De Wet bewaarplicht telecommunicatiegegevens

310

Onderzoek en beleid

De Wet bewaarplicht telecommunicatiegegevens

Over het bewaren en gebruiken van gegevens over telefoon- en internetverkeer ten behoeve van de opsporing

G. Odinot

D. de Jong

R.J. Bokhorst

C.J. de Poot

BOOM | LEMMA UITGEVERS

Wetenschappelijk Onderzoek- en Documentatiecentrum
Ministerie van Veiligheid en Justitie

Onderzoek en beleid

De reeks Onderzoek en beleid omvat de rapporten van onderzoek dat door en in opdracht van het WODC is verricht.
Opname in de reeks betekent niet dat de inhoud van de rapporten het standpunt van de Minister van Veiligheid en Justitie weergeeft.

Exemplaren van dit rapport kunnen worden besteld bij het distributiecentrum van Boom Lemma uitgevers:
Boom distributiecentrum te Meppel
Tel. 0522-23 75 55
Fax 0522-25 38 64
E-mail budh@boomdistributiecentrum.nl

Voor ambtenaren van het Ministerie van Veiligheid en Justitie is een beperkt aantal gratis exemplaren beschikbaar.
Deze kunnen worden besteld bij:
Bibliotheek WODC
Postbus 20301, 2500 EH Den Haag
Deze gratis levering geldt echter slechts zolang de voorraad strekt.

De integrale tekst van de WODC-rapporten is gratis te downloaden van www.wodc.nl.
Op www.wodc.nl is ook nadere informatie te vinden over andere WODC-publicaties.

ISBN 978-94-6236-041-9
ISBN 978-94-6094-919-7 (e-book)
NUR 820

Voorwoord

In september 2009 is, in navolging van de Europese Richtlijn Dataretentie, de Wet bewaarplicht telecommunicatiegegevens van kracht geworden in Nederland. Met deze wet wordt gewaarborgd dat telecommunicatiegegevens die van belang kunnen zijn voor de opsporing en vervolging van strafbare feiten voor een bepaalde periode worden opgeslagen en daarmee beschikbaar zijn voor opsporingsonderzoek naar ernstige misdrijven.
De Europese Richtlijn is niet in alle lidstaten positief ontvangen. Hoewel het evident is dat historische gegevens over telefoon- en internetverkeer van belang kunnen zijn voor de opsporing, vormt het feit dat deze privacygevoelige gegevens hiertoe standaard voor een bepaalde periode moeten worden opgeslagen een terugkerend punt van discussie.
Door de enorme vlucht die het gebruik van mobiele telefoons en smartphones heeft genomen, is de bruikbaarheid van telecommunicatiegegevens voor de opsporing in de afgelopen jaren sterk toegenomen. Zo geven analyses van telecommunicatieverkeer vaak een goed beeld van de handel en wandel van mensen. Daarmee is echter ook de privacygevoeligheid van deze gegevens toegenomen, en wordt met het opslaan van deze gegevens een grotere inbreuk gemaakt op de privacy van burgers dan vroeger het geval was. Het is daarom van belang om te onderzoeken op welke wijze telecommunicatiegegevens die op grond van de dataretentiewet beschikbaar moeten blijven voor de opsporing worden opgeslagen, bewaard, beveiligd en vernietigd en hoe op dit proces wordt toegezien. Daarnaast is het van belang om inzicht te krijgen in de wijze waarop deze gegevens in de opsporingspraktijk worden gebruikt. Wanneer en door wie kunnen de opgeslagen gegevens worden opgevraagd en op welke wijze kunnen deze gegevens bijdragen aan de opsporing en vervolging van misdrijven?

In dit rapport wordt een breed beeld geschetst van de wijze waarop de Wet bewaarplicht is vormgegeven en van de manier waarop de opgeslagen gegevens gebruikt worden in de opsporingspraktijk. Hiertoe is met een veertigtal professionals gesproken en is gebruikgemaakt van verschillende andere databronnen. Mede namens de auteurs dank ik alle personen die door hun medewerking aan de interviews, het verlenen van toegang tot gegevens en het verstrekken van informatie hebben bijgedragen aan dit onderzoek. Daarnaast gaat onze dank uit naar Nora Al Haider en Priya Soekhai die geholpen hebben bij het scoren van data en naar Ruud Kouwenberg voor zijn hulp bij het uitwerken van interviews. Tot slot gaat onze dank uit naar de leden van de begeleidingscommissie (zie bijlage 1), die met hun kritische vragen en hun zorgvuldige commentaar op de geschreven teksten een waardevolle bijdrage hebben geleverd aan dit onderzoek.

Prof. dr. F.L. Leeuw
Directeur WODC

Inhoud

Afkortingen

AIVD	Algemene Inlichtingen- en Veiligheidsdienst
AT	Agentschap Telecom
BOB	Bijzondere Opsporingsbevoegdheden
BoF	Bits of Freedom
BVH	Basisvoorziening Handhaving
BVO	Basisvoorziening Opsporing
CBP	College Bescherming Persoonsgegevens
CBS	Centraal Bureau voor de Statistiek
CIE	Criminele Inlichtingen Eenheid
CIOT	Centraal Informatiepunt Onderzoek Telecommunicatie
CvPG's	College van procureurs-generaal
DCS	Digitale Communicatie Sporen
EDPS	European Data Protection Supervisor
EHRM	Europese Hof voor de Rechten van de Mens
EVRM	Europees Verdrag voor de Rechten van de Mens
FIOD	Fiscale Inlichtingen- en Opsporingsdienst
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
JBZ-raad	Raad Justitie en Binnenlandse Zaken
IP	Internet Protocol
ISP	Internet Service Provider
ITU	International Telecommunication Union
KLPD	Korps Landelijke Politiediensten
MIVD	Militaire Inlichtingen- en Veiligheidsdienst
MvT	Memorie van Toelichting
NAT	Network Address Translation
NAW	Naam, Adres en Woonplaats
NFI	Nederlands Forensisch Instituut
NMa	Nederlandse Mededigingsautoriteit
OM	Openbaar Ministerie
OPTA	Onafhankelijke Post en Telecommunicatie Autoriteit
OvJ	officier van justitie
RC	rechter-commissaris
SIM	Subscriber Identity Module
Sv.	Wetboek van Strafvordering
TGO	Team Grootschalig Onderzoek
TNO	Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek
Tw	Telecommunicatiewet
ULI	Unit Landelijke Interceptie
VoIP	Voice over IP
WBP	Wet Bescherming Persoonsgegevens
WOB	Wet Openbaarheid van Bestuur
WODC	Wettenschappelijk Onderzoek- en Documentatiecentrum
zwacri	zware criminaliteit

Samenvatting

Het onderzoek: aanleiding, onderzoeksvragen en gegevensverzameling

Aanleiding en de onderzoeksvragen

De Wet bewaarplicht telecommunicatiegegevens, is op 1 september 2009 in werking getreden. De centrale gedachte achter de bewaarplicht is dat bepaalde gegevens over telefoon- en internetverkeer van belang kunnen zijn voor de opsporing en vervolging van ernstige misdrijven. Men kan met behulp van die gegevens bijvoorbeeld vaststellen op welk moment en op welke locatie met een bepaalde (mobiele) telefoon is gebeld. Ook is het mogelijk te achterhalen of en wanneer een computer of mobiele telefoon contact heeft gehad met het internet. In geval van een misdrijf waarvoor voorlopige hechtenis is toegestaan, bij een redelijk vermoeden dat misdrijven worden beraamd of gepleegd in georganiseerd verband en bij aanwijzingen van een terroristisch misdrijf, kan een vordering tot verstrekking van verkeersgegevens worden gedaan.
Het feit dat deze gegevens standaard voor een bepaalde periode moeten worden opgeslagen is echter een terugkerend punt van discussie. Zowel in Nederland als op Europees niveau (EU 18620/11) bestaat behoefte aan meer inzicht in het gebruik door politie en justitie van de gegevens die op grond van de Nederlandse Wet bewaarplicht worden opgeslagen.

Het doel van dit onderzoek is inzicht te bieden in de wijze waarop de Wet bewaarplicht uitwerkt in de praktijk. Strikt genomen vormt dit onderzoek geen evaluatie van de Wet bewaarplicht. Het onderzoek reikt verder dan een procesevaluatie (vgl. Wartna, 2005; Nelen et al., 2010), omdat er niet alleen behoefte bestaat aan inzicht in de wijze waarop de Wet bewaarplicht in de praktijk heeft vorm gekregen, maar vooral ook aan inzicht in de wijze waarop de gegevens die op grond van deze wet beschikbaar dienen te worden gehouden voor de opsporing in de praktijk worden gebruikt.
Het is echter niet mogelijk om – zoals het geval is bij een product- of effectevaluatie – vast te stellen wat de effecten zijn van de invoering van de Wet bewaarplicht het gebruik van verkeersgegevens in de opsporingspraktijk. De telecommuncatiegegevens waar het hier om draait waren ook vóórdat de Wet bewaarplicht werd ingevoerd beschikbaar voor de opsporing en werden ook vóór de invoering van de wet bewaarplicht gebruikt in strafrechtelijke onderzoeken naar ernstige misdrijven.
De Wet bewaarplicht heeft weliswaar geleid tot harmonisatie van de bewaartermijnen, maar doordat er in de tussentijd ook andere veranderingen zijn opgetreden zijn de effecten daarvan nauwelijks te meten én te onderscheiden. Veranderingen in de wijze waarop telecommuncatiegegevens in de praktijk worden gebruikt zijn vooral toe te schrijven aan de opkomst van de mobiele telefoon en de smartphone en aan de mogelijkheden om via het internet met elkaar te communiceren. Het is daarom wel mogelijk om te

onderzoeken op welke wijze telecommunicatiegegevens gebruikt worden in de opsporingspraktijk, maar het is niet goed mogelijk deze bevindingen te relateren aan de invoering van de nieuwe wet.
Dit onderzoek richt zich zowel op vragen over de wijze waarop de wet is vormgegeven als op vragen over het gebruik van de opgeslagen gegevens in de praktijk.

Bij het bewaren, beschikbaar houden en gebruiken van gegevens over telefoon- en internetverkeer ten behoeve van de opsporing en vervolging zijn verschillende organisaties en partijen betrokken. De aanbieders dienen de te bewaren gegevens op te slaan, te beveiligen, beschikbaar te stellen voor de opsporing, en tijdig weer te vernietigen. Het Agentschap Telecom ziet toe op dit proces. Het College Bescherming Persoonsgegevens heeft de algemenere taak toe te zien op het gebruik van privacygevoelige gegevens. Politie en Openbaar Ministerie maken gebruik van deze gegevens bij het opsporen en vervolgen van ernstige misdrijven, en de Zittende Magistratuur gebruikt de gegevens in de rechtelijke besluitvorming. In dit rapport wordt relatief veel aandacht besteed aan de wijze waarop de bewaarde gegevens gebruikt worden in de praktijk om daarmee inzicht te bieden in de nut en noodzaak van de bewaarplicht. De wijze waarop de Wet bewaarplicht uitwerkt in de praktijk vormt een ingewikkeld bouwwerk, dat in dit rapport weergegeven wordt door de wijze waarop deze verschillende partijen hun taken uitvoeren te beschrijven. In dit rapport wordt relatief veel aandacht besteed aan de wijze waarop de bewaarde gegevens gebruikt worden in de praktijk. Andere partijen worden belicht, maar vormen niet het zwaartepunt van dit onderzoek.

Gegevensverzameling

Om antwoord te kunnen geven op de onderzoeksvragen zijn verschillende methoden gebruikt. Naast de bestudering van nationale en internationale vakliteratuur, is kwantitatieve en kwalitatieve informatie verzameld over het gebruik van historische verkeersgegevens. Hierover zijn gegevens verzameld bij onder andere de Unit Landelijke Interceptie (ULI) van de landelijke politie eenheid, de politie, de rechterlijke macht (Openbaar Ministerie) en de advocatuur. Tevens is literatuuronderzoek verricht waarbij wetteksten en toelichtingen daarop, lagere regelgeving, Kamerstukken, schriftelijke stukken van uitvoeringsinstanties en wetenschappelijke literatuur zijn bestudeerd.
Voor het onderzoek zijn 17 face-to-face interviews en 16 telefonische interviews afgenomen, waarbij is gesproken met in totaal 41 personen in de periode lopend van juni tot oktober 2012. Daarnaast zijn vonnissen geanalyseerd om te bezien op welke wijze gegevens die op grond van de Wet bewaarplicht beschikbaar worden gehouden voor de opsporing door Nederlandse rechters gebruikt worden in de bewijsvoering van strafzaken.

Communicatie op afstand, ontwikkelingen en gevolg

De mobiele telefoon werd in de afgelopen jaren vervangen door de smartphone, en veel mensen zijn tegenwoordig 24 uur per dag, zeven dagen per week, online. Door het gebruik van smartphones wordt er steeds vaker gecommuniceerd in de vorm van korte berichtjes via apps en e-mail en bellen mensen ook steeds vaker via internet.
Technologische vernieuwingen, de daarmee gepaard gaande versnippering van communicatie en vooral het gebruik van verschillende diensten die op internet worden aangeboden, maken dat het moeilijk is om alle communicatie op afstand van een persoon in kaart te brengen. Bovendien vallen niet alle verkeersgegevens die daarbij worden gegenereerd onder de Nederlandse Wet bewaarplicht. Veel internetgebruikers hebben een e-mailaccount bij webmaildiensten zoals Hotmail, Gmail of Yahoo, waarvan de aanbieder een buitenlands bedrijf is. Dit betekent dat de gegevens niet per definitie beschikbaar worden gehouden voor de Nederlandse opsporing. Ditzelfde geldt vaak voor aanbieders van diensten in de *cloud*. Indien opsporingsdiensten toch willen beschikken over verkeersgegevens van buitenlandse aanbieders zal men een rechtshulpverzoek moeten indienen en moeten afwachten of de gevraagde gegevens nog beschikbaar zijn.

De wetsgeschiedenis en Europese regelgeving inzake de bewaarplicht van verkeersgegevens

Mede aangejaagd door de terroristische aanslagen in Madrid in 2004 en in Londen in 2005, is op 3 mei 2006 de EU-richtlijn in werking getreden die tot doel heeft te waarborgen dat bepaalde telecom- en internetgegevens bewaard blijven zodat deze beschikbaar zijn voor het onderzoeken, opsporen en vervolgen van ernstige criminaliteit.

Te bewaren data

In artikel 5 van de richtlijn worden de te bewaren categorieën gegevens genoemd die betrekking hebben op bijvoorbeeld de bestemming, de datum, het tijdstip en duur van de communicatie. Er mogen geen gegevens worden bewaard waaruit de inhoud van de communicatie kan worden opgemaakt. De lidstaten dienden de richtlijn vóór 15 september 2007 in wetgeving te hebben omgezet; voor de bewaringsverplichting van internetgegevens was er respijt tot 15 maart 2009. Niet alle lidstaten hebben de richtlijnen inmiddels omgezet in wetgeving. De term ‘ernstige criminaliteit’ is in de richtlijnen niet gedefinieerd. Dit is terug te zien in de verschillende gronden die in de wetgeving van de lidstaten zijn opgenomen die toegang tot de bewaarde gegevens voor strafvorderlijke doeleinden mogelijk maken. Evenals voor de duur

van de bewaartermijn, geldt hier dat de harmonisatie die met de EU-regelgeving is nagestreefd, slechts beperkt is verwezenlijkt.

Privacy

De Wet bewaarplicht raakt aan de privacy van de burgers. Allereerst neemt door het louter opslaan van telecommunicatiegegevens het risico toe dat onbevoegden – zoals hackers – toegang krijgen tot die gegevens. Een tweede en andersoortige inbreuk vindt plaats op het moment dat politie en justitie de beschikking krijgen over bewaarde gegevens in het kader van een onderzoek. Een beperking op het recht op privacy is volgens het Europees Verdrag tot bescherming van de rechten van de mens (EVRM) pas dan toegestaan als deze bij wet is voorzien en noodzakelijk is in een democratische samenleving.
In het Wetboek van Strafvordering (Sv.) is geregeld wie onder welke voorwaarden toegang heeft tot de opgeslagen telecom- en internetgegevens. De officier van justitie kan een vordering doen tot verstrekking van verkeersgegevens (art. 126n en 126u Sv.) ingeval van verdenking van een misdrijf waarvoor voorlopige hechtenis mogelijk is of bij een redelijk vermoeden dat in georganiseerd verband misdrijven worden beraamd of gepleegd. Een opsporingsambtenaar kan identificerende gegevens vorderen (art. 126na, 126ua Sv.). De gegevens die opgevraagd kunnen worden zijn de zogenaamde gebruikersgegevens (naam, adres, woonplaats, nummer en soort dienst). Ingeval van aanwijzingen van een terroristisch misdrijf kan de officier van justitie verkeersgegevens opvragen (art. 126zh Sv.) en kan een opsporingsambtenaar gebruikersgegevens vorderen (art. 126zi Sv.). Verder kan de officier van justitie bij een verkennend onderzoek naar terroristische misdrijven gegevensbestanden van publieke en particuliere instanties vorderen om de hierin opgenomen gegevens te doen bewerken (art. 126hh Sv.).

Het bewaren en beveiligen van de gegevens in de praktijk

De toezichthouders

Het toezicht op de naleving van de regels ligt in handen van het Agentschap Telecom (AT), dat opereert als een onafhankelijke toezichthouder en toeziet op de naleving van de Wet. Het AT is onderdeel van het ministerie van Economische Zaken, en legt rechtstreeks verantwoording af aan de Minister van Economische Zaken. Daarnaast ziet het College Bescherming Persoonsgegeven (CBP) toe op alle wettelijke regelingen waarin sprake is van het bewaren, gebruiken of verwerken van persoonsgegevens.

De aanbieders

Om te begrijpen hoe de aanbieders omgaan met de verplichtingen die de Wet bewaarplicht met zich meebrengt, is gesproken met vier aanbieders. Voor de invoering van de bewaarplicht liepen de bewaartermijnen tussen bedrijven uiteen. De implementatie van de wet bewaarplicht vormde ondanks de lange aanlooptijd van de wet bij de grote aanbieders een omvangrijk project.
Bij de twee grote aanbieders die zijn geïnterviewd voor dit onderzoek, wordt een database gevuld met gegevens die op grond van de Wet bewaarplicht dienen te worden bewaard. Deze gegevens worden automatisch vernietigd na het verstrijken van de bewaartermijn. Een kleine aanbieder die werd geïnterviewd voor dit onderzoek, is pas recentelijk actief met de bewaartermijnen aan de slag gegaan, omdat de hoeveelheid te beheren gegevens te groot werd. Wanneer een verzoek bij hun binnenkomt worden de gevraagde gegevens door een medewerker handmatig uit het systeem gehaald.
De overheid heeft een overeenkomst afgesloten met de grote Nederlandse aanbieders betreffende de vergoeding van de personele inzet die nodig is om op grond van verschillende wetten en regels opgeslagen gegevens aan de overheid te verstrekken. Kleine aanbieders vallen niet onder deze regeling.
De eigenaren van een vierde geïnterviewde aanbieder herkennen zichzelf wel in de documentatie van het AT als bewaarplichtige van de verkeersgegevens van de e-maildiensten die zij aanbieden, maar geven hieraan vanuit idealistisch standpunt geen gehoor. De onderzoekers hebben de vraag of de diensten die door dit bedrijf worden aangeboden onder de bewaarplicht vallen voorgelegd aan het AT. Volgens het AT is dit niet het geval, maar het AT ziet tegelijkertijd ook dat de wetgeving – als gevolge van technologische vernieuwingen – op bepaalde gebieden onduidelijk is geworden.

Toezichthouder

Op de juiste uitvoering van bedrijfsprocessen wordt toegezien door het AT. Het toezicht is geregeld in een toezichtscyclus, waarbij van de aanbieders gegevens worden opgevraagd over de wijze waarop de te bewaren gegevens worden opgeslagen, beveiligd en vernietigd. Het AT beschikt echter niet over de instrumenten en bevoegdheden om op de inhoud van de bewaarde en geleverde gegevens toe te kunnen zien. In artikel 18.7, tweede lid, van de Telecommunicatiewet (Tw) is uitdrukkelijk bepaald dat de toezichthouder niet bevoegd is verkeers- of locatiegegevens op te vragen die door de aanbieders op grond van artikel 13.2a Tw moet worden bewaard.

Het gebruik van historische verkeersgegevens in de praktijk

In de wet wordt een strikt onderscheid gemaakt tussen telefonie- en internetverkeersgegevens. Voor de duidelijkheid is in dit rapport deze tweedeling gehandhaafd. Echter, in de praktijk is dit onderscheid nagenoeg verdwenen en hanteert de Wet bewaarplicht, volgens experts, een onjuiste tweedeling.

Wat wordt bewaard?

In de bijlage behorende bij artikel 13.2a Tw staat een opsomming van de te bewaren gegevens betreffende telefonie. Het betreft gegevens over onder meer het nummer van oproeper en opgeroepene, tijd, duur van gesprek en locatie. Deze gegevens dienen bewaard te worden voor een periode van 1 jaar. De inhoud van een gesprek of een sms bericht valt niet onder de bewaarplicht. De verkeersgegevens van het verzonden of ontvangen bericht wel. Oproeppogingen waarbij geen contact tot stand is gekomen, vallen wel onder de bewaarplicht.

De inzet

Volgens professionals uit de opsporingspraktijk worden historische verkeersgegevens opgevraagd bij vrijwel alle grotere opsporingsonderzoeken waarbij verdachten of slachtoffers mogelijk gebruik hebben gemaakt van hun telefoon. In het jaar 2012 betrof het aantal vorderingen tot verstrekking van telecommunicatiegegevens 56.825.
Met deze vorderingen wordt informatie opgevraagd over het gebruik van telefoon en eventueel van IP-verkeer, zoals: met welk nummer is er gebeld, wanneer is er gebeld, hoe lang is er gebeld en vanaf welke locatie, en is er contact geweest met het internet? Deze gegevens spelen een belangrijke en zeer gewaardeerde rol in de opsporingspraktijk. Wanneer een opsporingsteam historische verkeersgegevens wil opvragen, dient het team toestemming te hebben van de officier van justitie. Het opsporingsteam moet aangeven welk doel ze met de gevraagde gegevens denken te bereiken en het opvragen van de gegevens dient proportioneel en subsidiair te zijn. De doelstellingen van opsporingsteams voor het opvragen van verkeersgegevens zijn onder te brengen in een aantal algemene categorieën, namelijk: (1) het identificeren van een gebruiker, (2) het achterhalen van contacten, (3) plaatsbepaling, (4) het traceren van een IMEI-nummer, en (5) het maken van een capaciteitsafweging alvorens te gaan tappen.

Relevantie en bewaartermijn telefoniegegevens

Alle geïnterviewde professionals en experts geven aan historische gegevens over telefoonverkeer zeer relevant te vinden. Een aantal geïnterviewde pro-

fessionals uit de opsporingspraktijk geeft aan niet alleen de begin locatie (*first cell*) van een telefoongesprek te willen ontvangen maar ook de eindlocatie (*last cell*). Echter, waar het gesprek eindigt, dus de laatste connectie met een zendmast, staat niet vermeld in de bijlage behorende bij artikel 13.2a Tw.
Tijdens de gesprekken bleek dat het merendeel van de professionals en experts bij de politie van mening is dat de bewaartermijn van een jaar voldoende is voor het werk dat zij doen.

Historische verkeersgegevens Internet

Wat wordt er bewaard?

Historische verkeersgegevens betreffende internet- en e-mail gebruik, kunnen inzicht bieden in onder meer de IP-adressen die door iemand zijn gebruikt, en in de e-mail contacten van zender en ontvanger. De inhoud van gesprekken, berichten of e-mails, zoektermen die zijn intypt in een zoekmachine en IP-adressen van bezochte internetpagina's vallen niet onder de bewaarplicht.

Relatief weinig ingezet

Tijdens de gesprekken die zijn gevoerd voor dit onderzoek werd duidelijk dat de voor dit onderzoek gesproken professionals uit de opsporingspraktijk weinig tot geen kennis hebben over de wijze waarop historische gegevens betreffende het internetverkeer gebruikt zouden kunnen worden in de opsporing. Daarnaast worden werkzaamheden die te maken hebben met aan internet gerelateerde zaken vaak uitgevoerd door experts omdat de digitalisering van de huidige samenleving nog niet behoort niet tot het dagelijkse werkterrein van veel opsporingsambtenaren. Tegelijkertijd constateren we dat de technologische ontwikkelingen heel snel gaan. Zo snel dat het voor de schaarse experts zelf maar met moeite bij te houden is.
Historische gegevens over internetverkeer worden veelal opgevraagd naar aanleiding van een misdrijf of delict dat met behulp van of via het internet is gepleegd zoals bijvoorbeeld het versturen van dreigmails, internetoplichting, mensenhandel of het verspreiden van kinderporno. Het *identificeren van een gebruiker* of van een aansluiting wordt als belangrijkste reden genoemd voor het opvragen van gegevens. Vaste IP-adressen zijn doorgaans langere tijd dezelfde en de gebruiker is eenvoudig te traceren bij de aanbieder of bij het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT). Echter, het identificeren van een gebruiker van mobiel internet door middel van historische verkeersgegevens verloopt moeizaam en is regelmatig niet mogelijk.

De relevantie en bewaartermijn internetgegevens

Volgens verschillende experts is het merendeel van de gegevens betreffende internet zoals beschreven in de bijlage behorende bij artikel 13.2a Tw is verouderd. De regeling past niet meer bij het huidige internet gebruik en bij de technische ontwikkelingen die zich in dit opzicht hebben voorgedaan sinds de invoering van de wet in 2009. Daarmee is een situatie ontstaan waarin gegevens van burgers worden bewaard die niet of nauwelijks worden gebruikt door opsporingsdiensten. Een zorgvuldige heroverweging van de regeling betreffende IP-verkeer en de te bewaren IP-gegevens lijkt dan ook op zijn plaats.
De voor dit onderzoek geïnterviewde professionals en experts die bekend zijn met internetverkeersgegevens zijn allen van mening dat de bewaartermijn van 6 maanden te kort is; er bestaat een duidelijke behoefte aan IP-verkeersgegevens die verder terug gaan in de tijd in opsporingsonderzoeken naar delicten waarvoor deze gegevens worden opgevraagd.

Het opvragen van zendmastgegevens

Het opvragen van verkeersgegevens op basis van een locatie levert gegevens op van alle mobiele telefoons die in het opgevraagde tijdsbestek zijn gebeld, zelf hebben getelefoneerd of connectie hebben gehad met het internet via de bevraagde mastlocatie. Om zendmastgegevens op te kunnen vragen moet er sprake zijn van een verdenking van een misdrijf zoals omschreven in artikel 67, lid 1 Sv. en het moet het gebruik van de gegevens in het belang zijn van het onderzoek.
Zendmastgegevens worden vooral opgevraagd bij seriematige delicten. In dat geval worden de gegevens van verschillende locaties met elkaar vergeleken, in de hoop een terugkerend nummer te kunnen identificeren. Uiteraard kan deze opsporingsmethode alleen slagen als de verdachte zijn telefoon rond het tijdstip van het misdrijf heeft gebruikt.

Alternatief?

Tegenstanders van de bewaarplicht zien het gericht bevriezen van gegevens als een minder privacy schendende oplossing omdat er in dat geval sprake is van een gerichte dataset die langer bewaard wordt in plaats van het bewaren van alle gegevens van alle klanten van een aanbieder. Geen van de sleutelpersonen die wij spraken vindt het bevriezen van gegevens een vergelijkbaar of gelijkwaardig alternatief voor een algemene bewaarplicht, omdat hiermee geen gegevens kunnen worden opgevraagd die langer geleden zijn vastgelegd. Om gebruik te kunnen maken van deze gegevens moet al van tevoren – op het moment dat de gegevens nog aanwezig zijn en bevroren kunnen worden – bekend zijn welke gegevens later nodig zijn. Aangezien misdrijven

soms pas laat ter kennis van de politie komen, en verdachten soms pas lang nadat een misdrijf heeft plaatsgevonden worden opgespoord, is het noodzakelijk gegevens te bewaren om deze later te kunnen gebruiken in het opsporingsproces.

Gebruik van verkeersgegevens in cijfers

In de Telecommunicatiewet is een regel opgenomen over de verplichting tot publicatie van het jaarlijkse aantal bevragingen door opsporingsdiensten van gegevens over telecommunicatieverkeer (art. 13.4 lid 4 Tw). In het jaar 2012 is er in totaal 56.825 keer een vordering gedaan tot verstrekking van verkeersgegevens. Echter, het door de minister bekend gemaakte aantal vorderingen bevat ook gegevens die niet onder de Wet bewaarplicht telecommunicatiegegevens vallen.
Tevens dient te worden opgemerkt dat het opvragen van telecomgegevens in Nederland wordt geregistreerd per telefoonnummer, IMEI-nummer, IP-adres, of 'paallocatie' waarover gegevens worden opgevraagd. Deze cijfers geven geen inzicht in het aantal personen van wie er jaarlijks telecommunicatiegegevens worden opgevraagd, of van het aantal opsporingsonderzoeken of de aard van de opsporingsonderzoeken waarvoor deze gegevens worden opgevraagd. Ook geven de cijfers geen inzicht in de mate waarin een vordering daadwerkelijk tot een verstrekking van de gegevens heeft geleid.

Rechterlijke vonnissen

In dit rapport bieden we ook inzicht in het gebruik en de waarde van verkeersgegevens in rechterlijke vonnissen. In totaal werden er tussen juli 2012 en februari 2013 74 uitspraken gevonden waarin de term historische verkeersgegevens betreffende telefonie voorkwam. In de vonnissen werden deze gegevens vooral gebruikt om 'contacten tussen verdachten' en 'plaatsbepalingen' aan te tonen.
Bij het zoeken naar zaken waarin gegevens over IP-verkeer waren gebruikt in het vonnis kwam een 26-tal uitspraken naar boven uit de periode januari 2009 - februari 2013. Deze IP-gegevens werden vooral genoemd in vonnissen van opsporingsonderzoeken naar kinderporno. Meer dan de helft van de vonnissen gaat over het downloaden/verspreiden van kinderporno. Bij het opvragen van deze gegevens gaat het niet zozeer om waar de verdachte was en met wie er wordt gecommuniceerd, maar om de vraag of de verdachte te koppelen is aan het gebruikte internetadres of aan andere gebruikersgegevens.

1 De Wet bewaarplicht telecommunicatiegegevens – een inleiding

Op 3 mei 2006 is een Europese richtlijn in werking getreden die tot doel heeft te waarborgen dat bepaalde telecommunicatiegegevens bewaard blijven en daarmee beschikbaar zijn voor politie en justitie ten behoeve van opsporingsonderzoeken naar ernstige misdrijven. Deze bewaarplicht van telecommunicatiegegevens geldt voor bedrijven zoals internetaanbieders en telefoonmaatschappijen (hierna ook aanbieders genoemd). Al langer hadden politie en justitie de bevoegdheid om dit type gegevens te vorderen, maar tegelijkertijd hadden bedrijven de verplichting de gegevens te vernietigen wanneer deze niet langer nodig waren voor de eigen bedrijfsvoering.[1] Dit kon betekenen dat opgevraagde gegevens na een bepaalde periode niet meer aanwezig waren. Deze richtlijn bevat bepalingen voor de bewaring en beveiliging van telecommunicatiegegevens, het toezicht daarop en de rechtsbescherming van betrokkenen over en van wie gegevens worden bewaard.
De centrale gedachte achter deze bewaarplicht is dat bepaalde gegevens over telefoon- en computergebruik van belang kunnen zijn voor de opsporing. Met behulp van die gegevens kan bijvoorbeeld worden vastgesteld op welk moment en op welke locatie met een bepaalde (mobiele) telefoon is gebeld. Ook is het mogelijk te achterhalen of en wanneer een computer of mobiele telefoon contact heeft gehad met het internet. Wanneer het een smartphone met mobiel internet betreft, is de locatie van waaruit het dataverkeer heeft plaatsgevonden ook te achterhalen. Daarmee is het veelal mogelijk om achteraf, door het opvragen van die bewaarde gegevens, de gangen van verdachten in een opsporingsonderzoek na te gaan. De periode waarover bedrijven de gegevens dienen op te slaan, kan op basis van de richtlijn variëren van ten minste een halfjaar tot ten hoogste twee jaar. Binnen deze bandbreedte zijn de lidstaten vrij om de duur van de verplichte bewaarperiode te kiezen.
De Dataretentie Richtlijn is niet in alle lidstaten positief ontvangen. Ook in Nederland zijn vragen gesteld over het nut en de noodzaak van deze bewaarplicht. Zo is de vraag of de bewaarplicht wel (voldoende) bijdraagt aan de versterking van de opsporing, expliciet aan de orde gesteld. Ook is de kritiek geuit dat de richtlijn in onevenredige mate de privacy van burgers zou schaden en op gespannen voet zou staan met artikel 8 van de *European Convention on Human Rights* en met artikel 7 van het *Charter of Fundamental Rights of the European Union*.[2] Een en ander heeft ertoe geleid dat in sommige lid-

1 Er bestond wel een beperkte bewaarplicht. Aanbieders hadden de verplichting om de verkeersgegevens van afnemers waarvan geen NAW-gegevens bekend waren (prepaid nummers waarmee anoniem kan worden gebeld) gedurende drie maanden te bewaren.

2 De Europese Toezichthouder Gegevensbescherming noemde de Europese richtlijn 'The most privacy invasive instrument ever adopted by the European Union' (Hustinx, 2010); door Electronic Frontier Foundation wordt de Europese richtlijn gezien als 'The most prominent example of a mandatory data retention framework (www.eff.org, geraadpleegd op 7 december 2012) en Frost en Sullivan (2010, p. 15) omschrijven de Richtlijn als 'the most extensive piece of data retention legislation adopted by any country or Union of countries today' (zie ook Hathaway, 2012, p. 40).

staten, zoals in Zweden en Oostenrijk, de richtlijn niet is omgezet in wetgeving. In Tsjechië, Duitsland en Roemenië hebben de constitutionele hoven de wetgeving ter omzetting van de richtlijn nietig verklaard.[3] In landen waarin die omzetting al wel heeft plaatsgevonden, loopt de duur van de verplichte bewaartermijn sterk uiteen, van een halfjaar tot twee jaar.

Nederlandse wet ter omzetting van de richtlijn

In Nederland is wetgeving van kracht geworden ter omzetting van de Europese richtlijn. Deze Wet bewaarplicht telecommunicatiegegevens, die we in het vervolg aanduiden als de Wet bewaarplicht, is op 1 september 2009 in werking getreden. Zoals gezegd, bestond al langer een wettelijke basis op grond waarvan politie en justitie gegevens konden opvragen over telefoon- en internetverkeer (zogenaamde verkeersgegevens).[4] Door de Wet bewaarplicht is daarin geen wijziging gekomen. In geval van een verdenking van een misdrijf waarvoor voorlopige hechtenis is toegestaan, bij een redelijk vermoeden dat misdrijven worden beraamd of gepleegd in georganiseerd verband en bij aanwijzingen van een terroristisch misdrijf, kon en kan een vordering tot verstrekking van verkeersgegevens worden gedaan.[5] Wel is het zo dat nu over een langere periode dan voorheen gegevens kunnen worden opgevraagd, omdat deze als gevolg van de nieuwe wetgeving langer bewaard dienen te blijven.

Bovendien zullen in meer gevallen dan voorheen gegevens voor opsporing en vervolging beschikbaar zijn, omdat aanbieders nu de wettelijke verplichting hebben deze gegevens voor dit doel te bewaren. Daarnaast heeft de invoering van de Wet bewaarplicht verandering gebracht in het toezicht op de te bewaren gegevens en aan de eisen die sindsdien worden gesteld aan de informatiebeveiliging en -vernietiging. In de situatie voor de invoering van de Wet bewaarplicht was het voor aanbieders mogelijk om gegevens onbeveiligd en voor onbeperkte tijd te bewaren.

In het wetsvoorstel werd ervoor gekozen om een bewaartermijn aan te houden van achttien maanden voor alle te bewaren gegevens, dus zowel voor gegevens die betrekking hadden op communicatie via vaste en mobiele telefonie als voor gegevens betreffende internettoegang. De Tweede Kamer bracht de voorgestelde bewaartermijn van achttien maanden terug naar

3 Evaluatieverslag van de Europese Commissie betreffende de Europese dataretentierichtlijn (COM (2011) 225 final).

4 In de wet wordt onderscheid gemaakt tussen gegevens 'over het communicatieverkeer met betrekking tot die gebruiker' (art. 126n/u/zh Sv.) en gegevens 'ter zake van naam, adres, postcode, woonplaats, nummer en soort dienst van een gebruiker van een communicatiedienst' (art. 126n/ua/zi Sv.). Deze twee categorieën van gegevens worden ook wel aangeduid als verkeersgegevens respectievelijk gebruikersgegevens. In het algemeen geldt dat de bevoegdheid tot het vorderen van verkeersgegevens ook de bevoegdheid tot het vorderen van gebruikersgegevens omvat.

5 In het Wetboek van Strafvordering wordt onderscheid gemaakt tussen drie soorten onderzoek. Voor het opvragen van verkeersgegevens ten behoeve van de opsporing van gepleegde strafbare feiten geldt artikel 126n Sv., voor het opvragen van verkeersgegevens ten behoeve van de opsporing van misdrijven die worden beraamd of gepleegd in georganiseerd verband geldt artikel 126u Sv. en voor het opvragen van verkeersgegevens ten behoeve van een opsporingsonderzoek op grond van aanwijzingen van een terroristisch misdrijf geldt artikel 126zh Sv. Gebruikersgegevens kunnen worden gevorderd op basis van respectievelijk artikel 126na, 126ua en 126zi Sv.

twaalf maanden. Hierdoor zijn historische verkeersgegevens betreffende telefonie tot een jaar terug op te vragen.
De bewaartermijn van twaalf maanden voor internetgegevens heeft tot een uitgebreide discussie geleid. Zo is er een hoorzitting over dit onderwerp gehouden met experts en heeft er over dit onderwerp een uitgebreide gedachtewisseling plaatsgevonden tussen de toenmalige Minister van Justitie en de Eerste Kamer. De minister pleitte voor een bewaartermijn van een jaar voor internetverkeer, onder meer met het argument dat telefonie via internet op den duur de traditionele telefonie zou vervangen.[6] Daarmee nam hij een voorschot op komende ontwikkelingen. In de beraadslagingen met de Eerste Kamer bleek een opslagtermijn van twaalf maanden voor internetgegevens, op grond van de oppositie, niet houdbaar. Daarom heeft de minister toegezegd de bewaartermijn van internetgegevens via een wetswijziging terug te brengen tot zes maanden, ná de aanneming van de Wet bewaarplicht door de Eerste Kamer. Een wetswijziging van die strekking[7] is in juli 2011 van kracht geworden.

Op grond van een vordering tot verstrekking van verkeersgegevens kunnen van een aanbieder van een communicatiedienst slechts verkeersgegevens worden verkregen indien er sprake is (geweest) van communicatieverkeer. Er moet dus een verbinding (of een poging daartoe) geweest zijn tussen een telefoon of een geautomatiseerd werk en een ander telecommunicatie aansluitpunt. Indien een mobiele telefoon slechts *stand-by* staat, worden er wel locatiegegevens van deze mobiele telefoon gegenereerd, de zogenaamde vluchtige gegevens, maar deze gegevens kunnen niet worden gevorderd op grond van artikel 126n/u/zh Sv., omdat er in dat geval geen sprake is (geweest) van communicatieverkeer en de gegevens daarmee niet vallen onder de bewaarplicht.[8]

De opslag van telecommunicatiegegevens
De gegevens die ontstaan bij het gebruik van een telecommunicatiedienst bestaan kortweg uit inhoudelijke gegevens, verkeersgegevens, locatiegegevens en andere gegevens, zoals identificerende gegevens (NAW-gegevens[9]) van de abonnementhouder. Gegevens over de inhoud van de communicatie mogen niet worden opgeslagen. Het is dus niet mogelijk om op grond van gegevens die volgens de Wet bewaarplicht moeten worden bewaard, iemands surfgedrag of de inhoud van zijn e-mails te achterhalen. Met historische gegevens over telefoonverkeer kan worden nagegaan op welk moment iemand met een bepaalde telefoon of met een bepaald telefoonnummer, waarvan de gegevens worden opgevraagd, contact heeft gelegd met een

6 *Kamerstukken I* 2008/09, 31 145, C. p. 8.
7 *Stb.* 2011, 350.
8 Vluchtige gegevens betreffende de locatie kunnen, in het geval een telefoon slechts stand-by staat, wel worden gevorderd op grond van de artikelen 126ng/ug jo., 126 nd/ud en 126ne/ue Sv.
9 Naam, Adres en Woonplaats.

ander nummer, hoe lang dit gesprek heeft geduurd en vanaf welke locatie dit gesprek werd gevoerd. Tevens kunnen de NAW-gegevens van de beller en van de gebelde worden opgevraagd. Met historische internetgegevens kan worden nagegaan op welk moment en vanaf welke locatie iemand met een computer of mobiele telefoon contact heeft gelegd met het internet en hoe lang dit contact heeft geduurd.
In de praktijk worden verkeersgegevens die op grond van de Wet bewaarplicht worden opgeslagen, decentraal bewaard bij de aanbieders, die tevens verantwoordelijk zijn voor de opslag, de beveiliging en de vernietiging van de gegevens. Het Agentschap Telecom (AT), dat opereert als toezichthouder, ziet erop toe dat de regels van de Wet bewaarplicht worden nageleefd. Hierbij maakt het AT gebruik van de registers van de Onafhankelijke Post- en Telecommunicatie Autoriteit (OPTA)[10] en wordt samengewerkt met het College bescherming persoonsgegevens (CBP). Het toezicht is georganiseerd in een jaarlijkse toezichtcyclus waarbij risico's worden geïnventariseerd waarop vervolgens wordt geacteerd. Daarnaast streeft het AT ernaar alle aanbieders in Nederland, ongeveer 600 geregistreerde aanbieders, elke vier jaar minstens één keer te bezoeken. De opgeslagen informatie kan door opsporingsdiensten voor opsporingsdoeleinden worden opgevraagd bij de aanbieders via de ULI van de Landelijke Eenheid.[11] De opvraagbare gegevens kunnen in Nederland tot een jaar (voor telefoongegevens) of tot een halfjaar (voor internetgegevens) voorafgaand aan de datum van de vordering beschikbaar worden gemaakt.

Aantallen vorderingen in Nederland
De Minister van Veiligheid en Justitie heeft in 2010 voor het eerst het aantal vorderingen tot verstrekking van telecommunicatiegegevens bekendgemaakt. In de tweede helft van 2010 waren dit er 24.012. In het jaar 2011 zijn 49.695 vorderingen ingediend. Het totaal aantal vorderingen in het jaar 2012 bedraagt 56.825. Deze vorderingen betreffen vooral informatie over het gebruik van bepaalde telefoon- of IP-nummers, zoals met welk nummer is er gebeld, wanneer is er gebeld, hoe lang is er gebeld en vanaf welke locatie, en is er contact geweest met het internet? Opsporingsdiensten gebruiken deze historische verkeersgegevens voor verschillende doelen. Zo wordt bij moordzaken met een onbekende dader meestal het historische telefoonverkeer van het slachtoffer opgevraagd, omdat deze gegevens inzichtelijk maken met welke personen (of in ieder geval met welke telefoonnummers) het slachtoffer in de periode voorafgaand aan zijn of haar dood in contact heeft gestaan. Als personen ervan verdacht worden samen een misdrijf te hebben gepleegd, kunnen historische verkeersgegevens gebruikt worden om te onderzoeken of en op welke momenten deze verdachten via de telefoon met

10 Sinds 1 april 2013 vormen de Consumentenautoriteit, de Nederlandse Mededingingsautoriteit (NMa) en de OPTA de nieuwe toezichthouder Autoriteit Consument & Markt.
11 De ULI was ten tijde van dit onderzoek ondergebracht bij het Korps Landelijke Politiediensten (KLPD). Sinds de omvorming tot Nationale Politie op 1 januari 2013 is deze Unit ondergebracht bij de Landelijke Eenheid.

elkaar in contact hebben gestaan en vanaf welke locaties deze gesprekken werden gevoerd. Ook kunnen verklaringen van verdachten over contacten met medeverdachten soms aan de hand van dergelijke gegevens worden getoetst. Historische verkeersgegevens kunnen ook worden gebruikt om sociale netwerken in kaart te brengen; zij kunnen inzicht bieden in locaties van waaruit bepaalde personen contact met elkaar hebben gehad. Daarnaast is het mogelijk om op grond van kennis over de locaties waar een misdrijf is gepleegd zicht te krijgen op mogelijke verdachten. Door verkeersgegevens op te vragen van telefoons die op tijdstip X contact hebben gehad met de zendmast bij plaats delict A (bijvoorbeeld de plek waar een overval werd gepleegd) en deze te vergelijken met de verkeersgegevens van telefoons die contact hebben gehad met de zendmast op plaats delict B (bijvoorbeeld de plek waar een uitgebrande vluchtauto werd teruggevonden) kunnen, wanneer de verdachte een telefoon heeft gebruikt voor communicatie, soms overeenkomstige nummers worden gevonden die kunnen leiden naar verdachten of betrokkenen. In dergelijke situaties vormen verkeersgegevens digitale sporen die door de daders zijn achtergelaten. Tot slot kunnen historische verkeersgegevens een rol spelen bij de besluitvorming over het al of niet inzetten van meer ingrijpende opsporingsmiddelen, zoals het inzetten van een telefoontap op een bepaald telefoonnummer.

Privacyschending versus opsporingsbelang

Het is evident dat historische gegevens over telefoon- en internetverkeer van nut kunnen zijn voor de opsporing en vervolging van strafbare feiten. Het feit dat deze gegevens standaard voor een bepaalde periode moeten worden opgeslagen, is echter een terugkerend punt van discussie. Zowel in Nederland als op Europees niveau (EU 18620/11) bestaat behoefte aan meer inzicht in het gebruik van de gegevens die op grond van de Wet bewaarplicht worden opgeslagen. In antwoord op vragen vanuit de Eerste Kamer over nut en noodzaak van de Wet bewaarplicht voor de opsporing, over de wijze waarop de opgeslagen gegevens worden beschermd en beveiligd en over de harmonisatie van de bewaarplicht op Europees niveau gaf de Minister van Veiligheid en Justitie onder meer aan dat er een onderzoek zou worden verricht naar de Nederlandse Wet bewaarplicht, waarin op deze vragen zou worden ingegaan. Inmiddels is er op 18 april 2011 een evaluatieverslag verschenen van de Europese Commissie betreffende de Europese Dataretentierichtlijn (COM (2011) 225 final). De hoofdconclusie uit dit verslag is dat de richtlijn een waardevol instrument is voor de opsporing en dat de richtlijn gehandhaafd wordt. Naar de mening van de Europese Commissie bestaat er echter te veel onderlinge variatie tussen de lidstaten in doelgebruik, bewaartermijn en soort te bewaren gegevens. De Commissie oriënteert zich daarom op mogelijkheden om via de richtlijn meer harmonisatie tussen de lidstaten te kunnen bewerkstelligen. In Nederland hebben zowel leden van de Eerste Kamer als van de Tweede Kamer zich kritisch uitgelaten over dit evaluatieverslag van de Euro-

pese Commissie (E110022), omdat het nut en de noodzaak van de richtlijn hierin onvoldoende zouden zijn belicht. Daarnaast zou de richtlijn te weinig inzicht bieden in nieuwe vormen van communicatie die buiten het bereik van de bewaarplicht vallen. Volgens beide Kamers blijven er hierdoor veel vragen betreffende de werking van de bewaarplicht onbeantwoord. Een aantal fracties ijverde er op grond hiervan zelfs voor om de richtlijn te laten intrekken (E110022).
Ook de Europese Toezichthouder voor Gegevensbescherming (EDPS) bekritiseerde de evaluatie van de Europese Commissie in een opiniestuk dat op 31 mei 2011 werd gepubliceerd. In dit stuk stelt de EDPS dat de dataretentierichtlijn niet voldoet aan de grondrechten op privacy en gegevensbescherming omdat: (1) de noodzaak voor dataretentie zoals beschreven in de richtlijn niet voldoende zou worden aangetoond; (2) dataretentie op een andere wijze geregeld zou kunnen worden die minder inbreuk zou maken op de privacy; (3) de richtlijn te veel ruimte zou laten voor lidstaten om zelf te beslissen over de doelen waarvoor zij de opgeslagen gegevens willen gebruiken, over het aanwijzen van degenen die toegang krijgen tot de verzamelde data en over de omstandigheden waaronder zij toegang krijgen.
Het doel van het voorliggende onderzoek is inzicht te bieden *in de wijze waarop de Wet bewaarplicht uitwerkt in de praktijk*. Daarbij zal worden nagegaan welke gegevens in de praktijk worden opgeslagen, op welke wijze dit gebeurt, door wie en onder welke omstandigheden de gegevens kunnen worden opgevraagd en op welke wijze de opgeslagen gegevens worden beschermd, beveiligd en vernietigd.
Daarnaast wordt in dit rapport aandacht besteed aan de vraag hoe de gegevens die op grond van de Wet bewaarplicht beschikbaar worden gehouden voor de opsporing, gebruikt worden in de opsporingspraktijk. Hiermee biedt het rapport inzicht in het nut van de gehanteerde bewaartermijnen en in de vraag of de termijnen die bij wet zijn vastgelegd voldoen. Ook wordt onderzocht of er andere opsporingsmiddelen beschikbaar zijn waarmee hetzelfde resultaat kan worden behaald en of dataretentie kan worden gerealiseerd op een wijze die minder inbreuk maakt op de privacy van grote groepen burgers.

Dit onderzoek richt zich op de wijze waarop de Wet bewaarplicht in de praktijk wordt uitgevoerd en op de wijze waarop de gegevens die op grond van deze wet worden opgeslagen in de praktijk worden gebruikt. Daarmee vormt dit onderzoek strikt genomen geen evaluatie van de Wet bewaarplicht. Het onderzoek reikt verder dan een procesevaluatie (vgl. Wartna, 2005; Nelen et al., 2010), omdat er niet alleen behoefte bestaat aan inzicht in de wijze waarop de Wet bewaarplicht in de praktijk vorm heeft gekregen, maar vooral ook aan inzicht in de wijze waarop de gegevens die op grond van deze wet beschikbaar dienen te worden gehouden voor de opsporing in de praktijk worden gebruikt. De wijze waarop deze gegevens gebruikt worden in de

opsporingspraktijk en de mate waarin de wettelijk vastgestelde bewaartermijnen volstaan, vormt feitelijk de kern van dit onderzoek.
Het is echter niet mogelijk om – zoals bij een product- of effectevaluatie het geval is – het effect vast te stellen van de invoering van de Wet bewaarplicht op de wijze waarop verkeersgegevens gebruikt worden in de opsporingspraktijk. Dit is niet goed mogelijk omdat de telecommunicatiegegevens waar het hier om draait ook vóór de invoering van de Wet bewaarplicht in het algemeen beschikbaar waren voor de opsporing en gebruikt werden in de opsporingspraktijk. Daarnaast heeft niet alleen de invoering van de Wet bewaarplicht in de afgelopen periode geleid tot mogelijke veranderingen in het gebruik van telecomgegevens in de opsporingspraktijk. Veranderingen daarin zijn vooral ook het gevolg van de opkomst van de mobiele telefoon en de smartphone en van de mogelijkheden om via het internet met elkaar te communiceren. Het is daarom wel mogelijk om te onderzoeken op welke wijze telecomgegevens gebruikt worden in de opsporingspraktijk, maar het is niet goed mogelijk om deze bevindingen te relateren aan de invoering van de nieuwe wet. Hoewel de invoering van de Wet bewaarplicht gezorgd heeft voor harmonisatie van de bewaartermijnen, zijn de gevolgen hiervan, mede doordat er in de tussentijd ook andere veranderingen zijn opgetreden, nauwelijks te meten. Er is gekozen voor een brede onderzoeksopzet waarbij zowel vragen over de wijze waarop de wet is vormgegeven als vragen over het gebruik van de opgeslagen gegevens aan de orde worden gesteld.
Bij het bewaren, beschikbaar houden en gebruiken van gegevens over telefoon- en internetverkeer ten behoeve van de opsporing en vervolging zijn verschillende organisaties en partijen betrokken. De aanbieders dienen de te bewaren gegevens op te slaan, te beveiligen, beschikbaar te stellen voor de opsporing en tijdig weer te vernietigen. Het AT ziet toe op dit proces. Het CPB heeft de algemenere taak toe te zien op het gebruik van privacygevoelige gegevens. Politie en Openbaar Ministerie (OM) maken gebruik van deze gegevens bij het opsporen en vervolgen van ernstige misdrijven en de Zittende Magistratuur gebruikt de gegevens in de rechterlijke besluitvorming.
De wijze waarop de Wet bewaarplicht uitwerkt in de praktijk, vormt een ingewikkeld bouwwerk, dat in dit rapport weergegeven wordt door de wijze te beschrijven waarop deze verschillende partijen hun taken uitvoeren. In dit rapport wordt relatief veel aandacht besteed aan de wijze waarop de bewaarde gegevens gebruikt worden in de praktijk. Andere partijen worden belicht, maar vormen niet het zwaartepunt van dit onderzoek.

