

17.10.2017

Effi ry:n lausunto luonnokseen "Satelliittinavigointijärjestelmien tehokas hyödyntäminen Suomessa"

Viite: [Lausuntopyyntö luonnoksesta satelliittinavigointijärjestelmien tehokas hyödyntäminen Suomessa - toimenpideohjelma 2017 – 2020 \(LVM/1737/02/2017\)](#)

Johdanto	1
EU:n European Electronic Toll Service -hanke	2
eCall	3
Tietoturva ja tietosuoja	3
Tietoturva	3
Tietosuoja	4

Johdanto

Effi ry kiittää LVM:n tavaksi tullutta käytäntöä antaa kansalaisjärjestöille mahdollisuus lausua käsiteltävästä asiasta aikaisin jo luonnosvaiheessa.

Luonnoksessa esitettyyn satelliittinavigointijärjestelmien hyödyntämisen toimenpideohjelmaan, ja siinä esitettyihin 14 toimenpide-ehdotukseen, **Effi suhtautuu yleisesti ottaen myönteisesti.** On positiivista huomata, että LVM seuraa teknistä kehitystä ja varautuu kehityksen mukanaan tuomiin mullistuksiin ja haasteisiin. Effi painottaa, että teknologian kehittyessä julkisella vallalla tulee olla ensisijaisesti tarpeettomia esteitä raivaava rooli. Julkisen vallan ei tule yleensä olla määrittämässä teknologian kehityssuuntia. Julkisen vallan ei tule myöskään juosta hypen mukana tuuliviirin lailla vaan reagoida kehitykseen, jolla on konkreettista substanssia.

Kappaleessa 2.4 on käsitelty sijaintitietoa yksityisyyden ja henkilötietojen suojan kannalta. Siinä todetaan selkeästi, että *"sijaintitieto on siis henkilötieto, jos se voidaan suoraan tai epäsuorasti yhdistää luonnolliseen henkilöön"*.

Effi kannattaa tätä määritelmää, ja on hyvä nähdä, että tämä on sanottu näin selkeästi. Joskus kuulee esitettävän myös suppeampia kantoja, joissa jotain sijaintitietoja ei mielletä henkilötiedoiksi, koska niissä ei ole mukana esimerkiksi henkilön nimeä tai henkilötunnusta - tai rekisterinumeroa. Tämä on kuitenkin virheellinen ajattelutapa: Myös täysin anonyymit tiedot voivat muodostua henkilötiedoiksi, jos useiden havaintojen tiedetään liittyvän samaan henkilöön. Esimerkiksi auton paikannustiedoista on yleensä varsin helppo päätellä, kenen autosta on kyse. Jos tätä tosiasiaa ei myönnettäisi, joudutaan yksityisyyden suojan ja perusoikeuksien kannalta heti väärälle polulle. Luonnoksessa esitetystä selkeästä periaatteesta on siis tärkeää pitää jatkossakin kiinni!

Erityisesti on huomattava, että yksityisyys voi vaarantua jopa epäsuorasti, vaikka sovellus sinänsä ei raportoi käyttäjän sijaintitietoja palvelimelle päin. Esimerkiksi jos auton päätelaite hakee palvelimelta tietyn tieosuuden ruuhkatietoja, voidaan käytännössä päätellä, että auto liikkuu kyseisellä tiellä.

Kappaleessa 4.4 on nykytilan arvioinnissa mainittu EU:n European Electronic Toll Service -hanke. Kyseessä on auton paikannukseen perustuva tienkäyttömaksujen keruujärjestelmä, joka olisi standardoitu koko EU:ssa. Samassa kappaleessa on myös ennustettu paikannusta käyttävän automaattisen hätäpuhelukeskityksen eCallin leviämistä, kuten myös raskaan liikenteen digitaalisen ajopiirturin yleistymistä.

Autojen paikannus ja juurikin samat hankkeet ja teknologiat, olivat viimeksi puheenaiheena Liikenneverkko-yhtiön (LIVE) perustamista käsitelleessä luonnoksessa (1/2017).

