

## VERKEERSGEGEVENS

*Een juridische en technische inventarisatie*

L. F. Asscher en A. H. Ekker (red.)

R. Hes  
A. H. Ekker  
B. J. Koops

ISBN 90 757 27 364  
Otto Cramwinckel Uitgever 2003  
[www.cram.nl](http://www.cram.nl)

Instituut voor Informatierecht  
2003

## INHOUDSOPGAVE

### INLEIDING

#### Verkeersgegevens in nieuwe generaties telecomsystemen

<b>LIJST VAN BEGRIPPEN</b>	<b>11</b>
<b>1 ACHTERGROND</b>	<b>12</b>
<b>2 CLASSIFICATIE VAN VERKEERSGEGEVENS</b>	<b>13</b>
2.1 Definitie van verkeersgegevens	13
2.2 Definitie van verkeersgegevens: wet en praktijk	15
2.3 Vastlegging van verkeersgegevens: wet en praktijk	19
<b>3 TECHNIEKSTUDIE: GPRS</b>	<b>20</b>
3.1 Principes van GPRS	21
3.2 Opbouw van een GPRS netwerk	23
3.3 Vastlegging van gegevens binnen GPRS	26
3.4 Privacyaspecten van billing	28
<b>4 LOKATIEGEGEVENS IN NIEUWE GENERATIE MOBIELE SYSTEMEN</b>	<b>29</b>
4.1 Inleiding	29
4.2.1 Systemen van plaatsbepaling	30
4.2.2 Cellulaire systemen van plaatsbepaling	30
4.2.3 Satellietgebaseerde systemen voor plaatsbepaling	31
4.3 Lokatiegebonden diensten: verstrekking van gegevens	32
4.4 Lokatie informatie voor billing	33
4.5 Juridisch-technische aspecten van plaatsbepaling	34
<b>5 SAMENVATTING</b>	<b>36</b>
<b>LITERATUURLIJST</b>	<b>38</b>

## Publiekrechtelijke bescherming van verkeersgegevens

<b>1 INLEIDING</b>	<b>41</b>
<b>2 VERKEERSGEGEVENS: EEN DEFINITIE</b>	<b>41</b>
<b>3 LOCATIEGEGEVENS</b>	<b>46</b>
<b>4 VERKEERSGEGEVENS EN PRIVACY</b>	<b>47</b>
<b>5 BESCHERMING VAN VERKEERSGEGEVENS DOOR ARTIKEL 8 EVRM EN DE RICHTLIJN BETREFFENDE PRIVACY EN ELEKTRO- NISCHE COMMUNICATIE</b>	<b>49</b>
5.1 Jurisprudentie	49
5.2 De richtlijn	49
<b>6 BESCHERMING VAN VERKEERSGEGEVENS OP NATIONAAL NIVEAU: ARTIKEL 10 EN 13 GRONDWET, DE WET BESCHERMING PERSOONSgegevens EN DE TELECOMMUNICATIEWET</b>	<b>51</b>
6.1 Bescherming door artikel 10 en 13 Grondwet	51
6.2 Een nieuw artikel 13 Grondwet	52
6.3 Bescherming van verkeersgegevens in de Wet bescherming persoonsgegevens en de Telecommunicatiewet	54
<b>7 CONCLUSIE</b>	<b>56</b>
<b>LITERATUURLIJST</b>	<b>57</b>

## Verkeersgegevens en strafrecht: een agenda voor discussie

<b>1 INLEIDING</b>	<b>59</b>
<b>2 HISTORISCHE CONTEXT</b>	<b>60</b>
2.1 Oud recht	60
2.2 Huidig recht	61
2.3 Komend recht	63
2.3.1 Commissie-Mevis	63
2.3.2 Wetsvoorstel 28059	64
<b>3 ALGEMENE UITGANGSPUNTEN</b>	<b>66</b>
3.1 Aparte categorie	66
3.2 Geen onderscheid in soorten	67
3.3 Inhoud versus verkeersgegevens	68
<b>4 VOORWAARDEN</b>	<b>70</b>
4.1 Soorten strafbare feiten	70
4.2 Bevoegde autoriteit	71
4.3 Deelname van de verdachte	72
4.4 Subsidiariteit	73
<b>5 OBJECT</b>	<b>73</b>
5.1 Inhoud	73
5.2 Toekomstige gegevens	74
5.3 Identificerende gegevens	75
5.4 Internetgegevens	76
5.4.1 Internetadressen	76
5.4.2 Netpost	77
5.5 Locatiegegevens	78
<b>6 BEWAARPLICHT</b>	<b>83</b>
<b>7 CONCLUSIE</b>	<b>91</b>

## Verlag van de workshop over verkeersgegevens

<b>1 TOELICHTING BIJ HET VERSLAG</b>	<b>93</b>
<b>2 TECHNISCHE ASPECTEN</b>	<b>93</b>
2.1 Presentatie	93
2.2 Discussie	94
<b>3 PUBLIEKRECHTELIJKE ASPECTEN</b>	<b>96</b>
3.1 Presentatie	96
3.2 Discussie	97
<b>4 STRAFRECHTELIJKE ASPECTEN</b>	<b>100</b>
4.1 Presentatie	100
4.2 Discussie	100
<b>NAWOORD</b>	<b>104</b>
Verkeersgegevens: een onderzoeksagenda	104
<b>LIJST VAN DEELNEMERS AAN DE WORKSHOP VERKEERSGEGEVENS</b>	<b>107</b>

## INLEIDING

Op vrijdag 6 september 2002 werd op het Instituut voor Informatierecht een workshop gehouden over verkeersgegevens. Doel van de workshop was in de eerste plaats om meer duidelijkheid te verkrijgen over de juridische en technische definities van verkeersgegevens. Daarnaast werden relevante juridische problemen rond de status en de bescherming van verkeersgegevens in kaart gebracht om de problematiek zodoende beter op de maatschappelijke en politieke agenda te krijgen. De aanleiding lag vooral in de toenemende aandacht voor verkeersgegevens vanuit de strafvorderlijke hoek en het uitblijven van een serieuze wetenschappelijke reactie hierop. Gekozen is voor een rondetafel-expertmeeting waarbij zoveel mogelijk vertegenwoordigers van verschillende standpunten waren genodigd.

Zo waren onder andere aanwezig een vertegenwoordiger van de Europese Commissie, twee personen namens het Ministerie van Justitie, een deelnemer vanuit het Ministerie van Verkeer en Waterstaat, een vertegenwoordiger van de OPTA, vertegenwoordigers van verschillende Nederlandse universiteiten, vertegenwoordigers van telecommunicatieaanbieders en internetproviders, de burgerrechtenorganisatie Bits of Freedom, en tenslotte medewerkers van het College Bescherming Persoonsgegevens (CBP) en het Instituut voor Informatierecht (IViR). Het programma omvatte drie presentaties over achtereenvolgens de technische, de publiekrechtelijke en de strafrechtelijke aspecten van de problematiek. De drie artikelen die in deze bundel zijn opgenomen zijn uitwerkingen van deze presentaties. Hierna is tevens een verslag opgenomen van de discussie die naar aanleiding van de presentaties plaatsvond.

De workshop werd georganiseerd door het Instituut voor Informatierecht (IViR) en het College Bescherming Persoonsgegevens (CBP) en kon plaatsvinden met steun van de Onafhankelijke Post en Telecommunicatie Autoriteit (OPTA), het Directoraat-Generaal Telecommunicatie en Post (DGTP) van het Ministerie van Economische zaken en het Nationaal Actieprogramma Informatietechnologie en Recht (ITeR).

De opbouw van dit boekje is als volgt. Het eerste stuk is een artikel van Ronald Hes over de technische aspecten van verkeersgegevens. Hes gaat in op de technische (on)mogelijkheid van een onderscheid tussen inhoud en verkeersgegevens. Vervolgens gaat Anton Ekker in zijn bijdrage in op een aantal publiekrechtelijke aspecten. Zo behandelt hij de wenselijkheid van constitutionele

bescherming van verkeersgegevens. Bert-Jaap Koops gaat specifiek in op de strafvorderlijke kant van verkeersgegevens. Hij gaat onder andere na onder welke omstandigheden en op welke voorwaarden verkeersgegevens gebruikt mogen worden in het strafproces. Na deze artikelen treft u een samenvatting aan van de tijdens de workshop gevoerde discussie alsmede een mogelijke agenda voor toekomstig onderzoek en debat.

