
# Notitie Juridische aspecten van C-ITS 2015

7 DECEMBER 2015

Marcel Otto - Wouter van Haaften
DITCM INNOVATIONS | WWW.DITCM.EU

# Notitie van de Landelijke Ronde Tafel Juridische Aspecten van C-ITS, 2015

## 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 voorlopersrol vervullen bij de ontwikkeling van C-ITS. De beoogde coöperatieve systemen zullen echter niet stoppen aan de grens. Dat betekent dat de ontwikkelingen in Nederland zullen moeten passen in deze internationale context. 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 het gaat om de vraag naar de juridische inbedding van C-ITS dan kun je onderscheid maken in twee soorten wetgeving. De eerste is de ordeningswetgeving waarin regels worden gesteld voor voertuigen en voor het verkeer. Deze regels zullen ongetwijfeld aan de veranderingen in de techniek, zoals zelfsturend en coöperatief rijden moeten worden aangepast. Deze uitdaging wordt op wereld schaal opgepakt in de vorm van aanpassing van het Verdrag van Wenen. Dat geldt minder voor de algemene rechtsgebieden die in het kader van C-ITS van belang zijn, zoals aansprakelijkheid, data-protectie en data-zeggenschap. Deze kennen hun eigen regels die niet zo snel aan een nieuw technisch en maatschappelijk fenomeen als C-ITC zullen worden aangepast. Een uitzondering vormt op termijn wellicht de aansprakelijkheid, die door de komst van zelfsturend en coöperatief rijden aanleiding kan geven tot de keuze in te grijpen in het wettelijk kader. Als je een jurist echter vraagt of zelfsturend of coöperatief rijden in de praktijk een juridische regeling vergt ten aanzien van dataprotectie of datazeggenschap, 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, met uitzondering van zeer specifieke wetgeving, vanzelf een plaats in het bestaande recht. Als vervolgens 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 nieuw recht zich aandient, dan zal overwogen worden dit nieuwe recht in de wet op te nemen.

Toch is het goed om goed te kijken naar de algemene 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 wilden we naartoe in 2015

In het tweede halfjaar van de Tafel Juridische Aspecten is het streven erop gericht geweest 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 ging daarbij vooral om:

- Het ontwikkelen van kennis en bewustzijn bij NL belanghebbenden over mogelijke juridische problemen en oplossingen op het terrein van C-ITS.
- Het ondersteunen van 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.

## Aanpak Connecting Mobility en Ditcm voor 2015 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 en met 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. De eerste fase is de voorbereiding van de workshops rond de verschillende rechtsgebieden. Deze zal met de meest betrokken tafelgenoten worden gedaan. Uitkomst van deze verkenning is een overzicht van gedetecteerde juridische issues. Deze zullen in verschillende workshops worden gehanteerd bij de risicoanalyse van de geselecteerde use cases.

## Waar staan we aan het eind van 2015

Aan de tafel 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.

### Dataprotectie.

De regels rond dataprotectie vloeien voort uit EU richtlijnen, die in Nederland zijn opgenomen in de Wet bescherming persoonsgegeven, terwijl de voor C-ITS relevante bijzondere dataprotectieregels zijn opgenomen in de Wet bescherming Persoonsgegevens(WBP), en de daaraan ten grondslag liggende Richtlijn (EG) nr 95/46. 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 vast, en dus zullen de activiteiten 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 voor 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. Om meer zicht te krijgen op de mogelijke privacy risico's binnen de verschillende C-ITS ontwikkelingen is een risico analyse dataprotectie uitgevoerd. Daarbij kwam de vraag aan de orde wat nu precies de privacy risico's zijn van C-ITS diensten en hoe de privacy van de gebruikers het beste kan worden beschermd. Ook werd al in de aanloop naar de sessie de vraag gesteld in welke mate anonimiseren van data mogelijk is en of dit een afdoende bijdrage kan leveren aan het behouden van de privacy van de gebruiker.

### Risico-analyse[1]

## Samenvatting

Op 3 september werd de risico-analysesessie dataprotectie gehouden aan de hand van de vier geselecteerde use cases: Road works warning, Spookfiles, Floating car data en Verkeerslicht beïnvloeding. Tijdens de sessie is de indeling in use cases losgelaten. Deels omdat de use cases waar het om privacy ging nogal overlapten, maar ook omdat tijdens de bijeenkomst bleek dat behandeling per use case met name voor de externe dataprotectie deskundigen een meer gedetailleerde voorbereiding vergen. Ondanks, of misschien wel dankzij, deze aanpassing is een groot aantal zeer uiteenlopende risico's benoemd. Om de risico's zinvol te kunnen analyseren, prioriteren en van maatregelen te voorzien zijn ze onder verdeeld in hoofd- en subgroepen. De hoofdgroepen zijn:

- Beleidsmatige risico's
- Operationele risico's

Na deze indeling bleef nog een zeer kleine restgroep over.

### Beleidsmatige risico's

De beleidsmatige risico's zijn onder te verdelen in verschillende groepen. Ten eerste de politieke risico's. Die liggen met name op het vlak van negatieve beeldvorming (zie KM heffing), ongeacht of deze op feiten is gebaseerd of niet. Ook een mogelijke of gepercipieerde bedreiging van de keuzevrijheid van de bestuurder om zijn route zelf te kiezen valt daaronder. Vervolgens kunnen problemen optreden bij de doelbinding. Hier gaat het om of de doelen helder genoeg zijn, of het doel niet wordt opgerekt of dat het onderscheid tussen doelen waarmee is ingestemd en wettelijke doelen zoals opsporing en –fiscale- controle wel helder genoeg is. Een andere groep risico's heeft betrekking op de grondslag van de verwerking van persoonsgegevens. Daarbij kan worden gedacht aan het doorleveren van gegevens zonder voldoende wettelijke grondslag, en tot het combineren van allerlei op zich legitiem verkregen persoonsgegevens tot een ongewenst persoonsbeeld (profiling). Het gebruik door bestuursorganen van hun wettelijke bevoegdheden tot het opvragen van gegevens is gebaseerd op een separate rechtsgrondslag. Onvoldoende besef van deze wettelijke bevoegdheden bij de gebruikers kan hier tot problemen leiden als deze niet vooraf worden gewezen op het feit dat de dienstverlener geen zeggenschap heeft over het gebruik van wettelijke bevoegdheden bij opsporing, staatsveiligheid en belastingcontroles.

[1] Bevindingen risico-analyse C-ITS 2015 in bijlage 5

Ook internationaal kan het nodige misgaan. Zo bestaan er, ondanks de zelfde wettelijke basis in de Privacy Richtlijn, aanzienlijke verschillen tussen de wetgevingen van de West-Europese landen. Ook van de kant van de OEM's komt een bedreiging voor zover zij bijvoorbeeld onvoldoende samenwerken. Dat laatste lijkt overigens niet het geval gelet op het gemeenschappelijk protocol dat de Europese OEM's recent hebben uitgebracht. Ook werd een teveel aan dataprotectiemaatregelen als een risico gezien.

### Operationele risico's

Bij de operationele risico's was er vooral zorg over externe inbreuken, waarbij een gebrek aan (fysiek) toezicht als reëel risico werd gezien. Dit zou kunnen leiden tot onbevoegd volgen van voertuigen en sabotage van het C-ITS systeem. Ook de niet-naleving van de wettelijke bepalingen werd als risico aangemerkt. Daarbij gaat het om het niet in acht nemen van bewaar- en vernietigingstermijnen, het op de juiste wijze invullen van de rol van de verantwoordelijke en bijvoorbeeld snelheidshandhaving door gebruik te maken van de C-ITS voorziening. Function creep behoort ook tot deze categorie. In de restcategorie kwam nog naar voren dat de privacy belangen heel goed op gespannen voet kunnen komen te staan met de commerciële belangen van dienstverleners en OEM's.