1.1 Probleemstelling en onderzoeksvragen

Doel van dit onderzoek is inzicht te bieden in de wijze waarop de Wet bewaarplicht in de praktijk wordt vormgegeven en in de wijze waarop de gegevens die op grond van de Wet bewaarplicht worden opgeslagen in de

praktijk door politie en justitie worden opgevraagd en worden gebruikt. Hierbij richten we ons op de volgende vragen:

— Hoe heeft de telefoon- en internetmarkt zich de afgelopen jaren ontwikkeld en welke gevolgen hebben deze ontwikkelingen gehad voor de wijze waarop historische verkeersgegevens over telefoon- en internetcommunicatie gebruikt kunnen worden in de opsporingspraktijk?
— Wat is het doel, de achtergrond en de inhoud van de Wet bewaarplicht in Nederland?
— Worden de gegevens die op grond van de Wet bewaarplicht beschikbaar moeten blijven voor de opsporing daadwerkelijk opgeslagen?
— In welke situaties en door wie kunnen deze opgeslagen gegevens worden opgevraagd?
— Op welke wijze worden de gegevens beschermd tegen onrechtmatig gebruik? Is de vergoeding van de overheid hiervoor toereikend?
— Op welke wijze worden de gegevens die volgens de Wet bewaarplicht beschikbaar moeten blijven voor de opsporing in de praktijk gebruikt in het opsporingsproces?
— Welke overwegingen en doelen liggen ten grondslag aan het opvragen van historische verkeersgegevens en welke resultaten kunnen ermee worden bereikt?
— Zijn de wettelijk vastgelegde bewaartermijnen van één jaar als het gaat om telecommunicatiegegevens en van een halfjaar als het gaat om internetgegevens nuttig, noodzakelijk en wenselijk of zou het opsporingsproces toe kunnen met kortere respectievelijk behoefte hebben aan langere opslagtermijnen?
— Hebben andere Europese lidstaten de dataretentie richtlijn geïmplementeerd?
— Zijn er opsporingsmiddelen beschikbaar die een minder grote inbreuk maken op de privacy van grote groepen burgers, waarmee hetzelfde resultaat zou kunnen worden bereikt als met het opvragen en onderzoeken van opgeslagen verkeersgegevens?

1.2 Opzet van het onderzoek

Op de hiervoor genoemde onderzoeksvragen is antwoord gezocht met behulp van verschillende onderzoeksmethoden. Voor het beschrijven van ontwikkelingen op de telefoon- en internetmarkt en de gevolgen hiervan voor het bewaren van deze gegevens en voor het gebruiken ervan ten behoeve van de opsporing, is gebruikgemaakt van literatuuronderzoek en van interviews met experts. Voor de beschrijving van de wet- en regelgeving is vooral gebruikgemaakt van literatuuronderzoek. Voor dit deel van het onderzoek zijn de wetteksten en toelichtingen daarop, lagere regelgeving, Kamerstukken, schriftelijke stukken van uitvoeringsinstanties en wetenschappelijke lite-

ratuur bestudeerd. Om zicht te kunnen bieden op de wijze waarop aanbieders in de praktijk tegemoetkomen aan de verplichtingen die voortvloeien uit de wet, en op de wijze waarop de opgeslagen gegevens worden beveiligd tegen misbruik, is gebruikgemaakt van interviews met het AT en met verschillende aanbieders. Tevens is hiertoe literatuur over dit onderwerp bestudeerd.
Om antwoord te kunnen geven op vragen over het nut en de noodzaak van de Wet bewaarplicht hebben we onderzocht *op welke wijze de gegevens die op grond van de Wet bewaarplicht beschikbaar moeten zijn voor de opsporing in de praktijk worden gebruikt.* Hiervoor zijn verschillende onderzoeksmethoden gehanteerd. Naast de bestudering van nationale en internationale vakliteratuur is kwantitatieve en kwalitatieve informatie verzameld over het gebruik van historische verkeersgegevens. Hierover zijn gegevens verzameld bij onder andere de ULI, de politie, de rechterlijke macht (OM) en de advocatuur. Gegevens zijn verzameld op landelijk en regionaal niveau. Tot slot hebben we hiertoe aan de hand van vonnissen geanalyseerd op welke wijze gegevens die op grond van de Wet bewaarplicht beschikbaar worden gehouden voor de opsporing door Nederlandse rechters gebruikt worden in de bewijsvoering van strafzaken. Hiermee geven we een aanvulling op het onderzoek van Mevis et al. (2005) die het nut en de noodzaak van een bewaarplicht voor verkeersgegevens onderzocht aan de hand van geanalyseerde opsporingsdossiers.

1.2.1 Geïnterviewde personen

Bij het uitvoeren en handhaven van de Wet bewaarplicht zijn verschillende spelers betrokken en de opgeslagen gegevens kunnen voor verschillende doelen worden gebruikt. Om een breed beeld te kunnen schetsen van de werking van de wet, van het gebruik van de opgeslagen gegevens en van de overwegingen die aan het opvragen van deze opgeslagen gegevens ten grondslag liggen, zijn interviews gehouden met experts en professionals uit de opsporingspraktijk. De personen die voor dit onderzoek zijn geïnterviewd, vormen een mix tussen enerzijds experts met specifieke kennis over bepaalde aspecten die een rol spelen bij het bewaren, beveiligen en opvragen van historische telecomgegevens of met het toezicht op dit proces en anderzijds een groep professionals met veel praktijkervaring op het gebied van de opsporing en vervolging van bepaalde soorten misdrijven en van de wijze waarop historische telecomgegevens in die zaken worden gebruikt. Er is gesproken met experts van onder meer de ULI, het Nederlands Forensisch Instituut (NFI), AT en het CBP. Voorts hebben we twee grote en twee kleine aanbieders van telecom- en internetdiensten geïnterviewd, is er gesproken met professionals die werkzaam waren bij verschillende teams van de politie en de rechterlijke macht (OM) en bij bijzondere opsporingsdiensten en spraken we met advocaten. Het onderzoek is verricht op landelijk en op regionaal niveau. Bij de

politie interviewden we vooral teamleiders en analisten die werkzaam waren bij verschillende teams. Voorts spraken we met enkele officieren van justitie (OvJ's) en advocaten die ervaring hadden opgebouwd in een breed scala aan strafzaken, met enkele experts van een bijzondere opsporingsdienst en met enkele experts die niet verbonden zijn aan de genoemde organisaties. In totaal hebben we 41 personen geïnterviewd. Hiervan spraken we 25 personen face-to-face en 16 telefonisch.[12] Hierna staat een overzicht van de organisaties waarbij de door ons geïnterviewde professionals en experts werkzaam zijn:

— ULI (1);
— politie (15);
— Fiscale Inlichtingen- en Opsporingsdienst (FIOD) (2);
— OM (2);
— NFI (1);
— advocatuur (3);
— aanbieders (6);
— AT (2);
— Bits of Freedom (BoF) (1);
— CBP (3);
— wetenschappers/juristen/specialisten (5).

1.2.2 Werkwijze van het empirisch onderzoek

Tijdens de face-to-face interviews werden de professionals en experts geïnterviewd aan de hand van een semigestructureerde vragenlijst die een aantal vaste onderwerpen bevatte. Deze vragenlijst werd aangepast aan de functie of positie van de geïnterviewde. Daarnaast werd bij de meeste interviews uitgebreider stilgestaan bij specifieke thema's. Deze interviews namen gemiddeld anderhalf uur in beslag. De telefonische interviews zijn afgenomen met behulp van een gestructureerde vragenlijst. Ook deze vragenlijst was aangepast aan de functie en positie van de professional of expert en duurde gemiddeld een half uur. Alle interviews zijn met toestemming van de geïnterviewde opgenomen op audioapparatuur en voorts letterlijk uitgewerkt. De ingevoerde interviews zijn geanonimiseerd en vervolgens door twee onderzoekers gecodeerd. De codelijst omvatte een puntsgewijze gedetailleerde uitwerking van alle onderwerpen die op de vragenlijsten aan de orde zijn gekomen. Onderwerpen of uitspraken die niet of moeilijk te scoren waren, zijn door de onderzoekers als 'overig' gelabeld en in een later stadium nader bekeken en waar relevant opgenomen in het rapport. Deze manier van werken maakt het mogelijk om met behulp van MaxQDa, een analyseprogramma voor kwalitatieve data-analyse, de uitspraken van de professionals en experts voor een bepaald onderwerp te selecteren en te analyseren. De codelijst heeft

12 Er vonden zeventien face-to-face interviews plaats, waarbij in acht gevallen met meerdere sleutelpersonen tegelijk werd gesproken, en zestien telefonische interviews.

als uitgangspunt gediend bij het schrijven van hoofdstuk 4 en 5 van dit rapport. De citaten die in dit hoofdstuk worden weergegeven staan niet op zichzelf. Ze zijn zorgvuldig gekozen en representeren – indien er meerdere professionals en experts zijn gesproken over het desbetreffende onderwerp – steeds de ervaringen van meerdere geïnterviewde professionals of experts. Indien dit niet het geval is, gaat het om de ervaringen van experts. De citaten dienen om de in de tekst beschreven onderwerpen te illustreren.

1.2.3 Opbouw van het rapport

Dit rapport bestaat uit zeven hoofdstukken waarin als eerste de veranderende wereld van telecommunicatie (hoofdstuk 2) wordt beschreven. Hierna worden in hoofdstuk 3 de wettelijke bepalingen en voorwaarden van het gebruik van verkeer- en locatiegegevens uiteengezet. Ook de vraag of andere Europese landen de Wet bewaarplicht geïmplementeerd hebben, komt in dit hoofdstuk aan de orde. Het bewaren en beveiligen van verkeers- en locatiegegevens wordt in hoofdstuk 4 beschreven. Hierin komen de aanbieders aan het woord en wordt het toezicht op de uitvoering van de Wet bewaarplicht beschreven. Het daadwerkelijke gebruik en de toepassingen van de bewaarde gegevens door opsporingsdiensten worden beschreven in hoofdstuk 5. In dit hoofdstuk komen verkeers- en locatiegegevens van telefonie en internetcommunicatie aan bod. In hoofdstuk 6 wordt het gebruik van historische verkeersgegevens weergegeven in cijfers. In dit hoofdstuk worden aantallen bevragingen gepresenteerd en daarnaast worden gerechtelijke uitspraken gepresenteerd, waarin verkeers- en locatiegegevens een rol hebben gespeeld. Tot slot volgt de slotbeschouwing in hoofdstuk 7.

2 Communicatie op afstand, ontwikkelingen en gevolgen

De bevoegdheid om bij telecomaanbieders historische verkeersgegevens op te vragen ten behoeve van de opsporing werd in 1926 ingevoerd (zie hierover Koops, 2002). In 2000 is deze bevoegdheid aangepast en ondergebracht bij de Wet bijzondere opsporingsbevoegdheden, een wet die dient als grondslag voor de inzet van heimelijke opsporingsmiddelen die een inbreuk maken op de persoonlijke levenssfeer. Met de opkomst van het internet werden de bevoegdheden die golden voor het opvragen van gegevens over telefoonverkeer ook gebruikt voor het opvragen van gegevens over internetverkeer.
Door de opkomst van de mobiele telefoon en door het steeds bredere gebruik van het internet ontstond er in het afgelopen decennium een sterke groei in het aantal verkeersgegevens dat werd opgeslagen en ook de bruikbaarheid van die gegevens voor de opsporing nam toe. Door de opkomst van de mobiele telefoon nam tevens het aantal gevoerde telefoongesprekken sterk toe. Daarnaast werd het mogelijk om bij benadering te bepalen waar een mobiel toestel zich ten tijde van een gevoerd gesprek bevond.[13] Door de koppeling van contactgegevens en locatiegegevens werd enerzijds de privacygevoeligheid van de historische verkeersgegevens vergroot, maar anderzijds ook de bruikbaarheid van deze gegevens voor de opsporing. De ontwikkeling van de mobiele telefonie bracht ook met zich mee dat deze privacygevoelige gegevens steeds meer in handen kwamen van private partijen. Hierdoor bleek het voor opsporingsdiensten niet in alle gevallen mogelijk te zijn om gegevens te vorderen (zie hierover Mevis et al., 2005). Gegevens die niet voor de eigen bedrijfsvoering werden opgeslagen, konden niet worden opgevraagd. Private partijen waren verplicht om alle historische verkeersgegevens te vernietigen als ze niet meer relevant waren voor de bedrijfsvoering.[14] De Wet bewaarplicht heeft hierin verandering gebracht. Door de Wet bewaarplicht werden private aanbieders verplicht om gegevens over communicatieverkeer gedurende een bepaalde periode beschikbaar te houden voor de opsporing.
Doordat het internet voor een steeds groter wordende groep mensen toegankelijk is geworden, heeft het een steeds grotere plaats ingenomen als communicatiemiddel. De mobiele telefoon werd in de afgelopen jaren vervangen door de smartphone en veel mensen zijn tegenwoordig 24 uur per dag, 7 dagen per week, online. Door het gebruik van smartphones wordt er steeds vaker gecommuniceerd in de vorm van korte berichten via apps en e-mail en bellen mensen ook steeds vaker via internet. Hierdoor worden er steeds meer privacygevoelige digitale sporen achtergelaten. Tegelijkertijd zorgen technologische veranderingen en vernieuwingen ervoor dat een toenemend deel van de van oudsher voorhanden zijnde verkeersgegevens niet meer onder de

13 Een mobiele telefoon moet zich aanmelden bij een zender om te kunnen telefoneren. Met gegevens over de gebruikte zender kan, afhankelijk van de bevolkingsdichtheid van het gebied, op enkele kilometers tot enkele honderden meters nauwkeurig worden bepaald waar dit telefoontoestel zich bevindt.
14 Er bestond wel een beperkte bewaarplicht (zie voetnoot 1).

Wet bewaarplicht valt of niet meer eenvoudig beschikbaar is voor opsporingsdiensten. Om de context te schetsen waarin de Wet bewaarplicht moet worden beschouwd, volgt hier een korte uiteenzetting over de huidige telefoon- en internetmarkt.

2.1 De telefoniemarkt

De telecommarkt is de afgelopen jaren drastisch veranderd. Mobiele telefonie heeft het laatste decennium een enorme vlucht genomen en het mobieltje is niet meer weg te denken uit het dagelijks leven. In het tweede kwartaal van 2012 waren er in Nederland 21,7 miljoen mobiele telefoonaansluitingen in gebruik en 7,1 miljoen vaste telefoonaansluitingen (OPTA, 2012). Vroeger richtte de telecommarkt zich vooral op spraak, maar tegenwoordig richt deze sector zich steeds meer op data. Data worden al lang niet meer alleen via een computer verzonden, maar ook meer en meer met mobiele telefoons. De OPTA[15] rapporteerde een toename in de omzet van 12% uit datagebruik en toename van het datavolume met 21% in het tweede kwartaal van 2012 ten opzichte van het laatste halfjaar van 2011 (OPTA, 2012). Tegelijkertijd neemt het aantal belminuten al jaren achtereen af. In 2009 nam het aantal belminuten per persoon per vaste telefoon af met meer dan 7%. Bellen met de mobiele telefoon groeide in dat jaar wel, maar niet genoeg om de daling in inkomsten van vaste telefonie te compenseren (OPTA, 2009). In het eerste kwartaal van 2012 nam het totale aantal gebelde minuten af van 5,8 naar 5,7 miljard (OPTA, 2012).
Een mobiele telefoon wordt niet meer alleen gebruikt om te bellen, maar bijvoorbeeld ook om e-mail mee te versturen, te communiceren via sociale media, te fotograferen, muziek te beluisteren, te gamen, te winkelen en te bankieren. Voor veel van deze functies is verbinding met het internet noodzakelijk. Het aantal breedbandaansluitingen in Nederland is inmiddels de 10 miljoen gepasseerd. Het overgrote deel van deze aansluitingen (8,9 miljoen) betreft een smartphone-aansluiting (OPTA, 2012).
De smartphone is inmiddels het meest frequent gebruikte apparaat om buitenshuis contact te maken met het internet. Cijfers van het Centraal Bureau voor de Statistiek (CBS) laten zien dat ruim 56 procent van alle Nederlanders tussen de 16 en 75 jaar in 2012 een smartphone gebruikte om mobiel te internetten. Onder jongeren tussen 12 en 25 jaar gebruikt 70% een smartphone om vrijwel dagelijks buitenshuis online te gaan.
Naast de smartphone wordt ook de laptop vaak gebruikt om buitenshuis gebruik te maken van het internet. Omdat er op steeds meer plekken Wi-Fi beschikbaar is, wordt het gebruik van de laptop onderweg aantrekkelijker, zo verklaart het CBS de stijging in 2012 ten opzichte van voorgaande jaren. Ove-

15 Sinds 1 april 2013 vormen de Consumentenautoriteit, de NMa en de OPTA de nieuwe toezichthouder Autoriteit Consument en Markt.

rigens ligt het gebruik van mobiel internet in Nederland ruim boven het gemiddelde in de EU.[16]

Er is in Nederland een hoogwaardige infrastructuur aanwezig om het bel- en dataverkeer te kunnen faciliteren. Er zijn zes grote telecommunicatieaanbieders die het netwerk in Nederland bezitten. Daarnaast zijn er serviceproviders en mobiele *virtual network operators* die geen eigen netwerk hebben, maar gebruikmaken van het netwerk van de grote aanbieders.
Om een vaste telefoonlijn te kunnen gebruiken. moet een abonnement worden afgesloten bij een van de aanbieders die de gewenste diensten levert. Bij het afsluiten van een abonnement moet de gebruiker zich laten registeren, zodat de maandelijkse kosten bij de abonnementhouder in rekening kunnen worden gebracht. De verkeersgegevens die deze klanten genereren zijn eenvoudig aan een adres te koppelen. Voor het activeren van een mobiele telefoon kan eveneens een abonnement worden afgesloten bij een aanbieder. Hiervoor zal de eigenaar van de mobiele telefoon zich, net als bij een abonnement op een vaste lijn, moeten registreren en legitimeren bij de aanbieder. De aanbieder levert vervolgens een SIM-kaart. Nadat deze in de mobiele telefoon is geplaatst, is het toestel gebruiksklaar en kan er door de aanbieder maandelijks een bedrag in rekening worden gebracht. Mobiele telefoons kunnen echter ook worden gebruikt zonder dat een abonnement wordt afgesloten en zonder dat men bekend is bij de aanbieder. Zo wordt in Nederland bij 31% van de mobiele telefoons gebruikgemaakt van een zogenaamde prepaid SIM-kaart (OPTA, 2011). Dit is een SIM-kaart die een bepaalde waarde vertegenwoordigt. Na plaatsing in een telefoon kan met deze kaart contact worden gemaakt met het netwerk van de aanbieder. Deze kaarten worden door verschillende telecombedrijven op veel plaatsen te koop aangeboden en kunnen op een later tijdstip opnieuw worden opgehoogd met een beltegoed. Hiervoor is geen registratie nodig en de gebruiker van het telefoonnummer dat aan de prepaid SIM-kaart is gekoppeld, is dan ook niet bekend bij de aanbieder. Verkeersgegevens zijn bij prepaid bellen anoniem en de gebruiker is door opsporingsdiensten niet eenvoudig te identificeren. Wanneer het beltegoed op is, kan de gebruiker ervoor kiezen om het beltegoed op te hogen op dezelfde SIM-kaart. In dat geval behoudt hij zijn telefoonnummer en blijft hij klant bij dezelfde aanbieder. Voor sommige gebruikers is het behouden van een telefoonnummer echter van ondergeschikt belang. Een telefoonnummer is immers niet nodig wanneer de telefoon vooral gebruikt wordt om zelf te bellen en om via internet te communiceren. Door een nieuwe prepaid SIM-kaart te kopen, heeft men opnieuw toegang tot het netwerk van een aanbieder, maar wijzigt het telefoonnummer van de gebruiker. Kortom, door het gebruik van prepaid SIM-kaarten is het mogelijk om anoniem te bellen en te internetten. Elk mobiel toestel heeft, naast een telefoonnummer dat gekop-

16 www.cbs.nl/nl-NL/menu/themas/vrije-tijd-cultuur/publicaties/artikelen/archief/2013/2013-3851-wm.htm (geraadpleegd op 8 juli 2013).

peld is aan de SIM-kaart, een uniek IMEI-nummer[17]. Beide nummers worden opgeslagen en over beide nummers kunnen historische communicatiegegevens worden opgevraagd door opsporingsdiensten.

2.2 Het internet

Het internet is een wereldwijd computernetwerk, waarvan het gebruik vooral sinds de jaren negentig een enorme vlucht heeft genomen. Volgens het CBS beschikte in 2010 ongeveer 94% van de Nederlanders in de leeftijd van 12 tot 75 jaar over internet. Het gebruik ervan is populair. Twee derde van de gebruikers bekijkt dagelijks e-mail en bijna 20% chat, bezoekt dagelijks online communities en bekijkt online video's (ITU, 2011). Tussen 2005 en 2010 is het aantal internetgebruikers wereldwijd verdubbeld. In een rapport van TNO werd geschat dat er in 2010 wereldwijd meer dan twee miljard internetgebruikers zouden zijn (TNO, 2010), waarmee ongeveer 35% van de wereldbevolking online is. Naar verwachting zal in 2020 ongeveer 60% van de wereldbevolking online zijn (Hathaway et.al., 2012).
Ook het gebruik van mobiel internet neemt fors toe. Volgens de OPTA was het totale dataverbruik in de eerste zes maanden van 2010 verachtvoudigd ten opzichte van het eerste halfjaar van 2008 (OPTA, 2011; TNO, 2011). Marktcijfers van het tweede kwartaal van 2012 laten zien dat deze stijging nog voortduurt. Het gebruik van mobiel internet wordt ook steeds meer gefaciliteerd door de 'hotspots' die op steeds meer plekken beschikbaar zijn. Dit zijn Wi-Fi-netwerken waarop een gebruiker als klant, soms tegen een vergoeding maar vaak ook gratis, kan inloggen om verbinding te maken met het internet. Deze hotspots worden vaak als 'niet openbaar' gekenmerkt en vallen daarmee niet onder de Wet bewaarplicht. Deze Wi-Fi-netwerken zijn bijvoorbeeld te vinden in de trein, op stations, in restaurants, hotels en in winkelcentra, waarbij klanten na het inloggen gebruik kunnen maken van het internet.
Het internet wordt onder andere gebruikt om te winkelen, informatie op te zoeken, televisie te kijken, te bellen, e-mails te versturen, te gamen, gebruik te maken van sociale media en voor het opslaan van gegevens. Voor het opslaan van persoonlijke gegevens en ook voor het bewerken daarvan kan gebruik worden gemaakt van de 'cloud'. Dit houdt in dat bijvoorbeeld foto's of andere gegevens bewaard en bewerkt kunnen worden op servers ergens in de wereld in plaats van op de lokale harde schijf van een personal computer (pc) of telefoon. Hierdoor kan een gebruiker via het internet altijd en overal bij zijn bestanden. Internetgebruikers maken steeds vaker gebruik van clouddiensten, zoals Google Docs, Google Drive, Dropbox en iCloud. Verwacht wordt dat cloud computing een belangrijk onderdeel wordt van het internetlandschap (Koops et al., 2012). Ook voor bedrijven biedt cloud computing

17 International Mobile Equipment Identity.

interessante mogelijkheden vanwege de flexibiliteit en schaalbaarheid[18] tegen relatief lage kosten.
Het internet is kortom een digitale omgeving waarop veel mensen acteren en die op veel verschillende manieren wordt gebruikt. De scheidslijn tussen de fysieke en digitale wereld vervaagt en het internet raakt meer en meer verweven met het 'gewone' leven. Ook wordt de scheidslijn tussen telefonie en internet steeds kleiner en zijn aanbieders zich steeds meer gaan richten op datastromen. Ten tijde van het opstellen van de Wet bewaarplicht bestond er nog wel een strikte scheiding tussen de telefonie-infrastructuur en het internet. Ook in de opsporing is nog een duidelijke scheiding in de kennis over en verwerking van gegevens betreffende telefoon- en internetverkeer. Voor de helderheid is in dit rapport deze tweedeling aangehouden. In de praktijk is dit onderscheid echter nagenoeg verdwenen.

2.3 Grenzen van de bewaarplicht

De hiervoor geschetste technologische veranderingen en vernieuwingen hebben er zoals gezegd voor gezorgd dat een toenemend deel van de digitale sporen van communicatie op afstand niet onder de Wet bewaarplicht valt of niet meer eenvoudig door opsporingsdiensten kan worden achterhaald. Dit probleem kunnen we het beste verduidelijken aan de hand van een alledaags voorbeeld.

> Mevrouw Janssen pakt haar spullen voor de werkdag bijeen. De laptop wordt, na het online bekijken van het laatste nieuws via het wifi-netwerk thuis, dichtgeklapt en naast de smartphone in de tas gestopt. Na het plegen van een telefoontje met de huistelefoon gaat zij van huis. Wachtend op de trein logt ze met haar smartphone in op de wifi-hotspot van haar aanbieder om het nieuws en haar Gmail-account te bekijken. Ze ontvangt een WhatsApp-bericht, waar ze direct even op reageert. Vervolgens wordt ze gebeld door haar secretaresse en al bellend stapt ze in de trein. Wanneer Janssen klaar is met bellen, stopt ze de mobiele telefoon terug in de tas en pakt ze de laptop om een bespreking voor te bereiden. Hiervoor wil ze iets opzoeken op internet. Ze maakt met haar laptop contact met het wifi-netwerk dat gratis wordt aangeboden in de trein. Eenmaal aangekomen op haar werkplek, sluit ze haar laptop aan op het interne netwerk van de werkgever en opent ze haar werkmail.

Dit voorbeeld illustreert een dagelijks ritueel van veel mensen en het laat zien dat communicatie via veel verschillende kanalen en verbindingspunten kan verlopen. Zo zijn verbindingen met het netwerk van de telefonie- en internet-

18 Schaalbaarheid is een term uit de IT-wereld die aangeeft dat bepaalde diensten of configuraties eenvoudig groter gemaakt kunnen worden.

aanbieder niet statisch en kunnen mensen op meerdere manieren vanaf verschillende locaties verbonden zijn. Mensen gebruiken vaak ook diensten die bij verschillende aanbieders worden afgenomen. Zo kan iemand een abonnement hebben afgesloten bij een aanbieder die diensten over de kabel levert, waarbij telefonie en internet in één pakket worden geleverd, en bij een andere aanbieder een abonnement hebben afgesloten voor telefoon- en/of internetdiensten voor de mobiele telefoon. Mobiel bellen en internet kunnen echter ook prepaid worden afgenomen. Hiervoor heeft de gebruiker een toestel nodig met de gewenste kenmerken en kan een SIM-kaart met een tegoed voor belminuten of internetdata worden gekocht, bijvoorbeeld in de supermarkt. Deze technologische vernieuwingen, de daarmee gepaard gaande versnippering van communicatie en vooral het gebruik van verschillende diensten die op internet worden aangeboden, maken dat het moeilijk is om alle communicatie op afstand van een persoon in kaart te brengen. Bovendien vallen niet alle verkeersgegevens die daarbij worden gegenereerd onder de Nederlandse Wet bewaarplicht, waardoor niet alle gegevens kunnen worden achterhaald.

Op verzoek van het ministerie van Economische Zaken onderzocht Stratix Consulting hoe de aftapbaarheid van communicatiediensten het beste gewaarborgd kan worden (Stratix Consulting, 2009; zie ook Koops et al., 2005). 'Aftapbaar' duidt op het veiligstellen van gegevens ten behoeve van een onderzoek, door gebruikers- en verkeersgegevens te vorderen of door gebruik te maken van een telefoon- of internettap. Een van de conclusies in dit rapport is dat de bruikbaarheid van de opvraagbare verkeersgegevens afneemt door technische ontwikkelingen en door ontwikkelingen op de telefoon- en internetmarkt. Veel internetgebruikers hebben een e-mailaccount bij webmaildiensten, zoals Hotmail, Gmail of Yahoo, waarvan de aanbieder een buitenlands bedrijf is. Deze aanbieders of aangeboden diensten vallen niet onder de Telecommunicatiewet en vallen daarmee ook buiten de Nederlandse Wet bewaarplicht. Dit betekent dat de gegevens niet per definitie beschikbaar worden gehouden voor de opsporing. Er is in dat geval een internationaal rechtshulpverzoek nodig om inzage te kunnen krijgen in de verkeersgegevens en de beschikbaarheid van deze gegevens is in dat geval niet gegarandeerd. Ook voor communicatie met socialemediadiensten, zoals Twitter, Windows Live Messenger[19], Hyves, Facebook, Ping, WhatsApp en Facetime, geldt dat de communicatie veelal via buitenlandse servers verloopt. In al die gevallen zijn verkeersgegevens niet of moeilijk te verkrijgen voor de Nederlandse opsporingsdiensten. Daarnaast wordt er tegenwoordig veel gebeld via internet, door gebruik te maken van Voice over InternetProtocol (VoIP). In eerste instantie werd bellen via internet vooral gebruikt voor internationale contacten, omdat het een goedkope manier van bellen was. Maar doordat er steeds meer telefoons zijn met internetaansluitingen en het dus steeds eenvoudiger wordt om met een mobiele telefoon te bellen via het

19 Voorheen MSN geheten.

internet, wordt er ook steeds vaker gebruikgemaakt van deze mogelijkheid voor dagelijkse binnenlandse communicatie. Deze diensten vallen niet onder de bewaarplicht of worden dikwijls aangeboden door aanbieders die buiten de Nederlandse Wet bewaarplicht vallen (*Kamerstukken II* 2007/08, 31 145, nr. 9, p. 6). Ditzelfde geldt vaak voor aanbieders van communicatiediensten in de *cloud*. Ook bij cloud aanbieders kunnen verkeersgegevens alleen worden opgevraagd wanneer het een in Nederland gevestigde openbare telecommunicatiedienst betreft (zie voor een uitgebreide beschrijving hierover Koops et al., 2012). De Nederlandse Wet bewaarplicht kan immers geen grondslag bieden voor een onderzoek in een geautomatiseerd werk dat onder de jurisdictie van een ander land valt.[20] Indien opsporingsdiensten toch willen beschikken over verkeersgegevens van buitenlandse aanbieders, zal men een rechtshulpverzoek moeten indienen en moeten afwachten of de gevraagde gegevens nog beschikbaar zijn.

Ook blijkt het steeds moeilijker te worden om een identiteit te koppelen aan een internetgebruiker. Een IP-adres kan regelmatig veranderen, mensen kunnen gebruikmaken van diensten waarbij ze anoniem over het internet surfen en e-mailadressen zijn eenvoudig te wijzigen, ook door de gebruiker zelf. Bovendien worden zoals gezegd op veel plekken gratis Wifi-netwerk aangeboden, zoals op stations, in treinen en in restaurants. Uit de verkeersgegevens die worden opgeslagen in het kader van de Wet bewaarplicht is een gebruiker achter het IP-adres van een wifi-netwerk niet te herleiden tot een individu, omdat een persoon die inlogt een IP-adres toegewezen krijgt dat ook gebruikt wordt door alle andere personen die op dat moment op het netwerk zijn ingelogd.

De definities in de Telecommunicatiewet blijken bij sommige telecommunicatiediensten en -netwerken voor grijze gebieden te zorgen. De bewaarplicht ziet op 'openbare telecommunicatiediensten', dat wil zeggen een 'dienst die geheel of hoofdzakelijk bestaat in het overbrengen van signalen via elektronische communicatienetwerken' en die 'beschikbaar is voor het publiek' (art. 1.1 Tw). Over de omvang of grootte van het netwerk wordt niets gezegd. Dit roept weleens vragen op. De OPTA[21], toezichthouder op de naleving van de wet- en regelgeving op het gebeid van post en communicatiediensten en onderdeel van het ministerie van Economische Zaken, onderzoekt jaarlijks voor tientallen bedrijven of zij aangemerkt kunnen worden als openbare elektronische communicatiediensten en/of -netwerken en zich als zodanig zouden moeten registreren. AT gebruikt het register voor het handhaven van de aftapverplichting en de bewaarplicht. Sinds 2003 hanteert de OPTA het uitgangspunt dat horecaondernemers die slechts hun eigen gasten (bijvoorbeeld via een wifi-netwerk) toegang tot internet willen bieden, zich over het algemeen niet hoeven te registreren bij de OPTA (OPTA, 2010). In 2009 heeft

20 *Kamerstukken II* 1989/90, 21 551, nr. 3, p. 12.

21 De OPTA is sinds 1 april 2013 gefuseerd met de Consumentenautoriteit en de NMa en zij vormen samen de nieuwe toezichthouder Autoriteit Consument en Markt (ACM).

SURFnet de vraag bij de rechter neergelegd of het, als aanbieder van internettoegang bij universiteiten en onderwijsinstellingen, geregistreerd zou moeten zijn bij de OPTA en daarmee allerlei plichten zou hebben, zoals het aftapbaar maken van zijn netwerk en het bewaren van verkeersgegevens. De OPTA vond toentertijd dat de doelgroep van SURFnet zo groot is dat deze neerkomt op 'het publiek', zoals bedoeld wordt in de Telecommunicatiewet. De uitleg van de telecomtoezichthouder was dat het ging om de vraag of de groep vooral onderling wil communiceren, zoals bij een bedrijfsnetwerk, of dat de groep vooral naar buiten wil, het internet op. Dat criterium nam de rechter niet over; dat het 'ook om communicatie met een ieder die gebruiker is van internet' gaat, acht de rechtbank geen omstandigheid om te kunnen spreken van een openbare dienst dan wel openbaar netwerk. De rechtbank is van oordeel dat de kring aan wie SURFnet zijn diensten aanbiedt, wel degelijk beperkt is te achten. Die kring is immers onder een doelgroep te scharen, namelijk instellingen die zich richten op wetenschappelijk onderzoek en hoger onderwijs. Naar het oordeel van de rechtbank is dit een voldoende afgebakende groep en is die groep niet toegankelijk voor het algemene publiek (*ECLI:NL:RBROT:2009:BH9324*). Ook bibliotheken, internetcafés, hotels, winkelcentra, banken, restaurants en cafés zijn gelegenheden die internet en/of belfaciliteiten aan hun klanten aanbieden. Volgens de OPTA zijn hotels, die wifi enkel aan eigen klanten beschikbaar stellen, geen aanbieders van openbare telecommunicatiediensten. Van de overige hiervoor genoemde gelegenheden is niet duidelijk of zij bewaarplichtig zijn. Noch het AT, noch de OPTA heeft hierover duidelijkheid verschaft.[22]
Het moge duidelijk zijn dat het huidige telefoongebruik, de opkomst van de smartphone, het feit dat mensen minder zijn gaan bellen, technologische veranderingen – zoals het aanbod van wifi-netwerken in de openbare ruimte – en de enorme toename van diensten op het internet, maken dat historische telecommunicatie- en internetgegevens die vallen onder de Telecommunicatiewet, slechts een beperkt deel betreffen van de communicatie via telefoon en internet.

22 Zie ook www.ictrecht.nl/ictrecht/overzicht-bewaarplicht-wie-wel-en-wie-niet (geraadpleegd op 4 april 2013).

3 De wetsgeschiedenis en Europese regelgeving inzake de bewaarplicht van verkeersgegevens

Op 3 mei 2006 is een Europese richtlijn in werking getreden die tot doel heeft te waarborgen dat bepaalde telecom- en internetgegevens bewaard blijven en daarmee beschikbaar zijn voor opsporingsonderzoeken naar ernstige misdrijven. De lidstaten van de Europese Unie zijn gehouden deze richtlijn in wetgeving om te zetten. De periode waarover de bedrijven de gegevens dienen op te slaan, kan op basis van de richtlijn variëren van ten minste een halfjaar tot ten hoogste twee jaar. In Nederland is wetgeving van kracht geworden ter omzetting van de richtlijn. In paragraaf 3.1 bespreken we de achtergronden en het doel van de richtlijn en de mate waarin de richtlijn in de verschillende lidstaten al dan niet is geïncorporeerd. Allereerst zullen we de implementatie van de richtlijn en de totstandkoming van de wetgeving in Nederland op hoofdlijnen behandelen. Het zwaartepunt ligt daarbij bij twee aspecten die in de discussie in het parlement en ook daarbuiten centraal hebben gestaan: aan de ene kant de functie van de wetgeving in het kader van versterking van de opsporing en aan de andere kant de bescherming van de privacy van de burgers die met het (langdurig) opslaan van eerdergenoemde gegevens is gemoeid.

3.1 Het wetsvoorstel

3.1.1 De aard van de gegevens

De wetgeving heeft betrekking op zogenaamde verkeers- en locatiegegevens. Onder verkeersgegevens worden de gegevens verstaan die worden verwerkt voor het overbrengen van communicatie over een elektronisch communicatienetwerk of voor de facturering ervan.[23] Dit kunnen onder andere zijn het aansluitnummer, de datum, het tijdstip en de duur van de communicatie en het soort communicatie. Locatiegegevens betreffen gegevens over de geografische positie van het gebruikte apparaat, bijvoorbeeld van de mobiele telefoon. Aan de hand daarvan kunnen, zo stelt de Memorie van Toelichting (MvT), verklaringen van personen over hun verblijfplaats op het moment dat de telefonische communicatie plaatsvond worden getoetst.[24]
Op grond van artikel 13.4 Tw bestond er al een beperkte bewaarplicht voor het verrichten van een zogenaamde bestandsanalyse. Deze dient ervoor om gegevens van een telecommunicatiegebruiker te kunnen achterhalen als deze niet reeds bij de aanbieder – door registratie – bekend zijn. Deze situatie doet zich voor bij de gebruiker van een prepaid telefoon. Om deze bestandsana-

23 Voor de betekenis van het begrip 'verkeersgegevens' is aansluiting gezocht bij de Telecommunicatiewet; *Kamerstukken II*, 2006/07, 31 145, nr. 3, p. 3.
24 *Kamerstukken II*, 2006/07, 31 145, nr. 3, p. 9.

lyse mogelijk te maken, waren de aanbieders verplicht de daarvoor benodigde gegevens drie maanden te bewaren.[25] Het voorgaande is nader uitgewerkt in het Besluit vorderen gegevens telecommunicatie.

Het Besluit vorderen gegevens telecommunicatie[26] geeft een limitatieve opsomming van verkeersgegevens. Meer precies vallen onder verkeersgegevens: naam, adres en woonplaats van de gebruiker; nummers van de gebruiker; naam, adres en woonplaats en het nummer van de persoon met wie de gebruiker verbinding heeft, heeft gehad of heeft getracht tot stand te brengen; de datum en het tijdstip waarop de verbinding met de gebruiker tot stand is gebracht en beëindigd en de duur van de verbinding, dan wel, ingeval er geen verbinding tot stand is gekomen, de datum en het tijdstip waarop is getracht verbinding met de gebruiker tot stand te brengen. Verder bevatten de verkeersgegevens de locatiegegevens van het netwerkaansluitpunt dan wel gegevens betreffende de geografische positie van de randapparatuur van een gebruiker in geval van een verbinding of poging daartoe; de nummers van de randapparatuur waarvan de gebruiker gebruikmaakt of heeft gemaakt; de soorten diensten waarvan de gebruiker gebruikmaakt of heeft gemaakt evenals de daarbij behorende gegevens; naam, adres en woonplaats van degene die de rekening betaalt voor de openbare telecommunicatiediensten en telecommunicatienetwerken die de gebruiker ter beschikking heeft of heeft gehad, indien deze een ander is dan de gebruiker.

Op grond van een vordering verstrekking verkeersgegevens kunnen van een aanbieder van een communicatiedienst slechts verkeersgegevens worden verkregen indien er sprake is (geweest) van communicatieverkeer. Dat wil zeggen dat er verbinding (of een poging daartoe) moet zijn (geweest) tussen een geautomatiseerd werk (zoals een telefoon of een computer) en een ander geautomatiseerd werk. Indien een mobiele telefoon slechts stand-by staat, worden er wel locatiegegevens van de desbetreffende mobiele telefoon gegenereerd, maar deze gegevens kunnen niet op grond van de artikel 126n/u/zh Sv. worden gevorderd. In dit geval is er namelijk geen sprake (geweest) van communicatieverkeer. Locatiegegevens kunnen, in het geval een telefoon op stand-by staat, wel worden gevorderd op grond van de artikel 126ng/ug jo. 126ne/ue Sv.

3.1.2 De bewaartermijn

In de MvT wordt in navolging van de richtlijn onderscheid gemaakt tussen aan de ene kant vaste en mobiele telefonie en aan de andere kant gegevens ter zake van internettoegang, e-mail en telefonie via internet. De richtlijn laat

25 *Stb.* 2002, 31. In een aantal landen van de Europese Unie worden kopers van prepaid telefoons geregistreerd. De bestandsanalyse was een door de aanbieders aangedragen alternatief voor de door hen niet gewenste registratie van kopers van een prepaid telefoonkaart.
26 *Stb.* 2004, 394, laatstelijk gewijzigd *Stb.* 2006, 730.

met betrekking tot de verplichte bewaartermijn ruimte om onderscheid te maken tussen deze categorieën. In het wetsvoorstel is er echter voor gekozen om een bewaartermijn van achttien maanden aan te houden voor alle te bewaren gegevens.
In de MvT is gekozen voor een bewaartermijn van achttien maanden, terwijl die – zoals we zagen – op basis van de richtlijn tussen de zes en vierentwintig maanden zou kunnen bedragen.
Deze keuze is gebaseerd op een aantal overwegingen. Allereerst zijn hierbij betrokken de uitkomsten van een onderzoek naar het gebruik van historische verkeersgegevens in de opsporing van Mevis et al. (2005). Volgens dit rapport zou een bewaartermijn van drie maanden gewoonlijk voldoende zijn, maar bij onder andere georganiseerde criminaliteit, fraude en ernstige levens- en geweldsdelicten zou er behoefte bestaan aan een langere bewaartermijn. Dit zou ook gelden bij cold cases en rechtshulpverzoeken. Volgens de Raad van Hoofdcommissarissen zou met name de bestrijding van georganiseerde criminaliteit en terrorisme een ruimere bewaartermijn noodzakelijk maken.
Ook in geval van vermissing van personen zouden, bij het aanhouden van een kortere bewaartermijn, de verkeersgegevens niet meer beschikbaar zijn wanneer deze persoon op een later moment teruggevonden wordt. Verder wijst de MvT er nog op dat door het gebruik van verkeersgegevens bij de opsporing zowel betrokkenheid van verdachten bij een delict kan worden vastgesteld als uitgesloten.
Al met al wordt ervoor gekozen om een zekere marge in te bouwen, zodat verkeersgegevens ook (nog) beschikbaar kunnen zijn voor meer complexe onderzoeken, cold cases en rechtshulpverzoeken.
De reden waarom niet gekozen is voor een bewaartermijn van vierentwintig maanden wordt – betrekkelijk kort – gemotiveerd door te stellen dat zolang de behoeft daaraan nog niet was gebleken, het opsporingsbelang niet zou opwegen tegen de kosten die daaraan verbonden zijn en de consequenties voor de persoonlijke levenssfeer.
Omdat de verwachting is dat internetgebruik en telefonie via internet in de toekomst alleen maar zal toenemen, is ervoor gekozen om eenzelfde bewaartermijn voor gegevens over telefonie en internet aan te houden.[27]
Alles afwegend, zo stelt de MvT, rechtvaardigt het grote belang van telecommunicatiegegevens voor de opsporing een bewaartermijn van achttien maanden, een termijn die men proportioneel acht in verhouding tot de belangen van de persoonlijke levenssfeer en de kosten die de bewaarplicht meebrengt.[28]

27 Aan die keuze lag ook ten grondslag een rapport van Bureau Verdonck, Klooster & Associates BV over de kosten die met implementatie van de bewaarplicht gemoeid zijn. Hierin zijn verschillende modellen doorgerekend met verschillende bewaartermijnen.
28 *Kamerstukken II*, 2006/07, 31 145, nr. 3, p. 9.

3.1.3 Bescherming van de persoonlijke levenssfeer

De verkeers- en locatiegegevens kunnen inzicht geven in de gedragingen van personen. Dat is juist het doel van het opvragen van die gegevens in het kader van een opsporingsonderzoek. Daarmee vindt een inbreuk plaats op de privacy van de desbetreffende personen. De bewaarplicht brengt mee dat, ter voldoening aan die bewaarplicht, gegevens bewaard blijven, ook zonder dat daartoe voor de bedrijven die over die gegevens beschikken nog langer een bedrijfsmatige noodzaak bestaat, bijvoorbeeld omdat de gegevens voor de eigen bedrijfsvoering, zoals facturering, nodig zijn.
Al langer bestond er een wettelijke basis op grond waarvan politie en justitie verkeersgegevens konden opvragen.[29] Door de Wet bewaarplicht is daarin geen wijziging gekomen. In geval van een verdenking van een misdrijf waarvoor voorlopige hechtenis is toegelaten, bij een redelijk vermoeden dat misdrijven in georganiseerd verband worden beraamd of gepleegd of bij aanwijzingen van een terroristisch misdrijf kon en kan een vordering tot verstrekking van verkeersgegevens worden gedaan (art. 126n, 126u en 126zh Sv.). Wel is het zo dat nu over een langere periode dan voorheen gegevens opgevraagd kunnen worden, omdat deze als gevolg van de nieuwe wetgeving langer bewaard dienen te blijven. Volgens de MvT wordt er dan ook geen verdergaande inbreuk gemaakt op de privacy van de (verdachte) burger; wel zullen in meer gevallen gegevens voor opsporing en vervolging beschikbaar zijn, hetgeen ook een doel is van het wetsvoorstel.
De MvT stelt dat de Wet bewaarplicht voldoet aan de eisen die uit het oogpunt van privacybescherming worden gesteld door artikel 8 Europees Verdrag van de Rechten van de Mens (EVRM) en artikel 10 van de Grondwet. De inbreuk op de privacy moet noodzakelijk zijn in een democratische samenleving en voldoen aan eisen van proportionaliteit en subsidiariteit. Hiernaast beoogt het wetsvoorstel te voorzien in waarborgen tegen misbruik of onzorgvuldig gebruik van de bewaarde gegevens. Daartoe moeten de aanbieders en telecombedrijven technische en organisatorische maatregelen nemen. Daarnaast is er de verplichtingen de bewaarde gegevens te vernietigen bij afloop van de bewaartermijn.
De klant van een aanbieder heeft recht op kennisneming van de gegevens die over hem worden bewaard,[30] ofschoon de verwachting is dat het aantal verzoeken om kennisneming beperkt zal blijven daar de gegevens over het belgedrag meestal aanwezig zijn op een gespecificeerde factuur. Het toezicht op

29 In de wet wordt onderscheid gemaakt tussen gegevens 'over een gebruiker van een communicatiedienst en het communicatieverkeer met betrekking tot die gebruiker' (art. 126n/u/zh Sv.) en gegevens 'ter zake van naam, adres, postcode, woonplaats, nummer en soort dienst van een gebruiker van een communicatiedienst' (art. 126na/zi Sv.). Deze twee categorieën van gegevens worden ook wel aangeduid als verkeersgegevens respectievelijk gebruikersgegevens.

30 Behoudens uitzonderingen in verband met het belang van opsporing of staatsveiligheid en de bescherming van de rechten van anderen dan de betrokkene (art. 43 WBP). De aanbieder mag geen mededeling doen van het feit of gegevens zijn verstrekt aan de AIVD of de MIVD (art. 35 WBP).

op naleving van de bepalingen uit het wetsvoorstel komt te liggen bij de Minister van Economische Zaken en het CBP.[31]

3.1.4 Notificatie

Als gebruik is gemaakt van strafvorderlijke bevoegdheden om gebruikersgegevens te vergaren, valt de vordering van de officier van justitie daartoe, tot verstrekking van gegevens over telecommunicatieverkeer,[32] onder de notificatieplicht van artikel 126bb Sv.[33] Dat houdt in dat de OvJ aan de betrokkene over wie gegevens zijn opgevraagd, mededeling moet doen zodra het belang van het onderzoek dit toelaat, behalve in gevallen waarin deze mededeling redelijkerwijs niet mogelijk is of betrokkene – als verdachte – door middel van de processtukken daarvan op de hoogte raakt.
Omdat deze mededelingsplicht reeds in het Wetboek van Strafvordering was opgenomen, was het niet nodig daar in het wetsvoorstel melding van te maken, aldus valt in de memorie van toelichting te lezen naar aanleiding van een opmerking van het CBP dat het wetsvoorstel aan notificatie geen aandacht besteedde. Inmiddels ligt een conceptwetsvoorstel[34] voor waarin wordt voorgesteld de notificatieplicht af te schaffen voor zover het gaat om het vorderen van verkeersgegevens. De belangrijkste reden hiervoor is, aldus het wetsvoorstel, dat de uitvoering van de notificatieplicht door het OM in de praktijk een buitengewoon zware administratieve belasting vormt. Om deze belasting te beperken, wordt voorgesteld de notificatieplicht tot de meer ingrijpende opsporingsbevoegdheden te beperken: 'Voor de bevoegdheden die een zware inbreuk maken op de privacy van de betrokken burgers blijft de notificatieplicht onverkort gehandhaafd. Voor die bevoegdheden die een minder zware inbreuk maken op de privacy wordt de notificatieplicht afgeschaft.'

Met betrekking tot het vorderen van verkeersgegevens wordt gesteld dat deze bevoegdheid een relatief lichte inbreuk op de privacy meebrengt en dat deze opsporingsbevoegdheid nagenoeg standaard in een opsporingsonderzoek wordt toegepast. 'Hoewel informatie betreffende de persoon kan worden verkregen, worden de gegevens door of bij derden beheerd. Bovendien weet de burger dat ook anderen dan hijzelf bij deze derden toegang tot de gegevens kunnen hebben.'

31 *Kamerstukken II*, 2006/07, 31 145, nr. 3, p. 13 en 28.
32 Op grond van de artikelen 126n, 126u en 126z Sv.
33 Met de Wet BOB, die op 1 februari 2000 van kracht is geworden (*Stb.* 1999, 245), is voorzien in een wettelijke regeling van een aantal bijzondere opsporingsbevoegdheden. De inzet van deze bevoegdheden vindt plaats zonder dat degene, jegens wie een bevoegdheid wordt ingezet, daarvan kennis heeft. Er is voorzien in een schriftelijke mededelingsplicht achteraf, die is vastgelegd in artikel 126bb Sv.
34 Conceptwetsvoorstel tot wijziging van het Wetboek van Strafvordering en het Wetboek van Burgerlijke Rechtsvordering in verband met de versterking van het presterend vermogen van de politie. Zie www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2012/09/03/consultatieversie-conceptwetsvoorstel.html (geraadpleegd op 1 mei 2013).

3.1.5 Behandeling wetsvoorstel in de Eerste Kamer

In de Eerste Kamer is uitgebreid stilgestaan bij de Wet bewaarplicht. Er is een hoorzitting met experts gehouden over het onderwerp en de gedachtewisseling tussen leden van de Eerste Kamer en de Minister van Justitie heeft onder andere geleid tot een toezegging van de kant van de minister dat de bewaartermijn voor internetgegevens zal worden teruggebracht van een jaar tot zes maanden. Een wetswijziging van die strekking[35] is 5 juli 2011 van kracht geworden. De schriftelijke gedachtewisseling met de Eerste Kamer en het debat spitsten zich in hoofdzaak toe op drie onderwerpen: de gevolgen voor de privacy van de burger; de effectiviteit van de bewaarplicht voor de opsporing; de kosten en lasten voor het bedrijfsleven. Dit alles tegen de achtergrond van de beoordeling van nut, noodzakelijkheid en proportionaliteit van de wetgeving en een daarbij passende bewaartermijn. Omdat de uitvoerige behandeling van het wetsvoorstel in de Eerste Kamer een goed inzicht geeft in de gewisselde argumenten pro en contra het wetsvoorstel (die deels ook bij de behandeling in de Tweede Kamer aan bod zijn gekomen), staan we daar in het navolgende wat uitgebreider bij stil.

