

Vergaderjaar 2005–2006

**23 490**

## **Ontwerp-besluiten Unie-Verdrag**

**AW**

### **BRIEF VAN DE MINISTER VAN JUSTITIE**

Den Haag, 23 september 2005

Bij brief van 20 juni 2005 (Kamerstukken II, 23 490, nr. 379) zond ik u het rapport «Wie wat bewaart die heeft wat» van de Erasmus Universiteit Rotterdam (EUR). In die brief zegde ik u toe spoedig met een inhoudelijke reactie op het rapport te zullen komen. Hierbij doe ik u, mede namens de ministers van Economische Zaken en Binnenlandse Zaken en Koninkrijksrelaties, die reactie toekomen. Hierbij wordt tevens ingegaan op de vragen zoals gesteld door de heer Franken in het Mondeling Overleg van 28 juni jl.<sup>1</sup>

#### *Opzet onderzoek EUR*

U heeft tijdens het AO van 1 december 2004 aangegeven de daadwerkelijke behoefte van de opsporingsinstanties ten aanzien van verkeersgegevens onderzocht te willen hebben. Hiertoe heb ik de Erasmus Universiteit opdracht gegeven deze behoefte in kaart te brengen. Het rapport van de EUR is gebaseerd op dossieronderzoek en interviews. Er zijn 65 dossiers van vrijwel allemaal onherroepelijke strafzaken onderzocht om te beoordelen in hoeverre verkeersgegevens van belang zijn voor opsporingsonderzoek, hetzij als zogenaamde sturingsinformatie, hetzij als bewijs in een strafzaak. In aanvulling op het dossieronderzoek zijn interviews gehouden met bij de onderzochte zaaksdossiers betrokken personen. Doel van het onderzoek is het in kaart brengen van de behoeftestelling van de opsporingsinstanties waardoor een bijdrage geleverd kan worden ter ondersteuning van het Nederlandse standpunt inzake het ontwerp kaderbesluit tot bewaring van verkeersgegevens, waarover momenteel in Brussel wordt onderhandeld.

In het onderzoek stonden twee vragen centraal:

1. Op welke wijze wordt uitvoering gegeven aan de bevoegdheid tot het vorderen van verkeersgegevens en welke knelpunten openbaren zich in dit verband?
2. Noopt de praktijk tot verruiming van de bewaringstermijn?

Beide vragen zijn bezien vanuit het perspectief van zowel de (klassieke) telefonie als het internet.

<sup>1</sup> 23 490, AT. Zie ook dossier 4.0.6. op [www.europapoort.nl](http://www.europapoort.nl)

## *Algemene bevindingen*

Voordat ik hierop in ga, wil ik nogmaals het belang van historische verkeersgegevens voor opsporing en terrorismebestrijding benadrukken. Ook in de terreuronderzoeken naar de recente aanslagen in Londen hebben historische verkeersgegevens een doorslaggevende rol gespeeld.

Uit het onderzoek is gebleken dat binnen de opsporing veelvuldig gebruik wordt gemaakt van de bevoegdheid tot het vorderen van historische verkeersgegevens. In nagenoeg alle onderzoeken wordt een standaardset aan gegevens gevorderd. Uit het onderzoek is gebleken dat er binnen de opsporing wordt uitgegaan van een, pragmatisch gegroeide, termijn van drie maanden. Deze vraag is afgestemd op hetgeen de telefonie- en internetaanbieders zeggen te kunnen leveren. Gegevens die binnen deze periode worden opgevraagd worden door de telefonieaanbieders nagenoeg altijd verstrekt. Dit geldt echter niet voor de Internet Service Providers. Er wordt melding gemaakt van een aantal gevallen waarin de gegevens niet (meer) beschikbaar waren over wie welk IP adres toegewezen gekregen had op een bepaald tijdstip. Dit maakte de betreffende zaken onoplosbaar.

