



Notitie ten behoeve van de Landelijke ITS Ronde Tafel Juridische aspecten van Smart Mobility

DINSDAG 11 JUNI 2015

Marcel Otto - Wouter van Haften
DITCM INNOVATIONS | WWW.DITCM.EU
9-6-2015

Notitie ten behoeve van de Landelijke ITS Ronde Tafel Juridische aspecten van Smart Mobility

Inleiding

De omarming van ITS (*Intelligent Transport Systems*) neemt internationaal een grote vlucht. Binnen Europa is het Platform C-ITS de plaats waar beleidsvoorbereiders, auto-industrie, ICT producenten en dienstverleners als infrastructuurbeheerders zich gezamenlijk buigen over de voorwaarden voor toepassing van C-ITS. Nederland wil binnen de EU, maar ook wereldwijd een voorlopers rol vervullen bij de ontwikkeling van ITS. Dat betekent dat de ontwikkelingen in Nederland zullen moeten passen in deze internationale context. De beoogde coöperatieve systemen zullen niet stoppen aan de grens. Op langere termijn zal een gestandaardiseerde EU brede uitrol noodzakelijk zijn. Voor het goed kunnen benutten van de technische ontwikkelingen, de beleidsontwikkelingen en de business ontwikkelingen is het van belang de juridische kaders in kaart te brengen en deze te confronteren met de bovengenoemde ontwikkelingen.

Juridische inbedding van C-ITS

Als je een jurist vraagt of zelfsturend of coöperatief rijden juridische problemen oplevert zal het antwoord al snel ontkennend luiden. Zolang je je aan de regels houdt kan er weinig misgaan, en ook als je je niet aan de regels houdt dan is altijd een gang naar de rechter mogelijk, die vervolgens een uitspraak doet en daarmee de zaak beslecht. Kortom juridisch is de wereld geregeld en nieuwe fenomenen krijgen vanzelf een plaats in het bestaande recht, totdat blijkt dat de gang naar de rechter niet leidt tot een bevredigende uitkomst, of dat rechters een zodanig eenduidige lijn volgen in hun uitspraken dat het tijd is om deze in de wet op te nemen.

Waarom dan toch kijken naar de juridische aspecten van C-ITS? In de eerste plaats om het voor ontwikkelaars en dienstverleners mogelijk te maken rekening te houden met het juridisch kader door een brug te slaan tussen techniek en dienstverlening aan de ene kant en het juridisch kader aan de andere kant. Daarnaast is een belangrijke reden het verkrijgen van een zo groot mogelijke mate van rechtszekerheid. Partijen die veel geld investeren in de ontwikkeling van C-ITS kunnen het zich niet veroorloven achteraf te worden verrast door een uitspraak van de rechter over bijvoorbeeld hun aansprakelijkheid bij schade of bij schending van de privacy of het datarecht.

De juridische inbedding van C-ITS is dus vooral een kwestie van samen optrekken en voorkomen dat juridische issues onnodig showstoppers kunnen worden. Het bereiken van zoveel mogelijk rechtszekerheid is daarbij een belangrijke doelstelling.

Waar willen we naartoe

In het komende halfjaar is het streven erop gericht om de belangrijkste juridische issues in C-ITS te benoemen, te agenderen en in gesprek met de stakeholders oplossingen te formuleren ten behoeve van de ontwikkeling van C-ITS. Het gaat er in het komende halfjaar om:

- Meer kennis en bewustzijn bij NL belanghebbenden over mogelijke juridische problemen en oplossingen op het terrein van C-ITS.
- Gecoördineerde en gedragen activiteiten vanuit NL partijen passend bij de ambities om koploper te zijn.

- het samen inventariseren, analyseren en prioriteren van risico's en beheersmaatregelen bij een aantal beeldbepalende en concrete use cases voor de toepassing van C-ITS. het opstellen en bijhouden van handreikingen (per onderdeel), met best practices en een overzicht van relevante publicaties, spelers en FAQ&A's.

Waar staan we nu

Recent is een aantal ontwikkelingen in gang gezet om beter zicht te krijgen op de juridische implicaties van zelfsturende auto's en ook van C-ITS op een drietal meest betrokken rechtsgebieden: Dataprotectie, Datazeggenschap en Aansprakelijkheid.

Bij de onderstaande paragrafen zijn vragen geformuleerd voor de discussie aan de juridische tafel C-ITS van 11 juni 2015.