3.1.6 Kosten

De kosten voor het bedrijfsleven worden door de minister in de memorie van antwoord aan de Eerste Kamer lager ingeschat dan ten tijde van de beraadslaging in de Tweede Kamer het geval was. Toen was op basis van een rapport van bureau Verdonck, Klooster & Associates BV[36] becijferd dat, uitgaande van een bewaartermijn van een jaar, de additionele kosten voor een opslag van twee jaar 14 miljoen euro zouden bedragen en bij verkorting van de termijn met een halfjaar, de kosten naar verwachting 7 miljoen euro lager zouden uitkomen.[37]
Als gevolg van de sterke daling van de kosten voor opslag van data zou met de dan geldende stand van de techniek de verkorting van de bewaartermijn met een halfjaar, een verlaging van de kosten van – nog maar – 4 miljoen euro meebrengen.[38] De minister gaat ervan uit dat een langere bewaartermijn niet evenredig meer kosten en belasting voor de bedrijven met zich meebrengt.[39]
In de verdere discussie over de effecten van de bewaarplicht voor het bedrijfsleven speelt het kostenaspect van de opslag geen (grote) rol meer. Dat geldt niet voor de positie van met name de kleine internetaanbieders (Internet Service Providers (ISP's)) die naar verhouding met hogere kosten te maken zouden krijgen als gevolg van de eisen die aan de beveiliging en

35 *Kamerstukken II* 2009/10, 32 185, nr. 2.
36 Verdonck, Klooster & Associates 'Onderzoek naar de nationale implementatie van de Europese richtlijn Dataretentie' d.d. 9 oktober 2006.
37 *Kamerstukken II* 2006/07, 31 145, nr. 3.
38 Eerder was gerekend met een bedrag aan kosten van € 34.000 per terabyte, terwijl die kosten later waren gedaald tot € 2.200 per terabyte. *Kamerstukken I* 2008/09, 31 145, C, p. 17.
39 *Handelingen I* 2008/09, 40, p. 1845.

opslag van de gegevens worden gesteld.[40] Onder andere uit de gehouden expertmeeting was gebleken dat de kleinere internetaanbieders voor relatief hoge kosten zouden komen te staan, daarbij in aanmerking genomen de verwachting dat het aantal bevragingen gering zou zijn.[41] Daarnaast zouden deze bedrijven[42] qua inrichting en gebruikte systemen zeer verschillend zijn, hetgeen standaardisatie van opslag bemoeilijkte. De minister heeft toegezegd de bijzondere positie van de kleinere ISP's in ogenschouw te nemen en met hen in overleg te treden. Het AT zou gevraagd worden een nulmeting te organiseren om na te gaan hoe de bewaarplicht door internetaanbieders wordt gerealiseerd en of redelijkerwijs van hen gevraagd kan worden dat zij (reeds) in de opstartperiode de benodigde voorzieningen zouden treffen. Deze toezegging hield verband met het feit dat voor september 2010 een Europese evaluatie van de richtlijn gegevensbewaring was voorzien die naar de mening van de een aantal Kamerfracties beter afgewacht kon worden, alvorens de internetaanbieders met hoge kosten op te zadelen.

3.1.7 Effectiviteit van de wet

Verschillende fracties in het parlement plaatsten vraagtekens bij de effectiviteit van de bewaarplicht, waarbij onderscheid valt te maken tussen enerzijds telefonieverkeersgegevens en anderzijds internetverkeersgegevens.
In algemene zin achtte men onvoldoende onderbouwd dat telefoniegegevens een relevante bijdrage aan de opsporing leverden, met name trok men in twijfel of daarvoor een langere bewaartermijn nodig was dan de zes maanden die de richtlijn als minimumgrens hanteert.
Zo vroeg de VVD-fractie naar het aantal onderzoeken waarin verkeersgegevens van belang waren gebleken en of dit dan van doorslaggevend, overwegend of ondergeschikt belang was geweest. De minister verwijst voor het aantonen van het nut van verkeersgegevens naar het rapport van Mevis et al. (2005), adviezen van het College van Procureurs-Generaal, de politie en enkele voorbeelden uit de jurisprudentie waarin verkeersgegevens een rol hebben gespeeld. Een langere bewaartermijn van verkeersgegevens zou vooral diensten bewijzen bij langer lopende onderzoeken naar georganiseerde criminaliteit, bij onderzoeken naar vermissingen, waarbij pas op een later moment duidelijk kan worden dat er sprake is van een strafbaar feit, en bij rechtshulpverzoeken in verband met de tijd die vaak gemoeid zijn met de uitvoering van een rechtshulpverzoek. Ook bij minder complexe onderzoeken zou pas op een later moment in het opsporingsonderzoek kunnen blijken dat bepaalde gegevens van belang zijn. Daarnaast is herhaalde malen het doen van onderzoek naar cold cases genoemd, hoewel dit argument minder valide is omdat onderzoek naar cold cases het opnieuw openen van een

40 Uitgewerkt in het Besluit beveiliging telecommunicatie (*Stb.* 2004, 394), laatstelijk gewijzigd *Stb.* 2012, 615.
41 *Kamerstukken I* 2008/09, 31 145, F, p. 14 (NMvA).
42 Het onderzoek van Verdonck, Klooster & Associates ging uit van een aantal van 255 kleinere internetaanbieders.

opsporingsonderzoek naar oude onopgeloste zaken betreft. Dat brengt mee dat een bewaartermijn van een jaar, maar ook van twee jaar, niet zal voorzien in de beschikbaarheid van verkeersgegevens daterend van rond de tijd dat het delict werd gepleegd.
De gegevens die op grond van de bewaarplicht voorhanden zijn, zouden met name inzicht kunnen bieden in de relatie tussen dader en slachtoffer en daarnaast in de aard en samenstelling van criminele netwerken.[43] Volgens de Minister zou in algemene zin gelden dat hoe eerder de gegevens vernietigd zouden worden, hoe groter het risico zou zijn dat ernstige strafzaken onopgelost blijven.

Met betrekking tot de effectiviteit van het gebruik van internetgegevens is de scepsis bij de leden van de Eerste Kamer groter. Mede naar aanleiding van het overleg met de expertgroep werd van verschillende kanten gewezen op de enorme omvang van de data die opgeslagen zouden moeten worden, waarbij dan nog het overgrote deel spam zou betreffen. Schattingen liepen daaromtrent op tot 95% van het e-mailverkeer. Daarbij zou naarmate de opslag van bewaarde gegevens zou toenemen, ook de kans op fouten in de data groter worden, naast het risico en de gevolgen van verlies van grote aantallen gegevens, zoals voorbeelden uit het buitenland hadden aangetoond.[44] In dit licht is verwezen naar een in de *NRC* van 21 mei 2008 gepubliceerde ingezonden brief van een aantal hoogleraren, waarin onder meer werd betoogd dat onschuldige burgers last zullen krijgen van fouten die onvermijdelijk in de praktijk gemaakt zullen worden. Fouten in de opslag van gegevens zouden leiden tot huiszoekingen en dwangmaatregelen op onjuiste gronden. Voor het aanzienlijke aandeel van spam in het internetverkeer memoreerde de minister als mogelijke maatregel dat spam door de aanbieders wordt uitgefilterd, zodat de overdracht van het bericht aan de ontvanger (eindgebruiker) niet tot stand komt. In dat geval hoeft de aanbieder de data van die e-mail dan niet te bewaren.[45]
Verder is erop gewezen dat de bewaarplicht verkeersgegevens eenvoudig omzeild kon worden door gebruik te maken van telecommunicatiediensten die niet onder de werkingssfeer van de wet vallen[46] zoals Hotmail, Gmail, Windows Live Messenger en Skype.[47] Ook zou het mogelijk zijn via bepaalde software de ware identiteit van de gebruiker te verhullen of zelfs die van een ander aan te nemen. Manipuleerbaarheid van digitale data zou dataretentie tot een bron van schijnveiligheid maken. In reactie hierop heeft de minister geantwoord dat niettegenstaande het gebruik van dergelijke diensten, nog steeds gebruik wordt gemaakt van telecommunicatie via de mobiele telefoon

43 *Kamerstukken I* 2008/09, 31 145, C, p. 3.
44 *Kamerstukken I* 2007/08, 31 145, B, p. 7.
45 Dit was een oplossingen die op 22 januari 2009 in een informeel overleg was besproken tussen experts over de implementatie van de Richtlijn dataretentie. *Kamerstukken I* 2008/09, 31 145, F, p. 3 (NMvA).
46 Buitenlandse e-mail- en internetdiensten vallen niet onder de Wet bewaarplicht; zie hierover Hoofdstuk 2.
47 Ook in de Tweede Kamer is dit punt besproken.

en van traditionele e-mail waarbij gebruik wordt gemaakt van Nederlandse aanbieders.[48] De discussie had in de kern de strekking dat alleen nog domme boeven zich lieten vangen als gevolg van het gebruik van verkeersgegevens bij de opsporing, maar dat de slimme boeven de dans ontsprongen; een punt dat eveneens in de expertmeeting naar voren was gebracht. De minister erkende dat 'handige lieden' bij telecommunicatie een en ander kunnen omzeilen en dat datgene wat daarover in de expertmeeting naar voren was gebracht, bekend was bij iedereen die een beetje geraffineerd met telecommunicatie weet om te gaan. Evenwel kwam het ook voor dat slimme boeven onder omstandigheden gemakzuchtig waren en dat ook telefoontaps nog steeds nuttig waren voor de opsporing.[49] De genoemde bezwaren hadden overigens meer betrekking op het relatieve nut van internetgegevens dan op het gebruik van verkeersgegevens met betrekking tot telefonie.

3.1.8 Privacy

De Wet bewaarplicht raakt aan de privacy van de burgers. Dit roept de vraag op hoe de Wet bewaarplicht zich verhoudt tot het in artikel 10 Grondwet en artikel 8 EVRM[50] gegarandeerde recht op privacy. Het bewaren van de gegevens als gevolg van de Wet bewaarplicht zou op twee manieren inbreuk (kunnen) maken op de privacy. Allereerst neemt door het louter opslaan van die gegevens het risico toe dat onbevoegden – zoals hackers – toegang krijgen tot die gegevens. De kans op een dergelijke schending van de privacy zou toenemen naarmate de bewaartermijn van de gegevens langer is. Een tweede en andersoortige inbreuk vindt plaats op het moment dat politie en justitie de beschikking krijgen over bewaarde gegevens in het kader van een onderzoek. Een beperking op het recht op privacy is volgens het EVRM pas dan toegestaan als deze bij wet is voorzien en noodzakelijk is in een democratische samenleving. Ten aanzien van de noodzakelijkheid zijn door Kamerfracties kritische kanttekeningen gemaakt. Zo moest, naar het oordeel van de CDA-fractie, gelet op de hiervoor besproken twijfel aan de waarde van verkeersgegevens voor de opsporing, de behoefte van politie en justitie daaraan eerder als wens '(nice to have)' worden beschouwd dan als noodzaak '(must)'.[51] In het verlengde daarvan ligt de geuite vraag of politie en justitie niet evengoed met de klassieke opsporingsmiddelen uit de voeten zouden kunnen.

48 *Kamerstukken I* 2008/09, 31 145, C, p. 30.

49 Het Lid Franken (CDA) meende dat de maatregel, gelet op de mogelijkheden tot omzeiling daarvan, alleen zou werken bij de zeer domme boeven, die geen gebruikmaken van Skype en Hotmail. *Handelingen I* 2008/09, 39, p. 1808. Overigens is ook in het arrest van het Bundesverfassungsgericht met zo veel woorden overwogen dat het loutere feit dat criminelen de opslag van data kunnen omzeilen nog niet aan de geschiktheid van een dergelijke regeling hoeft af te doen.

50 Artikel 8 lid 1: Een ieder heeft recht op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie, lid 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.

51 *Kamerstukken I* 2008/09, 31 145, C, p. 5.

Naar het oordeel van de minister waren verkeersgegevens echter van dermate groot belang voor de opsporing en vervolging van ernstige misdrijven dat aan het noodzakelijkheidscriterium werd voldaan.[52] Volgens de minister wordt de aantasting van de privacy niet zozeer veroorzaakt door het bewaren van de gegevens, als wel door de toegang tot die gegevens.[53] Gelet op de waarborgen waarmee de opslag van gegevens is omgeven (als uitgewerkt in een ontwerpbesluit beveiliging gegevens), zou het langer bewaren van gegevens geen extra nadeel voor burgers met zich meebrengen.[54]
Over de vraag of het louter bewaren van gegevens niet reeds een (ernstige) inbreuk op de privacy vormde, dacht de Eerste Kamer overwegend anders, waarbij onder meer werd verwezen naar een uitspraak van het *Bundesverfassungsgericht*[55] waaruit naar voren kwam dat reeds de opslag van verkeersgegevens als een inbreuk op de persoonlijke levenssfeer dient te worden beschouwd.

De toegang tot en het gebruik van verkeersgegevens vormt onomstotelijk een inperking van of – afhankelijk van de opvatting[56] – een inbreuk op de privacy van burgers. In het Wetboek van Strafvordering is geregeld wie onder welke voorwaarden toegang heeft tot de opgeslagen telecom- en internetgegevens.
Het vorderen van verkeersgegevens: de OvJ kan een vordering doen tot verstrekking van verkeersgegevens (art. 126n, 126u Sv.) in geval van verdenking van een misdrijf waarvoor voorlopige hechtenis mogelijk is en bij een redelijk vermoeden dat in georganiseerd verband misdrijven worden beraamd of gepleegd.
Een opsporingsambtenaar kan identificerende gegevens vorderen (art. 126na, 126ua Sv). In dat geval is verdenking van een misdrijf of een redelijk vermoeden van betrokkenheid bij georganiseerde criminaliteit voldoende. De gegevens die opgevraagd kunnen worden zijn de zogenaamde gebruikersgegevens (naam, adres, woonplaats, nummer en soort dienst). In geval van aanwijzingen van een terroristisch misdrijf kan de OvJ verkeersgegevens opvragen (art. 126zh Sv.) en kan een opsporingsambtenaar gebruikersgegevens vorderen (art. 126zi Sv.). Verder kan de OvJ bij een verkennend onderzoek naar terroristische misdrijven gegevensbestanden van publieke en particuliere instanties vorderen om de hierin opgenomen gegevens te doen bewerken (art. 126hh Sv.). Ofschoon deze wettelijke regeling voor het opvragen van de verschillende gegevens reeds bestond voor en onafhankelijk van de Wet bewaarplicht, is er in zoverre een relatie met de bewaarplicht dat naarmate er meer gegevens langer bewaard kunnen worden, daarmee ook het aantal bevragingen zal toenemen. Daarom is wel de vrees geuit dat de

52 *Kamerstukken I* 2008/09, 31 145, C, p. 11; *Kamerstukken I* 2008/09, 31 145, F, p. 12.
53 *Kamerstukken I* 2008/09, 31 145, C, p. 7.
54 *Kamerstukken I* 2008/09, 31 145, F, p. 6 (NMvA).
55 Van 11 maart 2008.
56 Zie hierover de discussie in Eerste Kamer over het juridische verschil in betekenis tussen de inbreuk op, of de inperking van, een recht.

opslag van gegevens zou leiden tot 'een grabbelton' waarin politie en justitie vrijuit konden zoeken. Volgens de minister kon daarvan geen sprake zijn, nu toegang tot en gebruik van die gegevens vallen onder het regime van strafvordering.[57] Weliswaar werden van grote groepen niet-verdachten gegevens opgeslagen, maar het opslaan diende volgens de minister van de toegang tot de gegevens te worden onderscheiden.

Het oordeel dat de noodzaak van de Wet bewaarplicht onvoldoende is aangetoond, leidde bij een aantal Kamerfracties tot de stelling dat daardoor de bewaartermijn zo kort mogelijk gesteld diende te worden, dat wil zeggen op zes maanden, de termijn die de richtlijn als minimum hanteert. De minister pleitte voor een bewaartermijn voor telefonie en internetverkeer van een jaar. Voor beide dus een gelijke periode, onder meer met het argument dat telefonie via internet de traditionele telefonie zou vervangen;[58] hij nam daarmee een voorschot op de komende ontwikkelingen.
In de beraadslagingen met de Eerste Kamer bleek een opslagtermijn van een jaar voor internetgegevens, gezien de oppositie daartegen, niet houdbaar. Dit heeft geleid tot de hiervoor reeds genoemde toezegging van de minister om de bewaartermijn van internetgegevens, ná de aanneming door de Eerste Kamer van de Wet bewaarplicht waarin nog een bewaartermijn van een jaar was opgenomen, via een wetswijziging terug te brengen tot zes maanden, hetgeen 5 juli 2011 is geschied.[59] Al met al is de bewaartermijn van telecom- en internetgegevens van de aanvankelijke in het wetsvoorstel opgenomen achttien maanden, met de aanneming van het amendement Anker,[60] verminderd tot twaalf maanden en als gevolg van de behandeling van het wetsvoorstel in de Eerste Kamer is daar voor internetgegevens nog eens zes maanden van afgegaan.

Zoals uit het voorgaande moge blijken, zag de Eerste Kamer zich gesteld voor het voldoen aan een Europese richtlijn 'contre coeur' nu 'Europa' daartoe verplichtte.[61] Dat had tot gevolg dat met name de Eerste Kamer de Europese ontwikkelingen op het gebied van dataretentie kritisch en proactief volgt. Zo zijn de in de Eerste Kamer uitgedragen bezwaren tegen de bewaarplicht opnieuw herhaald in een kritische reactie van de Raad Justitie en Binnenlandse Zaken (JBZ-raad)[62] en de vaste commissie voor justitie op een rapport met een evaluatie van de Europese Commissie van de richtlijn dataretentie.[63]

57 De op te vragen gegevens zijn aangewezen in het Besluit vorderen gegevens telecommunicatie (*Stb.* 2004, 394), laatstelijk gewijzigd *Stb.* 2006, 730.
58 *Kamerstukken I* 2008/09, 31 145, C, p. 8.
59 *Kamerstukken II* 2009/10, 32 185, nr. 2.
60 *Kamerstukken II* 2007/08, 31 145, nr. 14.
61 *Handelingen I,* 7 juli 2009, 40, p. 183 e.v. Zo merkte het lid Franken (CDA) op dat bepaalde gewisselde argumenten tegen de richtlijn waren, en niet zozeer de wet golden. Daarom diende men naar Brussel te gaan om de richtlijn veranderd te krijgen.
62 De raadsformatie Justitie en Binnenlandse Zaken.
63 Verslag van de Commissie aan de Raad en het Europees Parlement, Evaluatie van de richtlijn gegevensbewaring (Richtlijn 2006/24/EG). *Kamerstukken I* 2010/11, 32 797, A.

Deze bezwaren behelzen kort gezegd dat een overtuigende analyse van de noodzaak (*pressing social need*) van de richtlijn ontbreekt; dat er onvoldoende aandacht is voor de proportionaliteit van de maatregel; dat het rapport niet de vele mogelijkheden bespreekt die er zijn om de bewaarplicht te omzeilen en er veel vragen blijven leven over de effectiviteit van de richtlijn.[64] De daartoe in het rapport aangehaalde casusposities ter staving van het nut van dataretentie voor het strafrecht overtuigen beide commissies niet. Meer in het in bijzonder gold dat de door Nederland aangedragen casusposities, waarbij de evaluatie ten onrechte sprak van het opleveren van bewijs. 'Dit terwijl (aldus de reactie van de commissie) bewaargegevens[65] niet meer kunnen zijn dan een opsporingsmiddel dat aanleiding geeft om tot bewijs te komen.' Dit laatste is overigens niet geheel juist. In hoofdstuk 6 van dit rapport zijn voorbeelden opgenomen van rechterlijke uitspraken, waarin verkeers- en locatiegegevens direct als bewijs gebezigd zijn.

3.2 De Europese richtlijn

3.2.1 Europese achtergrond voor de bewaring van gegevens

Volgens de richtlijn gegevensbewaring moeten de lidstaten aanbieders van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken verplichten verkeers- en locatiegegevens tussen de zes maanden en twee jaar te bewaren voor het onderzoeken, opsporen en vervolgen van zware criminaliteit.[66]
Aanbieders van (tele)communicatiediensten verwerken, als onderdeel van hun werkzaamheden, persoonsgegevens met betrekking tot de tot stand gebrachte communicatie en bijvoorbeeld de facturering. Uit deze gegevens zijn onder meer de bron, de datum en het tijdstip, de duur, de locatie en de aard van de communicatie af te leiden. Op grond van Richtlijn 2002/58/EG betreffende privacy en elektronische communicatie moeten dergelijke verkeersgegevens uit oogpunt van privacybescherming in principe worden gewist of anoniem gemaakt, wanneer ze voor de dienstverlening als facturering niet langer noodzakelijk zijn.[67]
Voor de inwerkingtreding van de richtlijn konden de autoriteiten, in het belang van de rechtshandhaving, onder bepaalde voorwaarden de aanbieders toegang tot dergelijke gegevens vragen. Zo kon bijvoorbeeld worden opgevraagd welke abonnees een bepaald IP-adres gebruikten of waar een mobiele telefoon zich op een bepaald moment bevond.

64 *Kamerstukken I* 2010/11, 32 797, A, p. 2.
65 Waarschijnlijk wordt bedoeld: bewaarde verkeersgegevens.
66 De richtlijn is van toepassing op telefonie over een vast netwerk, mobiele telefonie, internettoegang, e-mail over het internet en internettelefonie (art. 1, lid 2; art. 3, lid 2, en art. 5).
67 Tenzij de abonnee of gebruiker er toestemming voor geeft deze gegevens te bewaren.

In Richtlijn 97/66/EG is voor het eerst het gebruik van gegevens voor de rechtshandhaving op EU-niveau geregeld. Die richtlijn gaf de mogelijkheid (maar niet de verplichting) om wettelijke maatregelen te treffen met het oog op – onder andere – de bescherming van de openbare veiligheid, de staatsveiligheid en de wetshandhaving op strafrechtelijk gebied. De e-privacyrichtlijn biedt de lidstaten de mogelijkheid bij wet af te wijken van het beginsel dat communicatie vertrouwelijk is en geeft aan onder welke voorwaarden het bewaren van, de toegang tot en het gebruik van gegevens voor rechtshandhavingsdoeleinden wordt toegestaan. Op grond van artikel 15, lid 1, van de Richtlijn 97/66/EG kunnen de lidstaten privacyrechten en -plichten beperken, bijvoorbeeld door gegevens voor een bepaalde periode te bewaren, 'indien dat in een democratische samenleving noodzakelijk, redelijk en proportioneel is ter waarborging van de nationale veiligheid, dat wil zeggen de staatsveiligheid, de landsverdediging, de openbare veiligheid of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of van onbevoegd gebruik van het elektronische-communicatiesysteem'.

Als gevolg van in het kader van Richtlijn 97/66/EG en e-privacyrichtlijn door verschillende lidstaten aangenomen wetgeving, ontstond de noodzaak voor aanbieders in die landen om apparatuur aan te schaffen en personeel in dienst te hebben om aan verzoeken van de rechthandhavende autoriteiten om informatie te kunnen voldoen. Dit, terwijl er in andere landen niet een dergelijke verplichting was. Dit leidde tot een verstoring van de interne markt. Hiernaast leidden ontwikkelingen in de dienstverlening door aanbieders ertoe dat er steeds minder verkeers- en locatiegegevens werden opgeslagen voor facturatie, waardoor er ook minder van dergelijke gegevens voor gebruik bij de rechtshandhaving beschikbaar waren. Mede aangejaagd door de terroristische aanslagen in Madrid in 2004 en in Londen in 2005, is tegen deze achtergronden de EU-richtlijn voor het bewaren van telecommunicatiegegevens aangenomen, welke voor alle lidstaten de verplichting in het leven roept om communicatiegegevens te bewaren, zodat deze beschikbaar zijn voor het onderzoeken, opsporen en vervolgen van ernstige criminaliteit. De richtlijn wijzigde artikel 15, lid 1, van de e-privacyrichtlijn door middel van een nieuwe bepaling die inhoudt dat artikel 15, lid 1, niet van toepassing is op gegevens die worden bewaard uit hoofde van de richtlijn gegevensbewaring.[68] Noch in de richtlijn, noch in de e-privacyrichtlijn is een definitie opgenomen van 'ernstige criminaliteit'.

68 Artikel 11 van de richtlijn luidt: In artikel 15 van Richtlijn 2002/58/EG wordt het volgende lid ingevoegd: '1 bis. Lid 1 is niet van toepassing op de uit hoofde van Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken te bewaren gegevens voor de in artikel 1, lid 1, van die richtlijn bedoelde doeleinden.'

3.2.2 Te bewaren data

In artikel 5 van de richtlijn worden de te bewaren categorieën gegevens genoemd:
- de bron van een communicatie;
- de bestemming van een communicatie;
- de datum, het tijdstip en de duur van een communicatie;
- het type communicatie;
- de communicatieapparatuur of de vermoedelijke communicatieapparatuur van de gebruikers; en
- de locatie van mobiele communicatieapparatuur.

De richtlijn heeft ook betrekking op oproeppogingen zonder resultaat.[69] Er mogen geen gegevens worden bewaard waaruit de inhoud van de communicatie kan worden opgemaakt.[70] Behoudens in België, voorziet de omzettingswetgeving in eenentwintig lidstaten in de bewaring van elk van deze categorieën gegevens.[71]

3.2.3 Omzetting richtlijn in de landen van de Europese Unie

De lidstaten dienden de richtlijn vóór 15 september 2007 in wetgeving te hebben omgezet; voor de bewaringsverplichting van internetgegevens was er respijt tot 15 maart 2009. In onder meer Oostenrijk en Zweden is de richtlijn nog niet omgezet in wetgeving. In Tsjechië, Duitsland en Roemenië hebben de constitutionele hoven van elke land de wetgeving ter omzetting van de richtlijn in die landen nietig verklaard.[72] De rechtsgrond van de richtlijn is vergeefs door Ierland aangevochten voor het Europese Hof van Justitie, omdat hoofddoel van de richtlijn zou zijn het onderzoeken, opsporen en vervolgen van ernstige criminaliteit. Daarmee zou de richtlijn onder de derde pijler, politiële en justitiële samenwerking in strafzaken, van de Europese Unie vallen. Het Hof was echter onder meer van oordeel dat de richtlijn handelingen regelt die losstaan van de uitvoering van enige eventuele vorm van politiële en justitiële samenwerking in strafzaken en dat de richtlijn in wezen de activiteiten van aanbieders van diensten in de betrokken sector van de interne markt betreft.[73]

69 Artikel 3, lid 2.
70 Dit geldt ook voor zoekopdrachten (*serverlogs*) omdat zij niet als verkeersgegevens, maar als inhoud beschouwd moeten worden.
71 Verslag van de Commissie aan de Raad en het Europese Parlement, Evaluatie van de richtlijn gegevensbewaring (Richtlijn 2006/24/EG, Publicatieblad van de Europese Unie, 13 april 2006).
72 Beslissing nr. 1258 van 8 oktober 2009 van het Roemeense constitutionele hof, Roemeens staatsblad nr. 789 van 23 november 2009; arrest van het Bundesverfassungsgericht 1 BvR 256/08 van 2 maart 2010, staatsblad van 1 april 2011; arrest van het Tsjechische constitutionele hof van 22 maart over de bepalingen van hoofdstuk 97, punt 3 en 4 van wet nr. 127/2005 over elektronische communicatie en tot wijziging van bepaalde daarmee verband houdende besluiten en decreet nr. 485/2005 over gegevensbewaring en doorgifte aan de bevoegde autoriteiten.
73 HvJ EG 10 februari 2009, nr. C-301/06 (Ierland/Europees Parlement en Raad van de Europese Unie).

In de landen waarin de richtlijn wel in geldende wetgeving is omgezet, is de duur van de gekozen bewaartermijn sterk verschillend. De bandbreedte die de richtlijn biedt, namelijk een bewaarplicht tussen minimaal 6 maanden en maximaal 24 maanden wordt geheel benut. Enkele landen, waaronder Nederland, hebben gekozen voor een in duur verschillende bewaarplicht, namelijk een die afhankelijk is van het type gegevens dat wordt opgeslagen. Grosso modo wordt hier onderscheid gemaakt tussen gegevens die betrekking hebben op verkeer via internet en telefonie. De opslagduur voor internetverkeer is dan telkens korter dan die van gegevens die betrekking hebben op vaste en mobiele telefonie.

Bij de kortste bewaarperiode beginnend is het volgende overzicht te geven.[74] Twee landen hanteren de minimale bewaartermijn van zes maanden, namelijk Cyprus en Luxemburg. Drie landen, te weten Malta, Nederland en Slowakije, hanteren een bewaartermijn van één jaar voor vaste en mobiele telefonie en van zes maanden voor internetgegevens. Elf landen hebben gekozen voor een bewaartermijn van één jaar: België, Bulgarije, Denemarken, Estland, Finland, Frankrijk, Griekenland, Hongarije,[75] Spanje, Portugal en het Verenigd Koninkrijk.[76] Slovenië en Letland hebben gekozen voor respectievelijk veertien (acht maanden voor internetgegevens) en achttien maanden. Drie landen, Italië, Ierland en Polen, hanteren de maximale opslagtermijn van twee jaar.
Uit dit overzicht blijkt dat met betrekking tot vaste- en mobieletelefoniegegevens in meer dan de helft van de gevallen sprake is van een bewaartermijn van één jaar, namelijk bij 14 van de in totaal 23 landen die de richtlijn hebben geïmplementeerd. Waar het gaat om de opslag van internetgegevens, ligt de verhouding iets anders. Zes landen opteren dan voor een bewaartermijn van zes maanden en elf landen voor een periode van een jaar.[77]

Hiervoor is reeds opgemerkt dat de term 'ernstige criminaliteit' in de richtlijnen niet is gedefinieerd. Dit is terug te zien in de verschillende gronden die in de wetgeving van de lidstaten zijn opgenomen die toegang tot de bewaarde gegevens voor strafvorderlijke doeleinden mogelijk maken. In tien landen wordt wat betreft het criterium ernstige criminaliteit uitgegaan van strafbare feiten waar een minimum gevangenisstraf – of in elk geval een gevangenis-

74 Verslag van de Commissie aan de Raad en het Europees Parlement, Evaluatie van de richtlijn gegevensbewaring (Richtlijn 2006/24/EG, Publicatieblad van de EU, 13 april 2006).
75 Voor oproeppogingen zonder resultaat geldt een bewaartermijn van zes maanden.
76 In Finland en Engeland bestaat voor kleine aanbieders geen verplichting om gegevens te bewaren, omdat de kosten die dit voor hen mee zou brengen, niet in verhouding zouden zijn met de opbrengsten op strafvorderlijk terrein.
77 Lidstaten 'met specifieke omstandigheden die een in tijd beperkte verlenging (...) rechtvaardigen, kunnen de maximale bewaringstermijn verlengen.' Daarvoor dient een dergelijke verlenging aan de Commissie te worden voorgelegd, die de verlenging kan bekrachtigen dan wel verwerpen. De maximale bewaringstermijn kan daarmee worden verlengd, maar niet worden verkort.

straf – op staat en waarbij wordt verwezen naar een overzicht van delicten die elders in de nationale wetgeving is opgenomen.[78]
In acht landen[79] geldt dat gegevens kunnen worden bewaard voor onderzoek naar alle strafbare feiten en het voorkomen van criminaliteit in het algemeen of om algemene redenen van nationale veiligheid.[80] In vier landen is de term 'ernstige criminaliteit' dan wel 'een ernstig strafbaar feit' in de wetgeving opgenomen zonder nadere definitie. Een aantal landen is verdergegaan in het verlenen van toegang tot de gegevens dan de richtlijn voorschrijft, zoals het voorkomen en bestrijden van criminaliteit in het algemeen, waar de richtlijn spreekt over 'ernstige criminaliteit'. De bewoordingen van de e-privacyrichtlijn maken dit mogelijk.
Evenals voor de duur van de bewaartermijn, geldt hier dat de harmonisatie die met de EU-regelgeving is nagestreefd, slechts beperkt is verwezenlijkt. Naar het oordeel van de Commissie zijn als gevolg van die gebrekkige harmonisatie de kosten voor aanbieders in de verschillende landen niet gelijk, omdat verschillen in het doel van de gegevensbewaring maken dat het aantal verzoeken om gegevens tussen de lidstaten kan variëren. Daarnaast zou dit kunnen betekenen dat er onvoldoende sprake is van de voorspelbaarheid die moet worden gesteld aan de wettelijke maatregel die de privacy beperkt.
De toegang tot de gegevens door anderen dan de aanbieders zelf, is in de lidstaten eveneens verschillend uitgewerkt. In alle lidstaten gelden politie en OM als bevoegde autoriteit die toegang kan krijgen tot de gegevens. In elf landen is daarbij toestemming van de rechter nodig. In veertien lidstaten kan ook de veiligheidsdienst gegevens opvragen. Daarnaast zijn er landen waar dit ook geldt voor de douane of de Belastingdienst.

3.2.4 Evaluatie van de richtlijn

De Europese commissie heeft ingevolge artikel 14 de toepassing van de Richtlijn gegevensbewaring geëvalueerd.[81] Doel daarvan is te bezien of de richtlijn voldoet of dat deze mogelijk moet worden aangepast. Tevens wordt daarin het effect van de richtlijn op grondrechten behandeld, dit in verband met de algemeen geuite kritiek op het bewaren van gegevens. Daarnaast besteedt de evaluatie aandacht aan zorgen over het anoniem gebruik van simkaarten bij criminele praktijken.
Om zicht te houden op de uitvoering van de richtlijn zijn de lidstaten verplicht om jaarlijks statistische informatie te verstrekken aan de Commissie over de gevallen waarin gegevens zijn opgevraagd, de ouderdom van de gege-

78 Bulgarije, Estland, Ierland, Griekenland, Spanje, Litouwen, Luxemburg, Hongarije, Nederland en Finland (zie: Evaluatieverslag van de Europese Commissie betreffende de Europese dataretentierichtlijn (COM (2011) 225 final), tabel 1, pp. 6-8).
79 Het rapport van de Europese Commissie is hier niet precies, omdat niet duidelijk wordt onderscheiden tussen de doelbinding bij het opslaan van gegevens en de toegang tot die gegevens voor strafvorderlijke doeleinden.
80 België, Bulgarije, Denemarken, Griekenland, Estland, Ierland, Spanje, Frankrijk.
81 Verslag van de Commissie aan de Raad en het Europees Parlement, Evaluatie van de richtlijn gegevensbewaring (Richtlijn 2006/24/EG, Publicatieblad van de EU, 13 april 2006).

vens[82] en de gevallen waarin de verzoeken konden worden ingewilligd. De aan de Commissie verstrekte statistieken verschilden qua omvang en gedetailleerdheid van de informatie, variërend van statistieken met informatie over soort communicatie en ouderdom van de gegevens tot statistieken zonder verdere indeling. In totaal hebben negentien lidstaten statistieken verstrekt over het aantal verzoeken om gegevens in 2009 en/of 2008. Daaronder vallen ook een aantal lidstaten die de richtlijn nog niet in wetgeving hadden omgezet of waarvoor gold dat de wetgeving nietig was verklaard. Zeven lidstaten die de richtlijn hadden omgezet in wetgeving, hebben geen statistieken verstrekt.

Over de inhoud van de statistieken kan worden gesteld dat de cijfers zeer moeilijk met elkaar kunnen worden vergeleken. Ook als het alleen gaat om kale tellingen van het aantal verzoeken om gegevensverstrekking, worden deze gegevens door de verschillende lidstaten verschillend geadministreerd (zie hierover ook Odinot et al., 2012, p. 295). In sommige lidstaten wordt bijgehouden over hoeveel personen verkeersgegevens worden opgevraagd, in andere over hoeveel nummers en IP-adresgegevens worden opgevraagd en in sommige landen, zoals Tsjechië, Letland en Polen, dient elk verzoek om gegevensverstrekking bij verschillende aanbieders te worden ingediend, waardoor elk verzoek diverse keren wordt ingediend en meegeteld. Of alle landen het aantal *verzoeken* tot gegevensverstrekking registreren, of dat er ook landen zijn die het aantal *daadwerkelijke gegevensverstrekkingen* registreren, wordt uit deze evaluatie niet duidelijk. In theorie is het mogelijk dat onbeantwoorde vragen in het ene land wel worden meegeteld in de statistieken (dit gebeurt bijvoorbeeld in Nederland, Tsjechië, Letland en Polen) en in het andere land niet. Door deze verschillen in de manier waarop de gegevens kunnen worden geregistreerd, loopt het aantal geregistreerde bevragingen tussen verschillende landen sterk uiteen van minder dan honderd per jaar (voor Cyprus) tot ruim één miljoen verzoeken per jaar (voor Polen).

In de evaluatie stelt de commissie vast dat de lidstaten later dan verwacht begonnen zijn met de toepassing van de richtlijn, vooral waar het om de internetgegevens gaat.[83] Een gevolg daarvan is dat niet door alle landen is voldaan aan de verplichting om alle statistische informatie, zoals is aangeduid in de richtlijn, aan de commissie te verstrekken.[84] In 2010 heeft de commissie de lidstaten gevraagd om informatie te geven over de mate waarin bewaarde verkeersgegevens van betekenis zijn geweest voor de rechtshandhaving. Tien landen hebben daaraan voldaan.

82 Dat wil zeggen, de tijdspanne tussen de datum waarop de gegevens zijn bewaard en de datum waarop de gegevens zijn opgevraagd.

83 De lidstaten dienden de richtlijn vóór 15 september 2007 in wetgeving te hebben omgezet, voor de bewaringsverplichting van internetgegevens was er respijt tot 15 maart 2009.

84 Genoemd in artikel 10 van de richtlijn. Negen lidstaten konden over de jaren 2008 en 2009 alle vereiste informatie verstrekken.

De lidstaten die een vragenlijst omtrent het nut van de gegevensbewaring hebben ingevuld, vinden de gegevensbewaring op zijn minst waardevol en in sommige gevallen onmisbaar voor het voorkómen en bestrijden van criminaliteit, de bescherming van slachtoffers en de vrijspraak van onschuldige personen in strafprocedures. Tsjechië vond de gegevens 'absoluut onmisbaar in veel gevallen'. Hongarije omschreef het als 'onmisbaar voor de activiteiten van rechtshandhavingsautoriteiten', Slovenië stelde dat het ontbreken van bewaarde gegevens de 'werking van rechtshandhavingsinstanties zou verlammen' en een politiedienst uit het Verenigd Koninkrijk gaf aan dat de beschikbaarheid van verkeersgegevens 'absoluut cruciaal' waren 'voor het onderzoek naar de dreiging van terrorisme en ernstige criminaliteit'.
Volgens de lidstaten konden met behulp van de bewaarde gegevens getuigen worden opgespoord die anders onbekend zouden zijn gebleven en bewijzen van of aanwijzingen voor medeplichtigheid aan een strafbaar feit worden geleverd. Sommige lidstaten beweerden ook dat dankzij bewaarde gegevens de onschuld van verdachten van strafbare feiten kon worden bewezen, zonder dat gebruik hoefde te worden van andere meer ingrijpende methoden, zoals interceptie en huiszoeking. Op grond van deze bevindingen wordt in de evaluatie geconcludeerd dat over het geheel genomen is aangetoond dat het bewaren van gegevens een waardevol instrument is voor de strafrechtsystemen en de rechtshandhaving. In de evaluatie wordt verder gesteld dat de richtlijn niet heeft geresulteerd in de gewenste harmonisatie als het gaat om doelbinding of bewaringstermijnen van gegevens. Met het oog op waarborging van de privacy en bescherming van de persoonsgegevens dient volgens de evaluatie te worden gestreefd naar een hoge mate van bescherming bij het opslaan en gebruik van verkeers- en locatiegegevens.

Hiervoor is reeds opgemerkt dat de term 'ernstige criminaliteit' in de richtlijnen niet is gedefinieerd. Dit is terug te zien in de verschillende gronden die in de wetgeving van de lidstaten zijn opgenomen die toegang tot de bewaarde gegevens voor strafvorderlijke doeleinden mogelijk maken.
Naast de richtlijn gegevensbewaring en de verplichtingen die daaruit voortvloeien, wijzen we hier nog op een andere EU-regeling die betrekking heeft op het bevriezen van gegevens (ook wel 'quick freeze' genoemd).[85]
Deze voorziet erin dat aanbieders naar aanleiding van een gepleegd strafbaar feit of van een verdenking daarvan een bevel kunnen krijgen om data vanaf een bepaald moment te bewaren.
In de discussie over voors en tegens van de bewaarplicht is wel aangevoerd dat bevriezing van gegevens, zodra daar een concrete aanleiding (een gepleegd ernstig misdrijf) toe bestaat, als alternatief kan dienen voor een veel verder strekkende algemene bewaarplicht van niet-verdachte burgers. Volgens de evaluatie zou nog niet onderzocht zijn in hoeverre de methode van bevriezen van gegevens vruchten afwerpt.

85 Artikel 16 van het Cybercrimeverdrag.

Met de betrekking tot de waarde voor de opsporing – op basis van informatie van een aantal lidstaten daarover – worden incidentele voorbeelden gegeven van concrete casus waarin telefonie- of internetgegevens hebben bijgedragen aan de oplossing van misdrijven. Zo kon aan de hand van IP-adressen onderzoek gedaan worden naar de leden van een internationaal pedofielennetwerk. Uit statistische informatie verstrekt over 2008 zou blijken dat in zo'n 90% van de gevallen informatie over een periode korter dan zes maanden was opgevraagd. Niettemin zou volgens de lidstaten informatie van een oudere datum dan zes maanden onder omstandigheden ook cruciaal voor de opsporing kunnen zijn. Hoewel geen statistische informatie voorhanden is over de waarde van opgevraagde gegevens voor het bewijs, zou het gebruik daarvan een vast onderdeel van de opsporing vormen.

3.3 Conclusie

Zowel in de Europese lidstaten als in het Nederlands Parlement werd zeer verschillend aangekeken tegen de noodzaak en wenselijkheid van een bewaarplicht van verkeersgegevens. De kosten van de implementatie daarvan, de inbreuk op de privacy van de burgers en de mate waarin het gebruik van verkeersgegevens zinvol en effectief was bij de opsporing en vervolging van misdrijven vormden in de discussie de belangrijkste kwesties. Een en ander heeft geleid tot een verschillende invoering van de richtlijn in de lidstaten waar het gaat om de termijnen waarover gegevens moeten worden opgeslagen en het gebruik van de gegevens. In die zin is de beoogde harmonisatie niet bereikt. In Nederland is uiteindelijk gekozen voor een bewaartermijn van een jaar voor telefoniegegevens en een halfjaar voor internetgegevens. Ofschoon er enig empirisch materiaal ten grondslag lag aan de gevoerde discussies over de effectiviteit van verkeersgegevens voor opsporing en vervolging (zie o.a. Mevis et al., 2005), verschafte dit maar een beperkte basis voor besluitvorming omtrent de lengte van de bewaartermijnen. Zo klonk er ook Nederlandse kritiek op de beperktheid van de gepresenteerde casus in de evaluatie van de Europese Commissie, zoals hiervoor genoemd. Dit gebrek aan empirische onderbouwing heeft overigens invloed gehad op de argumenten van zowel voor- als tegenstanders van (een uitbreiding van) de Wet bewaarplicht.

4 Het bewaren en beveiligen van de gegevens in de praktijk

In dit hoofdstuk wordt ingegaan op de rol van de aanbieders en de wijze waarop zij omgaan met de Wet bewaarplicht telecomgegevens, en op de rol van de toezichthouders: het AT en CBP. In dit hoofdstuk wordt beschreven hoe het toezicht op de bewaarplicht in de praktijk is geregeld. Echter, onderzoek naar de wijze waarop de toezichthouders hun controletaken verrichten, valt buiten de vraagstelling van dit onderzoek.
Voor het onderzoek zijn medewerkers op sleutelposities van twee grote aanbieders, een kleine aanbieder en een internethosting bedrijf, geïnterviewd. Daarnaast zijn interviews gehouden bij het AT en het CBP. We beschrijven in dit hoofdstuk eerst de rol van de toezichthouders. Voorts komen de aanbieders van telecommunicatiediensten aan bod.

4.1 De toezichthouders

De Wet bewaarplicht bevat niet alleen regels over de aard van de gegevens die moeten worden bewaard, de bewaartermijnen van deze gegevens en de omstandigheden waaronder deze gegevens door bepaalde diensten mogen worden gebruikt. De wet beschrijft tevens hoe het toezicht op naleving hiervan moet worden ingericht. Het gaat om het bewaren van privacygevoelige data. Het is dus van belang dat de bewaarde gegevens niet gebruikt worden door andere instanties of voor andere doelen dan waarvoor ze worden opgeslagen. Dit toezicht op de naleving van de regels ligt in handen van het AT, dat opereert als een onafhankelijke toezichthouder en toeziet op de naleving van de Wet. Het AT is onderdeel van het ministerie van Economische Zaken en legt rechtstreeks verantwoording af aan de Minister van Economische Zaken.[86] In dit hoofdstuk wordt een beeld geschetst van de wijze waarop het toezicht is georganiseerd. De Wet bewaarplicht bevat waarborgen om de privacy van gebruikers van telecomdiensten te beschermen. Daarnaast heeft ook het CBP een controlerende rol. Het CBP is een zelfstandig bestuursorgaan dat bij wet is ingesteld om erop toe te zien dat personen en organisaties (onder andere) de Wet Bescherming Persoonsgegevens naleven. Het CBP ziet toe op alle wettelijke regelingen waarin sprake is van het bewaren, gebruiken of verwerken van persoonsgegevens. Wat betreft de naleving van de Wet bewaarplicht ziet het AT er in samenwerking met het CBP op toe dat er geen oneigenlijk gebruik wordt gemaakt van de bewaarde gegevens. Het CBP verricht zelf geen metingen en doet geen zelfstandig onderzoek naar de naleving van de Wet bewaarplicht. Wanneer zich een incident of overtreding voordoet, meldt het CBP dit bij het AT, dat vervolgens actie onderneemt. Dit is vastgelegd in een convenant tussen het AT en het CBP.

86 Zie: www.agentschaptelecom.nl/sites/default/files/toezichtsarrangement-dataretentie.pdf, geraadpleegd op 1 juli 2013. Inmiddels wordt niet meer, zoals in het toezichtarrangement staat, verantwoording afgelegd aan de staatssecretaris, maar rechtstreeks aan de minister.

Het AT ziet erop toe dat alleen locatie- en verkeersgegevens worden opgeslagen en dus niet ook de inhoud van contacten of gesprekken; dat de opgeslagen gegevens niet in verkeerde handen vallen en dat de opgeslagen gegevens na het verstrijken van de bewaartermijnen op een adequate wijze worden vernietigd.
Het AT controleert of de aanbieders voldoende maatregelen hebben getroffen om de opgeslagen verkeersgegevens te kunnen beschermen. Aanbieders dienen daartoe een beveiligingsplan te hebben waarin staat beschreven hoe zij met deze gegevens omgaan. Het beveiligingsplan en de werkprocessen van de aanbieders moeten aan een aantal wettelijke eisen voldoen. Het AT ziet toe op het beveiligingsplan en controleert de processen. Wanneer het vermoeden bestaat dat regels niet voldoende worden nageleefd, gaat het AT naar de aanbieder toe voor een inspectie. Bij een overtreding wordt ingegrepen en kunnen sancties worden opgelegd.
Elke drie jaar wordt er door het AT een toezichtarrangement geschreven dat een geldigheidsduur heeft van drie jaar. Het arrangement is bedoeld om de marktpartijen te laten weten hoe het AT toezicht houdt en waar de speerpunten liggen in deze periode. De speerpunten zijn bepaald aan de hand van (recente) wetgeving, waardoor de marktpartijen kunnen zien hoe de toezichthouder de naleving van bepaalde wetten en regels zal controleren. In het toezichtarrangement wordt ook vermeld wat de eventuele maximale boete zal zijn bij een overtreding.
Het toezicht is in de praktijk georganiseerd in een jaarlijks terugkerende 'toezichtcyclus' waarbij alle bij het AT bekende aanbieders schriftelijk worden benaderd. Zij krijgen een enquêteformulier dat aansluit op de speerpunten uit het toezichtarrangement. In het vragenformulier wordt de aanbieders gevraagd aan te geven wat de stand van zaken is betreffende onder meer de dataretentiewetgeving.[87] De onderzoekers van het WODC hebben aan medewerkers van het AT gevraagd of zij van mening zijn als toezichthouder de juiste informatie te krijgen wanneer aanbieders door middel van een zelfrapportage moeten aangeven hoe de situatie binnen het eigen bedrijf is geregeld. De geïnterviewden hadden de indruk dat ze door de bedrijven correct werden geïnformeerd en gaven aan bij het beoordelen van de vragenlijsten alert te zijn op de mogelijkheid dat er sociaal wenselijke antwoorden werden gegeven. Op basis van de antwoorden en gegevens uit de door de aanbieders ingevulde enquêteformulier wordt door het AT beoordeeld wat de grootste risico's zijn. Hierop wordt extra gecontroleerd. Daarnaast worden de grootste relevante aanbieders geselecteerd. Vervolgens maakt AT een planning om bedrijven te bezoeken om zelf te kijken hoe de toestand werkelijk is, waarbij de bedrijven met het hoogste risico prioriteit hebben. Een leidend gegeven bij het bepalen en afwegen van de risico's is de omvang van het bedrijf. De geïnterviewden bij het AT geven aan dat de grootte van het bedrijf een indica-

87 Zie ook www.agentschaptelecom.nl/sites/default/files/eindrapport-nulmeting-wet-bewaarplicht-telecommunicatiegegevens.pdf (geraadpleegd op 26 juli 2013).

tie is voor het aantal klanten en dus voor de relevantie van de opgeslagen gegevens voor de opsporing. De grote telecomaanbieders dragen doorgaans ook zorg voor het bewaren van de verkeers- en locatiegegevens van kleinere aanbieders wanneer deze delen van het netwerk huren. Volgens de geïnterviewden bij het AT en volgens de grote aanbieders is hiermee het toezicht op de kleinere telecomaanbieders indirect gewaarborgd. De kleinere aanbieder heeft dan enkel zorg voor het uitvoeren van de bewaarplicht omtrent klantgegevens. Grotere aanbieders worden daarom eerder bezocht dan kleinere aanbieders.

> *'[...] als je effecten wil bereiken is het belangrijk dat het bij de grootste partijen goed op orde is, omdat je daarmee het grootste effect haalt.'* – AT

De OPTA[88] hanteert een klassensysteem dat de aanbieders indeelt in grootte. Dit gebeurt naar aanleiding van de omzet van de aanbieders. Deze zijn: klein, 0-2 miljoen euro; middel, 2-20 miljoen euro; en groot, 20 miljoen euro of meer. Een kleine aanbieder gaf echter aan dit geen waterdichte benadering te vinden. Deze aanbieder biedt tegen zeer lage kosten telefonie via het internet aan en zijn omzet is – vergeleken met de grote aanbieders – klein te noemen. Maar het aantal klanten van deze aanbieder stijgt al jaren, terwijl de omzet slechts bescheiden toeneemt vanwege de relatief lage inkomsten per klant. Dit in tegenstelling tot de complete diensten die een klant kan afnemen bij de grotere aanbieders tegen hogere kosten, hetgeen in verhouding voor een grotere omzet zorgt.
Het AT geeft aan dat naast de jaarlijkse enquêtes waarin de speerpunten van het toezichtarrangement extra aandacht krijgen, ook wordt geprobeerd om alle aanbieders, dit zijn ongeveer 600 officieel geregistreerde bedrijven, elke vier jaar te bezoeken. Punten waar in het huidige toezichtarrangement extra nadruk op wordt gelegd, is beveiliging, opslag en vernietiging. Voor beveiliging geldt dat zowel de fysieke toegang tot het gebouw als de beveiliging van de ICT-omgeving wordt gecontroleerd. Wat betreft de opslag wordt nagegaan of de juiste gegevensset wordt bewaard en of de vernietiging na het aflopen van de bewaartermijn correct is geregeld.[89]
Uit de nulmeting van de Wet bewaarplicht telecommunicatiegegevens (Agentschap Telecom, 2010) en uit het jaarbericht 'De staat van de Ether' (Agentschap Telecom, 2012) kan niet worden opgemaakt of er sancties zijn opgelegd aan partijen die niet voldoen aan de verschillende eisen van de Wet bewaarplicht.[90]

88 Sinds 1 april 2013 vormen de Consumentenautoriteit, de NMa en de OPTA de nieuwe toezichthouder Autoriteit Consument en Markt.

89 Zie ook: www.agentschaptelecom.nl/sites/default/files/toezichtsarrangement-dataretentie.pdf (geraadpleegd op 1 juli 2013).

90 www.agentschaptelecom.nl/sites/default/files/eindrapport-nulmeting-wet-bewaarplicht-telecommunicatie gegevens.pdf en www.agentschaptelecom.nl/sites/default/files/staatvdether_2012_digitaal.pdf (geraadpleegd 26 juli 2013).

4.2 De aanbieders

Om te begrijpen hoe de aanbieders omgaan met de verplichtingen die de Wet bewaarplicht met zich meebrengt, is gesproken met vier aanbieders: twee kleine en twee grote. De grote aanbieders zijn grote bedrijven die verschillende producten en diensten leveren, zoals internet en telefonie, voor zowel de zakelijke als de consumentenmarkt. In Nederland zijn zes grote aanbieders actief die samen het telecommunicatie netwerk bezitten. Deze bedrijven verhuren hun netwerk aan kleinere telecomaanbieders die op hun beurt weer diensten verkopen aan consumenten. Wanneer een kleine aanbieder een deel van een telefonienetwerk huurt bij een grote partij, zal deze grote partij de opslag van de verkeers-en locatiegegevens voor haar rekening nemen. Het gebruik van de opslagcapaciteit en de systemen die de grote aanbieder hiervoor heeft ingericht, zit bij de huur inbegrepen. De kleine aanbieder is nog wel zelf verantwoordelijk voor een juiste en veilige opslag van de NAW-gegevens van zijn klanten, zoals beschreven in de Wet bewaarplicht.
Voor de invoering van de Wet bewaarplicht liepen de bewaartermijnen tussen bedrijven uiteen. Een geïnterviewde geeft aan dat, voor de wet in 2009 van kracht werd, er bij dat bedrijf een bewaartermijn gehanteerd werd van drie maanden. Bij de andere aanbieder die voor dit onderzoek geïnterviewd is, werden de gegevens voor de invoering van de wet in 2009 juist langer bewaard. Bij dit bedrijf werd de bewaartermijn van twee jaar teruggebracht naar één jaar. Maar de invoering van de wet in 2009 kwam niet als een verrassing en hierop is door de grote aanbieders die door ons zijn geïnterviewd geanticipeerd.

