Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2008–2009

31 145

Wijziging van de Telecommunicatiewet en de Wet op de economische delicten in verband met de implementatie van Richtlijn 2006/24/EG van het Europees Parlement en de Raad van de Europese Unie betreffende de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare elektronische communicatiediensten en tot wijziging van Richtlijn 2002/58/EG (Wet bewaarplicht telecommunicatiegegevens)

D

VERSLAG VAN EEN EXPERTBIJEENKOMST

Vastgesteld 9 december 2008

De vaste commissie voor Justitie[1] heeft op 11 november 2008 met de heer Van den Boom van Ernst & Young en de heer Niesen van Deloitte Accountants BV gesproken over het onderhavige wetsvoorstel.

Van deze bijeenkomst brengt de commissie bijgaand verslag uit.

De griffier van de commissie,
Kim van Dooren

[1] Samenstelling:
Holdijk (SGP), Dölle (CDA), Tan (PvdA), Van de Beeten (CDA), (voorzitter), Broekers-Knol (VVD), De Graaf (VVD), Kneppers-Heynert (VVD), Kox (SP), Westerveld (PvdA), (vice-voorzitter), Russell (CDA), Engels (D66), Franken (CDA), Peters (SP), Quik-Schuijt (SP), Haubrich-Gooskens (PvdA), Ten Horn (SP), Janse de Jonge (CDA), Koffeman (PvdD), Böhler (GL), Van Bijsterveld (CDA), Strik (GL), Lagerwerf-Vergunst (CU), Rehwinkel (PvdA), Duthler (VVD) en Yildirim (Fractie-Yildirim).

KST125807
ISSN 0921 - 7363
Sdu Uitgevers
's-Gravenhage 2008

Voorzitter: Van de Beeten
Griffier: Van Dooren

Vragen en opmerkingen uit de commissie

De **voorzitter**: Ik heet de heren Niesen en Van den Boom van harte welkom. Zij zijn de experts die wij hebben uitgenodigd om vandaag met ons van gedachten te wisselen over een aantal technische aspecten van de Wet bewaarplicht telecommunicatiegegevens. Ook welkom aan de ambtenaren van het ministerie van Justitie, te weten de heer Mol Lous, mevrouw Jongeneel en de heer Van Oosterhout en aan de heer Parmentier van het ministerie van Economische Zaken.
Wij hebben voor dit overleg een uur uitgetrokken. In de uitnodigingsbrief zijn vijf vragen aan u voorgelegd. Het is inmiddels een aanzienlijk langere lijst geworden, zoals u hebt gezien.[1] Wij hebben dus betrekkelijk weinig tijd. Ik wil proberen die tijd zo efficiënt mogelijk te gebruiken. Ik doe dan ook geen voorstelronde. De leden hebben de cv's van de beide heren gezien; zij weten welk vlees zij in de kuip hebben.
Mijnheer Niesen en mijnheer Van den Boom, hoe denkt u dat wij deze vragen het beste kunnen doornemen? Ik heb begrepen dat u met elkaar overleg hebt gehad. Ik wil even een plan van aanpak maken. Wij moeten proberen zo ver mogelijk te komen. Misschien is enige uitloop mogelijk, maar ik wil het niet veel langer laten duren dan tot 18.00 uur.
Ik geef de leden de gelegenheid om vragen te stellen naar aanleiding van uw opmerkingen. Vanwege de tijd wil ik de ambtenaren niet de ruimte bieden om vragen te stellen, ook al kan ik mij voorstellen dat zij die wel hebben. Als wij op het eind van dit gesprek tot de conclusie komen dat wij er vandaag niet helemaal uitkomen, stel ik voor om met u te overleggen of een schriftelijk antwoord mogelijk is op vragen die niet beantwoord zijn.
Er wordt een stenografisch verslag gemaakt door de Dienst Verslag en Redactie. Vroeger zeiden wij gewoon de Stenografische Dienst, het blijft wennen om nu te spreken over de DVR. Ik heet de medewerkster van de Dienst Verslag en Redactie ook welkom.
Ik verzoek de leden om even hun naam te noemen als zij het woord krijgen, zodat de verslaglegging op een deugdelijke wijze kan geschieden.
Heren, hoe zullen wij het aanpakken?