## Conclusie

Als voorlopige conclusie kan worden vastgesteld dat anonimiseren van persoonsgegevens in een zo vroeg mogelijk stadium plaats moet vinden voor een optimale dataprotectie. Niettemin zullen privacy by design en privacy by default nooit alleen tot een goed resultaat kunnen leiden. Ook de verantwoordelijkheden voor data controller en data processor zullen goed moeten worden belegd voor de C-ITS en Connected toepassingen. Het ontwikkelen van privacy bewustzijn bij alle betrokkenen is een belangrijke voorwaarde voor succes. Dataprotectie is voor C-ITS toepassingen een license to operate. Zonder adequate dataprotectie is er voor de meeste C-ITS toepassingen geen bestaansrecht, laat staan een business case. [2]

### Datazeggenschap.

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 in principe een kwestie van bilaterale overeenkomsten tussen de verschillende betrokken partijen. Bij onderling dataverkeer tussen weggebruikers ligt een dergelijke overeenkomst niet voor de hand en zal moeten worden gekeken naar alternatieve rechtsvormen. Het overzicht dat ten behoeve van de Werkgroep 4 van het EU 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 en de wegbeheerder.

Bij het maken van een goede belangenafweging moet zeker de positie van de eindgebruiker worden betrokken. Tevens moet worden gezorgd voor transparantie en accountability met betrekking tot doel van en werkwijze bij de overdracht van data. Aan de hand van de uitkomsten van de risicoanalyse kan met alle betrokkenen worden gezocht naar een evenwichtig gemeenschappelijk

[2] Documenten in bijlage 3

model waarin alle partijen zich kunnen vinden. Daarbij zal met name de positie van de eindgebruiker als relatief zwakke partij moeten worden bewaakt.

Een bijzonder plaats als het gaat om datazeggenschap 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. Een van de vragen die het meest urgent lijkt binnen het datazeggenschapsdomein is hoe datazeggenschap op een evenwichtige manier moeten worden verdeeld tussen de verschillende stakeholders, van autofabrikant tot en met eindgebruiker.

### Risicoanalyse[3]

#### Samenvatting

Op 10 september werd de risico-analysesessie datazeggenschap gehouden aan de hand van de vier geselecteerde use cases: Road works warning, Spookfiles, Floating car data en Verkeerslichtbeïnvloeding. Bij Road works warning liggen de risico's vooral bij het ontbreken van consensus over de zeggenschapsverdeling, waardoor mogelijk bepaalde data misschien niet meer beschikbaar zijn in bepaalde gevallen. Hetzelfde risico kan zich voordoen bij Spookfiles. Het datazeggenschapsrisico bij Floating Car Data is vooral dat de zeggenschap niet goed geregeld is tussen de verschillende partijen, gebruikers, OEM's/SP's en wegbeheerder, terwijl deze data wel de basisgrondstof vormen voor veel C-ITS toepassingen. Ook belemmerende of uiteenlopende voorwaarden die OEM's stellen aan de levering van data zijn alleen met heldere afspraken over de datazeggenschap het hoofd te bieden. Bij de verkeerslicht beïnvloeding kan de datazeggenschap in relatie tot de prioritering bij de verkeerslichten tot onduidelijkheid leiden. Ook de zeggenschap over eventueel opgebouwde intelligentie in het systeem zal goed moeten worden geregeld[4].

### Aansprakelijkheid

Recent onderzoek van de VU naar de aansprakelijkheid in relatie tot zelfrijdende auto's, levert veel inzichten voor belanghebbenden. Ook fabrikanten van voertuigen en systemen alsmede verzekeraars lijken zich al tamelijk goed voor te bereiden op de mogelijke aansprakelijkheidskwesties, zoals onder meer blijkt uit het AON-rapport 'Als de auto autonoom wordt'. Om de ontwikkelingen goed te volgen en daarop zo nodig te anticiperen zal AON aan de juridische tafel worden uitgenodigd. In het rapport 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 dataprotectie- en datazeggenschapsvragen met zich brengen. Welke vragen en eisen dan vooral van toepassing zijn op C-ITS kan wel nader in beeld worden gebracht. Enkele van deze vragen werden al in de aanloop naar de risicoanalysesessies geformuleerd, zoals de vraag welke juridische issues de installatie van een EDR met zich mee kan brengen. En hoe te komen tot een afweging tussen belangen van voor o.a. gebruikers, fabrikanten en overheden. Ook de vraag naar de

[3] Bevindingen risico-analyse C-ITS 2015 in bijlage 5
[4] Documenten in bijlage 3

verdeling van de aansprakelijkheidsrisico's over partijen en de rol van de verzekeraars hierbij zal moeten worden beantwoord.

### Risico-analyse[5]

## Samenvatting

Op 10 september werd de risico-analysesessie aansprakelijkheid gehouden aan de hand van de vier geselecteerde use cases: Road works warning, Spookfiles, Floating car data en Verkeerslichtbeïnvloeding. Vooropgesteld kan worden dat de wettelijke bescherming van het slachtoffer niet verandert doordat de bestuurder slechts van advies wordt voorzien. Dus als het gaat om aansprakelijkheid bij Road works warning dan zal deze vooralsnog niet erg veranderen zolang het om adviezen gaat en niet om technische ingrepen in het voertuig. Wel zal de aansprakelijkheidsverdeling tussen wegbeheerder, in-car dienstverlener en bestuurder afhankelijk van de omstandigheden en de aard van de dienst onduidelijker kunnen worden. Bij Spookfiles speelt ook een adviessituatie en kan mogelijk dezelfde onduidelijkheid ontstaan. Wat gebeurt er als een aanrijding plaatsvindt terwijl de bestuurder het advies opvolgt? Of juist negeert? Dezelfde onduidelijkheid kan op den duur ontstaan bij het gebruik van Floating car data. Bij de verkeerslichtbeïnvloeding kan het falen van het systeem, waarbij beide rijrichtingen 'groen licht' hebben wellicht kunnen leiden tot een meer gedeelde aansprakelijkheid tussen de wegbeheerder en de verantwoordelijke voor het systeem. Daarbij komt nog het risico van samenloop en cumulatie van toepassingen die tot een exponentiele toename van de complexiteit kan leiden, met alle gevolgen voor de aansprakelijkheidsverdeling van dien.[6]

[5] Bevindingen risico-analyse C-ITS 2015 in bijlage 5
[6] Documenten in bijlage 3

Bijlage 1

**Use Cases**

Tijdens de tafelbijeenkomst van 6 juni is een viertal use cases geselecteerd om nader te onderwerpen aan een juridische risico-analyse die in de eerste helft van september zal plaatsvinden. Vastgesteld is dat de beschrijvingen van de use cases nog niet scherp genoeg zijn voor een dergelijke analyse. De desbetreffende tafel verwacht begin september de use cases voldoende scherp te hebben gedefinieerd. Het gaat om de volgende use cases:

### Snelheidsadviesdienst

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

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 verkeerslichten

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

Bijlage 2
EU C-ITS WG 4

**Documenten**

Ontwerp input CAM/DENM berichten derde meeting WG 4 Governance en Privacy

Het document is geschreven vanuit het ETSI perspectief met betrekking tot de security van Cam/Denm berichten. Een misvatting in het document lijkt dat met goede security ook de privacy beschermd is. Security is weliswaar een voorwaarde voor privacy, maar niet afdoende. Van groot belang bij privacy zijn niet alleen de externe- maar met name ook de interne bedreigingen. Wat gebeurt er met de verzamelde gegevens? Welke ketenpartners beschikken over persoonsgebonden lokatiegegevens?

