



Datum: 20 februari 2017

Onderwerp: Data uit voertuigen

“Data uit voertuigen” waar hebben we het over?

Werkgroep:

Leo Bingen (RAI Vereniging)

Wouter van Haaften (UvA)

Chris Huijboom (HAN)

Mike Pinckaers (ANWB)

Pierre van der Stokker (Beijer Automotive)

Opdrachtgever:

Joelle van den Broek (Ditcm)

Ronde Tafel Juridische Aspecten van Smart Mobility



| | |
|--|-----------|
| “DATA UIT VOERTUIGEN”, WAAR HEBBEN WE HET OVER? | 1 |
| 1. INLEIDING | 3 |
| 2. GEGEVENS UIT VOERTUIGEN | 3 |
| 2.1. VOERTUIGDATA | 4 |
| 2.1.1 INTERNE VOERTUIGSYSTEMEN | 4 |
| 2.1.1.1 DIAGNOSE-DATA, ALGEMEEN TOEGANKELIJK VIA EOBD/OBD2 | 4 |
| 2.1.1.2 PROPRIETARY DATA, BESLOTEN SENSORDATA VIA CAN-BUS | 5 |
| 2.1.2 ACHTERAF AANGEBRACHTE SYSTEMEN (AFTERMARKET) | 5 |
| 2.1.2.1 VOLLEDIG STAND ALONE | 5 |
| 2.1.2.2 AANGELOTEN OP DE OBD2 POORT | 6 |
| 2.1.2.3 ACHTERAF AANGEBRACHT MAAR RECHTSTREEKS OP DE CAN-BUS | 6 |
| 2.2 BESCHIKBAARHEID | 7 |
| 2.2.1 UITLEZEN ACHTERAF | 7 |
| 2.2.2. 'REAL-TIME' DATA-ONTVANGST | 7 |
| 2.3 JURIDISCHE ASPECTEN | 9 |
| 2.3.1 DATAPROTECTIE | 8 |
| 2.3.1.1 GEGEVENS DIE GÉÉN PERSOONSgegevens ZIJN | 8 |
| 2.3.1.2 PERSOONSgegevens | 8 |
| 2.3.1.2.1 INTERNE NETWERK (CAN-BUS) VAN DE AUTO | 8 |
| 2.3.1.2.2 ACHTERAF AANGEBRACHTE SYSTEMEN | 9 |
| 2.3.2 DATAZEGGENSCHAP | 10 |
| 2.3.2.1 DIAGNOSEgegevens | 9 |
| 2.3.2.2 OVERIGE VOERTUIGDATA | 9 |
| 2.3.3 AANSPRAKELIJKHEID | 11 |
| 3 VOORLOPIGE CONCLUSIES | 12 |



1. Inleiding

Systemen in moderne voertuigen produceren heden ten dage grote hoeveelheden data. Dat geldt voor zowel de personenauto, de bedrijfsauto als de motorfiets en zelfs de fiets. Deze data bieden een basis voor informatie over de conditie en het gebruik van het voertuig. Tevens bieden deze data, wanneer hiermee communicatie plaatsvindt met de omgeving, aanzienlijke mogelijkheden voor onder meer verkeersgeleiding, verkeersinformatie en incidentenmanagement; zowel nationaal als internationaal (Europees). Vanuit de private sector (o.a. autobranche en dienstverleners op gebied van mobiliteit) komen op grond van deze data uit voertuigen steeds meer (commerciële) diensten beschikbaar ten aanzien van het gebruik en conditie van het voertuig, zoals verkeersinformatie en attenderen voor onderhoud en reparatie en rijtaak-ondersteunende diensten in de after-market. De publieke sector (EU, nationale en lokale overheden) is zeer geïnteresseerd in de data uit voertuigen om haar informatievoorziening aan de weggebruiker te moderniseren (lees: digitaliseren) en te verbeteren. Maar er zijn nog veel meer mogelijkheden; zeker wanneer het voertuig een onlineverbinding met het internet krijgt.

In de praktijk is gebleken dat er nog veel onduidelijkheid bestaat over de vraag: “welke data worden verzameld in een voertuig, wie kan daar bij en wie kan/mag daar wat mee en onder welke randvoorwaarden?”

Dit geldt in brede zin voor belanghebbende partijen, zoals overheden, verzekeraars, nieuwkomers op de markt voor mobiliteitsdiensten en de mobiliteitssector zelf, met betrekking tot toepassingen voor onder meer veiligheid, comfort, voertuigconditie, verkeersinformatie, ongeval analyse, etc.

In dit document wordt getracht hierin enige duidelijkheid te scheppen, opdat partijen (publiek en/of privaot) weten waarover zij het hebben en gesignaleerde kansen ook daadwerkelijk kunnen worden benut.