*Amsterdam - december 2002*

<b>Lijst van begrippen</b>	
APN	Access Point Name
BSC	Base Station Controller
BTS	Base Transceiver Subsystem
CDR	Call Detail Record
CG	Charging Gateway
E-OTD	Enhanced Observed Time Difference
ETSI	European Telecommunication Standards Institute
FCC	Federal Communications Commission
GGSN	Gateway GPRS Support Node
GMLC	Gateway Mobile Location Centre
GPRS	General Packet Radio Service.
GPS	Global Positioning System
GSM	Global System for Mobile Communication
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
LCS	Location Service
MSC	Mobile Switching Center
MSISDN	Mobile Subscriber ISDN Number
PDP	Packet Data Protocol
POI	Privacy Override Indicator
SGSN	Serving GPRS Support Node
SMS	Short Message Service
UMTS	Universal Mobile Telecommunication System
URL	Uniform Resource Locator
VLR	Visitor Location Register
WAP	Wireless Application Protocol

2. G-CDR. Deze gegevens worden aangemaakt door de GGSN voor elke datasessie (PDP context). De velden zijn vrijwel dezelfde als die van de S-CDR.
3. M-CDR. Dit zijn gegevens omtrent het mobiliteitsgedrag van het mobiele toestel, aangemaakt door de SGSN. Een beperkte verzameling van velden, grotendeels vergelijkbaar met die van de S-CDR.

Daarnaast zijn er nog twee groepen CDR's die specifiek zijn voor het zenden, respectievelijk ontvangen van SMS berichten. De velden in deze CDR's komen sterk overeen met die in de vorige sets. In de volgende sets wordt echter ook de MSISDN ('het telefoonnummer') van de abonnee en die van het SMC-service-center opgenomen:

4. S-SMO-CDR en
5. S-SMT-CDR.

## **PUBLIEKRECHTELIJKE BESCHERMING VAN VERKEERSGEGEVENS**

*Anton Ekker\**

### **1 INLEIDING**

Deze bijdrage behandelt de bescherming van verkeersgegevens door het recht op eerbiediging van de persoonlijke levenssfeer en het communicatiegeheim op Europees en nationaal niveau. Op Europees niveau komt art. 8 EVRM aan de orde, dat het recht op respect voor correspondentie beschermt. Vervolgens wordt aandacht besteed aan de bescherming van verkeersgegevens in de ISDN richtlijn<sup>27</sup> en de nieuwe richtlijn inzake privacy en elektronische communicatie.<sup>28</sup> Op nationaal niveau vallen verkeersgegevens onder de algemene privacybescherming van artikel 10 Grondwet. Over de vraag of zij ook zouden moeten vallen onder het communicatiegeheim, zoals gewaarborgd in artikel 13 Grondwet, bestaat onduidelijkheid. De discussie hierover zal aan een analyse worden onderworpen. Daarna zal de verhouding met het begrip 'persoonsgegevens' in de Wbp worden bekeken. Allereerst wordt echter ingegaan op de vraag wat men precies onder verkeersgegevens moet verstaan en wat de relatie is met de privacy van individuen.

### **2 VERKEERSGEGEVENS, EEN DEFINITIE**

De grondrechtelijke bescherming van verkeersgegevens werd relevant toen in de tweede helft van de vorige eeuw de telefonie als massacommunicatiemiddel opkwam en overheden telefoongesprekken in het belang van de opsporing van strafbare feiten en de nationale veiligheid op steeds grotere schaal gingen afluisteren. De eerste uitspraken van het Europese Hof voor de Rechten van de Mens over 'metering records' zien alleen op eenvoudige gegevens als het gekozen telefoonnummer en tijdstip en duur van ieder gesprek. Inmiddels is het aantal verschillende communicatietechnieken en de hoeveelheid aan gegevens die bij communicatie wordt gegenereerd aanzienlijk toegenomen. Voor een grondige beschouwing over de status van verkeersgegevens is het

\* Mr. A. H. Ekker is projectonderzoeker bij het Instituut voor Informatierecht (IViR) van de Universiteit van Amsterdam.

<sup>27</sup> Richtlijn 97/66/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de telecommunicatiesector, *PbEG* 1997 L 24/1.

<sup>28</sup> Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie *PbEG* 2002 L 201/37.

daarom nodig goed af te bakenen welke categorieën van gegevens precies als verkeersgegevens kunnen worden aangemerkt. Hieronder wordt een aantal definities aan een analyse onderworpen.

Laten we beginnen bij de ISDN richtlijn. Volgens artikel 6 lid 1 moeten “verkeersgegevens met betrekking tot abonnees en gebruikers die worden verwerkt om oproepen tot stand te brengen en die worden opgeslagen door degene die een openbaar telecommunicatienetwerk en/of een algemeen beschikbare telecommunicatiedienst verzorgt bij beëindiging van de oproep worden gewist of anoniem gemaakt.” Uit dit artikel blijkt dat van een verkeersgegeven in ieder geval sprake is indien: (1) het gaat om gegevens met betrekking tot abonnees en gebruikers, (2) die zijn verwerkt om oproepen tot stand te brengen en (3) worden opgeslagen door de aanbieder van het netwerk of de dienst. Een gegeven kan echter ook in andere situaties een verkeersgegeven zijn. Het gaat hier immers om een omschrijving van verkeersgegevens die moeten worden gewist; niet van verkeersgegevens als zodanig. Blijkens artikel 11.5 van de Telecommunicatiewet (Tw) was het de bedoeling van de wetgever om de betekenis van het begrip op nationaal niveau verder uit te werken. Dit artikel bepaalt dat aanbieders van openbare telecommunicatienetwerken en -diensten bij beëindiging van iedere oproep dienen te zorgen voor verwijdering of anonimisering van “bij algemene maatregel van bestuur aan te wijzen verwerkte verkeersgegevens met betrekking tot abonnees en gebruikers”. De algemene maatregel van bestuur is tot op heden echter nog niet gepubliceerd.<sup>29</sup>

De nieuwe richtlijn betreffende privacy en elektronische communicatie biedt meer houvast. Deze richtlijn werd op 12 juli 2002 aangenomen en dient voor 31 oktober 2003 te worden omgezet in nationaal recht.<sup>30</sup> Verkeersgegevens worden hier in artikel 2 sub b gedefinieerd als “gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronische-communicatienetwerk of voor de facturering ervan.” Deze omschrijving is beter toegesneden op de informatiesamenleving. De definitie beoogt een techniekonafhankelijke regulering van zowel circuitgeschakelde als pakketgeschakelde communicatie. Het belang van datatransmissie via het Internet is tegenwoordig immers minstens even groot als dat van de klassieke telefonie.<sup>31</sup> De richtlijn spreekt daarom van “het overbrengen van communicatie” in plaats

<sup>29</sup> Schmidt e.a. 2001, p. 180.

<sup>30</sup> Artikel 17 lid 1 van Richtlijn 2002/58/EG.