> *'We hebben er wel wat werk aan gehad, maar de wet had een behoorlijke lange aanlooptijd. Bij deze wetswijziging was er al overleg met de partijen voordat die werd ingevoerd. Wij zijn in 2006 al begonnen met het inrichten van de database. [...] Je wilt niet verrast worden door een nieuwe wet.'*
> – aanbieder

Na het invoeren van de Wet bewaarplicht telecommunicatiegegevens moesten beide bedrijven niet alleen de gehanteerde bewaartermijnen aanpassen, maar ook de inhoud van datgene wat bewaard werd. Het veranderen van de inhoud of het verlengen of juist verkorten van bewaartermijnen klinkt misschien vrij eenvoudig, maar blijkt in de praktijk een complex technisch probleem.

> *'Data moet op een bepaalde manier gescheiden bewaard worden. [...] Je moet de mogelijkheid hebben om zoekopdrachten te geven in die bewaaromgeving. Je moet het op een andere manier clusteren dan je voor je eigen factuurproces hebt. [...] Bovenop het feit dat je de gegevens hebt, moet je ze*

zo groeperen, uit systemen bijeenbrengen om aan die verzoeken om informatieverstrekking te kunnen voldoen.' – aanbieder

De implementatie van de Wet bewaarplicht was ondanks de lange aanlooptijd van de wet bij beide aanbieders een omvangrijk project. Over de gemaakte kosten voor de implementatie van de bewaarplicht lopen de antwoorden tussen de twee grote aanbieders uiteen. Waar de ene aanbieder zegt miljoenen te hebben geïnvesteerd, geeft de andere aanbieder aan de benodigde infrastructuur zelf te hebben gebouwd, wat de kosten aanzienlijk heeft gedrukt. Beide geïnterviewde aanbieders geven aan hiervoor geen vergoeding van de overheid te hebben ontvangen.

De overheid heeft inderdaad geen vergoeding beschikbaar gesteld voor de investeringskosten die nodig waren om de databases in te richten ten behoeve van de bewaarplicht. Personele inzet om de gegevens te verstrekken, wordt wel vanuit de overheid vergoed.
Met de grote aanbieders is een overeenkomst afgesloten ten behoeve van de totale dienstverlening van de aanbieders aan de overheid op grond van het Wetboek van Strafvordering, de Telecommunicatiewet, de Wet op de inlichtingen- en veiligheidsdiensten 2002, de Politiewet 2012, de Algemene wet bestuursrecht, de Algemene wet inzake rijksbelastingen en de onderliggende regelgeving. Deze overeenkomst heeft ook betrekking op de verstrekking van gegevens in het kader van de Wet bewaarplicht, maar omdat de inhoud van de overeenkomst niet openbaar is, is het niet bekend of deze volstaat.

De gegevens die de aanbieders sinds 2009 moeten bewaren, worden opgeslagen in een eigen database die in een beveiligde omgeving staat en slechts voor een select aantal medewerkers van de aanbieder benaderbaar is. Dit in tegenstelling tot de normale database die elke aanbieder heeft voor de eigen administratie en die ook door het *callcenter* wordt gebruikt.
Iedere aanbieder beheert zijn eigen database die gevuld is met de gegevens zoals omschreven in de Telecommunicatiewet. Doordat elke aanbieder zijn eigen database vult, beheert en beveiligt, zijn de verkeers- en locatiegegevens van het telefoon- en IP-verkeer in Nederland, decentraal opgeslagen. Hier is het CBP blij mee.

'Wij hebben altijd gekozen voor decentrale opslag en dat ook aangemoedigd. In onze ervaring zijn met name de grote telecommunicatiebedrijven en Internet Servers Aanbieders (ISP's) behoorlijk bekwaam in het handhaven van een adequaat beveiligingsbeleid.' – CBP

In de wet staat dat na de aangegeven duur van verwerking de gegevens moeten worden verwijderd of geanonimiseerd. Anonimiseren houdt in dat de gegevens volledig en onomkeerbaar worden ontdaan van hun identifice-

rende kenmerken. Bij de twee grote aanbieders die zijn geïnterviewd voor dit onderzoek, wordt de database die wordt gevuld op grond van de Wet bewaarplicht automatisch vernietigd na het verstrijken van de bewaartermijn. Overige gegevens in de administratie worden geanonimiseerd en gebruikt voor bedrijfsdoeleinden tenzij de klant anders heeft aangegeven.

> *'De richtlijn geeft aan liever geen database te hebben bovenop de normale database die aanbieders hebben voor billing en dergelijke. Uit privacy redenen. [...] Maar dit is wat grote aanbieders doen en daardoor zit het vernietigen ook echt goed. Daar zit een script overheen en nog een extra script, zodat het onomkeerbaar vernietigd wordt en dat voldoet aan de wetgeving.'* – AT

De onderzoekers vroegen zich af of de gegevens die voor de bewaarplicht werden bewaard in de hiervoor speciaal gebouwde databases ook niet op een andere wijze bewaard worden in de andere systemen van de aanbieders. In dat geval zouden namelijk de gegevens in de database netjes volgens de wet vernietigd worden maar elders in het systeem niet. Navraag bij de aanbieders en het AT wees uit dat dit slechts ten dele het geval is. De aanbieder plaatst de NAW-gegevens en de te bewaren verkeersgegevens van de persoon die een dienst afneemt in een speciale database voor verkeersgegevens. Indien een klant wisselt van aanbieder, zullen de gegevens van deze klant vernietigd worden wanneer de bewaartermijn is verstreken.
Echter, deze NAW-gegevens van een persoon worden samen met de gegevens die te maken hebben met de gemaakte kosten ook elders opgeslagen om de financiële afhandeling van de afgenomen diensten te kunnen regelen. De relatie van deze gegevens met de Wet telecommunicatiegegevens is na een jaar verbroken. Wanneer het bedrijf de gegevens langer wil bewaren, vallen deze onder de Wet Bescherming Persoonsgegevens. Deze wet schrijft voor dat wanneer de aanbieder de gegevens na het verstrijken van de bewaartermijn niet wil vernietigen maar wil gebruiken voor bedrijfsdoeleinden, ze geanonimiseerd dienen te worden. Daarnaast moeten aanbieders de klanten op de hoogte stellen van de aard en de bewaartermijnen van de verkeersgegevens die bewaard worden ten behoeve van de facturering. Voor de andere doelen geldt dit ook, maar moet er van tevoren expliciet toestemming worden gevraagd aan de abonnee of gebruiker, wat overigens door de aanbieders vaak op een passieve manier gebeurt. De klant moet zelf actie ondernemen en aangeven wanneer hij niet wil dat zijn gegevens worden gebruikt voor bedrijfsdoeleinden. Locatiegegevens en ontvangen telefoongesprekken zijn daarentegen voor de financiële afrekening niet van belang en zitten niet in de normale database van de aanbieder. Dit geldt ook voor IP-gegevens die vaak weinig of niets met de financiële afhandeling met de klant te maken hebben. Deze gegevens worden enkel bewaard in het kader van de Wet bewaarplicht

en worden bij de geïnterviewde bedrijven automatisch vernietigd na het verstrijken van de bewaartermijn.

Bij de kleine aanbieder die geïnterviewd is voor dit onderzoek zijn de werkwijze en de wijze waarop wordt omgegaan met de verplichtingen die voortvloeien uit de Wet bewaarplicht op een andere manier geregeld. Deze aanbieder is pas recent actief met de bewaartermijnen aan de slag gegaan, omdat de hoeveelheid te beheren gegevens te groot werd. Het is voor deze aanbieder dus vooral een praktische overweging om de hoeveelheid bewaarde gegevens terug te brengen tot een jaar. Van een aparte database voor het beheren van verkeers- en locatiegegevens is geen sprake. Wanneer een verzoek bij hun binnenkomt, worden de gevraagde gegevens door een medewerker handmatig uit het systeem gehaald. Dit neemt ongeveer een half uur per aanvraag in beslag.

> *'We zijn de afgelopen jaren steeds gegroeid en dat gaat nog steeds door dus is er steeds meer verkeer. Daarom is het nu pas voor ons een zaak om een grens op de telecomgegevens te zetten. We zijn het nu actief aan het terug brengen naar een jaar. Daarvoor hadden we een aantal jaren liggen. Dat was wel eens handig om statistieken mee te bedrijven. Of een klant meldde zich aan en dan dachten wij; "He, misschien is die wel eerder met wanbetalingen weggegaan". Maar nu wordt de gegevensberg zo groot dat we actief stappen aan het ondernemen zijn om het terug te brengen tot 1 jaar.'* – aanbieder

Aan het naleven van de wettelijke verplichting om de gegevens één jaar te bewaren en vervolgens te vernietigen, zijn kosten verbonden, waar deze aanbieder geen vergoeding vanuit de overheid voor ontvangt. De uitvoering van deze verplichting is voor de kleine aanbieder echter nog een groter probleem. Zoals gezegd heeft de overheid een overeenkomst afgesloten met de grote Nederlandse aanbieders. In deze overeenkomst zijn afspraken gemaakt over de vergoeding van de personele inzet die nodig is om op grond van verschillende wetten en regels opgeslagen gegevens aan de overheid te verstrekken. Deze kleine aanbieder behoort echter niet tot de grote en ontvangt geen vergoeding. Volgens de geïnterviewde leggen de werkzaamheden die gepaard gaan met het naleven van de wettelijke verplichtingen een te grote druk op het bedrijf, dat slechts een handvol medewerkers in dienst heeft.

> *'De kosten [van opslag] zijn beperkt, onder de 5.000 euro per jaar. Je hebt een server, extra serverruimte huren en extra manuren om dat ding in de lucht te houden. We willen niet zielig doen. Maar wij zijn met X aantal medewerkers, wat een goed aantal is om het rendabel te maken, maar de technische ontwikkelingen gaan heel snel dus je moet heel veel energie investeren om bij te blijven. Dat is iets waar je geen behoefte aan hebt,*

want je hebt al een overvolle technische agenda en er zijn waslijsten van dingen die we allemaal nog willen doen en dit [de bewaarplicht] moet er dan toch tussendoor.' – aanbieder

De situatie bij deze kleine aanbieder en bij de grote aanbieders komt overeen met het beeld dat het AT heeft over de uitvoering van de bewaarplicht. In 2010 heeft het AT een nulmeting uitgevoerd betreffende de uitvoering van de Wet bewaarplicht bij ISP's.[91] Uit dit onderzoek kwam naar voren dat de uitvoering van de bewaarplicht bij de grote aanbieders goed op orde is en voldoet aan de bewaarplicht. Ook werd in het onderzoek vastgesteld dat kleinere aanbieders de bewaarplicht minder regelen volgens de letter van de wet en dat het vernietigen maar ook het bewaren van gegevens niet altijd correct gebeurt. Uit contact van het AT met de aanbieders blijkt dat vooral het samenspel tussen dataretentie en het gebruik van verkeers- en locatiegegevens voor bedrijfsdoeleinden complex is. Bewaarde verkeers- en locatiegegevens worden vaak niet tijdig vernietigd, omdat deze gebruikt worden voor bedrijfsdoeleinden. Het is de vraag of deze aanbieders voldoende op de hoogte zijn van de verplichtingen die aan het verwerken van verkeers- en locatiegegevens voor bedrijfsdoeleinden verbonden zijn. Dit wordt door het AT nader onderzocht.
Daarnaast zijn de kleinere aanbieders vaak onbekend met een beveiligingsplan of met standaarden. Overigens is het volgens de geïnterviewde experts bij het AT ook mogelijk om zonder gebruik te maken van een standaard beveiligingsmethodiek, te voldoen aan de veiligheidsvereisten en dienen deze bevindingen gerelativeerd te worden: het aantal keren dat kleine aanbieders een verzoek krijgen tot gegevensverstrekking is relatief klein. De kleine aanbieder die door de onderzoekers van het WODC werd geïnterviewd, kreeg ongeveer tien verzoeken tot informatieverstrekking per jaar.

Bij een vierde geïnterviewde aanbieder werd nog een andere situatie aangetroffen. Dit betreft een kleine aanbieder van web-hosting diensten, waarbij klanten onder andere hun website op de servers van dit bedrijf laten draaien. Hier bleek dat men de systemen op een dusdanige manier had ontworpen en ingericht dat er geen data worden opgeslagen. Het bedrijf wordt geleid door personen die privacy zeer belangrijk vinden en adverteren met het feit dat hun bedrijf een zogenoemd privacy-by-design principe hanteert. De eigenaren van dit bedrijf herkennen zich wel in de documentatie van het AT als bewaarplichtige van de verkeersgegevens van e-maildiensten die zij hun klanten aanbieden. Maar door het technische design van de systemen heeft deze aanbieder feitelijk geen gegevens om te bewaren.

91 www.agentschaptelecom.nl/sites/default/files/eindrapport-nulmeting-wet-bewaarplicht-telecommunicatiegegevens.pdf.

'De formulering van het Agentschap Telecom op hun website waar zij uitleg geven, wordt gezegd dat wanneer je een hostingaanbieder bent, dat je de mailgegevens wel dient te loggen. [...] Een van die dingen die we hebben gedaan is de mailserver zodanig aanpassen dat wij niks meer loggen.'
– aanbieder

De onderzoekers hebben de vraag of webhosting onder de bewaarplicht valt, voorgelegd aan het AT. Volgens het AT valt deze dienst niet onder hoofdstuk 13 van de Telecomwet. De OPTA registreert ook geen webhosting bedrijven in haar register van openbare elektronische communicatiediensten en/of -netwerken. Echter, voor e-mail ligt dit volgens het AT anders. Hierbij wordt onderscheid gemaakt tussen traditionele e-mail waarbij een e-mailapplicatie op een computer nodig is (bijvoorbeeld outlook) en webmail. Deze laatste dienst is benaderbaar via het internet. De traditionele e-mail valt wel onder de werking van hoofdstuk 13 van de Telecommunicatiewet en webmail niet. Volgens het AT is webmail in principe geen dienst waarbij signalen via elektronische communicatienetwerken worden overgebracht. Webmail is te vergelijken met een website met inhoud. Websites vallen ook buiten de werking van hoofdstuk 13 Telecommunicatiewet (zie ook *Kamerstukken II* 2006/07, 31 145, nr. 3, p. 37). Tot op heden heeft het AT bij webhostbedrijven enkel de webmailvariant aangetroffen.

'De wetgeving is door de nieuwe ontwikkelingen "grijs" geworden. Een zwart/wit antwoord wordt moeilijker. De ontwikkelingen op het gebied van onder andere e-mail gaan erg snel. Je ziet momenteel al allerlei "hybride" vormen waarbij traditionele e-mail en webmail in elkaar worden geweven. Deze trend zie je bij heel veel diensten. De wetgeving is hierop niet meer goed genoeg toegesneden.' – AT

4.3 Complexiteit van verkeers- en locatiegegevens

Tijdens de gesprekken met de grote aanbieders kwam naar voren dat het analyseren en interpreteren van de opgevraagde gegevens specialistenwerk is. Experts van beide bedrijven treden regelmatig op als telecomspecialist of als getuige-deskundige in rechtszaken. Hierbij signaleren deze experts dat de complexiteit van verkeers- en locatiegegevens nog wel eens problemen oplevert bij opsporingsdiensten door een tekort aan kennis bij opsporingsdiensten.

'Een onderzoeksteam heeft data verzameld, daar komen conclusies uit [...] daar waar het ter behandeling voor een rechter komt, dan krijg je de discussie pas scherp. Je weet dus niet wat er daarvoor allemaal is misgegaan.

Daarmee niet bedoelend dat iedereen bewust maar fouten zit te maken, maar het risico op fouten is gewoon enorm.' – aanbieder

'Er zijn een aantal zaken van de rol afgegaan omdat men fouten had gemaakt, informatie niet meegewogen waardoor een beslissing een heel andere kant op gaat. – aanbieder

'Belgegevens worden wel vaak verkeerd geïnterpreteerd. Dan zie je bijvoorbeeld een klant bellen in Rotterdam en ineens zie je er een gesprek in Groningen tussen staan, omdat het systeem die mast verkeerd vertaalt.' – aanbieder

De kleine aanbieder die voor dit onderzoek is geïnterviewd, biedt telefonie over het internet aan. Dit is een andere vorm van telefonie dan de ouderwetse telefonie en uit de verzoeken die deze aanbieder ontvangt blijkt dat de kennis van de aanvrager over deze vorm van communicatie niet altijd toereikend is.

'Wij kregen een selectienummer en wanneer een abonnee deze code voor zijn bestemmingsnummer draait dan belt hij via ons. Wij kregen het verzoek om daar in- en uitkomende verkeer van te geven, maar zo'n nummer heeft geen inkomend verkeer via ons. En uitgaand verkeer zou je ook via KPN of T-Mobile kunnen opvragen. Dus waarom bij ons het verzoek indienen? Het was een volstrekt nutteloos verzoek; het dekt de lading niet en de helft kan niet beantwoord worden.' – aanbieder

'Soms heb ik wel meer informatie over een nummer maar de bevraging is dan niet goed opgesteld.' – aanbieder

De geïnterviewde persoon bij dezelfde kleine aanbieder vertelde ook dat hij kortgeleden enkele internationale vorderingen had binnengekregen die het bedrijf bewust naast zich neer heeft gelegd. De verzoeken bevatten de zoekvraag of een buitenlands telefoonnummer X, waarmee gebeld was via het Nederlandse netwerk, het afgelopen jaar contact had gehad met een nummer uit het bestand van de desbetreffende aanbieder. De zoekvraag was volgens de aanbieder zo breed gesteld dat dezelfde vraag aan elke aanbieder in Nederland gesteld had kunnen worden. De geïnterviewde had hier graag melding van gedaan bij een officiële instantie, maar wist niet tot wie hij zich kon wenden. Dit punt werd ook door geïnterviewde experts bij het CBP onder de aandacht gebracht. Er is een wettelijke geheimhouding ten aanzien van vorderingen. Maar er bestaat geen wettelijke voorziening die toestaat om inhoudelijke informatie over vorderingen te delen met de toezichthouder. Het hiervoor beschreven voorval is teruggekoppeld aan de ULI. Sinds de tweede helft van het jaar 2010 verlopen alle verzoeken via de ULI, maar blijk-

baar is het systeem nog niet helemaal waterdicht. Deze brede ongerichte verzoeken zouden volgens de medewerker van de ULI uit de stapel gefilterd zijn. De ULI geeft aan dat deze bevinding reden is om nogmaals bij alle betrokken partijen onder de aandacht te brengen dat alle aanvragen altijd via de ULI dienen te verlopen.

4.4 Onregelmatigheden

Het functioneren van de toezichthouders en het beoordelen of het toezicht al dan niet adequaat wordt uitgevoerd, valt buiten de vraagstelling van dit onderzoek. Er is dan ook geen systematisch onderzoek verricht naar alle grote aanbieders en naar de output die op verzoek van opsporingsdiensten wordt geleverd. Tijdens het uitvoeren van dit onderzoek zijn de onderzoekers echter wel op enkele onregelmatigheden gestuit bij de uitvoering van de wet. Zo zagen de onderzoekers per toeval dat een grote aanbieder verkeers- en locatiegegevens leverde waarin de *Last Cell ID*, de locatie waarop een gesprek is beëindigd, was meegegeven, terwijl daarom niet met een speciale vordering was gevraagd. De wet schrijft voor dat alleen de *First Cell*, de startpositie van een gesprek onder de Wet bewaarplicht valt. Informatie over de locatie waarop een gesprek is beëindigd, kan voor de politie erg waardevol zijn. Tijdens gesprekken met opsporingsambtenaren gaven meerdere geïnterviewden aan dit waardevolle informatie te vinden. Echter, informatie betreffende de eindlocatie van een gesprek valt niet onder de gegevens zoals omschreven in de bijlage behorende bij artikel 13.2a Tw en zou niet standaard bij opgevraagde verkeers- en locatiegegevens op basis van de Wet bewaarplicht meegeleverd dienen te worden. Deze gegevens kunnen overigens wel worden opgevraagd op grond van artikel 13.4 lid 3 Tw.
Ook werd door de onderzoekers gesignaleerd dat drie grote aanbieders IP-verkeersgegevens leverden die ouder waren dan de bewaartermijn van een halfjaar. Dit mag in het geval er een prepaid internetdienst wordt afgenomen, maar niet als er sprake is van een abonnement. In de bestudeerde zaken ging het echter om gevorderde verkeersgegevens van een smartphone met een abonnement. Bij de historische verkeersgegevens betreffende telefonie werden ook de volledige historische IP-verkeersgegevens geleverd. Blijkbaar is het scheiden van telefoon- en IP-gegevens om de verschillende bewaartermijnen te kunnen handhaven door deze aanbieders niet doorgevoerd; mogelijk vanwege het extra werk dat hiermee gepaard gaat of vanwege de technische complexiteit. Navraag bij de aanbieders heeft bij één grote aanbieder inmiddels geresulteerd in aanpassing van de bewaartermijn voor IP-verkeersgegevens.
De onderzoekers hebben deze onregelmatigheden voorgelegd aan het AT. Daar was men niet op de hoogte van deze zaken. Het blijkt ook lastig te zijn voor het Agentschap om de naleving van de Wet bewaarplicht in de praktijk

te controleren. Op grond van artikel 18.7, tweede lid, Tw hebben toezichthouders niet de bevoegdheid om de verkeers- en locatiegegevens bij aanbieders op te vragen die door aanbieders op grond van artikel 13.2a Tw moeten worden bewaard.[92] Het AT mist hiermee een instrument om dit aspect van het toezicht te kunnen uitvoeren.

> *'Voor ons is het heel lastig om hierop toezicht te kunnen houden omdat we die gegevens niet mogen opvragen. [...] Wij kunnen alleen het proces controleren en dat doen we ook, maar de echte output van het proces is voor ons verboden op te vragen.'* – AT

4.5 Verzoek om inzage eigen verkeers- en locatiegegevens

Op grond van de WBP kunnen burgers een overzicht opvragen van de persoonsgegevens die een organisatie over hen bewaart. Verkeers- en locatiegegevens vallen hier ook onder, zoals te lezen is in de privacystatements van verschillende telecombedrijven.
Twee onderzoekers die betrokken zijn bij dit onderzoeksproject, hebben als klant bij hun eigen telecomaanbieder inzage gevraagd in de verkeers- en locatiegegevens van hun mobiele telefoon. Op de website van de desbetreffende aanbieders zijn formulieren te downloaden voor een verzoek tot inzage in de persoonsgegevens. Na het opvragen reageerden beide aanbieders met het toesturen van een compleet overzicht van de bij hen geregistreerde persoonsgegevens van de onderzoekers. Dit omvatte een compleet overzicht van de contactgegevens, soort en nummer van het identificatiebewijs, contract- en facturering gegevens, privacyinstellingen betreffende de nummeridentificatie, IMEI- en IMSI-nummer en vermelding in telefoongidsen. Verder verschaften beide aanbieders informatie over welke gegevens opgeslagen worden in het kader van de Telecommunicatiewet en door wie deze opvraagbaar zijn. Echter, voor het inzien van de daadwerkelijke verkeers- en locatiegegevens dienden beide onderzoekers opnieuw een aanvraag in te dienen. Beide aanbieders gaven aan een overzicht te geven voor een korte periode van tien tot veertien dagen. Langer zou volgens de aanbieders een onevenredige belasting van de bedrijfsvoering betekenen. Na het versturen van deze nieuwe aanvraag kwam van aanbieder A geen reactie. Acht weken later is, vanwege de voortgang van het onderzoek, besloten deze aanbieder telefonisch te benaderen. Tijdens het telefoongesprek werd geen antwoord gegeven op de vraag waarom geen inzage wordt verleend. Zelfs nadat de klant zichzelf bekend had gemaakt als onderzoeker van het WODC, werkende aan

92 Zie ook de MvT op de Wet bewaarplicht telecommunicatie (31 145, nr. 3, p. 55), alsmede de toelichting op artikel 18.7, lid 2, in Tekst & Commentaar 'Telecommunicatie- en privacyrecht', waarin wordt gesteld dat: 'Om eventuele onduidelijkheden weg te nemen en ter bescherming van de persoonlijke levenssfeer van de gebruiker van elektronische communicatiediensten wordt uitdrukkelijk bepaald dat de toezichthouder geen bevoegdheid heeft met betrekking tot deze gegevens.'

een rapport over de Wet bewaarplicht, leverde het telefoongesprek niets op. Echter, vijf dagen na dit telefoongesprek ontving de onderzoeker een brief met daarin de mededeling dat het niet mogelijk is om inzage te geven, daarbij verwijzend naar artikel 12.2d 'Verwerking van Persoonsgegevens van de algemene voorwaarden', die bij de brief gevoegd was. Dit artikel betreft de omgang van de aanbieder met de persoonsgegevens voor de volgende doeleinden: 'het analyseren van het gebruik van het netwerk voor zover dat met het oog op het verkeersbeheer, het waarborgen, verbeteren van de continuïteit en kwaliteit van de dienstverlening en de verantwoordelijke bedrijfsvoering van [de aanbieder] noodzakelijk is'. Een begrijpelijke uitleg waarom de inzage geweigerd is, ontbreekt. Aanbieder B nam, enkele dagen na het indienen van het inzageverzoek, telefonisch contact op met de vraag wat de reden was van het verzoek tot inzage. De onderzoeker had het gevoel als klant niet veel verder te komen en voelde zich genoodzaakt bekend te maken dat het opvragen van de gegevens onderdeel uitmaakte van een onderzoek naar de Wet bewaarplicht, uitgevoerd door het WODC. De aanbieder verstuurde binnen een week het gevraagde overzicht. In dit overzicht waren gegevens van derden onzichtbaar gemaakt in verband met de bescherming van de privacy. Dit komt echter wat vreemd over wanneer het nummers zijn van gesprekken die op initiatief van de klant zelf hebben plaatsgevonden. Verder is te zien op welke datum er communicatie heeft plaatsgevonden, het tijdstip van aanvang van de communicatie en of het telefoon-, sms- of dataverkeer betrof. Uit het overzicht zijn de locatiegegevens niet af te leiden. Deze kolommen zijn grotendeels leeg en uitleg bij de gevulde cellen ontbreekt.

Ondanks dat de WBP heel duidelijk is over het recht op inzage en het feit dat de aanbieders hiervan zelf in hun privacyvoorwaarden melding maken, is er bij de door de onderzoekers benaderde aanbieders geen sprake van een correcte afhandeling van een verzoek om inzage. De onderzoekers hebben het CBP gevraagd om een reactie op de bevindingen dat klanten nauwelijks tot geen inzage krijgen in hun eigen verkeers- en locatiegegevens. Daarover was men heel duidelijk; '*Dat is ten onrechte.*' [93]

> *'Het wetgevingsadvies benadrukt dat het van groot belang is dat de Minister erkent dat het inzagerecht van toepassing is. Wij zagen dat als enig lichtpuntje in het wetsvoorstel, dat betrokkenen in elk geval het recht hebben om te zien wat er over hen wordt bewaard.'* – CBP

Ook het Rathenau instituut maakt zich zorgen om het feit dat het in de WBP vastgelegde recht op inzage in de praktijk vaak niet meer is dan een papieren recht. Door het weigeren van inzage is het niet mogelijk om te controleren of de verwerking van de gegevens juist, volledig, relevant en rechtmatig is. Dit

93 Zie over de opvatting van het CBP betreffende dit recht ook www.rejo.zenger.nl/focus/bemiddeling-door-het-cbp-inzage-persoonsgegevens-bij-telfort (geraadpleegd op 26 juli 2013).

tast de rechtspositie van burgers aan en maakt hen verregaand afhankelijk van het naar behoren functioneren van het systeem.[94]

Een medewerker van *Bits of Freedom* (Bof) heeft eenzelfde ervaring bij het opvragen van zijn eigen verkeers- en locatiegegevens.[95] Na het indienen van het verzoek kreeg ook deze persoon geen inzage en pas tijdens de behandeling voor een rechtszaak is de zaak ingetrokken door de aanbieder, die alsnog de gevraagde gegevens heeft overhandigd.[96]

> *'Wat ik zelf heel belangrijk vind, is dat de betrokkenen, de burger, achter het net vist […] Het wrange van het inzagerecht zoals het in artikel 35 van de Wet bescherming persoonsgegevens staat, en die heel belangrijk is voor de bewaarplicht, is dat het niet werkt. Dit komt omdat aanbieders zeggen dat het hen teveel werk kost om die gegevens op een overzichtelijke manier aan hun klanten te verstrekken. De enige reden waarom ze het niet hoeven te geven is als het naar alle redelijkheid niet kan, en daar beroepen zij zich op. Ik denk dat dit niet correct is. Als opsporingsdiensten erom vragen moeten ze het ook makkelijk kunnen aanleveren, dus ik denk dat de bewerkingsslag eigenlijk wel beperkt is.'* – BoF

Tijdens een gesprek met een aanbieder werd de opmerking gemaakt dat inzage in de verkeers- en locatiegegevens feitelijk overbodig is, omdat de relevante gegevens over het belgedrag ook zijn af te lezen uit de gespecificeerde factuur. Een geïnterviewde expert van BoF denkt hier anders over:

> *'In de Memorie van Toelichting is geschreven dat de relevante gegevens over belgedrag doorgaans zijn af te leiden uit de gespecificeerde factuur. Dat is flauwekul, want op die factuur komen alleen maar gegevens te staan die te maken hebben met de hoogte van die factuur en bevat geen ontvangen telefoontjes en berichten en geen locatiegegevens.'* – BoF

4.6 Conclusie

De gegevens die worden opgeslagen in het kader van de Wet bewaarplicht bevat privacygevoelige informatie omtrent de contacten en bellocaties van personen. Om te waarborgen dat gegevens correct worden opgeslagen, beveiligd en vernietigd, hebben de aanbieders de wettelijke verplichting om

94 www.rathenau.nl/publicaties/publicatie/databases-over-ict-beloftes-informatiehonger-en-digitale-autonomie.html (geraadpleegd 25 juli 2013), zie ook: www.rathenau.nl/uploads/tx_tferathenau/Hand-out_ICT-commissie_Tweede_Kamer.pdf (geraadpleegd op 3 juli 2013).

95 Zie ook: www.bof.nl/2013/03/15/drie-overgebleven-dataweigeraars-datadagboek-5/ (geraadpleegd op 12 juni 2013). Uit een latere publicatie blijkt deze persoon overigens alsnog het gevraagde overzicht te hebben ontvangen van zijn aanbieder. Zie: www.bof.nl/2013/07/12/ohai-t-mobile-i-can-haz-my-data (geraadpleegd op 15 juli 2013) https://rejo.zenger.nl/focus/ik-de-ogen-van-t-mobile (geraadpleegd op 5 december 2012).

96 https://rejo.zenger.nl/focus/ik-de-ogen-van-t-mobile (geraadpleegd op 5 december 2012).

technische en organisatorische maatregelen te nemen om misbruik van de opgeslagen gegevens te voorkómen en zijn ze verplicht de bewaarde gegevens te vernietigen na afloop van de bewaartermijn. Om te voorkomen dat gegevens in verkeerde handen vallen of dat de gegevens oneigenlijk worden gebruikt, is goed toezicht op de uitvoering belangrijk. Het CBP voert geen actief beleid ten aanzien van de naleving van de verplichtingen die uit de Wet bewaarplicht voortvloeien. Overtredingen of meldingen worden aan het AT doorgegeven, zoals in een convenant tussen het CBP en het AT is vastgelegd. Het AT treedt actief op als toezichthouder ten aanzien van de Wet bewaarplicht en heeft als streven minstens eenmaal per vier jaar alle aanbieders in Nederland te bezoeken. Echter, het AT heeft enkel de mogelijkheid om toe te zien op de juiste uitvoering van bedrijfsprocessen en beschikt niet over de instrumenten die nodig zijn om op de inhoud van de bewaarde en geleverde gegevens toe te kunnen zien. Het AT heeft niet de bevoegdheid om de daadwerkelijke output van verkeers- en locatiegegevens van verschillende aanbieders in te zien. Hiermee mist het Agentschap een instrument om dit aspect van het toezicht goed uit te kunnen voeren. Wanneer een overheid besluit privacygevoelige informatie van burgers op te slaan en te bewaren, hoort daar een solide en effectief toezicht bij. Het verdient daarom aanbeveling om de rol van de toezichthouder op dit vlak te verbeteren.
Op grond van de WBP kunnen burgers een overzicht opvragen van de persoonsgegevens die een organisatie over hen bewaart. Echter, twee verzoeken om inzage van verkeers- en locatiegegevens werden niet of nauwelijks gehonoreerd. Volgens het CBP is dit ten onrechte en dienen aanbieders een verzoek om inzage gewoon te honoreren. De afhandeling door de aanbieders van dit soort verzoeken is voor verbetering vatbaar. Een burger zou binnen een redelijke termijn inzage in de eigen opgeslagen verkeers- en locatiegegevens moeten kunnen krijgen. Immers, opsporingsdiensten hebben deze gegevens ook binnen enkele dagen in hun bezit.

5 Het gebruik van historische verkeersgegevens in de praktijk

In het hierna volgende hoofdstuk wordt het gebruik van historische verkeersgegevens in de opsporingspraktijk beschreven. Het hoofdstuk is gebaseerd op interviews die zijn gehouden met sleutelpersonen die over de inzet en het gebruik van historische verkeergegevens zijn geïnterviewd. In dit hoofdstuk wordt als eerste ingegaan op het gebruik van historische telecommunicatiegegevens in de opsporing. Vervolgens wordt ingegaan op het gebruik van historische internetgegevens en mastbevragingen. Wanneer in de opsporing historische verkeersgegevens zijn opgevraagd, dient men de persoon te notificeren; de gegevens dienen te worden vernietigd als de zaak is gesloten. Hierop zal als laatste worden ingegaan.

5.1 Historische gegevens telefonie

In de bijlage behorende bij artikel 13.2a Tw wordt een opsomming gegeven van de gegevens die vallen onder de Wet bewaarplicht. Hierbij wordt een strikt onderscheid gemaakt tussen telefonie- en internetgegevens. Voor de duidelijkheid is in dit rapport deze tweedeling gehandhaafd. Echter, in de praktijk is dit onderscheid nagenoeg verdwenen en hanteert de Wet bewaarplicht, volgens experts, een onjuiste tweedeling. Ook telefonie verloopt steeds vaker via het internet. Vroeger gebruikte men Voice over IP-diensten (VoIP) om goedkoop te kunnen bellen met contacten in het buitenland. Maar tegenwoordig hebben veel mensen een abonnement bij een kabelbedrijf of aanbieder waarbij het telefoonverkeer via het internet verloopt. VoIP is daarmee een hele gangbare manier van telefoneren geworden. In het wetsvoorstel waarin de bewaartermijn voor internetgegevens gewijzigd wordt van twaalf naar zes maanden, is een uitzondering gemaakt voor VoIP-diensten[97], waarvoor de termijn van twaalf maanden bleef gelden. Deze uitzondering is gemaakt omdat de functionaliteit van de diensten kan worden aangemerkt als telefonie over een vast of mobiel netwerk. Ook de Experts Group Data Retention van de Europese Unie (DatRet/expgrp. 2010)[98] heeft een advies gegeven over de omgang met VoIP-diensten, waarin werd geadviseerd de definities voor de verschillende vormen van telefonie te harmoniseren. In de praktijk betekent dit dat wanneer verkeersgegevens worden opgevraagd van een telefoon waarmee via het internet wordt gebeld, er eenzelfde set gegevens geleverd wordt als wanneer het een 'ouderwetse' manier van telefonie betreft. In Nederland maakt de overheid onderscheid tussen de verschillende vormen van telefonie door de functionaliteit en belangrijkste kenmerken van de

97 *Kamerstukken II* 2009/10, 32 185, nr. 3.
98 http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/pdf/series_a_position_paper_5_final_14_07_2010_closer_understanding_of_the_term_internet_telephony_en.pdf (geraadpleegd op 1 juli 2013).

geboden telefoniedienst voorop te stellen.[99] Voor telefoniediensten, zoals traditionele telefonie, mobiele telefonie en VoIP waarbij bijvoorbeeld gebruik wordt gemaakt van het Nationale Nummerplan, waarbij doorschakeling mogelijk is en toegang wordt geboden tot het alarmnummer 112, geldt een bewaartermijn van twaalf maanden. Voor verkeersgegevens van spraakdiensten die gebruikmaken van het internet en die niet over deze functionaliteiten beschikken, geldt een bewaartermijn van zes maanden. In deze paragraaf zal specifiek worden ingegaan op het gebruik en de inzet van historische verkeersgegevens betreffende telecommunicatie. Als eerste zal hierna worden ingegaan op de vraag welke gegevens bewaard worden.

5.1.1 Wat wordt bewaard?

In de bijlage behorende bij artikel 13.2a Tw staat een opsomming van de te bewaren gegevens betreffende telefoonverkeer. De wet schrijft voor dat de volgende gegevens betreffende *telefonie* door de aanbieders bewaard dienen te worden voor een periode van één jaar:

a het telefoonnummer van de oproeper en het telefoonnummer die werden opgeroepen, in het geval van aanvullende diensten, zoals call forwarding of call transfer, het nummer waarnaar de verbinding is doorgeleid;
b namen en adressen van abonnees of geregistreerde gebruikers;
c datum en tijdstip aanvang en einde van de verbinding;
d de gebruikte telefoondienst (bijvoorbeeld vast, mobiel of VoIP);
e bij mobiele telefonie:
   – IMSI en IMEI nummer (het identificerende nummer van de simkaart en telefoon) van oproepende en van de opgeroepen deelnemer;
   – in geval van vooraf betaalde anonieme diensten, de datum en het tijdstip van de eerste activering van de dienst en aanduiding (Cell ID) van de locatie waaruit de dienst is geactiveerd;
   – locatieaanduiding bij het begin van de verbinding (First Cell ID);
   – gegevens voor het identificeren van de locatieaanduiding.

De inhoud van een gesprek valt niet onder de bewaarplicht. Ook de inhoud van een sms-bericht valt niet onder de bewaarplicht, de verkeersgegevens van het verzonden of ontvangen bericht wel. Een mobiele telefoon maakt regelmatig contact met het netwerk, ook zonder dat deze wordt gebruikt om te bellen of te internetten. Deze tussenliggende contactmomenten, de zogenaamde vluchtige gegevens, vallen niet onder de bewaarplicht en worden niet geleverd bij het opvragen van historische verkeersgegevens. Oproeppogingen, waarbij geen contact tot stand is gekomen, vallen wel onder de bewaarplicht en dienen door de aanbieders te worden bewaard.

99 Zie: www.agentschaptelecom.nl/onderwerpen/veiligheid/opslag-telecomgegevens (geraadpleegd op 1 juli 2013).

5.2 Telefonie – schets van de inzet bij verschillende misdrijven

Het algemene beeld dat uit de interviews naar voren komt, is dat historische telecommunicatiegegevens een belangrijke en zeer gewaardeerde rol spelen in de opsporingspraktijk. De geïnterviewde professionals en experts gaven vele voorbeelden van situaties waarin dergelijke gegevens in de opsporing kunnen worden benut. Uit deze verhalen blijkt dat de gegevens op een hele diverse manier worden ingezet in een uiteenlopend scala van misdrijven.
Zo spelen historische gegevens over telecommunicatieverkeer een belangrijke rol in de voorbereidende fase van een onderzoek naar georganiseerde misdaad. De gegevens worden gebruikt bij het in kaart brengen van criminele organisaties. Door een grondige analyse is in kaart te brengen wie met wie in contact staat. Hierbij zijn de locaties vanwaar gebeld wordt ook interessant, omdat het bewegingen van personen in kaart brengt. Tijdens de voorbereiding van een misdrijf realiseren verdachten zich vaak nog niet dat ze in een latere fase onderwerp kunnen worden van een opsporingsonderzoek. Ze zijn dan minder op hun hoede. Daarom kunnen juist historische verkeersgegevens volgens een geïnterviewde nog wel eens mooie bevindingen opleveren.
Maar ook bij een delict zoals een straatroof worden verkeersgegevens regelmatig ingezet. Hierbij kunnen bijvoorbeeld gegevens worden opgevraagd om te achterhalen of bepaalde personen die de politie in het vizier heeft, in de omgeving waren. Of wanneer sprake is van een reeks overvallen kan overwogen worden om verkeersgegevens te selecteren op de locatie van een zendmast. Zodoende kunnen op verschillende plaatsen delict telefoonnummers met elkaar worden vergeleken, in de hoop dat de verdachten bij verschillende overvallen dezelfde telefoon hebben gebruikt. Bij een dergelijke vergelijking worden de telefoonnummers of IMEI-nummers die vaker voorkomen in het totale bestand geselecteerd om op door te rechercheren. Dit is een opsporingstactiek die regelmatig bij seriematige delicten wordt ingezet. Hierbij kan gedacht worden aan brandstichting of een reeks overvallen. Ook wordt deze methode gehanteerd als er sprake is van twee plaatsen delict die iets met elkaar te maken hebben, bijvoorbeeld de plaats waar de vluchtauto wordt teruggevonden en de plaats van het delict zelf.
Ook kan het zinvol zijn om enige tijd nadat een roofoverval heeft plaatsgevonden waarbij een mobiele telefoon is meegenomen, de historische verkeersgegevens van dit toestel op te vragen. Op die wijze kan worden nagegaan of de gestolen telefoon nog in gebruik is en of er van simkaart is gewisseld. Er zijn voorbeelden van zaken waarbij de inzet van deze techniek naar een verdachte heeft geleid.
Door middel van historische verkeersgegevens kan inzichtelijk worden gemaakt of een telefoon binnen een bepaald gebied is geweest en kan worden getoetst of verhalen van verdachten of getuigen kloppen. Ook kunnen historische verkeersgegevens worden gebruikt om verklaringen te toetsen over wie wanneer voor het laatst contact heeft gehad met bijvoorbeeld een

slachtoffer of een vermist persoon. Zo vertelde een professional van de politie dat hij bij moordzaken waarbij de indruk bestaat dat een verdachte in de relationele sfeer moet worden gezocht, de verkeersgegevens opvraagt van familie en vrienden rond het slachtoffer. Door het opvragen van verkeersgegevens kan worden nagegaan waar deze personen zich bevonden op het moment dat het misdrijf plaatsvond. Hiermee kan een eerste richting in het opsporingsonderzoek worden bepaald en dit kan leidend zijn bij de besluitvorming over wie op het bureau wordt uitgenodigd voor een verhoor.
Na arrestatie van een verdachte kunnen verkeersgegevens worden opgevraagd om te onderzoeken of de persoon contact heeft gehad met een andere verdachte. Personen die – met name rondom het tijdstip van het misdrijf – veelvuldig contact hadden met de gearresteerde, zijn mogelijk interessant voor het onderzoek en informatie hierover kan tijdens een verhoor op tactische wijze worden ingebracht.
Ook kan het in opsporingsonderzoeken voorkomen dat een getuige vertelt dat hij 'gister rond een uur of drie' is gebeld door een bepaalde persoon die wordt gezocht, maar dat hij het nummer niet heeft. In zo'n geval kan een OvJ bijvoorbeeld een beroep doen op artikel 126n Sv. en daarmee eenvoudig het nummer achterhalen.
Naast de hiergenoemde voorbeelden zijn er nog veel meer specifieke situaties voorstelbaar waarbij historische verkeersgegevens een rol kunnen spelen in het opsporingsproces. De opsomming is dan ook zeker niet volledig en uitputtend. Deze voorbeelden geven wel een beeld van de vele manieren waarop historische telefoongegevens gebruikt kunnen worden in het opsporingsproces.

5.2.1 Overwegingen en doelstellingen

Wanneer een opsporingsteam historische verkeersgegevens wil opvragen van een telefoonnummer, dient dit gemotiveerd te worden in het aanvraagproces-verbaal. In deze motivatie dient onder andere te worden aangegeven met welk doel deze verkeersgegevens worden opgevraagd. Het opsporingsteam moet dus aangeven welk doel het met de gevraagde gegevens denkt te bereiken. Deze doelstellingen zijn onder te brengen in een aantal algemene categorieën, namelijk: het identificeren van een gebruiker; het achterhalen van contacten; plaatsbepaling; het traceren van een IMEI-nummer; en het maken van een capaciteitsafweging alvorens men gaat tappen. Uiteraard kunnen meerdere doelstellingen tegelijk een rol spelen bij het opvragen.
Een van de doelstellingen van het opvragen van historische gebruikersgegevens is het *identificeren van een gebruiker*. Vaak heeft een opsporingsteam enkel een telefoonnummer dat is gekregen via de Criminele Inlichtingen Eenheid of een nummer dat is verkregen door gebruik van een telefoontap en is het nog niet bekend wie daarvan gebruikmaakt. Het achterhalen van de identiteit van de gebruiker kan op verschillende manieren. Zo kan de

tenaamstelling van een telefoonnummer bij het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT) worden opgevraagd.
Het CIOT is de schakel tussen opsporingsdiensten en telecombedrijven. Dagelijks stellen de telecom- en internetbedrijven een kopie van hun klantenbestand met de wettelijk vastgelegde identificerende gegevens ter beschikking aan het CIOT in een beveiligde omgeving. Identificerende gegevens zijn naam, adresgegevens en woonplaats behorende bij telefoonnummers, e-mailadressen en IP-adressen. Deze kopie van het klantenbestand wordt 24 uur bewaard door de telecom- en internetbedrijven in de beveiligde omgeving en wordt automatisch ingelezen in de blackbox-omgeving van het CIOT-informatiesysteem. Elke 24 uur worden de gegevens ververst en opnieuw ingelezen in het CIOT-bestand.[100] Aan vaste en mobiele telefoonnummers op basis van een abonnement zijn identificerende gegevens gekoppeld en opsporingsdiensten kunnen bevragingen doen in het CIOT-systeem om deze te achterhalen.
Het CIOT kent echter twee beperkingen. Ten eerste beschikt het CIOT alleen over actuele identificerende gegevens, de gegevens bij het CIOT worden namelijk elke 24 uur geactualiseerd. Ten tweede staan prepaid telefoonnummers wel in het CIOT, maar hangen er veelal geen identificerende gegevens aan vast. Wel is uit het CIOT-bestand op te maken bij welke aanbieder het prepaid telefoonnummer is uitgegeven. Criminelen maken vaak gebruik van (meerdere) prepaid telefoons en simkaarten, wat de identificatie van de gebruiker van een bepaald telefoonnummer bemoeilijkt. Als het niet lukt om de gebruiker van een telefoonnummer te identificeren op basis van de gegevens die het CIOT heeft, is het mogelijk om, via de ULI, bij de telecomaanbieder van het uitgegeven telefoonnummer historische verkeersgegevens op te vragen. Nieuwe informatie betreffende de identiteit van de gebruiker zal de aanbieder niet hebben, maar wel is mogelijk om de vordering te voorzien van een datum en tijdstip die verder terug in de tijd gaat dan 24 uur. De opgevraagde verkeersgegevens kunnen ook inzicht geven in de vraag waar de telefoon zich bevond om zodoende meer informatie over de gebruiker te verzamelen.

Historische verkeersgegevens kunnen inzicht geven in de *contacten van een gebruiker* van een bepaald telefoonnummer. Bij het opvragen van historische verkeersgegevens is zichtbaar met welke telefoonnummers contact is geweest. Een aantal van deze contacten kan interessant zijn, omdat het bijvoorbeeld medeverdachten of getuigen kunnen zijn. Ook kan inzicht worden gekregen in tot dan toe onbekende contacten, hetgeen interessant kan zijn voor het onderzoek. Vaak is het opsporingsteam geïnteresseerd in het netwerk waarin de verdachte verkeert of waarin het slachtoffer verbleef. Met wie heeft/had hij telefonisch contact, wanneer en hoe vaak? Soms wordt een tele-

100 Voor meer informatie over het CIOT zie www.rijksoverheid.nl/onderwerpen/telecomgegevens-voor-opsporing (geraadpleegd 1 juli 2013).

foon enkel voor 'zakelijke' contacten gebruikt en krijgt het opsporingsteam een belcirkel van verdachten in beeld. Ook kan duidelijk worden dat een telefoonnummer enkel wordt gebruikt om één nummer mee te bellen, hetgeen inzicht geeft in heimelijke één-op-één-contacten en in afschermingstrategieën die de verdachte hanteert.
Ingeval iemand slachtoffer is geworden van bijvoorbeeld een verdwijning of een moord, is het ook interessant om te weten met wie hij of zij voor het laatst contact heeft gehad voordat hij of zij verdween of vermoord werd. Historische verkeersgegevens brengen dit in beeld.
Een andere, door de geïnterviewden veelgenoemde doelstelling van het opvragen van historische verkeersgegevens, is *plaatsbepaling*. Wanneer met een mobiele telefoon een gesprek wordt gestart, wordt contact gemaakt met een zendmast. Deze startlocatie (*First Cell ID*) valt onder de bewaarplicht en wordt dan ook door de aanbieder bewaard. Deze zendmasten staan op bepaalde locaties in Nederland en hebben een bepaald bereik waardoor opsporingsdiensten bij benadering kunnen zien waar de desbetreffende telefoon is geweest bij aanvang van het gesprek (zie ook paragraaf 5.4). Plaatsbepaling door middel van historische verkeersgegevens kan antwoord geven op vragen zoals: waar woont iemand; was iemand in de buurt van de plaats delict; wat waren de reisbewegingen van iemand; op welke locatie heeft iemand voor het laatst gebeld, et cetera. Als iemand is vermoord of is verdwenen, dan wil het opsporingsteam graag weten op welke locatie er voor het laatst met de telefoon van die persoon is gebeld.
Historische verkeersgegevens kunnen ook een grote rol spelen bij de overweging om een bepaald telefoonnummer al of niet te gaan tappen. Op basis van historische gegevens over het belgedrag kan een inschatting worden gemaakt van de capaciteit die nodig is om een eventuele tap uit te luisteren en te verwerken. Ook kan uit de verkeersgegevens blijken dat een telefoonnummer niet meer wordt gebruikt. In dat geval is een tap op het desbetreffende nummer zinloos. Tot slot worden historische verkeersgegevens aangevraagd als een OvJ het misdrijf niet zwaar genoeg vindt voor het inzetten van een tap. In dat geval kan een opsporingsteam aan de hand van verkeersgegevens toch zicht krijgen op de communicatiestromen.

5.2.2 Welk nummer opvragen?

Historische verkeersgegevens kunnen worden opgevraagd aan de hand van de naam van een telefoonnummer of een IMEI-nummer. Telefoonnummers van verdachten zijn soms reeds bekend en aanwezig in de systemen bij de politie, zoals BVO, BVH, Blueview, enzovoort, omdat ze eerder contact hebben gehad met de politie en daarbij hun telefoonnummer hebben opgegeven. Ook kan het zijn dat een verdachte een keer aangifte heeft gedaan van iets en daarbij zijn telefoonnummer heeft gegeven.

Daarnaast is het mogelijk om op basis van het unieke identificatienummer van de telefoon, een IMEI-nummer, verkeersgegevens op te vragen. Uiteraard is het ook mogelijk om achter een telefoonnummer te komen via de verdachte zelf, via een getuige of via een slachtoffer. Daarnaast worden telefoonnummers verkregen uit tapgesprekken of uit de historische verkeersgegevens van andere telefoonnummers. Zo kan er tijdens een tapgesprek een telefoonnummer genoemd worden dat interessant is voor de politie of ziet men een interessant tegennummer in de verkeersgegevens van een ander voorbijkomen waarvan vervolgens de historische verkeersgegevens kunnen worden opgevraagd. Een andere mogelijkheid om aan een telefoonnummer te komen, is via de Criminele Inlichtingen Eenheid (CIE). Dit politieonderdeel staat in contact met het criminele circuit en doet daar regelmatig informatie op, waaronder telefoonnummers van bepaalde personen. Deze informatie wordt doorgespeeld aan een opsporingsteam, dat vervolgens de verkeersgegevens kan gaan opvragen van het desbetreffende nummer. Voorts kan het opsporingsteam aan een telefoonnummer komen door het uitlezen van een in beslag genomen telefoon. Het opsporingsteam kan onderzoeken of daarin contacten zitten die mogelijk interessant zijn voor het onderzoek.