De onderzoekers van de EUR komen tot de conclusie dat het aanbeveling verdient een eenduidige bewaarplicht te scheppen voor verkeersgegevens met betrekking tot telefonie- en internetverkeer. Dit komt tegemoet aan de behoefte van de opsporing en biedt duidelijkheid aan alle betrokkenen over de vraag of, en zo ja welke, gegevens kunnen worden gevraagd. Daarnaast bieden regels over een bewaartermijn helderheid voor de opsporingsdiensten omtrent de vraag over welke periode gegevens kunnen worden gevorderd en zekerheid dat die gegevens daadwerkelijk worden geleverd. Dit voorkomt dat de politie massaal gegevens vraagt, vanwege de vrees dat belangrijke verkeersgegevens anders kwijt raken. Een langere bewaartermijn zal aldus resulteren in meer afgewogen en specifiekere vorderingen, zo concluderen de onderzoekers.

### *Bevindingen telefonie*

De onderzoekers bevelen ten aanzien van de telefonie aan aansluiting te zoeken bij de in het ontwerp kaderbesluit voorgestelde termijn van één jaar. Voor de niet te complexe zaken zal weliswaar een bewaartermijn van drie maanden doorgaans voldoende zijn, maar deze termijn is onvoldoende voor langlopende onderzoeken op regionaal en nationaal niveau en rechtshulpverzoeken. Daarvoor kan worden gedacht aan zwaardere zaken zoals onderzoeken naar terrorisme, verdovende middelen-criminaliteit, mensenhandel, grootschalige fraudes, levensdelicten en zware zedendelicten.

In nagenoeg alle onderzochte zaken wordt een standaardset aan gegevens gevorderd. De set bestaat uit informatie over het telefoonnummer van waar de communicatie plaatsvindt (de A-analyse, de B-analyse en het tijdstip en de duur van de verbinding) en aanvullend bij mobiele telefonie: de locatiegegevens behorende bij de A- en B-analyse, de identiteit van de SIM kaart (IMSI) en de identiteit van het toestel (IMEI).

### *Bevindingen Internet*

Bij het onderzoek naar de effectiviteit van een bewaarplicht voor de internetgegevens is gebleken dat er slechts een gering aantal dossiers beschikbaar bleek van afgeronde strafzaken waarin historische internetgegevens een rol hebben gespeeld. Dit houdt verband met het ontbreken van een wettelijke bevoegdheid tot het vorderen van zogenaamde

NAW-gegevens tot 1 september 2004, waardoor opsporingsonderzoek met behulp van internetgegevens nog in de kinderschoenen staat. Daarom hebben de onderzoekers op dit punt het dossieronderzoek aangevuld met een ronde tafelgesprek met deskundigen van de politie.

Deze werkwijze heeft echter consequenties voor de bruikbaarheid van de bevindingen. Op basis van het dossieronderzoek kunnen geen conclusies worden getrokken ten aanzien van de vraag of de praktijk van het vorderen van historische verkeersgegevens noopt tot een verplichte bewaartermijn van een bepaalde duur. Ten aanzien van telefonie via het Internet (VoIP) kan gesteld worden dat de behoefte naar verkeersgegevens vergelijkbaar is met die van traditionele en mobiele telefonie, aangezien van VoIP verwacht wordt dat het een vervanger zal worden van de traditionele telefonie. De aanvullende interviews met politiedeskundigen bevestigen deze behoefte.

In lopende strafrechtelijke onderzoeken worden vooral het aan een gebruiker toegewezen IP adres op een bepaald tijdstip en de daarbij behorende identificerende gegevens gevorderd. Daarnaast is uit het ronde tafelgesprek een meer uitgebreide lijst van gegevens als behoefte naar voren gekomen. Deze lijst is uitgebreider dan die welke in de huidige versie van het concept-kaderbesluit staat.

#### *Standpuntbepaling ontwerp Kaderbesluit*

Vanaf de aanvang van de onderhandelingen over het ontwerp kaderbesluit heeft de Nederlandse regering veel waarde gehecht aan de set van gegevens, die op grond van artikel 2 van het ontwerp kaderbesluit door de telecommunicatieaanbieders dienen te worden bewaard. De samenstelling van die set van gegevens is namelijk van groot belang voor de proportionaliteit van de regeling. Verder is de Nederlandse regering van oordeel dat, teneinde een evenwichtige regeling te treffen, bij de verdere uitwerking van de bewaarplicht en de bepaling van de bewaartermijnen ook rekening dient te worden gehouden met de huidige praktijk van de aanbieders, de kosten die uit een bewaarplicht voortvloeien, de mogelijke implicaties voor de bescherming van de persoonlijke levenssfeer. Dit alles mede in relatie tot de behoefte bij de opsporing.