<sup>31</sup> Toelichting bij het voorstel voor Richtlijn 2002/58/EG, p. 3.

van het “tot stand brengen van oproepen”. Voor de afbakening van het begrip verkeersgegevens wordt in artikel 2 sub b één criterium gehanteerd. Dit is het doel waarvoor de gegevens zijn verwerkt, te weten het overbrengen van communicatie of facturering. Overweging 15 van de richtlijn vult het begrip verkeersgegevens verder in:

*Een communicatie kan naamgevings-, nummerings- of adresseringsgegevens omvatten die door de verzender van een communicatie of door de gebruiker van een verbinding worden verstrekt om de communicatie tot stand te brengen. Wanneer deze gegevens door het netwerk waarover de communicatie wordt doorgegeven, worden omgezet om de transmissie tot stand te brengen, behoren zij ook tot de verkeersgegevens. Verkeersgegevens kunnen o.a. gegevens zijn met betrekking tot de routing, de duur, het tijdstip of het volume van een communicatie, het gebruikte protocol, de lokatie van de eindapparatuur van de verzender of de ontvanger, het netwerk waarop de communicatie begint of eindigt, het begin, het einde of de duur van de verbinding; ze kunnen ook bestaan in het formaat waarin een communicatie door het netwerk wordt overgebracht.*

Ook het Cybercrime verdrag<sup>32</sup> geeft een definitie van verkeersgegevens. Dit verdrag heeft als doel de bestrijding van strafbare feiten via computersystemen en netwerken. Artikel 1 sub d omschrijft verkeersgegevens als “alle computergegevens die verband houden met communicatie door middel van een computersysteem, voortgebracht door een computersysteem dat onderdeel vormde in de ketting van communicatie, die de herkomst van de communicatie, de bestemming, de route, de tijd, de datum, de grootte, de duur of het type van de onderliggende dienst aangeven.” Met de herkomst wordt verwezen naar het telefoonnummer, Internet Protocol (IP) adres of gelijksoortige identificatie van een communicatiefaciliteit waaraan een ISP een dienst verleent. De bestemming duidt op de gelijksoortige identificatie van de communicatiefaciliteit waarheen de boodschap wordt getransporteerd. Voorbeelden van typen van onderliggende diensten zijn elektronische mail, overdracht van een dossier of ‘instant messaging’.<sup>33</sup> De definitie is uitputtend bedoeld. Deze omschrijving is vanuit de doelstellingen van het verdrag logischerwijs beperkt tot computergegevens die zijn voortgebracht en worden getransporteerd door een computersysteem. Hoe het vereiste dat een gegeven ‘verband met communicatie’ moet hebben moet worden geïnterpreteerd wordt in het verdrag niet aangegeven.

<sup>32</sup> Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, *Trb.* 2002, 18.

<sup>33</sup> Zie Final Draft Explanatory Report to the Convention on Cybercrime, nr. 30.

De definitie van verkeersgegevens in de richtlijn betreffende privacy en elektronische communicatie is het duidelijkst en in de praktijk ook het meest van belang. In nationale regelgeving over de verwerking van verkeersgegevens zal immers deze definitie worden gehanteerd. De opsommingen in de richtlijn en het Cybercrime verdrag verschaffen vervolgens meer zekerheid over de vraag welke categorieën van gegevens precies als verkeersgegevens moeten worden aangemerkt. Deze opsommingen overlappen elkaar gedeeltelijk. Beide definities noemen de routing van de communicatie, de duur, het tijdstip en het volume of de grootte van de communicatie. De definitie van het Cybercrime verdrag is beperkt tot computergegevens en minder uitgebreid, maar bevat toch een aantal elementen die in de richtlijn niet voorkomen, zoals herkomst en bestemming. Deze moeten in de richtlijn waarschijnlijk geacht worden deel uit te maken van het begrip ‘routing.’ Het Cybercrime verdrag noemt ook datum (dat zou men onder het begrip ‘tijdstip’ kunnen brengen) en het type van de onderliggende dienst. De opsomming in de toelichting van de richtlijn is blijkens de woorden ‘onder andere’ niet uitputtend bedoeld.<sup>34</sup>

De genoemde categorieën kunnen worden onderverdeeld aan de hand van het doel waarvoor zij worden verzameld of het object waar zij betrekking op hebben. De nieuwe richtlijn onderscheidt drie doelen, te weten: (1) het mogelijk maken van de transmissie, (2) facturering en (3) het verlenen van toegevoegde waarde-diensten. Wat betreft het object van de gegevens zou men een ruw onderscheid kunnen maken tussen (1) algemene gegevens over het communicatiegedrag van de gebruiker, (2) gegevens over het transport en (3) gegevens over de vorm waarin de informatie wordt getransporteerd. De geschetste onderverdeling is schematisch weergegeven in tabel 1. Bij beide indelingen moet men overigens in gedachten houden dat het zeer vaak voorkomt dat één bepaald verkeersgegeven tegelijkertijd in meerdere categorieën kan worden ingedeeld en dat de verwerking van een bepaalde categorie meerdere doelen kan hebben. In de linkerkolom van het schema komt ‘de lokatie van de eindapparatuur’ bijvoorbeeld zowel voor onder ‘transmissie’ als onder ‘toegevoegde waarde-dienst.’ Tevens is de afbakening van de verschillende categorieën in veel gevallen niet geheel duidelijk (hoe zit het bijvoorbeeld met gegevens over bezochte websites en klikgedrag?). Dit is geen probleem zolang maar vaststaat dat het om een verkeersgegeven gaat en er geen verschil in beschermingsniveau bestaat tussen de verschillende categorieën.

<sup>34</sup> Met name van gegevens over Internetverkeer zoals bijvoorbeeld login-gegevens bezochte websites en aangeklikte links, is onduidelijk onder welke categorie van verkeersgegevens zij vallen.

Dit brengt ons op een ander punt. Men zou tussen de verschillende soorten verkeersgegevens ook een onderscheid kunnen maken op grond van privacygevoeligheid. In dat geval kan men betogen dat sommige verkeersgegevens meer bescherming verdienen dan andere. Prins betoogt dat men het adagium dat wet- en regelgeving techniekonafhankelijk dienen te zijn moet loslaten voor het veiligstellen van privacybelangen. Het bewaren van gegevens over mobiele communicatie levert naar haar oordeel namelijk veel meer privacygevoelige informatie op dan het vastleggen van verkeersgegevens met betrekking tot vaste communicatie.<sup>35</sup>

Doel van de verwerking	Object van het verkeersgegeven
<p>- <i>Transmissie</i></p> <p>De lokatie van de eindapparatuur, herkomst en bestemming, routing, het netwerk waarop de communicatie begint en eindigt.</p>	<p>- <i>Algemeen</i></p> <p>Duur, tijdstip (begin en einde), datum, de lokatie van de eindapparatuur, het type van de onderliggende dienst.</p>
<p>- <i>Facturering</i></p> <p>Duur, tijdstip (begin en einde), datum, herkomst en bestemming, het netwerk waarop de communicatie begint en eindigt, volume, de lokatie van de eindapparatuur, het type van de onderliggende dienst.</p>	<p>- <i>Routing</i></p> <p>Herkomst en bestemming, het netwerk waarop de communicatie begint en eindigt.</p> <p>- <i>Vorm en omvang</i></p> <p>Volume (grootte), het gebruikte protocol, het formaat.</p>
<p>- <i>Toegevoegde waarde-dienst</i></p> <p>De lokatie van de eindapparatuur.</p>	

Tabel 1

<sup>35</sup> Prins 2002, p. 322.

### 3 LOKATIEGEGEVENS

Een bijzondere categorie van verkeersgegevens zijn de zogenaamde ‘lokatiegegevens.’ Het is zinvol om aan deze gegevens bijzondere aandacht te besteden aangezien sommige locatiegegevens wel en andere niet als verkeersgegevens worden aangemerkt. Artikel 2 sub c van de richtlijn privacy en elektronische communicatie verstaat onder locatiegegevens “gegevens waarmee de geografische positie van de eindapparatuur van een gebruiker van een algemeen beschikbaar elektronische-communicatiedienst wordt aangegeven”.<sup>36</sup> Lokatiegegevens worden in digitale mobiele netwerken verwerkt om de transmissie van de communicatie mogelijk te maken. Een belangrijk verschil met (andere) verkeersgegevens is dat locatiegegevens niet alleen betrekking kunnen hebben op het communicatie-gerelateerd gedrag van de gebruiker maar ook op zijn feitelijk gedrag op momenten dat er niet wordt gecommuniceerd (waar is iemand en in welke richting en met welke snelheid verplaatst hij zich). Lokatiegegevens kunnen blijkens overweging 14 van de richtlijn verwijzen naar:

*de breedte, de lengte en de hoogte van de eindapparatuur van de gebruiker, de reisrichting, de nauwkeurigheidsgraad van de locatiegegevens, de identificatie van de netwerkcel waarin de eindapparatuur zich op een bepaald tijdstip bevindt, en het tijdstip waarop de locatiegegevens zijn opgeslagen.*

Blijkens de definitie van verkeersgegevens in artikel 2 sub b van de richtlijn kunnen locatiegegevens slechts als verkeersgegevens worden aangemerkt voor zover zij zijn verwerkt voor het overbrengen van communicatie of voor facturering. Deze zinsnede roept vragen op. Wat is bijvoorbeeld de status van locatiegegevens die worden gegenereerd wanneer de eindapparatuur op stand-by staat? Men zou kunnen stellen dat deze locatiegegevens niet worden verwerkt voor ‘het overbrengen van communicatie’, maar om contact te houden met het netwerk. De richtlijn geeft echter nergens uitsluitel over de vraag of deze gegevens verkeersgegevens zijn en of zij onder het communicatiegeheim vallen.