De heer **Niesen**: Wij hebben alle twee de vragen voorbereid. Als een van de twee het voortouw neemt, kan de ander zo nodig aanvullen. Dat lijkt mij efficiënt.

De heer **Van den Boom**: Dat is prima.

De heer **Niesen**: Ik heb het gevoel dat het leeuwendeel van de vijf vragen in de uitnodigingsbrief terugkomt in de 20 vragen die later gesteld zijn. Wij zouden kunnen starten met die 20 vragen.
De eerste vraag gaat over het aantal communicaties per dag. Het is belangrijk om vast te stellen dat het hier niet gaat om communicaties tussen mensen. Het zijn veelal communicaties die door systemen worden opgestart. Ik probeer wat referentiegegevens uit de branche te halen, aangevuld met het VKA-rapport[2]. Het gaat om aanzienlijke aantallen. Als ik het optel, komen wij op een miljard communicaties per dag.

Mevrouw **Duthler** (VVD): Zijn dat communicaties in Nederland of in de Europese Unie?

De heer **Niesen**: Het gaat om communicaties in Nederland.
Nogmaals, het is heel erg afhankelijk van hoe je het bekijkt. Communicatie is niet het opstarten van je mail; communicatie kan technisch gezien bete-

[1] De lijst met vragen is als bijlage opgenomen aan het eind van dit verslag.
[2] Ter inzage gelegd bij de afdeling Inhoudelijke Ondersteuning onder griffieummer 141553.07.

kenen dat onder water een machine met een andere machine communiceert. Daarvan zie je dus niets. Ook het aanloggen en afloggen van een internetserviceprovider is niet goed te meten.. Dat maakt het zo complex. Mijn modem staat altijd aan. Dat wordt gezien als één keer aanloggen. Het kan echter soms even uitgaan en direct daarna weer aangaan. Als gebruiker merk ik daar niets van. Het wordt ook niet door mij geïnitieerd, maar zorgt wel voor gegevens die onder deze wetgeving vallen en dus opgeslagen moeten worden.

De heer **Van den Boom**: Als je ook rekening houdt met zaken als spam, verveelvoudigt het aantal communicaties. Dan wordt het meer dan een miljard.

De heer **Franken** (CDA): In vraag 20 wordt gesteld dat 98% van het e-mail verkeer uit spam zou bestaan. Als u zegt dat die 1 mld. met een bepaalde factor moet worden vermenigvuldigd, is dat dan een factor 98? Wordt het dan 98 mld.?

De heer **Van den Boom**: In een aantal van de door ons gehanteerde rapporten is gerekend met 32 mails per account per dag. Die factor gaat omhoog. Bij 1 mld. is dat nu 450 000. Op die factor wordt het een verveelvoudiging.

De heer **Franken** (CDA): Hoeveel is die verveelvoudiging?

De heer **Van den Boom**: Een verveelvoudiging van 450 000.

De heer **Franken** (CDA): Wat is dan het uiteindelijke product, inclusief en exclusief spam? Misschien kunt u het zo zeggen, dan lijkt het of het btw is?

De heer **Van den Boom**: Exclusief spam komen wij uit op 451 miljoen communicaties per dag.

De heer **Franken** (CDA): Spam wordt ook allemaal bewaard?

De heer **Niesen**: Ja.

Mevrouw **Van Bijsterveld** (CDA): De communicatie in Nederland betreft ook buitenlands verkeer naar Nederland en Nederlands verkeer naar het buitenland, of is het alleen intern?

De heer **Niesen**: Het is zowel inbound als outbound verkeer. Nogmaals, het moet niet gehanteerd worden als een exact gegeven, want er is sprake van een grote bandbreedte. Dit zijn wat ons betreft de gegevens die door Nederlandse internetserviceproviders moeten worden opgeslagen.

De heer **Franken** (CDA): Dus geen telecomserviceaanbieders?

