



Ministerie van Infrastructuur en Milieu

Beter Benutten

# Rapportage onderzoek juridische inbedding Spookfiles A58

Leibniz Foundation For Law

Onderzoek uitgevoerd door:  
Prof. Dr. T.M. van Engers  
Mr. W. F. van Haften  
December 2014



## Inhoudsopgave

<b>Voorwoord</b>	<b>3</b>
<b>Afkortingenlijst</b>	<b>4</b>
<b>Samenvatting</b>	<b>5</b>
<b>1. Inleiding</b>	<b>12</b>
1.1 <i>Aanleiding voor het onderzoek</i>	12
1.2 <i>Coöperatief rijden, Spookfiles A-58</i>	12
1.3 <i>Onderzoeksvragen coöperatief rijden</i>	12
1.4 <i>Doel van het onderzoek</i>	13
1.5 <i>De onderzoeksopdracht</i>	13
1.6 <i>De onderzoeksaanpak</i>	14
1.7 <i>Conditie</i>	14
1.8 <i>Het onderzoeksteam - Leibniz Foundation for Law</i>	15
1.9 <i>Opbouw van de rapportage</i>	15
<b>2. Dataprotectie</b>	<b>16</b>
2.1 <i>Inleiding</i>	16
2.1.1 <i>Ontsluiting van data</i>	16
2.1.2 <i>Bescherming van de privacy</i>	16
2.1.3 <i>Privacy en locatie</i>	17
2.1.4 <i>Factoren voor location based privacy</i>	18
2.1.5 <i>Omslag in het denken over location based privacy</i>	19
2.2 <i>Specifieke condities bij Spookfiles A-58</i>	19
2.2.1 <i>Transparantie en accountability</i>	19
2.2.3 <i>Klantperspectief</i>	20
2.3 <i>Wettelijke bepalingen</i>	21
2.3.1 <i>Inleiding</i>	21
2.3.2 <i>Wet Bescherming Persoonsgegevens</i>	21
2.3.3 <i>Wet op de Telecommunicatie</i>	25
2.4 <i>Toepassingen Spookfiles A-58</i>	26
2.4.1 <i>Verwerking door coöperatief rijden dienstverleners</i>	26
2.4.2 <i>Verantwoordelijke (rechts)persoon</i>	27
2.4.3 <i>Risicoklassen</i>	28
2.4.4 <i>Beveiliging</i>	28
2.4.5 <i>Dataprotectiebeleid</i>	29
2.4.6 <i>Privacy by Design en Privacy-Enhancing Technologies</i>	30
2.5 <i>Conclusies</i>	32
<b>3. Aansprakelijkheid</b>	<b>33</b>
3.1 <i>Inleiding</i>	33
3.2 <i>Verschillende aansprakelijkheden</i>	33
3.2.1 <i>Contractuele aansprakelijkheid</i>	34
3.2.2 <i>Productaansprakelijkheid</i>	35
3.2.3 <i>Aansprakelijkheid uit onrechtmatige daad</i>	35
3.2.4 <i>Bestuurlijke aansprakelijkheid</i>	35

3.3	<i>Aansprakelijkheid binnen coöperatief rijden</i>	36
3.3.1.	Aansprakelijkheid van producenten/dienstverleners	36
3.3.2	Aansprakelijkheid van de wegbeheerder	40
3.3.1	Aansprakelijkheid van de automobilist	41
3.4	<i>Aansprakelijkheidsverdeling Spookfiles A-58</i>	44
3.5	<i>Conclusies</i>	46
<b>4.</b>	<b>Data-eigenaarschap</b>	<b>47</b>
4.1	<i>Inleiding</i>	47
4.2	<i>Data-eigenaarschap</i>	49
4.3	<i>Data-eigendom</i>	52
4.4	<i>Conclusies</i>	56
	<b>Bijlage</b>	<b>58</b>
	<b>Lijst van geraadpleegde literatuur</b>	<b>62</b>

## Voorwoord

De omarming van ITS (*Intelligent Transport Systems*) neemt internationaal een grote vlucht. Er worden hele congressen aan gewijd en over de hele wereld lopen tal van projecten en programma's, waar zowel auto-industrie, ICT producenten en dienstverleners als infrastructuurbeheerders bij betrokken zijn. De snelle ontwikkeling van automated driving, met de Google auto als belangrijke blikvanger, maar ook van coöperatieve systemen zoals 'platooning' roept allerlei vragen op in diverse vakgebieden. Nederland wil binnen de EU, maar ook wereldwijd een voorlopers rol vervullen bij de ontwikkeling van ITS. Dat betekent dat de ontwikkelingen in Nederland zullen moeten passen in deze internationale context. De ontwikkelingen zijn internationaal en zullen in verband met de interoperabiliteit ook internationaal moeten worden uitgerold. De beoogde coöperatieve systemen kunnen niet stoppen aan de grens. Daarom uiteindelijk is een gestandaardiseerde EU brede uitrol noodzakelijk. 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 genoemde ontwikkelingen.

In het voorliggende rapport is een eerste verkenning opgenomen van de relevante wet- en regelgeving op een drietal rechtsgebieden. Deze is geconfronteerd met een eerste coöperatief rijden project dat vanaf voorjaar 2015 live zal gaan: Spookfiles A-58. Vanuit juridisch perspectief een enigszins premature verkenning gelet op het feit dat de techniek nog in wording is en dat er van feitelijke uitvoering nog geen sprake is. Veel randvoorwaarden moeten nog worden ingevuld. Maar juist daarom is een juridische verkenning in dit stadium zo belangrijk. Tijdige onderkenning van de juridische aspecten past bij de wens van de gezamenlijke partijen om een solide basis te leggen voor de inrichting van coöperatief rijden, en niet het risico te lopen essentiële juridische voorwaarden niet mee te nemen in het basisontwerp. Met andere woorden het elimineren van de juridische kant van ITS als mogelijke show stopper.

Het participierend onderzoek waarvan deze rapportage de neerslag is levert daaraan een bijdrage op twee manieren: a. door het doen van een soort juridische o-meting voor coöperatief rijden en b. door het leveren van een actieve bijdrage in het project Spookfiles om zo de juridische bewustwording bij alle betrokken partijen te vergroten. In de rapportage worden de juridische ontwikkelingen tegen de voorziene techniek aangelegd, waarmee een bijdrage wordt geleverd aan het signaleren van knelpunten die zich in een volgende fase kunnen manifesteren.

Op dit moment is nog niet te overzien hoe de dergelijke knelpunten kunnen worden opgelost, in recht, in de techniek of door middel van combinatie beide. Juist het samen op weg gaan om de optimale oplossingsrichtingen te vinden is de uitdaging. In die zin is deze rapportage dan ook zeker geen eindrapportage, maar meer een startpunt voor een boeiende samenwerking tussen techniek en recht voor de komende jaren.

## Afkortingenlijst

ITS	Intelligent Transport Systems
ICT	Informatie en Communicatie Technologie
WBP	Wet Bescherming Persoonsgegevens
WRR	Wetenschappelijke Raad voor het Regeringsbeleid
Tw	Wet op de TeleCommunicatie
CBP	College Bescherming Persoonsgegevens
ID	IDentificatie
ANPR	Automatic Number Plate Recognition
BW	Burgerlijk Wetboek
I&M	Infrastructuur en Milieu
ADA	Automated Driving Assistance
ADAS	Automated Driving Assistance Systems
ISA	Intelligent Speed Adaptation
WAM	Wet Aansprakelijkheid Motorrijtuigen
WA	Wettelijke Aansprakelijkheid
M2M	Machine naar Machine communicatie
I-EMRs	Interconnected Medical Records

## Samenvatting

Het programma Beter Benutten heeft ten doel de beschikbare capaciteit van de infrastructuur in Nederland beter te gebruiken. Een van de projecten binnen Beter Benutten waarbij coöperatieve technologie zal worden ingezet is project Spookfiles A-58 in Noord-Brabant. Binnen dit project zijn in een pre-competitieve setting marktpartijen bij elkaar gebracht om een coöperatief systeem voor het voorkomen van files te realiseren. Naast technische realisatie en markt ontwikkeling is binnen het project voorzien in een inventariserend onderzoek naar de juridische aspecten van coöperatief rijden. De voorliggende rapportage is hiervan het resultaat.

Coöperatief rijden is een nieuw fenomeen waarbij weliswaar niet direct sprake is van juridische blokkades in, bijvoorbeeld, de wegenverkeerswetgeving, maar dat toch een aantal juridische vragen oproept. Het doel van het onderzoek is om zicht te krijgen op de juridische aspecten die spelen bij de invoering van coöperatief rijden, en hoe daarmee binnen het project Spookfiles A-58 kan worden omgegaan. Bij het onderzoek is daarom gekozen voor een participerende benadering, waarbij naast literatuuronderzoek ook tijd is ingeruimd voor het deelnemen aan overleggen en het actief betrekken van de projectdeelnemers bij bepaalde juridische aspecten. Daardoor kon al in de ontwerpfase rekening worden gehouden met te verwachten juridische vereisten. Het onderzoek heeft zich gericht op een drietal onderwerpen:

1. Privacy bescherming, wat gebeurt er met alle informatie die *in-car* wordt samengebracht? Welke regels zijn op de coöperatief rijden dienst van toepassing? Hoe kan je de gegeven regels naleven?
2. Aansprakelijkheid, wie is aansprakelijk voor wat? Wat betekent dit voor de verschillende betrokken spelers? Wat zijn de veranderingen ten opzichte van de huidige situatie?
3. Data-eigenaarschap, van wie zijn de data eigenlijk?

Op alle drie terreinen is de juridische stand van zaken in kaart gebracht, voor zover relevant in het kader van het project Spookfiles A-58. Het rapport is in die zin niet zozeer een eindrapportage, maar meer een momentopname van de juridische stand van zaken bij coöperatief rijden.

Wat doet de Spookfiledienst A-58? De dienst geeft een advies aan de automobilist in het voertuig zodat hij bijvoorbeeld zijn snelheid aan kan passen aan de 'verwachte' verkeerssituatie. Door de opvolging van het advies wordt de snelheid in het wegvak aangepast aan de capaciteit van de weg. Om met de Spookfiledienst goede adviezen aan de automobilist in het voertuig aan te kunnen bieden moet om te beginnen verkeersdata worden ingewonnen uit het voertuig van de klant. Deze data worden via het wegkantsysteem beschikbaar gesteld aan de data collectie service provider. Deze verrijkt de data met andere beschikbare data die van belang zijn voor de verkeerssituatie op dat wegvak. Op basis van deze data wordt een advies samengesteld dat op een geschikte wijze in het voertuig van de klant kan worden aangeboden. Coöperatief rijden levert zo een keten op die er als volgt uitziet:

Voertuig (voertuig)  
Voertuig-> wegkant SP -> data-collectie SP -> data-leverantie SP -> advies SP -> wegkant SP -> voertuig  
Voertuig (voertuig)

Tijdens het onderzoek is de veronderstelling bevestigd dat het huidige wettelijke kader afdoende is voor ontwikkelingen als coöperatief rijden. Op welke manier coöperatief rijden ook zal worden ingericht, elk juridisch probleem dat hier eventueel uit voortvloeit zal met het huidige recht kunnen worden opgelost. De onrust ten aanzien van de mogelijke juridische implicaties van coöperatief rijden wordt

dan ook met name ingegeven door de onvoorspelbaarheid van de toepassing van het recht op dit nieuwe fenomeen en de daaruit voortvloeiende onzekerheid.

Bij het verkrijgen van inzicht in de juridische issues binnen het coöperatief rijden speelt de veelheid aan functionaliteiten en interfaces verdeeld over eveneens een veelheid aan marktpartijen een complicerende rol. De applicaties die de marktpartijen ten behoeve van de Spookfiledienst ontwikkelen zijn niet in het onderzoek betrokken zodat het onderzoek zich vooralsnog heeft beperkt tot de koppelvlakken. Wel heeft de participatie in het project gezorgd voor meer juridische bewustwording bij de marktpartijen.

#### *Dataproductie*

In het onderdeel dataproductie zijn twee benaderingen gekozen. Om te beginnen is gekeken naar de privacy gevolgen van de toenemende rol van ITS in het verkeer<sup>1</sup>. Daarna is het coöperatief rijden zoals het wordt vormgegeven in het project bekeken in het licht van de geldende wet- en regelgeving.

Door de grotere rol van locatie-informatie als dimensie van privacy wordt ook onze traceerbaarheid steeds groter. Via de mobiele telefoon, de OV-chipkaart en op locatie gebaseerde dienstverlening, zoals coöperatief rijden, laten we steeds meer digitale sporen achter. Toch heeft de gebruiker behoefte aan controle over zijn persoonsgegevens, bijvoorbeeld door middel van *selective disclosure*: de mogelijkheid om naar eigen behoefte informatie te delen of af te schermen. Aan de andere kant is er steeds meer technologie beschikbaar die ons volgt. Bovendien kan deze technologie zich verheugen in een aanzienlijke commerciële en bestuurlijke populariteit. We zijn ons er van bewust geworden dat de digitale vastlegging van locatiegegevens geenszins triviaal is. Daarom is het denken over *location based privacy* inmiddels in gang gezet. Het CBP heeft daarbij vastgesteld dat de locatiegebonden persoonsgegevens tot de categorie gevoelige gegevens behoren. Tezamen met de aanwezigheid van allerlei technologische mogelijkheden ontstaat behoefte aan een samenspel van factoren dat een *selective disclosure* faciliteert. Daarbij moet men denken aan factoren als technische betrouwbaarheid, de houdbaarheid en herbruikbaarheid van data, de mogelijkheid van secundair gebruik en vooral de transparantie van en de accountability voor de verwerking van deze persoonsgegevens. Binnen coöperatief rijden is de noodzaak van het gebruik van locatiegegevens evident, zonder deze gegevens geen coöperatieve diensten. Private partijen zien daarbij ook mogelijkheden voor andere toegevoegde waarde diensten en *targeted advertising*. Voor zover dit gebruik gereguleerd is en instemming heeft van de klant bestaat hiertegen geen bezwaar.

Om aan de ene kant de rechtmatigheid te kunnen bewaken en aan de andere kant aan alle wensen en mogelijkheden ten aanzien van het (her)gebruik van locatie gebonden persoonsgegevens tegemoet te kunnen komen is transparantie noodzakelijk. En om te kunnen vaststellen of een verantwoordelijke voor de verwerking van locatie gebonden persoonsgegevens daadwerkelijk in staat is om de wettelijke bepalingen ten aanzien van de verwerking van persoonsgegevens na te leven is daarbij ook accountability nodig. Voor zowel transparantie als de daarbij behorende accountability geldt dat deze vereist is op zowel beleidsniveau als op het niveau van de individuele relatie tussen dienstverlener en gebruiker.

De juridische regeling van de bescherming van persoonsgegevens is opgenomen in de Wet Bescherming Persoonsgegevens en de Telecommunicatiewet. In overeenstemming met de wettelijke bepalingen zal de aanbieder zich moeten inzetten om zijn verantwoordelijkheid ten opzichte van de

---

<sup>1</sup> Rapport WRR, Privacy en vormen van 'intelligente' mobiliteit, Griffioen 2011.

klant waar te kunnen maken. In dit verband is kwaliteitsborging in de keten een bijzonder aandachtspunt, temeer vanwege de gevoeligheid van locatiegebonden persoonsgegevens. Door deze gevoeligheid hebben deze gegevens een hogere risicoklasse, hetgeen betekent dat ook de beveiliging tegen ongeoorloofde verwerking of verlies op een navenant hoger niveau moet plaatsvinden. Voor het leggen van een goede verbinding tussen de klant en aanbieder is een beschrijving van de dienst vanuit het klantperspectief noodzakelijk. Door de opzet van het huidige project Spookfiles-A58, waarbij alle partijen zich specifiek richten op hun onderdeel in het geheel, en (nog) geen sprake is van systeemintegratie, ontbreekt vooralsnog een beschrijving vanuit dit klantperspectief.

Gelet op het grote afbreukrisico van coöperatief rijden is een goede bescherming van de persoonsgegevens door de hele keten cruciaal. De organisatorische diversiteit en het grote verschil in omvang en bedrijfscultuur tussen de ketenpartijen is daarbij een risico. Om dit risico zoveel mogelijk in te dammen ligt een technologische borging van de privacy in de keten het meest voor de hand. De inzet van dergelijke technologie - *Privacy by Design* door middel van *Privacy Enhancing Technology* - wordt een belangrijke factor voor een adequate bescherming van de persoonsgegevens binnen de hele coöperatief rijden infrastructuur. Te denken valt aan toegangsbeveiliging en aan geautomatiseerde processen die losgekoppeld zijn van menselijke tussenkomst. Daarbij kan ook een vergaande scheiding van de privacy gevoelige persoonsgegevens en de inhoudelijke gegevens als locatie, snelheid, richting etc. tijdens het verwerkingsproces behulpzaam zijn. De persoonsgegevens zouden door middel van een volgende generatie *Privacy Ensuring Technology* tegen ongewenste verwerkingen kunnen worden beschermd. Gelet op de gevoeligheid van de gegevens en de omvang en de impact van de risico's ligt het voor de hand om technisch verdergaande oplossingen voor de bescherming van de privacy te zoeken.

### *Conclusie*

Ten aanzien van de verwerking van persoonsgegevens in het kader van coöperatief rijden kan worden vastgesteld dat sprake is van een uitdagende combinatie. Dat kan worden geïllustreerd aan de hand van enkele vaststellingen vanuit juridisch perspectief. Een eerste vaststelling is dat het recht op bescherming van de persoonlijke levenssfeer een 'mensenrecht' is, en dat inbreuken daarop in beginsel niet zijn toegestaan. Een tweede is dat gegevensvastlegging zoals voorzien bij coöperatief rijden fundamenteel afwijkt van een klassieke vastlegging op papier waar het gaat om het risico van schending van de privacy. Verder is door het CBP vastgesteld dat locatiegegevens in combinatie met persoonsgegevens gevoelig zijn vanwege de traceerbaarheid van de auto, en daarmee van de bestuurder. Een laatste vaststelling is dat locatiegebonden persoonsgegevens uitsluitend kunnen worden verwerkt met de uitdrukkelijke toestemming van de betrokkene.

### *Aanbeveling*

Aanbevolen wordt om privacy vanaf de start structureel een vaste plaats te geven bij het ontwikkelen van coöperatieve systemen (*Privacy by Design*) en zo de kwaliteit van transport en verwerking van gegevens te optimaliseren. Verder is aan te bevelen om een volgende generatie *Privacy-Ensuring Technologies* te ontwikkelen, waardoor de verwerkingsprocessen minder kunnen worden bedreigd door organisatiefactoren en voldoende transparantie en accountability bij de verwerking van persoonsgegevens in de keten mogelijk is. Ook het aanstellen van een functionaris gegevensbescherming binnen de branche is aan te bevelen, net als een goed gemeenschappelijk dataprotectie-beleid ten einde het privacy bewustzijn bij de betrokken markt en overheidspartijen verder te verhogen, te onderhouden en te borgen. Partijen zullen zich moeten gaan realiseren dat adequate privacybescherming een cruciale randvoorwaarde is voor hun bedrijfsvoering: een *licence to operate*.



### *Aansprakelijkheid*

In het onderzoek is waar het gaat om aansprakelijkheid gekeken naar de mogelijke gevolgen van coöperatief rijden binnen het Spookfile A-58 project onder de huidige wetgeving. Daarbij kwamen vragen op als: is er sprake van invloed op de wettelijke aansprakelijkheid? En in hoeverre wijken *in-car* adviezen af van de adviezen die de wegbeheerder door middel van elektronische borden boven de weg geeft? Wat zijn de gevolgen voor toepassing van de Wet aansprakelijkheid motorrijtuigen (WAM) bij het gebruik van coöperatieve systemen die vooralsnog niet rechtstreeks ingrijpen in de besturing van het voertuig, zoals bijvoorbeeld bij ‘*platooning*’<sup>2</sup> wel het geval is? Coöperatief rijden zoals voorzien in het project Spookfiles A-58 betreft een dienst gericht op doorstroming van het verkeer. Daarmee zal niet snel de verwachting kunnen ontstaan dat men op de adviezen kan vertrouwen in het kader van de verkeersveiligheid.

Tijdens het onderzoek is onder meer gebruik gemaakt van de indeling in vormen van aansprakelijkheid zoals die is opgenomen in het rapport van de EU-Commissie in het kader van de *ITS-Action Plan*. Daarin stelt de Commissie vast dat er geen specifiek aansprakelijkheidsregime bestaat voor ITS applicaties, maar dat er wel enkele vormen van aansprakelijkheid kunnen optreden bij het gebruik van ITS applicaties zoals coöperatief rijden, te weten: contractuele aansprakelijkheid, productaansprakelijkheid, aansprakelijkheid uit onrechtmatige daad en aansprakelijkheid voortvloeiend uit het wegenverkeersrecht. Het rapport geeft enkele redenen waarom de uitkomst van sommige aansprakelijkheidszaken waarin ITS een rol speelt moeilijk te voorspellen is, zoals: regels die verschillend zijn voor verschillende applicaties, toekomstige diensten en applicaties waarvoor de wetgeving wellicht nog moet worden aangepast, het ontbreken van een harmonisatie van aansprakelijkheidsregels op Europees niveau en het feit dat *disclaimers* en gebruiksvoorwaarden voor een gebruiker moeilijk te begrijpen zijn.

In het kader van deze rapportage is gekozen voor een insteek waarbij achtereenvolgens de aansprakelijkheidspositie van de producent/dienstverlener, die van de wegbeheerder en van de automobilist onder de loep wordt genomen.

### *Producenten/dienstverleners*

In het kader van de producenten/dienst-verleners aansprakelijkheid gaat het vooral om de verwachtingen die door de aanbieder worden gewekt ten aanzien van de prestaties van de dienst. Daarvoor is van groot belang hoe de dienst wordt gepresenteerd. Daarnaast spelen het te verwachten gebruik en de afweging tussen de voor- en nadelen van het systeem een rol. Tenslotte zal de dienst aan de geldende veiligheidseisen moeten voldoen.

Aangezien de Spookfiles A-58 dienst is gericht op het bevorderen van de doorstroming van het verkeer en ook op die manier zal worden gepresenteerd, kan worden aangenomen dat er binnen de Spookfile A-58 dienst geen verschuiving van aansprakelijkheid zal plaatsvinden. Daardoor zullen de verwachtingen van de gebruikers goed op het gebruik van de dienst kunnen worden afgestemd.

---

<sup>2</sup> Platooning is het rijden in een konvooi van voertuigen waarbij het voorste voertuig leidend is. Elk voertuig meet de afstand, de snelheid en de richting en past die aan aan het voorliggende voertuig. Alle voertuigen zijn virtueel verbonden, maar kunnen op elk moment het konvooi verlaten. Echter wanneer een voertuig in het konvooi deelneemt, dan kan de chauffeur zijn aandacht op andere zaken richten terwijl het konvooi zijn weg vervolgd. (Definitie ERTICO-Sartre project-2012)

Een aandachtspunt is dat achter de dienstaanbieder een keten van andere dienstverleners inclusief de wegbeheerder bijdraagt aan het tot stand komen ervan. In deze fase van coöperatief rijden, het brengen van een doorstromingsadvies in het voertuig is dat nog geen probleem. Maar als het coöperatieve systeem rechtstreeks gaat ingrijpen in het voertuig, zoals bij het eerder genoemde *platooning*, dan kan bij een falend systeem de vraag ontstaan welke component heeft gefaald. Waar nu nog de keuze is tussen de bestuurder en de leverancier van het voertuig kan bij coöperatief rijden sprake zijn van een hele keten van potentiële aansprakelijken. Het zal duidelijk zijn dat de tolerantie voor fouten bij een dergelijk systeem minimaal is.

Daarmee wordt de aansprakelijkheidsvraag om te beginnen een bewijsprobleem. Hoe kan worden vastgesteld wat in de keten is misgegaan en wie daarvoor verantwoordelijk is? Deze vaststelling leidt weliswaar niet rechtstreeks tot aansprakelijkheid, er is tegenbewijs door de leverancier van de component mogelijk, maar is wel noodzakelijk om de juiste partij aan te kunnen spreken. Een van de manieren om aan deze bewijsproblematiek het hoofd te bieden is bijvoorbeeld door gebruik te maken van een drive-data-recorder die de gegevens van de laatste minuten voorafgaand aan een incident vasthoudt.

#### *Wegbeheerder*

De aansprakelijkheid van de wegbeheerder is in de wet vastgelegd. De vraag die zich hierbij voordoet is in welke mate de wegkantapparatuur die voor coöperatief rijden nodig is deel uitmaakt van de weguitrusting. Is dat het geval dan zal de wegbeheerder ook deel uitmaken van de dienstverleningsketen en in geval van het falen van het systeem mogelijk aansprakelijk kunnen zijn. Wettelijk heeft de wegbeheerder namelijk een zorgplicht en mag van hem verwacht worden dat de infrastructuur van de weg, inclusief coöperatief rijden dienst, naar behoren functioneert. Dit geldt zeker op het hoofdwegennet waar zich zelfs in de fase van Spookfiles A58 al discrepanties zouden kunnen voordoen tussen het in-car advies en de wegkantsignalering. De wegbeheerder kan niet aansprakelijk worden gesteld voor schade van buitenaf, zoals blikseminslag of hacking. Wel rijst in zo'n geval de vraag of de wegbeheerder genoeg maatregelen heeft genomen om de schade te voorkomen.

#### *Bestuurder*

De aansprakelijkheid van de bestuurder bij coöperatief rijden ontwikkelt zich op twee manieren. Enerzijds kan deze verminderen als er een fout advies wordt gegeven. Dit zal bij de Spookfile A58 dienst beperkt zijn, omdat het gaat om een doorstroomadvies. Als echter in een volgende fase van coöperatief rijden het voertuig rechtstreeks vanuit het systeem wordt aangestuurd, dan kan de aansprakelijkheid van de bestuurder sterk afnemen of zelfs wegvallen. Anderzijds kan ook het 'gewaarschuwd mens telt voor twee' principe opgeld doen. Als de bestuurder een advies heeft dat hem beter in staat stelt de goede afweging in het verkeer te maken dan moet hij dat ook doen. Het negeren van het advies, of het uitzetten van de dienst kan in dat geval zelfs leiden tot een verhoogde aansprakelijkheid van de bestuurder.