Artikel 9 van de richtlijn ziet op “andere locatiegegevens dan verkeersgegevens die betrekking hebben op gebruikers of abonnees van elektronische communi-

<sup>36</sup> Lokatiegegevens worden alleen gegenereerd bij vormen van mobiele communicatie. Bij vaste telefonie is de plaats waar de eindgebruikers zich bevinden immers te achterhalen via de abonneegegegevens van de gebruiker op wiens naam het nummer geregistreerd staat. Het adres van de abonnee is doorgaans ook de plaats waar de aansluiting zich bevindt.

catienetwerken of -diensten”. Het gaat hier om locatiegegevens die nauwkeuriger zijn dan nodig is voor de transmissie van de communicatie en die worden gebruikt voor het aanbieden van diensten met toegevoegde waarde.<sup>37</sup> Voorbeelden zijn geïndividualiseerde verkeersinformatie en geleidingsdiensten voor bestuurders. Deze ‘andere’ gegevens mogen slechts worden verwerkt wanneer zij anoniem zijn gemaakt of wanneer de gebruikers of abonnees daarvoor hun toestemming hebben gegeven, voor zover en voor zolang zulks nodig is voor de levering van een dienst met toegevoegde waarde. Gebruikers moeten bovendien de mogelijkheid hebben om op eenvoudige wijze de verwerking van locatiegegevens kosteloos tijdelijk uit te schakelen. Deze locatiegegevens zijn geen verkeersgegevens.

### 4 VERKEERSGEGEVENS EN PRIVACY

Waarom zijn verkeersgegevens eigenlijk privacygevoelig? Het antwoord op deze vraag houdt verband met de mogelijkheid om verkeersgegevens te koppelen aan andere feitelijke gegevens en persoonsgegevens. Zodoende kan men veel te weten komen over het communicatiegedrag van personen, hun feitelijk handelen en soms ook over de inhoud van de communicatie. Er zijn globaal drie stadia te onderscheiden:

1. *‘Ruwe’ verkeersgegevens:* de gegenereerde gegevens bevinden zich in het systeem van de transporteur maar zijn nog niet gekoppeld aan persoonsgegevens. Zij kunnen betrekking hebben op alle objecten die zijn weergegeven in de rechterkolom van tabel 1.
2. *Verwerkte verkeersgegevens:* de verkeersgegevens zijn gekoppeld aan identificerende gegevens, bijvoorbeeld voor het doeleinde van facturering. Nu zeggen ze iets over het (communicatie)gedrag van een bepaalde zender en ontvanger. De nummers of adressen staan immers op naam van bepaalde personen. Voorbeelden:
  - Alice heeft Bob om zes uur ’s avonds opgebeld.
  - Alice heeft Bob om tien uur ’s ochtends een e-mail gestuurd.
  - Alice en Bob hebben van 2 tot 3 uur ’s middags samen deelgenomen aan een chat-sessie.

<sup>37</sup> Zie overweging 35 van Richtlijn 2002/58/EG.

In het geval van mobiele communicatie is bovendien te achterhalen vanaf welke plaats is gecommuniceerd:

- Alice heeft Bob om 3 uur 's middags opgebeld vanaf Den Haag Centraal Station, terwijl Bob zich bevond op het Museumplein te Amsterdam en zich verplaatste richting het Leidseplein.
3. *Verkeersgegevens gecombineerd met andere gegevens*: de verwerkte verkeersgegevens worden gecombineerd met aanvullende informatie over zender of ontvanger. Soms kan zodoende worden vastgesteld wat (ongeveer) de inhoud van de communicatie is geweest:
- Alice heeft gebeld met haar advocaat, haar psycholoog, het ziekenhuis, de nummerinformatie van de PTT, de Sociale Dienst, het Bureau Kredietregistratie, of het alarmnummer van de brandweer.
  - Alice heeft ingelogd op de website van Alcoholics Anonymous en deelgenomen aan een chatsessie.
  - Alice heeft ingelogd op de website van de gemeente Amsterdam en op een bulletin-board kritiek geuit op het parkeerbeleid van de gemeente.
  - Alice heeft van de website van een politieke partij het partijprogramma gedownload en een folder besteld waarmee zij lid kan worden van die partij.

Geconcludeerd moet worden dat verkeersgegevens twee dingen doen. Ten eerste koppelen zij communicatie en communicatiehandelingen via identificerende gegevens aan personen. Daarnaast kunnen verkeersgegevens iets zeggen over de inhoud van communicatie wanneer men ze combineert met andere informatie. Hieruit volgt een belangrijke constatering: informatie over het communicatiegedrag van individuen en soms ook de inhoud van de communicatie kan worden verkregen door verkeers- en persoonsgegevens met elkaar te combineren. Onder omstandigheden kan dit in strijd komen met het recht op eerbiediging van de persoonlijke levenssfeer. Dit probleem kan men oplossen door de betreffende verkeers- of persoonsgegevens te wissen of door anonimiseren: door er voor te zorgen dat zij niet meer met elkaar in verband gebracht kunnen worden.

## 5 BESCHERMING VAN VERKEERSGEGEVENS DOOR ARTIKEL 8 EVRM EN DE RICHTLIJN BETREFFENDE PRIVACY EN ELEKTRONISCHE COMMUNICATIE

### 5.1 Jurisprudentie

Een belangrijke garantie voor de vertrouwelijkheid van verkeersgegevens is gelegen in artikel 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM). Dit artikel beschermt het recht van een ieder op eerbiediging van zijn privé-leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.<sup>38</sup> In de uitspraak *Klass* bepaalde het Europese Hof dat onder het begrip 'correspondentie' naast briefwisseling, ook telefoonverkeer valt.<sup>39</sup> Later werden in *Malone* ook de 'metering records' en het gekozen telefoonnummer onder de bescherming van artikel 8 gebracht. Het ging daar om registratie van gekozen nummers, tijdstip en duur van ieder gesprek. Naar het oordeel van het Hof bevatten deze 'metering records' informatie die een integraal deel uitmaakt van de telefonische communicatie. Afgifte van deze gegevens door de telefoonmaatschappij aan de politie zonder toestemming van de betrokkene werd in strijd met artikel 8 bevonden.<sup>40</sup> In de zaak *P.G. and J.H. v. The United Kingdom* maakt het Hof onderscheid tussen het onderscheppen van communicatie enerzijds en het registreren van gesprekken anderzijds. Dat laatste is niet in strijd met artikel 8 EVRM wanneer het bijvoorbeeld wordt gedaan door telefoonmaatschappijen teneinde rekeningen te kunnen opstellen.<sup>41</sup>

### 5.2 De richtlijn

De uitspraken van het Europese Hof hebben betrekking op klassieke telefonie en geven dan ook geen antwoord op vragen die modernere communicatietechnieken oproepen. Wel hebben zij invloed gehad op de bescherming van verkeersgegevens in de nieuwe richtlijn. Het EVRM en de grondrechten die daarin zijn opgenomen worden immers gezien als fundamentele rechtsbeginselen die indirect doorwerken in de rechtsorde van de Europese Unie. Artikel 5 van de richtlijn zegt over verkeersgegevens het volgende:

<sup>38</sup> De volledige Nederlandse tekst van artikel 8 EVRM artikel luidt: '1. Een ieder heeft recht op respect voor zijn privé leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie. 2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.'

<sup>39</sup> EHRM 6 september 1978, AA 1979, p. 327-334 (*Klass*).

<sup>40</sup> EHRM 2 augustus 1984 (*Malone*), NJ 1988, 534, § 83 en 84.

<sup>41</sup> EHRM 25 september 2001 (*P.G. en J.H. v. The United Kingdom*), NJB 2001-42, p. 2051. Zie ook Asscher 2002, p. 133.