In het stuk wordt gerefereerd aan 'services'. Niet duidelijk is welke services worden bedoeld. In de Richtlijn wordt onderscheid gemaakt in drie soorten diensten:

1. Telecommunicatiediensten, geleverd door de telecom serviceprovider, zoals bellen sms etc.
2. Diensten van de informatiemaatschappij, geleverd door webwinkels. De beperkingen hebben betrekking op het plaatsen van cookies.
3. zou de summary vervangen door:

1. CAM en DENM messages bevatten persoonsgegevens met extra bescherming vanwege de combinatie met locatiegegevens.
2. Het gebruik van CAM DENM berichten vraagt altijd een informed consent van de voertuigeigenaar/gebruiker. De bewijslast ten aanzien van het verkrijgen van het consent en ten aanzien van het verstrekt hebben van de relevante informatie ligt bij de dienstverlener.

Legal basis for processing personal data in C-ITS context 0.1 (30 March 2015, Kujala)

Dit document kiest weer een ander uitgangspunt, niet beveiliging, maar de ETSI definitie. Dat levert het probleem op dat daarin de value added services anders worden gedefinieerd. Alle drie ETSI categorieën vallen binnen de Richtlijn definitie van value added services.

In het document wordt gekeken naar art. 7 van de Richtlijn 95/46/EC terwijl de gedetailleerde regeling voor telecommunicatiediensten te vinden is in Richtlijn 2002/58. Daardoor is het document slechts beschrijving en deels interpretatie van de Richtlijn. Meer van belang is om te kijken naar wat er feitelijk gebeurt.

Gelet op de basisrichtlijn en de meer specifieke Richtlijn 2002/58 stelt het document dat twee grondslagen voor de verwerking van data in C-ITS het meest voor de hand liggen:

1. informed consent , een verzwaarde vorm van het genoemde consent uit Art. 7a
2. Verwerking in het kader van de C-ITS dienstverleningsovereenkomst

De overige gronden zijn niet goed voorstelbaar tenzij er een C-ITS wet komt met verplichte deelname(7c), bijvoorbeeld op termijn voorstelbaar bij full automated driving, of e-call ter bescherming van een vitaal belang van de betrokkene wordt aangemerkt (7d), of de verkeersveiligheid als noodzakelijk publiek belang wordt gedefinieerd dat een inbreuk op de privacy rechtvaardigt (7e). zal niet snel als grond worden aangemerkt, tenzij bijvoorbeeld bij e-call. Bij de gerechtvaardigde belangen (7f) wordt verwezen naar een stuk van WP29, (Privacy commissioners) van 2014 over dit artikel. Het stuk geeft handvatten om in concrete gevallen tot een juiste afweging van de 'legitimate interests' te komen, maar lijkt mij minder geschikt om in het algemeen een toepasbaarheid van het artikel bij C-ITS uit af te leiden.

De conclusie stelt terecht dat buiten art 7a (informed) consent, er geen artikel in de Richtlijn 95/46/EG is dat de juridische basis voor het gebruik van persoonsgegevens in algemene zin rechtvaardigt. Deze conclusie valt samen met het in dit kader van toepassing zijnde Artikel 9 en overweging 35 van de Richtlijn 2002/58/EG, waarin over de behandeling van locatiegegevens niet zijnde verkeersgegevens wordt vastgelegd dat deze uitsluitende met ondubbelzinnige toestemming van de betrokkene mag plaatsvinden.

De vraag of de gebruikte data binnen C-ITS persoonsgegevens zijn wordt in een ander paper of hoofdstuk behandeld. (nog niet beschikbaar)

### Navigating the C-ITS Data Protection Landscape

Dit verzameldocument omvat ook de voorgaande documenten als hoofdstukken. Data protectie wordt sterk benaderd vanuit de beveiliging. Het document heeft bovendien dataprotectie in de kop, maar lijkt breder door het toevoegen van governance, data-elementen en procesinformatie. Aan de andere kant moet het stuk specifiek handreikingen gaan bieden voor de omgang met data door zowel de overheid als belangstellende app-bouwers. Het belang van locatie als essentieel data-element wordt niet onderkent, behalve bij diensten als points of interest, parking app's en lokale e-commerce. De geschetste bedreigingen omvat niet alleen dataprotectie- maar ook andere bedreigingen, zoals gebrek aan controle over dataverkeer vanuit de auto, hergebruik, profiling, verlies van anonimiteit, verlies van vertrouwen in het ITS-systeem en misbruik. Aan de andere kant worden de mogelijkheden van ongewenste identificatie via CAM en DENM berichten met persoonsgegevens onderkent. Daarbij wordt steeds uitgegaan van een aanval van buitenaf, en niet ingegaan op interne bedreigingen in de informatieketen van verantwoordelijke dienstverleners en verwerkers. Op de externe bedreigingen worden maatregelen genomen (Guidance) die door de lid-staten kunnen worden gebruikt bij proeven en implementatie. Naast aanbevelingen zijn voorlopige conclusies getrokken op basis van wat tot nu toe in het rapport is opgenomen. De belangrijkste is dat de privacyrichtlijnen van toepassing zijn, maar bij de interpretatie daarvan lijken nog geen deskundigen op het gebied van dataprotectie te zijn betrokken. In de commentaren van WG-leden wordt nader verwezen naar de EU dataprotectie richtlijnen zonder dat daaraan concrete conclusies worden verbonden. De aanbevelingen komen neer op het advies je aan de (privacy) wetgeving te houden.

### Report Osborne Clarke advocaten

In een rapportage van het advocatenkantoor van augustus 2014 wordt de regelgeving rond e-call en verzekeren met behulp van een EDR in de conceptfase weergegeven. Inmiddels is de Verordening e-call van kracht (Vo (EU) nr 305/2013), en de concept verordening dataprotectie kan eind 2015 gereed zijn.

Altijd aan de wet houden als het om dataprotectie gaat lijkt het devies, zowel uit juridisch als uit marketing oogpunt. Bij e-call is de dataprotectiewetgeving van toepassing. Er is dus geen sprake van een in te vullen juridisch tekort.

Het gaat ook hier vooral om een marketingafweging voor de verzekeraars zoals bijvoorbeeld: moet er een premiedifferentiatie komen naar mate van informatieverstrekking?