Uitgangspunt is en blijft dat de voertuig-verantwoordelijke aansprakelijk is voor schade die met (door) het voertuig is aangericht. Dat zal pas veranderen als het coöperatieve systeem rechtstreeks ingrijpt in het voertuig. Als het gaat om aanrijdingen tussen een auto en een ander soort weggebruiker zal de verplichte wettelijke aansprakelijkheidsverzekering de eventuele schade dekken. Bij aanrijdingen met een andere auto zal de aansprakelijkheid nader moeten worden vastgesteld op grond van de regels met betrekking tot onrechtmatige daad.

Dat bij coöperatief rijden de verantwoordelijkheid van de bestuurder serieus zal kunnen afnemen als sprake is van het rechtstreeks ingrijpen door het systeem maakt voor het slachtoffer overigens niet uit. De ‘verantwoordelijkheid van het voertuig’ blijft in stand, of nu de bestuurder, de autofabrikant of een van de coöperatief rijden dienstverleners uiteindelijk aansprakelijk blijkt te zijn. Deze partijen zullen onderling moeten uitmaken hoe het vergoeden van de schade wordt verdeeld. Daarbij speelt de verzekeraar een centrale rol. Deze is gehouden de schade te voldoen en vervolgens te verhalen op eventuele andere aansprakelijken.

Het is denkbaar dat de voorwaarden van de verplichte polis onder invloed van de ontwikkelingen op het gebied coöperatief rijden zullen worden aangepast, bijvoorbeeld door specifieke premies voor voertuigen die deelnemen aan coöperatief rijden, eisen ten aanzien van de voorwaarden van de dienstverlener en certificering van de verzekerde auto en de gebruikte technische apparatuur ten behoeve van coöperatief rijden.

#### *Conclusie*

Vooralsnog zal de aansprakelijkheid van een coöperatief rijdende auto in de fase van Spookfiles A-58 geen aansprakelijkheidsverschuiving met zich brengen omdat het systeem adviserend en ondersteunend is en gericht op doorstroming van het verkeer. Wel zal de beoordeling van de bestuurder in geval van schade kunnen veranderen vanwege de ondersteuning door het systeem. Ook zal de relatie tussen de verzekerde en de verzekeraar kunnen veranderen, bijvoorbeeld in de voorwaarden of bij de premiestelling.

Een belangrijk aandachtspunt is de balans tussen acceptatie van onvolkomenheden bij coöperatief rijden en de bescherming van potentiële slachtoffers. Problematisch voor het slachtoffer in dit verband is de kanalisatie van de claim van het slachtoffer. Hierbij kan het voorkomen dat een slachtoffer meerdere potentiële aansprakelijken moet aanspreken. Voorkomen moet worden dat de positie van het slachtoffer door coöperatief rijden verder verslechtert. Veel zal in dit verband afhangen van de ontwikkeling in de rechtspraktijk, hoe legt de rechter de bewijslastverdeling, en hoe gaat hij om met de interpretatie van de zorgvuldigheidsnorm.

In de rapportage staat een aantal oplossingsrichtingen voor de bewijsproblematiek bij coöperatief rijden, variërend van het onderbrengen van de aansprakelijkheid tussen motorvoertuigen onder de WAM verzekering van de bezitter, via het installeren van een *drive-data-recorder* in de auto bij toepassing van coöperatieve systemen, tot het opzetten van een stelsel van verkeersverzekeringen, waarmee verkeersongevallen uit de sfeer van het aansprakelijkheidsrecht raken.

#### *Aanbeveling*

Aanbevolen wordt om de discussie te starten over de bewijsproblematiek met alle belanghebbenden, zowel voor het creëren van bewustwording van de problematiek als voor het creëren van draagvlak voor een mogelijke oplossingsrichting. Daarbij zullen op korte termijn de verzekeraars en de vlooteigenaren bij de praktijkproeven moeten worden betrokken zodat eventuele juridische discussies tijdig worden gesignaleerd en gevoerd met alle belanghebbenden.

#### *Data-eigenaarschap*

Het derde onderwerp in het onderzoek naar de juridische inbedding van coöperatief rijden is data-eigenaarschap. Hoewel eigenaarschap een juridische begrip suggereert kan worden vastgesteld dat het

begrip vooral komt uit de wereld van het informatiemanagement. Data-eigenaarschap bestaat vanuit deze achtergrond bezien uit twee componenten: bezit en verantwoordelijkheid. Met name de laatste, de verantwoordelijkheid voor de data, geeft vorm aan het eigenaarschap omdat het een zekere zorgplicht impliceert. Bezit van en verantwoordelijkheid voor de data impliceren daarentegen geen juridische eigendom. De mogelijkheid van het vatbaar zijn voor juridische eigendom is voorbehouden aan stoffelijke objecten. Data behoren niet tot deze categorie.

Bij het bekijken van de juridische rechten op data binnen coöperatief rijden gaat het om verschillende soorten gegevens. In de eerste plaats om de als persoonsgegevens aan te merken gegevens die betrekking hebben op de locatie en de eventuele traceerbaarheid van de klant. Daarnaast gaat het over persoonsgegevens die worden gebruikt in de administratie, bijvoorbeeld de naam, adres, woonplaatsgegevens die worden gebruikt voor de facturering en verdere contacten met de klant. Ten slotte kunnen geanonimiseerde gegevens worden gebruikt voor real time of historische verkeersinformatie. Op deze verschillende soorten gegevens zullen ook verschillende rechtenregimes kunnen gelden. Veel van deze rechtsrelaties zullen vorm krijgen in de contracten tussen de verschillende partijen.

Op voorhand is de vraag wie de eigenaar is van data die in het kader van coöperatief rijden worden gegenereerd en verwerkt dan ook niet eenduidig te beantwoorden. Er zijn namelijk veel verschillende partijen betrokken bij de gegevensverwerking, die allemaal hun eigen relatie tot de data hebben. Wel kan in het kader van coöperatief rijden worden vastgesteld dat slechts een aantal van de mogelijke partijen rechten op de data kunnen doen gelden. Dit zijn in eerste instantie de serviceprovider die met alle andere partijen overeenkomsten sluit over de dienstverlening en de omgang met de daarvoor noodzakelijke data. Daarbij is de vrijheid om de rechten over de partijen te verdelen in beginsel groot. Wel is één partij in het bijzonder beschermd door wet- en regelgeving; namelijk de klant/gebruiker van de coöperatief rijden dienst. Deze heeft de wettelijke bescherming van zijn persoonsgegevens, die in acht moet worden genomen, en daarnaast de bescherming als consument van de geleverde dienst. Bij beide vormen van bescherming kunnen de voor de coöperatief rijden dienst verzamelde en verwerkte data een rol spelen.

### *Conclusie*

Juridische eigendom bestaat uitsluitend ten aanzien van stoffelijke objecten, niet ten aanzien van data. Data-eigenaarschap kan juridisch beter vertaald worden naar rechten en verplichtingen. De verdeling van deze rechten en plichten vindt, met in achtneming van de wettelijke voorschriften, plaats op basis van de overeenkomsten tussen de partijen. De waarde van de data, die bij deze verdeling een belangrijke rol speelt, komt tot stand door de verwerking van de data en door de context waarbinnen de gegevens worden gebruikt.

### *Aanbeveling*

Aanbevolen wordt om een discussie aan te gaan over de verdeling van de rechten op de data binnen coöperatief rijden waarbij het uitgangspunt is dat de rechten van de klant op 'zijn' data wordt erkent. Daarvoor is een transparante rechtenverdeling tussen partijen van belang. Deze zou in de beschrijving van de coöperatief rijden dienst voor de klant een plaats moeten krijgen. Het ontbreken van zo'n beschrijving leidt tot onduidelijkheid over de positie van partijen en kan een drempel opleveren voor de klant om in te stappen in coöperatief rijden.

## 1. Inleiding

### 1.1 Aanleiding voor het onderzoek

Het programma Beter Benutten heeft ten doel de beschikbare capaciteit van de infrastructuur in Nederland beter te gebruiken. Daartoe ondersteunt het programma ontwikkelingen die aan de verbetering een bijdrage kunnen leveren. Het gaat daarbij zowel om het ontwikkelen van de infrastructuur zelf, als om het verbeteren van de capaciteit van de infrastructuur met behulp van Intelligent Transport Systems (ITS), systemen die door middel van slimme technologie het transport ondersteunen. Een van de projecten binnen Beter Benutten waarbij ITS wordt ingezet is het project Spookfiles A-58 in Noord-Brabant. Binnen dat project wordt gewerkt aan de ontwikkeling van coöperatief rijden. Hierbij wordt op lokaal niveau tussen voertuigen onderling en met de wegwijk informatie gedeeld, waardoor informatie, verkeersmanagement en verkeersveiligheidsdiensten in-car samenkomen.

Binnen het project zijn in een pre-competitieve setting bedrijven uit de markt bij elkaar gebracht om met een startsubsidie een coöperatief systeem te realiseren om te voorkomen. Bij deze geheel nieuwe samenwerking is naast aandacht voor de bestuurlijke, de technische, de organisatorische en de commerciële aspecten ook behoefte aan inzicht in de juridische aspecten van coöperatief rijden. Het onderzoek verschaft inzicht in de juridische stand van zaken op enkele nader met de opdrachtgever vastgestelde juridische deelgebieden in relatie tot coöperatief rijden.

### 1.2 Coöperatief rijden, Spookfiles A-58

De Spookfiledienst A-58 geeft advies aan de automobilist in het voertuig. Op basis van dit advies kan de automobilist zijn snelheid en positionering ten opzichte van andere voertuigen en op het wegvak aanpassen met het doel het ontstaan van een spookfile te voorkomen of om een reeds ontstane spookfile te dempen. Om goede adviezen aan de automobilist in het voertuig aan te bieden moet om te beginnen verkeersdata worden ingewonnen uit dat voertuig. Deze data worden via het wegwijksysteem beschikbaar gesteld aan de data collectie service provider. Deze verrijkt de data met andere beschikbare verkeersdata die verband houden met hetzelfde wegvak. Op basis van deze data wordt een advies samengesteld dat op een daarvoor geschikte wijze in het voertuig van de klant kan worden aangeboden. Er moet dus ook een telecommunicatiedienst worden geleverd waarvoor een platform in het voertuig nodig is. Coöperatief rijden levert zo een keten op die er als volgt uitziet:

Voertuig	(voertuig)
Voertuig-> wegwijk SP -> data-collectie SP -> data-leverantie SP -> advies SP -> wegwijk SP -> voertuig	
Voertuig	(voertuig)

### 1.3 Onderzoeksvragen coöperatief rijden

Coöperatief rijden in de vorm van de Spookfiledienst A-58 is een nieuw fenomeen dat weliswaar niet wordt geconfronteerd met directe juridische blokkades, bijvoorbeeld in de wegenverkeerswetgeving, maar dat toch een aantal juridische vragen oproept. Het gaat bijvoorbeeld om vragen rond privacy: wat gebeurt er met alle informatie in het voertuig wordt verzameld? En over de onderliggende data: van wie zijn die data eigenlijk? Naast de positie van de bestuurder/passagier, zijn hierbij ook de posities van de autofabrikanten, de IT-service providers en de wegbeheerder betrokken. Welke verantwoordelijkheid hebben deze verschillende spelers en in hoeverre is die juridisch geregeld? Het gaat bijvoorbeeld om de positie ten opzichte van de private regelgeving: wat als er iets gebeurt waardoor schade ontstaat? Wie is aansprakelijk? Wat betekent dit voor de verschillende betrokken spelers? En op het snijvlak van publiek

en privaat: op welke manier zijn de verantwoordelijkheden van de betrokken spelers, wegbeheerder, bestuurder/passagier, autofabrikant en dienstverlener van de desbetreffende service geregeld. Wat zijn de veranderingen ten opzichte van de huidige situatie en hoe kan het ontstaan van een transparante en juridisch duidelijke situatie worden bereikt die een verantwoorde toepassing van de nieuwe technologie mogelijk maakt?

Aan de andere kant is binnen het onderzoek ruimte gecreëerd voor een dialoog met de technische- en marktontwikkelaars waardoor aan de hand van mogelijke juridische implicaties eventueel technische keuzes kunnen worden bijgesteld. Zo kan worden voorkomen dat het ontbreken van een juridische basis de invoering van ITS toepassingen blokkeert. Als (verkeers-) technisch geteste, en politieke gewenste oplossingen uiteindelijk, door het ontbreken van een juridische basis, niet kunnen worden ingevoerd, zullen immers ook de beoogde verkeerstechnische en maatschappelijke effecten niet optreden.

#### 1.4 Doel van het onderzoek

Het doel van het onderzoek is in eerste instantie om zicht te krijgen op de juridische implicaties met betrekking tot de gesignaleerde juridische vragen bij de introductie van coöperatief rijden. Daarbij is voor de opdrachtgever met name van belang of zich juridische obstakels voordoen en, zo ja, of die kunnen worden weggenomen. Maar ook als zich geen concrete obstakels voordoen dan is het van belang om inzicht te krijgen in de juridische posities van de spelers binnen coöperatief rijden en het Spookfileproject A-58. Dit om te voorkomen dat wat er in eerste instantie uit ziet als een onschuldig hobbeltje, uiteindelijk op de drempel van de uitvoering een showstopper zal blijken te zijn. Daarmee is ook een belangrijk nevendoeel aangegeven dat een flinke impact heeft gehad op het verloop van het onderzoek: het bevorderen van de juridische bewustwording bij de betrokken partijen. Een laatste doel van het inventariserend onderzoek was het creëren van een basis voor verder onderzoek en juridische begeleiding van coöperatief rijden. Overigens wordt in de eerste fase van het project gewerkt met ‘connected’ voertuigen. Aangezien dit een tijdelijke situatie is naar de juridische inbedding ervan geen nader onderzoek gedaan.

#### 1.5 De onderzoeksopdracht

Het onderzoek is uitgevoerd in opdracht van het programma Beter Benutten van het Ministerie van Infrastructuur en Milieu. Uitgangspunt van het inventariserend onderzoek is zoals gezegd het project Spookfiles A-58 en de daarbinnen ontwikkelende organisatorische en technische omgeving voor coöperatieve ITS. Binnen deze setting zijn drie onderwerpen benoemd die hierna kort worden toegelicht:

- *Privacy.* Het voertuig legt zelf allerlei data vast, en stelt deze data (plaats en tijdbepaling) vervolgens beschikbaar aan andere spelers die op hun beurt deze data weer gaan verwerken. Hier zijn vragen als: in hoeverre is de privacy van de automobilist gewaarborgd? En heeft de bestuurder van de auto zicht op wat er met ‘zijn of haar’ data gebeurt?
- *Aansprakelijkheid.* Hoe zijn de verhoudingen tussen de verschillende betrokken partijen, zoals bestuurders, voertuigeigenaren, wegbeheerders, autofabrikanten, ICT service providers etc. te duiden als het gaat om de verdeling van de aansprakelijkheid. Met andere woorden wie is bij coöperatieve ITS aansprakelijk voor wat, en op grond waarvan?
- *Data eigenaarschap.* Van wie zijn de betrokken data eigenlijk en welke juridische noties spelen een rol ter zake van de data in en om een voertuig bij coöperatieve ITS.

## 1.6 De onderzoeksaanpak

Gelet op de meervoudige doelstelling en de betrekkelijk korte doorlooptijd is vanaf de start van het onderzoek binnen het project Spookfiles A-58 een rechtstreekse verbinding gelegd tussen het project en de onderzoekers. Vervolgens zijn de benoemde aandachtsgebieden privacy, aansprakelijkheid en data-eigenaarschap vanuit op de onderwerpen betrekking hebbende literatuur onderzocht. In het kader van het participerend karakter van het onderzoek zijn de tussenresultaten regelmatig binnen de werkgroep “Authenticatie, Privacy en Juridische Aspecten” besproken. Daarbij is komen vast te staan dat de resultaten uit zowel het technisch/ organisatorische project als uit het onderzoek nog geen stevige basis hebben. Daarvoor is het veld nog teveel in een vroeg stadium van ontwikkeling en heeft het onderzoek nog teveel het karakter van werk in uitvoering.

Om die reden is in overleg met de opdrachtgever ervoor gekozen om nog geen valideringssessies te doen, maar de tijd zoveel mogelijk aan het onderzoek zelf en het contact binnen het project te besteden. Daarbij is de specifieke focus gehouden op concrete vragen en mogelijk obstakels ten aanzien van coöperatieve ITS, en op de bewustwording bij de projectpartijen. Op deze manier kon een enigszins afgerond resultaat worden bereikt ondanks de omvang van het veld en de relatief korte doorlooptijd van het onderzoek.

## 1.7 Conditities

Vanwege de beperkte doorlooptijd en de doelstelling van het onderzoek, inzicht verkrijgen in de juridische implicaties en bewustwording van deze implicaties bij de betrokken partijen, zijn enkele condities vastgesteld bij het begin van het onderzoek.

Om te beginnen wordt de veronderstelling dat het huidige juridische kader afdoende is voor ontwikkelingen als coöperatief rijden bevestigd. Op welke manier coöperatief rijden ook zal worden ingericht, elk juridisch probleem dat hier eventueel uit voortvloeit zal met het huidige recht kunnen worden opgelost. De onrust ten aanzien van de mogelijke juridische implicaties van coöperatief rijden wordt dan ook met name ingegeven door de onvoorspelbaarheid van de toepassing van het recht op dit nieuwe fenomeen. Deze onzekerheid manifesteert zich vooral in de sfeer van marketing en bij de overheid bij het bestuur.

Bij het verkrijgen van inzicht in de juridische issues binnen het coöperatief rijden speelt de veelheid aan functionaliteiten en interfaces verdeeld over eveneens een veelheid aan marktpartijen een complicerende rol. Om een goed beeld van de issues te krijgen is inzicht in zowel de functionaliteit van de applicaties als van de interfaces noodzakelijk. Daarbij is gebleken dat de interfaces wel gezamenlijk en transparant gedefinieerd kunnen worden, maar dat de applicaties tot het exclusieve terrein van de individuele marktpartijen behoren. Om die reden moest het onderzoek zich beperken tot het gemeenschappelijk deel van het coöperatief rijden systeem, het koppelvlakniveau. De applicaties van de marktpartijen zijn niet in het onderzoek betrokken. Wel heeft het project gezorgd voor meer juridische bewustwording bij de marktpartijen. Door de scope en de omvang van het onderzoek is de externe toetsing van de resultaten vooralsnog beperkt gebleven.

### 1.8 Het onderzoeksteam - Leibniz Foundation for Law

De Leibniz Foundation for Law van de Universiteit van Amsterdam is een onderdeel van de faculteit Rechtsgeleerdheid dat zich bezighoudt met juridisch kennismanagement en met de toepassing van het recht in een geautomatiseerde omgeving, het snijvlak van ICT en recht.

Het onderzoek staat onder leiding van Prof. Dr. T.M van Engers. Naast de dagelijkse supervisie is hij verantwoordelijk voor de eindrapportage van het onderzoek. Het onderzoek is gecoördineerd en voor het grootste deel verricht door Mr. W.F. van Haaften, senior onderzoeker. Hij heeft de contacten met de opdrachtgever onderhouden en heeft deelgenomen aan de geplande overleggen. Binnen het onderzoeksteam heeft hij ook de contacten met andere vakgroepen binnen de faculteit en met de experts daarbuiten onderhouden.

### 1.9 Opbouw van de rapportage

Bij het opstellen van de rapportages per onderwerp is ernaar gestreefd zoveel mogelijk concrete handvatten te bieden ten aanzien van de juridische inbedding van coöperatieve ITS als basis voor zowel concreet gebruik binnen het project, als voor verder onderzoek en ontwikkeling van een juridisch kader. De resultaten van het onderzoek hebben echter voor geen van de onderzoeksgebieden een afgerond karakter. Zij bevatten een tussenstand op een moment dat er van feitelijk coöperatief rijden nog geen sprake is. Niettemin geeft de rapportage op een aantal punten aan welke juridische issues moeten worden geadresseerd. Met name ten aanzien van de privacy en de aansprakelijkheid zal nog verder invulling moeten worden gegeven aan de juridische inbedding van de zich ontwikkelende technologie en markt. Data-eigenaarschap zal vooral zijn aangewezen op de ontwikkeling van heldere afspraken over de verdeling van datarechten over de verschillende partijen.



## **2. Dataproductie**

### **2.1 Inleiding**

#### **2.1.1 Ontsluiting van data**

In de afgelopen decennia is het verzamelen en verwerken van gegevens onder invloed van de elektronische mogelijkheden ingrijpend veranderd. Het zoeken van gegevens in een kaartenbak en het verzamelen van geografisch gespreid opgeslagen gegevens waren vroeger een tijdrovende bezigheid. Snel verbanden leggen tussen papieren gegevensverzamelingen was, en is nog steeds, niet aan de orde.

Hoe anders is dat in ons elektronische tijdperk, waarin het verzamelen van vrijwel ongelimiteerd hoeveelheden gegevens gepaard gaat met de mogelijkheden tot het aan elkaar koppelen van allerlei gegevensbestanden die tenminste een deel van de dataset gemeen hebben. Niet zelden bestaat deze dataset uit de identificerende gegevens van natuurlijke personen. Gegevens die bij allerlei gelegenheden worden afgegeven aan de overheid, op grond van wettelijke bepalingen of in het kader van de dienstverlening en, in nog veel grotere mate, aan private partijen, bijvoorbeeld bij aanschaf van goederen via internet of om mee te kunnen dingen naar prijzen in het kader van goed gestroomlijnde marketingcampagnes. Persoonsgegevens zijn overal en de bescherming ervan lijkt veel burgers niet een grote zorg te zijn. Slechts een enkele keer leidt een bericht over het gebruik van persoonsgegevens tot gefronste wenkbrauwen. Meestal gaat het dan om gegevens die niet met medeweten en/of toestemming van de betrokken persoon zijn verzameld. Daarbij gaat het vaak ook om een gegevens-set die naast de identificerende gegevens is voorzien van een extra gegeven dat in combinatie met het identificerend gegeven als bedreigend wordt ervaren. Het koppelen van locatiegegevens aan identificerende gegevens is hiervan een goed voorbeeld, zoals uit de volgende paragraaf zal blijken.

#### **2.1.2 Bescherming van de privacy**

Hoe gevoelig de privacy ligt in het verkeersdomein blijkt uit een aantal voorbeelden van informatieverzameling die recent de pers of zelfs de rechtszaal hebben gehaald. Zo was er een rechtszaak rond het gebruik van de permanente kentekenherkenning op de snelweg bij Zwolle die iedereen op die weg registreerde. In de zo ontstane database werd gezocht naar voertuigen die mogelijk betrokken waren bij criminele activiteiten. Het argument van het Openbaar Ministerie om deze handelwijze toe te staan was dat men ook een agent met een opschrijfboekje had kunnen neer zetten en dat de kentekenherkenning in feite slechts een technisch hulpmiddel was. Afgezien van het feit dat ook de agent met het opschrijfboekje waarschijnlijk een persoonsregistratie aanlegt en dus onder de WBP valt, zijn de schaalgrootte van de registratie, de automatische koppeling aan andere registraties zoals het kentekenregister, en de gemakkelijke geautomatiseerde verspreiding van de gegevens voor de rechter reden geweest om deze vorm van dataverzameling te verwerpen.

Een ander voorbeeld van de gevoeligheid van informatie over de locatie betrof de levering van geaggregeerde TomTom locatie-informatie aan de politie. Deze konden met de verkregen informatie meer gericht snelheidscontroles instellen op bepaalde locaties waar te hard werd gereden. Hoewel de informatie geaggregeerd was, en dus niet tot de persoon te herleiden, gaf de commotie wel aan hoe gevoelig het verwerken van persoonsgegevens is. Het CBP tikte TomTom op de vingers omdat de verstrekking aan de politie niet vooraf als mogelijk doel van de verwerking van persoonsgegevens was aangegeven. Overigens wel tot de persoon te herleiden waren de gegevens van autogebruikers die door de autoleasemaatschappijen zouden worden verstrekt aan Rijkswaterstaat ten einde deze gebruikers te kunnen enquêteren. De gegevens van de kentekens en bijbehorende eigenaren, de leasemaatschappijen, waren door RWS verkregen van de RDW onder voorwaarde dat deze niet mochten

worden doorgegeven. Door aan de leasebedrijven de namen van de gebruikers te vragen werd in strijd met de wetgeving een geheel nieuwe koppeling tussen kenteken en gebruiker tot stand gebracht. Met de beste bedoelingen ongetwijfeld, maar het is opmerkelijk dat een overheidsorganisatie als RWS geen gevoel bleek te hebben voor het ontbreken van de rechtmatigheid van een dergelijke actie. De daaraan verbonden risico's betreffen niet alleen imagoschade, maar men loopt de kans te worden teruggefloten, waardoor gedane investeringen teniet gedaan worden en mogelijk zelfs schadevergoeding moet worden uitgekeerd.

### 2.1.3 Privacy en locatie

In het WRR rapport 'Privacy en vormen van 'intelligente' mobiliteit'<sup>3</sup> wordt nadrukkelijk gewezen op de rol van locatie-informatie als dimensie van privacy, waardoor onze traceerbaarheid steeds groter wordt. De mobiele telefoon, de OV-chipkaart, maar ook op locatie gebaseerde dienstverlening, zoals coöperatief rijden, leiden tot een veelheid aan digitale sporen. Hoe houden we als gebruiker controle over onze persoonsgegevens? Een van de manieren om aan deze behoefte aan controle tegemoet te komen is in termen van *selective disclosure*. 'Zelfs voor de meest intieme relaties geldt dat menselijke interactie evenzeer wordt gekenmerkt door het 'reserveren' als door het 'delen' van informatie. Dit maakt controle over de manier waarop en de mate waarin men zich blootgeeft een belangrijk bezit', aldus het rapport.