*De lidstaten garanderen via nationale wetgeving het vertrouwelijke karakter van de communicatie en de daarmee verband houdende verkeersgegevens via openbare communicatienetwerken en via openbare elektronische communicatiediensten. Zij verbieden met name het afluisteren, aftappen, opslaan of anderszins onderscheppen of controleren van de communicatie en de daarmee verband houdende verkeersgegevens door anderen dan de gebruikers.*

Uit deze tekst blijkt dat verkeersgegevens bescherming verdienen. Er wordt echter niet expliciet gesteld dat verkeersgegevens onder het communicatiegeheim vallen. Overweging 26 van de richtlijn biedt meer duidelijkheid:

*de gegevens over abonnees die in elektronische-communicatienetwerken worden verwerkt om verbindingen tot stand te brengen en informatie over te dragen, bevatten informatie over het privé-leven van natuurlijke personen en betreffen het recht op respect voor hun correspondentie of de rechtmatige belangen van rechtspersonen.*

Naast de gewijzigde definitie bevat de richtlijn op een tweetal punten wijzigingen die gevolgen zullen hebben voor regelgeving over verkeersgegevens op nationaal niveau. De eerste wijziging betreft artikel 6 van de richtlijn dat in zijn geheel is gewijzigd aan verkeersgegevens. Het derde lid van dit artikel bepaalde in de oude richtlijn dat de verstrekker van een algemeen beschikbare telecommunicatiedienst voor de verkoop van eigen telecommunicatiediensten bepaalde verkeersgegevens mag verwerken mits de abonnee daarmee heeft ingestemd. Hetzelfde geldt nu ook voor verwerking van verkeersgegevens ten behoeve van de levering van diensten met toegevoegde waarde. Bovendien mogen ook gegevens van andere gebruikers dan abonnees worden verwerkt. Ten slotte is nu bepaald dat men de toestemming voor de verwerking te allen tijde in kan trekken. Daarnaast is een vierde lid ingevoegd dat bepaalt dat dienstenaanbieders abonnees en gebruikers in kennis moet stellen van de soorten verkeersgegevens die worden verwerkt en van de duur van de verwerking voor facturering, interconnectiebetaling en de doelen van het derde lid.

De tweede wijziging is de in artikel 15 geïntroduceerde mogelijkheid voor de lidstaten om wetgevingsmaatregelen te treffen die telecomaandieners verplichten om (verkeers)gegevens gedurende een beperkte periode te bewaren. Deze wijziging heeft nogal wat stof doen opwaaien. Voor een bespreking van deze wijziging verwijs ik naar de bijdrage van Bert-Jaap Koops.

## **6 BESCHERMING VAN VERKEERSGEGEVENS OP NATIONAAL NIVEAU: ARTIKEL 10 EN 13 GRONDWET, DE WET BESCHERMING PERSOONS- GEGEVENS EN DE TELECOMMUNICATIEWET**

### **6.1 Bescherming door artikel 10 en 13 Grondwet**

Hoewel verkeersgegevens op Europees niveau worden beschermd door het recht op eerbiediging van de persoonlijke levenssfeer, bestaat over de grondwettelijke status op nationaal niveau nog onduidelijkheid. Een belangrijk twistpunt betreft de vraag of zij dienen te vallen onder de algemene privacybescherming van artikel 10 Grondwet of tevens onder de meer specifieke bescherming van het communicatiegeheim in artikel 13 Grondwet. Het laatste artikel biedt een sterkere bescherming aangezien het telefoon- en telegraafgeheim in het tweede lid alleen kan worden geschonden “in gevallen bij de wet bepaald, door of met machtiging van hen die daartoe bij de wet zijn aangewezen.”<sup>42</sup> Artikel 10 Grondwet beschermt verkeersgegevens alleen voor zover zij als persoonsgegevens kunnen worden aangemerkt.<sup>43</sup>

Het antwoord hangt onder andere af van de manier waarop men het communicatiegeheim opvat. In de visie van het kabinet Kok II en de commissie ‘Grondrechten in het Digitale Tijdperk’<sup>44</sup> heeft het huidige artikel 13 Grondwet alleen betrekking op de inhoud van communicatie.<sup>45</sup> Verkeersgegevens zouden daarom alleen de bescherming van artikel 10 Grondwet verdienen. Dommering en Asscher brengen hiertegen in dat men het communicatiegeheim dient te interpreteren als een transportgeheim. Dit geheim

<sup>42</sup> Artikel 13 Grondwet luidt: 1. Het briefgeheim is onschendbaar, behalve, in de gevallen bij de wet bepaald, op last van de rechter. 2. Het telefoon- en telegraafgeheim is onschendbaar, behalve, in de gevallen bij de wet bepaald, door of met machtiging van hen die daartoe bij de wet zijn aangewezen.

<sup>43</sup> Artikel 10 Grondwet luidt: 1. Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer. 2. De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens. 3. De wet stelt regels inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens.

<sup>44</sup> Deze commissie, ook wel bekend als de commissie Franken, werd door de regering ingesteld om te adviseren over de gevolgen van nieuwe informatie- en communicatietechnologie voor de grondrechten.

<sup>45</sup> *Kamerstukken II 1996/97, 25 443, B, nr. 3, p. 3*: ‘Verkeersgegevens [...] verschillen fundamenteel van het type informatie dat verkregen wordt bij de interceptie van de inhoud van vertrouwelijke communicatie en vallen op grond van hun aard reeds niet onder dit begrip.’; Nota naar aanleiding van het nader verslag bij het wetsvoorstel voor de Wet op de inlichtingen- en veiligheidsdiensten 2002 (WIV 2002), *Kamerstukken II 1999/2000, 25 877, nr. 14, p. 35*: ‘van een inbreuk op het telefoongeheim is [sprake], indien het kennis nemen van de inhoud van een telefoongesprek gericht is op de inhoud zelf. Indien van de inhoud van een telefoongesprek kennis wordt genomen louter als kortstondig onderdeel van een onderzoek naar de identiteit van de personen of instellingen die met elkaar communiceren, zien wij dat niet als inbreuk op het telefoongeheim. Het is veeleer vergelijkbaar met een onderzoek naar verkeersgegevens. Een dergelijk onderzoek is wel te beschouwen als een inbreuk op het recht op privacy, zoals vastgelegd in artikel 10 van de Grondwet, doch niet als een inbreuk op het in artikel 13 van de Grondwet vastgelegde telefoongeheim’; zie ook Ekker 2002.

beschermt de verzender van een boodschap tegen kennisneming van de inhoud door de transporteur of door hen die via de transporteur toegang tot de boodschap zouden kunnen hebben. Het gaat daarbij niet om de inhoud van de boodschap maar om de vertrouwelijkheid van het communicatiekanaal.<sup>46</sup> Gegevens over het gebruik van dat kanaal vallen ook onder de bescherming aangezien de verzameling van deze gegevens de vrije communicatie belemmert.<sup>47</sup>

## 6.2 Een nieuw artikel 13 Grondwet

In haar voorstel voor een nieuw artikel 13 Grondwet wijst de commissie ‘Grondrechten in het Digitale Tijdperk’ de bescherming van verkeersgegevens af. Voor dit standpunt brengt zij, naast de hierboven genoemde argumenten, twee nieuwe argumenten naar voren.<sup>48</sup> In de eerste plaats wordt gewezen op een verschil tussen de bescherming van het voorgestelde artikel 10 en het voorgestelde artikel 13: artikel 10 laat beperkingen toe bij of krachtens de wet terwijl artikel 13 een rechterlijke last vereist. In de huidige redactie van artikel 13 Grondwet speelt dit probleem niet. Het vereiste van een rechterlijke last zou in verband met nieuwe strafvorderlijke wetgeving zoals de Wet bijzondere opsporingsbevoegdheden leiden tot een onwerkbare situatie, aldus de commissie. Het zou daarom de voorkeur verdienen verkeersgegevens onder artikel 10 Grondwet te brengen. Hier wordt het lagere beschermingsniveau van artikel 10 Grondwet dus juist als argument gebruikt om verkeersgegevens niet onder artikel 13 Grondwet te laten vallen.

Dit lijkt een onjuiste benadering. De vraag of verkeersgegevens onder de werkingssfeer van artikel 13 vallen dient men te beantwoorden op basis van de inhoud en betekenis van het communicatiegeheim. Als een rechterlijke last voor verkeersgegevens niet werkbaar is kan men dat ook oplossen door voor deze gegevens in artikel 13 Grondwet een apart regime te scheppen.<sup>49</sup> In haar preadvies inzake de wijziging van artikel 13 Grondwet deed de VMC studiec ommissie voorstellen voor een nieuwe tekst waarin is voorzien in een “enigszins mildere beperkingsclausulering” voor ‘transportgegevens’. In dit voorstel kan de vertrouwelijkheid van de transportgegevens worden beperkt in de gevallen

<sup>46</sup> Dommering 1997.