Uit de door de Erasmus Universiteit onderzochte dossiers blijkt dat historische verkeersgegevens een belangrijke rol spelen in de opsporing. Het rapport onderstreept verder dat een bewaarplicht voor telecommunicatiegegevens niet alleen duidelijkheid verschaft aan de opsporingsinstanties over de vraag welke gegevens aan de aanbieders kunnen worden gevraagd, maar tevens een wettelijke grondslag biedt om de aanbieders aan te spreken op de verstrekking van gegevens die voor de opsporing van groot belang zijn. Een bewaarplicht biedt ook helderheid voor de aanbieders inzake de reikwijdte van de verplichtingen jegens politie en justitie. Daarnaast zijn regels over bewaartermijnen van belang om te verzekeren dat de gegevens daadwerkelijk beschikbaar zijn voor de opsporingsdiensten, hetgeen tevens zal leiden tot meer afgewogen vorderingen.

Als voorzitter van de Raad heeft het Verenigd Koninkrijk op 27 juli jongstleden op basis van de uitkomsten van de raads werkgroep van 5 juli een herziene versie van het ontwerp Kaderbesluit verspreid. In deze versie vallen de volgende verkeersgegevens onder de bewaarplicht:

Ten aanzien van telefonie:

- Het bellende en het gebelde telefoonnummer of -nummers;

- Naam en adres van de gebruiker of abonnee waarop het telefoonnummer was geregistreerd op het tijdstip van de verbinding;
- Datum en tijdstip van begin en einde van de communicatie;
- De telefoniediensten die worden gebruikt, bijvoorbeeld spraak; conference call, Short Message Service (SMS), Enhanced Media Service (EMS) of Multi-Media Service (MMS), voor zover door de aanbieder aangeboden.

En aanvullend ten aanzien van mobiele telefonie:

- Het International Mobile Equipment Identity (IMEI) en de International Mobile Subscriber Identity (IMSI) van de inbellende of gebelde deelnemer aan de communicatie;
- Locatie aanduiding (Cell ID) bij de start en het einde van de communicatie.

Discussie is er nog over:

- Locatie aanduiding (Cell ID) gedurende de communicatie.

Ten aanzien van internettoegang, e-mailverkeer en voice over IP:

- Het Internet Protocol (IP) adres, hetzij dynamisch hetzij statisch, toegewezen door de Internet toegang provider aan een verbinding of van de ontvanger van een communicatie;
- User ID, bijvoorbeeld e-mail adres, van de bron van de communicatie;
- De «Connection Label» of User ID van de beoogde ontvanger van een communicatie;
- De «Connection Label» of User ID via welke de verbinding naar de Internet toegang provider tot stand is gekomen;
- De «Connection Label» of het telefoonnummer toegewezen aan enige communicatie die het publieke telefoonnetwerk binnenkomt;
- Naam en adres van de gebruiker of abonnee aan wie het IP Adres, Connection Label of User ID was toegewezen op het tijdstip van de communicatie;
- Datum en tijdstip van de log-in en log-off van een Internet sessie gebaseerd op een bepaalde tijdzone;
- Het inbellende nummer voor dial-up toegang;
- De asymmetric digital subscriber line (ADSL) of ander aansluitpunt van de initiatiefnemer van de communicatie;
- Het media access control (MAC) adres of ander identificerend gegeven van het apparaat van de initiatiefnemer van de communicatie;
- Of gebruik is gemaakt van e-mail of VoIP.

### *Overgangstermijnen*

Met het oog op de implementatie – de mogelijke aanpassing van de systemen van de aanbieders – geldt er een overgangstermijn van twee jaar na de inwerkingtreding van het kaderbesluit voor de volgende categorieën van gegevens:

- Onbeantwoorde oproepen op vaste of mobiele telefonie;
- EMS en MMS-diensten op vaste of mobiele telefonie;
- Internettoegang, e-mailverkeer en voice over IP .