Welke rol speelt locatie binnen het concept privacy? Ofschoon de rechter in de Verenigde Staten in 1983 het onderscheid tussen een surveillerende politieagent en een op een voertuig aangebracht 'tracking device' nog bagatelliseerde door het bestaan van privacy op de openbare weg te ontkennen<sup>4</sup>, wordt daar in Europa anno 2014 heel anders naar gekeken. De beschikbare technologie en applicaties, gecombineerd met hun commerciële en bestuurlijke populariteit hebben inmiddels het denken over *location based privacy* in gang gezet. We zijn ons er van bewust geworden dat de digitale vastlegging van locatiegegevens geenszins triviaal is. In de Deventer moordzaak bleek het bewijs voor een belangrijk deel op de, overigens discutabele, plaatsbepaling van de verdachte door middel van zijn mobiele telefoon te zijn gebaseerd. Kennelijk is de digitaal ontsloten ruimte radicaal veranderd nu beheerders van locatiedata op basis daarvan leefpatronen kunnen reconstrueren, zoals bij het gebruik van bijvoorbeeld *smartphones* het geval is, of bij de toepassing van ANPR<sup>5</sup>. Niet voor niets is het wetsvoorstel voor het invoeren van een Kilometerprijs mede gesneuveld op de claim van een deel van de oppositie dat met de on-board-unit de privacy van de burger in gevaar zou komen. De overheid zou immers door middel van het 'spionagekastje' de gangen van elke burger kunnen nagaan. De zorg over de haalbaarheid van *selective disclosure* wordt ook weerspiegeld bij de mobiliteitstheoreticus Urry<sup>6</sup>: 'gaan we voertuigen vernetwerken, dan gaan we ook mensen traceerbaar maken'.

Het is goed deze conclusie voor ogen te houden bij het ontwerpen van de Spookfiledienst A58, aangezien binnen coöperatief rijden veel informatie uit de auto nodig zal zijn om het collectieve doel, beter op elkaar afgestemd weggedrag, te realiseren. Om een real time snelheidsadvies mogelijk te maken zullen de betrokken auto's immers vrijwel permanent op zenden staan. Inventarisatie van de mogelijkheden van de nieuwe technologieën roept de vraag op of de huidige privacy wetgeving wel toereikend is, of juist te ruim of te krap?

---

<sup>3</sup> Wetenschappelijke Raad voor het Regeringsbeleid, 2011, Henk Griffioen.

<sup>4</sup> Knotts Supreme Court 2 maart 1983,

<sup>5</sup> Automatic number plate recognition

<sup>6</sup> Urry 2007, pp 289, geciteerd door H. Griffioen 2011

#### 2.1.4 Factoren voor location based privacy

Om bij alle technologische mogelijkheden greep te kunnen houden ‘op de manier waarop en de mate waarin men zich blootgeeft’ is een samenspel van factoren nodig dat deze *selective disclosure* faciliteert. Het gaat daarbij om factoren als technische betrouwbaarheid, de houdbaarheid en herbruikbaarheid van data, de mogelijkheid van secundair gebruik en vooral de transparantie van en de accountability voor de verwerking van deze persoonsgegevens.

##### *Technologische betrouwbaarheid*

Om te beginnen is, met het oog op de gevoeligheid van de informatie, de technologische betrouwbaarheid van de systemen waarmee data worden gegenereerd en opgeslagen van groot belang<sup>7</sup>. Met gebrekkige techniek is het bijvoorbeeld in het geval van coöperatief rijden onmogelijk om het subtiele evenwicht tussen privacy enerzijds en collectief belang anderzijds te bewaren. Om die reden zal aan de kwaliteit van de techniek hoge eisen moeten worden gesteld.

##### *Houdbaarheid en herbruikbaarheid data*

Daarnaast wordt de gewenste *practical obscurity*, het feitelijk ‘onzichtbaar’ zijn in de publieke ruimte, als uitgangspunt vooral bedreigd door de houdbaarheid van de verzamelde data en de daaruit voortvloeiende herbruikbaarheid. Door data te bewaren en in een later stadium te hergebruiken wordt de ‘zichtbaarheid’ van de automobilist opgerekt van een fysieke moment opname langs de weg tot een virtuele opname met een langlopende consequenties. Zelfs als de bewaartermijnen kort worden gehouden betekent dit dat personen op de openbare weg nu veel meer ‘zichtbaar’ zijn dan vroeger. Om goed te kunnen omgaan met deze extensie van de brute werkelijkheid zullen we moeten aanvaarden dat techniek meer is dan ‘*just an extension of men*’.

##### *Secundair gebruik*

Vrijwel alle betrokken partijen, publiek en privaat, geven hoog op over het nut van de verzameling van locatiegegevens. Binnen coöperatief rijden is de noodzaak daartoe evident, zonder locatiegegevens geen coöperatieve diensten. Private partijen zien daarbij ook mogelijkheden voor andere toegevoegde waarde diensten en *targeted advertising*. Voor zover dit gebruik gereguleerd is en instemming heeft van de klant bestaat hiertegen geen bezwaar. Wel zullen de service providers zich ervan bewust moeten zijn dat structureel hergebruik het risico van onrechtmatig gebruik kan vergroten. Vormen van secundair gebruik waarbij de gegevens zijn geanonimiseerd zijn weliswaar minder gevoelig, maar in bepaalde gevallen combinaties van geanonimiseerde gegevens toch weer resultaten kunnen opleveren die wel tot personen te herleiden zijn.

##### *Transparantie*

Om aan de ene kant de rechtmatigheid te kunnen bewaken en aan de andere kant aan al de wensen en mogelijkheden ten aanzien van het (her)gebruik van locatie gebonden persoonsgegevens tegemoet te kunnen komen is transparantie noodzakelijk. Deze transparantie is een vereiste zowel op beleidsniveau als op het niveau van de individuele relatie tussen dienstverlener en gebruiker. Transparantie schept vertrouwen in de beheerbaarheid en de beheersing van het systeem en daarmee in de bescherming van de persoonlijke levenssfeer. Het ontbreken ervan maakt privacy bescherming illusoir en kan daarom niet worden geaccepteerd.

---

<sup>7</sup> Ook hier kan de Deventer moordzaak als leermoment dienen, de GSM plaatsbepaling bleek verre van accuraat.

### Accountability

Om te kunnen vaststellen of een verantwoordelijke voor de verwerking van locatie gebonden persoonsgegevens daadwerkelijk in staat is om de wettelijke bepalingen ten aanzien van de verwerking van persoonsgegevens na te leven is accountability nodig op zowel beleids- als op operationeel niveau. De juiste toepassing van de bewaartermijnen en autorisaties zijn voor de buitenwereld niet goed waarneembaar zodat het van belang is om deze onderwerp te maken van (publieke) controle.

#### 2.1.5 Omslag in het denken over location based privacy

'Location Based Privacy is een complexe samenloop van rolpatronen tussen publiek en privaat, betrouwbaarheid en winstgevendheid, technologische- en bestuurlijk juridische oplossingen.' Naar aanleiding van deze conclusie wijst Griffioen op enkele noties die de spanning tussen het individuele belang en het algemene belang illustreren. Het individuele belang om niet zichtbaar te zijn, en vooral niet langer zichtbaar te zijn dan nodig is<sup>8</sup> en het algemene, collectieve, belang om in bepaalde gevallen over de privacygevoelige locatiedata te kunnen beschikken.

Daarbij moet wel worden bedacht dat digitale sporen steeds talrijker worden hetgeen ertoe noopt meer na te denken over de toegang tot die informatie: welke data moeten beschikbaar zijn voor wie?<sup>9</sup> Griffioen stelt dat als het gaat om *location based privacy* wellicht een omslag in denken nodig is omdat *floating car data* een steeds hogere vlucht zullen nemen en omdat nu al de traceerbaarheid van personen via hun *smartphone* groot is. Het is een illusie te denken dat de grote hoeveelheid data die beschikbaar is kan worden ingedamd. Daarom zal moeten worden geïnvesteerd in de inkadering van het gebruik van de informatie.

Een tweede reden voor de omslag in het denken is dat de huidige 'notie van controle over zelfopenbaring er enigszins van uitgaat dat het individu zelf primair verantwoordelijk is voor het op orde hebben van zijn of haar digitale zaken'. In het 'vertakte informatie-universum' is het echter niet goed mogelijk om de bescherming van de burgers geheel aan hun eigen 'kennis en actiebereidheid' over te laten.

Tenslotte is de omslag in het denken nodig om weer een deel van de verloren gegane *practical obscurity* terug te winnen. Door de stand van de techniek is deze notie van natuurlijke toestand verworden tot nastrevenswaardig principe. Daarom is het tijd om de mogelijkheid om 'de voorhanden zijnde informatierijkdom spaarzamer, zorgvuldiger en rechtmatiger te gebruiken' te faciliteren, en deze uiteindelijk ook institutioneel en door middel van techniek te waarborgen. Alleen op die manier kan het recht op bescherming van de persoonlijke levenssfeer ook in de toekomst blijvend worden gerealiseerd.

## 2.2 Specifieke condities bij Spookfiles A-58

### 2.2.1 Transparantie en accountability

Een complicerende factor bij coöperatief rijden is de deelname van een groot en wisselend aantal marktpartijen. Om in die omstandigheid het recht op bescherming van de persoonlijke levenssfeer te waarborgen is het nastreven van standaarden aan te bevelen. In dit verband kunnen de door de WRR

---

<sup>8</sup> In 1014 is dit recht om digitaal 'vergeten' te worden voor het eerst erkend door het EU Hof ()

<sup>9</sup> p 49, Privacy en vormen van intelligente mobiliteit, WRR 2011, Henk Griffioen.

opgebrachte begrippen transparantie en accountability van grote waarde zijn<sup>10</sup>. Om zicht te kunnen houden op de feitelijke gang van zaken en daarmee op de juiste toepassing van de privacywetgeving zal transparantie moeten worden betracht, zowel binnen de domeinen van de individuele marktdeelnemers als bij de koppelvlakken tussen de systeemonderdelen en bij de betrokken publieke partijen. Binnen een transparant systeem moet het mogelijk zijn om de accountability van alle betrokken partijen goed vast te stellen en te waarborgen. Daartoe kan worden overwogen om regels te ontwikkelen en vast te leggen omtrent de mate van transparantie en de wijze waarop deze kan worden bereikt en gecontroleerd.

### **2.2.3 Klantperspectief**

Bij de beoordeling van de bescherming van persoonsgegevens staat de persoon wiens gegevens het betreft, de betrokkene, centraal. De betrokkene is in dit geval de eindgebruiker van de dienst, de klant. Daarom is voor het leggen van een goede verbinding tussen de klant en de leverancier een beschrijving van de dienst vanuit het klantperspectief noodzakelijk. Door de opzet van het huidige project Spookfiles-A58, waarbij alle partijen zich specifiek richten op hun onderdeel in het geheel, en geen sprake is van systeemintegratie, ontbreekt vooralsnog een beschrijving vanuit dit klantperspectief. Daardoor wordt het lastiger om concreet aan te geven waar en door wie maatregelen ter bescherming van persoonsgegevens moeten worden genomen. Met name de positie van de verantwoordelijke voor de verwerking van persoonsgegevens in de zin van de WBP is daarbij van belang. In principe is dit de serviceprovider waarmee de gebruiker een overeenkomst sluit voor de coöperatieve dienst. Binnen de huidige structuur van het project Spookfiles-A58 treden echter verschillende partijen in meerdere rollen op en is niet altijd op voorhand duidelijk wie uiteindelijk de rol van verantwoordelijke zal hebben. Het ontbreken van een gedefinieerde relatie tussen de betrokkene en de verantwoordelijke bemoeilijkt een goede bewaking van de bescherming van persoonsgegevens in dit stadium. Bij het introduceren van de dienst zal erop moeten worden gelet dat de serviceproviders die op dat moment als verantwoordelijke zijn aan te merken voldoende maatregelen hebben genomen. Ook zullen zij over voldoende gegevens moeten kunnen beschikken om ook als verantwoordelijke op te treden voor eventuele achterliggende verwerkers.

---

<sup>10</sup> WRR-Privacy en intelligente vormen van mobiliteit, Griffioen 2011

## 2.3 Wettelijke bepalingen

### 2.3.1 Inleiding

Coöperatief rijden betekent dat het weggedrag van voertuigen onderling op elkaar wordt afgestemd<sup>11</sup>. Daartoe moet de informatie over de situatie van het een voertuig, zoals locatie snelheid, richting uit het voertuig worden verzameld in opdracht van de provider die de coöperatief rijden dienst levert. Deze informatieoverdracht omvat in veel gevallen tot een persoon te herleiden gegevens, ic. de bestuurder en/of eigenaar van het voertuig, en valt onder de bescherming van persoonsgegevens. Deze bescherming wordt primair geregeld in art 8 van het Europees Verdrag voor de Rechten van de Mens waarin het recht op een persoonlijke levenssfeer is opgenomen. Deze basis geeft goed het belang van de bescherming van de persoonlijke levenssfeer als fundamenteel mensenrecht weer. De noties uit dit Verdrag zijn vertaald naar Europees recht in de dataproductie Richtlijn 95/46/EG van het Europees Parlement en de Raad<sup>12</sup>. Nationaal zijn de belangrijkste wetten ter bescherming van de persoonlijke levenssfeer de WBP als algemene wet en de Tw<sup>13</sup> als lex specialis voor de telecommunicatiesector. De data overdrachten in het kader van de dienstverlening binnen coöperatief rijden vallen onder de algemene bepalingen van de WBP, voor zover niet de meer specifieke bepalingen met betrekking tot het dataverkeer in de Tw<sup>14</sup> van kracht zijn. In hoofdstuk 11 van deze wet zijn privacy bepalingen opgenomen met het oog op toepassing in de telecommunicatiesector. Daarbij vormen in het bijzonder de vermelde toegevoegde waarde diensten een aanknopingspunt met coöperatief rijden<sup>15</sup>. Coöperatief rijden zal moeten worden ingericht binnen dit wettelijk kader.

### 2.3.2 Wet Bescherming Persoonsgegevens

De WBP is een uitwerking van de Europese dataproductie Richtlijn (EG) 95/46. Persoonsgegevens zijn in de WBP gedefinieerd als gegevens betreffende een geïdentificeerde of identificeerbare persoon<sup>16</sup>. Met betrekking tot de omgang met persoonsgegevens schrijft de wet voor dat een verantwoordelijke voor de verwerking van persoonsgegevens, ic. de aanbieder van de coöperatief rijden dienst, zorgvuldig en behoorlijk met de persoonsgegevens van zijn klanten moet omgaan<sup>17</sup>. Daarbij is de invulling van het begrip zorgvuldig in het geval van private dienstverleners gerelateerd aan het zorgvuldigheidscriterium uit het Burgerlijk Wetboek<sup>18</sup>. In het desbetreffende artikel wordt zorgvuldigheid gekoppeld aan

<sup>11</sup> Coöperatieve systemen ondersteunen bestuurders bij hun rij-taken en communiceren hiervoor met andere voertuigen of met systemen langs de wegwijk, hierdoor beschikken zij over actuele informatie.

<sup>12</sup> Richtlijn van het Europees Parlement en de Raad van 24 oktober 1995 (PbEG nr. L281, p31-50)

<sup>13</sup> <http://wetten.overheid.nl/BWBR0011468/geldigheidsdatum01-12-2014>;

<http://wetten.overheid.nl/BWBR0009950/geldigheidsdatum01-12-2014>

<sup>14</sup> Aangezien de coöperatief rijden dienst geen basis communicatiedienst is maar duidelijk een inhoudelijke toevoeging betreft die door de dienstverlener inhoudelijk wordt gecontroleerd, moet ervan worden uitgegaan dat de dienst binnen deze definitie valt. Daarmee valt de dienst buiten de definitie van artikel 1, echter niet buiten het bereik van de hele Telecommunicatiewet. Met name met het oog op de privacy is hoofdstuk 11 van de Telecommunicatiewet opgenomen. Dit artikel beoogt de persoonlijke levenssfeer van gebruikers van telecommunicatie te beschermen. In art. 11.1 is een aantal definities opgenomen die betrekking hebben op de verwerking van persoonsgegevens in het kader van toegevoegde waarde diensten, onder uitdrukkelijke voorwaarde van toestemming van de gebruiker. Deze toegevoegde waarde diensten worden in artikel 11.5a nader benoemd.

<sup>15</sup> Artikel 11.5a Telecommunicatiewet

<sup>16</sup> Artikel 1, onder a WBP

<sup>17</sup> Artikel 6 WBP

<sup>18</sup> Artikel 6:162 BW

1. Hij die jegens een ander een onrechtmatige daad pleegt, welke hem kan worden toegerekend, is verplicht de schade die de ander dientengevolge lijdt, te vergoeden.

2. Als onrechtmatige daad worden aangemerkt een inbreuk op een recht en een doen of nalaten in strijd met een wettelijke plicht of met hetgeen volgens ongeschreven recht in het maatschappelijk verkeer betaamt, een en ander behoudens de aanwezigheid van een rechtvaardigingsgrond.

3. Een onrechtmatige daad kan aan de dader worden toegerekend, indien zij te wijten is aan zijn schuld of aan een oorzaak welke krachtens de wet of de in het verkeer geldende opvattingen voor zijn rekening komt.

handelen of nalaten in strijd met de wet of met ongeschreven regels of algemene opvattingen in het maatschappelijk verkeer. Het gaat dus om een open norm, die door de dienstverlener zelf zal moeten worden ingevuld aan de hand van de concrete omstandigheden. Daarbij is de verwerking van de gegevens aan een specifiek doel gebonden<sup>19</sup>. Ook is de verwerking alleen toegestaan met een wettelijke grond<sup>20</sup> en is de bewaartermijn voor bewerking van persoonsgegevens beperkt tot de periode die met het oog op het doel van de bewerking noodzakelijk is<sup>21</sup>. Verder mogen niet meer gegevens worden verzameld dan voor het doel noodzakelijk is<sup>22</sup>. De verantwoordelijken, ic. de coöperatief rijden dienstverleners, dragen zorg voor passende technische en organisatorische maatregelen om de gegevens te beveiligen<sup>23</sup>. Daartoe stellen zij eisen aan de achterliggende verwerkers van de (persoons)gegevens, en houden zij toezicht op de hen gecontracteerde verwerkers.

### *Grondslagen*

De WBP kent zes grondslagen voor de verwerking van persoonsgegevens, waarvan met name de eerste twee in het geval van coöperatief rijden van toepassing zouden kunnen zijn. Zo kunnen persoonsgegevens worden verwerkt op basis van een ondubbelzinnige toestemming van de betrokkene en kan de verwerking plaatsvinden in het kader van de uitvoering van een overeenkomst. Het CBP heeft echter vastgesteld dat locatiegegevens tot de categorie gevoelige gegevens moeten worden gerekend<sup>24</sup>. Daarbij stelt het CBP dat uit de locatiegegevens verplaatsingen kunnen worden afgeleid die een patroon kunnen opleveren waaruit specifieke gevoelige persoonsinformatie kan worden verkregen.

*Voorbeeld: Door een bepaald voertuig te volgen bij bijvoorbeeld ziekenhuis-, kerk- of moskeebezoek, zou informatie kunnen worden afgeleid met betrekking tot de gezondheidstoestand of de religie van de desbetreffende voertuighouder. Dat risico leidt ertoe dat de locatiegegevens in het geval van een dienstverleningsovereenkomst voor in car services als gevoelig moeten worden aangemerkt.*

Door de gegevens als gevoelig te bestempelen is de enige manier om in het kader van de dienstverlening het verbod te doorbreken het verkrijgen van de ondubbelzinnige toestemming van de betrokkene. Binnen de WBP krijgt de vereiste ondubbelzinnige toestemming vanwege het gevoelig karakter van de gegevens een andere wettelijke grondslag.<sup>25</sup> Overigens staat deze ondubbelzinnige toestemming in de Tw als enig mogelijke grond voor de verwerking van locatiegegevens niet zijnde meta-gegevens in het kader van het verlenen van toegevoegde waarde diensten genoemd. De toestemming is ondubbelzinnig als hij uit vrije wil is gegeven nadat de verantwoordelijke de betrokkene heeft geïnformeerd over wat er met zijn persoonsgegevens gebeurt, het zogenoemde *informed consent*. De bewijslast voor een ondubbelzinnige toestemming ligt bij de verantwoordelijke, die er goed aan doet dit bewijs vast te leggen. De betrokkene kan de toestemming te allen tijde terugtrekken, zij het niet met terugwerkende kracht. Van belang daarbij is dat de klant redelijker wijs geacht kan worden te begrijpen waarmee deze zich akkoord verklaart, met andere woorden: wat de expliciete en impliciete impact van zijn toestemming is.

---

<sup>19</sup> Artikel 7 en 9 WBP

<sup>20</sup> Artikel 8 WBP

<sup>21</sup> Artikel 10 WBP

<sup>22</sup> Artikel 11 WBP

<sup>23</sup> Artikel 13 WBP (Privacy by design)

<sup>24</sup> Ambtshalve onderzoek cbp naar de verwerking van geolocatiegegevens door TomTom N.V. 20 december 2011.

<sup>25</sup> Art. 23 lid sub a. WBP

*Voorbeeld: Dat de toestemming uit vrije wil moet zijn gegeven kan in een werkgever werknemer verhouding problematisch zijn. Recent heeft de rechter in Wenen een bedrijf verboden zijn service auto's uit te rusten met on board units die de route van de auto's zichtbaar maakten. Anders dan in Frankrijk, waar de wetgeving voorziet in het uitzetten van de apparatuur buiten diensttijd, vond de rechter dat het volgen van de medewerkers ook tijdens diensttijd te ver ging. Hun toestemming was, gelet op de gezagsverhouding tussen werkgever en werknemer, niet zodanig uit vrije wil gegeven dat deze kon worden geacht conform de wet te zijn. De zaak was aanhangig gemaakt door de ondernemingsraad/vakbond.*

### *Doelbinding*

Een belangrijke maatstaf bij het verwerken van persoonsgegevens is het doel waarvoor de gegevens mogen worden verwerkt<sup>26</sup>. Deze doelomschrijving moet welbepaald, uitdrukkelijk omschreven en gerechtvaardigd zijn. Verwerking van de gegevens in het kader van coöperatief rijden kan, mits goed gedefinieerd, als legitiem doel worden aangemerkt. Als een dienstaanbieder de gegevens ook voor andere toegevoegde waarde diensten wil gebruiken, dan zal erop moeten worden gelet dat deze verwerking niet onverenigbaar is met het doel waarvoor de gegevens zijn verkregen.<sup>27</sup>

Dit betekent dat er een verwantschap zal moeten zijn tussen het oorspronkelijke doel en het beoogde doel van de nieuwe verwerking. Zogeheten *function creep* ligt daarbij op de loer.

Ook de aard van de gegevens speelt in dat kader een rol. Hoe gevoeliger de gegevens, hoe eerder er sprake zal zijn van onverenigbaarheid met het oorspronkelijke doel. Gelet op de gevoeligheid van locatie-informatie is in het geval van coöperatief rijden voorzichtigheid geboden.

Naast de wijze waarop de gegevens zijn verkregen speelt ook de mate waarin de betrokkene de positieve of negatieve gevolgen ondervindt van de nieuwe verwerking een rol in de afweging. Tenslotte zijn de waarborgen voor een juridisch correcte verwerking van belang, hoe beter deze zijn geregeld, hoe minder snel sprake zal zijn van onverenigbaarheid.

### *Informatieplicht*

De verantwoordelijke heeft ten opzichte van de betrokkene een informatieplicht. Niet alleen moet de betrokkene goed worden geïnformeerd over het doel van de verwerking, ook moet de identiteit van de verantwoordelijke duidelijk zijn. Ten aanzien van de informatieplicht zijn twee situaties te onderscheiden, een waarbij de gegevens rechtstreeks van de betrokkene komen<sup>28</sup>, en een waarbij de gegevens op een andere manier worden verzameld<sup>29</sup>. In deze artikelen is het 'transparantiebeginsel' vormgegeven. Dit beginsel houdt in dat aan de betrokkene moet worden duidelijk gemaakt welke gegevens worden verwerkt, en waarvoor. In het kader van de dienstverlening coöperatief rijden zullen de gegevens in eerste instantie van - het voertuig van - de betrokkene komen. Door middel van het *informed consent* kan in dat geval aan de informatieplicht worden voldaan. Denkbaar is echter dat ook andere gegevensbronnen een rol spelen in het coöperatief rijden systeem. Over eventuele persoonsgegevens uit andere bronnen zal de betrokkene zo nodig achteraf geïnformeerd moeten worden.

---

<sup>26</sup> Art 7 WBP

<sup>27</sup> In de eerder genoemde TomTom casus wringde hier de schoen. Weliswaar waren de aan de politie geleverde gegevens geanonimiseerd, maar het doorleveren van de gegevens door TomTom aan de politie was niet opgenomen bij de informatie die in het kader van het verkrijgen van de toestemming was verstrekt.

<sup>28</sup> Art 33 WBP

<sup>29</sup> Art. 34 WBP



### *Kwaliteit van de gegevens*

Als het gaat om de kwaliteit van de gegevens dan geeft de WBP daarvoor een nadere invulling van de begrippen behoorlijk en zorgvuldig<sup>30</sup>. Zo mag de verzameling van persoonsgegevens niet bovenmatig zijn en moeten de gegevens juist zijn. Juist is in dit verband te onderscheiden in een formele juistheid en een materiele juistheid. Van de eerste is sprake als er sprake is van integere data, zonder invoerfouten (bijv. is het ingevoerde adres een bestaand adres?). Van het tweede is sprake als de gegevens in de database inhoudelijk juist zijn (bijv. woont betrokkene op het ingevoerde adres?).

### *Geheimhouding*

Om de persoonlijke levenssfeer van de betrokkene optimaal te kunnen beschermen is voorzien in een geheimhoudingsplicht voor allen die op enige manier met de verwerking van de gegevens bezig zijn, of anderszins toegang zouden kunnen hebben tot de gegevens<sup>31</sup>. De verantwoordelijke moet ervoor zorg dragen dat de geheimhoudingsplicht wordt nageleefd. Dit heeft consequenties voor de organisatorische als technische inrichting van data-verwerkende systemen.

### *Beveiliging*

Een van de manieren om aan deze verplichting te voldoen is het treffen van voldoende beveiligingsmaatregelen. Bij deze maatregelen moet rekening worden gehouden met de stand van de techniek en de risico's voor de betrokkene. De volgende maatregelen zijn in dit kader in ieder geval aan te bevelen:

- Een regeling met betrekking tot het gebruik van de gegevens,
- Een regeling van bevoegdheden, bijvoorbeeld voor de systeembeheerder,
- Een regeling en/of procedure voor de vernietiging van gegevens,
- Passende - state of the art - hard- en software, in het bijzonder bij draadloos gegevensverkeer zoals bij coöperatief rijden.