<sup>47</sup> Hofman 1995, p. 4-5; Dommering e.a. 1999, p. 71-72; Asscher 2000; Asscher 2002, p. 24.

<sup>48</sup> Commissie Grondrechten in het Digitale Tijdperk 2000, p. 137, 159-160 en 232-233; zie ook het standpunt van het kabinet op het advies van de commissie ‘Grondrechten in het Digitale Tijdperk’, *Kamerstukken II* 2000/2001, 27 460, nr. 1, p. 27.

<sup>49</sup> Zie in deze zin ook Dommering 1997.

bij de wet bepaald door of met machtiging van hen die daartoe bij de wet zijn aangewezen.<sup>50</sup>

Het tweede argument is dat:

*verkeersgegevens weliswaar in de informatiesamenleving veel over personen kunnen zeggen, maar dat datzelfde geldt voor veel meer gevoelige gegevens, die ook niet onder de werking van artikel 13 vallen. Er zijn geen goede argumenten aan te voeren om een onderscheid aan te brengen in het grondwettelijke beschermingsniveau tussen categorieën persoonsgegevens op grond van het feit dat zij al dan niet gerelateerd zijn aan een inhoud die zelfstandig grondwettelijke bescherming geniet. De Commissie licht nog toe dat persoonsgegevens omtrent iemands medische gesteldheid – ook erfelijke gegevens – niet door het recht op onaantastbaarheid van het menselijk lichaam (artikel 11 van de Grondwet) worden beschermd, doch eveneens door artikel 10 van de Grondwet.*

Ook dit argument snijdt om een aantal redenen geen hout. Wanneer men uitgaat van de bescherming van het kanaal wordt het onderscheid immers niet aangebracht op grond van het feit dat verkeersgegevens gerelateerd zijn aan een inhoud die zelfstandig grondwettelijke bescherming verdient. Bovendien gaat de analogie met medische gegevens mank. Niet alle grondrechten hoeven op exact dezelfde manier te worden afgebakend. Over de vraag of medische gegevens onder artikel 11 Grondwet horen te vallen is daarnaast nooit een uitgebreide discussie gevoerd. Men zou ook als volgt kunnen redeneren: wanneer men twijfelt over de grondwettelijke kwalificatie van een bepaalde categorie gegevens, dient men te kiezen voor de kwalificatie die de burger het meeste bescherming biedt. In de verhouding tussen het algemene artikel 10 Grondwet en het op communicatie toegespitste artikel 13 Grondwet voorziet artikel 13 in een meer specifieke en met meer waarborgen omklede bescherming.

De constitutionele status van verkeersgegevens blijft hoe dan ook onduidelijk. Over het voorstel voor het nieuwe artikel 13 Gw zijn grote meningsverschillen en het is de vraag op welke termijn dit voorstel zal worden aangenomen. Zoals Dommering opmerkt zal Nederland op grond van de richtlijn privacy en elektronische communicatie in haar wetgeving vooralsnog een beschermingsniveau dienen te verzekeren dat de Commissie Digitale Grondrechten op grondwettelijk niveau niet nodig vindt.<sup>51</sup>

<sup>50</sup> Studiec ommissie VMC 1999.

<sup>51</sup> Dommering 2001.

### 6.3 Bescherming van verkeersgegevens in de Wet bescherming persoonsgegevens en de Telecommunicatiewet

Op wettelijk niveau zijn voor de bescherming van verkeersgegevens de Wet bescherming persoonsgegevens (Wbp) en de Telecommunicatiewet (Tw) van belang. De Wbp is op verkeersgegevens van toepassing voor zover deze kunnen worden aangemerkt als persoonsgegevens en stelt algemene regels over verwerking. Deze verwerking is alleen toegestaan indien zij kan worden gebaseerd op een van de verwerkingsgronden van artikel 8 Wbp. Artikel 9 en 10 Wbp geven vervolgens regels over de verdere verwerking en het bewaren van persoonsgegevens (zie de bijlage). De Telecommunicatiewet stelt in hoofdstuk 11 regels over persoonsgegevens en de persoonlijke levenssfeer. Artikel 11.5 Tw is een telecomspecifieke uitwerking van artikel 10 Wbp en ziet alleen op het bewaren van verkeersgegevens in niet-geanonimiseerde vorm. Dit artikel bepaalt dat aanbieders van openbare telecommunicatienetwerken en -diensten bij beëindiging van ‘iedere oproep’ zorg dienen te dragen voor de verwijdering of de anonimisering van bij AMvB aan te wijzen verkeersgegevens. Hiervan kan op grond van in het tweede lid opgesomde gronden worden afgeweken (zie tevens de bijlage). Voorbeelden zijn het opstellen van een nota, het doen van marktonderzoek, verkoopactiviteiten, verkeersbeheer en het verstrekken van inlichtingen aan klanten.

De verhouding tussen Wbp en Telecommunicatiewet roept de vraag op in hoeverre de begrippen ‘persoonsgegeven’ en ‘verkeersgegeven’ elkaar overlappen en in welke gevallen verkeersgegevens ook persoonsgegevens zijn. Zwenne constateert dat deze begrippen in twee opzichten van elkaar afwijken.<sup>52</sup> In de eerste plaats zeggen verkeersgegevens alleen iets over het feitelijk gebruik van een netwerk, terwijl persoonsgegevens in principe betrekking kunnen hebben op ieder aspect van een persoon. Art. 1, onder a, van de Wbp definieert persoonsgegevens immers als “alle gegevens die in verband staan met geïdentificeerde of identificeerbare natuurlijke personen.” In dat opzicht is de reikwijdte van het begrip persoonsgegeven dus ruimer. Daar staat tegenover dat verkeersgegevens zowel betrekking kunnen hebben op natuurlijke en rechtspersonen, terwijl persoonsgegevens alleen betrekking hebben op natuurlijke personen. Rechtspersonen kunnen dus geen aanspraak maken op bescherming van hun verkeersgegevens als persoonsgegevens.<sup>53</sup> De geschetste overlapping is

<sup>52</sup> Zwenne 2000, p. 153.

<sup>53</sup> Volgens Zwenne gaat het om een beperkte categorie van gegevens waarvan het gebruik bij overeenkomst kan worden geregeld. Zie Zwenne 2000, p. 155.

hieronder weergegeven in tabel 2, ontleend aan Zwenne.

Verkeersgegevens (art. 11.5 Tw)	Persoonsgegevens (art. 1, onder a, Wbp)
Feitelijk gebruik van netwerk	Alle aspecten van een persoon
Natuurlijke en rechtspersonen	Alleen natuurlijke personen

Tabel 2

Verkeersgegevens zijn dus persoonsgegevens wanneer zij een verband hebben met geïdentificeerde of identificeerbare natuurlijke personen.<sup>54</sup> In de Memorie van Toelichting bij de Wbp wordt deze eis nader toegelicht. Of gegevens informatie over een persoon behelzen moet blijken uit de aard van de gegevens of anders uit de context waarin het gegeven wordt vastgelegd en gebruikt. Hiervoor kan van belang zijn of de gegevens bepalend zijn voor de wijze waarop de betrokken persoon wordt beoordeeld of behandeld. Van identificeerbaarheid is sprake wanneer de identiteit van een persoon redelijkerwijs, zonder onevenredige inspanning, kan worden vastgesteld. Bij het beoordelen van de identificeerbaarheid spelen naast de aard van de gegevens de mogelijkheden van de verantwoordelijke om identificatie tot stand te brengen een rol.