5.2.3 Moment van opvragen

Het opvragen van historische verkeersgegevens gebeurt gedurende het gehele onderzoek, maar het zwaartepunt ligt in het begin. Of men in het begin van het onderzoek al historische verkeersgegevens gaat opvragen, is afhankelijk van de hoeveelheid informatie die er al ligt.
Als er nog niet veel informatie is verzameld, maar men heeft wel een telefoonnummer, dan is het vrij eenvoudig om vanachter het bureau alvast een netwerk in kaart te brengen op basis van de telefoongegevens. Op basis van die informatie kan het opsporingsteam het verdere onderzoek dan weer vormgeven. Ook in geval van een straatroof waarbij een telefoon is buitgemaakt, wordt vrij snel besloten om historische verkeersgegevens van die telefoon op te vragen. Wanneer men in het begin historische verkeersgegevens opvraagt, ligt er meestal niet veel informatie waarmee men het onderzoek kan sturen.
Verkeersgegevens worden ook gedurende een onderzoek opgevraagd. Soms blijkt pas later dat de verkeersgegevens een missende schakel zijn in het onderzoek en worden ze alsnog opgevraagd. Of men stuit spontaan op een interessant telefoonnummer, waarvan de verkeersgegevens opgevraagd worden. Een geïnterviewde legt uit dat het ook voorkomt dat aan het einde van het onderzoek pas verkeersgegevens worden opgevraagd. Zij zegt:

> *'Maar het kan juist ook later zijn als de verdachten al binnen zitten en je hebt telefoons in beslag genomen. Dan ga je naar aanleiding van de in*

beslag genomen telefoons kijken naar IMEI-nummer, telefoonnummers die daar inzitten om daar de historische gegevens van op te vragen.' – politie

5.2.4 Proportionaliteit en subsidiariteit

Als een politieteam historische verkeersgegevens wil opvragen, dient het team toestemming te hebben van de OvJ. Hiervoor moet het team de aanvraag goed motiveren. Het opvragen van de gegevens dient proportioneel en subsidiair te zijn.[101] In het algemeen dient het politieteam het volgende aan te geven: wat voor soort onderzoek is het; hoe kom je aan het telefoonnummer; wat denk je ermee te bereiken. Als deze vragen in de aanvraag goed beantwoord worden, komt het zelden voor dat de OvJ de aanvraag afwijst. Opsporingsambtenaren geven aan dat wanneer ze verkeersgegevens opvragen, ze dit niet zonder reden doen en het dus logisch is dat er niet vaak wordt afgewezen. Wel gebeurt het dat de officier telefonisch terugkoppelt dat er iets veranderd of aangevuld moet worden in de aanvraag of dat de periode van aanvraag verkort moet worden. Daarnaast hangt de beoordeling af van de bekendheid van de OvJ in kwestie met de zaak, aldus de geïnterviewde. Een andere geïnterviewde zegt hierover:

'Heb je met je eigen zaaksofficier te maken, die kent de zaak, die heeft een 'riedeltje' nodig en dan weet hij waar het over gaat en dan ben je zo klaar. Maar heb ik een zaak die zich aandient en ik bel met een willekeurige officier die net dienst heeft, dan moet je vaak wel heel ver gaan in de beschrijving.' – politie

5.2.5 Frequentie en leeftijd

Het opvragen van historische verkeersgegevens gebeurt volgens respondenten in elk onderzoek waarin is voldaan aan de vereisten van proportionaliteit en subsidiariteit. Een professional, werkzaam als opsporingsambtenaar, omschrijft het opvragen van historische verkeersgegevens als een standaardprocedure. Anderen zeggen dat het 'heel veel' wordt opgevraagd. Dit correspondeert met de cijfers die in hoofdstuk 6 worden gepresenteerd.

'Ik heb op de hoeveelheid zelf geen zicht, maar het behoort bijna tot de standaardprocedures.' – politie

'Ja, dat doen we eigenlijk bij elk onderzoek. Bij elk beetje groot onderzoek maken we gebruik van dit soort gegevens.' – politie

101 Het *proportionaliteitsbeginsel* schrijft voor dat er een zekere evenredigheid moet zijn tussen de ingrijpendheid van een opsporingsmiddel enerzijds en de ernst van het op te lossen misdrijf anderzijds. De vraag of er in het specifieke geval een ander, minder ingrijpend opsporingsmiddel kan worden ingezet waarmee hetzelfde resultaat kan worden bereikt, betreft het *subsidiariteitsbeginsel*.

'(...) niet in elke zaak, maar in het merendeel van de zaken.' – advocaat

Tegelijkertijd geven meerdere geïnterviewde professionals aan dat niet van elk telefoonnummer dat ter ore komt van de politie de historische verkeersgegevens worden opgevraagd. Zo antwoordt een professional op de vraag of van elk telefoonnummer dat ze in handen krijgen en van belang achten voor het onderzoek de verkeersgegevens worden opgevraagd, het volgende:

'Nee, echt niet, we zijn daar wel kritisch in. Ik moet wel zeker weten dat er iets mee gedaan wordt. Het moet echt een doel hebben en niet zo zijn van, wat je vaak ziet, "We nemen drie telefoons in beslag en we vragen ook maar meteen de printgegevens op." Dan komen vervolgens die lijsten binnen en worden niet eens geopend. Dat zag je in het verleden wel eens, maar daar ben ik heel kritisch op.' – politie

In het kader van de bewaarplicht is het interessant om na te gaan hoe oud de gegevens zijn die worden opgevraagd. Uit tabel 1 in paragraaf 6.1.1 valt af te lezen dat driekwart van de opgevraagde gegevens niet ouder is dan zes maanden. Tijdens de interviews is gevraagd naar de redenen van de termijn waarover gegevens worden opgevraagd. Dit blijkt nauw samen te hangen met de aard van het onderzoek en met de aard van de onderzoeksvraag. Bij een onderzoek naar een beroving vragen de geïnterviewde professionals bij de politie standaardgegevens aan over 'een hele korte periode'. Een professional uit de opsporingspraktijk geeft als voorbeeld een straatroof, waarbij een mobiele telefoon wordt gestolen. In dat geval worden voor een aantal dagen de historische verkeersgegevens van die telefoon opgevraagd om te achterhalen waar de gestolen telefoon zich bevindt en wie er gebruik van maakt. Andere geïnterviewden zeggen dat ze standaardgegevens over een periode van een aantal maanden tot een halfjaar opvragen. Dit gebeurt bij onderzoeken die vaak langer duren, zoals bij moordzaken en onderzoeken naar georganiseerde misdaad. Zo antwoordt een professional uit de opsporingspraktijk op de vraag hoe lang zij terugvraagt:

'Dat is afhankelijk van je onderzoek. Je maakt altijd de afweging. Als ik een hele specifieke vraag heb; ik heb een moordzaak. En ik wil iets weten over de contacten van de week ervoor dan vraag je gewoon die week ervoor op. Als je probeert te analyseren wie iemand is, je wilt identificeren, wat zijn zijn tegencontacten, dan ga je langer opvragen. Of je wilt contacten in kaart brengen, dat mensen zeggen we bellen elkaar misschien een keer per maand. Nou ja als het belangrijk is dan kan je zeggen dan vragen we een jaar op en dan blijkt dat iemand tien keer per maand een heel jaar lang belt, dan geeft dat een heel ander beeld. Dus het ligt echt heel erg aan de vraag wat je opvraagt. Het is nooit standaard "oh doe maar een jaar". Daar heb je gewoon niet altijd wat aan.' – politie

5.2.6 Analyseren van de gegevens

Historische verkeersgegevens komen digitaal bij het opsporingsteam binnen. De ULI is slechts een bemiddelingspunt waar alle opgevraagde en geleverde gegevens samenkomen en doorgestuurd worden naar de belanghebbende. Hier vindt de ontsleuteling plaats, maar geen analyse van de bestanden. Verkeersgegevens worden niet altijd in hetzelfde format aangeleverd. Het vergt soms de nodige moeite om alles in hetzelfde format te gieten, hetgeen nodig is om de gegevens te kunnen analyseren en interpreteren. Sommige aanbieders versturen de verkeersgegevens versleuteld door naar de ULI, van waaruit de bestanden via een gesloten beveiligd netwerk weer worden doorgestuurd naar het korps. De opgevraagde informatie wordt in het algemeen versleuteld en beveiligd verstuurd. Echter, volgens de expert van het ULI werken sommige aanbieders niet goed mee aan de beveiligde overdracht zoals door de ULI wordt aangegeven. In dat geval worden de verkeersgegevens onversleuteld via de e-mail verstuurd.
Er is geen vaste standaard afgesproken voor het aanleveren van verkeersgegevens en iedere aanbieder doet dit op zijn eigen manier en in zijn eigen format. Het analyseren van de bestanden levert volgens sommige professionals en experts weleens problemen op. Verkeersgegevens kunnen zowel handmatig als met behulp van een analysetool worden geanalyseerd. De meeste geïnterviewde professionals geven aan gebruik te maken van het programma Digitale Communicatie Sporen (DCS) om de binnengekomen verkeersgegevens te analyseren. Het analyseren van verkeersgegevens is specialistisch werk dat meestal door een analist wordt gedaan. Echter, niet bij elk onderzoek is een analist betrokken, dus soms worden de verkeersgegevens door andere opsporingsambtenaren geanalyseerd.
Als de bestanden zijn ingelezen in DCS kan degene die ermee werkt de vragen gaan stellen die het opsporingsteam te weten wil komen, zoals: welke contacten heeft dit nummer, welke masten heeft dit nummer aangestraald, enzovoort. Het analyseproduct dat door middel van DCS is gegenereerd, heeft geen bewijskracht. Wanneer men iets als bewijs wil gebruiken, dient men terug te gaan naar het originele format en daarop (als dit mogelijk is)[102] het gedeelte aan te geven dat als bewijs moet dienen. Een geïnterviewde zegt hierover:

> *'Volgens mij is het gebruik van DCS ook bij justitie afgeregeld en goedgekeurd en toch wordt er nog steeds gezegd: je moet altijd terug naar het origineel. Dat snap ik wel, DCS interpreteert natuurlijk, en doet een extra stap. Ik kan ook wel een inschatting maken, hier kan DCS niks raars mee gedaan hebben. Het is een gesprek van A naar B en dan werp ik een snelle blik op het origineel en dan geloof ik het wel. Als het echt heel belangrijk wordt over aantal smsjes dan moet ik het origineel helemaal gaan uitplui-*

102 Sommige aanbieders leveren in XML-format aan. Dit is met het blote oog erg lastig te interpreteren.

zen. Bij [aanbieder X] begin ik daar niet eens aan. Want dat is een xml-formaat, dat kan ik je nu niet laten zien, maar daar word je echt niet gelukkig van. (…)' – politie

Professionals en experts van de politie vinden het teruggaan naar het originele document erg bewerkelijk en het komt volgens de geïnterviewde uit de opsporingspraktijk neer op het verrichten van dubbelwerk. Wanneer een specialist dit al als lastig en moeilijk omschrijft, is het maar de vraag of advocaten, OvJ en rechters kennis hebben om de originele verkeersgegevens op waarde te kunnen beoordelen wanneer deze in het procesdossier zitten. Deze vraag hebben we voorgelegd aan advocaten.

'In de pleitnota van een zaak zie ik dat de deskundige gesproken heeft over de "grofmazigheid van het Telfort-netwerk; over relaties met andere basisstations; over opstelpunt 15.913; het dichterbij gelegen basisstation 48.753, enzovoorts". Nou ja, daar ga je dan mee aan de slag en daar wordt je dan helemaal gek van.' – advocaat

Het analyseren van de historische verkeersgegevens wordt gezien als specialistisch werk dat, volgens een aantal experts bij de politie, enkel door analisten gedaan zou moeten worden. Er bestaat bij de politie een speciale opleiding voor het werken met historische verkeersgegevens. Tijdens die opleiding leert men omgaan met het analyseprogramma DCS. Omdat de telefoniemarkt snel verandert, worden er regelmatig updates aangeboden van de cursus. Naast de opleiding is het volgens respondenten ook een kwestie van jezelf verdiepen in de materie en kennis uitwisselen met collega's. De advocaten die we voor dit onderzoek hebben gesproken, hadden beiden ervaring met het inschakelen van deskundigen op het gebied van verkeers- en locatiegegevens. Echter, hieraan zijn hoge kosten verbonden en de meeste cliënten kunnen deze kosten niet dragen. Een advocaat vertelt dat hij zelf aan het tekenen is gegaan:

'Als het voor de zaak van belang is en de verdachte zegt dat het gewoon niet klopt, dan leg ik het niet naast me neer. We hadden een paar jaar geleden een moordzaak en daar heb ik toen zelf de tekeningen opnieuw gemaakt, opnieuw lijnen getrokken aan de hand van de verhoren bij de rechter-commissaris van de getuigen-deskundigen, waardoor het gebied waar mijn cliënt zich zou hebben bevonden, heel anders kwam te liggen. Het was veel kleiner doordat bleek dat een zendmast op dat moment uitgevallen was. [...] Dan blijkt dus dat het niet zulke harde informatie was. Het wordt vaak gebracht als een soort hard technisch bewijs, een objectief bewijsmiddel, en dat is het in het beginsel ook wel, maar de interpretatie is heel ingewikkeld.' – advocaat

'Je kunt wel een deskundige vragen. Die kunnen die ruwe data wel analyseren, maar die zijn hartstikke duur; dat kost algauw een paar duizend euro. Dat moet de klant dan wel kunnen opbrengen. Soms kan het wel, maar vaak ook niet; vaak is het geld er gewoon niet.' – advocaat

Daarnaast bestaat de mogelijkheid om de analyses en interpretaties in het proces-verbaal goed te controleren. Vooral aan de interpretatie van de analyse wordt nog wel eens getwijfeld.

'Het risico is dat je een gekleurde presentatie krijgt van die gegevens. Dan kun je wel vragen "mogen we die gegevens dan hebben", en dan komen de ruwe data naar je toe, maar dan krijg je honderden pagina's volstrekt onleesbare zendmastgegevens, want je hebt wel software nodig om die te analyseren. Die heb je als verdediging niet en daar kun je ook niet aankomen. Daar heb je dus niks aan, terwijl gedaan wordt alsof je het hebt kunnen controleren. Daar zit een risico in; in het middel en in de manier waarop het geïnterpreteerd wordt. [...] Eigenlijk zou je als advocaat die berg moeten kunnen krijgen en zeggen: "Kijken wat er uitkomt als ik mijn hypothese er in gooi". Maar dat kan niet.' – advocaat

'Je krijgt doorgaans een overzichtsproces-verbaal van de politie die zegt: "Wij hebben een telecommunicatieonderzoek gedaan en de conclusies daarvan zijn de volgende." Als die conclusies worden betwist door de cliënt dan willen we het achterliggende informatiemateriaal zien en controleren. [...] De kans dat je daarmee scoort is niet zo groot, want mijn ervaring is dat dit doorgaans klopt en dat het vaak zit op de subjectieve conclusie die er aan de gegevens worden verbonden.' – advocaat

5.2.7 Opbrengsten

Historische verkeersgegevens van telefonie worden door alle geïnterviewde professionals en experts als heel waardevol omschreven. Afhankelijk van de fase waarin het opsporingsonderzoek zich bevindt, levert het sturingsinformatie dan wel bewijs op. In het begin van het onderzoek leveren historische verkeersgegevens veelal sturingsinformatie op, informatie waarop het verdere onderzoek kan worden ingericht. Zo kan op basis van verkeersgegevens duidelijk worden wie de verdachten zijn en waar het opsporingsteam het observatieteam naartoe moet laten rijden. Zo zegt een professional van de politie:

'Het kan echt net een plusje zijn. Het is nooit het enige bewijs dat je hebt, want dat zou niet goed zijn, maar het is een waardevolle ondersteuning in de opsporing, in contact tussen telefoonnummers en eventueel tussen mensen. Het kan een selectiemiddel zijn. Het kan je heel veel werk besparen.

[…] Als je niet weet waar iemand woont, dan kijk je naar het eerste contact van de dag en het laatste en dan kijk je naar de zendmast en als ik daar een lijn in zie dan weet ik ongeveer waar iemand naar bed gaat. Die kan ik in een kaart gaan intekenen en dan kan ik zeggen stuur het observatieteam eens daar naar toe in plaats van daar. Dat maakt het efficiënt. Dat je gewoon net even wat gerichter je onderzoek kunt doen op sommige momenten.' – politie

Wanneer het onderzoek wat verder is gevorderd, kunnen de historische verkeersgegevens ook als bewijs dienen. De geïnterviewde professionals en experts spreken met name over 'ondersteunend bewijs': historische verkeersgegevens versterken de bewijslast maar zijn nooit het enige bewijs. Een mooi voorbeeld van bewijs, geleverd door historische verkeersgegevens, geeft onderstaande professional. Zij vertelt over een onderzoek naar phishing:

'De klant van een bank kreeg een mail thuisgestuurd met een gekloonde website, waar hij zijn gegevens moest invullen en vervolgens werd hij daarna gebeld door een zogenaamde bankmedewerker. Dat ging zo van: 'Ik ben mevrouw Janssen van de ABN AMRO en ik werk bij veiligheidszaken. Wij zijn in het kader van veiligheid bezig om alles te updaten. Kunt u even uw "identifier" en uw pasje erbij pakken. Dan gaan wij een en ander even doornemen.' Daar trappen toch heel wat mensen in. Bij een van onze verdachten hebben wij tijdens een doorzoeking heel wat simkaarten en telefoons aangetroffen. Daar hebben wij de historische verkeersgegevens van opgevraagd. Daar bleek dus wel uit dat daar heel veel slachtoffers mee zijn gebeld. Dat kun je dan weer mooi voegen in je zaakdossier en ook voor de OvJ.' – politie

Net zoals hiervoor bij de doelstellingen is besproken, geven de geïnterviewde professionals en experts aan dat de opbrengsten van historische verkeersgegevens met name ook juist die punten zijn: (1) het identificeren van een gebruiker; (2) het achterhalen van contacten; (3) plaatsbepaling; (4) het traceren van een IMEI-nummer; en (5) het maken van een capaciteitsafweging alvorens men gaat tappen.
Het komt wel eens voor dat historische verkeersgegevens worden opgevraagd maar uiteindelijk niet worden bekeken of geanalyseerd. Dat is inherent aan het politiewerk, aldus een geïnterviewde:

'Gebeurt niet heel veel maar ik heb het wel meegemaakt. Soms ben je ook echt van plan het te gebruiken, bijvoorbeeld om iemand te identificeren of te lokaliseren. Alleen het is nooit het enige waar je op inzet. Je hebt bijvoorbeeld ook nog een observatieteam of je hebt andere manieren van opsporing, waardoor je al iemands identiteit of verblijfplaats vaststelt voordat je

de histo hebt kunnen gebruiken. Dat gebeurt. Alleen daar kun je niet van tevoren van uitgaan. Soms is het een sneller dan het andere.' – politie

Daarentegen zegt een aantal professionals dat dit bij hen niet voorkomt: als het opgevraagd wordt, wordt het altijd bekeken. Weer een andere geïnterviewde zegt dat het iets is dat in het verleden wel voorkwam, maar tegenwoordig niet meer. Een rechercheur moet zich goed verantwoorden wat hij met die gegevens gaat doen en wat hij ermee denkt te bereiken.

5.2.8 Relevantie van de opgeslagen gegevens

De Wet bewaarplicht verplicht aanbieders bepaalde gegevens op te slaan en voor een bepaalde tijd beschikbaar te houden voor de opsporing. Bij de gesprekken is de geïnterviewde professionals en experts gevraagd of de opgeslagen gegevens allemaal even relevant worden gevonden of dat men juist belangrijke informatie mist.
Alle geïnterviewde professionals en experts geven aan de opgeslagen verkeersgegevens van telefonie zeer relevant te vinden. Een professional uit de opsporingspraktijk zegt echter geen gebruik te maken van de X- en Y-coördinaten van de zendmasten. De landelijke eenheid heeft een database, Route 66 genaamd, waarin de locaties van de zendmasten zijn aangegeven, hetgeen de X- en Y-coördinaten overbodig maakt, aldus deze geïnterviewde. Een aantal geïnterviewde professionals uit de opsporingspraktijk geeft aan pas te weten of de opgeslagen verkeersgegevens relevant zijn als ze deze gegevens in handen hebben. Soms blijkt na ontvangst van de verkeersgegevens van een bepaald telefoonnummer dat je er niets aan hebt, omdat het telefoonnummer bijvoorbeeld niet gebruikt wordt.

Een aantal professionals uit de opsporingspraktijk geeft aan niet alleen de beginlocatie (*first cell*) van een telefoongesprek te willen ontvangen, maar ook de eindlocatie (*last cell*). De beginlocatie, dat is de mast die wordt aangestraald aan het begin van een gesprek, valt onder de bewaarplicht. Echter, waar het gesprek eindigt – dus de laatste connectie met een zendmast – valt volgens de bijlage behorende bij artikel 13.2a Tw niet onder de bewaarplicht. Dit betekent dat wanneer iemand bellend de auto of trein instapt, uit de historische verkeersgegevens niet valt op te maken op welke locatie het gesprek eindigt. Echter, de eindlocatie van het gesprek blijkt door een grote aanbieder wel bij de verkeersgegevens te worden meegeleverd.[103] Dit is opmerkelijk te noemen, omdat tijdens een gesprek met AT naar voren kwam dat in het verleden een aanbieder hierop terecht gewezen is en de *last cell*, de eindlocatie, niet meer meegeleverd mocht worden met de gevorderde verkeersgegevens. De eindlocatie van een gesprek kan overigens wel met een andere vordering opgevraagd worden.

103 Zie hierover ook hoofdstuk 4, paragraaf 4.1.

5.2.9 Efficiëntere opsporing?

Het opvragen van historische verkeersgegevens is een van de vele opsporingsmiddelen die de politie heeft. Op de vraag of het opvragen van historische verkeersgegevens bijdraagt aan een efficiëntere opsporing, antwoorden de meeste geïnterviewde professionals en experts bevestigend. Met de opbrengsten van historische verkeersgegevens kunnen andere opsporingsmiddelen gerichter worden ingezet. Wanneer door middel van verkeersgegevens vaststaat in welke wijk iemand woont, maakt dat het observeren door het observatieteam efficiënter dan wanneer het observatieteam 'ergens in Groningen' moet zijn. Wanneer blijkt dat een telefoon nauwelijks wordt gebruikt, hoeft er geen tap te worden aangevraagd. En door een gestolen mobiele telefoon te lokaliseren, kan gericht naar verdachten worden gezocht. De Wet bewaarplicht heeft volgens een aantal professionals en experts tot een efficiëntere opsporing geleid, omdat de verkeersgegevens betreffende telefonie nu een jaar worden bewaard. Voordat de wet in werking trad, werd de bewaartermijn maar ook de vernietiging van deze gegevens aan de aanbieders zelf overgelaten. Er bestond wel een beperkte bewaarplicht van drie maanden voor prepaid nummers, maar de geïnterviewde professionals en experts geven aan dat gegevens in het algemeen korter beschikbaar waren dan ze nu zijn. Een professional zegt hierover het volgende:

> *'... Drie maanden ben je zo voorbij. Ook in onderzoeken waarbij je heel hard in het heden bezig bent, en ook omdat de advocatuur misschien wel iets vraagt, want dit is ook wel goed om te benadrukken. Die kunnen ook nog ontlastend zeggen dat hun cliënt nooit contact had. En als die gegevens dan vernietigd zijn, ze bestaan niet meer, het jaar is voorbij, dan kan je dat heel hard roepen, maar het kan niet bevestigd of ontkracht worden. En de verdediging komt pas later om de hoek kijken. In die zin kan ik me voorstellen, dat het juist zinvol is dat het één jaar is.'* – ovj

> *'Ik weet zeker dat als ik nu iets opvraag dat ik een jaar terug kan gaan. Dat was vroeger allemaal wat onzekerder. Dat was rommeliger toen was je echt afhankelijk van de aanbieder. En dat is nu gewoon duidelijk.'* – politie

5.2.10 Volstaat de bewaartermijn voor telefonie in de opsporing?

De Europese richtlijn laat de lidstaten de keuze in een bewaartermijn van 6 tot en met 24 maanden. Nederland heeft gekozen voor een bewaartermijn van 12 maanden voor telefoniegegevens.
Zowel tijdens de gesprekken als op basis van de statistieken in hoofdstuk 6 kan worden afgeleid dat er bij opsporingsdiensten soms behoefte bestaat aan verkeersgegevens uit de periode die ligt na het verstrijken van de bewaartermijnen. Een aantal bevragingen, zo is in tabel 1 van paragraaf 6.1.1 te zien,

wordt gedaan nadat de bewaartermijn is verstreken. Hiermee wordt geen wet- of regelgeving overtreden. Men mag een vordering indienen die verder teruggaat dan de bewaartermijn lang is. De behoefte aan deze oudere verkeersgegevens is er met name in cold cases, onderzoeken die na lange tijd zijn terugverwezen naar het Hof en waar soms nieuw of aanvullend onderzoek moet plaatsvinden, en onderzoeken waarbij na een jaar ineens tips binnenkomen. Tijdens de gesprekken bleek dat het merendeel van de professionals bij de politie van mening is dat de bewaartermijn van een jaar voldoende is voor het werk dat zij doen, maar zij wijzen er tegelijkertijd op dat de bewaartermijn in grote, langdurige onderzoeken te kort kan schieten.
Een geïnterviewde gaf als voorbeeld dat er in een onderzoek naar een overval een heel jaar verkeersgegevens van een verdachte waren opgevraagd. Toch was de bewaartermijn van een jaar hier niet toereikend:

> *'In dit onderzoek zouden wij liever wat verder terug willen, want wat blijkt nou? De auto die daarbij gebruikt is, is ook van een overval afkomstig en die overval heeft net buiten dat jaar plaatsgevonden, maar daar kwamen wij nou recentelijk pas achter. Dat vinden wij een gemiste kans. Maar goed, tot hoe lang moet je gaan bewaren?'* – politie

Enkele opsporingsteams daarentegen, bijvoorbeeld een straatroofteam, vragen de historische verkeersgegevens nooit voor een langere periode op en geven dan ook aan dat de bewaartermijn wat hen betreft korter kan. Maar de algemene conclusie onder de professionals en experts die vanuit het opsporingsperspectief spreken, is dat de bewaartermijn van een jaar voor verkeer- en locatiegegevens betreffende telefonie volstaat en ook niet korter zou moeten zijn.

5.2.11 Notificeren en vernietigen

Omdat bijzondere opsporingsbevoegdheden een inbreuk kunnen maken op de persoonlijke levenssfeer, dient het OM personen tegen wie een dergelijke bevoegdheid is ingezet daarover te notificeren (art. 126bb lid 1 Sv.). Na afloop van de zaak moet de informatie die is verkregen met de ingezette bijzondere opsporingsbevoegdheid vernietigd worden (art. 126cc lid 2 Sv.). Deze wettelijke regels gelden ook voor het vorderen van historische verkeersgegevens. Maar de bevoegdheid tot het vorderen van gebruikersgegevens (art. 126na/ua/zi Sv.) is uitgesloten van notificatie.
De wijze van notificeren is in dit onderzoek niet expliciet onderzocht, omdat hier al uitgebreid onderzoek naar werd gedaan in het vorig jaar gepubliceerde onderzoek naar het gebruik van de telefoon en internettap in de opsporing. Voor een uitgebreide beschrijving van het notificeren verwijzen we naar dit rapport (Odinot et al., 2012, p. 138). Dit onderzoek liet zien dat er

op de onderzochte parketten doorgaans wordt genotificeerd, maar dat ditgeen hoge prioriteit heeft.
Ook in zaken die uiteindelijk niet op zitting komen en in zwacri-zaken wordt volgens de geïnterviewde professionals in principe genotificeerd, 'mits toekomstige opsporingsbelangen daarmee niet worden geschaad'. Een professional die op de BOB-kamer werkte en zich fulltime bezighield met notificeren, zei dat in ongeveer tien tot twintig gevallen per jaar wordt besloten niet te notificeren na de inzet van een buitengewone opsporingsbevoegdheid, zoals een telefoontap, inzet van een observatieteam of vordering van historische verkeersgegevens. Dit, op een totaal van 2.000 te notificeren personen per jaar in de desbetreffende regio. Volgens hem werd er niet genotificeerd in mogelijke cold cases, embargozaken en zedenzaken. Daarnaast blijft het notificeren logischerwijs achterwege in de gevallen waarin justitie geen NAW-gegevens heeft kunnen achterhalen.

De professionals van politie en OM die voor dit onderhavige onderzoek zijn geïnterviewd, is gevraagd naar het vernietigen van gegevens dat drie maanden na het versturen van de notificatiebrief moet plaatsvinden. De geïnterviewde opsporingsambtenaren geven aan dat gegevens die door middel van bijzondere opsporingsbevoegdheden zijn verkregen, zoals opgevraagde historische verkeersgegevens, inderdaad na verloop van tijd worden vernietigd. Echter, dit vernietigen van gegevens verloopt niet vlekkeloos: zeker in geval van oude onderzoeken is het lastig om alle informatie weer boven tafel te krijgen. Volgens een expert van de politie betreft het een ICT-technisch probleem en zijn de systemen hier niet op ingericht. Volgens deze geïnterviewde expert zouden dit soort gegevens een digitaal label moeten krijgen, waarmee deze gegevens altijd door het systeem ter vernietiging herkend en opgeroepen kunnen worden. Historische verkeersgegevens worden vaak in politiesystemen gezet. Hieruit zou deze informatie na verloop van tijd ook verwijderd moeten worden. De geïnterviewde expert constateert dat dat niet altijd gebeurt, gewoonweg omdat de informatie moeilijk te vinden is. Het markeren van de informatie door het toevoegen van een digitaal label zou hiervoor uitkomst bieden.

5.3 Het gebruik van historische verkeersgegevens internet

Naast verkeersgegevens betreffende telecommunicatie kunnen opsporingsdiensten ook historische verkeersgegevens over internetcommunicatie opvragen. In deze paragraaf wordt ingegaan op de wijze waarop historische gegevens over internetverkeer gebruikt worden in de opsporingspraktijk. Daarbij zal worden ingegaan op de vraag welke gegevens precies bewaard worden en opvraagbaar zijn. Voorts zal een beeld worden geschetst van de

wijze waarop historische internetverkeersgegevens gebruikt worden bij de opsporing en vervolging van verschillende soorten misdrijven.

5.3.1 Wat wordt er bewaard?

De Telecommunicatiewet schrijft voor dat gegevens betreffende *internettoegang, e-mail over het internet en internettelefonie,* door de aanbieders bewaard dienen te worden voor een periode van zes maanden. Zoals eerder opgemerkt blijkt de wet op sommige punten ingehaald door technologische ontwikkelingen en door het veranderde telefoon- en internetgebruik. Dit geldt met name voor het deel van de bewaarplicht dat betrekking heeft op de gegevens betreffende internetverkeer. In de bijlage behorende bij artikel 13.2a Tw wordt internettelefonie bijvoorbeeld vermeld onder het thema internetverkeersgegevens. In de memorie van toelichting behorende bij het wetsvoorstel dat voorziet in de aanpassing van de bewaartermijn voor internetverkeersgegevens wordt een uitzondering gemaakt voor VoIP-diensten waarvan de functionaliteit zodanig nauw samenhangen met die van traditionele telefonie dat deze diensten worden aangemerkt als telefonie over een vast of mobiel netwerk. Voor deze diensten bleef een bewaartermijn van twaalf maanden gelden.[104] Als gevolg van dit besluit – en op advies van de Experts Group Data Retention van de Europese Unie – hebben de Nederlandse aanbieders het advies (DatRet/expgrp. 2010)[105] overgenomen, waarin werd geadviseerd de definities voor de verschillende vormen van telefonie te harmoniseren. In de praktijk betekent dit dat wanneer verkeersgegevens worden opgevraagd van een telefoon waarmee via het internet wordt gebeld maar daarbij gebruikmakend van een dienst die voldoet aan de functionaliteitseis, er eenzelfde set gegevens geleverd wordt als wanneer een 'ouderwetse' manier van telefonie wordt gebruikt. Dit is mogelijk door het onderscheid dat de overheid maakt tussen verschillende vormen van telefonie door de functionaliteit en belangrijkste kenmerken van de telefoniedienst voorop te stellen.[106] Voor VoIP-diensten waarbij bijvoorbeeld gebruik wordt gemaakt van het Nationale Nummerplan, waarbij doorschakeling mogelijk is en toegang wordt geboden tot het alarmnummer 112, geldt een bewaartermijn van twaalf maanden. Voor verkeersgegevens van spraakdiensten die gebruikmaken van het internet en die niet over deze functionaliteiten beschikken, geldt een bewaartermijn van zes maanden. Er zijn ook internettelefoniediensten zoals Skype, Icall, Axvoice, Facetime, enzovoort die buiten de bewaarplicht vallen, omdat het diensten zijn waarvoor geen bewaarplicht geldt of omdat de aanbieder in het buitenland is gevestigd.

104 *Kamerstukken II* 2009/10, 32 185, nr. 3.
105 http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/pdf/series_a_position_paper_5_final_14_07_2010_closer_understanding_of_the_term_internet_telephony_en.pdf (geraadpleegd op 1 februari 2013).
106 Zie: www.agentschaptelecom.nl/onderwerpen/veiligheid/Opslag-telecomgegevens (geraadpleegd op 4 maart 2013).

Zoals beschreven in bijlage B. behorende bij artikel 13.2a Tw worden de volgende gegevens opgeslagen voor een periode van zes maanden:

a de toegewezen gebruikersidentificatie (IP-adres) en de gebruikersidentificatie of telefoonnummer van de beoogde ontvanger van een internettelefoonoproep;
b de gebruikersidentificatie en het telefoonnummer toegewezen aan elke communicatie die het publieke telefoonnetwerk binnenkomt;
c naam en adres (NAW-gegevens) van de abonnee of de geregistreerde gebruiker aan wie het IP-adres, de gebruikersidentificatie of het telefoonnummer was toegewezen op het tijdstip van communicatie en naam en adres van de abonnee of de geregistreerde gebruiker en de gebruikersidentificatie van de beoogde ontvanger van communicatie;
d datum en tijdstip van de log-in en log-off van een internetsessie, gebaseerd op een bepaalde tijdzone, samen met het IP-adres, hetzij statisch, hetzij dynamisch, dat door de aanbieder van een internettoegangsdienst aan een communicatie is toegewezen en de gebruikersidentificatie van de abonnee of geregistreerde gebruiker;
e datum en tijdstip van log-in en log-off van een e-maildienst over het internet of internettelefoniedienst gebaseerd op een bepaalde tijdzone;
f de gebruikte internetdienst (wifi, dial-up, mobiel, et cetera);
g het inbellende nummer voor een inbelverbinding;
h de digital subscriber line (DSL) of ander eindpunt van de initiatiefnemer van de communicatie.

Historische verkeersgegevens betreffende internet- en e-mailgebruik kunnen inzicht bieden in de IP-adressen die door iemand zijn gebruikt en in de e-mailcontacten van zender en ontvanger. De inhoud van gesprekken, berichten of e-mails, zoektermen die zijn ingetypt in een zoekmachine en IP-adressen van bezochte internetpagina's vallen niet onder de bewaarplicht.

5.3.2 Relatief weinig ingezet

Tijdens de gesprekken die zijn gevoerd voor dit onderzoek werd duidelijk dat de voor dit onderzoek gesproken professionals ruime ervaring hebben met het werken met historische gegevens betreffende telefonie, maar weinig tot geen kennis hebben over de wijze waarop historische gegevens betreffende het internetverkeer in de opsporing gebruikt zouden kunnen worden.

> *'Het is mij onbekend dat IP-gegevens ook onder de bewaarplicht vallen en daar moet ik ook eens achteraan wat je dan allemaal krijgt. Waar krijg ik dat? Krijg ik dat zo? Krijg ik dat in mijn andere tapsysteem? Ik heb geen idee.'* – politie

'Het lijkt mij heel interessant. Alleen heb ik dus echt geen idee wat ik dan krijg.' – politie

'Wordt amper gebruikt, dat is iets van de laatste tijd. In mijn praktijk wordt dat amper gebruikt.' – advocaat

Uit de gesprekken met professionals en experts die wel bekend zijn met de bewaarplicht van gegevens over internetverkeer en met de wijze waarop die gegevens in de opsporing kunnen worden gebruikt, blijkt ook dat men in eerste instantie liever kiest voor historische telefoongegevens dan voor gegevens betreffende het internetverkeer. Dit komt ook naar voren in de cijfers over 2012 (zie paragraaf 6.1.1, tabel 1), waaruit blijkt dat het aantal bevragingen betreffende internet- en e-mailverkeer veel lager ligt dan het aantal bevragingen betreffende telefonie.

'Van IP wordt wel gebruikgemaakt, maar als je het vergelijkt met het aantal bevragingen over telefonie is dat echt een fractie, maar het is wel belangrijk. [...] Het is met name belangrijk als er bepaalde activiteiten geweest zijn vanuit een IP-adres.' – politie

'Ja, ik maak wel eens gebruik van IP-gegevens maar niet zo vaak als van telecomgegevens.' – politie

'We doen het wel eens maar het [opvragen van IP-gegevens] komt niet extreem vaak voor, maar we doen het wel.' – politie

'(…) alle rechercheurs hebben ook mobiele telefonie en laptops, maar er wordt toch heel klassiek vooral naar telefonie gekeken.' – OvJ

Veel professionals lijken last te hebben van koudwatervrees en van een gebrek aan kennis over de wijze waarop internetverkeersgegevens in de opsporing kunnen worden gebruikt. Dit beeld wordt bevestigd door een van de ondervraagde OvJ's:

'Er moet niet alleen veel kennis zijn over wat er allemaal mogelijk is, maar ook welke route je moet bewandelen. Dat merk ik in de praktijk ook nog wel eens en dat is heel hardnekkig. […] Ik denk dat bij een flink deel van de rechercheurs die kennis er niet is en ze weten niet dat ze kunnen doorvragen [door rechercheren].' – OvJ

'Er wordt heel veel geïnvesteerd door ons, door de ULI, door de regionale interceptiecoördinatoren, om het niveau op te krikken, om mensen duidelijk te maken hoe en wat. Maar op de een of andere manier is dat heel hardnekkig. Ik weet niet precies wat het is, eerlijk gezegd.' – OvJ

Dit kwam voor de onderzoekers niet als een verrassing. Gelijke bevindingen zijn gerapporteerd in het vorig jaar gepubliceerde rapport naar het gebruik van de telefoon- en internettap in de opsporingspraktijk (Odinot et al., 2012). Uit dat onderzoek kwam naar voren dat slechts weinig opsporingsambtenaren bekend zijn met de internettap en dat het opsporen op internet nog in de kinderschoenen staat. Daarnaast worden werkzaamheden die te maken hebben met aan internet gerelateerde zaken vaak uitgevoerd door experts, omdat de digitalisering van de huidige samenleving nog niet behoort niet tot het dagelijkse werkterrein van veel opsporingsambtenaren. Op dit punt valt er nog een wereld te winnen door bijvoorbeeld het binnenhalen van jonge mensen die deel uitmaken van de digitale samenleving, maar ook met gerichte opleidingen en andere vormen van kennisoverdracht.

> *'De klacht dat opsporingsdiensten tegenwoordig niet zoveel meer kunnen omdat er heel veel via internet gaat, valt in het niet bij de hoeveelheid gegevens die ze extra hebben gekregen en die ze nu veel makkelijker kunnen krijgen. Als gevolg van die technologie is er veel ook makkelijker geworden. Ik denk dat het goed is als de politie meer aandacht gaat besteden aan haar eigen kennisniveau.'* – BoF

Maar tegelijkertijd moeten we constateren dat de technologische ontwikkelingen heel snel gaan. Zo snel dat het voor de schaarse experts zelf maar met moeite bij te houden is. Het is dan ook niet zo eenvoudig om dit kennistekort bij de recherche te ondervangen.

> *'Er is echt een schreeuwend tekort aan digitale experts. Het is voor ons ook moeilijk om bij te blijven. Ik ga dit jaar ook weer trainingen volgen op internetgebied. Maar wij kunnen niet voor al die rechercheurs in die zaken bijlopen, dus daar blijven we echt ernstig in achter.'* – politie

> *'Er zijn te weinig mensen die voldoende kennis hebben. Gelukkig hebben wij ook nog een afdeling digitale expertise, dat zijn de mensen die meer gespecialiseerd zijn in computers en hardware uitlezen. Daar zitten gelukkig ook mensen bij die verstand hebben van netwerkverkeer, waarop ook nog wel eens wordt teruggegrepen. Maar dan nog blijven het te weinig mensen om daar het maximale rendement uit te halen.'* – politie

> *'Je moet niet in je eigen wereld blijven denken, want de generatie achter ons, de 14- en 15-jarigen hebben geen geld, maar wel altijd internet en weten precies te vinden waar gratis in te loggen.'* – aanbieder

5.3.3 Overwegingen en doelstellingen

Historische internetgegevens kunnen, via de ULI van de Landelijke Eenheid, worden opgevraagd bij een aanbieder. Historische gegevens over internetverkeer worden veelal opgevraagd naar aanleiding van een misdrijf of delict dat met behulp van of via het internet is gepleegd. Dit kunnen zaken betreffen zoals het versturen van dreigmails, internetoplichting, mensenhandel of het verspreiden van kinderporno. Maar de beslissing over het eventueel aansluiten van een internettap kan ook een aanleiding zijn om verkeersgegevens betreffende internet- of e-mailverkeer op te vragen. Dit om vooraf te onderzoeken of het desbetreffende internetadres of de mailbox wel gebruikt wordt. Professionals en experts die bekend zijn met het werken met internetverkeersgegevens, noemen het *identificeren van een gebruiker* of van een aansluiting als belangrijkste reden voor het opvragen van gegevens. Wanneer een internetadres wordt bezocht, kan het voorkomen dat opsporingsdiensten willen weten wie er achter een bepaald IP-adres schuilgaat. Zo noemt een expert een voorbeeld van een fraude zaak met kinderopvangtoeslagen. In dit geval heeft men het IP-adres van een bepaalde bezoeker van de Belastingdienst achterhaald. Door de gebruiker van dit IP-adres te identificeren, kon de verdachte worden geïdentificeerd en worden aangehouden. Ook bij fraude op internet wordt regelmatig gebruikgemaakt van internetverkeersgegevens, waarbij het identificeren van de gebruiker en het tijdstip waarop een site wordt bezocht als belangrijke informatie wordt genoemd.
Een andere expert noemt een mensenhandelzaak, waarbij een vaste computer thuis gebruikt werd bij de criminele activiteiten. Een ander voorbeeld vormt een grote kindermisbruikzaak waarbij de verdachten technieken gebruikten waarmee ze anoniem contact konden hebben met andere pedofielen. Ook in dit geval konden internetverkeersgegevens met succes worden ingezet om een verdachte te kunnen identificeren. Dit was ondanks de door de verdachte gebruikte afschermingstechnieken mogelijk, doordat een verdachte een menselijke fout maakte en een keer vergat gebruik te maken van de dienst die zijn identiteit verhulde.
Het gaat in de opsporing meestal om een combinatie van gegevens, zoals datum- en tijdsgegevens, soms aangevuld met een gebruikt e-mailadres, waarmee een bezoek van een bepaald IP-adres aan de desbetreffende site kan worden aangetoond. De combinatie van gegevens vraagt om een slimme en doordachte analyse van de bewaarde gegevens, zodat deze kunnen dienen als ondersteunend bewijs. Na het lokaliseren van het IP-adres is het de taak van de opsporingsdiensten om de verdachte op te sporen die dit adres gebruikte. Dit kunnen natuurlijk ook personen zijn die niet op het desbetreffende adres woonachtig zijn, maar wel gebruikmaken van het IP-adres door op het wifi-netwerk in te loggen of door als bezoeker gebruik te maken van het desbetreffende IP-adres. Dit kan overigens ook gebeuren buiten medeweten van de eigenaar van een IP-adres. Zo vertelde een professional over een

zaak waarin sprake was van misbruik van een IP-adres, doordat de verdachte op het slecht beveiligde netwerk van de eigenaar van dit IP-adres kon inloggen.
De hiervoor beschreven opsporingsonderzoeken, die allemaal gericht waren op het identificeren van een verdachte achter een IP adres, hebben één ding met elkaar gemeen. In alle gevallen ging het om het achterhalen van gebruiks- en verkeersgegevens afkomstig van een *vast* IP-adres. Deze IP-adressen zijn doorgaans voor langere tijd hetzelfde en daarnaast is voor een internetverbinding thuis een abonnement bij een aanbieder vereist. De gebruiker van de aansluiting van een vast IP-adres is in dat geval bekend en eenvoudig te traceren bij de aanbieder of bij het CIOT, dit in tegenstelling tot mobiel internet.

5.3.4 Mobiel internet

Uit de gesprekken komt naar voren dat het identificeren van een gebruiker van mobiel internet door middel van historische verkeersgegevens moeizaam verloopt en regelmatig niet mogelijk is. In tegenstelling tot een vaste internetverbinding, waarbij IP-adressen voor een langere tijd aan een gebruiker wordt gekoppeld, zijn de IP-adressen van mobiel internet dynamisch. Dit wil zeggen dat de internetadressen vaak wisselen. Ook worden door de schaarste aan Ipv4-adressen meerdere gebruikers onder één IP-adres geschaard, wat het identificeren van de individuele gebruiker onmogelijk maakt. Daarnaast maken veel gebruikers van mobiel internet regelmatig gebruik van wifi-netwerken of hotspots. Deze netwerken worden op steeds meer plaatsen aangeboden en zijn ook vaak gratis. Deze hotspots zijn echter niet altijd openbaar, omdat ze vaak enkel toegankelijk zijn voor klanten van de aanbieder van de hotspot. Niet-openbare wifi-netwerken vallen buiten de Wet bewaarplicht. Echter, wanneer een toestel is ingelogd op een wifi-netwerk, communiceert het op internet via hetzelfde IP-adres als alle andere medegebruikers van dat netwerk. Het is dan niet mogelijk om een individu op basis van alleen het gebruikte IP-adres te identificeren aan de hand van de internetverkeersgegevens.

> *'Voor dynamische IP-adressen is het natuurlijk heel lastig en zeker met het mobiele internetverkeer als er veel gebruikgemaakt wordt van hotspots.'* – OvJ

> *'Ja, met mobiel internet hebben we problemen. Het maakt het niet makkelijker. In een aantal gevallen lukt het wel, maar lang niet altijd.'* – politie

> *'Bij wifi kun je er niet achter komen en de telefoons zelf maken gebruik van variabele IP-adressen. Dus dat schiet ook niet erg op. Meestal wordt er verbinding gelegd met de provider en de provider gaat dan het internet op.*

Dan krijg je bijvoorbeeld een IP-adres van KPN op locatie in Den Haag, om maar wat te noemen. Dus dat schiet niet op.' – politie

Echter, een andere expert geeft aan dat wanneer de verkeersgegevens laten zien dat het IP-adres een tenaamstelling aangeeft van bijvoorbeeld een 'KPN Hotspot bv', het daarbij niet hoeft te stoppen.

Wij weten dan dat we geen directe koppeling hebben, maar dan weten we dawel van daaruit dat we een bevraging moeten doen aan [de aanbieder]; "Kunnen jullie ons vertellen welke IP-adressen of MAC-adressen in dat tijdvak contact hebben gehad op dat hotspot? […] Rechercheurs weten niet dat ze kunnen doorvragen. Dus ze stoppen bij het eerste station, maar weten vervolgens niet dat er ook nog een tweede station is, en dat ze wel even een belletje moeten plegen om dat maatwerk te krijgen, want dan gaat het om maatwerk.' – OvJ

Hierbij dient te worden opgemerkt dat de gegevens van de individuele gebruikers die op een hot spot ingelogd hebben, niet vallen onder de bewaarplicht.
De professionals van de politie geven aan dat historische internetgegevens van mobiel internet ook wel worden opgevraagd om over locatiegegevens van een mobiele telefoon te kunnen beschikken. Wanneer er met een smartphone contact wordt gemaakt met het internet, komt in de verkeersgegevens te staan met welke paal of mast dat contact geweest is. Zodoende is de locatie van het toestel redelijk accuraat vast te stellen. Ook wanneer iemand de telefoon niet gebruikt om te bellen maar enkel communiceert via het internet en daarvoor contact maakt met het netwerk, worden locatiegegevens gecreëerd. Echter, door onderliggende technische redenen worden deze gegevens door de professionals iets minder betrouwbaar genoemd dan locatiegegevens van telecommunicatie.

'Een histo van een internetsessie van een smartphone die zijn qua inhoud waardeloos, omdat je alleen maar ziet dat er een IP-sessie was tussen een telefoon en een provider, maar wat daar achter gebeurt zie je niet. Maar het locatiedetail, en dat is, opsporingtechnisch gezien al heel belangrijk, waar iemand was, dat komt wel mee in de histo.' – politie

Mobiel internet is ook prepaid mogelijk. In dat geval heeft de aanbieder geen gegevens over de gebruiker. Bij het opsporen binnen deze groep lijkt de meest dringende vraag, het identificeren van een gebruiker van een IP-adres, niet te beantwoorden. Uiteraard is het wel mogelijk om achteraf, wanneer een telefoon met prepaid internet in beslag wordt genomen of wordt aangetroffen bij een slachtoffer, de verkeersgegevens van de desbetreffende telefoon op te vragen.

5.3.5 E-mail

Ook gegevens betreffende de verzender en ontvanger van e-mailverkeer worden bewaard in het kader van de Wet bewaarplicht. Maar geen van de professionals en experts die is gesproken voor dit onderzoek geeft aan hier gebruik van te maken om te achterhalen wie met wie contact heeft. De enkele keer dat het wordt opgevraagd, gebeurt dit om te achterhalen of de mailbox wordt gebruikt. Als blijkt dat de mailbox wel gebruikt wordt, geven de professionals aan zo nodig een zogenaamde mailboxdump te vorderen bij de Nederlandse aanbieder waarbij de gegevens over het mailverkeer worden gevorderd. Dit betreft dan de inhoud van de mail wat niet onder de Wet bewaarplicht valt.

> *'Heel af en toe gebeurt het dat een team kijkt in het CIOT en die zien dan daar een e-mailadres staan bij een Planet klant bijvoorbeeld. […] Het enige dat je dan wilt weten is of deze mailbox actief is, of die wordt benaderd of niet. Een ja/nee-vraag aan de provider zou al voldoende zijn om te besluiten om wel of niet een tap te gaan zetten. Maar in de praktijk komt men niet zover omdat blijkt dat het niet gebruikt wordt.'* – politie

> *'… mijn ervaring is dat als jouw verdachte niet ouder is dan een jaar of 55, de kans heel klein is dat ie dat Nederlandse e-mailadres gebruikt.'* – politie

> *'Bij het vorderen van computers, dan hebben wij volledige mailboxen. En vaak jaren terug ook. Verkeersgegevens over mail daar hebben we weinig behoefte aan, want er staat in de kop en in de tekst waar het heen gaat en van wie het is. Verder niets.'* – FIOD

> *'Wanneer je te maken hebt met een slachtoffer en je wilt weten met wie die contact heeft gehad en je haalt iemand zijn e-mail die iemand thuis altijd gebruikt van [een Nederlandse kabel aanbieder] waar hij alles over doet, dan heeft het veel slagkracht. Maar dat zijn zeker niet de criminelen, want die weten dat ze dat niet moeten doen, maar een slachtoffer, een onschuldige burger. Die laat zoveel van zijn persoonlijke dingen achter in dat e-mailverkeer, dat is enorm.* – aanbieder

5.3.6 De bruikbaarheid van de bewaarde gegevens

Of men gebruikmaakt van historische internetverkeersgegevens, is afhankelijk van de aard van het delict. Wanneer een delict iets met internet te maken heeft, worden internetverkeersgegevens opgevraagd. Dit lijkt logisch, maar verkeersgegevens betreffende telefonie worden in een heel uiteenlopend scala aan delicten ingezet en niet enkel wanneer een delict iets met telefonie te maken heeft. Dit terwijl een groot deel van de huidige communicatiestromen tegenwoordig via het internet verlopen. Volgens verschillende experts

komt dit doordat van de internetgegevens die bewaard dienen te worden slechts een klein deel bruikbaar is voor de opsporing. Het merendeel van de gegevens betreffende internet, zoals beschreven in de bijlage behorende bij artikel 13.2a Tw, is volgens de experts verouderd. De regeling past niet meer bij het huidige internetgebruik en bij de technische ontwikkelingen die zich in dit opzicht hebben voorgedaan sinds de invoering van de wet in 2009. Een voorbeeld hiervan is het bewaren van log-in- en log-off-gegevens van internet- en e-mailsessies. Dit was relevant in de tijd dat men nog zelf actief een modem aanzette om contact te maken met het internet. Maar inmiddels zijn de meeste mensen 24 uur per dag, 7 dagen in de week verbonden met het internet via bijvoorbeeld wifi-netwerken en is er alleen sprake van een log-in of log-off wanneer het apparaat wordt uitgeschakeld. Met het veranderende aanbod van internetdiensten en als gevolg daarvan het veranderende internetgedrag van mensen heeft de bewaarplicht voor internetgegevens een beperkte waarde gekregen voor de opsporing.

> *'De dataretentie richtlijn is van het begin van dit decennium en ziet eigenlijk heel erg toe op de situatie van de periode daaraan voorafgaand, dus gaat over inbellen en pop-mail, korte mailophaalsessies. Toen was e-mail ook heel belangrijk. Dus de gegevens die nu bewaard worden, zo'n tien jaar later, gaan eigenlijk over de situatie van eind jaren 90, begin 2000, en welke gegevens er toen waren en wat we toen dachten dat belangrijk zou zijn voor de opsporing.'* – politie

> *'De lijn van de bewaarplicht was natuurlijk dat we aanbieders verplichten om verkeersgegevens van communicatie te bewaren. En omdat niemand toen kon bedenken dat we met z'n allen gingen social media-en….daar dacht niemand nog aan. Mail was net in. En er werd gewoon nog heel veel gebeld.'* – politie

> *'Sms is onder jongelui op sterven na dood. Bellen, als je de cijfers van OPTA zneemt ook af. Het is niet voor niks dat Hi stickers uitbrengt met "Wie belt er nou nog?" Dat doen ze natuurlijk om internetabonnementen te promoten. Je ziet mensen eigenlijk alleen nog maar whatsappen, pingen en op Facebook zitten. Mail van KPN, dat gebruikt men nog amper. Je communicatiedienstverlening is verschoven naar aanbieders die zich op internet bevinden. Het is allemaal web-gebaseerd.'* – NFI

Nederlandse aanbieders van internetdiensten, zoals omschreven in de Telecommunicatiewet, dienen zich te houden aan de bewaarplicht zodat voor opsporingsdiensten verkeersgegevens beschikbaar zijn die behulpzaam zijn bij de opsporing. Maar wanneer een persoon gebruikmaakt van de veelgebruikte buitenlandse serviceaanbieders, zoals Gmail, Hotmail, Facebook, enzovoort, zijn er geen verkeersgegevens voorhanden omdat deze bedrijven

niet onder de Nederlandse bewaarplicht vallen. In het huidige internetlandschap hebben deze aanbieders een prominente rol gekregen waarin voor de Nederlandse aanbieders slechts een bescheiden plaats is overgebleven. Opvallend genoeg zijn er buitenlandse dienstenaanbieders die zich actief en nadrukkelijk op de Nederlandse gebruikersmarkt richten en daar grote commerciële belangen bij hebben. Maar door zich achter het buitenlandse moederbedrijf te verschuilen, ontlopen ze de bewaarplicht. Een probleem dat zich ook voordoet bij de aftapplicht. De Nederlandse bewaarplicht heeft grenzen, terwijl het internet die niet heeft.