### *Rechten van de betrokkene*

De verantwoordelijke kan altijd de persoonsgegevens die hij onder zijn hoede heeft verstrekken aan de betrokkene. In het geval dat niet spontaan gebeurt kent de wet mogelijkheden om toch kennis te nemen van de eigen persoonsgegevens<sup>32</sup>. Dit recht op kennisneming hoeft niet te worden gemotiveerd. Als in de registratie van de verantwoordelijk fouten zitten, dan kan de betrokkene verzoeken om verbetering, aanvulling, verwijdering of afscherming<sup>33</sup>. De verantwoordelijke moet vervolgens binnen vier weken reageren op een dergelijk verzoek. Als de verantwoordelijk naar aanleiding van het verzoek de data aanpast, dan is hij gehouden dit ook aan zijn afnemers mee te delen.

### *Melding*

Iedere verantwoordelijke voor de geheel of gedeeltelijke geautomatiseerde verwerking van persoonsgegevens moet deze verwerking melden bij het CBP<sup>34</sup>. Handmatige verwerkingen zijn van de meldingsplicht uitgesloten. In het geval van coöperatief rijden zal er sprake zijn van een meldingsplicht, aangezien het geautomatiseerde gegevensverwerking betreft.

---

<sup>30</sup> Art. 11 WBP

<sup>31</sup> Art. 12 WBP

<sup>32</sup> Art. 35 WBP

<sup>33</sup> Art. 36 WBP

<sup>34</sup> Art. 27 WBP

### *Toezicht*

Het toezicht in het kader van de WBP is opgedragen aan het CBP<sup>35</sup>. Het CBP heeft tot taak toe te zien op de naleving van de wettelijke bepalingen in Nederland. Het kan in dat verband onderzoeken instellen en bestuurlijke boetes uitdelen in geval van overtredingen.

Voor die bedrijven of branches waarvoor de verwerking van persoonsgegevens een zeer prominente plaats in de bedrijfsvoering inneemt bestaat de mogelijkheid een functionaris voor de gegevensbescherming aan te stellen<sup>36</sup>. Deze natuurlijke persoon is onafhankelijk en ziet toe op de naleving van de WBP binnen zijn bedrijf of bedrijfstak. Voor coöperatief rijden zou een dergelijke functionaris, bijvoorbeeld in dienst van een branchevereniging coöperatief rijden, een goede rol kunnen vervullen gelet op het specifieke karakter van de gegevensverwerking en het grote aantal zeer uiteenlopende bedrijven dat bij coöperatief rijden betrokken zal zijn.

### **2.3.3 Wet op de Telecommunicatie**

In de Wet op de Telecommunicatie (Tw) is de privacy meer specifiek geregeld ten behoeve van de telecommunicatiesector, omdat die sector bijzonder privacygevoelig is en omdat de structuur en technische aspecten binnen de sector om een specifieke regeling vragen. Op Europees niveau is de Richtlijn 2002/58/EG vastgesteld. Deze richtlijn is in de Tw geïmplementeerd. Deze wet geeft daarmee een duidelijk kader voor de omgang van onder de wet vallende dienstverleners ten aanzien van de omgang met persoonsgegevens.

### *Locatiegegevens*

Coöperatief rijden is een dienst die in het bijzonder gebruikt maakt van locatiegegevens. In de Tw wordt bij locatiegegevens een onderscheid gemaakt tussen locatiegegevens als verkeersgegevens en locatiegegevens als basisgegevens voor de dienstverlening. Bij coöperatief rijden vallen de verkeersgegevens, in tegenstelling tot bij mobiele telefonie, in de laatste categorie. Locatiegegevens vormen immers het hart van de dienst, zowel bij de verzameling ervan als bij het verlenen van de dienst in het voertuig. In artikel 9 van de Richtlijn 2002/58 worden deze locatiegegevens onderscheiden van de meta-gegevens die slechts een ondersteunende rol hebben. In het geval van coöperatief rijden zijn extra maatregelen voor privacybescherming nodig omdat informatie vanuit een kastje in een passerend voertuig naar de walkant wordt gezonden, en vervolgens wordt verwerkt. Deze gegevens bevatten naast de locatie ook identificerende gegevens van de on-board-unit en dus ook van de gebruiker. In combinatie met de gegevens van medeweggebruikers op dezelfde locatie, leiden de verzamelde gegevens tot de mogelijkheid van het geven van een snelheidsadvies. Dit advies wordt via het communicatiekanaal op de locatie teruggezonden aan de on-board-unit in het voertuig. Hoewel dit signaal inhoudelijk geen identificerende gegevens bevat kunnen wel verkeersgegevens zoals een ID en locatiegegevens nodig zijn om het advies aan boord van een specifieke klant te krijgen.

### *Informeren gebruiker*

In de Tw zijn bijzondere bepalingen opgenomen voor de verwerking van persoonsgegevens ten behoeve van het verlenen van toegevoegde waarde diensten zoals coöperatief rijden. Hoofdregel is dat dit alleen mogelijk is nadat de gebruiker daarvoor uitdrukkelijk toestemming heeft gegeven<sup>37</sup>. Deze eis is gelijk aan

---

<sup>35</sup> Art. 51 e.v. WBP

<sup>36</sup> Art. 62 e.v. WBP

<sup>37</sup> Artikel 11.5a lid 2 TW

die op grond van de WBP, met name ten aanzien van gevoelige gegevens.. Voorafgaand aan het verkrijgen van deze toestemming wordt de volgende informatie door de aanbieder aan de gebruiker verstrekt:

- Soort locatiegegevens die worden verwerkt;
- Doeleinden waarvoor de locatiegegevens worden verwerkt;
- Duur van de verwerking en;
- Of de gegevens aan een derde zullen worden verstrekt, en zo ja aan welke.

In het geval van toestemming op basis van de vooraf aan de gebruiker verstrekte informatie (*informed consent*) mogen de gegevens worden verwerkt in het kader van het verlenen van de dienst met toegevoegde waarde en voor de facturering. Daarna moeten de gegevens direct worden vernietigd of geanonimiseerd<sup>38</sup>.

#### *Intrekken toestemming*

De toestemming kan te allen tijde door de gebruiker worden ingetrokken<sup>39</sup>. Ook moet de afnemer van de dienst de mogelijkheid worden geboden om kosteloos en op eenvoudige wijze de verwerking stop te zetten. De gegevens mogen slechts worden verwerkt door personen werkzaam onder het gezag van de aanbieder of van een derde mits dit aan de gebruiker is meegedeeld, en voor zover die verwerking nodig is om de toegevoegde waarde dienst te kunnen verlenen. Van belang is dat het de verantwoordelijke is die de toestemming krijgt van de gebruiker. Dit zal veelal de service provider zijn die de overeenkomst met de coöperatief rijden klant sluit. In dat geval zullen andere partijen in de keten die de dienst mogelijk maken als verwerker optreden. De aanbieder van een toegevoegde waarde dienst moet bovendien aan de betrokkene de mogelijkheid bieden om, kosteloos en eenvoudig, de verwerking en/of de overbrenging van zijn of haar gegevens via het openbare elektronische communicatienetwerk tijdelijk te beletten.

#### *Certificatiedienstverleners*

Aangezien binnen coöperatief rijden wordt nagedacht over het gebruik van certificaten ten einde het berichtenverkeer te kunnen authenticeren en ondertussen de privacy van de gebruiker optimaal te beschermen, is ook het artikel aangaande het verstrekken van certificaten in het kader van coöperatief rijden van belang<sup>40</sup>. Het artikel stelt dat ook dienstverleners die certificaten verstrekken de persoonsgegevens uitsluitend mogen verwerken met toestemming van de betrokkene, en voor zover de verwerking nodig is voor het verlenen van de dienst. Verder zijn de gebruikelijke bepaling over doelbinding opgenomen en een bijzondere bepaling voor afwijking van de uitdrukkelijke toestemming in het geval van opsporing van fraude en in andere gevallen die in de wet zijn bepaald.

## **2.4 Toepassingen Spookfiles A-58**

### **2.4.1 Verwerking door coöperatief rijden dienstverleners**

De meesten van ons herinneren zich nog wel het spelletje fluisterpost. De kinderen zitten in een kring en één van hen neemt een woord in gedachten. Dat woord fluistert hij in het oor van zijn buurman. Die geeft het weer door aan de volgende en die weer aan de volgende totdat de laatste in de kring vertelt wat hij heeft gehoord. In het gunstigste geval leek het woord op het oorspronkelijk ingebrachte woord, maar identiek was het vrijwel nooit. Onderweg waren meestal wel veranderingen opgetreden, bijvoorbeeld door gebrekkige articulatie bij het fluisteren, slecht luisteren door de ontvanger, teveel afleiding of door het bewust veranderen van het woord door een baldadige deelnemer. Het

---

<sup>38</sup> Artikel 11.5a lid 1 onder a TW

<sup>39</sup> Artikel 11.5a lid 4 onder a TW

<sup>40</sup> Artikel 11.5b TW

ongeschonden doorgeven van het woord vergde de wil om het woord goed over te brengen en de nodige concentratie bij de deelnemers. Daarbij bestaat het proces uit een koppelvlak, het fluisteren en luisteren, en een verwerkingsproces, het opnemen van het woord en het weer uitspreken ervan naar de volgende in de kring.

Coöperatief rijden zoals nu voorzien in het A-58 project, en in het bijzonder de verwerking van persoonsgegevens, lijkt in en aantal opzichten enigszins op fluisterpost. In dit project wordt op basis van informatie over de verkeerssituatie op de weg een snelheidsadvies gegeven aan zich op die weg bevindende voertuigen. Het proces start met een auto die een signaal met zijn locatie, snelheid en rijrichting aan de wegw kant doorgeeft, vergelijkbaar met de start van fluisterpost. Dit signaal wordt via de wegw kantoperator doorgegeven aan de serviceprovider. Deze verwerkt het signaal met behulp van andere service providers, de dataleveranciers en geeft het door voor verzending naar het voertuig. De wegw kantserviceprovider zorgt er uiteindelijk voor dat het advies in de auto komt. De bestuurder kan vervolgens het advies ter harte nemen en zijn snelheid aanpassen. Als de andere bestuurders op dezelfde weg dat ook doen dan kan de collectieve snelheid zo worden aangepast dat geen (spook) file ontstaat.

Aangezien de gegevens-set die in het systeem wordt ingebracht gevoelige persoonsinformatie bevat<sup>41</sup> moet in de hele keten van verwerking, waaronder zowel de overdracht van gegevens als de bewerking in het systeem van de dienstverlener valt, de bescherming van de gegevens worden gegarandeerd. Deze garantie wordt door de verantwoordelijke gegeven aan de betrokkene, de bestuurder en/of eigenaar van het voertuig. De andere dienstverleners in het proces zullen in de regel als verwerkers in het kader van de WBP optreden. De verantwoordelijke heeft de taak ervoor te zorgen dat op basis van de versterkte informatie het juiste advies in de auto komt en onderweg de privacy van de betrokkene optimaal is gewaarborgd.

#### **2.4.2 Verantwoordelijke (rechts)persoon**

Voor de betrokkene en de private dienstverleners is van belang dat de verantwoordelijke in het kader van de WBP altijd een natuurlijke- of een rechtspersoon is. Daarmee past de rol van verantwoordelijke goed in een bedrijfsmatig juridisch organisatie model. Aangezien door Beter Benutten wordt gestreefd naar marktontwikkeling waarbij verschillende dienstverleners op verschillende onderdelen van de dienstverlening actief kunnen zijn is de positie van de verantwoordelijke niet eenvoudig. Hij zal zicht moeten krijgen op de verwerking van de gegevens door de verwerkers in de keten zonder dat hem door de verwerkers inzicht wordt gegund in de precieze verwerking. De verwerkende dienstverlener kan immers op een ander moment een concurrent zijn. Hierdoor is de transparantie van de gegevensverwerking door de keten moeilijk te realiseren. Daarbij kan het van belang zijn of de verantwoordelijke opereert binnen een consortium zonder of met rechtspersoonlijkheid. Als het consortium rechtspersoonlijkheid heeft, dan zal het ook de dienst zelfstandig aanbieden en dus als verantwoordelijke worden aangemerkt. In dat geval vindt de verwerking mogelijk onder gezag van het consortium plaats. Is er geen sprake van rechtspersoonlijkheid van het consortium dan is de aanbiedende dienstverlener de verantwoordelijke. Deze moet dan door middel van overeenkomsten

---

<sup>41</sup> In de casus waarin Tomtom geanonimiseerde geodata had verwerkt zonder expliciete toestemming van de betrokkene ten aanzien van het doel van de verwerking heeft het CBP geoordeeld dat, gelet op het gevoelige karakter van de geodata, de verwerking uitsluitend kan worden gebaseerd op uitdrukkelijke toestemming van de betrokkene. Het CBP verwijst ook naar de opinie van de gezamenlijke EU privacy commissioners: WP29 185 Opinion 13/2011 on geolocation services on smart mobile devices, 16 May 2011. Deze keuze voor toestemming als enige grond correspondeert met de bepaling in Artikel 6 lid 3 van Richtlijn (EG) nr 2002/58 en met Artikel 11.5a van de daarop gebaseerde Wet op de Telecommunicatie.

met de verwerkers borgen dat de kwaliteit van de verwerking kan worden gegarandeerd. In ieder geval moet de regeling met betrekking tot de verantwoordelijkheid voor de verwerking binnen een samenwerkingsverband van dienstverleners helder zijn en niet tot een nadelige(r) positie van de betrokkene leiden.

### **2.4.3 Risicoklassen**

Om de juiste maatregelen te kunnen nemen ten aanzien van de verwerking van persoonsgegevens zal een analyse moeten worden gemaakt van de risicoklasse van de persoonsgegevens. Hiervoor moet worden gekeken naar de factoren die bij het bepalen van de risicoklasse een rol spelen. Daartoe moet eerst worden bepaald in welke processen binnen coöperatief rijden persoonsgegevens worden verwerkt. Nadat dit is vastgesteld zal vervolgens de aard van de gegevens moeten worden vastgesteld. Het CBP heeft aangegeven dat locatiegegevens in combinatie met persoonsgegevens tot de categorie gevoelige gegevens behoren, waarvoor een verzaamd regime geldt. Aan de hand van de gevonden parameters moeten eerst de risico's worden bepaald en moet uiteindelijk ook de risicoklasse worden vastgesteld. Er zijn vier risicoklassen voor de verwerking van persoonsgegevens benoemd. Hierna worden deze kort aangeduid met een illustrerend voorbeeld of toelichting:

- 0 publiek niveau, een voorbeeld hiervan is het telefoonboek;
- 1 basisniveau, voorbeelden zijn ledenadministraties, hotelboekingen;
- 2 verhoogd risico, gevoelige gegevens waarbij negatieve gevolgen voor de betrokkene zullen ontstaan bij verlies of onbehoorlijke verwerking;
- 3 hoog risico, opsporing, gevoelige gegevens, waarbij ernstige schade voor betrokkene mogelijk is bij verlies of onbehoorlijke verwerking.

Gelet op het feit dat locatie gebonden persoonsgegevens als gevoelige gegevens in het kader van de WBP worden aangemerkt zal de verwerking van persoonsgegevens binnen coöperatief rijden in klasse 2 of zelfs in klasse 3 vallen.

### **2.4.4 Beveiliging**

In de WBP is ook aandacht gegeven aan de beveiliging van de gegevens. In de WBP staat : 'de verantwoordelijke legt passende technische en organisatorisch maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking'<sup>42</sup>.

Daarbij moet de verantwoordelijke rekening houden met de stand van de techniek, en met inachtneming van een passend beveiligingsniveau gelet op de risico's van de verwerking en de aard van de gegevens. Een belangrijk aspect bij de concrete invulling van de wettelijke bepaling zijn de kwaliteitsaspecten waarmee rekening moet worden gehouden, deze zijn: exclusiviteit, integriteit en continuïteit.

- Exclusiviteit. Dit houdt in dat uitsluitend daartoe bevoegde personen toegang krijgen tot de gegevens.
- Integriteit. De persoonsgegevens moeten in overeenstemming zijn met het afgebeelde deel van de werkelijkheid.
- Continuïteit. De gegevensverwerking moet ongestoord voortgang kunnen vinden.

Om de kwaliteitsaspecten te waarborgen neemt de verantwoordelijke maatregelen zowel op technisch als op organisatorisch niveau. Deze twee elementen moeten altijd samenhangend worden ingezet in

---

<sup>42</sup> Artikel 13 WBP

relatie tot de te beschermen gegevens. Daarbij speelt in het geval van coöperatief rijden dat gevoelige persoonsgegevens via publieke en draadloze netwerken worden verzonden hetgeen bijzondere beschermende maatregelen, zoals gecertificeerde authenticatie, vereist.

De verantwoordelijke neemt passende maatregelen na analyse van de beveiligingsbehoefte. Daarbij maakt hij gebruik van drie afwegingsfactoren:

- Stand van de techniek,
- Kosten van de maatregelen,
- Risico's die de verwerking en de aard van de gegevens met zich brengen.

Als het gaat om de stand van de techniek, dan vraagt de wetgeving om 'state of the art' techniek toe te passen. In de eerste plaats zal moeten worden vastgesteld wat die techniek is. Vervolgens zal eventuele verouderde techniek die nog in gebruik is moeten worden vervangen. Een en ander houdt in dat de technische afweging in het licht van de technische ontwikkelingen periodiek opnieuw moet worden gemaakt. Ook moet de verantwoordelijke alert zijn op plotseling wijzigende omstandigheden, zoals bijvoorbeeld het succesvol optreden van hackers of updates van leveranciers met het oog op een verhoogd beveiligingsrisico.

Wat betreft de kosten is een afweging van kosten en baten noodzakelijk. De kosten moeten evenredig zijn aan het belang van het te beveiligen object, i.c. het systeem waarbinnen de persoonsgegevens worden verwerkt. Deze kosten zijn niet los te zien van het derde element: de gepercipieerde risico's. Deze moeten worden bezien aan de hand van de gebruikte techniek en de aard van de gegevens. Gelet op de vastgestelde gevoeligheid van de persoonsgegevens binnen coöperatief rijden en de aard van het verwerkingssysteem - communicatie tussen wegwagen en rijdende voertuigen en voertuigen onderling - is sprake van een hoog risicoprofiel (risico klasse 2 of 3) en is een substantieel beveiligingsniveau noodzakelijk. Dit kan leiden tot eveneens substantiële kosten voor de beveiliging.

Gelet op de vele serviceproviders die betrokken zijn bij de coöperatief rijden dienst is het bereiken van afdoende dataprotectie-bewustzijn in de hele keten een flinke uitdaging. In de eerste plaats omdat het voor de verantwoordelijke moeilijk is om controle te krijgen over de verwerkers van persoonsgegevens in de keten. Het feit dat de dienstverleners, naast het participeren in het systeem, op aanpalende gebieden elkaars concurrenten zijn maakt volledige openheid ten aanzien van elkaars bedrijfsprocessen lastig. Niettemin is het risico van de verwerking van de gevoelige persoonsgegevens evident en zal de discussie over wat toelaatbare kosten zijn voor de bescherming van de persoonlijke levenssfeer ook tussen verantwoordelijken en verwerkers moeten worden gevoerd. Daarbij zullen eventuele keuzes steeds moeten worden getoetst aan de genoemde kwaliteitsaspecten.

#### **2.4.5. Dataprotectiebeleid**

De vraag is hoe binnen de coöperatief rijden dienst een balans kan worden gevonden tussen de stand van de techniek, de kosten die beschermingsmaatregelen met zich brengen en de risico's die met de beschermingsmaatregelen worden afgedekt? De wet geeft aan dat zowel organisatorische als technische middelen moeten worden ingezet om deze balans te bereiken. De coöperatief rijden dienst wordt met één verantwoordelijke dienstverlener gerealiseerd in een keten van allerlei dienstverleners. Het gaat daarbij vaak om middelgrote technisch-commerciële organisaties die hun eigen afweging zullen maken ten aanzien van de balans tussen techniek, kosten en risico's. Het zal moeilijk zijn voor de verantwoordelijke dienstverlener om daar in organisatorische zin vat op te krijgen. Gebleken is dat de

bedrijven in het project als het om hun eigen processen gaat de kaarten tegen de borst houden. De discussies blijven in het algemeen beperkt tot de koppelvlakken. Daar komt bij dat de rollen van de dienstverleners heel verschillend zijn. Van dataleverancier tot weggant serviceprovider. De vraag is welke gegevens welke speler in het coöperatief rijden veld nodig heeft en waarvoor? Daarbij is ook nog een onderscheid mogelijk tussen de fase van verzameling en die van verwerking van de gegevens. Omdat een adequate beschrijving van het systeem in deze fase van het project nog ontbreekt konden deze vragen nog niet in deze rapportage worden geadresseerd.

De geadresseerde van het in te vullen dataprotectiebeleid is de verantwoordelijke. Hij is immers de opdrachtgever van de verwerkers en daarmee verantwoordelijk voor het realiseren van de organisatorische en technische maatregelen voor de wettelijke bescherming van de gegevens. Aan de organisatie van de verantwoordelijke de taak om al deze factoren in een samenhangend dataprotectiebeleid vorm te geven. Controle op en handhaving van de uitvoering van het beleid door middel van bijvoorbeeld audits moet daarvan deel uit maken en moet helpen de bescherming van persoonsgegevens te waarborgen. Verder kunnen het opstellen van een privacy policy document en de aanstelling van een functionaris gegevensbescherming hierbij een stimulerende en borgende rol spelen.

Gelet op de complexiteit van het netwerk van dienstverleners dat betrokken is bij de dienst en de diversiteit van de bedrijven lijkt een meer technische benadering van de bescherming van persoonsgegevens een aanlokkelijk perspectief, zowel als het gaat om beveiliging als in het kader van de kwaliteitsborging. Deze verschuiving van organisatorische naar technische maatregelen heeft echter grote consequenties voor de vormgeving van het coöperatief rijden systeem in het algemeen en het dataprotectiebeleid in het bijzonder. Om te beginnen zal een technische oplossing een vaste waarde moeten zijn bij het ontwerp van de architectuur en de uitwerking daarvan. Er zal een infrastructuur moeten ontstaan die een vertrouwde technische invulling van de verwerking van persoonsgegevens mogelijk maakt. Daarbij spelen de aard en de plaats van de gebruikte ICT-voorzieningen, zoals bijvoorbeeld de gebruikte hard- en software en of deze zich in het voertuig of in de back-office van de dienstverlener bevinden, een belangrijke rol. Een technologische oplossing op het niveau van de infrastructuur zal goed bij deze ICT-voorzieningen moeten aansluiten.

#### **2.4.6 Privacy by Design en Privacy-Enhancing Technologies**

In deze visie, waarin sprake is van Privacy by Design, zijn Privacy-Enhancing Technologies binnen de hele infrastructuur van coöperatief rijden van eminent belang. Deze technologie kan ervoor zorgen dat alle componenten tezamen - het netwerk, de databases, de opslagmedia en de verwerkende machine – leiden tot een adequate bescherming van de persoonsgegevens. Daarmee kan de afhankelijkheid van de aanwezigheid van een optimaal privacy bewustzijn in de hele keten worden verminderd.

*Privacy-Enhancing Technologies worden gedefinieerd als een samenhangend geheel van ICT maatregelen die de persoonlijke levenssfeer beschermen door het elimineren of verminderen van persoonsgegevens of het voorkomen van onnodige dan wel ongewenste verwerking van persoonsgegevens, een en ander zonder verlies van de functionaliteit van het informatiesysteem.*<sup>43</sup>

Daarbij gaat het bijvoorbeeld om zaken als toegangsbeveiliging, het technische afschermen en beperken van het aantal personen met toegang tot persoonsgegevens. Door het nemen van dergelijke

---

<sup>43</sup> Artikel 13 WBP

technische maatregelen kan het beveiligingsniveau beter worden gegarandeerd en is de toegangsbeveiliging minder afhankelijk van het correct functioneren en uitvoeren van beveiligingsmaatregelen op medewerkersniveau in de organisatie. Ook het geautomatiseerd handhaven van het privacy-beleid is een toepassing van *Privacy-Enhancing Technologies*. Door de invoering van een privacymanagementsysteem kan rule-based het privacy-beleid worden ondersteund en kunnen privacy-audits worden gefaciliteerd. Deze laatste kunnen door de verantwoordelijke of door het CBP worden ingesteld om het niveau van de privacybescherming in de coöperatief rijden keten te controleren.

#### *Scheiding van gegevens*

Een belangrijke toepassing van *Privacy-Enhancing Technologies* in het geval van coöperatief rijden is het scheiden van gegevens tijdens het verzamelingsproces. Daardoor zijn de locatiegegevens niet meer rechtstreeks aan de persoon te koppelen en wordt het moeilijker om de persoon door middel van zijn locatiegegevens te volgen. Binnen coöperatief rijden valt daaronder bijvoorbeeld het scheiden van locatiegegevens en persoonsgegevens door middel van pseudonimisering. Door bovendien te converteren van het ene pseudoniem naar een volgend pseudoniem binnen een beperkte tijd wordt het volgen van het voertuig verder bemoeilijkt. Een en ander is wel afhankelijk van de verkeersdichtheid, in de stad is een auto bijvoorbeeld moeilijker te volgen dan in plattelandsgebieden. In deze gebieden kan de pseudonimisering worden aangevuld met het verwijderen van de kop en de staart van de geregistreerde rit, zodat geen herleidbare patronen kunnen worden getraceerd. Anders dan bij pseudonimisering wordt hier een deel van de aan de persoon gekoppelde locatiegegevens gewist.

Om er zeker van te zijn dat het berichten verkeer van en naar het voertuig binnen het coöperatief rijden juridisch correct verloopt zal gebruik worden gemaakt van certificaten voor de authenticatie van de berichten. Deze certificaten zullen worden betrokken van een *Certification Authority*, die een onafhankelijke rol speelt ten aanzien van coöperatief rijden (*Trusted Third Party*). In een later stadium zullen de locatiegegevens zo snel mogelijk moeten worden geanonimiseerd, dat wil zeggen dat zij onomkeerbaar worden losgekoppeld van de identificerende gegevens voor hergebruik voor verkeersstatistiek<sup>44</sup>.