Bijlage 3, Documenten

Documenten Data Protectie

- NL-Wetgeving en toelichtingen
- Onderzoek juridische aspecten Spookfiles A58
- 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 grond 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. Het stuk vermijdt iedere verwijzing naar de van toepassing zijn de wetgeving, volgens welke de fabrikanten verantwoordelijk zijn voor de bescherming van de door hen verzamelde persoonsgegevens, hetzij als verantwoordelijke hetzij als verwerker van persoonsgegevens.*

- 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 van het voorstel zeer sterk afwijkt van het oorspronkelijk ontwerp van 2012, maar dat de wijzigingen ten opzichte van de huidige Richtlijn veelal beperkt zullen blijven tot aanscherpingen van het toezicht en de handhaving. Gezien de vele onzekerheden in de discussie hierover is een beoordeling voor het doel van de juridische tafel op dit moment minder zinvol. Inmiddels is de EU Raad van Ministers het eens geworden over een ontwerp tekst. Over de verschillende teksten zal in het komend halfjaar worden onderhandeld*

*tussen de EU Raad, het EU Parlement en de EU Commissie. Als er eind 2015 een Verordening is kan deze in 2018 in werking treden. De directie HBJZ van IenM zal in juli een impactanalyse te maken van de verordening voor ons beleidsterrein. In augustus gevolgd door een analyse van de wettelijke grondslag voor de uitgebreide dataverzameling met C-ITS. Daarbij zullen zij onder meer het advies van WRR van ca. twee jaar geleden, diverse adviezen Rathenau en de kamerbrief van de Minister van EZ van nov. 2014 over bi data, dataprofiling en privacy betrekken.*

- Stukken van WG4 (9 juni 2015) System's Governance & Privacy onder het Europese C-ITS Platform. (zie bijlage 2)

Documenten Data zeggenschap

- Relevante NL wetgeving
- Onderzoek juridische aspecten Spookfiles A58
- Access to vehicle resources and data (summary for the C-ITS Platform WP 6, nieuwe versie op komst). (nb. Dit document richt zich vooral op technische mogelijkheden en niet de principiële uitgangspunten).

Aansprakelijkheid

- 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)
- Als de auto autonoom wordt (AON, april 2015)
- Onderzoek juridische aspecten Spookfiles A58

Bijlage 4, Definities

Definities van connected en coöperatief, zoals gebruikt door WG5 van EU C-ITS Platform:

| |
|---|
| Connected means that data/information will be sent to and from vehicles/drivers (or broader road users) [by all communication means but mainly] by cellular 3/4G/LTE (for information and advice) and for specific critical services by short range Wifi-p (warnings). The information received in the vehicle will be used by the drivers themselves. |
| Cooperative means that the data will be sent from roadside to and from the vehicles (V2I2V) and between vehicles (V2V) [by all communication means but mainly] by short/range Wifi-p (control and warnings) [and less by cellular 3/4G/LTE (for less critical services)]. In the “cooperative” situation real coordination takes place between vehicles mutually and between vehicles and roadside. This coordination can take place by a driver action (max speed; initially during day one) or automatically by the vehicle systems themselves (eg CACC). |

[] tussen haakjes de tekst waardoor het veel gehanteerde onderscheid tussen cellular en Wifi-p wordt gerelativeerd.

Bijlage 5

# Risicoanalyse projecten C-ITS

## Samenvatting

Vroeg gelet op de stand van zaken. Daarom zal in vervolgtraject regelmatig bij juridische risicos moeten worden stilgestaan, met name op momenten waarbij strategische beslissingen worden genomen. De gekozen vorm was risico's per use case, maar bij privacy kon deze minder goed gevolgd worden door ontbreken van voldoende detailkennis over de use cases in de groep.

Bij privacy spelen, naast een aantal wettelijke vereisten waaraan de C-ITS oplossing moet gaan voldoen, twee risico's een bijzondere rol. Om te beginnen het politieke afbreukrisico, waarbij C-ITS geframed wordt als een bedreiging voor de privacy ('spionagekastje'). Hierdoor kan de voortgang van de ingezette ontwikkeling ernstig worden belemmerd. Daarnaast is ook de beveiliging van de open wifi-p communicatie van CAM berichten een punt van zorg. Doordat auto's onversleutelde CAM-berichte gaan uitzenden zullen deze berichten, die persoonsgegevens bevatten, door iedereen kunnen worden ontvangen en eventueel verwerkt. Dit is in strijd met de voorgeschreven data protectie in de Wet Bescherming Persoonsgegevens. Bij de huidige keuze voor Wifi -P ligt hier een uitdaging.

Bij data zeggenschap lijkt het risico vooral te zitten in het claimen van de zeggenschap door de OEM's en misschien in iets mindere mate de dienstverleners. Het feit dat de zeggenschap over de data niet transparant is maar diffuus wordt door velen als een risico gezien. Een vergroting van de zeggenschap van de gebruiker zou de acceptatiegraad van coöperatief rijden ten goede kunnen komen. Ook kan het ontbreken van een heldere data zeggenschapsverdeling leiden tot ontbreken van een heldere verantwoordelijke ten aanzien van de kwaliteit van de data. Zowel slechter bruikbare data als het totaal wegvallen van data stromen kunnen daarvan het gevolg zijn.

In het geval van aansprakelijkheid blijven de gevolgen beperkt omdat vooralsnog het model, uitgaat van een volledig verantwoordelijke bestuurder en een verplichte verzekering. De werkelijke juridische risico's gaan schuil achter de verzekeraars die hun eigen manieren zullen vinden om met de risico's die hen aangaan om te gaan. Wel zijn een aantal mogelijke juridische risico's benoemd. Die spelen meestal op het moment dat er een advies wordt gegeven waarbij zowel het opvolgen als het negeren ervan tot schade zou kunnen leiden. Dit speelt met name bij adviesdiensten. Een bijzondere positie heeft daarbij de wegbeheerder met een wettelijke taak waar hij niet omheen kan. Ook de risico's als een systeem autonoom zelflerend wordt en op basis daarvan beslissingen gaat nemen kan tot nieuwe aansprakelijkheden leiden.

## Inleiding

Bij de start van de ronde tafel juridische aspecten van C-ITS is de behoefte aangegeven aan het inschatten van de juridische risico's van een aantal C-ITS use cases. Daartoe is een risicoanalyse ingepland om zo vroeg mogelijk zicht te krijgen op mogelijke juridische bedreigingen bij het ontwikkelen en uitrollen van de verschillende use cases. Daarbij werd het feit dat de meeste use cases nog in een vrij pril stadium zijn en dat dus nog niet veel feitelijke uitrol had plaatsgevonden op de koop toe genomen. Doordat de gesignaleerde risico's door de deelnemers, leden van de juridische tafel aangevuld met enkele deskundigen, vanuit heel verschillende invalshoeken en disciplines werden aangedragen is een enigszins eclectisch beeld ontstaan dat weliswaar de aard van het veld in

dit stadium goed weergeeft, maar dat ook vraagt om updates van de risicoanalyse gedurende de ontwikkeling van de use cases.

## Doel en opzet risicoanalyse

Het doel van de juridische risicoanalyse was:

- Het tijdig signaleren van juridische knelpunten
- Het tijdig signaleren van de eventuele wenselijkheid van wetswijziging
- Het tijdig signaleren van de wenselijkheid van beheersactiviteiten als afspraken en communicatie
- Het tijdig signaleren van mogelijke showstoppers op basis van geldend recht

Om dit doel te bereiken is gekozen voor aparte sessies per juridisch aspect, dataprotectie, datazeggenschap en aansprakelijkheid. Vanuit een urgentieperspectief waren vier use cases aangewezen die in aanmerking kwamen om als eerste te worden geanalyseerd. In de sessies werden de use cases geconfronteerd met het juridisch kader op een van de juridische aspectgebieden. De uitkomsten van de brainstorm werden vastgelegd zijn in deze rapportage opgenomen.

## Use cases

Binnen het programma Connecting Mobility is een prioritering aangegeven van de verschillende projecten en bijbehorende use cases naar staat van ontwikkeling. De meest vergevorderde use cases komen het eerst voor een risicoanalyse in aanmerking. Dat geldt ook voor de juridische risicoanalyse. Op die basis zijn vier use cases vastgesteld voor risicoanalyse. Daardoor is bijvoorbeeld niet gekeken naar verscheidenheid in de mogelijke juridische aandachtspunten. De vier use cases zijn:

- Corridor (Waarschuwing wegwerkzaamheden)
- Spookfiles A58
- Floating car data (Probe data)
- Compass4D, (verkeerslicht beïnvloeding)

*Waarschuwing wegwerkzaamheden*

Bij Road works warning worden via wifi-p technologie waarschuwingen over wegwerkzaamheden beschikbaar gesteld. Dienstverleners (waaronder autoleveranciers) kunnen deze informatie in de auto naar de weggebruiker communiceren.