Vaikka autojen paikannukseen tai tienkäyttömaksuihin ei nyt käsillä olevassa selonteossa liitykään mitään erityistä toimenpide-ehdotusta, haluamme tässä yhteydessä lausua niihin liittyen joitakin kannanottoja, sekä myös yleisiä paikannustietoihin liittyviä tietoturvan ja tietosuojan hyviä periaatteita. Toivomme, että näistä periaatteista on LVM:lle hyötyä tässä ja vastaavissa tulevaisuuden hankkeissa, ja että niiden muistaminen tulevat näkymään tietoturvan ja tietosuojan yhä konkreettisempina läsnäolona kaikissa hankkeissa.

EU:n European Electronic Toll Service -hanke

Muun muassa taannoisesta LIVE-raportista olemme saaneet käsityksen, että EU:n Komission tavoite olisi siirtyä tienkäyttömaksuissa täysin kilometripohjaiseen hinnoitteluun, ja luopua kokonaan aikaperusteisista ns. vinjettimaksuista. Samoin saimme käsityksen, että Suomi olisi ainakin jonkin verran vastustanut tällaista suuntausta.

Myös **Effi vastustaa kaikkia hankkeita, joissa jonkinlainen paikannus on välttämätön edellytys julkisella tiellä liikkumiseen**. Suomen kanta tulee olla, että aina on tarjottava myös aikaan perustuvaa vaihtoehtoa. Suomi voisi EU:n suuntaan myös terävöittää kantaansa, esittämällä, että kyseessä on **perusoikeuskysymys**.

Sikäli kun paikannusta vaativia ratkaisuja otetaan käyttöön, tulee niiden noudattaa alla tarkemmin esitettyjä tietosuojaan hyviä periaatteita. Esimerkiksi ei ole missään olosuhteissa perusteltua standardoida, tai edes sallia, järjestelmiä, joissa tiellä liikkuvien kansalaisten sijaintitietoja raportoidaan viranomaisten palvelimille.

eCall

Myös eCall:n kaltaisille pakollisille erikoissovelluksille on oltava suhteellisuusperiaatteen mukainen välttämättömyysperuste. Perusteeksi ei riitä vain se, että uusi teknologia on olemassa.

Effi muistuttaa, että pakollinen eCall on poikkeus yksityisyydensuojaan, jota on perusteltu eCall:n suurella vaikutuksella liikennekuolemiin. Käyttötarkoitussidonnaisuudesta seuraa, että eCall-teknologiaa ei voi soveltaa muuhun kuin henkilövahinkoja vähentäviin tarkoituksiin. Jos osoittautuu, että Komission esittämät arviot eCall:n hyödyistä olivat ylimitoitettuja, koko eCall:n pakollisuutta on arvioitava uudelleen.

eCall järjestelmän tuloa uusiin autoihin joskus käytetään myös oikeutuksena muiden järjestelmien käyttöönotolle. Koska autossa on jo eCall, joka käyttää paikannusta, niin uudestakaan sovelluksesta ei voi olla mitään haittaa. Tässä kohtaa on syytä huomata, että eCall standardin laitteisto on selkeästi rajattu omaan käyttötarkoitukseensa: hätäilmoituksen tekemiseen. Suurin osa autoista ei koskaan tule edes käyttämään tätä toimintoa. On siis väärin verrata eCall-järjestelmää muihin sovelluksiin, jotka esimerkiksi aikoisivat tallentaa kansalaisen olinpaikan jokaisella hetkellä.

Tietoturva ja tietosuoja

- Tietoturva ja tietosuoja ovat suhteessa toisiinsa
 - Tietoturvalla käytännössä voidaan suojata yksityisiä tietoja
 - Siinä missä tietoturvalla pyritään estämään vahinkojen tapahtuminen, voidaan hyvillä tietosuojakäytännöillä minimoida vahinko, sitten kun se kuitenkin tapahtuu.
 - Toisaalta tietoturva on laajempi käsite. Kun autot ja muut liikennevälineet kytkeytyvät enenevässä määrin tietoverkkoihin, voi puutteellinen tietoturva johtaa jopa fyysisiin uhkakuviin, jos vaikkapa hakkerin on mahdollista päästä etäohjaamaan autoa, esimerkiksi siihen jälkiasennetun tienkäyttömaksulaitteen kautta.¹