> *'Google Nederland bv dat bestaat gewoon, maar die zeggen: "Nee, wij hebben dat [verkeersgegevens] niet, dan moet je naar de VS." Dat is natuurlijk een beetje vreemd.'* – politie

> *'(...) omdat die technische ontwikkelingen zo snel gaan, is de wet gewoon onvoldoende flexibel om daarmee om te gaan en missen we dus een groot deel van de informatie. […] Wat ik eigenlijk wil zeggen is: hoofdstuk 13 moet worden aangepast en daarna moet het begrip aanbieder worden aangepast.'* – politie

> *'(...) het is tegenwoordig allemaal webgebaseerd. Ik snap niet waarom de politiek, en dan hebben we het voornamelijk over Brussel, dat gewoon laat lopen. Daar, bij de online aanbieders in het buitenland, wordt, geld verdiend: advertenties, marketing, gegevens van gebruikers die boven water worden gehaald, maar op het moment dat wij maar een fractie van die gegevens willen gebruiken voor opsporing, dan begeven ze zich ineens achter de Amerikaanse grens en beroepen ze zich op een amendement uit de Amerikaanse grondwet.'* – NFI

De technische ontwikkelingen en diensten op internet staan ook nu niet stil. Wat op dit moment bruikbaar is voor de opsporing, kan over enige tijd, bijvoorbeeld na het invoeren van IPv6-adressen of andere technische wijzigingen en vernieuwingen, helemaal anders zijn. Daarnaast kunnen technische ontwikkelingen en vernieuwde toepassingen ook zorgen voor onduidelijkheid of tegenstrijdige regelgeving.

> *'Prepaid gegevens worden een jaar bewaard. Dat is een speciaal stukje wetgeving*[107] *dat er al was voor de dataretentiewetgeving. (…) Nu is discussie over prepaid wat betreft een kaartje voor je laptop. Dat is internet en dat wordt [volgens de Wet bewaarplicht] een halfjaar bewaard. Is internet prepaid dan een halfjaar of is internet prepaid dan een jaar bewaren? De memorie van toelichting van beide wetten spreken elkaar tegen. We hebben*

107 Artikel 13.4 lid 3 Tw. Hierin wordt beschreven dat zowel prepaid verkeers- als locatiegegevens voor een periode van een jaar bewaard dienen te worden. Dit geldt zowel voor telefonie als voor internetgegevens.

gezegd dat alles een jaar bewaard moet worden. Het is prepaid. Als wetgeving tegenstrijdig is, moet je als toezichthouder duidelijkheid geven.' – AT

'De toekomst vereist dat de regelgeving omtrent de bewaarplicht die ook flexibel genoeg is om aan te passen aan nieuwe ontwikkelingen.' – OvJ

'IPv6 dat straks geïntroduceerd wordt, dat heeft nog heel veel andere eigenschappen. Dat werkt iets anders dan IPv4. Ik denk dat deskundigen nog eens een keer goed moeten kijken [naar de bewaarplicht] van hoe zou je dat bewaard willen hebben. Wat wel en wat niet.' – NFI

Een ander probleem voor de opsporing waar experts de onderzoekers op wijzen, is het groeiend tekort aan IP-adressen. De IP-adressen die nu gebruikt worden, zijn doorgaans IPv4-adressen. Al jaren is bekend dat deze IP-adressen opraken en er gezocht moet worden naar een alternatief. Dit werd gevonden in IPv6-adressen. Naast een aantal andere voordelen is het IPv6-adres langer en zijn er daardoor veel meer adressen mogelijk.
Langzaamaan worden steeds meer netwerkapparaten geschikt gemaakt voor IPv6, maar het is niet aannemelijk dat een volledige overstap binnen afzienbare tijd mogelijk is. Omdat diensten op het internet die alleen IPv4 ondersteunen vereisen dat de gebruiker ook een IPv4-adres heeft, is het voor de gebruiker onwenselijk dat hij alleen een IPv6- adres zou kunnen gebruiken. Nu IPv4-adressen schaars worden, zal een aanbieder geneigd zijn zuinig met IP-adressen om te gaan. Dat kan door meerdere klanten gebundeld (via Network Address Translation) een IP-adres te laten delen of door IP-adressen slechts voor heel korte tijd aan de gebruiker toe te kennen.
Wanneer een internetaanbieder een groep abonnees gebruik laat maken van een enkel extern IP-adres, is het niet meer mogelijk om aan de hand van dat IP-adres te achterhalen waar vandaan bepaalde informatie is verzonden. Een CIOT-bevraging zal in zo'n geval meerdere hits opleveren. Maar wanneer aanbieders problemen hebben met het koppelen tussen de gebruiker en IP-adressen, dan zal een CIOT-bevraging geen hit opleveren. Ook als een IP-adres in combinatie met een tijdstip niet langer uniek is voor een specifieke abonnee, kan alleen vergaande vastlegging van gegevens en bevragingen van deze gegevens een indicatie geven welke abonnee verantwoordelijk is voor een bepaald bericht. Internetaanbieders zijn echter niet verplicht om logs bij te houden van de computers waarmee de abonnee op enig moment contact legde. Daarbij is de omvang van het internetverkeer te groot voor zulke nauwkeurige vastlegging van gegevens. Ook zijn aanbieders niet verplicht om andere unieke verbindende kenmerken van het internetverkeer vast te leggen, zoals aan het IP-adres gerelateerde poortadressen. De verwachting is daarom dat enkel een IP-adres de opsporingsdiensten steeds vaker naar een (grote) groep abonnees leidt, waaruit de opsporingsdiensten de juiste gebruiker dienen te identificeren.

5.3.7 CIOT-bevraging van IP-adressen

De gegevens van het CIOT worden eenmaal per 24 uur ververst en de database beschikt daarom niet over gegevens die ouder zijn. IP-adressen worden echter regelmatig opnieuw uitgegeven. Zeker bij mobiel internet kan het gebruikte IP-adres meerdere malen per dag wisselen. Maar ook wanneer het een vaste thuiscomputer is, kan het voorkomen dat het IP-adres wisselt. Een CIOT-bevraging kan in dat geval dus onbetrouwbare informatie geven. Bij het opvragen van een IP-adres is het tijdstip waarop dit adres actief was dus van essentieel belang om de juiste gegevens in de systemen terug te kunnen vinden. In de praktijk worden hier volgens geïnterviewde experts wel eens vergissingen mee gemaakt.

> *'Het CIOT wordt het meest bevraagd, maar voor IP-adressen heeft dat niet zoveel zin omdat die adressen vaak wisselend zijn, dus dan moet je toch een bevraging doen bij de provider. Maar dat is best een klus. Dat is niet iets dat je geautomatiseerd in grote hoeveelheden doet.'* – politie

> *'Ik ben bang dat er nog steeds heel veel IP-adresbevragingen naar het CIOT toegaan. Wat nu de tenaamstelling van het IP-adres is, is niet gelijk aan de tenaamstelling van het IP-adres van drie weken geleden. En daarvoor moet je er eigenlijk iets meer van af weten. Dus daar kunnen fouten in sluipen.'* – politie

> *'(...) die fout, dat men de actuele database gaat bekijken, is een aantal keren gemaakt. Dan kun je dus tot andere uitkomsten komen. Het is op zich niet ingewikkeld alleen moet je heel zorgvuldig zijn. De snelste bak is natuurlijk die CIOT-bak. Maar dat kan dus tot foute informatie leiden.'* – aanbieder

5.3.8 De bewaartermijn

Uit de voorgaande paragrafen blijkt dat internetverkeergegevens niet veel worden gebruikt. Dit is enerzijds te wijten aan de veroudering van de regelgeving waardoor de bruikbaarheid van de gegevens sterk is afgenomen, anderzijds ligt dat aan een kennistekort. Desondanks geven de professionals en experts die optreden in opsporingszaken waarbij internetgegevens worden ingezet unaniem aan de bewaartermijn van zes maanden als (te) kort te ervaren. Het betreft dan voornamelijk de gegevens die het identificeren van een gebruiker van een IP-adres mogelijk maken.

> *'(...) je werkt altijd in het verleden. Zo'n onderzoek komt ineens boven en je werkt dan meestal niet in de actualiteit en als je dan maar een halfjaar hebt, is dat heel krap.'* – FIOD

(...) hoe zwaarder de criminaliteit, hoe langer het onderzoek en hoe sneller je isituatie terecht zult komen dat je ook gegevens van langer dan zes maanden zult willen bevragen.' – OvJ

'Op het moment dat ik nu iemand oppak, de gegevens die hij nu heeft zijn actueel en dan lijkt een halfjaar heel erg lang. Maar mensen bewaren soms hun halve leven in de computer en dat betekent dat je voor heel veel gegevens toch achter het net vist.' – politie

Een paar geïnterviewde professionals en experts geven voorbeelden van onderzoeken, waarin het niet beschikbaar hebben van historische internetgegevens nadelig uitpakte. Zo vertelt een professional van de FIOD dat belastingaangiften altijd aan het eind van het (belasting)jaar worden gedaan en dat de FIOD bij eventuele fraude dit pas na de aangifte opmerken. Zo kwam bij de FIOD een zaak aan het licht betreffende fraude met kinderopvangtoeslag. Dit is een persoonsgebonden toeslag die enkel voor eigen kinderen opgevraagd kan worden. Een aanvraag kon worden ingediend via het internet. De FIOD constateerde tijdens het onderzoek dat er onder valse identiteiten over een klein aantal IP-adressen voor een onwaarschijnlijk aantal kinderen opvangtoeslag werd gevraagd. Tot zes maanden na signalering kon men de gebruikte IP-adressen achterhalen. Echter, sommige aanvragen waren eerder gedaan en daarvan konden de historische internetverkeersgegevens niet meer worden opgevraagd voor een tenaamstelling. Ook andere experts noemen voorbeelden van zaken waarin ze hinder ondervonden van de bewaartermijn van zes maanden:

'… Wij hebben een onderzoek gedaan naar de logs die op de computer stonden die gesprekken bevatten [betreffende kinderporno] en dat waren een heleboel logs, over meerdere jaren waren deze opgeslagen. De verdachte werd aangehouden in december. Ik denk tegen de tijd dat wij de data in het systeem hadden zitten zodat het analyseerbaar was geworden, was het ongeveer maart. [..] Op het moment dat het maart is en dat je dan een bewaarverplichting hebt voor zes maanden, kun je nog maar terug in de tijd tot oktober. Twee maanden hadden we maximaal de tijd om nog van de allerlaatste logs de IP-adressen te kunnen bevragen die zouden kunnen leiden naar een klant.' – politie

'Ik vind dat de bewaarverplichting onevenwichtig is omdat nu een heleboel gegevens worden bewaard die nooit bevraagd worden. Terwijl het enige wat wel veel bevraagd wordt, die IP-adressen, eigenlijk te kort beschikbaar zijn.' – NFI

Ook professionals die werkzaam zijn bij teams die werken aan langer lopende grote zaken, zoals liquidaties of georganiseerde misdaad, zouden graag zien

dat de termijn weer gelijkgesteld wordt aan die van telefoniegegevens. Daarnaast merken verschillende respondenten op dat verkeersgegevens die afkomstig zijn van een smartphone feitelijk niet los te koppelen zijn van het internet.

> *'Het is eigenlijk niet te splitsen, want de gegevens die voor de mobiele telefoon gelden, kun je eigenlijk niet los zien van het internet. Als een smartphone negen maanden geleden verbinding heeft gemaakt met het internet, dan zou het feit dat die internetsessie heeft plaatsgevonden niet door de provider bewaard hoeven te worden, maar wat de provider wel moet bewaren, zijn de datum en tijd wanneer het apparaat gebruik heeft gemaakt van zijn netwerk, dat moet een aanbieder weer wel bewaren. Dan krijg je natuurlijk direct de vraag van ons "negen maanden geleden heeft die smartphone iets gedaan en dat heeft een half uur geduurd en dat is gegaan vanaf die en die antenne et cetera" Dat werkt gelukkig niet zo, want die aanbieder zegt alleen dat het een IP-sessie was. Hoe die IP-sessie verlopen is, met welk locatiepunt, met welke dienst of met welk IP-adres dat kan die provider niet meer leveren.'* – politie

5.3.9 Rechtshulpverzoeken

Wanneer opsporingsdiensten willen beschikken over verkeers- en locatiegegevens van niet-Nederlandse personen of van communicatiediensten die door een niet-Nederlands bedrijf geleverd worden, kan men besluiten een rechtshulpverzoek in te dienen. Zoals al eerder opgemerkt geven de geïnterviewden aan dit niet snel te doen, omdat het langer duurt voordat men over de gegevens kan beschikken. Hoe lang dit gemiddeld duurt, kan volgens de geïnterviewde professionals verschillen. Soms worden de contacten die een team in het buitenland heeft gebruikt om de gegevens alvast te bevriezen om te voorkomen dat deze verloren gaan door de vertraging die een rechtshulpverzoek met zich mee kan brengen. Een telefoontje naar een bevriend team gaat dan vooruit op de formaliteiten van het internationale hulpverzoek. Internationale samenwerking blijkt onmisbaar omdat de Telecommunicatiewet stopt bij de Nederlandse grens.
Een expert gespecialiseerd in het bestrijden van internetcriminaliteit, geeft aan dat zijn team weinig gebruikmaakt van de gegevens die in eigen land zijn opgeslagen. Dit heeft niet te maken met een tekort aan kennis betreffende internetverkeersgegevens maar alles met de manier van werken en ook met de nationaliteit van de verdachte, als die al te identificeren valt. Deze expert geeft aan dat in de zaken waarbij men wel wil beschikken over verkeersgegevens, deze doorgaans worden opgevraagd in het buitenland. Hierin is men dus afhankelijk van de wijze waarop de bewaarplicht in andere landen is geregeld en uitgevoerd, waardoor men van tevoren niet weet welke gegevens geleverd kunnen worden.

'Voor eigen onderzoek met nationale verdachten is het vanwege onze grootte ook maar heel weinig aan de orde dat wij van één van die vier à vijf verdachten in Nederland een keer specifiek de gegevens moeten bevragen die voldoen aan die bewaartermijn, maar andersom doen wij regelmatig verzoeken aan het buitenland over wie op een bepaald moment de gebruiker of de eigenaar van dat IP-adres was. Dat gebeurt regelmatig en andersom ook.' – politie

'(...) het is jammer dat je niet een zelfde lijn hebt in Europa. Dat is wel een beetje een gemis [...] nu lijkt het alsof landen onderling er niet helemaal hetzelfde over denken; dat is jammer.' – OvJ

'Vaak zetten wij zaken door naar het buitenland, zodat ze [de zaak] daar zelf afhandelen. In Duitsland loop je er bijvoorbeeld tegenaan dat er nauwelijks een bewaarplicht is. Wat je nu hebt, heb je, maar als het niet in de computer zit, ben je het bij voorbaat al kwijt. Voor nu en de nieuwe kinderporno-organisatie, dat zijn elf teams in het land met 150 mensen, is het gewoon een heel belangrijk item [het identificeren van een gebruiker achter een IP-adres] om hier iets mee te kunnen'. – politie

Wanneer verkeersgegevens noodzakelijk zijn van internetdiensten die geleverd worden door buitenlandse partijen, zoals Google, Facebook, Microsoft en Apple, dan zijn deze voor opsporingsdiensten in Nederland alleen op te vragen met een internationaal rechtshulpverzoek. De diensten die deze bedrijven leveren vallen niet onder hoofdstuk 13 Tw, omdat het moederbedrijf in het buitenland gevestigd is. Tijdens de gesprekken met de professionals en experts kwam regelmatig ter sprake dat men het idee had informatie te missen betreffende veelgebruikte diensten op internet als Hotmail, Gmail, WhatsApp, Skype, Live Messenger, enzovoort. Er zijn geen Nederlandse cijfers bekend over de aantallen internationale bevragingen betreffende socialemediadiensten. Echter, de politie Limburg-Zuid heeft in het verleden, als gehoor op een WOB-verzoek van BoF, een lijst met bevragingen bij Hyves, Hotmail en Live Messenger van Microsoft openbaar gemaakt.[108] Over het jaar 2011 betrof dit 33 verzoeken bij Hotmail en Live Messenger en 6 verzoeken om informatie bij Hyves. Dit laatste bedrijf is overigens een internetdienst geleverd door een Nederlands bedrijf.
Op internet is ook het aantal bevragingen gepubliceerd dat gedaan is bij het bedrijf Google.[109] De diensten die dit bedrijf levert, zijn onder andere Gmail, Google Groups, Google Talk, Google Voice, enzovoort. Het bedrijf behandelt bevragingen in het kader van een strafrechtelijk onderzoek en controleert daarbij of is voldaan aan een aantal voorwaarden. Zo dienen de verzoeken in

108 www.bof.nl/live/wp-content/uploads/20120217-bevragingen-sociale-netwerken.pdf (geraadpleegd op 19 maart 2013).
109 www.google.com/transparencyreport/userdatarequests/NL/ (geraadpleegd op 19maart 2013).

overeenstemming te zijn met de letter en de geest van de wet.[110] Hieruit is op te maken dat over de tweede helft van 2012 59 verzoeken om gegevens uit Nederland bij het bedrijf zijn binnengekomen. Hiervan is 76% beantwoord. Of deze antwoorden compleet zijn, wie de aanvrager was en met welke redenen of op welke rechtsgronden de verzoeken zijn gedaan, wordt niet vermeld. Ook Microsoft heeft informatie openbaar gemaakt betreffende het aantal verzoeken in 2012 van opsporingsdiensten om informatie.[111] De online diensten die dit bedrijf levert, zijn onder andere Hotmail, Outlook.com, Skydrive, Xboxlive en Skype. Het bedrijf ontving in totaal 859 verzoeken van Nederlandse opsporingsdiensten die betrekking hadden op 1.438 accounts en/of gebruikers. In geen van de bevragingen werd de inhoud van de communicatie vrijgegeven. Wel werden in 78,1% verkeersgegevens geleverd aan de opsporingsdienst. In 21,9% van de gevallen werden geen data gevonden of werd het verzoek afgewezen, omdat niet aan de juridische eisen was voldaan. Skype ontving twee verzoeken van Nederlandse opsporingsdiensten, die betrekking hadden op twee gebruikers. Informatie werd ook hier niet geleverd. Het aantal malen dat Nederlandse opsporingsdiensten in de tweede helft van 2012 informatie opgevraagd hebben bij Twitter, is minder dan tien keer.[112]
Wat opvalt in deze openbaar gemaakte aantallen bevragingen bij de hiervoor genoemde buitenlandse aanbieders van internetdiensten, is dat het aantal bevragingen dat afkomstig is uit Nederland in vergelijking met de landen om ons heen zeer bescheiden te noemen is. Duitsland, Frankrijk en het Verenigd Koninkrijk dienen een veelvoud van het aantal Nederlandse bevragingen in.

5.3.10 De toekomst van de bewaarplicht internetgegevens

Het internet heeft een steeds groter aandeel gekregen in de communicatiestromen van mensen en dit aandeel neemt nog steeds toe. Uit het voorgaande wordt duidelijk dat de internetverkeersgegevens die bewaard worden in het kader van de dataretentiewetgeving, voor de opsporing slechts van beperkte waarde zijn. Een reden hiervoor is het feit dat de techniek, het gedrag van mensen en de wet niet meer op elkaar aansluiten. De vraag is echter welke gegevens dan wel bewaard moeten worden om de opsporing van dienst te zijn en of dit haalbaar en wenselijk is. Het bewaren van meer gegevens lijkt een logische stap, maar hoeft niet de gewenste oplossing te bieden. Het betreft een complex vraagstuk, waarvoor een zorgvuldige overweging door experts is gewenst.

> *'Een belangrijke discussie bij de totstandkoming van de richtlijn was natuurlijk bij telefonie bijlage A. Daarbij gaat het om de uiterlijke kenmer-*

110 www.google.com/transparencyreport/userdatarequests/legalprocess/ (geraadpleegd op 13 maart 2013).
111 http://blogs.technet.com/b/microsoft_on_the_issues/archive/2013/03/21/microsoft-releases-2012-law-enforcement-requests-report.aspx (geraadpleegd op 25 maart 2013).
112 https://transparency.twitter.com/information-requests-ttr2 (geraadpleegd op 25 maart 2013).

ken van het verkeer: wanneer belt welk nummer met welk nummer, hoe lang en vanaf welke plek. Bij internet is dat veel meer verweven met elkaar. Het is moeilijk de inhoud van de boodschap te scheiden van de uiterlijke kenmerken. Vaak zit in al die lagen van het internetprotocol en je moet algauw de onderste laag hebben om er wat aan te hebben. Daarbij wordt inhoud van de communicatie ook ineens deel van wat je zou moeten bewaren en dat is natuurlijk een hele verre stap verder. Opslag van een jaar internetverkeer, dat zou qua opslagcapaciteit exceptioneel zijn, maar ten tweede is dat dan de ultieme Big Brother.' – aanbieder

'(...) een WiFi-punt bij de Albert Heijn die heeft een bepaald IP-adres toegekend, dan moeten wij dus [aanbieder] die relatie van A naar B naar C vasthouden. Om dat te kunnen demonstreren, moet dat in de tijd specifiek zijn, bewijsbaar juist. Je moet voor de rechtbank aantonen dat het een correcte vastlegging is. [...] Dan moeten we echt de hele communicatie gaan vastleggen. Veel meer vastleggen dan we nu doen.' – aanbieder

5.4 Het opvragen van zendmastgegevens

De data die bewaard worden in het kader van de bewaarplicht kunnen op verschillende manieren opgevraagd en doorzocht worden. Naast het opvragen van historische gegevens van het telefoon- en internetverkeer van individuele nummers, IP-adressen of toestellen, kunnen ook verkeersgegevens op een bepaalde locatie worden opgevraagd. Bij de verkeersgegevens van zowel telefonie als internet wordt de locatie van de aanvang van de connectie bewaard, de zogenoemde *First Cell ID*. Deze gegevens verwijzen naar een zendmast van waaruit de aanvang van de connectie is verlopen. Dat wil zeggen dat wanneer een groep mensen via dezelfde zendmast een telefoongesprek begint, alle personen, naast hun individuele telefoonnummer, identieke locatiegegevens (*First Cell ID*) in hun verkeersgegevens hebben die verwijzen naar de desbetreffende zendmast.
Een zoekvraag op een bepaalde locatie wordt zodanig opgesteld dat in een database alle communicatie via zendmast X op tijdstip Y wordt geselecteerd. Het opvragen van verkeersgegevens op basis van een locatie levert gegevens op van alle mobiele telefoons die in het opgevraagde tijdsbestek zijn gebeld, zelf hebben getelefoneerd of connectie hebben gehad met het internet via de bevraagde mastlocatie. De eisen die aan het opvragen van gegevens betreffende een zendmastlocatie worden gesteld zijn: er moet sprake zijn van een verdenking van een misdrijf zoals omschreven in artikel 67, lid 1 Sv. en het moet in het belang zijn van het onderzoek.
Naast de wettelijke eisen die zijn gesteld aan het opvragen van verkeersgegevens op basis van een zendmastlocatie, zijn er ook vanuit de ULI afspraken gemaakt met aanbieders. Zo mag een maximumaantal zendmastlocaties per

vordering worden opgevraagd en is er een maximumperiode gesteld van drie uur per zendmastlocatie.

5.4.1 In de praktijk

Door het opvragen van gegevens betreffende een zendmastlocatie is het mogelijk om het telecommunicatieverkeer binnen een bepaald gebied voor de opsporing inzichtelijk te maken. De kans dat het opvragen van een locatie waarop een zendmast staat iets oplevert, is het grootst op het moment dat er een specifieke aanleiding is dat er is gecommuniceerd met de telefoon van de verdachte op de plaats delict. De verkeersgegevens die gecreëerd worden met communicatie vallen onder de bewaarplicht en zijn daarmee voor een bepaalde tijd op te vragen door de opsporingsdiensten.
Mobiele telefoons maken regelmatig contact met het netwerk, ook wanneer er geen telefoongesprek of dataverkeer plaatsvindt. Deze gegevens vallen niet onder de bewaarplicht en zijn slechts voor een aantal uur aanwezig, voordat ze worden overschreven. Ze kunnen door opsporingsdiensten gevorderd worden op basis van 126ng/ug jo. 126nd/ud en 126ne/ue Sv. Om dit overschrijven te voorkomen, dienen de gegevens eerst te worden 'bevroren', waarna ze kunnen worden gevorderd. Echter, volgens een expert zijn niet alle aanbieders in staat de vluchtige gegevens zeker te stellen door het uitvoeren van een zogenaamde Freeze.
In welke gevallen wil een opsporingsteam gegevens over een zendmast opvragen? En hoe gaat dit in zijn werk? Hierna zetten we een aantal voorbeelden uiteen.
Er is een moord gepleegd op een bepaalde locatie. De dader is onbekend. Een mogelijke opsporingshandeling is het nagaan of de dader zijn telefoon bij zich had en of deze telefoon contact heeft gehad met een zendmast in de omgeving van de plaats delict. Een telecommunicatiespecialist van de politie komt hiervoor metingen verrichten. Deze specialist gaat samen met een rechercheur uit het betrokken onderzoek naar de plaats delict, waarbij de vermoedelijke route van de verdachte wordt afgelegd aan de hand van andere sporen of verklaringen van getuigen. Op die plaatsen – en op de plaats delict zelf uiteraard – wordt vervolgens de dekking van de zendmasten gemeten. De meeste zendmasten hebben drie antennes die elk een gebied van 120 graden bestrijken. Deze aanstralingsgebieden worden cellen genoemd.[113] Bij meerdere zendmasten binnen een bepaald gebied kan enige overlap ontstaan. Toch zal een zendmast dominant zijn in een cel en dat hoeft niet de dichtstbijzijnde te zijn. Mobiele toestellen zullen contact zoeken met de dominante zendmast om communicatie mogelijk te maken. Goede metingen van een telecommunicatiespecialist zijn daarom nodig om te bepalen welke mastlocatie bevraagd moeten gaan worden en om de tijdstippen te bepalen

113 Zie voor meer uitleg: https://rejo.zenger.nl/focus/locatie-te-achterhalen-uit-call-detail-records/ (geraadpleegd op 1 mei 2013).

waarop naar relevante gegevens moet worden gezocht. Het opvragen van de gegevens van een locatie levert telefoonnummers en IMEI-nummers op die via die bepaalde zendmast is verlopen, welke vervolgens bijvoorbeeld weer opgevraagd kunnen worden bij het CIOT. Dan gaat het opsporingsteam bekijken of daar bekenden van de politie tussen zitten, zoals zedenklanten, recidivisten, bekende telefoonnummers, enzovoort. Deze werkwijze heeft echter niet de voorkeur vanwege de hoeveelheid werk die hiermee gemoeid is en wordt daarom alleen gedaan wanneer elk ander spoor doodloopt.
Een andere werkwijze om de identiteit van een verdachte te achterhalen, is het vergelijken van gegevens die afkomstig zijn van zendmasten op verschillende locaties. Als het vermoeden rijst dat er sprake is van twee of meer plaatsen delict, van een bepaalde route naar de plaats delict, van een verdachte die op verschillende momenten op verschillende plaatsen actief is geweest, zoals bij seriematige daders het geval is, kan men besluiten gegevens over meerdere locaties op te vragen om deze te vergelijken. Op dat moment gaat men een meting doen op de desbetreffende locaties en wordt de *best serving cell*, de cel die het sterkste bereik heeft op de desbetreffende locatie, van een zendmast opgevraagd. De gegevens afkomstig van de zendmasten op de verschillende locaties worden door een analyseprogramma vergeleken en de nummers of telefoons die dan vaker in de gegevensset te vinden zijn, worden eruit gelicht. Als op beide locaties eenzelfde telefoonnummer of IMEI-nummer wordt gevonden, kan dit de telefoon zijn van een mogelijke dader. Als voorbeeld noemt een geïnterviewde:

> *'Als hier iemand wordt doodgeschoten en een half uur rijden van hier wordt een auto die met de zaak in verband kan worden gebracht in brand gestoken, dan kun je de gegevens van die zendmasten vergelijken en bekijken of iemand op beide PD's is geweest. Wat een indicatie zou kunnen zijn dat iemand er iets mee te maken heeft.'* – politie

Ook kan later blijken dat bij twee verschillende voorvallen eenzelfde verdachte betrokken is geweest. Zo kan een overval op locatie X met een bepaalde modus operandi later vergeleken worden met een overval op locatie Y met dezelfde modus operandi, in de hoop dat er sprake is van eenzelfde verdachte. Als er aanleiding is dat er gebeld is, wordt een vergelijking gemaakt tussen de verkeersgegevens van de desbetreffende zendmasten op de locaties en dan wordt bekeken welke nummers overeenkomen. Tussen het opvragen van de verkeersgegevens op basis van een locatie van een mast en het vergelijken van de gegevensset afkomstig van meerdere locaties kan soms langere tijd zitten. Wanneer bijvoorbeeld met enige regelmaat sprake is van aangestoken branden, kunnen verkeersgegevens opgevraagd en bewaard worden. Dit om in de toekomst de eerder opgevraagde gegevens te kunnen vergelijken met die op de locatie van de meest recente brand. Belangrijk is dan wel dat de locaties ver genoeg van elkaar verwijderd zijn. Gebeurt dat

niet, dan zal een groot aantal mobiele telefoons van bijvoorbeeld de mensen die daar woonachtig zijn, uit de analyse naar boven komen. Maar ook kunnen mastgegevens in een later stadium van een onderzoek worden vergeleken met een mobiele telefoon die in beslag wordt genomen.

> *'Er heeft een kerel waarschijnlijk urenlang zijn slachtoffer op liggen wachten, waarna hij haar heeft aangerand en verkracht. Daar hebben we een meting gedaan. Later blijkt hij, in de vier uur dat hij daar in de bosjes heeft gelegen, toch een sms'je te hebben ontvangen en een internetverbinding heeft gehad. [...] Je kunt de mastgegevens bevragen, dan krijg je een enorme bulk data. [...] In dit geval was het zo dat we de verdachte later hebben aangehouden. Vervolgens is zijn gsm uitgelezen en zijn er historische verkeersgegevens opgevraagd waarin we een match zien tussen de cell-ID in de verkeersgegevens van de verdachte [locatie van de telefoon] en de door ons gemeten cell-ID's [locatie van de telefoonmast].'* – politie

Tijdens de gesprekken kwam naar voren dat met het opvragen van gegevens over een zendmastlocatie er als bijvangst soms getuigen achterhaald kunnen worden. Het kan voorkomen dat bijvoorbeeld meerdere getuigen tegelijkertijd 112 proberen te bellen. Slecht twee of drie personen krijgen dan contact met de centrale, terwijl andere getuigen dan de telefoon neerleggen, omdat ze in gaten krijgen dat anderen al aan het bellen zijn of omdat ze simpelweg geen contact krijgen. Voor de politie kunnen deze getuigen van groot belang zijn in het opsporingsonderzoek. Dit raakt volgens een geïnterviewde wel de rand van de wetgeving. Hij geeft het voorbeeld van het volgende incident:

> *'Hier in [plaatsnaam] hebben we een vervelende wijk, waar midden op straat, overdag, een Antilliaan uit zijn schoenen werd geschoten. Er was een hele volksoploop en mensen gaan 112 bellen. Bij de meldkamer hebben ze drie 112 bellers aan de lijn gehad. Dan ga je die masthisto's bevragen en dan blijkt dat er twaalf 112 bellers inzitten. Dan heb je die nummers en kun je ze gelijk bellen. (...) Het zijn wel belangrijke getuigen. Dat is een beetje het randje van de wet. Het is meestal bijvangst. (...)'* – politie

5.4.2 Privacy

Het opvragen van gegevens op basis van locaties van zendmasten is omstreden. Tegenstanders stellen dat het opvragen van een locatie de privacy schendt van grote groepen onschuldige burgers. Ook politiefunctionarissen zelf zien in dat de inbreuk groot kan zijn:

> *'Ik vind zelf dat met mastverkeersgegevens een zware privacyschending wordt gemaakt, omdat het 99,9% onverdachte mensen betreft. Niet zozeer dat artikel 126 over "verdachten" spreekt maar dat zijn mensen waar je*

eigenlijk totaal niks mee van doen hebt. Soms heb je een hele goede reden om het wel te doen, maar er zijn soms ook redenen waarvan je denkt, moet dat wel, kun je dat wel uitleggen, is het wel proportioneel?' – politie

Voorstanders daarentegen zeggen dat de inbreuk op de privacy wel meevalt. Het opvragen van gegevens op basis van de locatie van een zendmast is aan de vereisten van proportionaliteit en subsidiariteit verbonden. Er moet sprake zijn van een strafbaar feit waarvoor voorlopige hechtenis mogelijk is. Professionals uit de opsporingspraktijk die we hebben gesproken beseffen dat het een zwaar opsporingsmiddel is, waarvan ze juist willen voorkomen dat het standaard wordt ingezet. Tegenwoordig wordt veel bewuster omgegaan met dit soort zware opsporingsmiddelen en daarom is de afspraak gemaakt dat er over een maximale periode van drie uur gegevens kunnen worden opgevraagd. Daarbij geeft een geïnterviewde een voorbeeld dat een mastbevraging niet altijd nodig is:

'Soms stellen we alleen [op de plaats delict] vast welke antennes relevant zijn en verder niets. Dan worden er geen mast of verkeersgegevens gevorderd. Stel dat we een maand later tegen een verdachte en zijn telefoon aanlopen, dan vragen we historische verkeersgegevens op van zijn telefoon en kijken we of er een match is tussen de gemeten antennes en de antennes die in die historische verkeersgegevens voorkomen [locatiegegevens]. Zodat je zijn telefoon op een bepaald moment in de omgeving dan de plaats delict kunt brengen.' – politie

5.5 Alternatieven voor de bewaarplicht?

De geïnterviewde professionals en experts is gevraagd of zij alternatieven kunnen bedenken voor het werken met verkeersgegevens en de bewaarplicht. Zowel de professionals als de experts benadrukken dat de opsporing heel erg afhankelijk is van telecom. Er is in hun ogen niet echt een goed alternatief denkbaar. Wanneer men niet de beschikking zou hebben over verkeers- en locatiegegevens, zou men kunnen gaan tappen, maar dat maakt ten eerste een zwaardere inbreuk op de privacy en ten tweede kijk je daarmee in de toekomst en niet, zoals met historische verkeersgegevens, in het verleden. Een ander alternatief zou volgens verschillende geïnterviewden observeren kunnen zijn, maar dan moet het observatieteam wel weten waar het moet zijn, anders wordt er inefficiënt te werk gegaan. Een expert wijst erop dat als hij niet de verkeersgegevens voorhanden zou hebben, hij andere vormen van dataopslag of cameratoezichtsystemen zou raadplegen. Maar de conclusie blijft dat historische verkeersgegevens erg waardevol zijn en bovendien relatief onvervangbaar.

Als alternatief voor de bewaarplicht wordt het gericht bevriezen van gegevens genoemd. Bij bevriezen moet goed omschreven worden welke set gegevens bewaard moeten blijven voordat deze vernietigd worden. De gegevens worden ook niet direct aan de opsporingsdiensten overhandigd, maar pas als het onderzoek het vordert. Tegenstanders van de algehele bewaarplicht zien het gericht bevriezen van gegevens als een minder privacy schendende oplossing, omdat er in dat geval sprake is van een gerichte dataset die langer bewaard wordt in plaats van het bewaren van alle data van alle klanten van een aanbieder.
De onderzoekers hebben een aantal professionals en experts dit alternatief voorgelegd. Geen van deze geïnterviewde personen vindt het bevriezen van gegevens een vergelijkbaar en gelijkwaardig alternatief voor het opvragen van verkeersgegevens die voortkomen uit de bewaarplicht. Bij het bevriezen van data wordt al uitgegaan van een bewaartermijn en de huidige bewaarplicht heeft juist gezorgd voor harmonisatie van de bewaartermijnen bij de verschillende aanbieders.
Een ander voorbeeld van een situatie waarbij het bevriezen van gegevens niet werkt, is als een delict pas later bekend wordt. In de huidige situatie speelt dat nu al bij het bevriezen van vluchtige gegevens op een zendmast. Dergelijke gegevens zijn, zoals eerder is opgemerkt, maar enkele uren beschikbaar en kunnen dus alleen gevorderd worden als een delict snel ter kennis van de politie komt en als het snel duidelijk is waar dat delict is gepleegd. In andere situaties biedt het bevriezen van gegevens geen oplossing.

> *'Je kunt een aanbieder vragen om de vluchtige gegevens te bevriezen. Dat betekent dat er een foto wordt gemaakt van de gegevens van zo'n mast. Dat werkt dus ook alleen maar als je meteen op de hoogte bent van bijvoorbeeld een bepaald delict. Als je er nu achter komt dat er veertien dagen geleden iemand ergens is doodgeschoten, ja dan kun je bevriezen tot je en ons weegt maar dan is alles toch al weg.'* – politie

5.6 Samenvattend

In de opsporing houdt men nog erg vast aan de traditionele opsporingsmiddelen, zoals historische gegevens over telefoonverkeer. Deze gegevens worden zeer frequent in een breed scala van misdrijven ingezet. Uit de gesprekken met de geïnterviewde personen blijkt dat historische verkeers- en locatiegegevens veelvuldig en op hele diverse manieren worden ingezet in de opsporingspraktijk. De professionals uit de opsporingspraktijk zijn bekend met de werkwijze en vinden het een waardevol opsporingsinstrument. Een veelgenoemde reden om een beroep te doen op de bewaarplicht van telecommunicatiegegevens is het lokaliseren van personen. Door het opvragen van verkeersgegevens kan eenvoudig inzichtelijk worden gemaakt of en vanaf

welke locatie een telefoon is gebruikt en wat zowel voor belastend als ontlastend bewijs wordt gebruikt. Ook voor het inzichtelijk maken van contacten worden verkeersgegevens frequent ingezet. Het analyseren van verkeers- en locatiegegevens is volgens de geïnterviewde professionals en experts specialistenwerk. Echter, niet elk team heeft de beschikking over een analist die de werkzaamheden kan uitvoeren.
Bij het opvragen van mastgegevens wordt in de database met verkeers- en locatiegegevens gezocht op locatie. Hierdoor worden telefoonnummers geselecteerd die op een bepaald tijdstip, op een bepaalde locatie gebruikt zijn om te communiceren. Dit type bevragingen wordt vooral ingezet bij seriematige delicten om verschillende locaties met elkaar te kunnen vergelijken in de hoop dat een verdachte zijn telefoon heeft gebruikt.
Volgens de experts zijn de opgeslagen gegevens betreffende telefonie relevant, zoals deze worden beschreven in de bijlage behorende bij artikel 13.2a Tw. Men geeft aan wel informatie te missen die nu niet automatisch bij de opgevraagde verkeers- en locatiegegevens worden meegeleverd. Een voorbeeld hiervan is de eindlocatie van een gesprek. In de huidige situatie is enkel de startlocatie van een gesprek uit de opgevraagde gegevens op te maken. De bewaartermijn wordt door de professionals en experts uit de opsporingspraktijk in het algemeen als voldoende beschouwd. In sommige gevallen blijkt een jaar te kort om een onderzoek goed te kunnen uitvoeren, maar dit is eerder uitzondering dan regel.
Professionals en experts die regelmatig optreden in opsporingszaken waarbij het internet een rol speelt, zijn van mening dat de bewaarde internetverkeersgegevens slechts van beperkte waarde zijn bij het opsporen van deze zaken. De te bewaren gegevens, zoals de Telecommunicatiewet voorschrijft, passen niet meer bij de huidige techniek en het huidige internetgebruik. Hierdoor is een situatie ontstaan, waarbij gegevens van burgers worden opgeslagen en bewaard die volgens de professionals en experts niet of nauwelijks door de opsporingsdiensten worden opgevraagd.
In dit onderzoek komt ook naar voren dat de techniek achter internetverkeersgegevens complex is en het gebruik en de analyse van deze gegevens de nodige kennis vraagt. Deze kennis is volgens de geïnterviewde experts niet voldoende aanwezig, ondanks pogingen vanuit het OM en de politieorganisatie om dit tekort aan te vullen en te ondervangen.
De bewaartermijn van zes maanden wordt door geïnterviewden die optreden in opsporingszaken waarbij internetverkeersgegevens een rol kunnen spelen, unaniem als te kort ervaren. Dit betreft voornamelijk de identificerende gegevens van een gebruiker van een IP-adres.
Een zorgvuldige heroverweging van de regeling betreffende de te bewaren internetverkeersgegevens en de daarbij onlosmakelijk verbonden afweging betreffende de bewaartermijn is daarom wenselijk.

6 Het gebruik van historische verkeersgegevens in cijfers

6.1 Bevragingen bij de Unit Landelijke Interceptie

In de Telecommunicatiewet is een regel opgenomen over de verplichting tot publicatie van het jaarlijkse aantal bevragingen door opsporingsdiensten van gegevens over telecommunicatieverkeer (art. 13.4 lid 4 Tw). Ook in de Europese richtlijn wordt geschreven over een jaarlijkse publicatie van het aantal bevragingen (Directive 2006/24/EC, art. 10). Uit de Europese evaluatie bleek echter dat weinig lidstaten aan deze verplichting voldoen. In het geval er wel cijfers worden gepubliceerd, zijn het format en het type gegevens zo uiteenlopend dat de cijfers moeilijk kunnen worden vergeleken. Recentelijk heeft het *Platform for Electronic Data Retention for the Investigation, Detection and Prosecution of Serious Crime* een paper gepubliceerd voor de lidstaten dat kan dienen als leidraad bij het publiceren van de jaarlijkse cijfers.[114]
De Minister van Veiligheid en Justitie heeft in 2010 voor het eerst de aantallen vorderingen tot verstrekking van telecommunicatiegegevens bekendgemaakt. In de tweede helft van 2010 waren dit er 24.012. In het jaar 2011 zijn er 49.695 vorderingen ingediend. Het totaalaantal vorderingen in het jaar 2012 bedraagt 56.825. Dit is een stijging van 14,3% ten opzichte van 2011.
Bij deze cijfers dient te worden benadrukt dat het opvragen van telecomgegevens in Nederland wordt geregistreerd per telefoonnummer, IMEI-nummer, IP-adres of 'paallocatie', waarover gegevens worden opgevraagd.[115] Omdat mensen vaak meerdere telefoons gebruiken, geven deze cijfers geen inzicht in het aantal personen van wie er jaarlijks telecomgegevens worden opgevraagd of van het aantal opsporingsonderzoeken of de aard van de opsporingsonderzoeken waarvoor deze gegevens worden opgevraagd. Ook geven de cijfers geen inzicht in de mate waarin een vordering daadwerkelijk tot een verstrekking van de gevraagde gegevens heeft geleid. Alleen de vorderingen worden immers geregistreerd en niet het aantal keren dat er daadwerkelijk gegevens worden geleverd.
Over de periode vóór 2010 zijn geen betrouwbare cijfers beschikbaar, omdat de registratie van de aanvragen toentertijd niet via een centraal punt verliep en de korpsen zelf contact zochten met een aanbieder met een verzoek om gegevensverstrekking. In 2010 is deze situatie veranderd en sindsdien komen alle vorderingen betreffende gegevensverstrekking, waaronder ook historische verkeersgegevens, binnen bij de ULI, van de Landelijke Eenheid. Daar vindt de centrale registratie plaats van alle binnengekomen vorderingen.
Bij ontvangst van een vordering controleert de ULI of de naam van de aanbieder klopt, of de gevraagde gegevens ook door de aanbieder geleverd kunnen worden, over welke periode er gegevens worden opgevraagd of de vorde-

114 http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/data-retention/experts-group/docs/guidance_on_statistics_position_paper_16_datret_final_en.pdf (geraadpleegd op 20 maart 2013).
115 Wanneer de vordering gegevens een smartphone betreft, wordt door de aanbieder zowel informatie over het telefoonnummer als over het IP-adres verstrekt.

ring voldoet aan de afspraken die gemaakt zijn met de verschillende partijen en of de zoekvraag redelijk te noemen is. Dit laatste kan niet inhoudelijk, de ULI beschikt immers niet over zaaksinformatie, maar men kan wel controleren of de zoekvraag uitvoerbaar is. De vorderingen worden door de ULI doorgestuurd naar de desbetreffende aanbieder. Voorts worden de gevraagde gegevens – indien deze beschikbaar zijn – door de aanbieder naar de ULI gestuurd. De ULI stuurt deze weer door naar het korps.
Het totaalaantal vorderingen gegevensverstrekking in het jaar 2012 bedraagt 56.825. De cijfers voor het jaar 2012 zijn voor het eerst uitgesplitst naar de verschillende categorieën die we hierna één voor één zullen doornemen en beschrijven. Echter, het door de Minister bekendgemaakte aantal vorderingen gegevensverstrekking bevat ook gegevens die niet onder de Wet bewaarplicht vallen. Deze zijn zo veel mogelijk uit tabel 1 (in paragraaf 6.1.1) geweerd. Vorderingen die door de ULI in een 'restcategorie' zijn geplaatst, zijn daarom niet opgenomen in tabel 1. Vorderingen in deze categorie betreffen bijvoorbeeld vorderingen voor een mailboxdump, waarbij ook de inhoud van mailverkeer wordt gevorderd en niet enkel de verkeersgegevens. Het totaal van de tabel op komt daarmee uit op 54.813 bevragingen. Doordat deze uitsplitsing niet eerder mogelijk was, is niet vast te stellen waar het zwaartepunt ligt van de stijging ten opzichte van voorgaande jaren en wat hiervan een eventuele oorzaak zou kunnen zijn.

In het jaar 2012 zijn 41.658 vorderingen ingediend die betrekking hebben op 'historische verkeersgegevens telecommunicatie'. Dit betreft informatie over het gebruik van de telefoon en eventueel van IP-verkeer, zoals met welk nummer is er gebeld, wanneer is er gebeld, hoe lang is er gebeld, vanaf welke locatie en is er contact geweest met het internet? Wanneer de vordering verkeersgegevens van een smartphone betreft, wordt zowel informatie over telefoonverkeer als over IP-verkeer door de aanbieder verstrekt. Wanneer een vordering enkel IP-verkeer betreft, en er dus geen verkeersgegevens betreffende telefonie worden opgevraagd, dan wordt dit geregistreerd onder 'Historische verkeergegevens IP'.
Van het totaalaantal vorderingen historische verkeersgegevens telecommunicatie betreft 42,6% gegevens die niet ouder zijn dan drie maanden. De gemiddelde periode waarover inzage wordt gevraagd, bedraagt 27 dagen. Het aantal vorderingen van historische verkeersgegevens die vier tot zeven maanden oud zijn, bedraagt 9.487; dit is 23% van het totaal. De gemiddelde periode waarover dan inzage is gevraagd, is 97 dagen. Hierbij valt op dat wanneer men informatie wil hebben over een periode die verder terug ligt in de tijd, de gemiddelde periode waarover inzage wordt gevraagd langer wordt.
Zoals in hoofdstuk 4 is beschreven, hebben de onderzoekers een overzicht van de historische verkeersgegevens aangetroffen van een smartphone, die IP-verkeersgegevens bevatte die ouder waren dan de bewaartermijn voor IP-gegevens van een halfjaar. Uit tabel 1 is echter niet op te maken of de IP-

gegevens die onder deze categorie vallen wel of niet tijdig worden vernietigd. In totaal gaan 3.376 bevragingen (8,2%) verder terug in de tijd dan de maximale bewaartermijn.

De regel 'Bevragingen van masten' betreft 6.361 vorderingen van verkeers- en locatiegegevens, waarbij een aanbieder de zoekvraag krijgt welke telefoons op een bepaalde locatie (de *cell ID*) een mast aanstraalde om communicatie mogelijk te maken.
Met deze vorderingen, die zijn gericht op verkeersgegevens met locatieaanduiding (de *cell ID*), wordt een overzicht verkregen van alle mobiele gesprekken die, bij het tot stand komen van de verbinding via de mast, op de desbetreffende locatie gecommuniceerd hebben.
Een vordering voor verkeersgegevens op basis van artikel 126n Sv. betreft altijd één nummer of identificerend kenmerk. Alleen bij mastbevragingen is dit anders, omdat daarbij meerdere cellen worden opgevraagd die elkaar overlappen in dekking op een bepaalde plaats. Maar een bevraging van mastgegevens wordt slechts eenmaal meegeteld in de statistieken. Een exact getal van het aantal gevorderde telefoonnummers zou namelijk een vertekend beeld geven, omdat het bij een bevraging van een mast kan gaan om grote aantallen mobiele telefoons waarvan uiteindelijk na een grondige, vaak automatische analyse, slechts een klein deel in aanmerking komt voor vervolgonderzoek.
Meer dan driekwart van het aantal vorderingen betreffende een zendmastlocatie (79%) gaat niet verder terug in de tijd dan drie maanden. In onderling gemaakte afspraken tussen de ULI en de korpsen is overeengekomen dat een vordering betreffende verkeersgegevens van een zendmastlocatie niet langer dan een periode van drie uur mag betreffen. Dit verklaart de gemiddelde opgevraagde periode van 0,2 dagen. Echter, deze afspraak gaat blijkbaar niet helemaal meer op wanneer de op te vragen periode langer teruggaat in de tijd dan drie maanden. Navraag bij de ULI leert dat in uitzonderlijke gevallen afgeweken wordt van de '3-uurs regel', wat de oorzaak is van de tijdsintervallen langer dan drie uur.

'Historische verkeersgegevens e-mail' worden evenals 'Historische verkeersgegevens IP' slechts in zeer beperkte mate opgevraagd. Historische gegevens over e-mailverkeer werden 213 maal opgevraagd, historische IP-verkeersgegevens 39 maal. De verklaring hiervoor ligt vermoedelijk in het feit dat voor e-mail geldt dat slechts de Nederlandse aanbieders verplicht zijn om de gegevens over e-mailverkeer te bewaren voor opsporingsdiensten. Voor de verkeersgegevens IP geldt dat de 'meerwaarde' van het opvragen in deze categorie bestaat uit het verkrijgen van de log-on- en log-off-gegevens (zie hiervoor hoofdstuk 5, paragraaf 5.3.1) die dan worden geleverd. Deze gegevens blijken echter van zeer weinig waarde voor opsporingsdiensten. Wanneer het om verkeersgegevens gaat die van een smartphone afkomstig zijn, is het meer

voor de hand liggend om 'historische verkeersgegevens' op te vragen en zodoende telefonie en internetverkeer in beeld te krijgen. De IP-verkeersgegevens in deze categorie verschaffen geen antwoord op de vraag welk IP-adres iemand in gebruik had. Dit type vorderingen wordt geadministreerd onder de regel 'Historische NAW-gegevens' (de laatste categorie). Opvallend is dat zowel voor het opvragen van historische gegevens over e-mailverkeer als over IP-verkeer procentueel gezien een behoorlijk aantal vorderingen na het verstrijken van de bewaartermijn valt, die voor deze gegevens zes maanden bedraagt.

De gevorderde gegevens in de laatste categorie van tabel 1, 'Historische NAW-gegevens', kunnen betrekking hebben op zowel telefonie als IP-bevragingen. Dit kunnen vragen zijn zoals: 'door wie was dit telefoonnummer twee maanden geleden in gebruik?' of 'wie had dit IP-adres vijf dagen geleden om 15.02 uur in gebruik?'. Het totale aantal bevragingen in deze categorie bedraagt 6.542. Hiervan is 64% niet ouder dan drie maanden. De zoekvraag in deze categorie gegevens wordt overigens zeer gericht opgesteld. Bij dit type bevragingen is het tijdstip waarop een telefoonnummer of IP-adres door iemand in gebruik was, van doorslaggevend belang. Dit is terug te vinden in het feit dat de gemiddelde opgevraagde periode slechts twee dagen bedraagt.