De heer **Niesen**: Nee, deze vraag heeft alleen betrekking op internet-telefoonoproepen en in- en uitloggegevens.

De heer **Franken** (CDA): Het is goed om vast te stellen dat de telecommunicatie daar nog bovenop komt. Kunt u daarvan een schatting maken?

De heer **Niesen**: Eerlijk gezegd heb ik mij daarin niet verdiept. Het ligt daar ook anders. Zij loggen dit soort dingen al op dit moment, terwijl het hier een geheel nieuwe vorm van vastlegging betreft.

De **voorzitter**: Mag ik de leden vragen om terughoudend te zijn met tussentijds vragen te stellen, anders komen wij er zeker niet doorheen?

Mevrouw **Strik** (GroenLinks): Verderop zien wij dat buitenlandse internetaanbieders niet onder de bewaarplicht vallen, maar wordt een mail van deze aanbieders hier wel geregistreerd als een communicatie?

De heer **Niesen**: Als een mail in Nederland binnenkomt bij een internetserviceprovider, valt die hier onder de bewaarplicht. De vraag is, of je die mail terug kunt traceren naar de afzender. Het antwoord op die vraag is nee, want dat valt er niet onder.

Mevrouw **Duthler** (VVD): Dus die 450 mln. communicaties per dag exclusief spam betreffen het berichtenverkeer van abonnees van Nederlandse internetserviceproviders? Zeg ik dat goed?

De heer **Niesen**: Ik zit even met het woord abonnees. Ik denk dat mevrouw Duthler het goed zegt.

De **voorzitter**: Even heel precies: in Nederland gevestigde internetproviders moeten die hoeveelheid gegevens verwerken. Daar komt het op neer?

De heer **Niesen**: Inderdaad. Een serviceprovider kan geen onderscheid maken tussen wel of geen spam.

De heer **Van den Boom**: De tweede vraag luidt, of er hardware- en softwaretechnologie bestaat om de duizenden simultane communicaties live te bevragen en die informatie weg te schrijven.
Technisch gezien is het inderdaad mogelijk om de gevraagde gegevens weg te schrijven. De in bijlage A en bijlage B genoemde gegevens kunnen worden weggeschreven uit de systemen en vervolgens opgeslagen en bevraagd worden.

De **voorzitter**: Welke capaciteit is daarvoor nodig?

De heer **Van den Boom**: In het VKA-rapport wordt een aantal hoeveelheden genoemd. Ik weet niet exact hoeveel capaciteit daarvoor nodig is. Dat zou ik moeten onderzoeken. Technisch gezien is het inderdaad mogelijk.
Aan de kant van de telecom worden gebruiksgegevens ook weggeschreven. Het verhoogt de complexiteit substantieel als het gaat om het daadwerkelijk live doorzoeken van gegevens. Het live wegschrijven van gegevens, deze bewaren en op een gegeven moment beschikbaar stellen om zoekqueries op te draaien bijvoorbeeld of een bepaalde communicatie heeft plaatsgevonden, of een bepaalde burger heeft gecommuniceerd naar een bepaald nummer of naar een bepaald e-mailadres, is technisch heel goed mogelijk. Het wordt complexer als het real time on line moet plaatsvinden, bijvoorbeeld dat wanneer iemand begint te bellen, direct een alarmsignaal afgaat. De telecomwereld is veel verder dan de ISP's. In de telecomwereld worden de communicaties in feite vastgelegd.

De **voorzitter**: Bij real time praten wij over een ander wettelijk regime; het gaat daarbij om het vorderen van gegevens en over de wettelijke bevoegdheden die daarvoor zijn neergelegd in het Wetboek van Strafvordering. Dat staat buiten het wettelijk kader van het thans voorliggende wetsvoorstel.