Dit document beperkt zich tot de *personenauto*, hoewel het meeste van hetgeen wordt besproken ook van toepassing is op (lichte) bedrijfswagens. Tevens beperkt dit document zich tot de data die aanwezig zijn in het *interne* netwerk van de auto en evt. gegenereerd worden door achteraf vast in het voertuig aangebrachte voorzieningen. Ofwel: *voertuig gebonden* systemen. In dit stadium worden *persoonsgebonden* (mobiele) systemen, zoals smartphones en tablets en de data die door deze systemen worden afgescheiden, vooralsnog buiten beschouwing gelaten.

2. Gegevens uit voertuigen

Ten aanzien van data uit een voertuig kunnen verschillende aspecten worden onderscheiden die relevant zijn in het kader van deze notitie. Deze aspecten zijn:

- 2.1. Voertuigdata
- 2.2. Beschikbaarheid
- 2.3. Juridische aspecten

Dit onderscheid is zowel van toepassing op de *interne* (merk-)systemen van een auto als op evt. *achteraf* aangebrachte (vaste) systemen (een “kastje”).

2.1. Voertuigdata

Verreweg de grootste onduidelijkheid lijkt er te zijn omtrent voertuigdata. Bij velen is onvoldoende bekend welk *stysteem* welke data produceert binnen het voertuig en voor welk doel.

Voorts is vaak niet duidelijk hoe deze data voor welke toepassingen en voor welke instanties toegankelijk zijn. In deze paragraaf worden verschillende soorten voertuigdata nader geïnventariseerd. Daarbij beperken we ons tot data betreffende de primaire autofuncties. Service- en entertainmentdata worden buiten beschouwing gelaten.

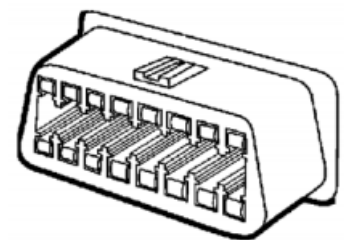
2.1.1 Interne voertuigsystemen

De databronnen (voertuig sensordata) zijn beschikbaar in het interne netwerk van het voertuig. Het uitlezen van voertuigdata door telematica-systemen vanuit dit interne netwerk van het voertuig via de zogenaamde 'CAN-bus' (Controller Area Network) in het voertuig, kan op verschillende wijzen gebeuren. Er kan een fysieke aansluiting gemaakt worden op de diagnose-bus van de standaard diagnose-stekker (On Board Diagnostics, kortweg OBD) die men in elke moderne auto aantreft. Hiermee krijgt men toegang tot een selectie van in het voertuig aanwezige data.

Daarnaast kan rechtstreeks een fysieke aansluiting gemaakt worden op het CAN-bus netwerk, dat ook in elke moderne auto aanwezig is.

2.1.1.1 Diagnose-data, algemeen toegankelijk via EOBD / OBD2

Elke moderne auto is vanaf de fabriek voorzien van een diagnose-stekker, ook wel Data Link Connector (DLC) of On Board Diagnostics (OBD) connector genoemd. OBD is een Amerikaanse emissie-standaard. Inmiddels is de versie OBD2, die gelijk is aan de Europese variant hiervan, EOBD de emissie-standaard die geldt voor in Europa verkochte auto's.



Vanaf 2001 (benzinemotoren) en 2003 (dieselmotoren) moet elke nieuwe in de EU toegelaten auto voorzien zijn van een gestandaardiseerde diagnose-stekker. Met deze standaard moet het ook voor niet-merkgebonden autobedrijven mogelijk zijn om in het geval van een afwijking aan de mengselregeling (en daarmee aan de emissie) een diagnose te kunnen stellen. Als zich een storing of afwijking aan de mengselregeling voordoet wordt een storingscode in de elektronica van de auto opgeslagen en wordt de bestuurder geïnformeerd door middel van een melding op het dashboard. Met behulp van een diagnoseapparaat kunnen deze storingscodes en/of data dan worden uitgelezen via vastgelegde protocollen. Dat diagnoseapparaat wordt aangesloten op de diagnose-stekker en zendt (schrijft) een verzoek, een zogenaamde PID (Parameter ID), naar de elektronica in de auto, waarna deze antwoordt met de betreffende storingscode. Dit kan bijvoorbeeld gedaan worden via bepaalde netwerkprotocollen in de auto zoals PWM, ISO of KWP, maar inmiddels veelal via de CAN-bus. Elke autofabrikant doet dit op zijn eigen manier.

Naast de diagnose-toepassing waar de diagnose-bus initieel voor bedoeld is, is het mogelijk tijdens een autorit emissie bepalende data van het voertuig uit te lezen. Het betreft overigens slechts een *beperkt* aantal parameters zoals o.a. snelheid, toerental, motorbelasting en koelvloeistof-temperatuur.