*Spookfiles A58*

In het spookfileproject wordt een coöperatieve verkeersadviesdienst verleend, waarbij data uit het voertuig, via wifi-p naar de wegkant naar een SP wordt geleid. Verrijkt wordt doorandere SP's en vervolgens via de wegkant terug wordt geleverd in de vorm van een snelheidsadvies in het voertuig. Snelle doorloop door gebruik wifi-p. Dienst kan werken met beloningen en on line aanbiedingen van vb benzinestations. Gestart is met een connected spoor, via het mobiele telefoonnet. Het wifi-p spoor moet nog worden opgestart.

*Floating car data*

Floating car of probe data is data die op verschillende manieren vanuit voertuigen wordt verzameld. Deze data bevat onder meer trajectorium (ritkenmerken), op mac-adres. Ten behoeve van verschillende services worden onder meer de volgende gegevens gedestilleerd: brake down in reistijdinfo, herkomstbestemming info en druktemeter.

*Compass4D (verkeerslichtbeinvloeding)*
In dit project worden verkeerslichten voorzien van Wifi en kunnen zij communiceren met een beperkt aantal weggebruikers in 3 categorieën: vrachtvervoer, openbaar vervoer en hulpdiensten. Door in contact te staan met de aangesloten voertuigen kan het systeem de verkeerslichten per categorie optimaliseren, hoge snelheid voor de hulpdiensten en doorstroming voor bijvoorbeeld vrachtverkeer voor een lagere milieubelasting door minder remmen en optrekken.

### Uitvoering risicoanalyse

De uitvoering van de risicoanalyse heeft plaatsgevonden in drie sessies over twee dagdelen: op 3 en 10 september 2015. Het eerste dagdeel was gereserveerd voor dataprotectie. Een heel dagdeel omdat de groep ten opzichte van de deelnemers aan de juridische tafel het meest was uitgebreid en bij dit onderwerp de meeste discussies en heikele punten te verwachten waren. De sessies datazeggenschap en aansprakelijk bevatten a priori wat minder controversiële punten waardoor de gestructureerde aanpak aan de hand van use cases goed kon worden gevolgd.

## *Dataprotectie*

### Inleiding

In de data protectiesessie bleek al snel dat voor een goede confrontatie van de use cases met de geldende dataprotectie-wetgeving een veel gedetailleerder kennis van de use cases vereist was. Om die reden werd, met overigens de use cases in het achterhoofd, gekozen voor een brainstorm aanpak waarbij iedere deelnemer de door hem of haar gepercipieerde juridische risico's kon inbrengen. Na deze inbreng werden de resultaten in een gemeenschappelijke ronde toegelicht en waar nodig verduidelijkt. De lijst met risico's is vervolgens ten behoeve van de leesbaarheid geclusterd en van een zekere indeling voorzien. Daarbij is onderscheid gemaakt tussen risico's die zich in de voorbereidende fase van een project voordoen en en operationele risico's die van buitenaf komen na uitrol van de voorziening.

### Wettelijk kader

Bij dataprotectie is in de eerste plaats van belang welke gegevens worden verwerkt, en of deze als persoonsgegeven zijn aan te merken. Vastgesteld is dat gegevens uit een voertuig identificeerbaar zijn, en dus als persoonsgegeven aan te merken. De verwerking vindt plaats door de verzending van de gegevens en ook in de back office van de Serviceprovider(s). De set gegevens voor de toepassing van de use cases is zeer beperkt, maar met name de gevoelige locatiedata zijn essentieel voor het functioneren van de use case. De verwerking van de data moet voldoen aan de eisen van de Wet Bescherming Persoonsgegevens. Dat betekent dat het doel van de verwerking vooraf moet zijn vastgesteld, dat op basis van het informed consent van de gebruiker de verwerking kan plaatsvinden waarbij de kwaliteit van de gegevens en de verwerking wordt bewaakt en precies wordt aangegeven waarvoor de gegevens worden gebruikt en aan wie gegevens mogelijk worden doorgeleverd. Daarbij zal de verantwoordelijke zorg moeten dragen voor afdoende beveiliging en afscherming voor onbevoegden. Hergebruik van gegevens kan alleen plaatsvinden met uitdrukkelijke toestemming van

de betrokkene. Degene die de aard en omvang van de verwerking bepaald is de verantwoordelijke. Binnen C-ITS, waar veel partijen samen tot een service komen is niet altijd duidelijk wie de verantwoordelijke is. Dit zal voorafgaand aan ieder verwerkingstraject moeten worden vastgesteld.

### Use cases

In alle use cases wordt data naar de auto gezonden en/of data uit de auto verzonden door middel van een mobiele verbinding of door middel van Wifi-P. De gegevens bevatten naast voertuiggegevens ook locatiedata en een timestamp. Bij het Corridor project waarschuwing wegwerkzaamheden zijn geen gegevens uit de auto nodig en wordt het waarschuwingssignaal via broadcasting naar de auto gebracht. Bij Spookfiles gaat de locatie, snelheid en richting informatie uit het voertuig via mobiel of via Wifi-P naar de serviceprovider die per omgaande een snelheidsadvies terug levert. Hier is dus sprake van gegevens van het zenden van data uit het voertuig naar de Serviceprovider aan de wegkant. Bij floating car data gaat het om vanuit voertuigen verzamelde gegevens die in beginsel ontdaan zijn van de identificerende kenmerken. Compass4D verkeerslicht beïnvloeding maakt gebruik van een signaal naar en van de auto. De gegevens mogen niet langer bewaard dan nodig voor de verwerking. Uitzondering is de bewaarplicht voor sommige gegevens op grond van openbaar belang. De vernietiging van gegevens moet aan de eisen van transparantie en accountability voldoen, en de beveiliging moet afdoende zijn, tegen een redelijke inspanning, met state of the art technologie. In het gehele proces, vanaf het informed consent van de gebruiker tot en met het beëindigen van de dienst spelen transparantie en accountability een doorslaggevende rol.

## *Resultaten*

De brainstormsessie in de risicoanalysesessie dataprotectie leverde een veelheid aan zeer diverse risico's op. Alle risico's zijn verwerkt en gecategoriseerd. Binnen deze categorieën zijn weer verschillende groepen benoemd. De indeling in de spreadsheet is uitsluitend bedoeld om de brainstormresultaten hanteerbaar te maken.

De eerste categorie kan zich reeds manifesteren voorafgaand aan de uitrol terwijl operationele risico's pas kunnen optreden nadat er sprake is van uitrol van de C-ITS voorziening. Binnen de categorie risico's in de ontwerpfase zijn de volgende categorieën onderscheiden:

- Politieke risico's
- Risico's ten aanzien van doelbinding
- Risico's ten aanzien van wettelijke grondslag
- Risico's ten aanzien van mogelijke function creep
- Internationale risico's
- Risico's van overmatige dataprotectie.

De meer operationele risico's zijn onderverdeeld in de volgende categorieën:

- Risico's van externe inbreuken
- Risico's ten aanzien van inbreuken op wettelijke bepalingen
- Algemene operationele risico's.