Data protectie.

De regels rond dataprotectie vloeien voort uit EU richtlijnen, die in Nederland zijn opgenomen in de Wet bescherming persoonsgegevens, terwijl de voor C-ITS relevante bijzondere dataprotectieregels voor de telecommunicatiesector zijn opgenomen in de Telecommunicatiewet. Daarnaast zijn ook andere wetten relevant, zoals blijkt uit het volgende voorbeeld.

Recent speelde bijvoorbeeld dat de Belastingdienst parkeergegevens op kenteken opvroeg bij een parkeergarage. Na aanvankelijke weigering op grond van privacyoverwegingen bij het parkeerbedrijf bepaalde de rechter dat de gegevens aan de Belastingdienst moesten worden overgedragen. Daarmee werd de privacy van de klanten niet geschonden, de Belastingdienst heeft immers geheimhoudingsplicht. Het informatierecht van de fiscus ging in dit geval voor, en aangezien dit informatierecht niet snel zal worden beperkt is het goed om hiermee bij het opzetten van C-ITS diensten en het communiceren daarover rekening te houden

Met de stakeholders is afgesproken om zowel naar coöperatieve als connected toepassingen te kijken. Het wettelijk kader ligt dus vast, maar en de activiteiten zullen worden gericht op het toelichten van de wettelijke regeling in relatie tot ontwikkelingen in het veld, zoals privacyverklaringen van voertuigfabrikanten. Daarbij wordt gestreefd naar het praktisch hanteerbaar maken van het kader door de stakeholders, bijvoorbeeld door het ontwikkelen van concrete handreikingen. Een nauwkeurige beschrijving van de werking van de C-ITS toepassing is van groot belang als startpunt van zo'n handreiking, aangezien de wijze van inrichting daarvan kan bepalen of wel of niet aan de wettelijke verplichtingen kan worden voldaan. Doelbinding, transparantie en accountability zijn hierbij de sleutelbegrippen.

Het onderscheid tussen connected en coöperatief is in relatie tot data protectie in het bijzonder relevant. Bij connected diensten is er een een op een verbinding met de service provider die het mogelijk maakt de persoonlijke data te scheiden van de generieke voertuiglocatiegegevens die met Wifi-P naar de wegwant en andere voertuigen worden gezonden. Bij op zich goed beveiligde coöperatieve Wifi-P berichten blijft de vraag op welke kan worden voorkomen dat serviceproviders, medeweggebruikers en andere derden de beschikking krijgen over identificeerbare persoonsgebonden locatiegegevens.

Vragen:

1. Hoe kan de privacy van de gebruiker van C-ITS diensten het beste worden beschermd?
2. In welke mate is anonimisering mogelijk en kan dit een bijdrage leveren aan het beschermen van de privacy van de C-ITS gebruiker?

Documenten:

- NL-Wetgeving en toelichtingen
- Data Protection Principles For Connected Vehicles (Verband Der Automobilindustrie-VDA, 3 november 2014)

De dataprotectieverklaring van de Europese autofabrikanten heeft ten doel aan te geven dat de fabrikanten privacy aandacht geven bij hun ontwerpen (Privacy by design) maar ook om de klanten te wijzen op hun eigen verantwoordelijkheid ten aanzien van dataprotectie. Hoewel met geen woord wordt gerept over de in de EU vigerende wetgeving, komt deze wel op verschillende plaatsen impliciet terug, in de vorm van tegemoetkoming aan de klant in plaats van een harde verplichting. In die zin zijn de principes wat misleidend. De scope van de verklaring is met name de innovaties in connected en vernetwerkte voertuigen. Onder de kop transparantie verwijst de verklaring naar het streven van de leveranciers naar adequate informatievoorziening omtrent de data in de voertuigen en het gebruik van deze data. Daarbij worden 6 categorieën data onderscheiden. Deze categorieën komen ten dele overeen met de categorieën uit de EU Richtlijn, maar het lijkt erop dat de autofabrikanten de privacy aspecten verbinden aan de zeggenschap over de data. Met name de technische en service data lijken op die manier minder bescherming te genieten omdat zij 'van de fabrikant zijn'. Daar is juridisch geen reden voor, privacy wordt altijd beschermd, ongeacht wie de beschikking of de zeggenschap over de data heeft, en daarbij is de aard van de data bepalend. In lijn met de Richtlijn wordt het informed consent opgevoerd als middel om de data met toestemming van de klant te kunnen gebruiken. Daarbij gaat het echter over data in het kader van services die door de klant separaat worden afgenomen. Technische data en service data van het voertuig lijken daar niet onder te worden begrepen. De VDA streeft naar de implementatie van dezelfde sterke veiligheidscultuur in het connected voertuig, als ook in de industrie gebruikelijk is. Daarbij zal gebruik worden gemaakt proactief ontwikkelde beveiligingsmaatregelen om de data in het voertuig te beschermen, inclusief cryptografische maatregelen. Deze maatregelen betreffen zowel technische als persoonsgebonden data.