#### *Privacy-Ensuring Technologies*

Vanuit het perspectief van de betrokkene en de verantwoordelijke is een optimale bescherming van de persoonsgegevens gediend met *Privacy Enhancing Technologies* die in staat zijn om de verwerking zoveel mogelijk onafhankelijk te maken van menselijke tussenkomst en door middel van de techniek zelf de verwerking van persoonsgegevens in de hele keten in goede banen leiden. Dergelijke *Privacy-Ensuring Technologies*<sup>45</sup> zouden het voor de verantwoordelijke gemakkelijker moeten maken om inhoud te geven aan zijn verantwoordelijkheid. Te denken valt bijvoorbeeld aan een scheiding tussen inhoudelijke en persoonsgegevens gedurende het verwerkingsproces of het gebruik van *secure distributed data spaces* waarmee alleen die gegevens aan de verwerker worden verstrekt die hij voor zijn deel van het verwerkingsproces nodig heeft. Deze technologie zou gedurende de verwerking in de hele keten de verwerkte gegevens kunnen beschermen tegen ongewenste verwerkingen. Gelet op de risico's in een keten met veel verschillende marktpartijen die gevoelige persoonsgegevens verwerken is het de moeite waard om in consortiumverband naar dergelijke technisch verdergaande oplossingen voor de bescherming van de privacy te zoeken.

---

<sup>45</sup> Op basis van privacy wetgeving te ontwerpen technologie die als basis kan dienen voor het waarborgen van de privacy bij ITS toepassingen.



## 2.5 Conclusies

Ten aanzien van de verwerking van persoonsgegevens in het kader van coöperatief rijden zijn een aantal voorlopige conclusies te trekken. Voorlopig omdat de techniek nog dermate in ontwikkeling is dat de inzet van *Privacy-Enhancing Technologies* een aantal drempels verder kan wegnemen. Het juridische kader ligt wel goed vast en dat kan niet anders dan de nodige spanning opleveren. Belangrijk is dan om de hoofdlijn van de bescherming van persoonsgegevens vast te houden:

- Bescherming van de persoonlijke levenssfeer is een mensenrecht, en inbreuken daarop zijn in principe niet toegestaan.
- Persoonsgegevens binnen coöperatief rijden bevatten locatiegegevens en zijn daarmee gevoelige gegevens.
- De impact van de verwerking van persoonsgegevens op papier verschilt fundamenteel van digitale gegevensverwerking vanwege de reproduceerbaarheid en de mogelijkheid van digitale gegevenskoppeling.
- Gevoelige persoonsgegevens kunnen uitsluitend worden verwerkt met uitdrukkelijke toestemming van de betrokkene.
- Gebaseerd op deze uitgangspunten en de ontwikkelingen binnen het project kunnen de volgende conclusies worden getrokken:
- Het juridisch kader lijkt vooralsnog toereikend om coöperatief rijden mogelijk te maken onder gelijktijdige bescherming van de privacy, mits hoge kwaliteits- en beveiligingsstandaarden worden gehanteerd,
- Het privacy bewustzijn bij de betrokken markt en overheidspartijen groeit, maar moet nog worden vergroot, onderhouden, en ondersteund,
- Om de complexe netwerkomgeving voldoende transparant te maken en de verantwoordelijke de mogelijkheid te bieden om accountable te zijn voor de verwerking van persoonsgegevens in de hele keten zal moeten worden gezocht naar een volgende generatie technologie die de bescherming van persoonsgegevens langs technische weg afdoende kunnen waarborgen.
- Het eventueel veronachtzamen van het privacy-aspect binnen coöperatief rijden brengt een groot afbreukrisico met zich mee, zowel politiek/bestuurlijk als commercieel. (Privacybeleid als licence to operate)

### Aanbevelingen

- Geef privacy vanaf de start een vaste plaats bij het ontwikkelen van coöperatieve systemen (*Privacy by Design*),
- Locatiegegevens zijn privacygevoelig en hebben een hoge risico-klasse. Draag daarom zorg voor hoge kwaliteits- en beveiligingsstandaarden bij verwerking en verzending,
- Voer, gelet op de complexiteit van de ketens in de markt, de bescherming van persoonsgegevens zoveel mogelijk uit door middel van *Privacy-Enhancing Technologies*.
- Bevorder de ontwikkeling van een volgende generatie *Privacy-Ensuring Technologies* om onafhankelijk van organisatiefactoren voldoende transparantie en accountability bij de verwerking van persoonsgegevens in de keten mogelijk te maken,
- Overweeg het aanstellen van een functionaris gegevensbescherming en zorg tenminste voor een goed gemeenschappelijk dataprotectiebeleid ten einde het privacybewustzijn bij de betrokken markt en overheidspartijen verder te vergroten, te onderhouden.

### 3. Aansprakelijkheid

#### 3.1 Inleiding

In het kader van de verkenning naar de juridische implicaties van coöperatief rijden kan ook een beschouwing over de aansprakelijkheid niet ontbreken. Het gaat daarbij om verschillende aansprakelijkheden van verschillende spelers, de bezitter/bestuurder van het voertuig, de producent van de technische voorzieningen ten behoeve van coöperatief rijden en de wegbeheerder op wiens weg coöperatief gereden wordt, alsmede alle organisaties die een rol spelen bij de verwerking van gegevens. Naast deze potentiële aansprakelijken, is ook de benadeelde, degene die de aansprakelijkheid inroept, een belangrijke partij. Daarbij is het van belang om te bedenken dat deze partij niet direct vertegenwoordigd is in de discussie over coöperatief rijden en aansprakelijkheid.

In dit hoofdstuk zal aansprakelijkheid worden gezien vanuit de huidige wetgeving en met het oog op de veranderingen die het coöperatief rijden met zich kan brengen. Daarbij zal gekeken worden naar de mogelijke gevolgen van coöperatief rijden onder de huidige wetgeving<sup>46</sup>. Is er sprake van invloed op de wettelijke aansprakelijkheid? En in hoeverre wijken *in-car* adviezen af van de adviezen die de wegbeheerder door middel van elektronische borden boven de weg geeft? Wat zijn de gevolgen voor toepassing van de Wet aansprakelijkheid motorrijtuigen (WAM) bij het gebruik van coöperatieve systemen die voorsnog niet rechtstreeks ingrijpen in de besturing van het voertuig, zoals bijvoorbeeld bij *'platooning'*<sup>47</sup> wel het geval is? Coöperatief rijden zoals voorzien in het project Spookfiles A-58 betreft een dienst gericht op doorstroming van het verkeer. Daarmee zal niet snel de verwachting kunnen ontstaan dat men op de adviezen kan vertrouwen in het kader van de verkeersveiligheid. De bestuurder blijft de volledige en ongedeelde controle over het voertuig houden. Veel van de hierna besproken aansprakelijkheidsissues zullen zich pas voordoen als coöperatief rijden de bestuurder bepaalde zaken uit handen neemt, zoals bijvoorbeeld een coöperatief bestuurde *Adaptieve Cruise Control*.

#### 3.2 Verschillende aansprakelijkheden

##### *ITS Action plan*

In het rapport over aansprakelijkheid in het kader van de *ITS-Action Plan* van de Europese Commissie is een aantal conclusies getrokken over de aansprakelijkheid ten opzichte van de ontwikkeling van coöperatief en verschillende fases van geautomatiseerd rijden<sup>48</sup>. Zo stelt de Commissie vast dat er geen specifiek aansprakelijkheidsregime bestaat voor ITS applicaties. Wel is van enkele vormen van aansprakelijkheid vastgesteld dat zij kunnen optreden bij het gebruik van ITS applicaties zoals coöperatief rijden. Het gaat om de volgende vormen van aansprakelijkheid:

- Contractuele aansprakelijkheid
- Product aansprakelijkheid
- Aansprakelijkheid uit onrechtmatige daad
- Aansprakelijkheid voortvloeiend uit wegenverkeersrecht.

---

<sup>46</sup> De belangrijkste regelingen zijn: Burgerlijk Wetboek boek 3 art. 15d lid 3, boek 6 art. 162, art 173, art 174, art. 196c en de Wegenverkeerswet art. 185

<sup>47</sup> Platooning is het rijden in een konvooi van voertuigen waarbij het voorste voertuig leidend is. Elk voertuig meet de afstand, de snelheid en de richting en past die aan aan het voorliggende voertuig. Alle voertuigen zijn virtueel verbonden, maar kunnen op elk moment het konvooi verlaten. Echter wanneer een voertuig in het konvooi deelneemt, dan kan de chauffeur zijn aandacht op andere zaken richten terwijl het konvooi zijn weg vervolgd. (Definitie ERTICO-Sartre project-2012)

<sup>48</sup> ITS Actionplan, Actie 5.2, Berlin, 07.12.2012

### *Geen specifiek aansprakelijkheidsregime*

Dat nog veel onduidelijkheid is over hoe de aansprakelijkheid bij coöperatief rijden zal uitpakken is niet zo verwonderlijk gelet op de grote diversiteit aan componenten en services. Die onduidelijkheid heeft meer betrekking op het toepassen van de complexe regelgeving en casuïstiek dan op de regelgeving zelf. Voor de meeste al toegepaste ITS applicaties kan worden vastgesteld dat we op basis van de huidige wetgeving en jurisprudentie goed in staat zijn om eventuele claims op een adequate manier af te handelen. Hoewel er best op onderdelen nieuwe vraagstukken zullen opduiken is de algemene indruk dat er geen sprake is van een wettelijk tekort of een ander juridisch probleem. Wel is de uitkomst van sommige aansprakelijkheidszaken waarin ITS een rol speelt moeilijk te voorspellen. Redenen daarvoor zijn volgens het EU-rapport:

- De regels kunnen verschillen per service of applicatie,
- Voor toekomstige diensten en applicaties moet de wetgeving waarschijnlijk worden aangepast,
- De harmonisatie van aansprakelijkheidsregels op Europees niveau laat nog op zich wachten,
- Voor een gebruiker zijn *disclaimers* en gebruiksvoorwaarden moeilijk te begrijpen.

De stakeholders van coöperatief rijden ervaren het gebrek aan toegesneden juridische instrumenten als een belemmering bij de het lanceren van nieuwe ITS toepassingen. Het ontbreken van een glashelder aansprakelijkheidsregime is dan ook meer een beleids- en marketingprobleem dan een juridisch tekort. In het rapport worden de volgende ITS applicaties aangemerkt als ‘aansprakelijkheidsgevoelig’:

- Verregaande vormen van geautomatiseerd rijden,
- Coöperatieve systemen en daarmee verbonden applicaties en diensten.

### *EU Verordening?*

Geautomatiseerd rijden valt buiten het bestek van dit onderzoek, maar voor coöperatief rijden met rechtstreekse ingrepen in het voertuig is gebleken dat de keten van aansprakelijkheden complex kan zijn. Het rapport gaat ervan uit dat de implementatie van coöperatief rijden pas kan plaatsvinden als de regels met betrekking tot de aansprakelijkheden van de verschillende betrokkenen met hun instemming zijn aangepast. Vanuit juridisch perspectief is het de vraag of het nodig is: het geldende recht zal in voorkomende gevallen tot een rechterlijke uitspraak leiden. Veel van de opgeworpen (juridische) problemen, zoals de authenticatie van coöperatieve berichten zijn langs technische weg, bijvoorbeeld met een PKI-infrastructuur, op te lossen.

Zo stelt het EU rapport voor om voor coöperatieve systemen vast te houden aan het algemene principe dat iedere stakeholder slechts aansprakelijk is voor het deel van de coöperatief rijden dienst waarover hij de controle heeft. Het rapport stelt tevens voor dat in een EU Verordening zal worden voorzien die voor aansprakelijkheidskwesties bij coöperatief rijden rechten en plichten vastlegt van de partijen aangaande de onderdelen van de dienst waarvoor zij verantwoordelijk zijn. Gelet op de voorwaarde dat de instemming van alle betrokken partijen hierbij noodzakelijk valt deze wetgeving, zo al mogelijk, niet op korte termijn te verwachten.

### **3.2.1 Contractuele aansprakelijkheid**

Binnen het project werken vele geselecteerde marktpartijen, en zit een aantal partijen op de bank, klaar om in te stappen. Zodra het project operationeel wordt zullen deze partijen samen moeten optrekken. Dit kan op basis van samenwerkingsovereenkomsten en serviceniveau overeenkomsten (*service level agreements*) tussen individuele partijen en consortia. In de fase waarin coöperatief rijden nog niet op eigen kracht verder kan, zou mogelijk op basis van een overeenkomst met de opdrachtgever kunnen worden geacteerd. In dat geval zal een mogelijke interferentie met de bestuurlijke aansprakelijkheid

van de opdrachtgever nader moeten worden geanalyseerd. Ook de eindgebruiker, bijvoorbeeld een automobilist op de A58, heeft een contractuele relatie met zijn coöperatief rijden dienstverlener waaruit aansprakelijkheid kan voortvloeien. Door de aard van de toepassing, namelijk als doorstromingsadvies, zal de contractuele aansprakelijkheid van de dienstverlener echter niet snel leiden tot een aansprakelijkheid jegens mogelijke slachtoffers.

### 3.2.2 Productaansprakelijkheid

Coöperatief rijden wordt vormgegeven als een dienst waardoor niet zozeer de regels voor productaansprakelijkheid van toepassing zijn als wel die voor de aansprakelijkheid ten aanzien van telecommunicatiediensten BW 3: 15d lid 3 en BW 6: 196c. Deze regeling houdt in dat de dienstverlener niet aansprakelijk is indien hij aan een aantal voorwaarden heeft voldaan. Deze voorwaarden impliceren een passieve houding ten opzichte van de informatie zoals in het geval van een telecomprovider, maar sluiten actieve dienstverlening waarbij de dienstverlener de inhoud van de berichten bepaalt, zoals bij de coöperatief rijden dienst, uit. Dit betekent dat in het geval van toegevoegde waarde diensten, zoals de coöperatief rijden dienst, de dienstverlener in beginsel aansprakelijk is voor fouten in de dienst.

Naar de aansprakelijkheid bij actieve coöperatief rijden dienstverlening - vb. *platooning*, waarbij de berichten rechtstreeks ingrijpen in het voertuig - zal nader onderzoek moeten worden gedaan.<sup>49</sup> Wel geldt de productaansprakelijkheid wellicht voor de aansprakelijkheid voor het goed functioneren van de *on-board-unit*. Het kan daarbij zowel gaan om contractuele aansprakelijkheid, in het kader van een levering aan een niet-natuurlijke persoon, als om een levering aan een natuurlijk persoon, zoals geregeld in de EG-Richtlijn 85/374 uit 1985 en EU-Richtlijn 2001/95, in Nederland verwerkt in BW afdeling 6.3.3.. Deze regeling houdt in dat de producent aansprakelijk is voor de schade die een gebrek aan zijn product veroorzaakt, ongeacht of dat gebrek door schuld van de producent is ontstaan.

### 3.2.3 Aansprakelijkheid uit onrechtmatige daad

Een ander vorm van aansprakelijkheid waarbij geen sprake is van een contractuele- of productaansprakelijkheid is die uit onrechtmatige daad<sup>50</sup>. Deze vorm van aansprakelijkheid is de gebruikelijke bij een schade tussen twee gemotoriseerde weggebruikers. Daarbij zal naast de schade ook de gedraging van de veroorzaker van de schade en de toerekenbaarheid daarvan, alsmede het causale verband tussen de gedraging en de schade moeten worden aangetoond. Onder de paragraaf aansprakelijkheid van de automobilist komen de hieruit voortvloeiende bewijsproblemen nader in beeld.

### 3.2.4 Bestuurlijke aansprakelijkheid

Als opdrachtgever van het project vindt het Ministerie van I&M er geen doekjes om dat coöperatief rijden uiteindelijk door de markt zal moeten worden gerealiseerd. Niettemin bestaat er in elke

---

<sup>49</sup> Dit onderzoek wordt in opdracht van het Ministerie van I&M gedaan door Kiliaan van Wees aan de Vrije Universiteit in Amsterdam.

<sup>50</sup> Artikel 6:162 BW

Hij die tegen een ander een onrechtmatige daad pleegt, welke hem kan worden toegerekend, is verplicht de schade die de ander dientengevolge lijdt, te vergoeden.

Als onrechtmatige daad wordt aangemerkt een inbreuk op een recht en een doen of nalaten in strijd met een wettelijke plicht of met hetgeen volgens ongeschreven recht in het maatschappelijk verkeer betaamt, een en ander behoudens de aanwezigheid van een rechtvaardigingsgrond.

Een onrechtmatige daad kan aan de dader worden toegerekend, indien zij te wijten is aan zijn schuld of aan een oorzaak welke krachtens de wet of de in het verkeer geldende opvattingen voor zijn rekening komt.

verschillende fasen op weg naar die situatie een zekere mate van bestuurlijke betrokkenheid. Hoewel deze zal afnemen als het doel, overname door de markt, gerealiseerd is, zal de publieke verantwoordelijkheid nooit geheel verdwijnen. Daar komt bij dat het project deels in ‘concurrentie’ treedt met voorzieningen die door de overheid zelf worden beheerd, zoals de verkeersinformatie die Rijkswaterstaat beschikbaar stelt via de matrix borden langs de weg. Ook de walkant-stations van het Spookfile-A58 project zullen deel gaan uitmaken van de weginfrastructuur. Rijkswaterstaat opereert daarbij vanuit zijn publieke verantwoordelijkheid als wegbeheerder, en is uit dien hoofde aansprakelijk bij falende dienstverlening op het gebied van wegbeheer. De vraag hoe de positie van de overheid zich verhoudt tot die van de deelnemende marktpartijen is niet uitgewerkt in deze rapportage en zal eventueel nader moeten worden onderzocht.

### **3.3 Aansprakelijkheid binnen coöperatief rijden**

In deze paragraaf wordt op hoofdlijnen een beeld geschetst van de aansprakelijkheden van de verschillende (groepen van) deelnemers aan coöperatief rijden. Bij de samenstelling is dankbaar gebruik gemaakt van een artikel dat Van Wees in 2010 aan het onderwerp wijdde<sup>51</sup>. In dit artikel wordt ervan uitgegaan dat de coöperatieve component rechtstreeks ingrijpt in de techniek van het voertuig. Binnen het project Spookfiles A-58 is dat nog niet het geval. Dat systeem heeft slechts ten doel door middel van snelheidsadvies te komen tot een betere doorstroming. Daarom zijn de gevolgen met betrekking tot de aansprakelijkheid vooralsnog beperkt. Achtereenvolgens komen de aansprakelijkheid van producenten/dienstverleners, wegbeheerders en automobilisten aan bod.

#### **3.3.1. Aansprakelijkheid van producenten/dienstverleners**

##### *Afwegingsvarianten*

Voor de dienstverleners die langs elektronische weg een coöperatief rijden dienst aanbieden de aansprakelijkheid voor de aangeboden dienst contractueel worden overeengekomen tussen de gebruiker en de dienstverlener. Hoe deze overeenkomsten worden ingericht zal nader moeten worden onderzocht aan de hand van de verschillende belangen die in het geding zijn. Het gaat daarbij om het collectieve belang van het beschikbaar zijn van de diensten voor de overheid, het individueel belang van het ontvangen van de dienst door de gebruiker en het verlenen van de dienst tegen een vergoeding door de dienstverlener.

Anders dan bij dienstverlening bestaat voor producenten en leveranciers een productaansprakelijkheid voor alle bij het rijden gebruikte materialen en voorzieningen. Deze aansprakelijkheid is afhankelijk van onder meer de presentatie van het product en de daaruit voortvloeiende verwachtingen bij de gebruiker. De gebruiker op zijn beurt moet bij zijn gebruik rekening houden met de aard van het product en de beperkingen die daaraan zijn verbonden. Het gaat daarbij niet om absolute normen, maar om een permanente afweging tussen de voor- en nadelen van intelligente voertuigsystemen, ook gedurende het gebruik. Wel zal de producent ervoor moeten zorgdragen dat het ingezette ADA product aan wettelijke veiligheids- en andere voertuigeisen voldoet.

De volgende afwegingsvarianten zijn in het kader van de producenten/dienstverleners aansprakelijkheid het meest relevant:

- Het verwachtingspatroon van het publiek
- De presentatie van het product/dienst
- Het redelijkerwijs te verwachten gebruik

---

<sup>51</sup> Over intelligente voertuigen, slimme wegen en aansprakelijkheid, Kiliaan van Wees (VU), Verkeersrecht artikelen 2010

- De afweging van voor- en nadelen van het systeem
- Het voldoen aan de veiligheidseisen.

Aandachtspunt bij deze indeling is dat de verschillende afwegingsvarianten, waarvan de eerste drie zijn opgenomen in artikel 6: 186 BW aangaande de productaansprakelijkheid, in de praktijk snel in elkaar overlopen en dat de afwegingen een sterk casuïstisch karakter zullen hebben.

#### *Verwachtingen*

Als het gaat om coöperatief rijden dan is in het kader van het verwachtingspatroon van belang dat medeweggebruikers niet verrast worden door het gedrag van een 'coöperatief' rijdend voertuig. Zo zal een bestuurder bij druk verkeer op in en uitvoerstroken een kortere afstand tussen voertuigen accepteren, er vanuit gaand dat alle weggebruikers zich van deze bijzondere omstandigheid bewust zijn. De bestuurder van een voertuig dat gebruikt maakt van een coöperatief rijden adviesdienst zal op zo'n moment het snelheidsadvies dat hij heeft gekregen niet kunnen volgen en zal zijn weggedrag moeten aanpassen om onnodige gevaarlijke situaties te voorkomen. Als er sprake is van een coöperatief gestuurd voertuig kan het noodzakelijk zijn dat dit voertuig als zodanig herkenbaar is voor medeweggebruikers.

#### *Presentatie*

Voor de aanbieder zelf is van groot belang hoe een voorziening wordt gepresenteerd. De presentatie bepaalt in belangrijke mate de verwachtingen van de gebruiker. Wordt de voorziening als een comfort verhogende ondersteuning gepresenteerd of als een veiligheidsvoorziening. Voor de productaansprakelijkheid kan de presentatie een wezenlijk verschil maken. In dit kader is het opvallend dat een systeem als Adaptieve Cruise Control niet als een veiligheidsverhogend systeem in de markt wordt gezet, maar als comfortsysteem, hoewel het een duidelijk veiligheidsverhogend effect heeft. De aanbieder moet ook duidelijk waarschuwen voor de risico's van een voorziening. Gebruikers hebben in de regel weinig inzicht in de werking ervan en daarom is het van belang dat de aanbieder die risico's expliciet aangeeft. Dergelijke waarschuwingen geven overigens geen vrijwaring van de aansprakelijkheid. De beste methode om problemen te voorkomen is als de aanbieder ervoor zorgdraagt dat het systeem niet **kan** worden gebruikt in omstandigheden waarin het niet goed functioneert. Een voorbeeld hiervan is dat een Cruise Control systeem dat wordt ingeschakeld om te accelereren naar een vooraf ingestelde hogere snelheid maar dat niet doet zolang het voertuig (nog) in een bocht rijdt.

Voor de coöperatief rijden dienst op basis van advies aan de bestuurder geldt hier dat de snelheids- en andere adviezen als adviezen worden gepresenteerd en dat zij de eigen verantwoordelijkheid van de bestuurder onverlet zullen laten. Dit wordt pas anders als coöperatief rijden wordt verbonden met rechtstreekse ingrepen in het voertuig, waarop de bestuurder geen of beperkt invloed kan uitoefenen.

#### *Anticipatie*

Een aanbieder moet tot op zekere hoogte rekening houden met eventueel onzorgvuldig gedrag van de gebruiker. De vraag is echter hoever deze anticipatieplicht reikt. Daarbij is vooral de inschatting van de risico's van belang, en wie het beste tot die inschatting in staat is. Daarbij speelt ook een rol dat bij nieuwe producten het moeilijker is voor de gebruiker om de risico's in te schatten dan bij voorzieningen waarmee al de nodige gebruikerservaring is opgedaan. De onderzoekspllicht naar deze risico's ligt bij de aanbieder, waarbij een afweging moet worden gemaakt tussen de vermoede

potentiele risico's en de kosten en inspanningen van een dergelijk onderzoek. Ook het aantal (potentiele) slachtoffers en de draagkracht van een aanbieder spelen daarbij een rol.

Bij het geven van adviezen kunnen vorm en inhoud van het advies in belangrijke mate de reactie van de bestuurder bepalen. De dienstverlener zal moeten anticiperen op mogelijke reacties van de bestuurder en dit aspect bij de ontwikkeling van de dienst moeten meenemen. Daartegenover staat dat de nu voorziene adviesdienst een zodanig karakter heeft - gericht op verkeersdoorstroming - dat een aansprakelijkheidsclaim bij de dienstverlener niet voor de hand ligt.

#### *Systeemeigenschappen*

Ook zal er een afweging moeten worden gemaakt ten aanzien van de voor- en nadelen van een systeem. Daarbij gaat het erom of de voordelen van het product in termen van een bijdrage aan comfort, veiligheid of milieuaspecten opwegen tegen de nadelen die het systeem heeft, bijvoorbeeld door technische beperkingen. Zo blijkt het voor een botsing-vermijdend systeem lastig om een kind van een overwaaiende kartonnen doos te onderscheiden. De noodstop die het systeem maakt kan tot een aanrijding leiden, waarbij de noodstop in het geval van een kind gerechtvaardigd zal zijn terwijl dat bij de overwaaiende kartonnen doos duidelijk anders ligt. De vraag is dan of dergelijke technische beperkingen een gebrekkig systeem opleveren. In het algemeen zullen ongewenste neveneffecten van coöperatieve systemen niet snel aanvaardbaar zijn en dus leiden tot een gebrekkig systeem. Dit is met name het geval als de bestuurder niet in staat is om de gevaren, en daarmee het veiligheidsrisico, te vermijden. Anders dan bij medicijnen, waar de bijwerkingen individueel tegen de mogelijke individuele genezing worden afgewogen is bij coöperatief rijden het slachtoffer van de gebrekkigheid van het systeem vaak een ander dan de gebruiker zelf. De tolerantie voor gebreken is dan ook zeer beperkt, waarbij voor een voorziening die beoogt is om in een noodsituatie te redden wat er te redden valt, zoals een systeem dat automatisch ingrijpt als de bestuurder de macht over het voertuig dreigt te verliezen, een grotere tolerantie zal gelden dan voor een systeem dat mede dient voor het verbeteren van het rijcomfort, zoals *Adaptive Cruise Control*.

Als het gaat om coöperatief rijden met behulp van adviezen, dan spelen de eigenschappen van de dienst en een belangrijke rol. De dienst zal op een voldoende niveau moeten zijn om de voorgespiegelde functionaliteiten te kunnen bieden. De producteigenschappen spelen alleen ten aanzien van de *on-board-unit* een rol. Voor beide zullen onder meer gebruikerstesten in de ontwikkelfase, met name ook van de *human interface*, tot een goede dienst en een goed product moeten leiden, maar in het kader van mogelijke verschuiving van de aansprakelijkheid ligt een claim bij de dienstverlener meer voor de hand dan bij de door deze ingezette *on-board-unit* fabrikant.