### Politieke risico's

Als politiek risico werd in de eerste plaats gesignaleerd een ontstaan van een sentiment in de publieke opinie dat C-ITS een bedreiging zou zijn voor de privacy. Hoewel voor een dergelijk sentiment geen enkele aanleiding hoeft te zijn kan de beeldvorming het C-ITS project flink in de wielen rijden. Het voorbeeld van kilometerheffing in 2010 (spionagekastjes) laat zien dat de realiteit bij een dergelijk sentiment een ondergeschikte rol speelt. Voor alle betrokkenen is het dus zaak om te voorkomen dat er iets mis gaat in de privacybescherming bij projecten. Daarmee wordt het risico niet uitgebannen maar kan het wel beperkt worden. Overigens hebben alle partijen er belang bij dat C-ITS niet wordt gehinderd of zelfs gestopt door een negatieve pers.

Een ander risico op politiek niveau treedt op wanneer het coöperatieve systeem routes en alternatieve routes gaat voorschrijven op basis van coöperatieve informatie, met het oog op het – algemeen – verkeersbelang. Mocht het zover komen dan zal deze werkwijze goed met de weggebruiker moeten worden gecommuniceerd.

### Risico's doelbinding

Ten aanzien van de doelbinding werd het risico gesignaleerd dat het opvragen van gegevens op basis van wettelijke bepalingen door overheidsdiensten, zoals Politie, Justitie, AIVD en Belastingdienst bij de betrokkene tot de gedachte leidt dat de verantwoordelijke zich niet aan de afgesproken doelbinding houdt. Het risico is te beperken door de wettelijke rechten uit de WBP duidelijk naar de betrokkene te communiceren.

Ook werd als risico gezien dat het doel binnen C-ITS niet helder genoeg is omschreven, waardoor oprekking van de doelstelling mogelijk wordt. Om dit risico in te dammen zou wellicht een heldere model-doelstelling voor C-ITS geformuleerd kunnen worden.

Zelfs als het doel helder geformuleerd wordt sluit dat niet uit dat de verantwoordelijke het doel oprekt. Hier kunnen transparantie en communicatie veel ongelukken voorkomen.

### Risico's ten aanzien van de grondslag

Een van de gesignaleerde risico's was dat de overheidsdiensten hun bevoegdheden op grond van de wet kunnen oprekken, waardoor zgn. 'function creep' ontstaat. Hoewel dit geen specifiek C-ITS probleem is werd het wel duidelijk als reel risico benoemd, met name door de aanwezige overheidspartijen. Transparantie bij het gebruik van persoonlijke data door de overheid kan een hier belangrijke bijdrage leveren aan het indammen van het risico.

Het gebruik van Big Data zonder toestemming van de betrokkene kan leiden tot het ontstaan van nieuwe persoonsgegevens. Hierdoor ontstaat het risico van bijvoorbeeld profiling zonder dat de betrokkene daar weet van heeft. Naast het betrachten van transparantie en accountability zal hierop door de toezichthouder moeten worden gehandhaafd.

### Grensoverschrijdende risico's

Onder de kop internationale risico's werd met name gewezen op het risico dat er ondanks het feit dat de basis wetgeving gelijk is , toch verschillen bestaan in de interpretatie tussen de lidstaten. Ook nadat de nieuwe Verordening van kracht is geworden zullen er tussen lidstaten juridische verschillen blijven bestaan die op trajecten als de Corridor tot problemen kunnen leiden.

Datzelfde risico geldt voor het communiceren tussen voertuigen van een verschillend merk. Door het vooralsnog ontbreken van standaards en open source oplossingen kan het gebrek aan interoperabiliteit tussen landen remmend werken op de introductie van C-ITS.

### Risico van teveel dataprotectie

Een curieus risico dat werd gesignaleerd is dat van een teveel aan dataprotectie. Daardoor zou bij de gebruiker terughoudendheid kunnen ontstaan: 'zoveel kleine lettertjes, laat ik dit maar niet doen'. Privacy by design en bij default lijken hiervoor goede oplossingen.

Ook kunnen wettelijke beperkingen van het data gebruik er toe leiden dat innovatie en gebruik stokken. Privacy by design en privacy by default kunnen in dit verband goede oplossingen zijn.

### Risico van externe inbreuken

Een eerste risico in deze categorie betrof de fysieke bewaking van wegkantbakens. Inbraak, manipuleren van gegevens en onbevoegd aftappen van gegevens zijn een bedreiging van de privacy. Het systeem zal om dit risico te mitigeren afdoende moeten worden beveiligd.

Het onbevoegd verzamelen van - onversleutelde - CAM berichten is ook een extern risico. Het risico hier zit niet zozeer in de applicatie maar in het feit dat coöperatieve voertuigen zich gedragen als rijdende zendmasten, zoals nu met de keuze voor Wifi-P het geval is. Het roept de vraag op of de berichten toch versleuteld moeten worden. Als dat niet mogelijk is, dan zal moeten worden naar andere (technische) methoden om data-protectie te waarborgen.

Ook het onbevoegd verzamelen van locatiegegevens en traceren van verplaatsingsgedrag – bijvoorbeeld met behulp van verkeerslichtregelingbeinvloeding is een ander potentieel risico dat door middel van privacy by design gecombineerd met transparantie en accountability het hoofd kan worden geboden.

### Risico's ten aanzien van de wettelijke bepalingen

Bij deze risico's gaat het vooral om het niet naleven van de wettelijke bepalingen, zoals het niet in achtnemen van bewaartermijnen, het niet afdoende invullen van de rol van de verantwoordelijke, het misbruiken van data bijvoorbeeld voor analyse van het rijgedrag ten behoeve van verkeersbeïnvloeding of van verzekeraars. Veel van deze risico's zullen door transparantie en good governance moeten worden afgewend en in het uiterste geval worden gehandhaafd door de toezichthouder.

### Algemene risico's

Het betreft hier risico's van algemene aard die inherent zijn aan de gekozen techniek en aan het gekozen businessmodel. In technische zin is privacybescherming een licence to operate. Het niet beschermen van de privacy is immers geen optie. Hierdoor kan het risico ontstaan dat er geen techniek kan worden gevonden die C-ITS faciliteert, maar tegelijkertijd ook de privacy afdoende beschermd. Dit vergt een zorgvuldige afweging bij het inrichten van het systeem.

Een soortgelijk risico geldt ook ten aanzien van het gekozen business case. In de business case worden de commerciële belangen van de dienstverlener geconfronteerd met de privacybelangen van de betrokkene. Dit kan leiden tot ongewenste keuzes ten aanzien van de privacy aangezien anders de business case niet kan worden gehaald. Ook dit vergt een zorgvuldige afweging bij de keuze voor een bepaald business model.

## *Datazeggenschap*

In de sessie over datazeggenschap is wel de indeling naar de use cases gevolgd. Doordat datazeggenschap in het algemeen een minder prominent onderwerp is dat zich vooral tussen juristen of informatici afspeelt bleek het lastig om een goed beeld te krijgen bij de juridische risico's. Door de gekozen structuur naar aanleiding van de use cases was de inbreng van de verschillende deelnemers echter goed in het schema onder te brengen. Door het ontbreken van dwingende wetgeving verbaast het niet dat de gesignaleerde juridische risico's beperkt is in aantal.

### *Resultaten*

Hieronder zijn de resultaten van de risico-analysesessie datazeggenschap per use-case weergegeven. Bij de gesignaleerde risico's zijn remedies vermeld voor zover deze in de sessie naar boven zijn gekomen.