Autofabrikanten zijn in de regel zeer huiverig voor het gebruik van de OBD2 poort voor toegang tot de CAN-bus data door derden. Deels hangt dit samen met het feit dat voor het verkrijgen van de



bepaalde CAN-data via de OBD2 poort er eerst een bericht op de CAN-bus moet worden “geschreven”, om vervolgens de gewenste data als *antwoord* te krijgen. Wanneer dit niet met de juiste apparatuur en juiste deskundigheid gebeurt, bestaan risico's voor de juiste werking van de interne systemen van de auto, Niettemin zullen verrichtingen aan de auto met betrekking tot de verkeers-)veiligheid van de bestuurder van de auto en medeweggebruikers altijd moeten kunnen worden verricht door daartoe (wettelijk) gerechtigde partijen.

2.1.1.2 Proprietary data, besloten sensordata via CAN-bus

De andere manier om voertuigdata uit te lezen is vanaf het CAN-bus netwerk. Sinds 2003 is vrijwel elke nieuwe auto voorzien van een netwerk met een of meerdere CAN-bussen. Via dit CAN-bus netwerk zijn de regeleenheden en sensoren op elkaar aangesloten en wisselen deze hun gegevens uit. In veel automodellen zijn dit “gesloten” CAN-bussen zonder uitlees-stekker, maar er zijn ook auto's waarbij de selectie van data op een of meerdere CAN-bussen in de diagnose-stekker uitkomt, al dan niet met een geïntegreerde diagnose-bus.

In tegenstelling tot de beperkte, *algemeen toegankelijke* data op een diagnose-bus is er op het CAN-bus netwerk een schat aan data te vinden die slechts met de juiste expertise, gedestilleerd kan worden. We hebben het dan bijvoorbeeld over parameters als snelheid, kilometerstand, gebruik remmen, remkracht, gebruik ruitenwissers, gebruik mistlampen, buitentemperatuur, gordelcontacten, stoelcontacten, tankniveau enzovoort, ook wel **Probe Vehicle Data** genoemd. Deze data zijn in de regel echter “proprietary”; ofwel: niet algemeen toegankelijk en meestal door de autofabrikant “encrypted” waardoor deze doorgaans niet zonder meer begrijpelijk en bruikbaar zijn voor meer algemene toepassingen.

De terughoudendheid van autofabrikanten geldt ook hier, voor het slechts “lezen van/luisteren naar” data rechtstreeks op de CAN-bus, vandaar o.a. deze encryptie, hoewel de risico's bij gebruik van de juiste apparatuur en juiste deskundigheid, hier beperkt zijn. Er zijn echter momenteel veel systemen in de handel verkrijgbaar waarvan op voorhand onvoldoende duidelijk is wat hiervan de kwaliteit is en wat hiervan de mogelijke risico's zijn voor de integriteit van de in-car systemen en daarmee samenhangende risico's voor aansprakelijkheid, veiligheid, garantie, etc.

2.1.2 Achteraf aangebrachte systemen (after-market)

Naast het hiervoor besproken interne netwerk van een auto dat af-fabriek is aangebracht, is het mogelijk om achteraf systemen aan te brengen in een voertuig, om voertuig sensordata te lezen en eventueel zelf data te genereren. Dit kunnen systemen zijn die:

1. volledig *stand-alone* zijn en dus niet aangesloten zijn op het interne (CAN-bus)netwerk van de auto
2. systemen die aangesloten worden op de OBD2 poort
3. systemen die achteraf wel rechtstreeks op de CAN-bus worden aangesloten

Bij de onder 2 en 3 vallende systemen gaat het om kastjes of dongles van heel diverse leveranciers en dienstverleners. Deze systemen worden, voor zover zij niet door de dealer worden ingebouwd, in de zgn. “after-market” (retrofit) aangebracht en vallen daarmee buiten het gezichtsveld van de autofabrikant en diens merkorganisatie. Zoals gezegd zijn autofabrikanten doorgaans huiverig voor aansluiting van achteraf aangebrachte systemen op de OBD2 poort. Aan de andere kant zijn veel van deze systemen probleemloos ingevoerd waarbij de kwaliteit van zowel het systeem zelf als van de



data kennelijk voldoende op orde zijn. Sinds kort maken ook de OEMs zelf gebruik van zgn. dongles bij hun dienstverlening.

2.1.2.1 Volledig stand alone

Voorbeelden van stand alone systemen zijn onder meer: navigatiesystemen, voertuigvolgsystemen (Track&Trace), fleet-managementsystemen, ritregistratiesystemen, etc.. Deze systemen bevatten *eigen* sensoren die nodig zijn voor de toepassingen die ermee worden beoogd, zoals een GPS-module, sensoren voor snelheid, versnelling/vertraging, hellingshoek, etc. en, voor de communicatie met een back-office, bijv. een SIM-kaart. Voor deze “eenvoudige” systemen is doorgaans geen koppeling nodig met het interne (CAN-bus) netwerk van de auto.