#### *Veiligheid*

Het is evident dat een product moet voldoen aan de wettelijk daaraan gestelde eisen en veiligheidsvoorschriften. Echter het voldoen hieraan vrijwaart de producent niet van aansprakelijkheid. Wel kan het voldoen aan de eisen een onderdeel vormen bij de beoordeling van een eventueel gebrek. In het geval van coöperatief rijden ligt het voor de hand dat veel specifieke veiligheidsnormen nog niet beschreven zullen zijn. De totstandkoming van normen voor ADAS en coöperatieve systemen kan een bijdrage leveren aan het reduceren van de aansprakelijkheidsrisico's van aanbieders. In het kader van coöperatief rijden op basis van dienstverlening is nóg minder bekend over de veiligheid. De veiligheidsrisico's zullen in de testfase moeten worden vastgesteld en gemitigeerd. In de adviesfase zal de dienst, gelet op de aard van het systeem - het bevorderen van doorstroming - niet tot een aansprakelijkheidsverschuiving leiden, mits de veiligheidsvoorschriften in acht worden genomen.



### *Diverse aanbieders*

Bij de huidige opstart van coöperatief rijden binnen Spookfiles-A58 wordt een systeem gebouwd waarin verschillende serviceproviders in verschillende consortiumverbanden samenwerken, terwijl een centrale aansprakelijke figuur ontbreekt. Daarbij is de technische complexiteit door de verknooptheid van systemen aanzienlijk. Het gevolg daarvan is dat als er iets mis gaat vele bewijs- en afbakeningsvragen zullen opkomen. Zo zal een botsingsvermijdingssysteem dat ongewenst in de remmen gaat niet als gebrekkig kunnen worden aangemerkt als het commando door een andere speler binnen de infrastructuur werd gegeven. Daarmee wordt de aansprakelijkheid verspreid over meerdere partijen en daarmee ook moeilijker eenduidig te beantwoorden. Van het coöperatief rijden systeem mag worden verwacht dat de communicatie tussen de verschillende componenten afdoende is beveiligd tegen, bijvoorbeeld, hackers. Het feit dat de oorzaak van het falen van een coöperatief systeem niet aan een partij is toe te schrijven en mogelijk zelfs buiten het systeem kan liggen leidt tot een complexe bewijspositie voor een eventueel slachtoffer. In dergelijke gevallen zal een sluitend bewijs van aansprakelijkheid niet, of alleen tegen zeer hoge kosten te leveren zijn. Als dit bewijs niet wordt geleverd, dan zal een rechter bij het strikt hanteren van de bewijsregels zelfs kunnen besluiten tot het verwerpen van de claim. Daarbij komt dat in beginsel alle partijen binnen de keten hun eigen voorwaarden kunnen vaststellen waardoor voor de gebruiker en het slachtoffer moeilijk wordt om bij de uiteindelijk aansprakelijke terecht te komen. Begeleiding van het opstellen van algemene voorwaarden vanuit de overheidsverantwoordelijkheid zou aan dit bezwaar tegemoet kunnen komen.

### *Bewijsperikelen*

Die begeleiding kan ook nodig blijken ten aanzien van de te hanteren bewijsmiddelen. Binnen de rechtspraak zal de rechter door het hanteren van bewijsvermoedens tot een betere positie voor de benadeelden kunnen komen. Maar ook dan zal bij coöperatieve systemen de ruimte om een systeemgebrek door middel van feitelijke vaststelling te bewijzen geringer zijn. Ook gebreken in voertuigexterne componenten en tussenliggend dataverkeer kunnen plausibele oorzaken zijn voor het falen van het systeem. Bovendien leidt een vermoeden van een systeemgebrek nog niet direct tot aansprakelijkheid van de aanbieder. Deze staat het vrij om het vermoeden door middel van tegenbewijs te ontkrachten. Duidelijk is dat met name de bewijsproblemen een soepel functioneren van het aansprakelijkheidsrecht bij coöperatief rijden in de weg staan.

### *Drive-data-recorder*

Een andere mogelijkheid om aan de bewijsproblematiek een einde te maken zou zijn de introductie van een *drive-data-recorder*, waarin alle gegevens omtrent het functioneren van het systeem, en het rijgedrag van de bestuurder, worden opgeslagen. Door deze voorziening te introduceren worden de gedragingen van alle betrokkenen goed vastgelegd, en daarmee de bewijsvoering aanmerkelijk vereenvoudigd. De *drive-data-recorder* zou bijvoorbeeld de laatste fase voorafgaand aan een incident kunnen registreren en vasthouden, zoals ook in de burgerluchtvaart gebruikelijk is.

Een volgende vraag die zich aandient in het kader van de bewijslastproblematiek bij coöperatief rijden is of het niet monteren van een *drive-data-recorder* ook niet tot een omkering van de bewijslast ten nadele van de producent moet leiden? Immers de aanbieder heeft de keuze om de *drive-data-recorder* wel of niet tot onderdeel van het systeem te maken.<sup>52</sup> Door een dergelijke keuze wordt het voor de aanbieder

---

<sup>52</sup> In dit kader laat zich een vergelijking trekken met de in het Duitse recht bestaande productwaarnemings- en documentatieplichten



onmogelijk het verweer te voeren dat hij geen gegevens ten behoeve van het bewijs kan leveren, hetgeen de bewijspositie van eventuele slachtoffers verslechterd. Deze situatie had hij immers kunnen vermijden, bijvoorbeeld door het aanbrengen van zo'n *drive-data-recorder*. Wel roept het introduceren daarvan vragen op over de mate waarin gegevens uit de recorder ook voor andere doeleinden kunnen worden gebruikt (zie hoofdstuk 2).

### 3.3.2 Aansprakelijkheid van de wegbeheerder

Bij de introductie van coöperatief rijden spelen de wegbeheerders een belangrijke rol. In de eerste plaats vanwege hun wettelijke verantwoordelijkheid voor het ontwerp, de aanleg en het onderhoud van wegen, maar zeker ook vanwege het feit dat coöperatieve systemen gebruik zullen maken van in de infrastructuur aangebrachte sensoren, of weggant apparatuur. Daarmee komt ook de mogelijke aansprakelijkheid van de wegbeheerder in beeld. Stel dat een plaatselijk gevaar, bijvoorbeeld gladheid, als gevolg van gebrekkige weggant apparatuur niet aan een coöperatief rijdend voertuig is doorgegeven, en het voertuig verongelukt? In zo'n geval zou een schadeclaim tegen de wegbeheerder onder omstandigheden succesvol kunnen zijn. De vraag is of dat ook het geval is zolang het advies nog slechts gericht is op doorstroming, en niet op verkeersveiligheid.

#### *Wettelijke basis*

Artikel 6:174 BW stelt dat de publieke wegbeheerder ervoor moet zorgen dat de openbare weg in goede staat verkeert en dat de wegbeheerder aansprakelijk is als de weg niet voldoet aan de eisen die men daaraan in de gegeven omstandigheden mag stellen. Onder het begrip weg vallen het weglichaam en de weguitrusting. Onder weguitrusting wordt verstaan alle voorwerpen aangebracht voor het inrichten van de weg voor verkeersgebruik, zoals vangrails, verkeersborden en -lichten. Ook weggantvoorzieningen voor coöperatief rijden kunnen worden gezien als voorwerpen aangebracht voor het inrichten van de weg voor verkeersgebruik. Daarmee vallen zij onder de risicoaansprakelijkheid van artikel 6:174 BW. Als de werking van de weggantapparatuur afhankelijk is van een op afstand geplaatst informatie-verwerkingssysteem dan rijst de vraag of dit systeem ook nog deel uitmaakt van de weguitrusting. De technische ontwikkelingen, in relatie tot de eis dat de voorziening duurzaam met de weg verenigd moet zijn, roepen in toenemende mate de vraag op naar de reikwijdte en toepasbaarheid van de bepaling. In het kader van aanstaande proeven met coöperatief rijden op de A58 in het Spookfile-project zal de wegbeheerder nog niet direct met een aansprakelijkheid voor het advies worden geconfronteerd.

#### *Weguitrusting*

Het draait bij de vaststelling van de aansprakelijkheid van de wegbeheerder om de vraag of de weguitrusting gebrekkig is of niet. Ook hier speelt de verwachting van de weggebruiker een belangrijke rol. Zo is de waarschijnlijkheid dat bepaalde gebreken doe tot ongevallen leiden zich voordoen van belang evenals de bezwaarlijkheid van de te nemen tegenmaatregelen. In het geval van informerende systemen zal van een aansprakelijkheid van de wegbeheerder niet zo snel sprake zijn, aangezien deze slechts de informatiepositie van de bestuurder verbeteren door informatie te verschaffen over mist, gladheid, stilstaande voertuigen, kruisend verkeer etc.. Daarbij kan vaak ook het proefkarakter van de voorziening worden benadrukt, waardoor de verwachtingen van de weggebruiker verder kunnen

---

(Produktbeobachtungspflicht resp. Befundssicherungspflicht). Indien later niet meer kan worden vastgesteld of een gebrek vóór of ná het in het verkeer brengen is ontstaan, kan de producent zich niet op het ontbreken van gegevens beroepen. Dit is gebaseerd op de gedachte dat de producent zich niet op een feitelijke onzekerheid mag beroepen als hij die onzekerheid zelf had kunnen vermijden door producten vooraf te testen en de bevindingen daarvan te documenteren. (Van Wees, Over intelligente voertuigen, slimme wegen en aansprakelijkheid. Verkeersrecht 2010).

worden getemperd. Bij systemen echter die zelf ingrijpen in de rijtaak of die een specifieke instructie aan de bestuurder inhouden, ligt dat anders. Ten aanzien van deze systemen mag worden verwacht dat zij naar behoren functioneren, zoals ook mag worden verwacht dat als een stoplicht op groen staat, het licht voor het kruisende verkeer op rood staat. Bij een gebrek aan een infrastructurele component is de wegbeheerder in principe aansprakelijk voor schade die daaruit voortvloeit, ongeacht zijn bekendheid met het gebrek of eventuele verwijtbaarheid. Wel dient natuurlijk het causaal verband tussen het gebrek en de schade te worden aangetoond. Of dat het geval is zal afhangen van de mate van gevaar die het gebrek teweeg heeft gebracht en van de mate waarin de bestuurder zijn gedrag heeft kunnen aanpassen.

#### *Voorbeeld*

*Neem het voorbeeld van een zogenoemde intelligente snelheidsbegrenzer (ISA), waarbij vanuit de infrastructuur 'elektronisch' de maximumsnelheid wordt opgelegd. Wanneer deze maximum snelheid niet wordt opgelegd aan het voertuig als gevolg van een gebrek in de infrastructurele component (en het voertuig dus te hard rijdt), en ontstaat korte tijd later een ongeval omdat een ander voertuig de snelheid van het ISA-voertuig (terecht) onderschatte, dan lijkt toch dat spoedig geoordeeld kan worden of er een causaal verband tussen het gebrek en het ongeval is of dat dit verband niet bestaat. Of er is sprake van (gedeeltelijke) eigen schuld, ervan uitgaande dat snelheidsborden waren blijven staan en de bestuurder dus had kunnen weten dat er kennelijk sprake was van een gebrek en zijn rijgedrag daaraan had kunnen en moeten aanpassen.*

#### *Geautomatiseerde infrastructuur*

Als een gebrek in de infrastructurele component echter leidt tot een situatie waarin de bestuurder geen verwijt van zijn reactie kan worden gemaakt, dan is er sprake van een causaal verband en zal de wegbeheerder aansprakelijk gesteld kunnen worden. Bij coöperatief rijden door middel van advies zal deze situatie zich niet zo snel voordoen. Ook de bekendheid met het mogelijke gevaar speelt daarbij een rol. Bij coöperatieve systemen zal er met name in de beginfase een grotere zorgplicht rusten op de wegbeheerder omdat de bekendheid met het systeem bij de weggebruiker nog beperkt is. In het algemeen zal voortschrijding van de automatisering effect hebben op de gerechtvaardigde verwachting ten aanzien van de weg. Aan een snelweg zullen hogere eisen mogen worden gesteld dan aan een B-weg. Bij een geautomatiseerde snelweg zou men kunnen verwachten dat geen enkel risico meer voor rekening van de weggebruiker komt, voor zover hem de rijtaak uit handen is genomen.

#### *Zorgplicht*

Volgens de geldende wetgeving kan de wegbeheerder niet aansprakelijk worden gesteld voor schade die het gevolg is van oorzaken van buitenaf, zoals hacking of blikseminslag. Dat roept wel meteen de vraag op in hoeverre de wegbeheerder verantwoordelijk is voor de hacking- en blikseminslag bestendigheid van de gebruikte apparatuur. Voldoet deze nog wel aan de eisen die men hieraan redelijkerwijs mag stellen? Het zal duidelijk zijn dat op voorhand geen eenduidig antwoord te geven is, maar dat een voortdurende toetsing van de zorgvuldigheid bij het introduceren van coöperatieve systemen noodzakelijk is.

### **3.3.1 Aansprakelijkheid van de automobilist**

Zolang er geen sprake is van een rechtstreeks ingrijpend coöperatief systeem en de automobilist nog achter het stuur plaats neemt met als doel om, al of niet geassisteerd door ondersteunende voertuigsystemen, de auto zelf te besturen is hij/zij ook primair aansprakelijk voor de gedragingen van de auto, en dus ook voor de schade die daaruit eventueel voortvloeit. De vraag is welke invloed de introductie van coöperatief rijden heeft op dit uitgangspunt. Enerzijds kan men stellen dat de

aansprakelijkheid van de bestuurder zou kunnen afnemen in die zin dat bij het falen van het ondersteunende ADA systeem een deel van de verantwoordelijkheid bij het falende systeem kan komen te liggen. Anderzijds verbetert het gebruik van ondersteunende systemen de informatiepositie van de bestuurder waardoor hogere eisen gesteld zouden kunnen worden aan zijn of haar performance. Welke aansprakelijkheid is op de bestuurder van toepassing?

#### *Wettelijke basis*

De wet kent drie mogelijkheden voor slachtoffers om een bestuurder van een motorrijtuig aansprakelijk te stellen:

- Artikel 185 van de Wegenverkeerswet, ingeval het slachtoffer niet zelf ook een motorvoertuig bestuurde.
- Artikel 6:162 van het Burgerlijk Wetboek, ingeval het een aanrijding tussen motorvoertuigen betreft.
- Artikel 6:173 van het Burgerlijk Wetboek, ingeval het een aanrijding tussen motorvoertuigen betreft waarvan de oorzaak ligt in het niet functioneren van de ADA voorziening, en het motorvoertuig als een gebrekkige zaak moet worden aangemerkt. In dat geval zal ook de leverancier van de ADA voorziening aansprakelijk kunnen worden gesteld.

#### *Motorvoertuigen en andere weggebruikers*

Om te beginnen is art 185 WVV van toepassing waarin is vervat dat bij een schade aangericht door een motorvoertuig aan een niet gemotoriseerde weggebruiker. Art 185 WVV stelt dat de eigenaar/houder aansprakelijk is voor de door zijn motorvoertuig aangerichte schade, tenzij er sprake is van overmacht. Overmacht moet niet snel worden aangenomen. Het gebruik van ADA bijvoorbeeld binnen coöperatief rijden is zoals reeds aangegeven geen reden om de aansprakelijkheid weg te nemen. Integendeel, het kan goed zijn dat door het gebruik van ADA een betere beheersing van de omstandigheden van de bestuurder mocht worden verwacht dan zonder ADA het geval zou zijn geweest. Zelfs als een gebrek aan de ADA het ongeval zou hebben veroorzaakt, dan nog zou de keuze om ADA te gebruiken in beginsel de aansprakelijkheid van de eigenaar/bezitter niet verminderd. Slechts in het geval hij kan bewijzen dat een slecht functionerende ADA de enige oorzaak van het ongeval was, en de bestuurder geen enkel verwijt treft, zal de aansprakelijkheid van de bestuurder worden beperkt.

#### *Motorvoertuigen en andere motorvoertuigen*

Bij schade door een motorvoertuig aangebracht aan een andere motorvoertuig is artikel 6:162 BW van toepassing, de bestuurder is in dat geval aansprakelijk wegens onrechtmatige daad. Dit houdt in dat hij aansprakelijk is voor de schade die te wijten is aan de schuld van de automobilist, of aan een oorzaak die op grond van de wet of de in het verkeer geldende opvattingen voor zijn rekening komt. Daarbij staat het rijgedrag van de schade toebrengende bestuurder van het motorvoertuig centraal. Uitgangspunt bij de beoordeling daarvan is de ‘perfecte’ chauffeur, zeker als het slachtoffer geen enkel verwijt valt te maken.

Deze zeer strikte maatstaf laat weinig ruimte voor een beroep op niet toerekenbaarheid vanwege het gebruik van ADAS. Het gebruik van ADAS kan ook geen verminderde aandacht van de bestuurder rechtvaardigen, met name niet wanneer een dergelijk ondersteunend systeem bepaalde beperkingen kent.

#### *Voorbeeld:*

*Twee met coöperatiefsnelheidsadvies systeem uitgeruste auto's rijden op een snelweg op korte afstand van elkaar. Door een systeemfout krijgt de bestuurder in het voorste voertuig het advies hard te remmen, terwijl dit advies in het tweede voertuig*

*niet wordt gegeven, met een kop-staart botsing tot gevolg. Gelet op het feit dat dergelijke adviezen niet onfeilbaar zijn wordt aangenomen dat de bestuurder van de tweede auto de botsing had kunnen vermijden door met onvolkomenheden in de coöperatieve systeem rekening te houden. Zijn aansprakelijk blijft in stand. Dat zou anders zijn als het om elektronisch gekoppelde voertuigen zou gaan. In dat geval zou de bestuurder van het tweede voertuig het ongeluk niet hebben kunnen vermijden. In dat geval zou de aansprakelijkheid geheel of gedeeltelijk beperkt kunnen zijn.*

#### *Technisch gebrek*

Tenslotte is het ook mogelijk dat het ongeval en de daaruit voortvloeiende schade het gevolg is van een gebrek aan de het motorvoertuig of aan de gebruikte ADAS. Ook in dat geval is de bezitter van het voertuig aansprakelijk, echter niet vanwege zijn rijgedrag, maar vanwege het feit dat de bezitter gebruik heeft gemaakt van een zaak waarvan bekend is dat die bij niet-functioneren groot gevaar oplevert. Of het defect zelf bekend was doet daarbij niet ter zake. Een externe oorzaak neemt in beginsel de aansprakelijkheid niet weg.

Deze aansprakelijkheid op grond van Art 6:173 BW is echter op twee manieren beperkt, namelijk als:

- Er geen sprake is van onrechtmatige daad van de bezitter
- De gebrekkige zaak als gebrekkig product kan worden beschouwd.

Het ontbreken van een onrechtmatige daad kan bijvoorbeeld het gevolg zijn van overmacht of van buiten komende omstandigheden. Ook als er sprake is van een gebrekkig product dan is de bezitter niet aansprakelijk. De aansprakelijkheid van de fabrikant wordt in dat geval de hoofdregel.

Voor het slachtoffer betekent dit hij in dat geval mogelijk zowel de bezitter als de fabrikant moet aanspreken. In het geval de fabrikant de claim met succes verwerpt, dan kan met die uitspraak in de hand vervolgens de bezitter worden aangesproken. De vraag is of in het geval van coöperatieve systemen ook niet de wegkant- en back-office serviceproviders kunnen worden aangesproken. Bij coöperatieve diensten is namelijk niet op voorhand duidelijk dat de gebrekkigheid van het ADAS zich in het voertuig bevindt. Bovendien geldt productaansprakelijkheid niet voor diensten. Dit kan tot complexe procedures met betrekking tot de aansprakelijkheid leiden en verdient aandacht bij het opzetten van samengestelde coöperatief rijden diensten, bijvoorbeeld in de vorm van gemeenschappelijke leveringsvoorwaarden.

#### *Verhoogde aansprakelijkheid*

Een ander aspect dat bij het gebruik van ADAS een rol speelt is in hoeverre het gebruik van dergelijke systemen de aansprakelijkheid van de chauffeur vergroot. Doordat de chauffeur beter geïnformeerd is over de situatie op de weg, bijvoorbeeld door signalering van gladheid, of naderende file etc. heeft hij ook meer mogelijkheden de juiste keuzes te maken. Een beroep op onwetendheid van de gladheid of file zal moeilijker worden. Het probleem in deze situaties zit in de bewijslast. Aangetoond zal moeten worden dat het systeem uitstond, of dat de waarschuwing door het systeem is genegeerd. Anders dan bij systemen die adviseren is bij systemen die automatisch ingrijpen in de rijtaak, bijvoorbeeld om een aanrijding te voorkomen, het besluit van de bestuurder om het systeem wel of niet te activeren van invloed op de aansprakelijkheid. Het niet aanzetten van het systeem zou in dat geval tot een grotere aansprakelijkheid kunnen leiden. Een drive-data-recorder zou een goede manier kunnen zijn om het bewijsprobleem in dezen aan te pakken.

### *Balans nodig*

Binnen het kader van coöperatief rijden met rechtstreekse ingrepen in het voertuig zal een balans gevonden moeten worden tussen enerzijds de veranderingen die coöperatief rijden met zich brengt ten aanzien van de aansprakelijkheid van de bezitter/eigenaar van het voertuig en de eventuele (mede) aansprakelijke leveranciers en wegbeheerders, en anderzijds de bescherming van de slachtoffers van ongevallen waarbij coöperatief rijdende motorvoertuigen zijn betrokken.

## **3.4 Aansprakelijkheidsverdeling Spookfiles A-58**

### *Verantwoordelijkheid bestuurder*

Uitgangspunt is en blijft dus dat de voertuig-verantwoordelijke aansprakelijk is voor schade die met (door) het voertuig is aangericht. Als voertuig-verantwoordelijke is primair aan te wijzen de bestuurder van het voertuig. Hij/zij kan immers de meeste invloed uitoefenen op het (weg)gedrag van het voertuig. Daarnaast spelen zaken als de interactie tussen weggebruikers en ook omstandigheden, zoals overzichtelijkheid van de weg en weersinvloeden, een belangrijke rol. Het eenduidig verantwoordelijk stellen van de bestuurder van het voertuig in het geval van een aanrijding is in de fase van een snelheidsadvies gericht op doorstroming goed mogelijk. Dat zal pas veranderen als het coöperatieve systeem rechtstreeks ingrijpt in het voertuig.

### *Hoge schadebedragen*

Gelet op de massa van motorvoertuigen, gekoppeld aan de snelheid waarmee zij kunnen voortbewegen, kan de schade veroorzaakt bij een aanrijding zeer aanzienlijk zijn. Dat kan het geval zijn bij zuiver materiele schade, aan andere voertuigen of zaken langs de weg, maar speelt des te meer bij fysieke schade aan personen. De kosten van medische behandeling, revalidatie inkomensverlies en dergelijke lopen snel op tot voor individuele weggebruikers onmogelijk te vergoeden bedragen.

### *Verplichte verzekering*

Om te voorkomen dat slachtoffers van een aanrijding met een motorvoertuig om die reden onvoldoende voor hun schade gecompenseerd kunnen worden, is een verzekering voor deze aansprakelijkheid wettelijk verplicht gesteld. Deze verzekering, geregeld in de Wet Aansprakelijkheid Motorvoertuigen (WAM), moet worden afgesloten door de eigenaar, de houder, de gebruiker of de bestuurder van het voertuig. Hier wordt al direct duidelijk dat de prominente positie van de bestuurder in dezen moet worden gerelativeerd. De verzekering wordt als het ware gekoppeld aan het voertuig, en geabstraheerd van de bestuurder. In plaats daarvan komt de verzekerde, die verantwoordelijk is voor het afsluiten van de verzekering ten einde de risico's van ongevallen af te dekken, niet alleen voor zich zelf, maar voor alle gebruikers van het voertuig.

### *Verantwoordelijkheid bezitter/houder*

Veranderd door deze verzekering op het object, de auto, ook de mate van verantwoordelijkheid van de verschillende betrokkenen? En welke verantwoordelijkheid is dat dan. De bestuurder van het voertuig kan in beginsel verantwoordelijk worden gehouden voor zijn eigen rijgedrag en voor het hebben van een WA verzekering. Niettemin hoeft hij niet degene te zijn die de verzekering afsluit. Daarvoor ligt de eigenaar of houder van het voertuig meer voor de hand. Het object van de verzekering is tenslotte het voertuig en niet de bestuurder. De eigenaar, of houder, heeft het eerste belang bij het verzekerd zijn van het voertuig dat de openbare weg opgaat. Vanaf dat moment kunnen immers schades ontstaan, ongeacht wie de bestuurder is.

### *Verantwoordelijkheid in coöperatief rijden*

Als de bestuurder geassisteerd wordt door een bijvoorbeeld een interactief navigatiesysteem, dan zal dat niet afdoen aan zijn verantwoordelijk voor de gedragingen van het voertuig. Ook niet als de informatie in het navigatiesysteem verzorgd wordt door een externe service provider.

Datzelfde geldt als de bestuurder wordt geassisteerd door elektronica in de auto zelf. Als een ingestelde adaptieve cruise control wordt gebruikt dan mag daarvan verwacht worden dat deze zijn werk naar behoren doet. En mocht er door een noodstop van de voorganger toch een aanrijding plaatsvinden, bijvoorbeeld omdat de Adaptieve Cruise Control niet voldoende afstand hield, dan doet dat niets af aan de aansprakelijkheid van het 'voertuig'. In de eerste plaats zal daarbij worden gekeken naar de bestuurder, en vervolgens naar degene die gehouden zijn de aansprakelijkheidsverzekering af te sluiten, naast de bestuurder de houder, de eigenaar en de gebruiker. Voor het slachtoffer maakt dit allemaal geen verschil. Of het geld uiteindelijk komt van de bestuurder, of op grond van productaansprakelijkheid van de fabrikant, of van de WA verzekering van het voertuig, deze laatste is verplicht te betalen en kan het onterecht betaalde bedrag vervolgens bij de andere verantwoordelijken terughalen.