Een aantal lidstaten heeft op dit punt studievoorbehouden gelegd. Nederland heeft een studievoorbehoud aangetekend bij de bewaarplicht van en overgangstermijn voor de onbeantwoorde oproepen vanwege de mogelijke lasten voor de aanbieders in relatie tot het belang voor de opsporing. Om die reden gaat Nederland vooralsnog niet akkoord met de opname van onbeantwoorde oproepen.

De overige gegevens rond Internet en internetdiensten, zoals gegevens over welke websites bezocht zijn en gegevens over de bron en de bestemming per IP-pakket, zijn niet opgenomen op de lijst en vallen dus niet onder de bewaarplicht. Dit betekent een aanzienlijk minder zware last

voor de aanbieders, die uit het kaderbesluit kunnen voortvloeien ten opzichte van het oorspronkelijke voorstel. Het voorstel strekt zich alleen uit tot aanbieders van openbare telecommunicatienetwerken en -diensten, voorzover hun diensten onder de reikwijdte van de Telecommunicatiewet vallen en is verder, voor wat betreft internet, beperkt tot aanbieders van internettoegangsdiensten, emaildiensten en VoIPdiensten. Dit betekent dat de verplichting zoals deze in dit kaderbesluit besproken wordt zich niet uitstrekt tot bijvoorbeeld de e-mail afkomstig van domeinen die niet aangeboden worden in het kader van een internettoegangsdienst, zoals bedrijfs-email.

In de gegevens ten aanzien van de (klassieke) telefonie constateer ik geen afwijkingen ten opzichte van de behoefte zoals die is gebleken in het onderzoek van de EUR op één uitzondering na.

Dit betreft de gegevens betreffende naam en adres en soort dienst behorend bij een telefoonnummer. In Nederland wordt deze informatie op dit moment geleverd door tussenkomst van het Centraal Informatiepunt Onderzoek telecommunicatie (CIOT) te Zoetermeer. De historie van een telefoonnummer is opvraagbaar via de stichting COIN die verantwoordelijk is voor de uitvoering van het systeem van nummerportabiliteit. Hoewel deze gegevens niet in het rapport van de EUR zijn opgenomen, is het belang van deze gegevens evident. Een verkeersgegeven heeft aanzienlijk meer waarde wanneer daaraan een identificatie van een persoon kan worden gekoppeld. Ik meen ook dat, gelet op de voorzieningen die nu reeds aanwezig zijn, zonder disproportionele inspanning aan deze eis kan worden voldaan. Om deze redenen zie ik geen bezwaar om met opname van deze gegevens in het kaderbesluit in te stemmen.

De overige gegevens betreffen wat in het EUR onderzoek wordt aangeduid als A- en B-analyse, tijdstip en duur van de verbinding, lokatiegegevens van de A- en B-analyse en het IMEI nummer. Tegen opname van deze gegevens in het kaderbesluit heb ik dan ook geen bezwaar.

Ten aanzien van Internet constateer ik dat het ontwerp kaderbesluit is beperkt tot de gegevens inzake de toegang tot Internet, e-mail en Internettelefonie. Het merendeel van de gegevens heeft betrekking op het IP-adres en overige identificerende gegevens. Hier geldt, evenzeer als bij de klassieke telefonie, dat identificerende gegevens uiterst waardevol zijn bij het gebruik van de overige verkeersgegevens. Als identificerende gegevens worden in het Kaderbesluit genoemd: «connection label», user ID, telefoonnummer, NAW-gegevens, ADSL of ander aansluitpunt en MAC-adres. In het onderzoek van de EUR is de behoefte aan IP adres en identificerende gegevens ook in opsporingsonderzoeken onderkend. Bovendien concludeert het rapport tot een bewaarplicht van een gelijksoortige set van gegevens voor internettelefonie (VoIP) als voor klassieke telefonie. De internetgegevens in het ontwerp kaderbesluit betreffen een beperkte set van gegevens die veelal reeds door de internetaanbieders voor kortere of langere tijd bewaard worden. Om die reden kan ik met opname van deze gegevens in het Kaderbesluit instemmen.

Het gegeven van datum en tijdstip van log-in en log-off is eveneens van groot belang in een onderzoek. Immers, wanneer handelingen niet gekoppeld kunnen worden aan een datum- en tijdregistratie, heeft het gegeven geen waarde voor het bewijs (mogelijk wel als sturingsinformatie voor het onderzoek). Dergelijke gegevens worden standaard in loggings opgenomen en kunnen derhalve zonder disproportionele

inspanning worden vastgelegd. Ook met opname van dit gegeven in het Kaderbesluit kan ik derhalve instemmen.