¹ <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>

Tietoturva

- Tietoturva on suhteellista
 - Järjestelmissä on aina tietoturva-aukkoja. Toisissa enemmän, toisissa vähemmän.
 - Tietoturvaan panostetaan **riskianalyysin** mukaan: kuinka arvokasta tietoa suojellaan, ja ketä hyökkääjää vastaan. Esimerkiksi koko EU:ssa käytetty tietojärjestelmä on lähtökohtaisesti houkuttelevampi kohde kuin jonkun pienen startupin järjestelmä, ja aiheutettu vahinkokin laajempi.
 - Lähtökohta kuitenkin on, että ennemmin tai myöhemmin tietoturva-aukkoja löytyy. Tällöin huomio kohdistuu siihen, mitä vahinkoa silloin seuraa.
- Tietoturva on kokonaisuus
 - Kyse on turvallisista **prosesseista** ja käytännöistä, ei vain tuotteen ominaisuuksista ja aukoista.
 - Esimerkiksi myös kiinnijäämisen riski ja rangaistus vaikuttavat siihen, että tietoturvaongelma ei välttämättä realisoidu, vaikka aukkoja on.
- Järjestelmän tietoturva on yleensä sen **elinkaaren** ja vuorovaikutuksen tulos. Uudessa järjestelmässä on yleensä aukkoja, jotka sitten löydetään ja korjataan. (**lifecycle, maturity**)
 - Monissa uusissa paikannusteknologiaa hyödyntävissä hankkeissa, on pyritty ratkaisemaan myös olemassaolevan autokannan mukaan saaminen erilaisilla "mustilla laatikoilla". Nämä ovat tietoturvanäkökulmasta yleensä ongelmallisia, varsinkin jos musta laatikko sisältää mahdollisuuden internet-yhteyden luomiseen. Vanhojen autojen elektroniikkaa ei ole suunniteltu sillä lailla turvallisesti, että olisi huomioitu avoimen internetin kautta avautuvia tietoturvauhkia.
 - Alan relevantti termi on "**air gap**". Vanha autokanta pysyy turvallisena silloin kun sitä ei kytetä tietoverkkoihin ollenkaan.
- Tietoturva ja tietosuoja - erikseen - ovat omia **erikoisalojaan**
 - Tiivistettynä voidaan sanoa, että insinööri on hyvä rakentamaan tuotteen ja tietoturva-asiantuntija on hyvä rikkomaan sen.
 - Kun esimerkiksi paikannukseen liittyviä hankkeita LVM:n alaisuudessa tehdään, kannattaa jo pilotointivaiheessa erikseen pyytää mukaan tietoturva- ja tietosuoja-ammattilaisia. Lähtökohtaisesti ei tule olettaa, että esimerkiksi GPS:ää tai auton sulautettuja ohjelmistoja tuntevat insinöörit osaavat huomioida näitä näkökulmia.
 - **Kun tietoturvan ja suojan ammattilaiset ovat mukana myös teknisissä hankkeissa**, vältetään siltä kovin yleiseltä virheeltä, jossa periaatetasolla näihin on sitouduttu vahvastikin, mutta käytännön projekteissa aina välillä pääsevät unohtumaan tai yrityksestä huolimatta jäävät puutteellisiksi.

Tietosuoja

Seuraavassa on esitelty tietosuojan olennaisimmat periaatteet.