Bij de cijfers die in tabel 1 worden gepresenteerd, dient een belangrijk voorbehoud te worden gemaakt. Niet alle vorderingen die hierin zijn opgenomen blijken betrekking te hebben op gegevens die onder de bewaarplicht vallen. De managementsystemen van de ULI zijn niet in staat om cijfers te genereren die enkel betrekking hebben op vorderingen gegevensverstrekking die onder de bewaarplicht vallen. Bij bedrijven en aanbieders die bijvoorbeeld diensten op internet aanbieden maar niet bewaarplichtig zijn, kunnen opsporingsdiensten ook vorderingen indienen voor het verkrijgen van opsporingsrelevante informatie. Deze bevragingen vallen onder dezelfde administratie als de vorderingen van gegevens die wel onder de bewaarplicht vallen. Vorderingen waarvan duidelijk is dat het om gegevens gaat die niet onder de Wet bewaarplicht vallen, zijn om die reden niet opgenomen in tabel 1. Dit verklaart het verschil tussen het aantal vorderingen tot gegevensverstrekking dat de minister bekendmaakt en het totaalaantal vorderingen dat is opgenomen in tabel 1. Hoe groot het aantal vorderingen is dat betrekking heeft op informatie die niet onder de bewaarplicht valt maar wel is opgenomen in tabel 1, is niet bekend.
Overigens zou dit een mogelijke verklaring kunnen bieden voor het feit dat een behoorlijk aantal vorderingen in een tijdvak valt dat na het verstrijken van de bewaartermijnen ligt. Een andere verklaring hiervoor zou kunnen zijn dat een strikte manier van administreren ertoe leidt dat een vordering die even blijft liggen totdat deze wordt geregistreerd, in een volgende kolom van de tabel valt. Ook wordt bij het opvragen geen onderscheid gemaakt tussen

abonnee en prepaid, terwijl prepaid IP voor een periode van een jaar bewaard dient te worden op basis van artikel 13.4 lid 3 Tw. Tot slot is het ook mogelijk dat van een aantal vorderingen die liggen na het verstrijken van de bewaartermijn, de opgevraagde termijn inderdaad langer is dan de maximale termijn van zes maanden of een jaar. In een dergelijk geval wordt de vordering met het gevraagde tijdvak geadministreerd. Dat betekent echter niet dat de geleverde informatie van de aanbieder per definitie ook de maximale bewaartermijn overschrijdt. Als de aanbieder de gegevens conform de regels vernietigt nadat de bewaartermijnen zijn verstreken, zullen deze gegevens immers niet meer voorhanden zijn. Maar vragen staat vrij en opsporingsambtenaren mogen dus bevragingen doen over een periode die verder reikt dan de bewaartermijn die de wet voorschrijft. Of het ook voorkomt dat de gegevens nog voorhanden zijn nadat de bewaartermijnen verstreken zijn – en of de aanbieders de gegevens in die gevallen leveren aan de ULI – is aan de hand van dit onderzoek niet te achterhalen. Helaas geven de beschikbare cijfers geen inzicht in de mate waarop aanbieders antwoord geven op de gestelde zoekvragen. Het aantal positieve en negatieve antwoorden dat door de aanbieders wordt gegeven, wordt niet geregistreerd. Een vraag zoals 'Door wie was dit telefoonnummer drie maanden geleden in gebruik?' kan door een aanbieder beantwoord worden met 'Het was mevrouw Janssen' of met 'Onbekend'. Beide antwoorden worden geteld als zijnde een dataleverantie. Dit omdat de ULI de antwoorden van de aanbieders doorstuurt en niet inkijkt.

Ook geven de cijfers geen inzicht in het aantal personen waarvan jaarlijks verkeersgegevens worden opgevraagd. Criminelen hebben vaak meerdere (voornamelijk prepaid) telefoons- en simkaarten in gebruik. Prepaid IP-gegevens dienen overigens voor een periode van een jaar te worden bewaard (art. 13.4 lid 3 Tw) in tegenstelling tot de bewaartermijn van zes maanden voor abonnees. Hierin wordt bij het administreren van de bevragingen geen rekening gehouden. Wanneer iemand onderwerp is van een opsporingsonderzoek, kunnen er voor meerdere telefoons, IP-adressen of e-mailaccounts gegevens worden opgevraagd. Het aantal personen op wie de in tabel 1 gepresenteerde cijfers betrekking hebben, is door de huidige manier van administreren niet bekend.

Overigens zitten in het aantal bevragingen geen dubbeltellingen zoals dat bij de jaarlijks gepubliceerde aantallen telefoon- en internettaps wel het geval is. Wanneer er een telefoon- en IP-tap op een smartphone wordt aangesloten, wordt deze als twee taps in de statistieken weggeschreven. Dit is niet het geval bij verkeersgegevens. Wanneer historische verkeersgegevens van een smartphone worden opgevraagd, wat zowel telecom- als IP-informatie oplevert, telt deze bevraging slechts één keer mee in de statistieken en valt deze onder 'Historische verkeersgegevens telecommunicatie'.

6.1.1 Conclusie

In het algemeen kan worden geconcludeerd dat het zwaartepunt van de vorderingen betrekking heeft op verkeersgegevens die maximaal een halfjaar oud zijn; een kwart van de bevragingen heeft betrekking op gegevens die langer dan een halfjaar terug gaan in de tijd. Om in de toekomst een beter beeld te krijgen van het exacte aantal bevragingen dat jaarlijks wordt gedaan, is het van belang de managementsystemen van de ULI zodoende aan te passen dat hierover betrouwbaardere gegevens kunnen worden gegenereerd. Daarnaast zou meer inzicht geboden kunnen worden in de mate waarin Nederlandse opsporingsdiensten een inbreuk maken op de privacy van verdachten en betrokkenen door de inzet van dit opsporingsmiddel, bijvoorbeeld door te registreren hoe vaak een vordering tot gegevensverstrekking daadwerkelijk tot een levering van gegevens heeft geleid. De uitgave van het *Platform for Electronic Data Retention for the Investigation, Detection and Prosecution of Serious Crime* zou in dat geval als leidraad kunnen dienen bij het publiceren van de jaarlijkse cijfers.[116] Hierin wordt onder andere geadviseerd om ook het aantal antwoorden te tellen dat negatief is of dat geen informatie bevat. Verder zou hierin meer inzicht kunnen worden geboden door de vorderingen zodanig te registreren dat zichtbaar wordt over hoeveel personen er jaarlijks telecommunicatieverkeersgegevens worden opgevraagd, in hoeveel zaken dit gebeurt en voor welke soort zaken deze gegevens worden opgevraagd.

116 http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/data-retention/experts-group/docs/guidance_on_statistics_position_paper_16_datret_final_en.pdf (geraadpleegd op 20 maart 2013).

Tabel 1 **Het aantal vorderingen tot verstrekking van telecommunicatiegegevens in het jaar 2012**

Cijfers 2012		Bewaartermijn uitgesplitst											
		0 t/m 3 maanden			4 t/m 6 maanden		7 t/m 12 maanden			13 t/m 24 maanden		>24 maanden	
	Totaal	Aantal bevragingen	Gem. opgevraagde periode in dagen		Aantal bevragingen	Gem. opgevraagde periode in dagen	Aantal bevragingen	Gem. opgevraagde periode in dagen		Aantal bevragingen	Gem. opgevraagde periode in dagen	Aantal bevragingen	Gem. opgevraagde periode in dagen
Historische verkeersgegevens telecommunicatie	41.658	17.754	27		9.487	97	11.041	216		3.298	352	78	1.309
Bevraging van masten	6.361	5.004	0,2		952	0,5	200	1,1		18	284	0	0
Historische verkeersgegevens e-mail	213	68	22		85	96	42	131		18	350	0	0
Historische verkeersgegevens IP	39	14	11		10	27	14	115		1	169	0	0
Historische NAW-gegevens	6.542	4.167	2		1.349	37	696	84		230	191	100	659

6.2 Het gebruik van verkeersgegevens in de rechtspraak

In deze paragraaf bespreken we of en hoe in vonnissen van de Nederlandse rechter het gebruik van verkeersgegevens in de bewijsvoering aan de orde komt. In dit onderzoek is een selectie van rechterlijke uitspraken betrokken, omdat eerder onderzoek van Mevis et al. (2005), zich vooral richtte op politiegegevens en -dossiers. Ook is de rol van verkeersgegevens in rechterlijke uitspraken in dit onderzoek maar zeer summier aan bod gekomen.[117] Om in deze lacune te voorzien, zijn op de website rechtspraak.nl gepubliceerde vonnissen van strafrechters doorzocht op zoektermen als (historische) verkeersgegevens en daaraan gerelateerde termen die wijzen op het gebruik van verkeersgegevens, zoals zendmasten, mastgegevens en telecomgegevens. Daarnaast is gezocht op de zoekterm IP-adres.
De website rechtspraak.nl bevat een grote verzameling gepubliceerde uitspraken van onder meer de rechtbanken, gerechtshoven en de Hoge Raad. Er zijn verschillende selectiecriteria op basis waarvan beoordeeld wordt of de publicatie van een rechterlijke uitspraak op rechtspraak.nl geboden of zelfs verplicht is. Dit laatste geldt in elk geval – voor zover voor ons onderwerp van belang – voor de uitspraken in strafzaken waarin de tenlastelegging (mede) is gebaseerd op een levensdelict of wanneer in de uitspraak een onvoorwaardelijke gevangenisstraf van vier jaar of meer en/of een tbs-maatregel is opgelegd. Daarnaast volgt publicatie wanneer een zaak mediabelangstelling heeft gekregen of wanneer publicatie om juridische redenen interessant is. Deze selectiecriteria brengen mee dat ernstige misdrijven oververtegenwoordigd zijn in het geheel van uitspraken die jaarlijks op de website worden gepubliceerd.
Onze selectie van uitspraken vormt ook om andere redenen geen representatie van de zaken die voor de rechter zijn gebracht en waarin tijdens het opsporingsproces verkeersgegevens zijn gebruikt. Vaak zal het feit dat verkeersgegevens zijn opgevraagd tijdens een opsporingsonderzoek of dat ze een rol hebben gespeeld tijdens het opsporingsproces, niet worden in het vonnis opgenomen. Als een verdachte bijvoorbeeld bekent bij de politie of bij de rechter of als er ander overtuigend en doorslaggevend bewijs aanwezig is, dan zijn de verkeersgegevens vaak niet meer nodig voor het bewijs en zullen deze – ook al vormen ze belastend materiaal – niet noodzakelijkerwijs in het vonnis worden genoemd, terwijl ze misschien een cruciale rol hebben gespeeld in de opsporing. Hetzelfde geldt voor ontlastend bewijs en voor vrijspraken. De zaken die hierna worden besproken, hebben alle betrekking op (deels) ontkennende verdachten.
Ondanks deze beperkingen is onze selectie van rechterlijke uitspraken interessant, omdat het inzicht biedt in de bewijswaarde die door de rechter aan

117 Zie eerder het beknopte overzicht van rechterlijke uitspraken ten behoeve van de gedachtewisseling met de Kamer.

dit type gegevens kan worden verbonden en laat zien op welke wijze verkeersgegevens een rol kunnen spelen in een vonnis.

In dit hoofdstuk bieden we dus inzicht in het gebruik en de waarde van verkeersgegevens in rechterlijke vonnissen en impliciet ook in de rol van verkeersgegevens in de opsporing, omdat datgene wat we in de rechtspraak aantreffen een weerslag is van de opsporing.[118] Het is echter niet mogelijk om op basis van de vonnissen iets te zeggen over het *moment* en de *periode waarover* verkeersgegevens zijn opgevraagd. We kunnen dus niet aangeven of het gaat om gegevens die van enkele maanden, een jaar of nog langer terug dateren, omdat deze gegevens gewoonlijk niet zijn opgenomen in het vonnis en hieruit ook niet betrouwbaar kunnen worden gereconstrueerd.
Daarnaast merken we hier op dat de selectie van zaken met zich meebrengt dat het succesvolle gebruik van verkeersgegevens hier de boventoon voert. Dat ligt voor de hand, omdat het een selectie betreft van zaken waarin vervolging is ingesteld. Dit betekent dat het OM door de zaak bij de strafrechter aan te brengen, reeds meende dat er voldoende bewijs voorhanden was. Opsporingsonderzoeken waarin wel verkeersgegevens zijn opgevraagd (in combinatie met andere opsporingsmethoden) maar die niet hebben geleid tot de opsporing van een verdachte, of waarin geen vervolging is ingesteld, treffen we in deze selectie niet aan. In enkele gevallen zullen we hierna ook zien dat de rechter van mening is dat de verkeersgegevens niet of onvoldoende kunnen bijdragen aan een veroordeling.
In dit hoofdstuk presenteren we achtereenvolgens de resultaten van de zoektocht naar de termen 'historische gegevens' en 'IP-adres'. Reeds op voorhand kan gezegd worden dat het aantal treffers met de term 'IP-adres' beduidend lager lag dan die met de term 'historische (verkeers)gegevens'. Om die reden is over een langere periode gezocht naar vonnissen waarin het woord IP-adres voorkwam. Met betrekking tot de term historische (verkeers)gegevens zijn vonnissen bekeken die gepubliceerd zijn tussen juli 2012 en februari 2013. De periode waarin gezocht is op de term IP-adres liep van januari 2009 tot februari 2013. Om een indruk te geven van het totale aantal gepubliceerde en voor ons onderzoek relevante vonnissen waarbinnen is gezocht op de term historische verkeersgegevens geven we eerst het volgende overzicht (tabel 2).

Tabel 2 Aantal strafzaken gepubliceerd in de periode juli 2012–februari 2013

Instelling	Aantal strafzaken
Rechtbank	2.437
Hof	839
Totaal	3.276

118 Zie voor de rol van verkeersgegevens in de opsporing in het bijzonder hoofdstuk 5.

Hiervan is een nadere selectie gemaakt. Strafzaken voor de politierechter zijn niet meegenomen. Vanwege de geringere ernst van de zaken die door de politierechter behandeld worden, zal er meestal geen sprake zijn van het gebruik van dergelijke gegevens. Overigens doet de politierechter in de meeste zaken ook mondeling uitspraak. Van de zaken die dienden bij de rechtbank, zijn enkel de zaken van de meervoudige kamer geselecteerd, en van de zaken die bij het Hof dienden enkel de hogerberoepszaken.

Instelling	Aantal strafzaken
Rechtbank meervoudig	2.344
Hof (hoger beroep)	823

De voor ons onderzoek niet relevante tbs-zaken – dit betreffen zaken waarbij het gaat om tbs-verlengingen – kunnen hier nog van worden afgetrokken. Dit betreffen 28 zaken van het Hof en 149 zaken van de rechtbank.
Hierdoor blijft de volgende selectie van zaken over.

Instelling	Aantal strafzaken
Rechtbank meervoudig	2.195
Hof (hoger beroep)	795

Dat betekent dus dat er in een totaal bestand van 2.195 rechtbankzaken en 795 hofzaken is gezocht op (historische) verkeersgegevens en daaraan gerelateerde termen die wijzen op het gebruik van verkeersgegevens, zoals zendmasten, mastgegevens en telecomgegevens en op de zoektermen IP-adres en IP-gegevens.

6.2.1 Telefoonverkeersgegevens

In het uitsprakenregister van rechtspraak.nl is gezocht op historische (verkeers)gegevens. In totaal werden 74 uitspraken gevonden waarin de term historische gegevens voorkwam. In deze vonnissen treffen we (daarnaast) ook termen aan als mastgegevens en paallocaties. Als we de vonnissen nader analyseren naar de rol of functie van deze gegevens zoals die uit het vonnis naar voren komen, vallen verschillende soorten van gebruik van die gegevens te onderscheiden.
De categorieën die het meest voorkomen, zijn te vatten onder de noemer ‘contacten tussen verdachten’ en ‘plaatsbepaling’. Onder plaatsbepaling verstaan we hier dat op basis van zendmastgegevens een bepaalde plaats wordt gelokaliseerd waar gebruik is gemaakt van een mobiele telefoon; veelal is dat de plaats delict, maar niet altijd. Het gaat hier om ‘statische’ plaatsbepaling. Naast plaatsbepaling onderscheiden we nog een kleinere categorie ‘reisbewegingen’, waarin feitelijk aan de hand van evenzoveel plaatsbepalingen kan worden gereconstrueerd langs welke weg een verdachte van A naar B is gereisd.

Het vaststellen van contacten tussen medeverdachten en plaatsbepaling valt veelal samen. Het gaat bijvoorbeeld om zaken waarin door meerdere personen een woonhuis of juwelier is overvallen en er kort voor of na de overval telefonisch of sms-contact geweest is tussen de verschillende verdachten. Daarnaast zien we dat op basis van historische gegevens kan worden vastgesteld dat verdachten met een slachtoffer contact hebben gehad of met derden (getuigen). Verder zien we in de vonnissen wel terug dat verklaringen van de verdachten expliciet worden gecontrasteerd met de gegevens die uit de historische verkeersgegevens (zouden) volgen. In de volgende tabel zijn de verschillende te onderscheiden functies weergegeven. Daarbij moet worden opgemerkt dat in een vonnis soms verschillende functies zijn terug te vinden. Allereerst volgt hierna een overzicht van de delicten waarop de geselecteerde vonnissen betrekking hadden (tabel 3); voorts volgt een overzicht van de functie van de gebruikte verkeersgegevens (tabel 4).

Tabel 3 Overzicht van de delicten waarbij verkeersgegevens werden gebruikt

Delicten	Aantal keer voorkomend in vonnissen
Inbraak	24
Overval woning/winkel	14
Moord/doodslag	13
Drugshandel	8
Diefstal met geweld/straatroof/afpersing	5
Ontvoering/gijzeling	4
Bedreiging	2
Oplichting	1
Ramkraak	1
Brandstichting	2

Als we kijken naar de functie van de verkeersgegevens in deze vonnissen valt op dat deze gegevens vooral worden gebruikt als bewijs voor het feit dat mensen op bepaalde plaatsen zijn geweest en voor het feit dat ze met anderen in contact hebben gestaan. Hierna volgt een overzicht van de functies van deze gegevens. Soms gaat het in de vonnissen ook om combinaties van functies (zie tabel 4).

Tabel 4 Overzicht van de functies van de gebruikte verkeersgegevens

Functie verkeersgegevens	Aantal keer gebruikt in vonnissen
Plaatsbepaling	39
Contact verdachten	24
Reisbeweging	19
Contrast in verklaring	12
Contact slachtoffer	6
Contact getuige	3
Bewijs diversen	10

Hierna bespreken we een aantal vonnissen, grofweg gegroepeerd rond de verschillende hiervoor genoemde functies en delicten.

6.2.2 Lokalisering van verdachten of van netwerk en vaststellen van contacten

Verkeersgegevens blijken relatief vaak ingezet te worden voor de lokalisering van verdachten in vonnissen die betrekking hebben op overvallen. Hierna volgen daarvan diverse voorbeelden.

> *Een verdachte wordt tot zes jaar veroordeeld voor een tweetal woningovervallen, met mededaders. Tijdens de woningovervallen werd de verdachte telefonisch voorzien van informatie over waar in de woning geld zou liggen. Het Hof overwoog dat blijkens de historische verkeersgegevens van de mobiele telefoons van twee verdachten – anders dan een verdachte had verklaard – naar voren was gekomen dat de verdachten ten tijde van de woningovervallen telefonisch contact hadden gehad met medeverdachten. (ECLI:NL:GHSGR:2012:BY1648)*

> *Een verdachte wordt veroordeeld tot vier jaar en zes maanden voor een overval in vereniging op een speelgoedwinkel, de eigenaar is daarbij met een vuurwapen bedreigd. Uit historische verkeergegevens was gebleken dat de verdachte en zijn medeverdachte, van wie vingerafdrukken en DNA zijn aangetroffen op de plastic zak die door één van de overvallers in de winkel was achtergelaten – kort voor de overval – twee keer telefonisch contact hebben gehad, waarbij beider telefoons gebruikmaakten van een zendmast in de directe omgeving van de woning van medeverdachte. Daaruit leidt de rechtbank af dat verdachte zijn medeverdachte kort voor de overval thuis heeft opgehaald. (ECLI:NL:RBSGR:2012:BX6147)*

> *De volgende zaak betreft een woningoverval in vereniging waarbij met een wapen is gedreigd en het slachtoffer is mishandeld en vastgebonden. De telefoon van verdachten straalt aan op een zendmast in de omgeving van de woning. De rechtbank overweegt verder dat het 'opvallend was (...) dat vanaf het moment van de overval het telefoonnummer niet meer gebruikt is om te bellen dan wel sms-berichten te versturen en nog slechts sporadisch een zendmast aanstraalde.' (ECLI:NL:RBSGR:2012:BX5776)*

In verschillende zaken werden aan de hand van verkeersgegevens ook de reisbewegingen van verdachten voorafgaand aan een overval in beeld gebracht. Zo werden bijvoorbeeld de reisbewegingen aan de hand van paallocaties gereconstrueerd van de verdachte van een woningoverval, vanaf diens woonplaats tot aan de woning van het slachtoffer. Bij een *rip deal* met dodelijke afloop worden historische en zendmastgegevens gebruikt bij het

vaststellen van de door verdachten afgelegde route en hun aanwezigheid bij de plaatst delict. (*ECLI:NL:GHARN:2012:BX6121*)

> *Bij een gewelddadige overval op een woning waarbij het slachtoffer zwaar lichamelijk letsel opliep, werd nauwgezet, met weergave van duur en tijdstip van een gesprek en de straatnaam van de locatie van de zendmasten, een voor het bewijs relevante route van verdachten in kaart gebracht. Daarnaast stelde de rechtbank vast dat de relevante telefoonnummers zijn gebruikt door de daders van de overval en dat de telefoons speciaal voor gebruik bij de overval waren aangeschaft. (ECLI:NL:RBARN:2012:BY2895)*

> *Met betrekking tot verdachten die – als zwarte pieten verkleed – een overval op een koerier zouden hebben gepleegd, overwoog de rechtbank dat een van de verdachten elders was geweest dan waar deze beweerde, wat onder andere werd afgeleid uit telefoongegevens. (ECLI:NL:RBSGR:2012:BX5105)*

Tot slot noemen we hier een overval op een McDonald's.

> *Uit onderzoek van historische gegevens blijkt dat een bepaald telefoonnummer bij verdachte in gebruik is en uit twee belcontacten van dit nummer blijkt dat deze achtereenvolgens op twee verschillenden locaties plaatshadden, waar de McDonald's precies tussen lag. Met betrekking tot het verweer van verdachte dat hij in de plaats woont waar de McDonald's zich bevindt, overweegt de rechtbank dat als uitgangspunt dient te gelden 'dat zendmastgegevens in beginsel een ondersteunend karakter hebben maar dat die gegevens in onderling verband beschouwd en in samenhang met andere uit het dossier blijkende feiten en omstandigheden voor de bewezenverklaring redengevend kunnen zijn. (...) Ten aanzien van de overval op de McDonald's (...) is echter gebleken dat in de zes maanden voorafgaand aan de overval de telefoon van de verdachte de desbetreffende zendmasten geen enkele keer heeft aangestraald.'*

> *Met betrekking tot een tweede overval, ook op een snackbar, wordt eveneens vastgesteld dat, gelet op de aangestraalde zendmasten, de plaats van de overval globaal gelegen is in de omgeving tussen beide zendmasten. Dit wordt bezien in samenhang met de tijdstippen waarop de masten zijn aangestraald en het tijdstip van de overval. (ECLI:NL:RBALK:2012:BX4768)*

Uit de bestudeerde rechtspraak komen ook voorbeelden van het gebruik van locatiegegevens bij het vaststellen van contacten tussen verdachten die op andere misdrijven betrekking hebben dan (woning)overvallen. Zo is een verdachte veroordeeld voor het medeplegen van een liquidatie vanuit een bestelbus op een parkeerplaats aan de snelweg. Reisbewegingen van verdachten – en dat verdachten bij een winkel zijn geweest waar bivakmutsen en

handschoenen zijn gekocht – blijken uit verkeersgegevens. (*ECLI:NL:RBUTR:2012:BX2092*).

We noemen hier enkele voorbeelden van deze zaken:

In een onderzoek naar een poging liquidatie treft de politie op een gasfornuis een gedeeltelijk verbrande telefoon aan. Onderzoek door het Nederlands Forensisch Instituut aan deze 'pannetjestelefoon' en historische gegevens van het (kennelijk) aldus achterhaalde nummer van de telefoon wijst uit dat de telefoon onderdeel was van een zogenaamd gesloten telefooncircuit. Daarin wordt louter onderling gebeld met de telefoons die van dat circuit deel uitmaken, gewoonlijk om tracering van de (prepaid) nummers aan de hand van belcontacten met derden tegen te gaan. De historische gegevens geven inzicht in de rijroute van verdachten en de aanwezigheid in de directe nabijheid van de plaats delict. (ECLI:NL:RBAMS:2012:BX1952)

Bij een groot onderzoek naar de productie van synthetische drugs wordt een contact tussen verdachten vastgesteld aan de hand van een bij een doorzoeking aangetroffen briefje met een telefoonnummer. Met dit nummer was blijkens de historische gegevens enkele malen naar een bepaalde buzzer gebeld. (ECLI:NL:GHSHE:2012:BW7042)

Een poging tot doodslag waarbij het slachtoffer met een schroevendraaier in de hals is gestoken. Het hof gaat ervan uit dat verdachte op de plaats delict – een garage – is geweest en overweegt daartoe onder meer dat een telefoonmast werd aangestraald in de nabije omgeving van deze garage. (ECLI:NL:GHAMS:2012:BY2562)

Een verdachte wordt veroordeeld voor wederechtelijke vrijheidsberoving en verkrachting van een zes jaar oud meisje. Het slachtoffer was met een smoes de auto in gelokt waar het misbruik plaatsvond. Uit historische telefoongegevens kwam naar voren dat verdachte zich op bewuste datum en tijdstip in het gebied had bevonden waar een man het slachtoffer op straat had aangesproken. (ECLI:NL:RBSGR:2012:BY0109)

Een andere zaak had betrekking op een groot aantal inbraken/kluiskraken in winkels en supermarkten verspreid over het land door een grote groep daders. Uit de historische gegevens werd onder meer afgeleid dat verdachten bij inbraken dan wel bij voorverkenningen ten behoeve van de inbraken aanwezig zijn geweest. (ECLI:NL:RBUTR:2012:BX9634)

In een onderzoek naar ladingdiefstallen vanuit vrachtwagens duidden print- en mastgegevens erop dat twee telefoonnummers die in gebruik waren bij twee verdachten, rondom hetzelfde tijdstip als een in het voertuig

van verdachten geplaatst peilbaken aangaf, aanstraalden op masten in de buurt van de plaats delict. (ECLI:NL:RBUTR:2012:BX9634)

De telefoon van een verdachte maakt contact met een zendmast in de buurt waar een aantal inbraken zijn geweest. In samenhang met – onder meer – de verklaring van een medeverdachte, die de ochtend daarop verdachte in het gezelschap van anderen zag thuiskomen in het bezit van spullen die later in de door verdachte bestuurde auto waren aangetroffen, leiden tot een veroordeling voor een aantal diefstallen. (ECLI:NL:GHAMS:2012:BY1810)

Naast deze geweldsmisdrijven valt ook te noemen een onderzoek naar een verdachte die meerdere banken, op verschillende plaatsen in het land, heeft opgelicht. Zendmastgegevens zijn gebruikt om te onderbouwen dat de verdachte in de buurt was, dan wel op weg naar de banken waar de oplichting plaatsvond. (ECLI:NL:RBBRE:2012:BX4244)

Tot slot noemen we hier de veroordeling van een verdachte voor de invoer van cocaïne.

De rechtbank stelt op basis van historische printgegevens vast dat verdachte een bepaald telefoonnummer heeft gebruikt en dat vervolgens met dat nummer contact is gemaakt met een zendmast bij een Terminal te Schiphol. (ECLI:NL:RBHAA:2012:BW2968)

Uit de voorgaande voorbeelden blijkt dat voor het vaststellen waar een verdachte op een bepaald tijdstip was, historische gegevens en zendmastgegevens van belang kunnen zijn. Wanneer er, zoals bij enkele berovingen en woningovervallen het geval was, telefonische contacten (nodig) zijn tussen meerdere verdachten, kan dat voor de opsporing relevante onderzoeksgegevens opleveren. Een telefonisch contact dat op of rond het tijdstip van het misdrijf plaatsvindt, ook als dat om de aflevering van een partij drugs gaat, vergroot de opsporingsmogelijkheden voor politie en justitie.

6.2.3 Ondersteunen of ontkrachten van verklaringen

Er zijn echter meer manieren waarop historische gegevens en zendmastgegevens gebruikt worden als (ondersteunend) bewijs in de bestudeerde vonnissen. Een voorbeeld hiervan is dat de rechter expliciet ingaat op het niet stroken van verklaringen van verdachten – of juist het nalaten een verklaring af te leggen – met, respectievelijk over de in het dossier opgenomen verkeersgegevens. Het is uiteraard goed denkbaar dat gedurende de zitting een verdachte wordt geconfronteerd met (bepaalde gevolgtrekkingen uit) de verkeersgegevens, maar het gaat ons hier om de gevallen waarin in het vonnis expliciet

aandacht wordt besteed aan de waardering van die gegevens tegen de achtergrond van verklaringen van de verdachte daarover. Een door verdachte aangevoerde verklaring voor in het dossier aanwezige (belastende) verkeersgegevens wordt aldus getoetst en in een aantal gevallen ongeloofwaardig bevonden. Ook komt het voor dat juist het niet willen uitleggen, waar uitleg op zijn plaats lijkt, de bewijswaarde van de verkeersgegevens kennelijk versterkt.

Zo ook in het geval van een verdachte van verduistering van een groot geldbedrag uit een geldtransportwagen die pas enkele weken na het delict een verklaring aflegt die volgens de rechtbank op meerdere punten tegenstrijdig blijkt te zijn.

> *Deze verdachte zou zijn telefoon hebben afgegeven aan een kennis, terwijl uit historische gegevens van de telefoon bleek dat hij zijn zus nog een sms had gestuurd. Bij de politie wilde de verdachte daarover geen opheldering geven, ter zitting zegt verdachte inderdaad een sms te hebben gestuurd, maar ter bescherming van zijn zus daarover niets te hebben willen zeggen. De rechtbank lijkt dit met een korrel zout te nemen waar zij stelt dat verdachte niet duidelijk heeft kunnen maken hoe, aldus de rechtbank, zijn eerdere, onjuiste verklaringen konden bijdragen aan het beschermen van zijn zus. (ECLI:NL:RBROT:2012:BX1291)*

> *In een andere zaak acht de rechtbank de verklaring van een verdachte van een overval – waar historische verkeersgegevens een verdenking op hem laadden – dat hij zijn telefoon mogelijk wel zal hebben laten liggen in de auto van één van zijn straatvoetbalvrienden, ongeloofwaardig. Temeer, aldus de rechtbank, omdat de verdachte tijdens diverse verhoren nooit heeft verklaard over zijn straatvoetbalvrienden die, volgens verdachte, wellicht de overvallen hadden gepleegd en daarbij gebruik hadden gemaakt van zijn spullen. (ECLI:NL:RBALK:2012:BX4768)*

> *In een zaak tegen een verdachte van een gewapende overval in vereniging stelt de rechtbank dat verdachte met betrekking tot zijn aanwezigheid op een bepaalde plaats wisselende verklaringen heeft afgelegd. Verdachte zou zijn verhaal aanpassen wanneer in het onderzoek nieuwe informatie naar voren kwam, dat gold in het bijzonder voor verklaringen over de historische verkeersgegevens van zijn telefoon en de verklaring van medeverdachte. De rechtbank kende daarom geen waarde toe aan de verklaring van verdachte dat hij niet bij de overval betrokken was geweest. (ECLI:NL:RBAMS:2012:BX5674)*

> *Bij een rip deal met dodelijke afloop (eerdergenoemd) stelt het Hof onder meer vast dat de verklaringen die verdachte en medeverdachte hebben gegeven niet passen bij – onder meer – de historische printgegevens en*

zendmastgegevens. De haast die zij zouden hebben gehad in verband met een verjaardag elders, strookte niet met deze gegevens waaruit volgde dat men een uur in Arnhem was gebleven. Ook wanneer een patatje was gegeten, zou een verblijfsduur van een uur in Arnhem zonder andere activiteiten onwaarschijnlijk lang zijn. De periode van verblijf in Arnhem wordt afgeleid uit de belgegevens en het delict is in (de nabijheid) van Arnhem gepleegd. (ECLI:NL:GHARN:2012:BX6113)

In een zaak van diefstal met geweld met zwaar lichamelijk letsel tot gevolg wijst het Hof erop dat de verdachte een verklaring geeft voor telefonische contacten met zijn medeverdachten, waaruit volgens het Hof zou volgen dat de verdachten ten minste tweemaal die avond in de directe omgeving van de woning van het slachtoffer zijn geweest. Ten aanzien van een verklaring van verdachte over een bepaald moment waarop zou zijn gebeld, merkt het Hof op dat die verklaring gelet op de telecommunicatiegegevens aantoonbaar onjuist is. Zowel uit historische printgegevens van de telefonische contacten als uit de aangifte van een inbraak bleek dat verdachte en zijn medeverdachten tot laat in de avond en begin van de nacht samen op pad zijn geweest en zich een aantal malen hebben verplaatst. (ECLI:NL:GHARN:2012:BW8652)

Een spiegelbeeldige zaak deed zich voor in een onderzoek waarin juist de verdachte zijn verklaring ondersteund wilde zien door onderzoek naar telecomgegevens van een medeverdachte.

In een moordzaak legde de medeverdachte een belastende verklaring af over verdachte. Door onder andere het doen van telecomonderzoek is getracht na te gaan of slachtoffer en medeverdachte elkaar kenden, zo wordt door de officier van justitie gesteld tegenover het verweer dat OM en politie eenzijdig onderzoek hadden gedaan. Het enkele feit dat dit niet tot een bevestiging leidde van de verklaring van verdachte maakte het onderzoek daarmee nog niet eenzijdig. De rechtbank is van mening dat daar waar aanknopingspunten geboden werden om verklaringen van verdachten te controleren – bijvoorbeeld door middel van telecomgegevens, aldus de rechtbank – dit is gedaan. (ECLI:NL:RBAMS:2012:BX3164)

6.2.4 Andere functies van het gebruik van verkeersgegevens

Naast het feit dat uit verkeersgegevens door de rechter, in de hiervoor besproken situaties, wordt afgeleid dat verdachten met elkaar contact hebben gehad en dat dit – in samenhang met andere belastende informatie – kan bijdragen aan het bewijs, hebben we in de bestudeerde zaken ook gezien dat telefonische contacten tussen verdachten en slachtoffer of tussen verdachten en andere betrokkenen voor bewijs relevant waren. Hiervoor kwam dit al kort

aan bod in de casus, waarin het versturen van een sms aan een zus de verklaring van verdachte deed wankelen. In een geval van doodslag door de partner van het slachtoffer wordt met behulp van historische verkeersgegevens in het kader van een tijdlijn vastgesteld op welk moment een telefooncontact van het *slachtoffer* met een derde had plaatsgevonden, waarna geen levensteken van het slachtoffer meer vernomen was (*ECLI:NL:RBSHE:2012:BY0575*). In een onderzoek naar een doodslag zonder dat een lijk was aangetroffen heeft een nauwgezette reconstructie van verkeersgegevens en belcontacten tussen de verdachte en het slachtoffer geleid tot een veroordeling (*ECLI:NL:RBNNE:2013:BY9376*).

> *In een zaak betreffende een inbraak en schietpartij met dodelijke afloop bij een hennepkwekerij wordt – met betrekking tot de inbraak waarvoor verdachte veroordeeld wordt – aan de hand van historische gegevens vastgesteld dat het slachtoffer op een bepaald moment nog in leven was, omdat er op dat moment nog een telefonisch contact plaatshad tussen het slachtoffer en een getuige. (ECLI:NL:GHSHE:2012:BX9271)*

> *In een andere zaak acht de rechter een door de vriendin van een verdachte gegeven alibi, namelijk dat verdachte bij haar was op het moment dat een roofoverval met dodelijke afloop had plaatsgevonden, niet geloofwaardig omdat uit de historische gegevens bleek dat de verdachte op de bewuste avond veelvuldig telefonisch contact had gehad met zijn vriendin. (ECLI:NL:RBDHA:2013:BZ0962)*

> *In een gijzelingszaak wordt op basis van historische verkeersgegevens aangenomen dat een bepaald nummer bij verdachte in gebruik was, omdat met dit nummer (veelvuldig) was gebeld met de vrouw en familieleden van een medeverdachte en – onder andere – uit mastgegevens bleek dat het nummer aanstraalde bij de woning van de ouders van een andere medeverdachte. (ECLI:NL:RBUTR:2012:BX5072)*

> *Bij een overval op een woning wordt terug gerechercheerd vanuit een nummer, waarmee naar het latere slachtoffer tweemaal kort was gebeld. Omdat dit nummer bleek aan te stralen in de buurt van de woning van het slachtoffer, leidde een spoedtap op de telefoon uiteindelijk naar verdachte. (ECLI:NL:RBSGR:2012:BX5776)*

Het komt ook voor dat wanneer gebeld is met een slachtoffer, dit in combinatie met de duur van het gesprek bijdraagt aan het bewijs van een delict, anders dan door gangen van verdachten of contacten met medeverdachten vast te stellen.

Zo wordt in geval van – onder meer – een bedreiging, door het slachtoffer gezegd dat zij de stem van verdachte herkende. Uit historische gegevens blijkt dat er een kortdurende verbinding tussen nummers behorend aan verdachte en het slachtoffer is geweest. De korte duur van het gesprek (zes seconden) past bij de geuite bedreiging (voor 1 juli betalen, anders gaat je kop eraf!). (ECLI:NL:RBAMS:2012:BW3724)

De hiervoor besproken voorbeelden hebben alle betrekking op uitspraken waarin historische verkeersgegevens zijn gebruikt voor het bewijs en de zaak met een veroordeling is geëindigd.
Hierna bespreken we enkele zaken waarin uit het vonnis naar voren kwam dat historische verkeersgegevens niet konden bijdragen aan het bewijs en waarin soms een vrijspraak volgde.

6.2.5 Vrijspraken

In een aangifte kinderontvoering overweegt de rechtbank dat het door aangeefster gegeven relaas van de tijdstippen en gebeurtenissen met betrekking tot het ophalen van de kinderen en een daarmee verband houdend telefoontje van verdachte vanuit België, niet geloofwaardig is. De rechtbank baseert dit mede op het gegeven dat verdachte elders was, hetgeen werd ondersteund door historische gegevens. (ECLI:NL:RBROE:2012:BY0623)

Een verdachte wordt vrijgesproken van een schietpartij. De rechtbank overwoog onder meer dat de omstandigheid dat verdachte op tijdstippen rond de schietpartij telefonisch contact had gehad met een mogelijke medeverdachte, op basis waarvan bevindingen in het procesdossier waren opgenomen met betrekking tot verdachtes locatie op die bewuste tijdstippen, onvoldoende aanwijzing vormde voor zijn betrokkenheid. (ECLI:NL:RBSHE:2012:BW2684)

Hoewel het dossier volgens de rechtbank grond biedt voor een verdenking van betrokkenheid van verdachte bij twee overvallen op een juwelier, ontbreekt daarvoor bewijs. De officier achtte de verdachte schuldig, mede op grond van beschikbare telecomgegevens, waaruit onder andere blijkt dat verdachte veelvuldig contact had met twee wel veroordeelde medeverdachten rond 10 juni 2011. Voor beide overvallen gold volgens de officier van justitie dezelfde werkwijze: drie overvallers, dezelfde juwelier en dezelfde vluchtroute. Ter zitting ontkende verdachte dat een bepaald mobiel nummer van hem was. De rechtbank is van oordeel dat uit de bewijsmiddelen onvoldoende naar voren komt dat dit nummer bij verdachte in gebruik is geweest. Daar komt bij dat het nummer op de bewuste data wel in de omgeving van Dongen aanstraalde, maar niet in Dongen zelf. (ECLI:NL:RBBRE:2012:BX8759)

De rechtbank spreekt verdachte vrij van het medeplegen van brandstichting in een moskee. Het feit dat verdachte daarbij betrokken zou zijn, berustte voornamelijk op de verklaring van de medeverdachte. De in het dossier aanwezige camerabeelden en historische telefoongegevens waren, aldus de rechtbank, niet in strijd met de lezing van verdachte en medeverdachte. (ECLI:NL:RBSGR:2012:BX7529)

Een verdachte van vier overvallen wordt vrijgesproken. Met betrekking tot de historische printgegevens waaruit zou blijken dat één van de telefoons van verdachte ongeveer tien minuten na het tijdstip van de overval een paar straten verder van de plaats delict aanstraalde, merkt de rechtbank op dat dit verdachte slechts in de buurt van de plaats van de overval lokaliseert, en dat verdachte bovendien in Apeldoorn woonachtig is. Omdat om die reden het niet onlogisch was dat zijn telefoon een mast in Apeldoorn aanstraalde, linkte dit gegeven volgens de rechtbank verdachte niet of onvoldoende aan de overval. (ECLI:NL:RBZUT:2012:BW9618)

Tot slot noemen we een zaak waarin de rechtbank expliciet twijfelt aan de betrouwbaarheid van de historische verkeersgegevens:

In een drievoudige moord-/doodslagzaak wordt verdachte tot een levenslange gevangenisstraf veroordeeld. De resultaten van het onderzoek naar de mobiele telefoon van verdachte worden niet voor het bewijs gebruikt (maar waren ook niet noodzakelijk), omdat deze gegevens volgens de rechtbank onjuist waren. (ECLI:NL:RBDOR:2012:BX9919)

6.3 Internetverkeersgegevens

Bij de selectie van zaken met de term IP-adres kwam een aantal vonnissen naar boven waarin deze zoekterm voorkwam, maar waarbij onvoldoende duidelijk was of het IP-adres door een aanbieder was geleverd of bijvoorbeeld door een site als Marktplaats.nl. Deze vonnissen zijn daarom buiten beschouwing gelaten.
Uit een 26-tal zaken uit de periode januari 2009 - februari 2013 springen onderzoeken naar kinderporno er in aantallen uit: meer dan de helft (15) van de vonnissen gaat over het downloaden/verspreiden van kinderporno. Andere soorten delicten komen incidenteel voor, variërend van stalking en bedreiging tot oplichting. Als het gaat om de hiervoor onderscheiden functies waar het de historische gegevens betreft, laat het gebruik van internetverkeersgegevens een wat ander beeld zien. De gevallen zijn te onderscheiden van de voorgaande doordat het niet zozeer gaat om de *whereabouts* van de verdachte (waar was hij en met wie), maar doordat het gebruikte middel meer (inhoudelijk) instrumenteel is geweest bij het te plegen van het delict

en daarmee ook inhoudelijke informatie prijsgeeft, zoals uit navolgende voorbeelden naar voren komt. Enigszins analoog aan het hiervoor gegeven voorbeeld waarin een relatie wordt gelegd met de *duur* van een gesprek en de in dat gesprek – en met de duur van dat gesprek overeenkomende – geuite bedreiging.

6.3.1 Kinderporno

> *Een verdachte wordt veroordeeld voor het bezit van kinder- en dierenporno. Uit door Interpol aangeleverde informatie volgt een onderzoek naar onder meer IP-adressen via welke bestanden zijn gedownload. Uit zogenaamde logfiles bleek dat het IP-adres van de verdachte daarvoor gebruikt is. (ECLI:NL:RBUTR:2012:BW8244)*

Er zijn meerdere vonnissen waarin feitelijk op dezelfde wijze via Interpol-informatie tot de verdachte is gekomen, telkens met een veroordelend vonnis. Veelal gaat het om informatie uit verschillende landen. In een zaak kwam de informatie uit Brazilië, waar het ging om zeer ernstige kinderporno, waarbij verdachte als gebruiker van een peer-to-peerprogramma ook foto's verspreidde. In één zaak leidden juridische gronden tot een vrijspraak, hetgeen we hierna bespreken.

> *Na informatie van Interpol over kinderporno volgt een onderzoek naar een IP-adres. Het IP-adres blijkt op naam van een persoon X te staan, zeven computers blijken aan dit (kantoor)netwerk te zijn gekoppeld. Verdachte maakt gebruik van een van die computers en zegt op zoek te zijn geweest naar kinderpornografische afbeeldingen, op basis waarvan de rechtbank aanneemt dat verdachte de gedownloade afbeeldingen heeft gezien. Omdat het enkel bekijken van afbeeldingen (zonder het opslaan daarvan) in de tenlastegelegde periode destijds niet strafbaar was, komt het tot een vrijspraak. (ECLI:NL:RBSGR:2012:BV2841)*

6.3.2 Advertenties

Er zijn verschillende voorbeelden te geven van advertenties op internet, waarbij de advertentie een rol speelt bij het strafbare feit of bij strafbare feiten van verschillende aard. Allereerst is er een geval van grootschalige oplichting door het aanbieden van goederen via marktplaats. De gedane betalingen werden via rekeningen van katvangers ontvangen. Onder meer droegen overeenkomsten tussen de door verdachten gebruikte IP-adressen gerelateerd aan de geplaatste advertenties bij aan het bewijs van de (vele) feiten. (*ECLI:NL:RBSGR:2012:BV2841*)

Een andere advertentie had betrekking op verkoop van slaapmiddelen.

Een verdachte wordt met een mededader veroordeeld voor het zonder handelsvergunning bedrijfsmatig handelen in slaap- en kalmeringsmiddelen. Het bewijs komt onder meer voort uit op internet geplaatste advertenties, waarbij van een bepaald IP-adres gebruik was gemaakt. Bij een doorzoeking op 9 maart 2011 van de woning is het IP-adres van de daar aangetroffen laptop uitgelezen. Dit bleek hetzelfde IP-adres te zijn. (ECLI:NL:RBSGR:2012:BX4547)

Een verdachte wordt met zijn mededader veroordeeld voor mensenhandel. Verdachte heeft een minderjarige aangezet tot prostitutie. Er zijn daartoe advertenties geplaatst op internet, die zijn aangemaakt vanaf het IP-adres van verdachte. Diens stelling dat iemand anders van zijn computer gebruik zou hebben gemaakt, acht de rechtbank om verschillende redenen niet aannemelijk. (ECLI:NL:RBSGR:2012:BW5833)

Een advertentie/uitnodiging voor seksuele ontmoetingen liep voor diegenen die daar gehoor – en gevolg – aan gaven slecht af, doordat de opsteller van de advertentie, en deelneemster aan de seksuele ontmoetingen, nadien de deelnemers beschuldigde van verkrachting. Uit informatie van de provider konden de advertenties herleid worden tot het IP-adres van verdachte. Zij werd veroordeeld voor het doen van valse aangiften. (ECLI:NL:RBZUT:2011:BR3110)

6.3.3 Bedreiging

Ook via internet geuite bedreigingen kunnen herleidbaar zijn tot de dader. In een geval van belaging/belastering van een burgemeester worden berichten verstuurd vanaf verschillende openbare computers, onder andere van een bibliotheek. Uit onder meer dezelfde werkwijze op het internet en het gegeven dat verdachte zeer regelmatig op die plaatsen kwam om te internetten, komt de rechter tot een veroordeling voor een deel van de aan verdachte toegeschreven verstuurde berichten. (ECLI:NL:RBUTR:2012:BV7040)

In geval van een op internet geplaatste bedreiging met een schietpartij op een school leiden internetgegevens uiteindelijk tot de onbeschermde internetverbinding van de buren van de verdachte. (ECLI:NL:RBBRE:2010:BO3363)

In een zaak betreffende belastingfraude en valsheid in geschrifte in georganiseerd verband, wordt een verdachte tot vier jaar gevangenisstraf veroordeeld. Voor het bewijs wordt onder meer gebuikt dat aangiften omzetbelasting via het IP-adres van het bedrijf van verdachte zijn verstuurd (ECLI:NL:RBSGR:2012:BX0774).

Tot slot geven we nog voorbeelden van enkele andere delicten waarbij de sporen die het handelen van verdachte op internet heeft nagelaten tot verdachte herleid kunnen worden.

Een leraar wordt veroordeeld voor ontucht met een minderjarige leerlinge. Voor het bewijs is relevant dat computerberichten vanaf het IP-adres van verdachte zijn verstuurd. Het verweer dat iemand anders die berichten zou hebben verzonden, acht de rechtbank niet aannemelijk. (ECLI:NL:RBSHE:2012:BV8201)

Een verdachte wordt onder meer veroordeeld voor grootschalige mensensmokkel vanuit Iran. De verdachte begeleidde personen vanuit Iran naar het Verenigd Koninkrijk. De tickets werden via internet besteld. De betaling via VISA, een gebruikt e-mailadres en IP-adres werden gelinkt aan een adres in Nederland, dat volgens de rechter rechtsreeks aan verdachte gekoppeld kon worden. (ECLI:NL:RBMAA:2011:BQ8509)

Verdachte wordt veroordeeld voor onder meer voorbereidingshandelingen van diefstal met geweld. Via een tot de woning van verdachte herleidbaar IP-adres wordt vastgesteld dat verdachte een MSN chatgesprek heeft gevoerd over de levering van een vuurwapen. Verder wordt aan de hand van raadpleging van een internetadres vastgesteld dat vanaf dat adres veelvuldig informatie is gezocht en bekeken over inbraken, overvallen, ramkraken en plofkraken. (ECLI:NL:RBUTR:2012:BX2092)

6.4 Tot slot

Uit de weergegeven vonnissen van de Rechterlijke Macht blijkt dat verkeersgegevens een substantiële rol kunnen spelen bij het leveren van het bewijs in een strafzaak. De term substantieel is hier op zijn plaats, omdat de rechter in de bewijsmiddelen – of als datgene wat tot de overtuiging van de rechter heeft bijgedragen – de verkeersgegevens en de conclusies die daaraan door de rechter worden verbonden in het (veroordelende) vonnis heeft opgenomen. In enkele gevallen geeft de rechter ook aan dat de verkeersgegevens onvoldoende bewijs opleveren. Dit speelde vooral wanneer uitsluitend uit de verkeersgegevens de aanwezigheid van een verdachte bij de plaats van een misdrijf werd afgeleid. In de literatuur en in de politieke discussie is wel aangevoerd dat ook de onschuld van een verdachte met behulp van verkeersgegevens zou kunnen worden aangetoond. We zijn hiervan één voorbeeld tegengekomen. Daarnaast is het mogelijk dat dergelijke gevallen zich reeds in een eerder stadium – tijdens het opsporingsonderzoek – hebben voorgedaan. Ofschoon het nut van het gebruik van verkeersgegevens uit de besproken vonnissen duidelijk kan worden, werpt dit onderzoek geen licht op de ouder-

dom van de opgevraagde gegevens. Wel kan in het licht van de gegeven voorbeelden gezegd worden dat het belang van dit type gegevens niet noodzakelijkerwijs afneemt naarmate de op te vragen gegevens verder teruggaan in de tijd.
Op verschillende manieren kunnen verkeersgegevens bijdragen aan het bewijs, allereerst doordat verdachten aan een bepaalde locatie verbonden kunnen worden en aan medeverdachten. Dit komt het meeste voor. Daarnaast kunnen ook (belastende) contacten met slachtoffers en derden blijken. Bij het gebruik van het internet bij het plegen van strafbare feiten valt op dat de daarop betrekking hebbende verkeersgegevens vaak rechtstreeks verbonden zijn met het gepleegde strafbare feit. Ter verduidelijking: het feit dat uit telefonische contacten blijkt dat verdachten elkaar kennen, zegt op zichzelf nog niet iets over het strafbare feit waarvan zij verdacht worden en van de wijze waarop dit feit is gepleegd. Daarentegen is de downloader van kinderporno of diegene die personen oplicht via Marktplaats – indien identificatie van de verdachte mogelijk is en indien de verdachte de enige gebruiker is van de computer – direct gekoppeld aan het strafbare feit. De computer, of het internet, is meer instrumenteel bij de uitvoering van het delict en veel ander bewijs is dan niet meer noodzakelijk.
Dit kan erop wijzen dat internetverkeersgegevens vooral worden opgevraagd en geanalyseerd bij delicten waarbij het internet gebruikt wordt om delicten te plegen, en minder om dagelijkse contacten of locaties vast te stellen die als ondersteuning kunnen dienen bij andere soorten delicten.

7 Slotbeschouwing

In dit rapport is de Wet bewaarplicht onderzocht en de wijze waarop gegevens over telefoon- en internetverkeer gebruikt worden in de opsporingspraktijk. Het onderzoek schetst een beeld van de implementatie van de Wet bewaarplicht in de praktijk. Er is onderzocht hoe de Wet bewaarplicht, drie jaar na invoering, functioneert. Hierbij is gekeken hoe verkeers- en locatiegegevens in de praktijk worden ingezet bij de opsporing, vervolging en bewijsvoering van misdrijven. Daarbij is ook onderzocht hoe vaak de verkeers- en locatiegegevens worden opgevraagd en hoe het toezicht op de naleving van de wet is georganiseerd.
De bevindingen zijn gebaseerd op literatuuronderzoek en interviews die zijn gehouden met opsporingsambtenaren, OvJ's, advocaten, aanbieders van telecomdiensten, toezichthouders en enkele andere personen die beroepshalve te maken hebben met de bewaarplicht van telecommunicatiegegevens.