### *Road Works Warning*

Bij Road works warning worden via WiFi-p technologie waarschuwingen over wegwerkzaamheden beschikbaar gesteld. Dienstverleners (waaronder autoleveranciers) kunnen deze informatie in de auto naar de weggebruiker communiceren. De dienstverlening in de auto valt buiten de scope van het project ITS corridor.

De belangrijkste risico's die werden gesignaleerd waren:

1. het ontbreken van internationale consensus zeggenschapsverdeling
2. een gebrek aan kwaliteit en consistentie signaal door onduidelijkheid datazeggenschap.
3. Het niet doorgeven van data in de auto door SP/OEM.

Aangezien Road Works Warning als corridor systeem een internationale toepassing zal moeten krijgen is het van groot belang dat de verdeling van de zeggenschap tussen de verschillende partijen eenduidig wordt geregeld in de verschillende betrokken landen. Zo niet dan kan dit ertoe leiden dat de dienst slechts op nationaal niveau van de grond komt.

Remedie:
Streven naar internationale en bij voorkeur EU brede afspraken over data-zeggenschap.

Een ander probleem dat werd gesignaleerd was dat de onduidelijkheid over de zeggenschap kan leiden tot afname van de kwaliteit van het signaal, bijvoorbeeld omdat bepaalde data niet wordt doorgegeven.

Remedie:
Helder kader voor datazeggenschap voorstellen en daarover met de betrokken partijen in overleg gaan.

Dat laatste speelt helemaal als de SP/OEM geen concreet belang hebben bij het verzenden van de informatie naar de klant. Als bijvoorbeeld de OEM zich op het standpunt stelt dat alleen informatie via zijn eigen kanaal in de auto kan worden getoond.

Remedie:
Eigenlijk zijn beide voorgaande remedies hier nodig, zowel internationale afspraken, in verband met bijv. de interoperabiliteit, en een helder kader voor de verdeling van de zeggenschap om het risico verder te mitigeren.

*Spookfiles A58*

In het spookfileproject wordt een cooperatieve verkeersadviesdienst verleend, waarbij data uit het voertuig, via wifi-p naar de wegkant naar een SP wordt geleid. Verrijkt wordt door andere SP's en vervolgens via de wegkant terug wordt geleverd in de vorm van een snelheidsadvies in het voertuig. Er is een snelle doorloop mogelijk door het gebruik van wifi-p. Dienst kan werken met beloningen en on line aanbiedingen van bijvoorbeeld benzinestations, waardoor de kring van datazeggenschap mogelijk verder wordt uitgebreid.

Bij deze use case werd de onduidelijkheid rondom de datazeggenschap tussen de verschillende spelers, de gebruiker, de in-car dienstverlener, de wegkantdienstverlener, de toeleverancier en de wegbeheerder als risico genoemd voor het functioneren van het project.

Remedie:
Ook hier is de remedie gelegen in het maken van afspraken tussen de verschillende spelers. Daar bij kan een complicerende factor zijn dat de wegbeheerder vanwege zijn wettelijke taak verantwoordelijk is voor de veiligheid van de weg en dus een iets ander juridisch paradigma heeft. Een test van het systeem voorafgaand aan de uitrol kan mogelijke problemen aan het licht brengen.

*Floating car data*

Floating car of probe data is data die op verschillende manieren vanuit voertuigen wordt verzameld. Deze data bevat onder meer trajectorium (ritkenmerken), op mac-adres. Ten behoeve van verschillende services worden onder meer de volgende gegevens gedestilleerd: brake down in reistijdinfo, herkomstbestemming info en druktemeter.

Binnen deze use case werd een viertal risico's gesignaleerd tijdens de sessie:

1. Floating car data is een belangrijke grondstof voor C-ITS, maar de zeggenschap is diffuus,
2. De OEM's kunnen belemmerende voorwaarden stellen,
3. Verschillende OEM's kunnen ook verschillende voorwaarden stellen,
4. De intensiteit van de verzameling in combinatie met gebruikte algoritmes kunnen leiden tot discussie over een mogelijk gedeelde zeggenschap.

Omdat floating car data een vaste grondstof wordt voor C-IS toepassingen is helderheid over de zeggenschap gewenst. Op dit moment kunnen met name de OEMs de facto het dataverkeer vanuit de auto controleren zonder dat andere betrokkenen daar iets aan kunnen doen. Daar komt bij dat niet alle OEMs op dit punt eenzelfde lijn volgen, zoals bijvoorbeeld op het gebied van data-protectie wel het geval is. De verwerking van floating car data kan tot nieuwe data leiden waarvan de zeggenschap nog diffuser is dan van de oorspronkelijke data. Immers meer partijen hebben betrokkenheid gehad bij de totstandkoming van deze data[7].

Remedie:
Het zal niet verbazen dat ook hier is de remedie is gelegen in het maken van afspraken tussen de verschillende stakeholders. Een complicerende factor daarbij is dat veel van de data anoniem wordt verzameld, waardoor een zeggenschap van de gebruiker niet voor de hand ligt. Ook speelt een rol dat floating car data als grondstof voor C-ITS, maar ook nu al voor verkeersinformatie en verkeersonderzoek, een reële marktwaarde heeft. Bij het maken van afspraken zal dit element een belangrijke rol gaan spelen.

[7] Een lijst van mogelijke gronden voor het claimen van datazeggenschap is opgenomen in bijlage 2

### *Compass4D (verkeerslicht beïnvloeding)*

In dit project worden verkeerslichten voorzien van Wifi en kunnen zij communiceren met een beperkt aantal weggebruikers in 3 categorieën: vrachtvervoer, openbaar vervoer en hulpdiensten. Door in contact te staan met de aangesloten voertuigen kan het systeem de verkeerslichten per categorie optimaliseren, hoge snelheid voor de hulpdiensten en doorstroming voor bijvoorbeeld vrachtverkeer voor een lagere milieubelasting door minder remmen en optrekken.

Ten aanzien van het project werden twee datazeggenschapsrisico's gesignaleerd:

1. Onduidelijkheid omtrent de zeggenschap over de prioritering?
2. Onduidelijkheid omtrent de zeggenschap over zelflerende applicatie en de resultaten daarvan?

Omdat de wegbeheerder een doorslaggevende rol speelt bij de bepaling van de instellingen van de verkeerslichten als eerstverantwoordelijke voor de verkeersveiligheid op de kruispunten, zal een aanzienlijk deel van de zeggenschap bij hem liggen. Niettemin kunnen ook andere stakeholders legitieme aanspraken hebben op de data. Te denken valt aan de hulpdiensten die gebruik maken van het systeem om bij calamiteiten sneller ter plaatse te zijn. En aan de dienstverlener, de leverancier van de apparatuur en mogelijk ook andere gebruikers. De positie van de dienstverlener en leverancier speelt in het bijzonder als het gaat om de zeggenschap over de zelflerende applicatie zoals bij het tweede risico is aangegeven.

Remedie:
Door de heel concrete wettelijke rol van de wegbeheerder lijkt de ruimte voor andere zeggenschap beperkt. Toch is het goed om de publieke verantwoordelijkheid van de wegbeheerder en de private rechten van de dienstverlener/leverancier beide goed in ogenschouw te nemen bij het maken van, ook hier, afspraken.

## *Aansprakelijkheid*

Ook bij het thema aansprakelijkheid is de indeling naar use cases gevolgd. Hier meer inhoudelijke discussie tussen de verschillende deskundigen over hoe aansprakelijkheden binnen C-ITS verschuiven ten opzichte van de huidige situatie en wetgeving. De use cases boden voldoende ruimte om de gesignaleerde relevante issues een plaats te geven. Ook hier een beperkt aantal risico's, met name omdat in de use cases de rol van de bestuurder als verantwoordelijke voor de veiligheid in de auto (nog) niet verandert.