2.1.2.2. Aangesloten op de OBD2 poort

In de markt zijn systemen verkrijgbaar die met een stekker in de OBD2 (diagnose)-poort kunnen worden gestoken. De meest bekende vorm hiervan zijn de zgn. “dongles”. Dit zijn kleine kastjes met een ingebouwde stekker, die rechtstreeks in de OBD2 poort kunnen worden gestoken. Hoewel sommige leveranciers van dongles aangeven dat met de dongle ongeveer alle data aan het interne netwerk van de auto kan worden onttrokken, is dit doorgaans niet juist. Het betreft in de regel slechts de data die, zoals voorgaand beschreven, *algemeen toegankelijk* en beperkt in omvang zijn. Indien een dongle of ander systeem, aangesloten via de OBD2 poort op de CAN-bus, niettemin in staat is om door middel van een *schrijfactie* data aan het CAN-bus te onttrekken, ontstaan de eerder genoemde risico's voor de fabrikant, zeker als er schrijfacties onder het rijden plaatsvinden.

Daarnaast lijkt de eenvoudige installatie een groot voordeel van het gebruik van dongles. Elke berijder kan namelijk zelf de diagnose-aansluiting in zijn auto opzoeken en daar de dongle in steken. Dit gebruiksgemak wordt door de gebruikers zeer gewaardeerd. Dit blijkt onder meer uit een pilot van de ANWB, waarbij slechts 2% van de gebruikers het moeilijk vond om de dongle te installeren. In de praktijk blijkt echter ook dat door fysieke verschillen in uitvoering van de diagnose-aansluiting tussen de vele merken en modellen dongles niet altijd goed functioneren. Daarnaast is er een grote variëteit in kwaliteit van dongles op de markt.

Met name ook met het oog op cyberveiligheid is voorzichtigheid geboden bij het gebruik van de diagnose(OBD2) poort voor koppeling met achteraf aangebrachte systemen. Het vaststellen van minimumeisen voor het gebruik van aftermarket systemen, zoals dongles maar ook vast ingebouwde systemen, kan mogelijk de genoemde bezwaren wegnemen

2.1.2.3 Achteraf aangebracht maar rechtstreeks op de CAN-bus

Via een *rechtstreekse* CAN-bus koppeling kan in beginsel alle elektronica van een voertuig worden *gelezen*; zij het via een *specifiek protocol* dat afhankelijk is van de betreffende voertuigfabrikant, -type en -bouwjaar. Met een dergelijke aansluiting op het CAN-bus netwerk ontstaat een universele voorziening waarmee alle in het voertuig aanwezige- en nuttige voertuigdata flexibel voor meerdere diensten en services beschikbaar gemaakt kunnen worden. Dit door slechts te “luisteren” naar de CAN-bus.

Dit vereist echter wel slimme technologieën en vooral de juiste expertise om deze CAN-data niet alleen te kunnen beluisteren maar ook nog te kunnen *begrijpen*, zonder dat “schrijven” op de CAN-bus nodig is om deze data te ontsluiten. Daarnaast is het nodig om de “encrypted” (merkgebonden) data te *converteren* naar bruikbare data die *universeel* kan worden gebruikt voor informatie.



Er bestaan nu al after-market oplossingen waarmee deze merk- en voertuig specifieke protocollen voor alle gangbare voertuigen kunnen worden geïnterpreteerd/geconverteerd naar universeel bruikbare voertuiginformatie en sensordata. Hoewel er op deze wijze *niet* op de CAN-bus hoeft te worden *geschreven* om de gewenste data te ontsluiten, ontstaat niettemin een “opening” voor ondeskundigen en/of kwaadwillenden om in te breken. Om dit inbreken echt te voorkomen hebben professioneel aangebrachte CAN-bus connecties fysiek doorgaans geen schrijf-mogelijkheid ingebouwd.

2.1.2.4. Gebruik en diensten

Ondanks de hiervoor genoemde kanttekeningen bij systemen die achteraf rechtstreeks op de OBDII-poort worden aangesloten (zoals een dongle), kunnen dergelijke systemen niettemin een toegevoegde waarde hebben voor met name de consument die slechts een beperkte functionaliteit wenst. De mogelijkheid om dergelijke systemen eenvoudig aan te kunnen brengen, makkelijk mee te kunnen nemen naar een ander voertuig en de relatief lage aanschafprijs¹, kunnen hierbij een rol spelen. Het opstellen van “randvoorwaarden”, zoals genoemd in 2.1.2.2., voor deugdelijke systemen kan een belangrijke bijdrage leveren aan meer en beter meer inzicht in de kwaliteit en betrouwbaarheid van dergelijke systemen en mogelijke risico's. Zowel de data die door de interne systeem van het voertuig worden gegenereerd als door een achteraf aangebracht systeem, kunnen de basis vormen voor het aanbieden van (commerciële) diensten aan de bestuurder/gebruiker van het voertuig. De mate waarin de gebruiker zelf kan bepalen welke data voor welke toepassing naar welke partij gaat, is in hoge mate van invloed op de keuze van de gebruiker voor bepaalde diensten.

