Leading partners in Smart Mobility

DITCM Innovations

Bevindingen juridische risicoanalysesessies

3 en 10 september 2015

Wouter van Haaften
DITCM INNOVATIONS | WWW.DITCM.EU
31-10-2015

Bevindingen juridische risicoanalysesessies

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[1].

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.

[1] 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	
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
Ernstjan 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.