### *Resultaten*

Hieronder zijn de resultaten van de risico-analysesessie aansprakelijkheid per use-case weergegeven. Bij de gesignaleerde risico's zijn geen remedies vermeld omdat daarvoor de expertise in de sessie ontbrak. Daardoor zijn allen de gesignaleerde juridische risico's ten aanzien van aansprakelijkheid in deze rapportage opgenomen.

#### *Road Works Warning*

Bij Road works warning worden via WiFi-p technologie waarschuwingen over wegwerkzaamheden beschikbaar gesteld. Dienstverleners (waaronder autoleveranciers) kunnen deze informatie in de auto naar de weggebruiker communiceren. De dienstverlening in de auto valt buiten de scope van het project ITS corridor.

Bij Road Works Warning blijft de verantwoordelijkheid voor het voertuig volledig bij de bestuurder. Deze krijgt alleen een bepaald signaal dat er wegwerkzaamheden zijn binnen een bepaalde afstand op de weg waarop wordt gereden. Dat signaal is de verantwoordelijkheid van de wegbeheerder, die daarmee ook een zekere verantwoordelijkheid draagt. Ten aanzien van de dienst werden de volgende risico's gesignaleerd:

1. Aanrijding ondanks waarschuwingssysteem,
2. Aanrijding als gevolg van onderbroken of verkeerd signaal,
3. Onduidelijke aansprakelijkheidsverdeling tussen wegbeheerder, dienstverlener en bestuurder, afhankelijk van de omstandigheden en de aard van de dienst.

#### *Spookfiles A58*

In het spookfileproject wordt een cooperatieve verkeersadviesdienst verleend, waarbij data uit het voertuig, via wifi-p naar de wegkant naar een SP wordt geleid. Verrijkt wordt door andere SP's en vervolgens via de wegkant terug wordt geleverd in de vorm van een snelheidsadvies in het voertuig. Snelle doorloop door gebruik wifi-p. Dienst kan werken met beloningen en on line aanbiedingen van bijvoorbeeld benzinestations.

Bij het Spookfile A58 project is in deze fase sprake van een in-car adviesdienst die de klant snelheidsadviezen geeft waarmee bij het volgen daarvan mogelijk files kunnen worden vermeden. Daarbij wordt een deel van de taak van de wegbeheerder, signalering, als het ware ingevuld door een service provider. Binnen Spookfiles zijn enkele aansprakelijkheids risico's onderkend.

1. Aanrijding na opvolgen advies,
2. Aanrijding na negeren advies,
3. Adviessnelheid hoger dan tijdelijke max snelheid op borden wegbeheerder.

*Floating car data*

Floating car of probe data is data die op verschillende manieren vanuit voertuigen wordt verzameld. Deze data bevat onder meer trajectorium (ritkenmerken), op mac-adres. Ten behoeve van verschillende services worden onder meer de volgende gegevens gedestilleerd: brake down in reistijdinfo, herkomstbestemming info en druktemeter.

Omdat bij Probe data de relatie tussen de dienstverlening en de gebruikte data indirect is lijkt er geen directe relatie tussen de data enerzijds en de weggebruiker of wegbeheerder anderzijds. Niettemin zal het kunnen voorkomen dat een op probe data gebaseerde dienst leidt tot een juridisch risico. Met name als er sprake is van een:

1. Onduidelijke aansprakelijkheidsverdeling tussen wegbeheerder, dienstverlener en bestuurder, afhankelijk van de omstandigheden en de aard van de dienst.

## *Compass4D (verkeerslicht beïnvloeding)*

In dit project worden verkeerslichten voorzien van Wifi en kunnen zij communiceren met een beperkt aantal weggebruikers in 3 categorieën: vrachtvervoer, openbaar vervoer en hulpdiensten. Door in contact te staan met de aangesloten voertuigen kan het systeem de verkeerslichten per categorie optimaliseren, hoge snelheid voor de hulpdiensten en doorstroming voor bijvoorbeeld vrachtverkeer voor een lagere milieubelasting door minder remmen en optrekken.

In het geval van verkeerslichten liggen aansprakelijkheden veel directer aan de oppervlakte. Hoewel de wettelijke aansprakelijkheid van de wegbeheerder en de gebruiker ongewijzigd blijven is er wel sprake van een gewijzigde praktijk bij stoplichten. Daaruit vloeide de volgende vragen voort ten aanzien van de aansprakelijkheid bij verkeerslicht beïnvloeding. Hoe is de aansprakelijkheid geregeld als een:

1. Hulpdienst een aanrijding krijgt omdat systeem niet goed werkt,
2. Dynamisch systeem de afgesproken performance niet kan waarmaken,
3. Zelflerend systeem verkeerslichten optimaliseert zonder tussenkomst van een verantwoordelijke partij,
4. Bij een groen/groen aanrijding ingeval gebruik wordt gemaakt van verkeerslicht beïnvloeding.

# 5. Bijlage 1

Lijst van deelnemers aan de risico-analyse sessies

Data-protectie, 3 september 2015

| | |
|---|---|
| Gilles Ampt | Ronde Tafel Security |
| Tanja Braun | V-tron |
| Gerbrand Klijn | Grontmij |
| Marcel Otto | DGB (voorzitter) |
| Mike Pinckaers | ANWB |
| Josee Sombekke | SIMS4u |
| Sussanne Strolenberg | RWS |
| Wim Vossebelt | V-Tron |
| Meine van Essen | RWS |
| Vincent Habers | IAM/pBB |
| Matilda Troost | RWS |
| Evert-Jeen van der Meer | Aon |
| Martijn van der Veen | Privacy First |
| Wouter van Haaften | Universiteit Amsterdam |
| Peter de Lannoy | ANL (notulist) |

Data zeggenschap en aansprakelijkheid, 10 september 2015

| | |
|---|---|
| Tanja Braun | V-tron |
| Steven Kuiper | St. SIMS |
| Peter de Lannoy | ANL (notulist) |
| Marcel Otto | DGB (voorzitter) |
| Mike Pinckaers | ANWB |
| Josee Sombekke | SIMS4u |
| Joëlle van den Broek | DITCM |
| Wouter van Haaften | Universiteit Amsterdam |

Bijlage 2

Lijst van stakeholders die mogelijk een beroep kunnen doen op (een deel van) de datazeggenschap.

| | |
|---|---|
| De vervaardiger | de partij die de data genereert, |
| De afnemer | de partij die de data gebruikt, |
| De samensteller | de partij die data verzameld en selecteert van verschillende bronnen, |
| De onderneming | alle data die in een onderneming binnenkomt of wordt vervaardigd is geheel eigendom van de onderneming |
| De opdrachtgever | de partij die opdracht geeft tot het vervaardigen van data, |
| De decoder | de partij die versleutelde informatie ontsleutelt en zo toegankelijk maakt, |
| De verspreider | de partij die informatie verzameld en in een ander format doorlevert aan een specifieke markt of consumenten, |
| De lezer | de partij die de data tot zich neemt en toevoegt aan zijn eigen informatie, |
| Het subject | de partij die onderwerp is van de data en die eigenaarschap claimt met name als reactie op andere eigenaarschap claims, |
| De koper/licentienemer | de partij die een recht verkrijgt op het gebruik van de data en daarmee van een zekere mate van eigendom. |