De heer **Niesen**: Ik heb de vraag iets anders opgevat. Zou je naar de winkel kunnen gaan en het kunnen kopen op dit moment? Het antwoord

op die vraag is nee, het is geen standaardpakket dat gekocht kan worden. Dit is iets dat gemaakt zal worden. ISP's zijn organisch gegroeid en absoluut niet gestandaardiseerd. Zij hebben allemaal hun eigen systemen en die zijn niet erop ingericht om dit soort gegevens op te leveren. Dat betekent dat elke ISP het op zijn eigen manier moet gaan implementeren. Ik ben het helemaal met de heer Van den Boom eens dat dit technisch gezien kan. Er zijn ingewikkelder dingen gemaakt dan dit. Het is echter niet als een tv die je koopt en die speelt als je de stekker in het stopcontact steekt. Het zal veel tijd, effort en mensenwerk kosten om ervoor te zorgen dat het op een goede manier wordt opgeslagen en vervolgens op een goede manier wordt ontsloten.
Er is ook een vraag over de kosten. Ik denk dat de opslagcapaciteit zelf slechts 5% à 10% van de totale kosten bedraagt. Dat zijn alleen maar de harde schijven waar het op komt te staan. Vervolgens moet het ontsloten worden en dat maakt het duur. Moet het heel snel kunnen worden ontsloten? De wet spreekt over onverwijld. Mij is niet duidelijk wat daarmee precies wordt bedoeld. Als het binnen enkele uren moet, vallen veel opties af. Het vereist een veel complexere en zwaardere systematiek van gegevensontsluiting dan wanneer je daarvoor enkele dagen de tijd krijgt.
Vervolgens moeten de hardware en de software gekoppeld worden aan de operationele systemen waarop de mensen aan- en uitloggen. Omdat de ISP-wereld niet zodanig is opgebouwd dat dit vanuit de facturatiestroom in ieder geval al wordt gelogd, zullen sommige internetserviceproviders dingen wel opslaan en andere niet. Afhankelijk daarvan zal er bijgebouwd moeten worden. De ISP's moeten uren investeren om dat voor elkaar te krijgen. Ik kan mij voorstellen dat het voor een gemiddelde ISP een investering van enkele miljoenen vergt om te komen tot een werkend systeem. De opslagcapaciteit vormt daarvan maar een klein onderdeel.

De heer **Van den Boom**: Ik onderschrijf dat. Om te voldoen aan de wet, moet bijgebouwd worden. Daarbij spelen vragen als: welke controles ingebouwd moeten worden, welke uitgangspunten moeten worden gehanteerd en hoe moet worden omgegaan met definities? In de wettekst wordt gesproken over schoning een jaar na het moment van vastlegging. Is het een jaar nadat de communicatie heeft plaatsgevonden? Hoe ga je daarmee om? Dat soort definities moeten helder zijn en vervolgens moet een en ander worden ingericht. De vraag is dan of het handmatig gaat gebeuren. Als je dagelijks gaat opschonen, heb je daarvoor dus dagelijks menskracht nodig. Als het automatisch moet gebeuren, worden de initiële kosten van de programmering een stuk hoger. Bij het inrichtingsproces komen ook aspecten als acquisitie, opslag en bevraging aan de orde. Het zijn behoorlijke kosten.

De **voorzitter**: Is vraag 2 hiermee afdoende behandeld?

Mevrouw **Duthler** (VVD): Ik heb nog een vraag, voorzitter. Er wordt gezegd dat ISP's miljoenen euro's moeten investeren. Kun je dat differentiëren naar omvang van een ISP? Is dat voor kleine providers evenveel als voor grote?

De heer **Niesen**: Nee. Ik denk dat wij langzaam bij vraag drie komen.

De **voorzitter**: Ik denk inderdaad dat wij daar al zitten en eigenlijk ook in vraag 4.

De heer **Niesen**: Uiteindelijk gaat het om de vraag hoe snel die gegevens moeten worden opgeleverd. Ik kan mij voorstellen dat voor een kleine ISP met enkele tienduizenden actieve accounts, het bevragen van die gegevens bij wijze van spreken in een tekstbestand gelogd kan worden en de

gegevens vervolgens handmatig of met queries op een vrij eenvoudige manier kunnen worden verkregen, waardoor het nog wel binnen de gevraagde termijn kan. Dan hebben wij het over heel andere infrastructuur, een heel andere zwaarte van consultancydiensten of aantallen uren die daarin geïnvesteerd moeten worden. Voor dat soort ISP's zullen de kosten voor hardware en software een groter deel van het totaal bedragen dan het aantal uren.