Een bijzondere positie wordt hierbij ingenomen door de zgn. EDR (Event Data Recorder). Dit, overigens in de USA al verplichte device, registreert gedurende de laatste seconden voorafgaand aan een ongeval, een aantal relevante data. Deze data kunnen ondersteunend zijn bij de analyse van de toedracht van ongeval. Verkeersdeelnemers, verzekeraars, politie en justitie kunnen belang hebben bij toegang tot deze data. De EDR wordt ook in Nederland al vaak standaard geleverd in nieuwe auto's; soms zonder dat de koper van de auto dit weet. Mede om die reden is er nog veel discussie over wie onder welke omstandigheden toegang heeft tot de data uit de EDR, wat ermee mag worden gedaan en wat hiervan de mogelijke gevolgen zijn voor de aansprakelijkheid en de data protectie.

¹ Naast de (mogelijk relatief lage) aanschafprijs van een systeem, moet rekening worden gehouden met periodiek terugkerende kosten zoals voor datacommunicatie en de geleverde diensten.

2.2. Beschikbaarheid

Tot slot kan er m.b.t. data uit voertuigen ook nog onderscheid worden gemaakt naar:

- Data die achteraf wordt uitgelezen
- Data die near real-time uit het rijdend voertuig wordt ontvangen.

2.2.1 Uitlezen achteraf

Bij offline data gaat het om gegevens die *periodiek/incidenteel* aan het voertuig worden onttrokken. Denk hierbij aan het onttrekken van diagnose-gegevens aan het voertuig in de werkplaats van het autobedrijf, met behulp van een speciale testapparatuur bij onderhoud of een storing. Daartoe wordt een stekker van de testapparatuur aangesloten op de hiervoor beschreven OBD2 poort van het voertuig. Het geheugen van het interne systeem van het voertuig wordt hiermee uitgelezen, inclusief evt. foutcodes. Het gaat hier om zowel de *algemeen* toegankelijke data als de *proprietary* data hoewel ten aanzien van deze laatste beperkingen gelden (zie ook 2.1.1.2). Tevens kunnen de interne systemen hiermee, indien nodig en met voldoende autorisatie, door het autobedrijf worden gereset.

2.2.2. 'Real-time' data-ontvangst

Steeds meer nieuwe voertuigen zijn af fabriek in staat om (near-) *real-time* of in ieder geval periodiek, data te verzenden naar de cloud of naar een eigen back-office (connected). Maar ook oudere auto's kunnen met een achteraf aangebracht systeem (alsnog) connected worden gemaakt. Het kan hierbij gaan om zowel de data van hun interne (CAN-bus)systeem, als om data die via een achteraf aangebracht systeem zijn verzameld en worden verzonden. Het betreft hier doorgaans data waarbij een (near-) real-time verzending (en -verzameling door de ontvanger) van belang is voor de toepassing die hierop gebaseerd is.

Zo is het bij een ritregistratiesysteem voor fiscale toepassingen van belang dat met grote regelmaat in een backoffice wordt vastgelegd waar het voertuig zich op enig moment bevond. Daarbij dient een dergelijk systeem op eenduidige wijze aan het voertuig gekoppeld te zijn en/of dienen nadere maatregelen te worden getroffen om de continuïteit van de datastroom te waarborgen. Ook voor op maat verstrekte verkeersinformatie is een (near-) real-time verbinding noodzakelijk ten behoeve van de gewenste actualiteit.

Momenteel verlopen de meeste 'real-time' verbindingen (nog) via het GSM-netwerk. Bij (hoog-) frequente datatransmissie kunnen daarmee aanzienlijke kosten gemoeid zijn.

Ontwikkelingen ten aanzien van datacommunicatie - snelheden en kosten - gaan echter snel. Na 3G en 4G komen nu WiFi-p en 5G communicatie mogelijkheden in zicht. De (near-) real-time data die door dataverbindingen van voertuigen wordt uitgezonden zijn momenteel nog beperkt in omvang. Ook de geadresseerden van de datastromen zijn nog vrij eng gedefinieerd: veelal slechts de autofabrikant of een door hem ingehuurde of aan het after-market apparatuur verbonden service



provider. Niettemin is de verwachting dat hier op (zeer) korte termijn verandering in gaat komen, naarmate meer auto's zowel af-fabriek als met behulp van after-market systemen connected gaan worden.