- Consumer Privacy Protection Principles (Alliance of Automobile Manufacturers INC., Association of Global Automakers INC., 12 november 2015)

Deze dataprotectieverklaring van de wereldwijde auto-industrie onderkent de gevoeligheid van lokatiegegevens als gevoelige gegevens (covered information). Verder worden dezelfde issues benoemd als in de geldende EU Richtlijnen, zij het wat minder strak geformuleerd. Het heeft een beperkte juridische waarde, aangezien de wetgeving van de staten waar de dienst wordt verleend doorslaggevend is. De verklaring geeft aan dat de autofabrikanten zich bewust zijn van de privacy issues en dat ze van plan daar zorgvuldig mee om te gaan.

- Voorstel voor een nieuwe data protectie verordening (nog in wording)

Navraag bij het Ministerie van V&J levert op dat de huidige tekst zeer sterk afwijkt van het oorspronkelijk ontwerp van 2012. Gezien de vele onzekerheden in de discussie hierover is een beoordeling voor het doel van de juridische tafel op dit moment minder zinvol. Hete hangijzers zijn met name de rechtmatigheid van de verwerking, de aansprakelijkheid en nog tal van kleinere issues, die overigens voor de relatie met coöperatief rijden in het bijzonder van belang kunnen zijn.

Data zeggenschap.

Coöperatieve ITS, waarbij voertuigen onderling en voertuigen en wegkant doorlopend met elkaar in verbinding staan, betekent dat grote hoeveelheden data van en naar voertuigen worden gezonden. In feite worden voertuigen rijdende zendmasten. De zeggenschap over de uitgezonden en ontvangen data is een kwestie van bilaterale overeenkomsten tussen de verschillende betrokken partijen. Het overzicht dat ten behoeve van de Werkgroep 4 van het C-ITS platform is gemaakt biedt een basis voor de discussie. In het document worden de verschillende wijzen waarop door

stakeholders met de data wordt omgegaan geïnventariseerd. Daarbij wordt sterk vanuit de positie van de fabrikanten en dienstverleners gedacht, en minder vanuit de consument.

Om een goede belangenafweging te kunnen maken moet echter ook de positie van de eindgebruiker worden betrokken. Alleen op die manier kan de transparantie en accountability met betrekking tot doel van en werkwijze bij de overdracht van data worden gerealiseerd en kan tot een bevredigend resultaat worden gekomen. Aan de hand van de documentatie kan het gesprek worden aangegaan met betrokkenen, en worden gezocht naar een gemeenschappelijk model waarin alle partijen zich kunnen vinden.

Een bijzonder plaats als het gaat om data-zeggenschap wordt ingenomen door de data die moet worden verstrekt aan officiële instanties, bijvoorbeeld met het oog op toelating van een voertuig, of bij het organiseren van dealer-onafhankelijk onderhoud. Hierbij kunnen zeggenschapskwesties gemakkelijk tot maatschappelijk ongewenste effecten leiden, zoals inperking van concurrentie tussen onderhoudsbedrijven en een gebrek aan adequate informatie met betrekking tot toelating van een voertuig, omdat de software van de systemen in de auto op elk moment kan worden gewijzigd.

Vraag:

Hoe zou datazeggenschap op een evenwichtige manier moeten worden verdeeld tussen de verschillende stakeholders, van autofabrikant tot eindgebruiker?