- **Minimointi**

- Tietoa kerätään vain siltä osin kuin se on **välttämätöntä** (suhteessa ilmoitettuun tavoitteeseen)
- Luovutetaan toiselle osapuolelle vain se tieto mikä on välttämätöntä
- Kerättyä tietoa **ei käytetä muihin tarkoituksiin** kuin mitä tarkoitusta varten se on tallennettu ja kuluttaja on **antanut suostumuksensa**
- **Anonymisoidaan** heti kun voidaan; ja
- **Tuhotaan (deletoidaan)** heti kun voidaan

- **Keskitetty ja hajautettu rekisteri**

- Tiedon keskittäminen (esimerkiksi suomalaiselle tai eurooppalaiselle viranomaiselle) luo aina haavoittuvamman järjestelmän, verrattuna siihen, että tieto on hajautetusti (esimerkiksi kussakin autossa)
- Paksu, eli älykäs, ajoneuvolaite sisältää itsessään tarpeeksi ohjelmistoa, jotta se voi laskea esimerkiksi paikkatietojensa perusteella, minkälainen maksu ajoneuvon haltijan tulee suorittaa. Viranomaisen keskitettyyn kantaan ilmoitetaan vain euromääräinen loppusumma.
- Ohut, eli tyhmä, ajoneuvolaite taas sisältää itsessään minimaaliset toiminnot esim GPS paikkatiedon keräämiseen, jotka sitten lähetetään keskitettyyn kantaan laskentaa varten.
- Ohut laite on siis tietosuojan kannalta olennaisesti huonompi vaihtoehto. Valitettavasti se on myös halvempi arkkitehtuuri toteuttaa. Viranomaisen tulee reguloinnilla ohjata, että hajautetun käsittelyn periaate toteutuu esimerkiksi paikkatietoja käsitellessä. Laitteiden ja järjestelmien toimittajia ei saa päästää standardoimaan heille edullisempia, mutta yksityisyyden suojan (eli perusoikeuksien kannalta) vaarallisempia vaihtoehtoja.

- **Sijaintitietoja sisältävä data**

- ...on lähtökohtaisesti aina henkilön tunnistamisen mahdollistavaa dataa, vaikka se ei sinänsä sisältäisi esimerkiksi sosiaaliturvatunnusta tai nimeä.
- Esimerkiksi voidaan helposti selvittää, missä osoitteessa auto on pysäköitynä joka yö.
- Yksityisyyttä voidaan loukata jo hyvin viattoman oloisilla tiedoilla. Esimerkiksi tieto siitä, että puolison auto on liikkunut naapurimaakunnan alueella, tai kilometrejä on kertynyt poikkeuksellisen paljon, voi loukata yksityisyyttä.
- Viime viikon julkisessa keskustelussa esitettiin lieventävänä argumenttina, että tietovuoto ei ollut vakava, koska data ei sisältänyt henkilön tunnistamistietoja. Tämä on väärä ja asiantuntematon, hankkeen uskottavuuden kannalta haitallinen kommentti.