Ten aanzien van de gegevens met betrekking tot Locatie aanduiding (Cell ID) gedurende de communicatie heeft Nederland een studievoorbehoud gelegd vanwege de mogelijke lasten die dit meebrengt voor de aanbieders in relatie tot de behoefte van de opsporing. Dit zal nader worden onderzocht.

Samenvattend kom ik tot de conclusie dat ik, op een tweetal punten na waar nog een studievoorbehoud is gemaakt – onbeantwoorde oproepen en locatie aanduiding tijdens de communicatie –, kan instemmen met de set van gegevens in het ontwerp kaderbesluit dat thans voorligt.

#### *Bewaartermijnen*

De standaardtermijn voor de bewaring van deze verkeersgegevens is bepaald op 12 maanden met de mogelijkheid deze te bekorten tot 6 maanden of te verlengen tot 48 maanden. Gelet op de uitkomsten van het onderzoek van de EUR meen ik dat met de voorgestelde termijnen voor wat betreft de klassieke telefonie kan worden ingestemd, met dien verstande dat bij de implementatie van het kaderbesluit nader zal worden besloten over de precieze wettelijke bewaartermijn binnen de door het kaderbesluit gestelde kaders. Voor internet geeft de EUR aan dat een bewaarplicht wel aanbeveling verdient, maar kunnen op grond van het dossieronderzoek geen conclusies worden getrokken ten aanzien van een bepaalde bewaartermijn. Gelet op de ontwikkeling van telefonie over het Internet (VoIP) en de daarmee verband houdende mogelijke verplaatsings-effecten valt niet goed in te zien waarom ten aanzien van deze gegevens een andere bewaartermijn zou worden gehanteerd. Gelet op de beperkte set van gegevens die in het ontwerp Kaderbesluit is opgenomen, ben ik geneigd daarin mee te gaan, waarbij ik opmerk dat de door het kaderbesluit voorgestelde bewaartermijnen enige flexibiliteit bieden.

#### *Proportionaliteit en kosten*

Prof. mr. H. Franken heeft in de Eerste Kamer een uitvoerig betoog gehouden over onder andere de proportionaliteit van de voorgestelde maatregelen in het kaderbesluit. Daaronder begrijp ik tevens de mogelijkheden om de bewaarplicht te ontwijken. Inmiddels heb ik zijn betoog ook op schrift ontvangen.

In de eerste plaats constateer ik dat de set van gegevens zoals die thans in het ontwerp kaderbesluit is opgenomen beperkter is dan waar de heer Franken in zijn betoog nog vanuit ging. In ieder geval is de set ten aanzien van het Internet – waar de kritiek van de heer Franken zich hoofdzakelijk op richtte – aanzienlijk beperkter dan de in het EUR rapport genoemde set van gegevens en ook beperkter ten aanzien van het aantal partijen, aangezien webhosting en belwinkels niet onder het Kaderbesluit vallen.

Bovendien moet rekening worden gehouden met het feit dat het kaderbesluit inmiddels een mogelijkheid bevat van een minimum bewaartermijn van zes maanden. Waar de heer Franken ervan uitgaat dat providers alle verkeer moeten bewaren en daar vervolgens de relevante gegevens uit moeten destilleren, is het mijn overtuiging dat de onderhavige set gegevens door de providers zonder bovenmatige inspanning kan worden vastgelegd.

Aan het beperken van de kosten voor de aanbieders kan verder ook de wijze van uitvoering van de bewaarplicht bijdragen. In het rapport van

KPMG, dat ik u bij brief van 20 december 2004 heb toegezonden, zijn twee varianten uitgewerkt voor de uitvoering van een bewaarplicht. Een variant waarbij de opslag bij de aanbieders ligt en een variant volgens het zogenaamde CIOT-model. In het rapport van KPMG wordt dit model uitgebreid beschreven. In de praktijk werkt het CIOT op dit moment voor de opslag en bevraging van telefoonnummers en de bijbehorende NAW gegevens.