Documenten:

- Relevante NL wetgeving
- Access to vehicle resources and data (summary for the C-ITS Platform WP 6, nieuwe versie op komst)

Aansprakelijkheid

Bij aansprakelijkheid wordt er, gelet op de beperkte tijd en capaciteit, voor gekozen om hieraan op dit moment geen prioriteit te geven binnen de juridische tafel. Recent onderzoek van de VU naar de aansprakelijkheid in relatie tot zelfrijdende auto's, levert al veel inzichten voor belanghebbenden. Ook fabrikanten van voertuigen en systemen alsmede verzekeraars lijken zich al tamelijk goed voor te bereiden op de mogelijke aansprakelijkheidskwesties. Het is wel van belang om die ontwikkelingen goed te volgen en daarop zo nodig te anticiperen. Zo wordt bijvoorbeeld ten aanzien van de bewijslast nadrukkelijk gesproken over de mogelijkheid om een zogenoemde Event-data-recorder (EDR) in coöperatieve voertuigen te installeren, om zo de bewijsvoering bij ongevallen te vergemakkelijken. Een dergelijke voorziening zal wel onmiddellijk nieuwe dataproctectie- en datazeggenschapsvragen met zich brengen. Welke vragen en eisen dan vooral van toepassing zijn op C-ITS kan wel nader in beeld worden gebracht. Die behoefte lijkt er bijvoorbeeld wel te zijn bij projecten van BBV, al is het maar om van mogelijke fouten te leren.

Vraag:

Welke juridische issues kan de installatie van een EDR met zich meebrengen?

Documenten:

- Relevante NL wetgeving
- Onderzoeksrapporten in opdracht van het Ministerie van I&M
 - Zelfrijdende auto's en het Verdrag van Wenen inzake het wegverkeer (I&M-VU 2015)

- Aansprakelijkheidsaspecten van zelfrijdende auto's (I&M-VU 2015)

[Aanpak Connecting Mobility en Ditcm na de kick-off meeting](#)

In de eerste juridische tafelsessie is in samenspraak met de aanwezige stakeholders de nodige richting gegeven aan de aanpak voor de voorziene tafelperiode, tot 1 oktober 2015. Afgesproken is om op basis van de lijst van use cases die ook bij de tafels 'Dutch Profiles' en 'Architectuur' worden gebruikt een viertal use cases te selecteren voor nadere analyse. De doelstelling is om binnen de afgesproken format te komen tot een samenhangend inzicht waardoor juridische issues kunnen worden gedetecteerd en zo nodig opgelost.

Bijlage 1

Voorgestelde use cases aan de juridische tafel van 11 juni 2015.

Voorstel:

Breng in het kader van de risk-assesment bij de onderstaande use cases de juridische risico's in kaart.

Use Cases

Coöperatieve adviesdienst data

Bij deze dienst grijpt het coöperatieve systeem niet rechtstreeks in in de techniek van het voertuig, maar voorziet een display in de auto in adviezen ten aanzien van de snelheid of rijbaan, vooralsnog alleen op snelwegen. De bestuurder blijft dus in control van het voertuig. Voorbeeld: Spookfiledienst A58.

Floating vehicle data

Floating vehicle data zijn verkeersgegevens die doorlopend worden verzameld van GSM en GPS systemen die weggebruikers aan hebben staan, zoals bijvoorbeeld reistijden. Bij deze use case spelen zowel de herleidbaarheid van de gegevens tot een concrete weggebruiker, de zeggenschap over deze gegevens, die immers een commerciële waarde vertegenwoordigen en de aansprakelijkheid bij het gebruik van de gegevens een rol.

Road works warning data

Floating vehicle data zijn verkeersgegevens die doorlopend worden verzameld van GSM en GPS systemen die weggebruikers aan hebben staan, zoals bijvoorbeeld reistijden. Bij deze use case spelen In het kader van Road Works Warning (RWW) ontvangt het naderende verkeer bij wegwerkzaamheden waarschuwingen en beperkingen van bijvoorbeeld snelheid of inhaalmogelijkheden. De juridische aspecten zitten hier met name in de dataprotectie bij het gebruik van de floating car data en de aansprakelijkheid door eventuele fouten die tot schade leiden.

Compass4D verkeerslichtdata

Bij Compass4D zendt en ontvangt een voertuig via een on board unit doorstroom informatie. Hierdoor kunnen de verkeerslichten worden beïnvloed hetgeen de doorstroming bevordert. Bijzondere voorrang kan worden gecreëerd voor bijvoorbeeld hulpdiensten en openbaar vervoer. Juridische vragen kunnen zich voordoen rond privacy en aansprakelijkheid.