidaan antaa seuraavat suositukset:

- Tulisi noudattaa ”älykäs ajoneuvolaite” (smart client) -konseptia, jossa data säilytetään hajautetusti ja pysyy käyttäjän hallinnassa riippumatta siitä, säilytetäänkö ne ajoneuvolaitteessa vai pilvessä
- Yksityiskohtainen reittitieto tulee tuhota heti, kun sitä ei enää tarvita
- Tietojen käyttäminen muihin tarkoituksiin (esim. "pay-as-you-drive” vakuutukseen), tulisi olla mahdollista vain käyttäjän selkeällä ja yksiselitteisellä suostumuksella
- Valvonnassa käyttäjän henkilöllisyyttä tulisi selvittää vain, jos on todisteita väärinkäytöksestä
- Kaikkien käyttäjälaitteen rajapintojen tulisi perustua avoimiin määrittelyihin ja rajapintojen ajurien tulisi perustua avoimeen lähdekoodiin.

Voidaan päättää seuraavalla lainauksella Sofia Memorandumista:

”Yksityisyyden tietosuojan perusperiaatteita on pyrkimys säilyttää kuljettajan yksityisyys ja teknologiaa pitäisi ja voidaan soveltaa siten, että se suojaa henkilöllisyyttä. Jokainen poikkeama tästä periaatteesta merkitsisi taas uutta loukkausta informaatioyhteiskunnan jo heikentämää yksityisyyttä kohtaan.

Työstettäessä jatkossa järjestelmäarkkitehtuuria noudattaen ”Yksityisyys suunnittelemalla” (Privacy by Design) paradigmaa, huomio tulisi olla kohdistettuna siihen, missä tiedot säilytetään ja käsitellään ja kenen toimesta, rajapintojen tunnistamiseen, tietovirtojen määrittelyyn sekä tiedon suojaamiseen.

8. Lyhenteet

ANPR	Automatic Number Plate Reading
BAG	Bundesamt für Güterverkehr (German Federal Office for Goods Transport)
CN	Cellular Network (e.g. GSM or UMTS)
CNIL	Commission nationale de l'informatique et des libertés (French data protection authority)
DSRC	Dedicated Short-Range Communication
EETS	European Electronic Toll Service (as defined by Interoperability Directive 2004/52/EC)
EFC	Electronic Fee Collection
EU	European Union
GNSS	Global Navigation Satellite System (such as GPS and GALILEO)
GPS	Global Positioning System (US satellite-based positioning system)
GSM	Global System of Mobile communications
ICT	Information and Communication Technology
IP	Internet Protocol
IT	Information Technology
ITS	Intelligent Transport Systems (synonymous to Traffic Telematics)
IWGDPT	International Working Group for Data Protection in Telecommunications
LSVA	Leistungsabhängige SchwerVerkehrsAbgabe (Distance-dependent heavy vehicles fee)
MIT	Massachusetts Institute of Technology
OBE	On-Board Equipment
OECD	Organisation for Economic Cooperation and Development
PAYD	Pay-As-You-Drive (insurance)
PC	Personal Computer
PET	Privacy Enhancing Technology
RFID	Radio-Frequency Identification
VAS	Value Added Service

9. Lähteet

Communications Privacy Directive, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector

Data Protection Directive, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Data Retention Directive, Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

EETS Decision, Commission Decision of 6 October 2009 on the definition of the European Electronic Toll Service and its technical elements

EU Fundamental Rights Charter, Charter of fundamental rights of the European Union, Official Journal of the European Communities, 18 Dec. 2000, 364/01

Interoperability Directive, Directive 2004/52/EC of the European Parliament and of the Council of 29 April 2004 on the interoperability of electronic road toll systems in the Community

ITS Directive, Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport

ITS & Personal Data Protection, ITS Action Plan – ITS & Personal Data Protection, Final Report, Study by Algoé/Rapp Trans AG (Stefan Eisses, Tom van de Ven, Alexandre Fievée) for the European Commission Directorate-General Mobility and Transport, Oct 2012, http://ec.europa.eu/transport/themes/its/studies/its_en.htm

Keolis Case, Délibération n°2009-002 du 20 janvier 2009 de la formation restreinte prononçant un avertissement à l'encontre de la société KEOLIS RENNES; CNIL, France; January 2009

MIT Location Privacy Study, Unique in the Crowd: The privacy bounds of human mobility, by Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen and Vincent D. Blondel, Scientific Reports Volume 3 / 1376, http://www.nature.com/srep/2013/130325/srep01376/ full/srep01376.html

OECD Recommendations, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, The Organization for Economic Co-Operation and Development, January 1999 (updated) http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

PET Communication, Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs), COM(2007) 228 final, Brussels, 2.5.2007

Proposed Data Protection Regulation, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25.1.2012, COM(2012) 11 final

Road Pricing Act NL, Regels voor het in rekening brengen van een gebruiksafhakelijke prijs voor het rijden met een motorvoertuig (Wet kilometerprijs), November 2009, http://www.rijksoverheid.nl/documenten-enpublicaties/kamerstukken/2009/11/13/200910898-aanbieding-documenten-wetkilometerprijs.html

Sofia Memorandum, Report and Guidance on Road Pricing – "Sofia Memorandum", 45th meeting of the IWGDPT, 12-13 March 2009, Sofia (Bulgaria), http://www.datenschutz-berlin.de/attachments/647/WP_Road_Pricing_Final_675.38.12.pdf

TFEU Treaty on the functioning of the European Union, Official Journal of the European Union, 9 May 2008.

TomTom Case, Rapport van bevindingen - Ambtshalve onderzoek CBP naar de verwerking van geolocatiegegevens door TomTom N.V., College Bescherming Persoonsgegevens (NL), December 2011