De heer **Van den Boom**: Het is wel zo dat bij de kleinere ISP's de processen minder volwassen zijn. Er moet een initiële slag gemaakt worden om de privacyaspecten van de opgeslagen gegevens te waarborgen. Als er geen of minimaal persoonsgebonden gegevens worden opgeslagen, is er sprake van heel andere beveiligingseisen dan in een setting waarbij daadwerkelijk gedurende een jaar gegevens worden opgeslagen. Bij kleinere internetserviceproviders gaat het om veel lagere kosten dan bij grote. Men zal wel grote stappen moeten zetten en behoorlijke investeringen moeten doen om dat op niveau te krijgen. Het betreft niet alleen technische zaken, men moet zich ook bewust worden van de beveiliging, de manier van werken en het organiseren van processen zodat de gegevens niet op straat belanden.

De heer **Niesen**: In vraag 3 spelen twee zaken. Allereerst de manier van bevragen en vervolgens hoe snel het moet gaan.
Het type vraagstelling stuurt in grote mate de manier waarop moet worden opgeslagen. Ik geef een voorbeeld. Als gevraagd zou worden om de mailtjes die persoon A naar persoon B heeft gestuurd op tijdstip X, vind ik dat een redelijk simpele vraag. Ook als er sprake is van een groot bestand, zou dat op een veel snellere manier kunnen gebeuren dan als gevraagd wordt om alle mailtjes die van A naar B zijn gestuurd en waarop B binnen tien minuten heeft geantwoord. Dat is een meer gestapelde vraag. Bij een dergelijke complexe vraag moeten er allerlei verbanden gelegd worden binnen de gegevensset. Als je die informatie onverwijld moet leveren, moeten die gegevens gecorreleerd worden opgeslagen. Bij het opslaan van de data moeten die gegevens al op een slimme manier bij elkaar gebracht worden. Dat betekent in ieder geval dat het niet in tekstbestanden kan, dan moet gedacht worden aan databases. Dat werkt kostenverhogend en vereist een veel complexere programmatuur dan wanneer het in silo's kan worden opgeslagen. Afhankelijk van de vraag kan worden bekeken of door het knopen van silo A aan silo B het antwoord geabstraheerd kan worden.

De **voorzitter**: Vraagt u in feite niet of de branche de datamining moet doen of de overheid? Wilt u weten of u het wel in tekstbestanden mag opslaan omdat het anders niet meer te behandelen zou zijn door de overheid?

De heer **Niesen**: Het zou helpen als er consensus zou zijn over het type vragen dat gesteld moet worden. De telecomproviders of de ISP's zouden op basis daarvan hun opslagsystematiek op een sterke manier kunnen sturen. Het is nog altijd zo dat de ISP gevraagd wordt om gegevens te leveren en niet om al zijn logbestanden over te dragen.

De **voorzitter**: Het is inderdaad een vraagpunt of het allemaal centraal moet worden opgeslagen om het überhaupt te kunnen behappen.

De heer **Franken** (CDA): De ISP zal dus een bepaalde selectie moeten toepassen? Hij zal geselecteerd materiaal moeten uitleveren? Hij moet dus dat zoekwerk doen en daarvoor moet hij de programmatuur hebben.

De heer **Niesen**: In het VKA-rapport worden verschillende scenario's beschreven. Het gaat inderdaad die richting op. De registratie vindt plaats bij de ISP. De ISP kan daaruit op verzoek delen opleveren.

De heer **Van den Boom**: Ik interpreteer de stukken zodanig dat de ISP op verzoek daadwerkelijk gaat zoeken in de opgeleverde bestanden. Zij hebben die zoeksoftware nodig.

De heer **Niesen**: De ISP levert het antwoord; laat ik het zo zeggen.