Het CIOTmodel kent vele voordelen, waaronder de kosteneffectiviteit. Dit model is aanzienlijk goedkoper dan het model waarbij aanbieders afzonderlijk systemen moeten ontwikkelen om aan de bewaarplicht te voldoen. Voor de aanbieders is het voordeel van toepassing van het CIOT-model gelegen in het feit dat het bewaren, doorzoekbaar maken en zoeken van de gegevens wordt verricht door het CIOT. Ingeval het mogelijk is de te bewaren gegevens door middel van een zogenaamde black box onder te brengen bij het CIOT, dan kan ook de opslag van de gegevens worden verzorgd door het CIOT en zouden de lasten voor de aanbieders kunnen zijn beperkt tot het beschikbaar stellen van de gegevens en de aanpassingen in hun systemen voor die beschikbaarstelling. Bovendien is uit de huidige toepassing van het CIOT gebleken dat ook aan overheidszijde een aanzienlijke besparing kon worden gerealiseerd op de kosten van bevragingen. Deze besparing was zodanig dat de ontwikkeling van het CIOT systeem in enkele jaren kon worden terugverdiend. Om deze redenen vind ik het van belang nader onderzoek te doen naar de mogelijkheid om de bewaarplicht uit te voeren via dit CIOT model.

Daarmee kom ik tot de conclusie dat de bewaarplicht, zoals die nu in het ontwerp-Kaderbesluit is vastgelegd, niet leidt tot buitenproportionele kosten voor de aanbieders.

Een laatste punt is in hoeverre de bewaarplicht ontwijkbaar is voor gebruikers van telecommunicatiediensten die zich om wat voor reden dan ook daaraan willen onttrekken. Daarbij kan een onderscheid worden gemaakt tussen twee situaties.

Ten eerste kunnen van een bepaalde communicatie geen gegevens zijn vastgelegd. Dit beperkt zich tot de gevallen waarin gecommuniceerd wordt buiten de aanbieder om of via aanbieders die zich buiten de reikwijdte van de Europese lidstaten bevinden. In alle andere gevallen immers zullen de gegevens door de aanbieder in Nederland of één van de lidstaten van de Unie worden vastgelegd. Ten aanzien van de in het ontwerp-Kaderbesluit genoemde diensten kan hierover het volgende worden opgemerkt.

Ten aanzien van het gebruik van telefonie, zowel voor vast als mobiel, kan gesteld worden dat het ontwijken van de bewaarplicht niet eenvoudig is. Door de centrale rol die de aanbieders in het netwerk hebben, hebben zij altijd zicht op het telefoonverkeer van en naar een aansluiting. Dit betekent niet dat zij altijd zicht hebben op de daadwerkelijke gebruiker, zoals bijvoorbeeld bij het gebruik van een telefoon in een café, prepaid mobiele telefonie of het gebruik van buitenlandse mobiele telefoons. Om het toch mogelijk te maken de gebruiker in dergelijke gevallen te identificeren beschikt de opsporing nu al over adequate juridische en technische middelen.

Voor internetcommunicatie geldt dat de rol van de aanbieders beperkter is dan die in de telefonie. De internettoegangs-aanbieders bieden in eerste aanleg alleen een verbinding met het Internet en verlenen daarvoor een bepaald IP-nummer aan de gebruiker. Zij hoeven verder geen rol te spelen bij de verdere wijze waarop van het Internet gebruik gemaakt wordt. Voor

de gegevens uit het kaderbesluit geldt, dat het niet eenvoudig zal zijn om geautoriseerd verbinding te maken met het Internet, zonder dat dat bij een aanbieder bekend is.