Sciarone-Gorgels constateert dat de kwalificatie van verkeersgegevens als persoonsgegevens afhangt van de context waarin de verkeersgegevens gebruikt worden en van de relatie tussen de betrokken persoon en de verantwoordelijke. Zo zijn verkeersgegevens die worden vastgelegd voor het doeleinde van facturering bepalend voor de wijze waarop de betrokken persoon wordt behandeld. De rekening wordt immers op basis van deze gegevens opgesteld. Deze verkeersgegevens zijn daarom aan te merken als persoonsgegevens. Een telefoonnummer is volgens Sciarone-Gorgels daarentegen niet altijd een persoonsgegeven. Het nummer heeft immers als primaire functie het identificeren van de telefoonaansluiting en ook anderen dan de abonnee zelf kunnen hiervan gebruik maken. Daarnaast kan men zich afvragen of verkeersgegevens voor

<sup>54</sup> Kamerstukken II 1997/98, 25 892, nr. 3, p. 46-48.

facturering ook persoonsgegevens zijn van de abonnee van de *opgeroepen* aansluiting. De opgeroepene zal immers meestal geen effect ondervinden van het verwerken van zijn nummer en vaak zal hij niet of moeilijk identificeerbaar zijn voor het telecommunicatiebedrijf dat de rekening opstelt.<sup>55</sup> Aan de door Sciarone-Gorgels gegeven voorbeelden kan men toevoegen dat ook verkeersgegevens die uitsluitend worden gebruikt om het goed functioneren van een netwerk te waarborgen geen persoonsgegevens zijn zolang elke reële mogelijkheid is uitgesloten dat hiermee het communicatiegedrag van individuen in kaart wordt gebracht.<sup>56</sup>

## 7 CONCLUSIE

Uit het voorgaande kunnen drie conclusies worden getrokken. In de eerste plaats is de definitie van het begrip verkeersgegevens in de richtlijn betreffende privacy en elektronische communicatie niet geheel duidelijk. Dit is met name het geval waar het gaat om lokatiegegevens die worden gegenereerd wanneer het mobiele toestel in de stand-by stand staat.

De tweede conclusie betreft de grondwettelijke status van verkeersgegevens. De analyse van de richtlijn en het standpunt van het kabinet Kok II en de commissie 'Grondrechten in het Digitale Tijdperk' onthult een discrepantie op het punt van de interpretatie van het communicatiegeheim. Waar in de richtlijn verkeersgegevens onder dit geheim bescherming vinden, wijzen kabinet en commissie bescherming door artikel 13 Grondwet af.

Ten slotte dient aandacht te worden besteed aan een betere onderlinge afbakening van de begrippen 'verkeersgegeven' en 'persoonsgegeven.'

<sup>55</sup> Sciarone-Gorgels 1999, p. 197-198.

<sup>56</sup> Prins & Berkvens 2002, p. 418.

## LITERATUURLIJST

### Asscher 2000

L.F. Asscher, 'Trojaans hobbelpaard, een analyse van het rapport van de commissie Grondrechten in het Digitale Tijdperk', Mediaforum 2000-7/8, p. 228-233.

### Asscher 2002

L.F. Asscher, *Communicatiegrondrechten. Een onderzoek naar de constitutionele bescherming van het recht op vrijheid van meningsuiting en het communicatiegeheim in de informatiesamenleving*, Amsterdam: Otto Cramwinckel Uitgever 2002.

### Commissie Grondrechten in het Digitale Tijdperk 2000

Commissie Grondrechten in het Digitale Tijdperk, *Rapport*, Den Haag, 2000; zie [http://www.minbzk.nl/gdt/artikelen/rapport\\_gdt\\_5-00.pdf](http://www.minbzk.nl/gdt/artikelen/rapport_gdt_5-00.pdf).

### Dommering 1997

E.J. Dommering, 'Een grondrecht op vertrouwelijke communicatie', gepubliceerd onder de titel 'Geen telefoongeheim op de elektronische snelweg', Mediaforum 1997-10, p.142-147.

### Dommering e.a. 1999

E.J. Dommering e.a., *Handboek telecommunicatierecht. Inleiding tot het recht en de techniek van de telecommunicatie*, Den Haag: SDU Uitgevers 1999.

### Dommering 2000

E.J. Dommering, 'De nieuwe Nederlandse Constitutie en de informatietechnologie', *Computerrecht* 2000-4, p. 177-185.

### Dommering 2001

E.J. Dommering, 'De Nieuwe Brusselse Telecommunicatierichtlijnen', *Computerrecht* 2001-1, p. 4-10.

### Ekker 2002

A.H. Ekker, 'Het onderscheppen van telecommunicatie door de inlichtingen- en veiligheidsdiensten', *Computerrecht* 2002-2, p. 77-83.

**Hofman 1995**

J.A. Hofman, *Vertrouwelijke communicatie. Een rechtsvergelijkende studie over de geheimhouding van communicatie in grondrechtelijk perspectief naar internationaal, Nederlands en Duits recht* (diss. Amsterdam VU), Zwolle: Tjeenk Willink 1995.

**Prins 2002**

J.E.J. Prins, 'Wapenwedloop in cyberspace. Gegevensmunitie ten koste van privacy?', *Ars Aequi* 2002/5, p. 315-323.

**Prins & Berkvens 2002**

J.E.J. Prins & J.M.A. Berkvens, *Privacyregulering in theorie en praktijk*, Deventer: Kluwer 2002.

**Sciarone-Gorgels 1999**

G.N.M. Sciarone-Gorgels, 'Hoofdstuk 11 van de Telecommunicatiewet. Rijp voor revisie?', *Privacy en Informatie* 1999/5, p. 196-204.

**Schmidt e.a. 2001**

A.H.J. Schmidt e.a., *Telecommunicatiewet: de tekst van de Telecommunicatiewet voorzien van commentaar met toevoeging van aanverwante nationale en Europese regelgeving*, Deventer: Kluwer, 2001.

**Studiecommissie VMC 1999**

Studiecommissie VMC, 'Preadvis inzake een nieuwe tekst voor de artikelen 7 en 13 van de Grondwet', *Mediaforum* 1999-11/12, p. i-viii.

**Zwenne 2000**

G.J. Zwenne, 'Verkeersgegevens in de Telecommunicatiewet en de Wet bescherming persoonsgegevens', *Mediaforum* 2000/5, p. 154-157.

**VERKEERSGEGEVENS EN STRAFRECHT:  
EEN AGENDA VOOR DISCUSSIE**

*Bert-Jaap Koops\**

**1 INLEIDING**

Het opvragen van verkeersgegevens is een belangrijke opsporingsbevoegdheid, die volop in beweging is. Hoewel de bevoegdheid ooit terloops is ingevoerd en lange tijd als ondergeschikt werd gezien aan de bevoegdheid tot het tappen van telefoons, is het inmiddels een zelfstandige bevoegdheid geworden, met een eigen waarde voor de strafvordering. Momenteel wordt de strafrechtelijke regeling herzien en worden discussies gevoerd over een mogelijke bewaarplicht van verkeersgegevens. Het begrip 'verkeersgegevens' komt overigens niet voor in het Wetboek van Strafvordering; de wetgever hanteert de omschrijving "inlichtingen terzake van alle verkeer dat over een openbaar telecommunicatienetwerk, dan wel met gebruikmaking van openbare telecommunicatiediensten, heeft plaatsgevonden."

In deze bijdrage geef ik een overzicht van de belangrijkste discussiepunten die bij de huidige ontwikkelingen een rol (zouden moeten) spelen, waarbij ik me concentreer op de wettelijke regeling; aan de praktijk kan ik in dit bestek geen aandacht besteden. Daarbij ga ik vooral in op de voorwaarden waaronder de bevoegdheid mag worden ingezet, aangezien deze bepalen in hoeverre justitie inbreuk mag maken op de privacy in dezen, en op het object van de bevoegdheid, aangezien de vraag welke gegevens vallen onder de verkeersgegevensbevoegdheid evenzeer relevant is voor de mogelijke privacyinbreuk door justitie. Na een overzicht van de historische context, ga ik in op de voorwaarden waaronder de bevoegdheid mag worden ingezet, het object van de bevoegdheid en een bewaarplicht voor verkeersgegevens. Bij de analyse betrek ik steeds het geldende recht en de voorgestelde regelingen. Terzijde noem ik nog de regeling van het opvragen van verkeersgegevens door inlichtingen- en veiligheidsdiensten, maar ik ga daar niet diep op in.

\* Dr. E.J. Koops (1967) werkt als universitair hoofddocent aan het CRBI van de Universiteit van Tilburg en houdt zich vooral bezig met privacy en informatietechnologie.