De heer **Van den Boom**: Het verlengen van de bewaarperiode heeft naar mijn idee met name consequenties voor de opslagcapaciteit, voor het aantal schijven dat nodig is om data op te slaan, voor de beheerskosten van die data en voor de benodigde beheerscapaciteit omdat de bestanden groter worden en voor de bevragingscapaciteit. Als ik een grotere bak met gegevens moet doorzoeken, zijn daarvoor meer tijd en wellicht complexere tools nodig. Daarin zitten met name de kostenverhogende factoren. De initiële kosten zijn namelijk al gemaakt.

Mevrouw **Duthler** (VVD): Dat betreft vooral hardware en software?

De heer **Van den Boom**: Hardware, software en personeelskosten voor het beheer van die hardware en software. Verder zijn er kosten voor het doorzoeken. Als een behoeftesteller vraagt om de bestanden te gaan doorzoeken en de totale omvang van die bestanden is groot, is er meer tijd nodig om die te doorzoeken.

Mevrouw **Duthler** (VVD): Maar de personeelskosten heb je al, ook voor een kortere bewaarperiode.

De heer **Niesen**: Ja, maar men heeft meer personeel nodig. In het VKA-rapport staat dat het verlengen of verkorten van de opslag procentueel gezien tot een gering verschil zal leiden. Omdat de set-up kosten voor kleine ISP's redelijk hoog zijn, moeten wij ons wel realiseren dat dit voor hen wel bottom line is. Het zijn kleinere schouders die deze kosten moeten dragen. Ik onderschrijf volledig de opmerking van de heer Van den Boom dat de volwassenheid van processen bij dat soort bedrijven op een lager niveau ligt. Zij moeten echt een slag maken om dit op een goede manier te beheersen en te beheren. Of het nu zes maanden of twaalf maanden is, het zal in beide gevallen hetzelfde zijn, maar het is wel een aspect dat meespeelt.
In vraag 6 wordt gevraagd of bij push-e-maildiensten als Blackberry, iPhone en Microsoft Windows Mobile helemaal geen sprake is van in- en uitloggen. Bij ons bedrijf wordt ook gewerkt met pushmail, gewoon op onze laptops. Dat gaat veel verder dan alleen maar de mobiele devices. Ik heb wat problemen met de vraagstelling. Er wordt een relatie gelegd tussen het aan- en afloggen en het wel of niet onder de bewaarplicht vallen. Bij pushmail ben je eigenlijk altijd aangelogd. Je authenticeert je maar één keer, namelijk bij het aandoen van je telefoon. Dan meld je je eigenlijk aan. Alle systemen werken iets anders, maar in principe is het zo dat er wel degelijk verkeer is tussen de device en de e-mailserver. Ik zie dat niet anders dan dat je gewoon een e-mail verstuurt van een ISP aan een laptop of een desktop. Het antwoord op vraag 6 is dus nee.

De heer **Franken** (CDA): Het valt dus niet buiten de bewaarplicht?

De heer **Van den Boom**: Wat mij betreft niet.

De **voorzitter**: Het genereert in ieder geval verkeersgegevens die registreerbaar zijn.

De heer **Van den Boom**: Er is geen sprake van frequent in- en uitloggen.

De **voorzitter**: Valt het dan wel onder de begripsomschrijving in de bijlagen A en B bij het wetsvoorstel?

De heer **Van den Boom**: Ja, want er is eigenlijk altijd een verbinding. De volgende vraag heeft betrekking op de technische mogelijkheid om gegevens te wissen na 12 maanden. Dat is technisch inderdaad mogelijk. Men kan bijvoorbeeld records voorzien van een timestamp en op basis daarvan selecteren en wissen. Afhankelijk van de gemaakte afspraken wordt daarvoor een bepaalde dag, een bepaald uur of een bepaalde seconde gekozen. Dat kan heel gedetailleerd gebeuren. Met name voor kleinere partijen die dit handmatig gaan doen, is het niet mogelijk om de gegevens op secondebasis te wissen. Een dag is dan veel logischer. Als een grotere partij werkt met automatische tooling, kan het geautomatiseerd worden en maakt het niet zo veel uit welke selectie en interpretatie gegeven wordt aan de termijn voor vernietiging. Technisch gezien kan het wel.