- **Aggregointi**

- Tarkoittaa tietojen summausta, keskiarvoistamista, jne. Lopputuloksena on jalostettua tietoa, joka ei enää kerro yksittäisen henkilön yksityiskohtia.
- Otetaan esimerkiksi raskaan liikenteen tienkäyttömaksu: Sen sijaan, että jokainen auto ilmoittaa ajamansa kilometrimäärän - tai pelkän euromäärän - viranomaiselle, voidaan ajatella, että autot omistava logistiikkayhtiö kerää omien autojensa tiedot keskitetysti, ja tilittää viranomaisille yhtenä summana kaikkien autojensa tienkäyttömaksut. Näin viranomaiselle ei siirry yksittäisestä autosta yhtään mitään tietoa.
- **Valtion (ja EU:n) rooli** verrattuna yksityisiin yrityksiin
 - Valtiolle asetetaan tietosuojan suhteen korkeammat vaatimukset kuin markkinaehtoisesti toimiviin yrityksiin
 - Historiallisesti pahimmat perusoikeuksien loukkaukset ovat tapahtuneet valtioiden toimesta. Kansalaisuus ja esimerkiksi tiellä liikkuminen eivät ole samalla lailla vapaaehtoisia valintoja kuin esimerkiksi Facebookin tai Googlen käyttö.
 - On realistista, että lähitulevaisuudessa autot sisältävät jatkuvan paikannuksen toimintoja, varsinkin niiden muuttuessa itseohjautuviksi. Tulevaisuudessa enemmistö autoista varmaan raportoivat sijaintinsa reaaliaikaisesti auton valmistajalle, vakuutusyhtiölle, kännykkäoperaattorille ja Google Mapsille - ehkä myös HERE Mapsille.
 - Vaikka enemmistö kansalaisista tuleekin käyttämään tällaisia ratkaisuja, kaikki eivät tule, eikä valtio voi edellyttää sitä kansalaisilta. EU:n halu siirtyä pelkästään kilometripohjaisiin tienkäyttömaksuihin on siksi perusoikeusnäkökulmasta kestävä. Päinvastoin, EU:n tulisi sitoutua puolustamaan periaatetta, että EU:n kansalainen voi liikkua Euroopassa raportoimatta sijaintiaan koko ajan viranomaiselle.
 - Valtion tai EU:n ei myöskään tulisi aktiivisesti kannustaa tai luoda kannustimia kehitykselle, jossa kansalaiset "vapaaehtoisesti" luopuvat yksityisyydestään, esimerkiksi koska se on halvempaa.
 - Siltä osin kuin tulevaisuudenkuva realisoituu joka tapauksessa, valtionyhtiö voi sallia, että yksityiset tahot (Google, Tesla, jne) käyttävät paikkatietodataa, joka niillä joka tapauksessa on jo hallussaan, myös tienkäyttömaksun summan laskemiseen. Valtion ja EU:n tulee kuitenkin pysyä tämän kehityksen suhteen passiivisena ja neutraalina toimijana.
 - Regulaattorin roolissa julkisen vallan tulee ohjeistaa ja standardoida yksityisen sektorin toimijoiden järjestelmäsuunnittelua niin, että etäyhteydessäkin olevien ajoneuvojen käyttö on turvallista erittäin suurella varmuudella. Julkisen vallan tulee myös pidättäytyä asettamasta vaatimuksia, jotka tekisivät etäyhteyksistä välttämättömiä. Lähtökohtana tulee olla, että julkinen valta ei vaaranna kenenkään oikeutta liikkua etäyhteyksistä riippumatta.
- **Tietoliikenteen ja lokien anonymisointi ja minimointi**
 - Kun viranomaisella on tarjota maantieteelliseen sijaintiin liittyviä palveluja, vaikkapa sääätietoja, ruuhkatietoja, huoltoasemien sijaintitietoja, jne on hyvä huomata, että

tällainen palvelu voi epäsuorasti tulla keränneeksi kansalaisen sijaintitietoja, vaikka palvelun varsinainen tarkoitus ei olekaan paikantaa kansalaista (tai hänen autoaan).

- Esimerkiksi: Jos auton päätelaite hakee palvelimelta ruuhkatiedot ajamaltaan tieltä, ja päätelaitteeseen liittyy jokin yksilöivä tunniste (kuten ip-osoite!), tulee palvelin käytännössä keränneeksi kyseisen auton päivittäin ajamat matkat.
- Sijaintiin liittyviä palveluita tuleekin pyrkiä suunnittelemaan niin, että asiakas ei edes epäsuorasti paljasta sijaintiaan palvelimelle:
 - **Paikkatiedon minimointi:** Tiedon siirto voidaan toteuttaa niin, että päätelaite kopioi esimerkiksi koko Suomen tietopaketin, eikä vain oman tieosuutensa tietoja. Kun tietojen käsittely tapahtuu päätelaitteessa, ei palvelimelle jää tietoa missä päin Suomea kansalainen oli liikkeellä.
 - **Päätelaitteen anonymisointi:** Tietoliikenne voidaan ohjata esim välityspalvelimen kautta, tai broadcast-tyyppisesti niin, että päätelaite ei ollenkaan ota suoraa yhteyttä palvelimeen.
 - **Tuhoaminen:** Palvelun HTTP-palvelimen lokitiedot kannattaa tuhota huomattavasti tiheämmin kuin yleensä tehtäisiin, koska ne eivät ole palvelun kannalta olennaista tietoa.

Henrik Ingo
Effin asiantuntija
henrik.ingo@effi.org

Marko Santala
Effin asiantuntija