Telefoonverkeersgegevens
Historische verkeers- en locatiegegevens betreffende telecommunicatie worden veelvuldig opgevraagd en geanalyseerd ten behoeve van de opsporing. Professionals en experts waarderen de mogelijkheden die deze gegevens hen kunnen bieden voor de opsporing. Vooral voor het in kaart brengen van netwerken en het lokaliseren van een telefoon wordt vaak een beroep gedaan op verkeers- en locatiegegevens. De geïnterviewde professionals uit de opsporingspraktijk zien het opvragen van verkeersgegevens als een opsporingsmiddel dat op verschillende manieren voor uiteenlopende zaken kan worden ingezet. Veel professionals en experts zijn van mening dat het werken met verkeers- en locatiegegevens specialistenwerk is. In de praktijk blijken de gegevens complexe vragen te kunnen opleveren. De variatie aan nieuwe technische snufjes en technologische ontwikkelingen maakt het er niet eenvoudiger op.
Verkeersgegevens kunnen niet alleen gezien worden als een belangrijk opsporingsmiddel, maar kunnen ook een rol spelen in de bewijsvoering. Uit een analyse van openbaar gepubliceerde vonnissen kan worden afgeleid dat de rechter gegevens over telecommunicatieverkeer tussen juli 2012 en februari 2013 in verschillende situaties als bewijsmiddel heeft gebruikt en een plek heeft gegeven in de motivering van het vonnis.

Internet verkeers- en locatiegegevens
Een analyse van verkeers- en locatiegegevens van het telefoon- en internetverkeer van een persoon geeft een gedetailleerd beeld van diens leven. Tegelijkertijd is het een illusie dat met de bewaarplicht van verkeers- en locatiegegevens het communicatiegedrag van iemand volledig in kaart kan worden gebracht. Tegenwoordig verloopt steeds meer communicatie via het internet, waarbij in veel gevallen gebruik wordt gemaakt van diensten die buiten de Nederlandse Wet bewaarplicht vallen. De Wet bewaarplicht stopt bij de Nederlandse grens, terwijl het internet grens- en locatieloos is. Dit wringt.

Professionals en experts die regelmatig betrokken zijn bij opsporingszaken waarbij vermoed wordt dat verdachten via het internet communiceren, geven aan dat zij graag zouden beschikken over verkeersgegevens betreffende deze online communicatie. Echter, het aantal Nederlandse bevragingen bij buitenlandse bedrijven die veel gebruikte internetdiensten aanbieden blijft ver achter in vergelijking met landen om ons heen. Hoe dit komt, is niet duidelijk.
Uit de interviews blijkt dat de in Nederland opgeslagen historische verkeers- en locatiegegevens betreffende internetverkeer, zoals omschreven in bijlage B behorende bij artikel 13.2a Tw, weinig worden gebruikt. De geïnterviewde professionals en experts geven aan dat een aanzienlijk deel van de opgeslagen en bewaarde gegevens over internetverkeer slechts van beperkte waarde is bij het opsporen van nieuwere vormen van criminaliteit, waarbij het internet een rol speelt. Hierdoor worden onder de huidige regelgeving gegevens opgeslagen die niet of nauwelijks door opsporingsdiensten worden opgevraagd.
Tegelijkertijd echter blijkt volgens de experts dat het kennisniveau bij de politie niet zodanig is dat de beschikbare IP-verkeersgegevens volledig kunnen worden benut. Het blijkt complexe materie en daarnaast behoort het internet, en het optimaal gebruiken van digitale gegevens, nog niet tot de dagelijkse praktijk van alle door ons geïnterviewde personen die zich bezighouden met de opsporing en vervolging van strafbare feiten.
Van de opgevraagde gegevens blijken, naast het lokaliseren van een telefoon aan de hand van dataverkeer, vooral de tenaamstellingen van IP-adressen van grote waarde te zijn voor de opsporing. Voor opsporingsdoeleinden wil de politie regelmatig weten wie de gebruiker is van een bepaald IP-adres. Bij vaste IP-adressen – doorgaans thuisaansluitingen die op naam zijn geregistreerd bij de aanbieders – levert het identificeren van een gebruiker geen problemen op, omdat de Wet bewaarplicht voorziet in deze gegevens. Maar het achterhalen van een gebruiker van mobiel internet vormt wel regelmatig een probleem waarvoor de Wet bewaarplicht geen oplossing biedt. Dit wordt veroorzaakt doordat veel gebruikers inloggen op een zogenaamde hotspot. Dit is een wifi-netwerk waarbij ingelogde toestellen gebruik kunnen maken van het internet. Bij een wifi-netwerk worden alle gebruikers onder één IP-adres geschaard, waarmee ze kunnen acteren op het internet. Hierdoor zijn individuele gebruikers niet te achterhalen. Overigens vallen veel aangeboden wifi-netwerken niet onder de huidige bewaarplicht, omdat deze niet als openbaar kunnen worden aangemerkt.
Ook het tekort aan IPv4-adressen blijkt een groeiend knelpunt. Door dit tekort worden IPv4-adressen door aanbieders aan meerdere klanten tegelijk toegewezen, hetgeen ook problemen oplevert bij de identificatie van een individuele gebruiker. De Wet bewaarplicht voorziet hierdoor steeds minder in de vraag betreffende de identificatie van een gebruiker van een IP-adres. Dit is overigens niet verwonderlijk, omdat de Telecommunicatiewet is

geschreven in een tijdperk waarin de wereld van de telecommunicatie er nog heel anders uitzag dan nu. De lijst van te bewaren gegevens in de bijlage behorende bij artikel 13.2a Tw blijkt inmiddels gedateerd te zijn en is ingehaald door technologische ontwikkelingen. Hierdoor is een situatie ontstaan waarbij gegevens van burgers worden opgeslagen die niet of nauwelijks door opsporingsdiensten worden gebruikt. Een herbezinning op de regeling betreffende IP-verkeer en de te bewaren gegevens lijkt dan ook op haar plaats.

Wettelijke waarborgen/privacy
Mobiele telefonie heeft een enorme vlucht genomen en tegenwoordig hebben veel mensen een smartphone. Dit multifunctionele apparaat, dat ook toegang geeft tot het internet, is niet meer weg te denken uit het dagelijks leven. Hierdoor is de gedetailleerdheid waarmee een analyse van telefoon- en internetgegevens inzicht kan geven in iemands leven, de afgelopen jaren sterk is toegenomen. Met behulp van verkeersgegevens is het mogelijk een beeld te schetsen van het sociale netwerk waarin iemand zich beweegt. De opgeslagen locatiegegevens kunnen inzichtelijk maken waar iemand zich bevond op de momenten dat er met het toestel werd gecommuniceerd. Als er gecommuniceerd wordt met een smartphone, is uit de bewaarde gegevens niet alleen af te leiden met wie, hoe lang en vanaf welke locatie er contact is gelegd, maar ook op welke momenten en vanaf welke locaties er contact is gelegd met het internet. Daarmee is de privacygevoeligheid van verkeers- en locatiegegevens in de loop der jaren toegenomen.
Het bewaren van deze gegevens kan op twee manieren inbreuk maken op de privacy. Allereerst neemt door het louter opslaan van die gegevens het risico toe dat onbevoegden – zoals hackers – toegang krijgen tot die gegevens. Een tweede en andersoortige inbreuk vindt plaats op het moment dat politie en justitie de beschikking krijgen over bewaarde gegevens in het kader van een onderzoek. In het jaar 2012 zijn 56.825 vorderingen gegevensverstrekking bij de ULI verwerkt. Echter, de wijze van administreren geeft geen inzicht in het feitelijke aantal keren dat er gegevens worden geleverd, het aantal personen waarop deze verzoeken zich richten en het aantal en de aard van de zaken waarbij dit opsporingsmiddel wordt ingezet. Daardoor is het ook moeilijk te achterhalen bij hoeveel personen inbreuk wordt gemaakt op de privacy door de inzet van dit opsporingsmiddel. Daarnaast is het niet bekend hoe vaak de ingediende vorderingen betrekking hebben op gegevens die onder de bewaarplicht vallen. Hiervoor dienen de managementsystemen van de ULI zodanig te worden aangepast dat hierover betrouwbare gegevens kunnen worden gegenereerd. De uitgave van het *Platform for Electronic Data Retention for the Investigation, Detection and Prosecution of Serious Crime* kan als leidraad dienen bij het publiceren van de jaarlijkse cijfers en bij een herin-

richting van de database.[119] Hierin wordt onder andere geadviseerd om niet alleen het aantal vorderingen, maar ook het aantal antwoorden van aanbieders te tellen, door bij te houden hoe vaak een antwoord negatief is – in de zin dat de gevraagde gegevens niet achterhaald kunnen worden – of geen informatie bevat.
Een vaak genoemd alternatief voor de bewaarplicht van verkeersgegevens waarbij de privacyschending minder omvangrijk is, is het gericht bevriezen van gegevens. Dit blijkt echter geen gelijkwaardig alternatief te zijn voor een algemene bewaarplicht, omdat hiermee geen gegevens opgevraagd kunnen worden die langer geleden zijn vastgelegd. Om gebruik te kunnen maken van deze gegevens dient men al van tevoren – op het moment dat de gegevens nog aanwezig zijn en bevroren kunnen worden – te weten welke gegevens op een later tijdstip nodig zijn. Aangezien misdrijven soms pas laat ter kennis van de politie komen, en verdachten soms pas lang nadat een misdrijf heeft plaatsgevonden worden opgespoord, is het noodzakelijk gegevens te bewaren om deze later te kunnen gebruiken in het opsporingsproces.
Om te waarborgen dat de gegevens volgens de Wet bewaarplicht correct worden opgeslagen, beveiligd en vernietigd – en daarmee het risico dat onbevoegden toegang kunnen krijgen tot de gegevens wordt verminderd – hebben aanbieders en telecombedrijven de wettelijke verplichting om technische en organisatorische maatregelen te nemen om misbruik van de opgeslagen gegevens te voorkómen en zijn ze verplicht de bewaarde gegevens te vernietigen na afloop van de bewaartermijn. Daarnaast hebben klanten van de aanbieders het recht op kennisneming van de gegevens die over hen worden bewaard. Echter, de twee voor dit onderzoek ingediende verzoeken om inzage van eigen verkeers- en locatiegegevens werden niet of nauwelijks gehonoreerd.
Het toezicht op naleving van de genoemde verplichtingen van de aanbieders en telecombedrijven ligt bij het AT en daarmee uiteindelijk bij de Minister van Economische Zaken. Ook het College Bescherming Persoonsgegevens heeft een controlerende rol en ziet toe op alle wettelijke regelingen waarin sprake is van het bewaren, gebruiken of verwerken van persoonsgegevens.
De toegang tot en het gebruik van verkeersgegevens door opsporingsdiensten vormt onomstotelijk een inbreuk op de privacy van burgers. Deze inbreuk moet noodzakelijk zijn en voldoen aan eisen van proportionaliteit en subsidiariteit. In het Wetboek van Strafvordering is daarom geregeld wie onder welke voorwaarden toegang heeft tot de opgeslagen telecom- en internetgegevens. Bovendien is hierin vastgelegd dat betrokkenen over wie verkeersgegevens zijn opgevraagd, hierover dienen te worden ingelicht zodra het

119 http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/data-retention/experts-group/docs/guidance_on_statistics_position_paper_16_datret_final_en.pdf (geraadpleegd op 20 maart 2013).

belang van het onderzoek dit toelaat. Er ligt echter een conceptwetsvoorstel[120] waarin wordt voorgesteld de notificatieplicht af te schaffen voor zover het gaat om het vorderen van verkeersgegevens, omdat wordt verondersteld dat deze bevoegdheid 'een relatief lichte inbreuk' op de privacy meebrengt. Deze redenering wringt met het feit dat door de enorme vlucht die het gebruik van de mobiele telefoon heeft genomen, de gedetailleerdheid waarmee een analyse van telefoon- en internetgegevens inzicht kan geven in iemands leven, in de afgelopen jaren sterk is toegenomen.

Opslag, beveiliging en toezicht
De bewaarplicht heeft betrekking op het opslaan van privacygevoelige gegevens waaruit informatie kan worden afgeleid over verblijfslocaties en contacten van personen. Hierdoor is goed toezicht op de uitvoering van de Wet bewaarplicht een vereiste. Hiermee kan worden voorkómen dat de gegevens in verkeerde handen vallen of dat ze oneigenlijk worden gebruikt.
In Nederland worden de verkeersgegevens die op grond van de Wet bewaarplicht moeten worden opgeslagen, decentraal bewaard bij de aanbieders zelf, die verantwoordelijk zijn voor de opslag, beveiliging en vernietiging van deze gegevens. Deze informatie kan voor opsporingsdoeleinden door opsporingsdiensten worden opgevraagd bij de aanbieders via de ULI. De opvraagbare telefoongegevens kunnen in Nederland tot een jaar voorafgaand aan de datum van de vordering beschikbaar worden gemaakt; de opvraagbare internetgegevens tot een halfjaar voorafgaand aan die datum.
Het AT treedt op als toezichthouder, maar heeft enkel de mogelijkheid om toe te zien op de juiste uitvoering van bedrijfsprocessen. Het AT beschikt niet over de bevoegdheden die nodig zijn om op de inhoud van de bewaarde gegevens toe te kunnen zien. Wanneer een overheid besluit privacygevoelige informatie van burgers op te slaan en te bewaren, hoort daar solide en effectief toezicht bij, zowel op de inhoud van de gegevens die worden bewaard als op de gegevens die uiteindelijk aan de opsporingsdiensten worden geleverd. Het is echter zo dat in de huidige situatie het AT de geleverde verkeersgegevens, op grond van artikel 18.7, tweede lid Tw, niet kan inzien en controleren. Het verdient daarom aanbeveling om de rol van de toezichthouder op dit vlak te heroverwegen.

De bewaartermijnen
De bewaartermijnen voor verkeers- en locatiegegevens van telefoonverkeer bedraagt een jaar. Deze termijn wordt door de geïnterviewde professionals en experts heel werkbaar gevonden. In sommige gevallen blijkt een jaar te kort om een onderzoek goed te kunnen uitvoeren, maar dit is eerder uitzondering dan regel, en de geïnterviewde professionals en experts vragen zich af

120 Conceptwetsvoorstel tot wijziging van het Wetboek van Strafvordering en het Wetboek van Burgerlijke Rechtsvordering in verband met de versterking van het presterend vermogen van de politie. Zie www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2012/09/03/consultatieversie-conceptwetsvoorstel.html (geraadpleegd op 1 mei 2013).

hoe lang gegevens bewaard zouden moeten worden om ook deze zaken te kunnen oplossen. Uiteindelijk gaat het om privacygevoelige gegevens die je niet onnodig lang ergens wil opslaan.
De geldende termijn voor historische internetverkeersgegevens bedraagt zes maanden. Het is niet helemaal duidelijk op grond van welke argumenten in het verleden is besloten de bewaartermijnen voor telefoon- en internetverkeersgegevens van elkaar te laten verschillen. Hieraan zouden onder andere privacyargumenten ten grondslag liggen. Echter, door de aard van de huidige bewaarde gegevens wordt met de opslag van internetgegevens geen grotere inbreuk gemaakt op de persoonlijke levenssfeer van gebruikers dan met de opslag van gegevens over telefoonverkeer. Bij internetverkeersgegevens gaat het immers alleen om informatie waaruit de locatie van een internetcontact kan worden afgeleid en over het IP-adres dat werd gebruikt. Enkel bij het opvragen van e-mailverkeer wordt inzichtelijk gemaakt met wie een persoon contact heeft gelegd. Dit in tegenstelling tot gegevens over telefoonverkeer, waarmee, indien gebruik wordt gemaakt van de telefoon, een sociaal netwerk in kaart gebracht kan worden gebracht.
De bewaartermijn van zes maanden wordt door de professionals en experts die optreden in opsporingszaken waarbij deze gegevens van belang kunnen zijn, unaniem als te kort ervaren. Juist bij de ingewikkelde zaken waarbij deze gegevens een rol kunnen spelen, zijn de gegevens volgens de geïnterviewde professionals en experts te kort beschikbaar. Het betreft dan vooral gegevens die kunnen worden ingezet bij het identificeren van een gebruiker van een IP-adres.
Gezien het feit dat de omvang van het dataverkeer in de toekomst zal toenemen terwijl het telefoonverkeer vermoedelijk verder zal afnemen – en gezien het feit dat de bewaarde telefoon- en internetverkeersgegevens met de huidige regelgeving geen duidelijk verschillende inbreuk maken op de privacy van burgers en in de opsporing deels op dezelfde wijze worden gebruikt (zeker als het gaat om Smartphones) – zou een gelijkstelling van de bewaartermijnen voor de hand liggen. Het gelijkstellen van de bewaartermijnen zou een oplossing bieden voor een aantal technische en praktische problemen waar aanbieders op dit moment tegenaan lopen en de wet zou in dat geval op dezelfde wijze kunnen worden toegepast voor alle vormen van mobiel of prepaid internet. De huidige wetgeving lijdt tot inconsequent beleid waar het gaat om internetverkeersgegevens die gegenereerd zijn door prepaid kaartjes versus gegevens die door abonnementhouders zijn gegenereerd. Voor abonnementhouders geldt een bewaartermijn van een halfjaar; voor gebruikers van prepaid kaartje een termijn van een jaar. Dit verschil vloeit voort uit het feit dat de wetgeving betreffende de bewaartermijnen voor prepaid telecommunicatiegegevens, wordt beschreven in artikel 13.4 lid 3 Tw.
Voor verschillende telefoniediensten als traditionele telefonie, mobiele telefonie en internettelefonie (VoIP), waarbij de overheid heeft gekeken naar een gelijke functionaliteit en de belangrijkste kenmerken, geldt een bewaarter-

mijn van twaalf maanden. Dit terwijl het bij internettelefonie strikt genomen om internetverkeersgegevens gaat. Hiervoor wordt in de wet een bewaartermijn van zes maanden genoemd. Dit is verwarrend, vooral omdat op het internet ook spraakdiensten worden aangeboden die weer onder de bewaartermijn van zes maanden vallen. Zo is het ook voor aanbieders van communicatiediensten niet altijd duidelijk of ze wel of niet bewaarplichtig zijn.

Algemeen
Het gebruiken van verkeersgegevens in de opsporing kan gekarakteriseerd worden als een 'traditionele' manier van opsporen. De huidige opsporingspraktijk leunt nog zwaar op deze traditionele opsporingsmethode, waarmee overigens nog steeds veel bruikbare informatie over menselijke contacten kan worden achterhaald.
Door de voortschrijdende technische ontwikkelingen is de huidige bewaarplicht voor internetgegevens grotendeels achterhaald. De wet is geschreven in een tijdperk dat men inlogde op het internet met een modem, terwijl veel mensen tegenwoordig 24 uur per dag, 7 dagen in de week online zijn. De lijst van te bewaren gegevens in de bijlage behorende bij artikel 13.2a Tw is gedateerd, waardoor gegevens van burgers worden opgeslagen die niet of nauwelijks door opsporingsdiensten worden gebruikt. Dit is een onwenselijke situatie.
Het strikte onderscheid tussen telefonie en internet zoals deze in de huidige Wet bewaarplicht wordt gehanteerd, is niet meer van deze tijd en dit zorgt voor onduidelijkheden en technische en praktische problemen. Een zorgvuldige heroverweging van de regeling, de bewaartermijn en in het bijzonder de te bewaren gegevens betreffende IP-verkeer lijkt dan ook op haar plaats. Met het aanpassen van de te bewaren internetverkeersgegevens is onlosmakelijk een zorgvuldige heroverweging van de bewaartermijn verbonden. De privacygevoeligheid van de nieuw op te nemen gegevens in de Wet bewaarplicht dient daarbij een doorslaggevende rol te spelen.
Tegelijkertijd ziet het er echter naar uit dat met het opvragen van telecommunicatiegegevens in de toekomst steeds minder nuttige informatie kan worden opgevraagd. Andere vormen van communicatie, bijvoorbeeld via sociale media en via games, vallen buiten de bewaarplicht en kunnen niet worden achterhaald. De huidige wetgeving sluit niet aan bij deze ontwikkelingen en het is onwaarschijnlijk dat 'lokale' Nederlandse wetgeving dit kan ondervangen en zinvol is in de grens- en locatieloze ruimte van het internet. Gezien het grensoverschrijdende karakter van veel vormen van criminaliteit is Europese harmonisatie betreffende de bewaartermijnen en het opvragen van gegevens gewenst, maar ook Europese harmonisatie biedt geen antwoord op alle mogelijkheden en uitdagingen die de virtuele ruimte biedt. Een ruime uitbreiding van de bewaarplicht naar mogelijkheden voor het gebruik van internetverkeersgegevens om daarmee de opsporing slagvaardiger te maken is een vanuit het 'veiligheidsdenken' aangestuurde gedachte. Vanuit

het perspectief van de privacy van de burgers is dit echter een ongewenste ontwikkeling. Bovendien zal de beschikbaarheid van veel persoonsgebonden inhoudelijke informatie niet alleen opsporings- en veiligheidsautoriteiten, maar ook derden gretig maken om toegang te krijgen tot dergelijke data. De opslag van dit soort gegevens brengt daarom een groter misbruikrisico met zich mee. Bovendien betekent het beschikken over meer gegevens niet per se dat de opsporing efficiënter wordt, omdat door meer gegevens ook meer ruis wordt veroorzaakt, wat een efficiënte opsporing kan bemoeilijken. Het zoeken naar een alternatief voor de algemene bewaarplicht, waarmee enerzijds de opsporing van misdrijven waarbij communicatie plaatsvindt via internet kan worden gediend en anderzijds de privacy zo min mogelijk wordt geschonden, is een fikse uitdaging. Echter, het ontwikkelen van opsporingsmogelijkheden voor het bestrijden van nieuwe vormen van criminaliteit zal ons in de toekomst vaker voor uitdagende en complexe vraagstukken stellen, waarbij dilemma's keer op keer zorgvuldig dienen te worden afgewogen.

Summary

The Dutch implementation of the Data Retention Directive

On the storage and use of telephone and internet traffic data for crime investigation purposes

The study: background, research questions and data collection

Background to the research questions

The Dutch implementation of the Data Retention Directive was adopted at the 1th of September 2009. The main reason for the storage of call detail records of telephony and internet traffic data is that the data may be helpful in the investigation and prosecution of serious crimes. This data can be used, for example, to ascertain the time and place at which a certain mobile telephone was used to make a call. It is also possible to find out whether and when a computer or mobile telephone made an internet connection. Telecommunication traffic data can be used in cases involving a crime that merits pre-trial detention, a reasonable suspicion of a crime being planned or committed in an organised context and indications of a terrorist offence.
However the fact that this data has to be stored for a certain period of time is a recurring point of debate. There is a need both in the Netherlands and at European level (EU 18620/11) for a clearer understanding of how the police and judicial authorities use the data kept under the Telecommunications Data (Data Retention Directive) Act (referred to below as 'the Act'.

The purpose of this study is to clarify how the Act works in practice. This study does not strictly take the form of an evaluation. It extends beyond the scope of a process evaluation (cf. Wartna, 2005; Nelen et al., 2010), because there is a need not only for an understanding of how the Act has been shaped in practice but also of how the data to be kept available under this Act is actually used for criminal investigations in practice.
It is not however possible – as it would be in a product or effect evaluation – to ascertain how the introduction of the Act has affected the use of traffic data in criminal investigations. The telecommunication data at issue here was already available for criminal investigation purposes before the Act was introduced, and was already being used in criminal investigations into serious crimes prior to the introduction of the Act.
Although the Act has resulted in the retention periods being harmonised, the fact that other changes have taken place in the meantime means that it is only barely possible to measure and identify the effects of this. Changes in how telecommunication data is used in practice can be attributed primarily to the emergence of the mobile telephone and the smartphone and to the ability of people to use the internet to communicate with each other. It is

therefore possible to look into how telecommunication data is used in criminal investigations, but it is less easy to relate the findings to the introduction of the new Act.
This study focuses both on questions about how the Act has been given shape and questions about how the retained data is used in practice.

Various organisations and parties are involved in storing, maintaining and using telephone and internet traffic data for criminal investigation and prosecution purposes. The providers are required to retain and secure the data, keep it available for criminal investigation purposes and to destroy it at the prescribed time. This process is regulated by the Radiocommunications Agency Netherlands (Agentschap Telecom). The Dutch Data Protection Authority has the more general task of regulating the use of privacy sensitive data. The Police and Public Prosecution Service use this data for the investigation and prosecution of serious crime, and the judiciary uses it in the legal decision-making process. This report focuses relatively sharply on how the stored data is used in practice, thus providing a clearer understanding of the usefulness and necessity of the retention obligation. How the Act works in practice is a complex issue, which is reflected in this report by describing how the various parties perform their tasks. This report provides fairly detailed information about how the stored data is used in practice. Other parties are touched upon, but do not form the main focus of this study.

Data collection

Various methods have been used to answer the research questions. As well as studying national and international professional literature, quantitative and qualitative information on the use of historical traffic data has been collected. Data has been collected from organisations such as the National Interception Unit of the national police, the Dutch National police, the judiciary (Public Prosecution Service) and the legal profession. A desk study was also carried out, which involved examining legal texts and their explanatory notes, secondary legislation, parliamentary papers, written documents of implementing agencies and scientific literature.
Seventeen face-to-face interviews and 16 telephone interviews were conducted for the study, which involved speaking to a total of 41 people in the period from June to October 2012. Additionally, court judgements were analysed to ascertain how the Dutch courts had used data kept available under the Act for criminal investigation purposes as evidence in criminal trials.

Remote communication, developments and implications

In recent years the mobile telephone has been replaced by the smartphone, and many people are online 24/7 these days. The use of smartphones means that people are much more likely to communicate in the form of short messages via apps and email, and phone calls are being made increasingly online as well.
Technological innovations and the accompanying fragmentation of communication and the use of various online services makes it difficult to keep track of all of a person's remote communication. Additionally, not all traffic data that is generated comes under the Act. Many internet users have email accounts with webmail services such as Hotmail, Gmail or Yahoo, which are provided by a foreign company. Consequently, the data is not necessarily retained for Dutch criminal investigation purposes. The same applies to providers of services in the *cloud*. In cases where investigative services none the less want to obtain traffic data from foreign suppliers they need to submit a request for legal assistance and have to wait and see whether the data is still available.

The legislative history and European regulations on the Data Retention Directive

Partly in response to the terrorist attacks in Madrid in 2004 and in London in 2005, 3 May 2006 saw the introduction of the EU Directive aimed at guaranteeing that certain telecom and internet data are retained and kept available for the investigation and prosecution of serious crime.

Retained data

Section 5 of the Directive stipulates the categories of data to be retained with regard to aspects including the designation, the date, the time and the duration of the communication. It is not permitted to retain data from which the content of the communication can be derived. The Member States were required to convert the Directive into national legislation by 15 September 2007; an extension was given until 15 March 2009 for the obligation to retain internet data. Not all the Member States have converted the directives into legislation. The term 'serious crime' has not been defined in the directives. This is reflected in the various grounds laid down in the legislation of the Member States that facilitate access to the retained data for criminal investigation and prosecution purposes. As with the duration of the retention period, the harmonisation envisaged by the EU legislation has only been achieved to a limited extent.

Privacy

The Act affects the privacy of members of the public. In the first place, the storage of telecommunication data involves a risk of unauthorised persons – such as hackers – gaining access to that data. A second, different type of breach takes place as soon as the police and judicial authorities are granted access to retained data in the context of an investigation. According to the ECHR it is permissible to limit the right to privacy only if provided for by law and necessary in a democratic society.
The Netherlands Penal Code stipulates who has access to the retained telecom and internet data and under which conditions. The Public Prosecutor can claim the issue of traffic data (Sections 126n and 126u of the Netherlands Penal Code) if there is a suspicion of an offence that merits pre-trial detention or a reasonable suspicion that crimes are being planned or committed in an organised context. An investigating officer can claim identifying data (Sections 126na, 126ua, of the Penal Code). The details that can be obtained are what are known as the user details (name, address, place of residence, number and type of service). If there are indications of a terrorist offence, the Public Prosecutor can obtain traffic data (Section 126zh of the Penal Code) and an investigating officer can claim user data (Section 126zi of the Penal Code). For an exploratory investigation into terrorist offences the Public Prosecutor can also claim databases of public and private bodies in order to have their details processed (Section 126hh of the Penal Code)

The retention and securing of the data in practice

The regulatory authorities

Compliance with the rules is supervised by the Radiocommunications Agency Netherlands, which operates as an independent regulatory authority and supervises compliance with the Act. The Radiocommunications Agency is a division of the Ministry of Economic Affairs and reports directly to the Minister of Economic Affairs. Additionally, the Dutch Data Protection Authority regulates all statutory regulations concerning the retention, use and processing of personal data.

The providers

Meetings were held with four providers in order to gain an understanding of how they approach the obligations under the Act. Prior to the retention obligation being introduced the retention periods varied between companies. Despite the Act's long start-up period, its implementation proved to be a sizeable project for the large providers.

At the two large suppliers interviewed for this investigation, a database is filled with data to be retained under the Act. This data is automatically destroyed when the retention period ends. A small provider interviewed for this study only recently actively started operating the retention periods because the quantity of data to be retained became too large. When they receive a request, the data applied for has to be taken manually out of the system by an employee.
The government has concluded an agreement with the large Dutch suppliers concerning remuneration for the personnel deployment needed to issue data retained under the various Acts and regulations to the government. Small providers are not covered by this arrangement.
The owners of a fourth interviewed supplier recognise themselves in the documentation of the Radiocommunications Agency as parties obliged to retain the traffic data of the email services they offer, but indicate that they do not comply with this for idealistic reasons. The researchers have asked the Radiocommunications Agency whether the services offered by this company are subject to the retention obligation. According to the Radiocommunications Agency they are not, but it acknowledges that certain parts of the legislation have become unclear owing to technological innovations.

Regulatory authority

The Radiocommunications Agency also oversees the implementation of operational processes. The supervision is provided for in a regulatory cycle in which the data suppliers are questioned about how they retain, secure and destroy the data. The Radiocommunications Agency does not however have the instruments and powers to regulate the content of the retained and delivered data. Section 18.7 (2) of the Dutch Telecommunications Act expressly stipulates that the regulatory authority is not authorised to retrieve traffic or location data retained by the providers under Section 13.2a of the Telecommunications Act.

The use of historical traffic data in practice

The Act makes a clear distinction between telephony and internet traffic data. To be perfectly clear, this report maintains that distinction. But in practice the distinction has virtually faded away and experts feel that the Act operates an incorrect division into two categories.

What is retained?

The annex to Section 13.2a of the Telecommunications Act contains a summary of the telephone data to be retained. This data includes the number of

the caller and the party called, the time and duration of the call and the location. This data must be kept for a period of 1 year. The content of a call or an SMS is not subject to the retention obligation. The traffic data of the sent or received message is subject to that obligation. Attempted calls in which no connection is made come under the retention obligation, too.

What is at stake

According to crime investigation professionals historical traffic data is retrieved in virtually all larger criminal investigations in which suspects or victims may have used their telephone. In 2012 the number of claims for the issue of telecommunication data totalled 56,825.
These claims were used to obtain information about the use of the telephone and possible IP-traffic, such as: the number that was used to make the call, when the call was made, the duration of the call and from which location, and whether there was any online contact. This information plays an important and highly valued role in criminal investigations. If an investigating team wants to obtain traffic data it has to obtain the approval of the Public Prosecutor. The investigating team has to indicate what it is seeking to achieve with the information, and obtaining the information must be proportional and observe the principal of subsidiarity. The intentions of the investigating teams in obtaining traffic data can be placed in a number of categories: (1) to identify a user, (2) to establish contacts, (3) to determine a location, (4) to trace an IMEI number, and (5) to make a decision on capacity before intercepting.

Relevance and retention period of telephony data

All of the interviewed professionals and experts said that they found historical data on telephone traffic to be highly relevant. A number of interviewed crime investigation professionals indicated that they wanted to obtain not only the start location (*first cell*) of a telephone call, but also the end location (*last cell*). However, the call ends, i.e. the final connection with a transmitter mast, is not stated in the annex to Section 13.2a of the Telecommunications Act.
It emerged from the interviews that most of the professionals and experts among the police felt that the one-year retention period is sufficient for the work that they do.

Historical internet traffic data

What is retained?

Historical traffic data concerning internet and email usage can yield information about matters such as the IP addresses someone has used, and the email contacts of the sender and receiver. The content of calls, messages or emails and search terms entered in a search engine and the IP addresses of searched internet pages are not covered by the retention obligation.

Relatively little deployment

It became clear during the interviews conducted for this study that the criminal investigation professionals had little or no knowledge of how historical data concerning internet traffic could be used for crime investigation purposes. Additionally, the work related to internet matters is often carried out by experts because the digitisation of today's society does not yet form part of the day-to-day work of many investigating officers. At the same time we established that technological developments move at a very fast pace. So fast that it is difficult even for the scarce experts to keep pace with them.
Historical internet traffic data is often retrieved in response to a crime or offence committed with the aid of or via the internet, such as sending threatening emails, internet fraud, human trafficking and the distribution of images of child sex abuse. The most important reason given for retrieving data is to *identify a user* or a connection. Fixed IP addresses usually remain unchanged for longer periods and the use can easily be traced either at the provider or at the Central Telecommunications Investigation Information Point. However identifying a mobile internet user on the basis of historical traffic data is a laborious process and in many cases not possible.

The relevance and retention period of internet data

According to various experts the majority of the internet data described in the annex to Section 13.2a of the Telecommunications Act is outdated. The regulation is no longer in keeping with today's internet usage or with the technological developments that have taken place in this area since the Telecommunications Act was introduced in 2009. This has led to the retention of data of members of the public that is not or is only barely used by the criminal investigation services. A meticulous review of the regulation governing IP traffic and the retention of IP data therefore appears appropriate.
The professionals and experts interviewed for this study and who are familiar with the internet traffic data all believe that the 6-month retention period is too short; there is clearly a need for IP traffic data that goes back further in time for criminal investigations into offences for which this data is retrieved.

The retrieval of transmission mast data

Retrieving traffic data based on a location yields information about all mobile telephones which, in the indicated time frame, have been called, have made calls or had an internet connection via the mast location in question. For permission to retrieve transmission mast data there must be a suspicion of an offence as specified in Section 67 (1) of the Netherlands Penal Code and the use of the data must be in the interest of the investigation.
Transmission mast data is retrieved mainly for serial offences. In such cases the data of various locations is compared with the aim of pinpointing a recurring number. Of course, this detection method only has a chance of success if the suspect used his telephone around the time of the offence.

Alternative?

Opponents of the retention obligation regard the targeted freezing of data as being a less privacy-violating solutions because this involves a specific data set that is retained for longer rather than retaining all the data of all of a provider's customers. None of the experts we spoke to felt that freezing data was a comparable or equivalent alternative to a general retention obligation because this would rule out the possibility of retrieving data retained a longer time ago. To be able to use this data it is necessary to know in advance – when the data is still available and can be frozen – what data will be needed at a later date. Given that it is sometimes not until later that offences come to the knowledge of the police, and suspects are sometimes not identified until long after a crime has been committed, it is necessary to retain this data for later use in the criminal investigation process.

The use of traffic data in figures

The Telecommunications Act makes it compulsory to publish the number of enquiries about telecommunications traffic made by criminal investigation services each year (Section 13.4 (4) of the Telecommunications Act. In 2012 a total of 56,825 claims for the issue of traffic data were made. However the number of claims announced by the Minister also includes data not covered by the Telecommunications Data (Retention Obligation) Act.
It should also be noted that the retrieval of telecom data in the Netherlands is registered by telephone number, IMEI number, IP address or 'mast location' on which data is retrieved. These figures do not provide an insight into the number of people whose telecommunication data is retrieved each year, or the number of criminal investigations or the nature of the investigations for which the data was retrieved. Neither do the figures provide any insight into the extent to which a claim has actually resulted in data being issued.

Court judgements

This report also provides an insight into the use and value of traffic data in court judgements. A total of 74 rulings were found between July 2012 and February 2013 in which the term historical traffic data concerning telephony occurred. This data was generally used in the rulings to demonstrate 'contact between suspects' and 'locations'.
A search for cases in which IP traffic data was used in the judgement revealed 26 judgements in the period from January 2009 to February 2013. This IP data was mentioned mainly in the rulings on criminal investigations into images of child sex abuse. More than half of the judgements concerned the downloading and/or distribution of images of child sex abuse. The retrieval of this data is not so much about where the suspect was and with whom he communicated, but sooner whether the suspect can be linked to the internet address that was used or other user data.

Literatuur

Agentschap Telecom (2010). *Eindrapport Nulmeting Wet bewaarplicht telecommunicatiegegevens*. Geraadpleegd op 1 juni 2013: www.eerstekamer.nl/behandeling/20100817/_eindrapport_nulmeting_wet/f=y.pdf.

Agentschap Telecom (2012). *Staat van de Ether*. Geraadpleegd op 29 juni 2013: www.agentschaptelecom.nl/onderwerpen/frequentiemanagement/staat-van-de-ether.

Agentschap Telecom (z.j.). *Opslag telecomgegevens*. Geraadpleegd op 4 april 2013: www.agentschaptelecom.nl/onderwerpen/veiligheid/opslag-telecomgegevens.

Arbeitskreis Vorratsdatenspeicherung (2011a). *Report on data retention and serious crime in Germany*. Geraadpleegd op 7 december 2012: www.vorratsdatenspeicherung.de.

Arbeitskreis Vorratsdatenspeicherung (2011b). *German police statistics prove telecommuncations data retention superfluous*. Geraadpleegd op 7 december 2012: www.vorratsdatenspeicherung.de/content/view/455/55/lang,en.

Bits of freedom (2012). *Ons advies aan ministerie voor evaluatie bewaarplicht*. Geraadpleegd op 1 december 2013: www.bof.nl/2012/06/25/ons-advies-aan-ministerie-voor-evaluatie-bewaarplicht.

Boot, R., Van der Bosch, J. Vervaet, E., & Varkevisser, K. (2006). *Onderzoek naar de nationale implementatie van de Europese richtlijn dataretentie*. Verdonck, Klooster & Associates. Geraadpleegd op 1 juni 2013: www.eerstekamer.nl/behandeling/20081209/onderzoek_naar_de_nationale/f=y.pdf.

Chipchase, J. (2007). *Jan Chipchase over mobiele telefoons*. Geraadpleegd op 7 december 2012: www.ted.com/talks/jan_chipchase_on_our_mobile_phones.html.

DatRet/Expgrp (2009). Position Paper No 5. Closer understanding of the term'Internet Telephony' in relation to its application in Directive 2006/24/EC. Geraadpleegd op 20 maart 2013: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/pdf/series_a_position_paper_5_final_14_07_2010_closer_understanding_of_the_term_internet_telephony_en.pdf.

DatRet/Expgrp (2012). *Position Paper No. 16: Guidance on the Member States obligation to submit to the Commission annual statistics pursuant to Directive 2006/24/EC*. Geraadpleegd op 20 maart 2013: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/data-retention/experts-group/docs/guidance_on_statistics_position_paper_16_datret_final_en.pdf.

Electronic Frontier Foundation (2012). *Mandatory Data retention: Europe*. Geraadpleegd op 7 december 2012: www.eff.org/issues/mandatory-dta-retention/eu.

Europese commissie (2011). *Verslag van de Commissie aan de Raad en het Europese Parlement. Evaluatie van de richtlijn gegevensbewaring (Richtlijn 2006/24/EG)* . http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:nl:PDF.

Frost & Sullivan (2010). *Meeting the challenges of data retention: Now and in the future*. Geraadpleegd op 1 december 2012: www.frost.com.
Google. *Transparantierapport*. Geraadpleegd op 13 maart 2013: www.google.com/transparencyreport/userdatarequests/legalprocess.
Google. *Transparantierapport*. Geraadpleegd op 19 maart 2013: www.google.com/transparencyreport/userdatarequests/NL.
Handelingen I 2008/09, 39, p. 1808.
Handelingen I 2008/09, 40, p. 1839 e.v.
Handelingen I 2008/09, 40, p. 1845.
Hathaway, M.E. (2012). *Preliminary considerations: On national cyber security*. In Klimburg, A. (red.), *National Cyber security framework manual* (pp. 1-43). Tallin, Estland: NATO Cooperative Cyber Defence Centre of Excellence.
Hustinx, Peter (2010). *The moment of truth for the Data Retention Directive*. Presentatie op conferentie 'Taking on the Data Retention Directive', Brussel, 3 december 2010.
ICT-recht (2011). *Overzicht bewaarplicht wie wel en wie niet*. Geraadpleegd op 4 april 2013: https://ictrecht.nl/ictrecht/overzicht-bewaarplicht-wie-wel-en-wie-niet.
ITU (International Telecommunication Union) (2011). *World telecommunication/ICT indicators database* (15e editie).
Kamerstukken I 2007/08, 31 145, B.
Kamerstukken I 2008/09, 31 145, F.
Kamerstukken I 2008/09, 31 145, F (NMvA).
Kamerstukken I 2008/09, 31 145, C.
Kamerstukken I 2010/11, 32 797, A.
Kamerstukken II 1989/90, 21 551, nr. 3.
Kamerstukken II 2006/07, 31 145, nr. 3.
Kamerstukken II 2007/08, 31 145, nr. 9.
Kamerstukken II 2007/08, 31 145, nr. 14.
Kamerstukken II 2009/10, 32 185, nr. 2.
Kamerstukken II 2009/10, 32 185, nr. 3.
Koops, B.J. (2002). *Strafvorderlijk onderzoek van (tele)communicatie 1838-2002: Het grensvlak tussen opsporing en privacy*. Deventer: Kluwer.
Koops, B.J., Bekkers, R., Bongers, F., & Fijnvandraat, M. (2005). *Aftapbaarheid van telecommunicatie: Een evaluatie van hoofdstuk 13 Telecommunicatiewet*. Tilburg: TILT - Centrum voor Recht, Technologie en Samenleving.
Koops, B.J., Leenes, R., Hert, P. de, & Olislaegers, S. (2012). *Misdaad en opsporing in de wolken: Knelpunten en kansen van cloud computing voor de Nederlandse opsporing*. Tilburg: TILT – Centrum voor Recht, Technologie en Samenleving.
Munnichs, G., Schuijff, M., & Bestters, M. (2010). *Databases: Over ICT-beloftes, informatiehonger en digitale autonomie*. Den Haag: Rathenau Instituut.

www.rathenau.nl/publicaties/publicatie/databases-over-ict-beloftes-informatiehonger-en-digitale-autonomie.html.
Mevis, P.A.M et al. (2005). *Wie wat bewaart heeft wat: Onderzoek naar nut en noodzaak van een bewaarverplichting van historische verkeersgegevens van telecommunicatie*. Rotterdam: Erasmus Universiteit.
Nelen, H., Leeuw, F,. & Bogaerts, S. (2010) *Antiterrorisme beleid en evaluatie-onderzoek: Framework, toepassingen en voorbeelden*. Den Haag: Boom Juridische uitgevers.
Odinot, G., De Jong, D., Van der Leij, J.B.J., de Poot, C.J, & Straalen, E.K. (2012). *Het gebruik van de telefoon- en internettap in de opsporing*. Den Haag: Boom Juridische uitgevers. Onderzoek en beleid 304.
OPTA (Onafhankelijke Post en Telecommunicatie Autoriteit) (2009) *Jaarverslag en Marktmonitor*. Den Haag: OPTA.
OPTA (Onafhankelijke Post en Telecommunicatie Autoriteit) (2010). *Toezichtactie registratieplicht bij 15 internetleveranciers in de hotelbranche*. Geraadpleegd op 11 december 2012: www.opta.nl/nl/actueel/alle-publicaties/publicatie/?id=3296.
OPTA (Onafhankelijke Post en Telecommunicatie Autoriteit) (2011). *Presentatie Markt Monitor 2010*. Den Haag: OPTA.
OPTA (Onafhankelijke Post en Telecommunicatie Autoriteit) (2012). *Marktcijfers tweede kwartaal*. Den Haag: OPTA.
Rathenau Instituut (2013). *Handout ICT-commissie Tweede Kamer*. Geraadpleegd op 1 juni 2013: www.rathenau.nl/publicaties/publicatie/hand-out-ict-commissie-tweede-kamer.html.
Rijksoverheid (z.j.). *Telecomgegevens voor opsporing*. Geraadpleegd op 1 juni 2013: www.rijksoverheid.nl/onderwerpen/telecomgegevens-voor-opsporing.
Rijksoverheid (2012). *Conceptwetsvoorstel tot wijziging van het Wetboek van Strafvordering en het Wetboek van Burgerlijke Rechtsvordering in verband met de versterking van het presterend vermogen van de politie*. Geraadpleegd op 1 mei 2013: www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2012/09/03/consultatieversie-conceptwetsvoorstel.html.ith, B. (2013). *Microsoft releases 2012 law enforcement requests report* . Geraadpleegd op 25 maart 2013: www.blogs.technet.com/b/microsoft_on_the_issues/archive/2013/03/21/microsoft-releases-2012-law-enforcement-requests-report.aspx.
Staatsblad (2002). Besluit van 18 december 2001, houdende regels voor de vergaring van nummergegevens door middel van afwijkend frequentiegebruik en bestandsanalyse met het oog op het onderzoek van telecommunicatie (Besluit bijzondere vergaring nummergegevens telecommunicatie). *Staatsblad*, nr. 31.
Staatsblad (2004). Besluit van 3 augustus 2004, houdende aanwijzing van de gegevens over een gebruiker en het telecommunicatieverkeer met betrekking tot die gebruiker die van een aanbieder van een openbaar telecommu-

nicatienetwerk of een openbare telecommunicatiedienst kunnen worden gevorderd (Besluit vorderen gegevens telecommunicatie). *Staatsblad*, nr. 394.
Staatsblad (2006). Besluit van 21 december 2006, houdende voorschriften ter uitvoering van enkele bepalingen van het Wetboek van Strafvordering in verband met de opsporing van terroristische misdrijven (Besluit opsporing terroristische misdrijven). *Staatsblad*, nr. 730.
Staatsblad (2011). Wet van 6 juli 2011 tot wijziging van de Telecommunicatiewet in verband met de aanpassing van de bewaartermijn voor telecommunicatiegegevens met betrekking tot internettoegang, e-mail over het internet en internettelefonie. *Staatsblad*, nr. 350.
Stratix Consulting (2009). *Grenzen aan de aftapbaarheid?* Hilversum: Stratix.
Knol, P.C., & Zwenne, G.J. (2013). *Tekst en Commentaar 'Telecommunicatie- en Privacyrecht'*. Den Haag: Wolters Kluwer.
TNO (Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek) (2010). *Marktrapportage Elektronische Communicatie*. Delft: TNO.
TNO (Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek) (2011). *Marktrapportage Elektronische Communicatie*. Delft: TNO.
Twitter (2012). *Information requests* . Geraadpleegd op 25 maart 2013: https://transparency.twitter.com/information-requests-ttr2.
Wartna, B. (2005). *Evaluatie van daderprogramma's*. Den Haag: Boom Juridische uitgevers.
Zenger, R. (2011a). *Ik, in de ogen van T-mobile*. Geraadpleegd op 5 december 2012: https://rejo.zenger.nl/focus/ik-de-ogen-van-t-mobile.
Zenger, R. (2011b). *Locatie te achterhalen uit call detail records?* Geraadpleegd op 5 december 2012: https://rejo.zenger.nl/focus/locatie-te-achterhalen-uit-call-detail-records.

Jurisprudentie

Europese Hof voor de Rechten van de Mens (EHRM)
EHRM 4 december 2008, nr. 30562/04 (S and Marper/The United Kingdom).

Hof van Justitie van de Europese Gemeenschappen (HvJ EG)
HvJ EG 10 februari 2009, nr. C-301/06 (Ierland/Europees Parlement en Raad van de Europese Unie).

Gerechtshof
Gerechtshof 's-Gravenhage, 26 oktober 2012, ECLI:NL:GHSGR:2012:BY1648
Gerechtshof 's-Hertogenbosch, 30 mei 2012, ECLI:NL:GHSHE:2012:BW7042
Gerechtshof 's-Hertogenbosch, 2 oktober 2012, ECLI:NL:GHSHE:2012:BX9271
Gerechtshof Amsterdam, 31 oktober 2012, ECLI:NL:GHAMS:2012:BY1810

Gerechtshof Amsterdam, 6 november 2012, ECLI:NL:GHAMS:2012:BY2562
Gerechtshof Arnhem, 18 juni 2012, ECLI:NL:GHARN:2012:BW8652
Gerechtshof Arnhem, 30 augustus 2012, ECLI:NL:GHARN:2012:BX6113
Gerechtshof Arnhem, 30 augustus 2012, ECLI:NL:GHARN:2012:BX6121

Rechtbank
Rechtbank 's-Gravenhage, 5 januari 2012, ECLI:NL:RBSGR:2012:BW5833
Rechtbank 's-Gravenhage, 3 februari 2012, ECLI:NL:RBSGR:2012:BV2841
Rechtbank 's-Gravenhage, 16 april 2012, ECLI:NL:RBSGR:2012:BX0774
Rechtbank 's-Gravenhage, 14 augustus 2012, ECLI:NL:RBSGR:2012:BX4547
Rechtbank 's-Gravenhage, 21 augustus 2012, ECLI:NL:RBSGR:2012:BX5105
Rechtbank 's-Gravenhage, 27 augustus 2012, ECLI:NL:RBSGR:2012:BX5776
Rechtbank 's-Gravenhage, 30 augustus 2012, ECLI:NL:RBSGR:2012:BX6147
Rechtbank 's-Gravenhage, 17 september 2012, ECLI:NL:RBSGR:2012:BX7529
Rechtbank 's-Gravenhage, 15 oktober 2012, ECLI:NL:RBSGR:2012:BY0109
Rechtbank 's-Gravenhage, 7 februari 2013, ECLI:NL:RBDHA:2013:BZ0962
Rechtbank 's-Hertogenbosch, 8 maart 2012, ECLI:NL:RBSHE:2012:BV8201
Rechtbank 's-Hertogenbosch, 19 april 2012, ECLI:NL:RBSHE:2012:BW2684
Rechtbank 's-Hertogenbosch, 19 oktober 2012, ECLI:NL:RBSHE:2012:BY0575
Rechtbank Alkmaar, 14 augustus 2012, ECLI:NL:RBALK:2012:BX4768
Rechtbank Amsterdam, 19 april 2012, ECLI:NL:RBAMS:2012:BW3724
Rechtbank Amsterdam, 18 juli 2012, ECLI:NL:RBAMS:2012:BX1952
Rechtbank Amsterdam, 20 juli 2012, ECLI:NL:RBAMS:2012:BX3164
Rechtbank Amsterdam, 23 juli 2012, ECLI:NL:RBAMS:2012:BX5674
Rechtbank Arnhem, 14 november 2012, ECLI:NL:RBARN:2012:BY2895
Rechtbank Breda, 9 november 2010, ECLI:NL:RBBRE:2010:BO3363
Rechtbank Breda, 25 maart 2011, LJN BP9283
Rechtbank Breda, 9 augustus 2012, ECLI:NL:RBBRE:2012:BX4244
Rechtbank Breda, 1 oktober 2012, LJN BX8759
Rechtbank Dordrecht, 11 oktober 2012, LJN BX9919
Rechtbank Haarlem, 19 april 2012, ECLI:NL:RBHAA:2012:BW2968
Rechtbank Maastricht, 20 juni 2011, ECLI:NL:RBMAA:2011:BQ8509
Rechtbank Noord-Nederland, 24 januari 2013, ECLI:NL:RBNNE:2013:BY9376
Rechtbank Roermond, 12 oktober 2012, ECLI:NL:RBROE:2012:BY0623
Rechtbank Rotterdam, 27 maart 2009, ECLI:NL:RBROT:2009:BH9324
Rechtbank Rotterdam, 12 juli 2012, ECLI:NL:RBROT:2012:BX1291
Rechtbank Utrecht, 27 februari 2012, ECLI:NL:RBUTR:2012:BV7040
Rechtbank Utrecht, 4 juni 2012, ECLI:NL:RBUTR:2012:BW8244
Rechtbank Utrecht, 29 juni 2012, ECLI:NL:RBUTR:2012:BX2092
Rechtbank Utrecht, 20 augustus 2012, ECLI:NL:RBUTR:2012:BX5072
Rechtbank Utrecht, 9 oktober 2012, ECLI:NL:RBUTR:2012:BX9634
Rechtbank Zutphen, 26 juli 2011, ECLI:NL:RBZUT:2011:BR3110
Rechtbank Zutphen, 27 juni 2012, ECLI:NL:RBZUT:2012:BW9618

Bijlage 1 Samenstelling begeleidingscommissie

Voorzitter

Prof. mr. M.J. Borgers	Hoogleraar straf(proces)recht, Vrije Universiteit Amsterdam

Leden

Prof. dr. E.J. Koops	Hoogleraar regulering van technologie, Tilburg Institute for Law, Technology and society (TILT), Universiteit van Tilburg
Dhr. R. van Bosbeek	Unit Landelijke Interceptie, Landelijke Eenheid, Nationale Politie
Mr. L.J.A. van Zwieten	Landelijke officier van justitie Cybercrime, Landelijk parket Rotterdam
Mr. A. Sterneberg	Hoofd Security Vodafone, vertegenwoordiging van Platform 13 (overleg tussen overheid en aanbieders van telecommunicatie)
Mr. B.A. Stap	Ministerie van Veiligheid en Justitie, Stafbureau Platform Interceptie Decryptie & Signaalanalyse
Drs. C.J.A.M. Meijer	Ministerie van Veiligheid en Justitie, afdeling Fraude en Ordening