### *Positie slachtoffer*

Het uitgangspunt is helder, als een voertuig schade aanricht en aansprakelijkheid wordt vastgesteld, dan is deze schade verzekerd via de verplichte aansprakelijkheidsverzekering, ongeacht de mate van assistentie bij het rijden. Wel zou de verzekeringsmaatschappij een claim kunnen krijgen op de verzekerde als daarvoor een juridische grond bestaat, bijvoorbeeld rijden onder invloed, of rijden met behulp van een niet-gecertificeerd coöperatief systeem. Maar ook als er wel sprake is van een gecertificeerd systeem, maar dit niet naar behoren blijkt te werken, dan laat de productaansprakelijkheid van de fabrikant de rechten van het slachtoffer ten aanzien van de WA verzekering van het voertuig dat de schade heeft veroorzaakt ongemoeid.

### *Relatie verzekerde/verzekeraar*

In de schaderelatie met het slachtoffer is de wet behoorlijk eenduidig. Dit ligt anders voor de relatie tussen de verzekeraar en de verzekerde houder of eigenaar van het voertuig. Het is heel wel denkbaar dat de voorwaarden van de verplichte polis onder invloed van de ontwikkelingen op het gebied coöperatief rijden zullen worden aangepast. Te denken valt daarbij aan specifieke premies voor voertuigen die deelnemen aan coöperatief rijden, en aan eisen die de verzekeraar zal stellen bijvoorbeeld in de vorm van invloed op de voorwaarden van de dienstverlener, aan certificering aan de verzekerde auto en aan de gebruikte technische apparatuur ten behoeve van coöperatief rijden.

### 3.5 Conclusies

Voorzichtige conclusie is dat vooralsnog de aansprakelijkheid van een coöperatief rijdende auto geen onoverkomelijke issues met zich brengt voor zover het systeem adviserend en ondersteunend is en gericht op doorstroming van het verkeer. Wel zal de beoordeling van de bestuurder kunnen veranderen in geval van schade als de bestuurder gebruikt maakt van een ondersteunend systeem. Ook zal de relatie tussen de verzekerde en de verzekeraar kunnen veranderen, bijvoorbeeld in de voorwaarden of bij de premiestelling.

Bij coöperatieve systemen die rechtstreeks ingrijpen in het voertuig wordt de balans tussen acceptatie van onvolkomenheden bij coöperatief rijden en de bescherming van potentiële slachtoffers een aandachtspunt. Problematisch voor het slachtoffer in dit verband is de kanalisatie van de claim door het slachtoffer.<sup>53</sup> Hierbij moet een slachtoffer naast de bestuurder ook de producent aanspreken voor het geval de bestuurder niets te verwijten valt en er sprake is van een systeemfout. Door de voorgestelde marktwerking bij coöperatieve systemen kan dit een onevenredig zware klus worden, aangezien deze ingewikkelde samengestelde diensten tot veel meer potentieel aansprakelijken kunnen leiden. Voorkomen moet worden dat het slachtoffer de dupe wordt en zijn positie verder verslechterd. Veel zal in dit verband afhangen van de ontwikkeling in de rechtspraak, hoe legt de rechter de bewijslastverdeling, en hoe gaat hij om met de interpretatie van de zorgvuldigheidsnorm.

Van Wees geeft in zijn artikel uit 2010 een aantal oplossingsrichtingen aan voor met name de bewijsproblematiek bij coöperatief rijden:

- Het onderbrengen van de M2M aansprakelijkheid onder de WAM verzekering van de bezitter,
- Het installeren van een *drive-data-recorder* in de auto bij toepassing van coöperatieve systemen,
- Het verleggen van de bewijslast naar automobilist of het wegnemen van de kanalisatie naar producent.
- Het opzetten van een stelsel van verkeersverzekeringen, waarmee verkeersongevallen uit de sfeer van het aansprakelijkheidsrecht raken.

#### *Aanbevelingen*

Start een brede discussie over de bewijsproblematiek met alle belanghebbenden, zowel voor het creëren van bewustwording van de problematiek als voor het creëren van draagvlak voor een mogelijke oplossingsrichting.

Betrek de verzekeraars en de vlooteigenaren op korte termijn bij de praktijkproeven om ervoor te zorgen dat eventuele juridische discussies tijdig worden gesignaleerd en gevoerd.

---

<sup>53</sup> BW 6:173 lid 2.



## 4. Data-eigenaarschap

### 4.1 Inleiding

Een vraag die in het kader van het verwerken van data binnen coöperatief rijden onvermijdelijk opkomt is: wie is de eigenaar van de data? Het is opvallend hoeveel partijen zichzelf als eigenaar van de aan hen toevertrouwde gegevens beschouwen. Zonder zich overigens alle consequenties daarvan te realiseren. Data eigenaarschap is onder meer relevant bij het bepalen van de verantwoordelijkheid voor de data-kwaliteit. Aan het eigenaarschap hangen dan ook rechten en plichten vast met betrekking tot het beschikbaar stellen van deze data. Dat beschikbaar stellen brengt doorgaans kosten met zich mee, zodat data eigenaarschap ook financiële gevolgen heeft. Daarmee komen ook commerciële belangen in beeld als reden voor het claimen van juridisch eigendom van data.

Ook de bescherming van de privacy kan aanleiding geven tot het claimen van data-eigenaarschap. En steeds komt dezelfde vraag terug bij het verzamelen en verwerken van data: wie is de eigenaar van de data? Zonder een helder antwoord op die vraag lijken partijen in een data-uitwisselingssituatie zich ongemakkelijk en onzeker te voelen. In dit hoofdstuk zal nader worden ingegaan op data-eigenaarschap. Daarbij zal om te beginnen de vanuit de informatiekunde worden gekeken naar de elementen die bij het bepalen van data-eigenaarschap een rol spelen. Vervolgens zullen deze elementen worden aangelegd tegen de juridische variant van eigenaarschap, eigendom.

Over de juridische aspecten van data-eigenaarschap is het meest geschreven in de relatie tot medische gegevens. In de Verenigde Staten is vooral de tegenstelling tussen de privacy van de patiënt enerzijds en het belang van wetenschappelijk onderzoek ten behoeve van de volksgezondheid als geheel anderzijds bepalend voor de discussie<sup>54</sup>. Op deze discussie en de juridisch relevante elementen zal nader worden ingegaan. Dichter bij huis is een interessante analyse gemaakt ten behoeve van de totstandkoming van het elektronisch patiëntendossier<sup>55</sup>. Hierin wordt de Nederlandse juridische positie van medische gegevens nader toegelicht. Aan de hand hiervan wordt de omgang met gegevens en het data-eigenaarschap binnen een concept als coöperatief rijden besproken.

#### *Data-eigenaarschap als concept*

De binnen de informatisering gebruikte term data-eigenaarschap heeft een andere invulling dan het juridische concept eigendom. Uit de literatuur valt vooral een dienende functie van data-eigenaarschap te destilleren. Eigenaarschap als verantwoordelijkheid voor de data, als houder, kwaliteitsbewaker en verzorger van de data (stewardship). Ook is de eigenaar verantwoordelijk voor de integriteit en daarmee ook voor de beveiliging van de data. In die zin lijkt data eigenaarschap eerder een last, terwijl volle eigendom in juridische zin juist een lust suggereert. Niettemin doemt het beeld van juridisch eigendom onherroepelijk op bij de discussie over het eigenaarschap van de data, namelijk als het hebben van volledige zeggenschap over de data, met uitsluiting van dat recht voor anderen. Afgezien van het feit dat een dergelijk absoluut eigendomsrecht ook juridisch niet bestaat is bij de kamerbehandeling van het wetsvoorstel voor het Nieuw Burgerlijk Wetboek door de Minister van Justitie vastgesteld dat eigendom alleen betrekking kan hebben op stoffelijke objecten. Data behoren niet tot deze categorie. Dat laat zich misschien nog het beste illustreren door het feit dat de wettelijke juridische hoofdregel is dat degene die een stoffelijk object in zijn bezit heeft in principe als eigenaar moet worden aangemerkt. Voor data is het overduidelijk dat dit principe onverenigbaar is met de gemakkelijke

---

<sup>54</sup> Much Ado About Data Ownership, Evans, Harvard Journal of Law & Technology 2011.

<sup>55</sup> Van Wie Is Het Dossier, Ekker, Nictiz 2010.



reproduceerbaarheid en de verspreiding van data. Daarbij komen meerdere bezitters van dezelfde data voor, zodat een juridisch eigendomsrecht niet zinvol valt op te eisen. Wat dan wel? Data zijn dan weliswaar niet vatbaar voor juridische eigendom, dat betekent niet dat er geen plichten en rechten en geen plicht- en rechthebbenden ten aanzien van de data zijn.

#### *Data rechten*

Op data zijn talloze omvangrijke en minder omvangrijke rechten mogelijk. In specifieke situaties is dit recht benoemd en geregeld, zoals in het auteursrecht en het databanken recht. Maar ook als er geen sprake is van deze rechten kan bijvoorbeeld degene die de data genereert rechten op de data doen gelden. Zodra de data uit meerdere bronnen bij elkaar worden gebracht zullen ook de rechten van die bronnen gerespecteerd moeten worden. Bij coöperatief rijden valt te denken aan de klant, als leverancier van zijn persoons- en reisgegevens, waaronder locatiegegevens. Deze laatste kan hij overigens alleen leveren met behulp van anderen, i.c. de service provider die de meetapparatuur gebruikt om deze locatiegegevens te genereren en de wegkantapparatuur-beheerder die een deel van het transport van de data verzorgt. Als verzamelaars en bewerkers van de data hebben de service providers een belangrijke verantwoordelijkheid (verplichting) naar de leverancier van die data, de klant, en naar de afnemer van de data in de vorm van informatie, zoals de klant, de service provider zelf, dienstverleningspartners, de wegbeheerder, en eventueel andere betrokkenen. Deze groepen hebben niet zozeer eigenaarschap van de data, als wel kunnen zij gebruiksrechten hebben op bepaalde delen ervan. Gebruiksrechten zijn bijvoorbeeld het hebben van toegang, het creëren van nieuwe data met de bron data, het standaardiseren van de data of het modifieren ervan. Deze rechten en plichten en de daarmee gepaard gaande rechtsverhoudingen zullen moeten worden vastgelegd in de onderlinge overeenkomsten die de betrokkenen met elkaar sluiten.

Samenvattend kan worden gesteld dat de termen data eigenaarschap en juridische data rechten uit verschillende ecosystemen afkomstig zijn en zich slecht laten vergelijken. Toch lijkt er een verband tussen beide in die zin dat een juridisch recht op data veelal gepaard zal gaan aan een verantwoordelijkheid (plicht) om deze data goed te onderhouden zodat andere rechthebbende kunnen vertrouwen op kwalitatief goede data voor hun deel van het systeem.

#### *Coöperatief rijden*

De vraag wie de eigenaar is van data die in het kader van coöperatief rijden worden gegenereerd en verwerkt is niet eenduidig te beantwoorden. Er zijn namelijk veel verschillende partijen betrokken bij de gegevensverwerking, die allemaal hun eigen relatie tot de data hebben. Wel kan in het kader van coöperatief rijden worden vastgesteld dat slechts een aantal van de mogelijke partijen rechten op de data kunnen doen gelden. Dit zijn in eerste instantie de serviceprovider die met alle andere partijen overeenkomsten sluit over de dienstverlening en de omgang met de daarvoor noodzakelijke data. Daarbij is de vrijheid om de rechten over de partijen te verdelen in beginsel groot. Wel is één partij in het bijzonder beschermd door wet- en regelgeving; namelijk de klant/gebruiker van de coöperatief rijden dienst. Deze heeft de wettelijke bescherming van zijn persoonsgegevens, die in acht moet worden genomen, en daarnaast de bescherming als consument van de geleverde dienst. Bij beide vormen van bescherming kunnen de voor de coöperatief rijden dienst verzamelde en verwerkte data een rol spelen.

## 4.2 Data-eigenaarschap

Zoals gezegd is de discussie over data-eigenaarschap met name gevoerd in de Verenigde Staten, en spitst deze zich toe op medische gegevens waarbij de strijd om het eigenaarschap gaat tussen de patiënt en diens privacybelangen aan de ene kant en de wetenschappelijke onderzoekers, zowel publiek als privaat, als hoeders van het algemeen onderzoeksbelang, en de commerciële belangen van de farmaceutische industrie aan de andere kant. Hoewel dit veld op een aantal punten duidelijk afwijkt van de situatie bij coöperatief rijden in Nederland en Europa kunnen de overzeese analyses een bijdrage leveren aan de begripsvorming in het kader van deze rapportage. In de bijlage is een samenvatting opgenomen van de discussie zoals die in de Verenigde Staten is gevoerd in de aanloop naar een wetsvoorstel waarbij de omgang met medische gegevens wordt geregeld.

### *Elementen data-eigenaarschap*

Voor een analyse van elementen die een rol spelen bij data-eigenaarschap kunnen we terecht bij een uitgave van het ORI<sup>56</sup>, het Office for Research Integrity (ORI) in Chicago. In de uitgave, gedaan in het kader van het bewaken van de integriteit van met name wetenschappelijk onderzoek, wordt een goed onderbouwd overzicht gegeven van de implicaties van data-eigenaarschap op verschillende niveaus: conceptueel, juridisch en economisch. Daarbij wordt er om te beginnen van uitgegaan dat data-eigenaarschap is opgebouwd uit twee componenten: bezit en verantwoordelijkheid. Eigenaarschap impliceert in die visie bevoegdheid, en verantwoord beheer. Deze definitie van eigenaarschap houdt niet alleen toegang in tot de data en de mogelijkheid tot creatie, aanpassing, verzending en exploitatie van data, maar met name ook het recht om deze privileges aan anderen over te dragen.

In deze opvatting<sup>57</sup> van Loshin gaat het bij eigenaarschap om dat er altijd iemand moet instaan voor de data-kwaliteit, inclusief de bijbehorende bevoegdheden en beheermogelijkheden. Daarbij komt dat data eigenaarschap voor hem inhoudt dat deze bevoegdheden door de eigenaar kunnen worden overgedragen.

Voor Scofield (1998)<sup>58</sup> staat minder de bevoegdheid, maar meer de verantwoordelijkheid voor de data centraal. Om dit te benadrukken suggereert hij dan ook om de term 'ownership' te vervangen door 'stewardship'.

Garner (1999)<sup>59</sup>, zoekt aansluiting bij het intellectuele eigendomsrecht over data, zoals in de wet reeds is opgenomen en beschermd. Daarbij stelt hij echter niet zozeer de juridische als wel de economische kant van het data-eigenaarschap centraal, data als waarde.

### *Eigenaarschap en wetenschappelijke data*

Als het gaat om wetenschappelijke data stelt het *Panel on Scientific Responsibility and the Conduct of Research*,<sup>60</sup> in 1992 vast dat het delen van data een aantal algemene maatschappelijke voordelen biedt, en in het bijzonder de integriteit van wetenschappelijke data dient.

---

<sup>56</sup> , Northwestern University Chicago, Illinois

<sup>57</sup> Loshin, (2002). Knowledge Integrity: Data Ownership (online 2004)

<sup>58</sup> Scofield, M. (1998) Issues of data-ownership (online 2004)

<sup>59</sup> Garner, (1999) Black's Law Dictionary, 7th edition. West Group

<sup>60</sup> Panel on Scientific Responsibility and the Conduct of Research, 1992

Fienberg, Martin, Straf hebben daarvoor in hun rapport over het delen van data al in 1985 opgemerkt dat het delen van data het open wetenschappelijk debat en onderzoek bevordert en een diversiteit aan analyse en conclusies teweeg brengt. Zij vatten de voordelen als volgt samen:

- Herverificatie van gepubliceerde resultaten
- Alternatieve en aanvullende analyses
- Analyses om te controleren of de uitkomsten voldoende robuust zijn bij veranderde aannames.

*De kosten-baten analyse van het delen van (wetenschappelijke) data moet worden gemaakt op ethisch, institutioneel, juridisch en professioneel niveau. Daarbij zal een balans moeten worden gevonden tussen het paradigma van data-eigenaarschap, het 'hamsteren' van data, data eigenaarschapsbeleid, rechten en plichten en beschikbare technologie.*

#### *Tien potentiële data-eigenaars*

Wie kunnen als potentiële data-eigenaar worden aangemerkt en waarom? Loshin ontleedt de complexiteit van het begrip data-eigenaarschap door een lijst van mogelijke eigenaren en de daarbij behorende eigenaarschap verschaffende elementen te benoemen. Deze eigenaars claims zijn gebaseerd op het soort en op de mate van betrokkenheid bij de totstandkoming van de data. De lijst omvat:

- 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,<sup>61</sup>
- 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.

#### *Data-eigenaar coöperatief rijden*

Deze indeling helpt bij het ontwikkelen van inzicht in de posities van potentiële data-eigenaren of verantwoordelijken/rechthebbenden. Kijkend naar de data die in het kader van coöperatief rijden wordt gegenereerd kan worden vastgesteld dat alle bovengenoemde 'eigenaren' zich potentieel als data-eigenaar zouden kunnen melden. Bezien vanuit de informatisering zal degene die de data verzameld en verwerkt het grootste deel van het eigenaarschap toekomen. Dat is in beginsel de service provider die de dienst exploiteert en die een contractuele relatie zal hebben met alle andere betrokken partijen. Hij heeft de verantwoordelijkheid voor het goede beheer van de data. Kijkend naar de opsomming kan hij een flink aantal van de genoemde rollen vervullen: die van vervaardiger, van afnemer, van samensteller, van opdrachtgever, van verspreider, van koper/licentienemer.

Is de opsomming geschikt om ook vanuit juridisch perspectief een zekere rangorden te kunnen aanbrenge(n)? Dit lijkt inderdaad het geval. Zo zal vanuit de gedachte van bescherming van

---

<sup>61</sup> Het begrip eigendom is hier gebruikt in de economische zin, data als waarde.

persoonsgegevens het subject, degene over wie de gegevens worden verzameld goede papieren hebben als rechthebbende. Ook de koper/licentienemer, ic. de coöperatief rijden service provider, heeft goede papieren mits zijn recht is verkregen van degene die dat ook kon verschaffen. De belangrijkste relatie is in dat verband de overeenkomst tussen de service provider en de klant. Daarnaast zullen ook in de contractuele relaties tussen de service provider en zijn onderaannemers en de wegbeheerder data een belangrijke plaats innemen.

#### *Negen redenen om data-overdracht te weigeren*

Een andere invalshoek als het gaat om data-eigenaarschap is de bevoegdheid om rechten te delen, of om dat juist niet te doen. Met name dat laatste kan tot al of niet ongewenste onvolkomenheden in de informatievoorziening leiden. Dit zou die de doelstelling van de informatievoorziening, wat deze in een bepaald geval ook is, kunnen bedreigen. Interessant is in dit verband een analyse van factoren die de beslissing van een rechthebbende om toegang tot data te onzeggen beïnvloeden (Sieber 1989). Hij komt tot een negental redenen die een rol spelen bij de beslissing om gegevens niet te delen:

- Kosten voor de verstrekking,
- Bescherming van eigendoms- economische of beveiligingsbelangen,
- Extreem dure en tijdrovende verzameling van data ten behoeve van de ontsluiting,
- De noodzaak om de data uit te breiden om tot een goed begrip van de bestaande data te komen,
- Technische obstakels,
- Vertrouwelijkheid,
- Zorgen over de kwalificaties van de verzoekers van de data,
- Persoonlijke motieven,
- Kosten voor de ontvangers,
- Kosten voor de opdrachtgevers.

De eerste vier overwegingen zijn eigenlijk terug te voeren op economische factoren. Voor een bezitter van de data, tevens rechthebbende, is het verstrekken van de data een kostenpost die bedrijfseconomisch wordt afgewogen. Spontane overdracht ligt niet voor de hand als een van deze factoren zich voordoet. Alleen van buiten af, bijvoorbeeld door een wettelijke- of contractuele verplichting, of tegen vergoeding zal de dataverstrekking tot stand komen. Technische obstakels vallen deels ook in deze categorie, maar kunnen ook absoluut zijn, d.w.z. niet met een financiële inspanning op te lossen. De daarop volgende drie obstakels zijn deels subjectief en kwalitatief van aard, terwijl de kosten van ontvangers en opdrachtgevers met name door henzelf als reden voor het niet delen van gegevens zullen worden ingebracht.

Als deze factoren worden aangehouden tegen Spookfiles en coöperatief rijden, dan lijkt het erop dat deze redenen geen grote obstakels vormen voor het data verkeer in operationele zin. Aangezien de data op basis van overeenkomsten wordt verkregen en geleverd, zullen mogelijke obstakels bij het aangaan van de overeenkomst kunnen worden benoemd en opgelost. Wel kunnen bepaalde obstakels spelen vanuit het wettelijk kader. In het kader van de WBP kan de informatievoorziening aan de betrokkene door de verantwoordelijke bijvoorbeeld worden beperkt doordat deze onevenredig duur en/of tijdrovend is.

#### *Data eigenaarschapsbeleid*

Om de kwaliteit van data goed te kunnen bewaken is beleid ten aanzien van het verzamelen, opslaan en gebruiken van data noodzakelijk. Voordat een bepaalde activiteit waarvoor data worden gebruikt wordt

gestart, moet worden vastgesteld hoe binnen de activiteit en door de daarbij betrokken spelers met de data wordt omgegaan. Discussie over het gebruik van data en zelfs vergaande conflicten kunnen ontstaan als het gebruik en de eigenaarschap van de data onvoldoende is geregeld en vastgelegd. Dergelijke afspraken zijn eveneens nodig om oneigenlijk gebruik van data tegen te gaan.

### 4.3 Data-eigendom

#### *Eigendom en data*

De partijen die bij de verwerking van gegevens in het kader van coöperatief rijden betrokken zijn hebben allemaal een belang bij een bepaalde mate van zeggenschap. Het is dan ook begrijpelijk dat het begrip eigendom in de discussie over de gegevens binnen het coöperatief rijden systeem veelvuldig wordt gebruikt. Eigendom wordt immers voorgesteld als een ‘absoluut recht’: het hebben van uitsluitende beschikkingsbevoegdheid ten opzichte van anderen. De achttiende-eeuwse Engelse jurist Sir William Blackstone verwoordde de menselijke kijk op eigendom als volgt: ‘Het despotisch domein waarbinnen iemand het recht claimt en uitoefent over aardse zaken, met uitsluiting van het recht van welk ander individu dan ook in het universum’. Aan de lichte ironie in het citaat valt op te maken dat een dergelijk eigendomsbegrip in de ogen van Blackstone niet bestaat. Ook in de huidige tijd is een volledige en ongeclausuleerde eigendom van een goed een illusie, en kan het denken in dergelijke termen de discussie over data-eigenaarschap vertroebelen.

#### *Eigendom van data in Nederland*

Zoals reeds gesteld kunnen eigendomsrechten in het Nederlandse recht alleen rusten op ‘stoffelijke objecten’<sup>62</sup>. Dat betekent dat wel de gegevensdragers vatbaar zijn voor eigendom, maar niet de zich daarop bevindende gegevens. Hetzelfde geldt voor fysieke dossiers en het daarin opgeborgen papier. Doordat gegevens niet stoffelijk zijn kunnen ze zich ook tegelijkertijd op meerdere plaatsen bevinden, bij meerdere partijen. Overigens betekent dat niet dat gegevens juridisch onbeschermd zijn. Het veranderen, wissen of onbruikbaar maken van gegevens kan onder bepaalde omstandigheden zelfs strafbaar zijn<sup>63</sup>.

In zijn analyse met betrekking tot het elektronisch patiëntendossier stelt Ekker in plaats van eigendom een drietal rechten voor die op de gegevens uit het patiëntendossier van toepassing kunnen zijn. Hoewel hij het data-vraagstuk benadert vanuit het elektronisch patiëntendossier, is de indeling ook bruikbaar voor de kwalificatie van data die in het kader van coöperatief rijden worden gegenereerd. Hij onderscheidt:

1. zeggenschapsrechten,
2. contractuele rechten en verplichtingen, en
3. intellectuele eigendomsrechten.

---

<sup>62</sup> De minister van justitie verwoordde dit als volgt:

‘Wij verzetten ons evenzeer tegen de toepassing van noties, ontleend aan het eigendomsrecht, met betrekking tot gegevens. De geregistreerde, noch de houder kunnen worden aangemerkt als «eigenaar» van persoonsgegevens. Het multiple karakter van gegevens, in de zin dat dezelfde gegevens ter beschikking kunnen staan van meerdere personen, die er feitelijk zonder medewerking van de ander vrijelijk over kunnen beschikken zonder dat de ander deze daardoor komt te ontberen, staat aan een dergelijke juridische benadering in de weg. Het juridische begrip «eigenaar» of «eigendom» is niet bruikbaar, ook niet naar analogie, in deze samenhang.’ Zie Kamerstukken II, vergaderjaar 1991–1992, 21 561, nr. 11: p. 25 en 26.

<sup>63</sup> Zie artikel 350a en 350b Wetboek van Strafrecht.

### *Verschillende partijen*

De zeggenschapsrechten van de persoonsgebonden gegevens liggen in beginsel bij de klant, en zijn dienstverlener voor zover deze de data genereert. De contractuele rechten kunnen, afhankelijk van gesloten overeenkomsten, bij alle partijen liggen. Bij de klant, zijn dienstverlener, de partners van de dienstverlener en zelfs de wegbeheerder. Voor zover er sprake kan zijn van intellectuele eigendomsrechten zullen deze liggen bij de serviceprovider en zijn partners. Zij bewerken immers de data tot een nieuwe dataset.

### *Zeggenschapsrechten*

Binnen de coöperatief rijden dienst hebben zowel klanten als hun dienstverleners bepaalde zeggenschap over de binnen de dienst gegenereerde gegevens. De rechten van de klant beschermen in het bijzonder zijn privacy, nader beschreven in hoofdstuk 2. De dienstverlener heeft zeggenschap in het kader van zijn verantwoordelijkheid voor het goed uitvoeren van de dienst.

### *Zeggenschap van de dienstverlener*

Bij het aangaan van de overeenkomst voor de verlenen van de coöperatief rijden dienst verwerft de dienstverlener een gebruiksrecht op de data die in het kader van de dienst worden gegenereerd. Zonder het recht de data van het coöperatief rijdend voertuig met de persoonsgegevens van de klant te kunnen gebruiken, kan de dienst niet tot stand komen. Bij het sluiten van de overeenkomst zal de dienstverlener zich wel moeten houden aan de bepalingen uit de WBP en Tw, zoals beschreven in hoofdstuk 2.