2.3 Juridische aspecten

2.3.1 Dataproductie

Een deel van de voertuigdata is gekoppeld aan de berijder/eigenaar/houder van het voertuig. Derhalve is van belang om inzicht te krijgen of, en zo ja in welke mate, er ten aanzien van data uit een voertuig sprake is van persoonsgegevens, waarop de dataproductiewetgeving van toepassing is. Het gaat daarbij om gegevens die identificerend zijn, zoals naam, adres, kenteken, VIN, maar ook om gegevens die op het eerste gezicht niet identificerend zijn, maar die in combinatie met andere gegevens wel tot een persoon herleidbaar kunnen zijn. Daarbij is met name van belang of de verwerker van de gegevens toegang heeft tot dergelijke andere gegevens.

2.3.1.1 Gegevens die géén persoonsgegevens zijn

Gegevens zijn in dit document geen persoonsgegevens als: gegevens (data) puur betrekking hebben op het functioneren van de interne systemen in het voertuig en daarmee de basis kunnen bieden voor informatie over de feitelijke conditie en het gebruik van het voertuig en alle daarmee samenhangende systemen en sensoren². Dit geldt voor zowel het interne netwerk van de auto (CAN-bus) als data afkomstig van achteraf aangebrachte systemen. Deze data kunnen op hun beurt weer worden onderscheiden naar data voor uitsluitend diagnose van het voertuig en data voor overige (merk-) toepassingen. Voorwaarde is dat deze gegevens geen data bevatten die kunnen leiden tot identificatie van een persoon. Te denken valt daarbij aan voertuig identificatiegegevens en locatiedata van het voertuig.

2.3.1.2 Persoonsgegevens

Als het voertuig, of de daarin achteraf aangebrachte systemen, *persoonsgegevens* - met inbegrip van *tot persoon herleidbare gegevens* - produceert, dan is de Wet Bescherming Persoonsgegevens (WBP)³ van toepassing. Dit betekent dat er ten aanzien van deze gegevens, conform deze wet, grote zorgvuldigheid moet worden betracht ten aanzien van de *verzameling, opslag en gebruik* hiervan. Ook zal de OEM of dienstverlener het recht op inzage in, en op correctie van persoonsgegevens door de gebruiker moeten faciliteren. Een nadere beschrijving van de data protectie aspecten valt buiten de scope van deze notitie.

2.3.1.2.1 Interne netwerk (CAN-bus) van de auto

Data afkomstig van het interne (CAN-bus) netwerk van het voertuig bevatten doorgaans geen directe persoonsgegevens, maar er kan wel sprake zijn van "tot een persoon herleidbare" gegevens; vooral

² Over wat als persoonsgegevens moet worden beschouwd bestaat nog geen consensus. Duitse DPA: voertuigdata geen persoonsgegevens als de gegevens het voertuig niet verlaten. Franse DPA: alle gegevens in het voertuig zijn persoonsgegevens.

³ Deze wet wordt in mei 2018 vervangen door de Verordening (EU nr. 2016/679



wanneer een combinatie van deze data met andere gegevens omtrent het voertuig wordt gemaakt. Hierbij kan worden gedacht aan *locatiegegevens* van het voertuig, gecombineerd met het *kenteken* of *VIN* (Vehicle Identification Number). Langs deze weg zou in beginsel de berijder/houder van het voertuig kunnen worden achterhaald en zou kunnen worden vastgesteld waar deze is geweest en wanneer. Globaal kan worden gesteld, dat *alle* voertuigdata, tot een persoon herleidbaar kunnen zijn *in combinatie* met bijv. kenteken en/of VIN. Voor zover een dergelijke koppeling niet plaatsvindt zal aan de hand van de feitelijke verwerking moeten worden vastgesteld of het om persoonsgegevens gaat. Daarbij spelen locatiegegevens van het voertuig en de mate waarin de informatie buiten het voertuig 'zichtbaar' is een belangrijke rol. Met name de discussie over de mate waarin Cooperative Awareness Messages (CAM) - door het voertuig uitgezonden berichten voor coöperatief rijden toepassingen - als persoonsgegevens moeten worden beschouwd is nog niet afgerond. Er is reden om aan te nemen dat op grond van de nieuwe Algemene Verordening Persoonsgegevens (AVG) een belangrijk deel van de gegevens die door het voertuig gaan worden uitgezonden, en daarmee door derden kunnen worden verwerkt, als persoonsgegevens zullen worden beschouwd.

2.3.1.2.2 Achteraf aangebrachte systemen

Door de aard van de toepassing van sommige achteraf aangebrachte systemen, kunnen data uit deze systemen ook rechtstreeks persoonsgegevens bevatten, of tot de persoon herleidbare gegevens.

Bij achteraf aangebrachte systemen kan ook onderscheid worden gemaakt naar data, die specifiek voor diagnose doeleinden t.a.v. het voertuig worden vergaard (als onderdeel van de toepassing van het systeem) en specifieke sensordata, die nodig zijn voor een bepaalde specifieke toepassing van het achteraf aangebrachte systeem. Denk hierbij aan bijv. Track & Trace systemen of Ritregistratie systemen. Bij deze systemen kan sprake zijn van een directe koppeling met de persoonsgegevens van de berijder/houder van het voertuig vanwege de aard van de toepassing van het systeem en dient rekening te worden gehouden met de dataproctiewetgeving.