## NAWOORD

### Verkeersgegevens: een onderzoeksagenda

Uit het verslag van de discussie tijdens de workshop “verkeersgegevens” van 6 september 2002 en uit de in dit boekje opgenomen artikelen is een aantal algemene conclusies te trekken. In de eerste plaats is gebleken dat verkeersgegevens zowel technisch als juridisch een lastig definieerbaar begrip vormen. Tegelijkertijd kan worden vastgesteld dat het belang van verkeersgegevens voor opsporing, privacy en communicatiegeheim dusdanig is dat een publieke discussie over de beschermingswaardigheid van die gegevens noodzakelijk is. We zagen verschillende voorbeelden van het belang van verkeersgegevens voor opsporing, de privacygevoeligheid van dergelijke gegevens en de invloed van nieuwe technologieën op de rol van verkeersgegevens. Gebleken is dat er drie zaken spelen, technische aspecten, juridische aspecten, maar ook praktische vragen (wie doet wat, wie betaalt). Tijdens de discussie van 6 september ontstond op sommige vragen wel al het begin van een antwoord.

Hieronder formuleren we een aantal vraagstellingen die ons inziens op de agenda van de publieke discussie thuishoren. Daaruit blijkt dat de discussie over verkeersgegevens zowel binnen de (juridische) wetenschap als elders gevoerd dient te worden.

1. Inhoud versus verkeersgegeven. Een vraag die telkens in de discussie terugkeert is of differentiatie in beschermingsniveau mogelijk is. Daarvoor moet het onderscheid tussen inhoud en verkeersgegevens in de praktijk wel gemaakt kunnen worden. Zowel in de discussie over de technische aspecten van verkeersgegevens als in de juridische debatten worden vraagtekens geplaatst bij de wenselijkheid om nog onderscheid te maken tussen de inhoud van communicatie en de verkeersgegevens.
2. Een andere belangrijke vraag betreft de huidige en toekomstige status van een aantal specifieke groepen gegevens zoals de ‘subject line’ van een email of de bezochte webadressen en de omgang met zoekvragen. Hoe je die informatie, die in technische zin tot de verkeersgegevens behoort, maar die in feite veel over de inhoud vertelt, dient te behandelen, is in toenemende mate onduidelijk.
3. Een vraag met betrekking tot de toekomstige rol van de verkeersgegevens is die naar de betekenis van verticale en horizontale netwerkintegratie. Tij-

dens de workshop werd vastgesteld dat er sprake is van een sterke integratie tussen de verschillende communicatieprocessen en actoren. In sommige gevallen zullen verkeersgegevens bij één partij pas betekenis krijgen (informatie worden) indien ze gecombineerd worden met die van andere partijen in de keten. Dit betekent dat de beschikkingsmacht over de verkeersgegevens enerzijds bij zeer veel verschillende partijen komt te liggen maar dat het anderzijds door de veelheid van betrokken partijen moeilijk is één verantwoordelijke aan te wijzen.

4. Een vraagstuk dat met de vorige vraag samenhangt is wie bij verkeersgegevens de *verantwoordelijke* is. Wie kan worden aangesproken op het al dan niet wissen of bewaren van deze gegevens? Wie moet worden gezien als de voornaamste verwerker van verkeersgegevens in de zin van de Wet bescherming persoonsgegevens? Moet de verantwoordelijkheid worden toegerekend aan bepaalde spelers of worden gedeeld? Helderheid hierover is van groot belang voor de aansprakelijkheid van tussenpersonen, voor de handelswijze van operators en voor de positie van de telecomconsument.
5. Belangrijke vervolgvraag in het debat over verkeersgegevens is de vraag in hoeverre er bij het opvragen van die gegevens sprake is van een opsporingsbevoegdheid die het klassieke tappen steeds meer zal gaan vervangen. En als dat zo is, welke consequenties zou dit dan moeten hebben voor het beschermingsniveau van verkeersgegevens in bijvoorbeeld de Grondwet en het Wetboek van Strafvordering? In welke fase van het strafonderzoek worden de verkeersgegevens eigenlijk opgevraagd? Gaat het om de fase van het Gerechtelijk Vooronderzoek of bevinden we ons in een voorfase waarin de verkeersgegevens vooral nuttig zijn voor het uitvoeren van ‘visexpedities’?
6. Een vraag die nauw samenhangt met de opvraagbevoegdheid van verkeersgegevens is die naar de wenselijkheid van een bewaarplicht. In hoeverre is het invoeren van een ruime bewaarplicht een trendbreuk in ons systeem van strafvordering? Verdient de elektronische wereld een dergelijke uitzonderingspositie? En is een dergelijke bewaarplicht uitvoerbaar in toekomstige systemen?
7. Bij de bespreking van de publiekrechtelijke aspecten kwam de verhouding tussen verkeersgegeven en persoonsgegeven aan de orde. Het is duidelijk dat hier geen eenvoudige één op één relatie bestaat. Vraag is in hoeverre de definitie van een persoonsgegeven kan samenvallen met die van een ver-

keersgegevens en wat dit vervolgens betekent voor de daadwerkelijke bescherming van verkeersgegevens op grond van de WBP of anderszins.

8. De positie van het bedrijfsleven dient eveneens meer belicht te worden. Op wie worden de kosten van een eventuele bewaarplicht afgewenteld? Wat betekent een algemene bewaarplicht voor de verhouding tussen bedrijfsleven en strafvorderlijke overheid? Kan het bedrijfsleven worden verplicht ook bewerkingen uit te voeren op de bestanden met gegevens die men geacht wordt te bewaren?
9. De lokatiegegevens vormen een geheel eigen categorie van verkeersgegevens. Zelfs de vraag of het hier gaat om verkeersgegevens is niet eenvoudig te beantwoorden. Als privacygevoeligheid een factor is bij de beoordeling van het beschermingsniveau van verschillende categorieën verkeersgegevens, hoe moeten we dan de lokatiegegevens inschatten? Vooral de situatie waarbij niet gecommuniceerd wordt, terwijl het toestel wel aan is (en dus stand-by staat) is relevant. Enerzijds kan in dat geval niet worden gesteld dat het lokatiegegeven tevens een verkeersgegeven is daar niet wordt voldaan aan de (gangbare) definities van het verkeersgegeven. Anderzijds moge duidelijk zijn dat de vastlegging van de route van de houder van het mobiele toestel toch grote gevolgen voor de privacy van de gebruiker heeft. Overigens heeft ook de EU-regelgever ingezien dat dit punt grote aandacht verdient.

Deze en andere vragen dienen op korte termijn te worden beantwoord om op een zinvolle wijze te discussiëren over de bescherming en de opsporing van verkeersgegevens en om te zorgen voor een goed begrip van verkeersgegevens in de toekomst.

## LIJST VAN DEELNEMERS AAN DE WORKSHOP VERKEERSGEGEVENS 6 september 2002

Marijn Artz	O2 (Netherlands) BV
Lodewijk Asscher	Instituut voor Informatierecht
Ruud Beugelsdijk	College Bescherming Persoonsgegevens
Jan Willem Broekema	College Bescherming Persoonsgegevens
Rob Dielemans	Ministerie van V&W
Egbert Dommering	Instituut voor Informatierecht
Frans van den Dool	Verdonck, Klooster & Associates
Nico van Eijk	Instituut voor Informatierecht
Anton Ekker	Instituut voor Informatierecht
Hans Fischer	Technische Universiteit Delft
Eric-Jan van Goor	OPTA
Marian Grubben	Europese Commissie – DG Informatiemaatschappij
Ronald Hes	Lucent Technologies
Bernard Hulsman	College Bescherming Persoonsgegevens
Peter Hustinx	College Bescherming Persoonsgegevens
Marleen Jongeneel	Ministerie van Justitie
Jan Kabel	Instituut voor Informatierecht
Hans Keijzer	Vodafone
Bert-Jaap Koops	Katholieke Universiteit Brabant – Centrum voor Recht, Bestuur en Informatisering
Hans Leemans	NLIP – Branchevereniging Nederlandse Internet Providers
Natascha Linssen	OPTA
Luit Lous Mol	Ministerie van Justitie
Edwin Mac Gillavry	Rijksuniversiteit Groningen
Sjoera Nas	XS4ALL Internet BV
Arno van Oosterhout	Ministerie van Justitie – DG politie
Jacques Penders	KPN
Maurice Wessling	Bits of Freedom