### *Vastleggen*

De zeggenschap van de klant en de dienstverlener zullen dus moeten worden vastgelegd in de coöperatief rijden overeenkomst, en vallen binnen de van kracht zijnde wetgeving. Dit betekent dat ook eventuele belangenconflicten tussen de klant en de dienstverlener binnen het kader van de overeenkomst en de wetgeving moeten worden opgelost. Welk belang bij een botsing van zeggenschapsrechten als in zo'n geval prevaleert valt in zijn algemeenheid niet te zeggen, maar hangt af van de wet, de situatie en de inhoud van de overeenkomst.

### *Meerdere dienstverlenende partijen*

De vraag is of ook de andere betrokken partijen, niet zijnde de contracterende dienstverlener, eigen zeggenschapsrechten hebben, of dat deze rechten slechts afgeleid zijn van het recht van de contracterende dienstverlener. De vergelijking met de rol van de bewerker in de WBP dringt zich op. Het zal met name van de onderliggende contractuele verhoudingen afhangen hoe de rechten op de data verdeeld zijn. Net als de dienstverlener kan de partner die een deel van de dienst uitvoert juridische eigenaar zijn van een van de gegevensdragers (het informatiesysteem) waarop in het kader van coöperatief rijden data worden vastgelegd. Deze partner is dan tevens verantwoordelijk voor de beveiliging van de data en moet er voor zorg dragen dat er geen onbevoegden toegang kunnen krijgen tot data die als vertrouwelijk moeten worden beschouwd.

### *Contractuele rechten en verplichtingen*

Contractuele rechten en verplichtingen met betrekking tot locatiegegevens spelen in verschillende verhoudingen een rol. Een coöperatief rijden dienst kan niet functioneren zonder dat daartoe met de klant een overeenkomst is gesloten, waarbij overigens het wettelijk kader, en met name de WBP en Tw, steeds onverkort van toepassing is. Ook tussen de betrokken dienstverleners zowel op het gebied van content als op het gebied van ICT-dienstverlening zullen overeenkomsten worden gesloten waarin

afspraken kunnen worden gemaakt waarbij de verantwoordelijke dienst aanbieder de omgang met de data door andere dienstverleners regelt. Contractuele afspraken zullen veelal betrekking hebben op de volgende onderwerpen:

- door een dienstverlener te leveren diensten;
- (effectuering van) privacy-rechten
- intellectuele eigendomsrechten;
- aard en omvang van de gegevensuitwisseling;
- betrouwbaarheid en beschikbaarheid;
- informatiebeveiliging;
- aansprakelijkheid.

In het kader van data-eigenaarschap zijn met name de intellectuele eigendomsrechten van belang. Op deze categorie zal hierna nader worden ingegaan.

#### *Intellectuele eigendomsrechten*

De term intellectuele eigendomsrechten is enigszins verwarrend aangezien het in juridische zin geen eigendomsrechten betreft. Zij geven de rechthebbende (niet de 'eigenaar') het recht om de gegevens te gebruiken, mogelijk zelfs rechten aan anderen toe te kennen en om bepaalde vormen van gebruik van de gegevens te verbieden. Bij coöperatief rijden zouden met name het databankenrecht en eventueel het auteursrecht aan de orde kunnen komen. Deze rechten hebben als doel om de economische belangen van de rechthebbende te beschermen.

#### *Databankrechten*

Het databankenrecht geeft de producent van een databank het alleenrecht op het kopiëren, verspreiden, tentoonstellen en anderzijds 'openbaar maken' of 'reproducen' van de databank als geheel, gedurende 15 jaar. Een databank is een geordende verzameling van werken, gegevens of andere zelfstandige elementen die afzonderlijk toegankelijk zijn.

Binnen coöperatief rijden zou het invoeren van het databankenrecht zich vooral voor kunnen doen op het moment dat de gegenereerde locatiegegevens moeten worden verspreid ten behoeve van het verlenen van de coöperatief rijden dienst. Maar de geanonimiseerd bewaarde gegevens kunnen ook eventueel voor bijvoorbeeld verkeersinformatie of statistische doeleinden worden gebruikt.

#### *Eis van substantiële investering*

Materieel zal de gegevensverzameling die door het coöperatief rijden wordt gegenereerd kwalificeren als databank. De bescherming van het databankenrecht geldt echter voor een producent die een 'substantiële investering' heeft gedaan in de samenstelling of het onderhoud van de databank. Dat kan een financiële- of een feitelijke inspanning zijn, zolang deze maar uitsluitend gericht is op het aanleggen en onderhouden van de databank als zodanig en niet op het creëren van de gegevens die, naderhand, in een databank kunnen worden bijeengebracht. Omdat hiervan geen sprake als de databank is ontstaan uit een andere hoofdactiviteit van de producent, i.e. de coöperatief rijden dienst, zal het databankenrecht geen rol gaan spelen binnen coöperatief rijden.

#### *Auteursrecht*

Nog minder is dat het geval bij het auteursrecht, waarbij het te beschermen werk aan een aantal eisen moet voldoen die zich met dataverzameling in het kader van coöperatief rijden niet goed laten

verenigen. Het auteursrecht is namelijk bedoeld voor de bescherming van creatieve prestaties en stelt dan ook als voorwaarde dat het werk een 'oorspronkelijk karakter' heeft en het 'persoonlijk stempel' draagt van de maker. Een in het kader van coöperatief rijden ontstane datastroom zal dan ook niet kwalificeren.

#### *Geen eigendom van data coöperatief rijden*

Uit het voorgaande blijkt dat het begrip eigendom bij de verwerking van data, of het nu patiëntgegevens zijn of andere persoonsgerelateerde data, niet bruikbaar is. Afgezien van het feit dat eigendom als juridisch begrip is voorbehouden aan stoffelijke zaken, suggereert het bovendien dat er slechts er één partij is die exclusieve zeggenschap heeft, hetgeen in de praktijk meestal niet het geval is. Wel dienen dienstverleners en hun partners, klanten en wegbeheerders zich bewust te zijn van de verscheidenheid aan rechten en verplichtingen die op de data kunnen rusten. In de overeenkomsten die tussen de partijen worden gesloten zal de verdeling van de rechten op de binnen de coöperatief rijden dienst gegenereerde data moeten worden vastgelegd. Het wettelijk kader, met name de WBP, zal bij die vastlegging doorlopend in het oog moeten worden gehouden.

#### *Verskil tussen medische data en coöperatief rijden data*

Naast een aantal overeenkomsten zijn er ook duidelijke verschillen als het gaat om data verwerking bij een patiëntendossier of bij coöperatief rijden. Hierna is de vergelijking in een staatje aangegeven:

- |   |  |
|---|--|
| <ul style="list-style-type: none"><li>• <i>Persoonsgegevens in kader behandelovereenkomst, onder WBP</i></li><li>• <i>Inhoudelijke (medische) gegevens gegenereerd door behandelaar</i></li><li>• <i>Medische gegevens blijven als persoonsgegevens in EPD, op verschillende plaatsen beschikbaar.</i></li><li>• <i>Geanonimiseerde gegevens voor onderzoek beschikbaar</i></li></ul> | <ul style="list-style-type: none"><li>• <i>Persoonsgegevens in het kader van coöperatief rijden overeenkomst onder WBP</i></li><li>• <i>Inhoudelijke (locatie/voertuig) gegevens gegenereerd door systeem</i></li><li>• <i>Inhoudelijke gegevens real time (geanonimiseerd) te gebruiken voor coöperatief rijden dienst, tijdelijk beschikbaar voor en tot facturering.</i></li><li>• <i>Geanonimiseerde gegevens als real time en historisch verkeersinfo beschikbaar</i></li></ul> |
|---|--|

Zowel medische gegevens als coöperatief rijden gegevens zijn aan te merken als persoonsgegevens in de zin van de WBP. Daarbij behoren medische gegevens tot de categorie 'bijzondere' gegevens waarvoor de wet voorziet in extra bescherming (art. 21 WBP). In beide gevallen worden de gegevens met toestemming van de betrokkene door derden (behandelaars, of een on-board-unit in de auto) toegevoegd. Een groot verschil tussen beide zit in de periode van bewaren van de data. Zo heeft het medische dossier naar zijn aard een lange levensduur waarin het dossier cumulatief wordt opgebouwd met actuele medische gegevens. Bij coöperatief rijden heeft de dataset, naar zijn aard een beperkte levensduur. Na gebruik blijven alleen de identificatie en administratieve gegevens achter. De basisgegevens voor de coöperatief rijden dienst zijn na facturering niet meer nodig en moeten ofwel worden vernietigd, ofwel worden geanonimiseerd voor gebruik ten behoeve van bijvoorbeeld verkeersstatistiek. Hoewel zowel de medisch-inhoudelijke gegevens als de locatie- en andere coöperatief rijden gegevens tussen verschillende partijen worden getransporteerd, stelt het draadloze transport van de coöperatief rijden gegevens extra eisen aan de beveiliging ervan.



#### *Gebruik voor onderzoek*

Medische gegevens worden in beginsel in een gesloten systeem van medici gebruikt in relatie tot de behandeling van, en de communicatie met de patiënt. Daarnaast kunnen de gegevens collectief worden aangewend voor wetenschappelijk onderzoek. Deze gegevens zullen op dat moment veelal geanonimiseerd zijn. Bij medische gegevens zijn de individuele toepassing en de collectieve toepassing doorgaans goed te scheiden, zodat geen persoonsgegevens naar de collectieve toepassing worden overgebracht. Het patiëntendossier blijft bij de behandelaar en voor collectieve toepassingen kan worden volstaan met een anonieme kopie. Ook de administratieve handelingen rond de behandeling kunnen op basis van het patiëntendossier worden verricht.

#### *Gebruik voor real time services*

Bij een coöperatief rijden dienst, zoals bijvoorbeeld de Spookfiledienst, zijn de klantgegevens, naam, adres, woonplaats gekoppeld aan het kenteken. Vervolgens worden door het systeem reeksen locatiegegevens gegenereerd die naar de wegkant worden gezonden. De aldus ontstane gegevens set vormt het dynamische klant dossier. Uit dit dossier moeten vrijwel gelijk met het ontvangen van de locatiegegevens met een snelheidsadvies terug worden gezonden naar het voertuig. Voor zover deze gegevens over het openbare kanaal gaan zullen zij geanonimiseerd zijn. Gaan zij over een privaat kanaal, als persoonlijk advies, dan worden, naast de inhoudelijke gegevens, ook de identificerende gegevens uit het dossier meegezonden. Dit stelt hoge eisen aan de beveiliging van het dataverkeer.

### **4.4 Conclusies**

Voorlopig kan worden geconcludeerd dat aan de term data-eigenaarschap geen juridische connotatie kan worden meegegeven omdat het begrip vooral komt uit de wereld van het informatiemanagement. Data-eigenaarschap bestaat vanuit deze achtergrond uit twee componenten: bezit en verantwoordelijkheid. Bezit van en verantwoordelijkheid voor de data impliceert echter nog geen juridische eigendom aangezien juridische eigendom is voorbehouden aan stoffelijke objecten. Data eigenaarschap kan juridisch beter vertaald worden naar rechten en verplichtingen, termen die ook beter aansluiten bij de informatiekundige begrippen bezit en verantwoordelijkheid. De verdeling van deze rechten en plichten vindt, met in achtneming van de wettelijke voorschriften, plaats op basis van de overeenkomsten tussen de partijen. De waarde van de data, die bij deze verdeling een belangrijke rol speelt, komt tot stand door de verwerking van de data en door de context waarbinnen de gegevens worden gebruikt.

In het kader van deze rapportage is met name gekeken naar de juridische aanspraken op gegevens binnen coöperatief rijden. Daarbij gaat het om verschillende soorten gegevens. In de eerste plaats om de als persoonsgegevens aan te merken gegevens die betrekking hebben op de locatie en de eventuele traceerbaarheid van de klant. Daarnaast gaat het over persoonsgegevens die worden gebruikt in de administratie, bijvoorbeeld de naam, adres, woonplaatsgegevens die worden gebruikt voor de facturering en verdere contacten met de klant. Ten slotte kunnen geanonimiseerde gegevens worden gebruikt voor real time of historische verkeersinformatie. Op deze verschillende soorten gegevens zullen ook verschillende rechtenregimes kunnen gelden. Veel van deze rechtsrelaties zullen vorm krijgen in de contracten tussen de verschillende partijen.

#### *Aanbevelingen*

Start een discussie over de verdeling van de rechten op de data binnen coöperatief rijden waarbij het uitgangspunt is om de klant het gevoel van controle over 'zijn' data te geven. Aangezien de verdeling van data rechten een zaak is tussen private partijen is een transparante rechtenverdeling van belang.

Deze zou in de beschrijving van de coöperatief rijden dienst voor de klant een plaats moeten krijgen.  
Het ontbreken ervan kan een drempel opleveren voor de klant om in te stappen in coöperatief rijden.

### *Discussie over omgang met medische gegevens in de Verenigde Staten<sup>64</sup>*

#### *Inleiding*

In de Verenigde Staten heeft de afgelopen jaren een debat gewoed met als inzet de vraag hoe het gebruik van medische gegevens voor onderzoek en volksgezondheid enerzijds en de bescherming van de privacy van de patiënt anderzijds moest worden geregeld. Daarbij kwamen vragen aan de orde als: van wie zijn de medische gegevens? Kun je medische gegevens bezitten? En maakt het wat uit of je ze bezit of dat je het gebruiks- of inzage recht hebt?

Het verschil tussen Nederland en de Verenigde Staten is dat gezondheidsonderzoek daar met name door commerciële research partijen wordt gedaan en dat de medische gegevens daardoor een bepaalde commerciële waarde krijgen. Met name dit punt noopte ertoe om de beschikbaarheid van medische gegevens wettelijk te regelen. Daarbij speelde de verschillende visies op data-eigenaarschap een belangrijke rol.

#### *Data 'eigendom'*

In de Verenigde Staten is data-eigenaarschap, overigens net als bij ons, niet in de wetgeving gedefinieerd. In de discussie werden verschillende posities betrokken. Zo ging het bij eigenaarschap van patiënten data volgens sommigen vooral om privacy bescherming, terwijl anderen het belang van de volksgezondheid om de data zoveel mogelijk toegankelijk te maken benadrukten. Weer anderen zagen de data het liefst publiek eigendom worden. Wel leek iedereen het er over eens dat het ging om een probleem dat moest worden opgelost.

Zoals reeds eerder uitgebreid vastgesteld moet vanuit juridisch perspectief met enige scepsis worden gekeken naar het begrip eigendom. Een strikte eigendomsopvatting kwam in de VS met name van de advocaten die de privacybelangen wilden beschermen. Zij eisten het de volledige eigendom van de patiëntengegevens op voor hun cliënten, de patiënten. Een uitspraak zoals in Nederland, waarbij werd vastgesteld dat eigendom uitsluitend mogelijk is ter zake van een stoffelijk object, was in de Verenigde Staten kennelijk niet voorhanden.

Anderen trokken deze opvatting in twijfel door te stellen dat een eigendomsrecht niet zo absoluut is als werd gesuggereerd. Zij stelden dat hogere belangen, zoals die van de volksgezondheid als geheel, een inbreuk op het recht kunnen rechtvaardigen. In geval van een belangenconflict zullen belangenafwegingen altijd uitgaan van een zekere openheid van de normen die gehandhaafd moeten worden. In dat kader is het overigens de vraag in hoeverre het wettelijk toekennen van 'eigendom' van data aan de persoon op wie de data betrekking heeft de positie van die persoon wat betreft zijn of haar rechten wezenlijk zou veranderen.

#### *Waarde van de data*

Het taaie gevecht om de zeggenschap over de data illustreerde dat de patiëntendata een zekere waarde vertegenwoordigde. Daarbij rijst de vraag op welk moment data waarde krijgen en voor wie. Een ruwe patiëntendatabase bijvoorbeeld heeft maar een betrekkelijke waarde als het gaat om een bruikbare

---

<sup>64</sup> Much Ado About Data Ownership, Evans, Harvard Journal of Law & Technology 2011

toepassing ervan. Bruikbare data vereisen naast ruwe data ook allerlei technische en infrastructurele voorzieningen. De business case voor het tot stand brengen van die voorzieningen kan worden belemmert door een 'volle eigendom' van die data bij, bijvoorbeeld, het subject van die data.

#### Toepassing bij 'coöperatieve' gegevens

De spanning tussen de privé bescherming van data en de collectieve waarde en gebruik speelt zowel bij medische- als bij verkeersgegevens. In beide gevallen moeten de grenzen van het gebruiksrecht worden bepaald aan de hand van open normen. Gegevens delen in 'het algemeen belang', een wat gedateerd klinkende term, kan een complex dilemma opleveren.

Bij een beperkt aantal patiëntendossiers voor een bepaald onderzoek kan een groep individuele weigeraars de kwaliteit van het onderzoek aantasten en zo de volksgezondheid 'bedreigen'.

Bij coöperatieve systemen ten behoeve van de verkeersveiligheid en de doorstroming is een bepaalde hoeveelheid deelnemers noodzakelijk om de gewenste dienst goed te kunnen verlenen. Een te laag aantal deelnemers maakt de dienst kwalitatief minder goed. Verkeersdeelnemers die hun privacy belangrijker vinden dan doorstroming en collectieve verkeersveiligheid hebben daarmee een negatieve invloed op het systeem. In die zin zou je kunnen zeggen dat de keuze voor privacy niet neutraal is ten opzichten van het collectieve belang.

#### *Bescherming privacy vs collectief gebruik*

Op de vraag of 'data-eigendom' in juridische zin, zoals bepleit door de advocaten van de patiënten, de privacy beter beschermt dan een beperkter gebruiksrecht waren in de discussie in de VS de meningen verdeeld. Advocaten proberen het data eigenaarschap met name als dam voor de bescherming van de privacy te gebruiken. Daarbij speelt een belangrijke rol dat dat de collectieve onderzoeken in de Verenigde Staten, zoals gezegd, worden gedaan door private partijen. Deze partijen zijn bereid om te betalen voor de gegevens die de basis vormen voor hun research. Het risico bestaat dat het principe van 'informed consent', zoals wij dat ook kennen, daarbij verwordt tot het te gelde te maken van het recht van het subject, de patiënt, op de patiëntgegevens. Dit element kan de privacy discussie in bepaalde gevallen in een ander daglicht plaatsen, immers: hoe voller de eigendom hoe hoger de vergoeding.

De voorstellen die uiteindelijk werden gedaan vielen uiteen in twee categorieën:

1. Voorstellen ter bescherming van de privacy
2. Voorstellen om collectief gebruik van de data mogelijk te maken.

De privacy beschermers gingen uit van de eigendom van de rechten op het patiëntendossier van de patiënt. Zij suggereerden een absoluut individueel recht, in de Blackstoniaanse zin.<sup>65</sup> De visie van de privacy lobby op data-eigenaarschap was kort samengevat: een geregelde toegang tot data en de macht om niet-toegestemd gebruik te stoppen.

De collectivisten, waaronder de private onderzoekslaboratoria, zagen de rechten op het patiëntendossier meer als een samenstel van - potentiële - rechten. In hun visie leidde de afweging tussen de privacy en de inzet van data in het belang van de volksgezondheid tot een verdeling van rechten tussen de partijen.

---

<sup>65</sup> Blackstone: on how people imagine ownership

Vanuit het Nederlandse perspectief zou de tegenstelling gemakkelijk overbrugbaar moeten zijn: tot de persoon te herleiden medische data vallen onder de privacybescherming, voor onderzoeksdoeleinden kan gebruik worden gemaakt van geanonimiseerde data. In de Verenigde Staten echter blijkt de rechter ook het individueel recht op privacy te passeren ten gunste van private onderzoeken ten behoeve van de volksgezondheid.

#### *Betaling voor rechten*

De component van de betaling brengt ook andere aspecten mee die ook raken aan het coöperatief rijden. De vraag bijvoorbeeld wat de scope is van het begrip algemeen belang? En of je alleen kunt profiteren van de collectieve verworvenheden als je bereid bent om mee te investeren door middel van het beschikbaar stellen van je eigen gegevens? En hoe bepaal je de waarde van de data? Zo zou wel eens kunnen blijken dat bij 100% dataprotectie de bruikbaarheid, en daarmee de waarde, van de data nihil is omdat ze dan niet ontsloten kunnen worden.

Een bekende formule is om geen vergoeding voor data zelf te hoeven geven, omdat deze slechts waarde hebben binnen de context van bijvoorbeeld een onderzoek. In die gevallen blijft wel de mogelijkheid voor een vergoeding van de transport- en verwerkingskosten open. De eigenaarschap van de data is in dat geval dus minder van belang.

#### *Uitzonderingsituaties*

Een andere beperking van de eigenaarschap van het subject is dat er mogelijkheden zijn om zonder toestemming van de patiënt toegang te krijgen in bepaalde gegevens. Daarbij valt te denken aan het opsporen van strafbare feiten en de acute bescherming van de volksgezondheid. In het kader van coöperatief rijden zou kunnen worden gedacht aan heel specifieke uitzonderingen in verband met een acuut belang voor de verkeersveiligheid.

Het recht in de Verenigde Staten maakt het mogelijk om de strikte regels rond privacybescherming niet toe te passen, bijvoorbeeld als een 'informed consent' in de praktijk moeilijk te verkrijgen is. Zelfs als een dergelijke overdracht plaats vindt naar een private organisatie kan van de regels worden afgeweken, mits deze organisatie onder toezicht staat van de overheid! Tenslotte kan van de regels worden afgeweken als een private research organisatie meer capaciteit heeft dan de overheid om de data te verwerken, en als de gegevens om die reden aan de private organisatie worden verstrekt.

Daarbij komt dat naast de patiënt zelf en zijn zorgverlener ook verzekeraars en zorgverleners op een deel van de rechten op de data doen gelden, bijvoorbeeld omdat zij een deel van de data zelf leveren. In dat geval is sprake van gedeeld eigenaarschap (gedeelde rechten).

#### *Wettelijke regeling*

Om tot een wettelijke oplossing te komen werden twee mogelijke beleidsinterventies voorgesteld om aan het dilemma in de VS een einde te maken. De eerste opvatting was er een waarbij de overheid een 'trusted' rol kreeg. Alle geanonimiseerde medische data zouden daarbij in bewaring worden gegeven bij de overheid (Rodwin). Deze anonieme en 'trusted' opslag maakte een 'non consensual' toegang, een toegang zonder toestemming van de betrokken patiënt mogelijk. Ook de 'bijverdienste' voor patiënten met een interessant medisch dossier werd op die manier afgesneden.

De andere keuze was meer geënt op de commerciële praktijk en voorzag erin dat alle medische data in bewaring zouden komen bij de private marktpartijen (Hall&Schulman). Deze zouden de dossier mogen

gebruiken als zogenoemde interconnected medical records (I-EMRs). Hiervoor zou dan wel een consensual toegang, toestemming van de patiënt, nodig zijn.

Deze laatste variant lijkt nog het meest sterke juridisch recht in zich te bergen, inclusief recht van overdracht van rechten. Dit recht gaat echter zeker niet zover als de volledige bescherming die de advocaten voorstaan die het eigendomsrecht inroepen om de privacy van hun cliënt te beschermen.

## Lijst van geraadpleegde literatuur

Vehicle Safety Regulations and ADAS: Tensions Between Law and Technology

K.A.P.C. van Wees 2004

Over intelligente voertuigen, slimme wegen en aansprakelijkheid

Dr. K.A.P.C van Wees 2010

Universitair docent privaatrecht, Vrije Universiteit Amsterdam

Automated vehicles are probably legal in the United States

Bryant Walker Smith / November 1, 2012

Product liability for ADAS; legal and human factors perspectives

Kiliaan van Wees and Karel Brookhuis

EJTIR, 5, no. 4 (2005), pp. 357-372

Environmental, safety, legal and societal implications of autonomous driving systems

Alexander Robertsson, Anders Eugensson, et.al. 2013

Online tracking: Questioning the power of informed consent

Eijk, N. van, Helberger, et. al. Paper September, 2011

Wet bescherming persoonsgegevens en ICT

Mw. Mr. S. M. Huydecoper, Monografieën Recht en Informatietechnologie, 2006.

Kroniek Technologie en recht

Remy Chavannes en Niels van der Laan1, NJB 12-10-2012

Privacy en vormen van ‘intelligente’ mobiliteit, de impact van ict-applicaties door de weg en het spoor

Henk Griffioen WRR 2011

Towards Safe and Efficient Driving through Vehicle Automation: The Dutch Automated Vehicle Initiative

Raymond Hoogendoorn, Bart van Arem, et.al.

30 October 2013 -

Verkeersgegevens ; Een juridische en technische inventarisatie

L. F. Asscher en A.H. Ekker (red.) Instituut voor Informatierecht 2003

ITS Action Plan - Action 5.2

Final Report of the Study regarding liability aspects of ITS applications and services, Berlin, 07.12.2012

Beter Benutten van Intelligente Mobiliteit

Programma Beter Benutten 2013

Much ado about data ownership,

Barbara J. Evans, Harvard Journal of Law & Technology, Volume 25, Number 1 Fall 2011

Knowledge Integrity: Data Ownership (Online)

D. Loshin, June 8, 2004

Ensuring the integrity of the research process

Panel Sci. Responsib. Conuct. Res. 1992

Why not one big database? Principles for data ownership

Marshall Van Alstyne, Erik Brynjolfsson, et.al. 1995

Ownership of data and the need for information exchange

M. Keunovic, Fellow IEEE 2002

Van wie is het dossier? Rechten en plichten rondom patiëntgegevens.

Anton Ekker (Nictiz), 29 oktober 2010

Eindadvies Strategisch Beraad Verkeersinformatie en Verkeersmanagement

Oktober 2011

EU-Commission, Opinion 13/2011 on Geolocation services on smart mobile devices

Adopted on 16 May 2011

Advies Besluit meldingsformaliteiten en gegevensverwerking scheepvaart CBP 24 januari 2012

Kiezen voor privacy Hoe de markt door persoonsgegevens beter kan

CPB Policy Brief | 2014/04 Michiel Bijlsma et al.

Rapport van bevindingen: Ambtshalve onderzoek CBP naar de verwerking van geolocatiegegevens

door TomTom N.V., Openbare versie 20 december 2011

Agencia Española de Protección de Datos, Mario Costeja González

Hof van Justitie van de Europese Unie, Luxemb., 13 mei 2014, Arrest in zaak C-131/12

EU-Commission - Right to be forgotten ruling 2014 C131-12