2.3.2 Datazeggenschap

Als het gaat om de zeggenschap over de voertuiggegevens dan is het goed om allereerst vast te stellen dat deze zeggenschap onderwerp is van de overeenkomst tussen de betrokken partijen. Zo kan bijvoorbeeld de autokoper worden uitgenodigd om toestemming te geven voor het gebruik van voertuigdata door de OEM. Met de ondertekening van de overeenkomst is daarmee de zeggenschap over de data tussen de koper van het voertuig en de OEM in beginsel geregeld. De vraag is wel wat de gevolgen zijn van het opnemen van zo'n datazeggenschapsclausule in de koopovereenkomst van het voertuig. De fabrikant mag namelijk niet op voorhand de garantie op de auto afhankelijk maken van de toestemming. De vraag is dus of de OEM exclusief gebruik kan claimen of dat ook de voertuigeigenaar gebruiksrechten op de data kan doen gelden? Daarbij kunnen verschillende situaties worden onderscheiden. Om te beginnen speelt het onderscheid tussen data die via de OBD2 poort toegankelijk is en de, op voorhand niet toegankelijke, overige voertuigdata. Een bijzondere positie wordt daarbij ingenomen door data die van belang zijn voor garantiewerkzaamheden, en die ook (wettelijk) mogen verricht door andere partijen dan de (vertegenwoordiger van) de voertuigfabrikant.



2.3.2.1 Diagnosegegevens

Diagnosegegevens zijn beperkt tot informatie die nodig is voor het onderhoud van het voertuig. De gegevens worden, door middel van beperkte schrijfrechten op de CAN-bus, door de OEM ter beschikking gesteld aan merkdealers en ook aan de niet-merkgebonden onderhoudsbedrijven. Voor dat laatste is een wettelijke verplichting⁴ vastgesteld. Het schrijven houdt in dat vragen worden gesteld aan het systeem. Daarop wordt door het systeem antwoord gegeven in de vorm van data. Daarmee wordt aan alle bedrijven een beperkt gebruiksrecht verleend in het kader van het onderhoud aan het voertuig. Het onderhoudsbedrijf krijgt daarmee tegen een vergoeding een beperkt gebruiksrecht met betrekking tot de data voor het specifieke onderhouds- en reparatiedoel.

2.3.2.2 Overige voertuigdata

Andere data dan diagnosedata zijn in principe niet vrij beschikbaar. Wel zijn sommige bedrijven in staat om uit de ruwe CAN-bus data te ontsluiten, waardoor meer informatie beschikbaar komt dan door de OEM is voorzien. Deze gegevens (data) moeten echter een ingrijpende bewerking ondergaan om tot toegankelijke informatie te leiden. Afgezien van het feit dat deze data ook persoonsgegevens kunnen bevatten, ontstaat de vraag of de zeggenschap over deze data niet ook (voor een deel) bij de eigenaar/gebruiker van de auto zou moeten liggen⁵. Op dit moment wordt in opdracht van de EU Commissie (DG-Move) een onderzoek uitgevoerd waarin verschillende modellen voor het beheer van voertuiggegevens onder de loep worden genomen. Met name het verschil in belangen tussen OEM's enerzijds en consumenten en after-market anderzijds wordt daarbij nader doorgelicht naar aanleiding van de discussie hierover tussen ACEA (autofabrikanten) en de FIA die meer de gebruikers vertegenwoordigen.⁶ De uitkomsten van de survey, waarin enkele modellen worden voorgesteld, kunnen een verdere ontwikkeling van de datazeggenschap rond het voertuig faciliteren.

2.3.3 Aansprakelijkheid

Een ander aspect dat een grote rol speelt bij de afscherming van de voertuiggegevens door de OEM's is het risico van schrijven door derden op de CAN-bus. Hiervoor is al aangegeven dat OEM's in verband met de productaansprakelijkheid, invloeden van buitenaf op de CAN-bus zoveel mogelijk willen beperken. De CAN-bus data bevatten gegevens van veel vitale functies van het voertuig. Voor de aansturing van deze functies is CAN-bus data onontbeerlijk. Omdat de OEM instaat voor de integriteit van de voertuigdata, en een fout in de data op de CAN-bus tot wijziging en uitval van functies in het voertuig kan leiden, worden geen of slecht beperkte schrijfrechten op de CAN-bus verstrekt. Schrijven is alleen mogelijk op de beveiligde en afgeschermdde OBD2 poort, binnen de kaders zoals bij 2.1.1.1 is beschreven. Wel kan worden geluisterd op de CAN-bus, waarbij de integriteit van de data niet in het geding is. De te beluisteren stroom data behoeft echter nog veel bewerking. Sommige gespecialiseerde after market bedrijven houden zich hiermee bezig (zie ook 2.3.2.2.).