Voor het gebruik van Voice over IP geldt dat het internet het mogelijk maakt om direct tussen twee internetverbindingen een gesprek op te zetten, zonder gebruik van een aanbieder. In de eerste plaats geldt dat alle betrokken partijen moeten hebben gekozen voor VoIP zonder tussenkomst van een aanbieder, ook het eventuele slachtoffer van een misdrijf. Afgezien daarvan verwachten wij niet dat deze specifieke vorm van van VoIP, namelijk zonder dat er een aanbieder bij betrokken is, een dermate hoge vlucht zal gaan nemen dat het de waarde van een bewaarplicht significant zou reduceren. Het ligt weliswaar in de lijn der verwachting dat de «traditionele» aanbieders van telecommunicatiediensten zich de komende jaren op het terrein van de internettelefonie zullen begeven, maar daarbij zullen de telefoniediensten op basis van het thans bekende systeem van telefoonnummers worden afgewikkeld en zal de bewaarplicht onverkort van toepassing zijn. Voor e-mail geldt dat het mogelijk is dat de gebruiker gebruik maakt van een eigen domein, eigen mailserver of een buitenlandse aanbieder om de bewaarplicht te ontwijken. Toch heeft de opsporing nog steeds veel profijt van de gegevens betreffende de maildienst die door ISP's bij hun abonnement geleverd worden.

De tweede situatie betreft het geval dat wel gegevens zijn vastgelegd maar deze niet leiden naar de feitelijke bron van de communicatie.

Dit doet zich bijvoorbeeld voor wanneer iemand gebruik maakt van bijvoorbeeld een niet-beveiligde WiFi-verbinding om draadloos gebruik te maken van de Internetaansluiting van een ander. Dit kan ervoor zorgen dat de eigenaar van die niet-beveiligde verbinding in eerste instantie aangesproken wordt op het misbruik van die verbinding. Niet voor niets wijst de campagne Surf op Safe op de risico's van een niet-beveiligde verbinding. Echter voor het overgrote deel van het internetgebruik zal de bewaarplicht wel helderheid kunnen verschaffen over welke abonnee een IP-adres toegewezen gekregen had op een bepaald moment.

Ook kan het zijn dat iemand gebruik maakt van anonimiseringsdiensten. In die gevallen leveren de verkeersgegevens nog altijd waardevolle informatie op over het verkeer dat heeft plaatsgevonden. Met de aldus verkregen informatie kan via een vordering van de officier van justitie of, in het geval de dienstenaanbieder zich in het buitenland bevindt, via een rechtshulpverzoek, de feitelijke bron van de communicatie worden achterhaald.

Tenslotte merk ik nog op dat niet alleen moet worden gedacht aan het bewaren van de communicatie van de dader, deze hoeft nog niet in beeld te zijn en heeft misschien bewust geprobeerd de bewaarplicht te ontwijken, maar ook dat van het slachtoffer die veelal niet een motivatie heeft om de bewaarplicht te ontwijken. Het communicatiegedrag van het slachtoffer kan ook interessante sporen geven die leiden tot het vinden van de dader.

#### *Tijdschema behandeling ontwerp kaderbesluit*

Tijdens het Britse voorzitterschap zal het ontwerp kaderbesluit onderwerp van bespreking vormen in de informele JBZ-Raad, die wordt gehouden op 8 en 9 september in Newcastle. Er zal een hoorzitting worden georganiseerd met deskundigen op het terrein van politie, justitie en rechtshandhaving voor wat betreft de technische aspecten van het voorliggende voorstel.



Op 13 juli jongstleden heeft de Raad in reactie op de bomaanslagen in Londen een verklaring aangenomen. Hierover heb ik, mede namens de minister voor Vreemdelingenzaken en Integratie en de minister van Binnenlandse Zaken en Koninkrijksrelaties, Uw Kamer bij brieven van 12 juli en 12 augustus jongstleden ingelicht (TK, 2004–2005, 23 490, nrs. 381 en 382). In die Raadsverklaring is neergelegd dat de Raad zal besluiten over enkele kaderbesluiten, waaronder het kaderbesluit inzake de bewaring van telecommunicatiegegevens (oktober 2005). Dit betekent dat de door de Europese Raad gestelde termijn van 1 juni 2005 is aangepast. Gelet op de vragen over de inhoud van dit voorstel die er nog leven bij de fracties van Uw Kamer, onder meer over de kosten van een bewaarplicht, de lasten voor de aanbieders en de rechtsgrondslag, acht ik een dergelijke termijn voor Nederland zeer ambitieus. Ik zal uiteraard met alle vermogen ernaar blijven streven om in Brussel gehoor te vinden voor de zorgpunten die in het overleg met de leden van Uw Kamer over dit onderwerp aan de orde zijn.

Ik zal uw Kamer gaarne op de hoogte houden van de stand van zaken.

De Minister van Justitie,  
J. P. H. Donner