⁴ Hiervoor is Europese regelgeving van toepassing; de zgn EURO V/VI regelgeving m.b.t. Repair & Maintenance Information

⁵ Volvo heeft zich recent in die richting uitgelaten. De Duitse auto industrie lijkt nog niet zo ver.

⁶ Research by TRL 'In-vehicle data and resources survey ' 2016-2017



3 Voorlopige conclusies

Wat betekent de voorgaande inventarisatie concreet? Wat is de korte termijn verwachting? Het beeld binnen de werkgroep is dat de hoeveelheid data in voertuigen groot is en groeiende. De OEM's lijken vooralsnog niet bereid veel verder te gaan dan het vrij verstrekken van de data die via de OBD2 poort uit het voertuig kan worden gehaald. Deze verplichte datastroom is echter voor veel ITS toepassingen te beperkt.

Op korte termijn lijken de CAN-bus data van voertuigen alleen breder toegankelijk via after-market bedrijven die de data uit de CAN-bus verzamelen en decoderen. Met deze data worden op dit moment talloze voertuig gerelateerde diensten in de markt gezet. De volgende vraag is of en in welke mate dit kan worden opgeschaald? De werkgroep constateert dat met de beschikbare after-market-voorzieningen, data kunnen worden opgeschaald mits dit gebeurt met kleine stappen en vooral met een beperkt aantal door de vraagkant bepaalde datasoorten en kwalitatief betrouwbare systemen. Vaak is bijv. met slechts drie data-elementen al een waardevolle dienst te creëren. Verder moet er een business case zijn. Om van aanbod gestuurd - 100 data-elementen beschikbaar - naar vraag gestuurd - drie data-elementen nodig - te komen lijkt een bottom up aanpak vooralsnog de aangewezen weg, waarbij niet alles van te voren in een keer kan worden geregeld.

Wat zijn de belemmeringen en moeten we energie steken in het opruimen ervan? Vooral de focus op grote stappen kan een belemmering worden volgens de werkgroep. In feite is de ontsluiting en het gebruik alleen op gang te brengen met aansprekende use cases. De werkgroep verwacht dat de meest succesvolle toepassingen zullen beginnen met een beperkte dataset en een beperkte gebruikersgroep, die overigens wel snel kan groeien. Het mogelijke gebrek aan bereidheid bij de OEM's om data ter beschikking te stellen en het gebrek aan kennis om de ontsluiting op andere manieren te organiseren, is momenteel nog een beperking. Op dit moment lijkt het data gebruik binnen ITS vooral te worden opgepakt vanuit de after-market, met CAN-bus data of via andere devices zoals OBU's en Smartphones. Deze toepassingen kunnen voor Smart Mobility wellicht het vliegwiel op gang brengen zodra duidelijk wordt dat nieuwe toepassingen ook werkelijk functioneren. Mogelijk zijn ook problemen te verwachten in de strijd om de datazeggenschap. Het lopende, door de EU ingestelde, TRL onderzoek moet bouwstenen bieden voor die discussie. Verder zal een deel van de data als persoonsgegevens kunnen worden aangemerkt, bijvoorbeeld omdat zij zijn opgehangen aan een voertuigidentificatie. Dit kan de bruikbaarheid van de gegevens voor andere toepassingen flink bemoeilijken.

Eveneens in Europese context is het vraagstuk van data uit voertuigen met betrekking tot wie er bij kan en wat ermee kan/mag worden gedaan, een zeer "hot" onderwerp tussen de private (sector-) partijen onderling. Vanuit de automobilisten wordt zeggenschap geclaimd die door de OEMs moet worden gerealiseerd. Binnen de automotive sector speelt de discussie zich voornamelijk af tussen de Europese koepels ACEA (OEM's), CLEPA (automotive industry toeleveranciers), de FIA (Federation Internationale de l'Automobile, koepel van automobilisten/consumenten) en de FIGEFA (aftermarket-partijen) en daaraan gelieerde partijen. De voorgestane oplossing door partijen variëren van creëren van onderhandse agreements (bijv. een neutrale server met een selectie van voertuigdata voor derde-partijen) tot gewenste wet- en regelgeving.



Tot slot is een punt van aandacht, de kwaliteit van de voorhanden data. Als de data onvoldoende kwaliteit hebben zal het moeilijker zijn om een succesvolle App te maken. Het recent door de Hogeschool Arnhem/Nijmegen (HAN) opgestarte project "VIA-NOVA" beoogt hier een significante bijdrage aan te leveren. Ook het databeheer kan nog een issue worden in die zin dat de beherende partij voldoende trusted moet zijn om succesvol de beheer rol te kunnen spelen. Immers, onder de huidige omstandigheden lijkt het erop, dat iedere zweem van partijdigheid de datastromen tot stilstand kan brengen.

-0-0-0-0-0-0-