De heer **Niesen**: Ik wil een nuancering aanbrengen. Het probleem is dat de wet niet duidelijk is over het moment van communicatie. Is dat tijdens het opstarten van een communicatie of nadat de communicatie klaar is? Dat is nog niet uitgewerkt in de definitie. Als je kiest voor het moment waarop de communicatie klaar is, ben ik het helemaal met de heer Van den Boom eens. Als je echter zegt dat het het moment is waarop het eerste contact wordt gemaakt, kan ik een heleboel situaties bedenken, bijvoorbeeld een VoIP-gesprek dat voor middernacht begint en na middernacht eindigt, waarbij problemen ontstaan als je het op dagbasis leeggooit. Het loopt dan namelijk over een datum heen.
In de meeste gevallen zal het absoluut geen probleem opleveren, maar er zijn situaties te bedenken waarin dat wel het geval is. Een ander voorbeeld is het kabelmodem dat eigenlijk altijd is aangelogd. Wanneer leg je dat dan vast? Wanneer ga je dat weggooien? Het kan best drie maanden duren voordat het weer wordt afgelogd. Wil je de gegevens dan pas na een jaar en drie maanden weggooien of na precies een jaar?

De heer **Franken** (CDA): Dat is precies de vraag. Uw antwoord is dat je dat dus niet kunt scheiden?

De heer **Niesen**: Dat kun je pas scheiden wanneer je vaststelt wat het moment moet zijn. Wat is de timestamp? Is dat het begin of het einde van de communicatie? Het is een definitiekwestie.

De **voorzitter**: Ik denk dat wij vrij gemakkelijk kunnen proberen om dat punt nog te verhelderen.

De heer **Niesen**: Het eerste deel van vraag 8 is wat mij betreft correct. Dat gebeurt heel veel. Technisch gezien is openbaar en niet-openbaar verkeer hetzelfde. Als een server ergens staat op een IP-adres, kun je zeggen dat het niet openbaar is. Op basis van dat IP-adres zou je het kunnen scheiden. Dat is niet in de systemen ingebakken. Er zijn manuele processen nodig om dat voor elkaar te krijgen.

De heer **Franken** (CDA): Wat is dan uw concluderend antwoord op die vraag? De aanbieder van de connecting service moet de gegevens bewaren en desgevraagd uitleveren. Er gebeuren echter dingen die hij niet ziet, terwijl hij daarvoor wel verantwoordelijk is.

De heer **Van den Boom**: Er gebeuren dingen die hij niet ziet.

De heer **Franken** (CDA): Er wordt een server geplaatst en langs die server vindt een bepaalde berichtenuitwisseling plaats. De ISP zelf heeft geen zicht op de gegevens die daar langsgaan. Die gaan buiten zijn weten via de server die bij hem in het gebouw staat.

De heer **Van den Boom**: Dat klopt. Er zijn voorbeelden van mensen die een abonnement hebben bij een internetserviceprovider en via dat abonnement bijvoorbeeld gebruikmaken van skypetelefonie. Er vindt dan geen registratie plaats van een skypetelefoongesprek en van het feit dat er van A naar B een gesprek plaatsvindt. Skype is een voorbeeld, maar zo zijn er verschillende messaging services. Het is ook mogelijk om tunnels te bouwen over het internet, waarbij gesprekken die via internet plaatsvinden niet via de bekende labels als Skype of Microsoft messenger maar via specifiek op maat gemaakte oplossingen die niet zichtbaar zijn. Dat klopt.

De **voorzitter**: Er vindt dus communicatie plaats zonder dat die enig verkeersgegeven genereert dat geregistreerd wordt en onder de werking van deze wet zal vallen. Zeg ik dat goed?

De heer **Van den Boom**: Er wordt geregistreerd dat bijvoorbeeld mijnheer Jansen uit Utrecht een internetverbinding heeft openstaan. Dat is terug te vinden, maar het soort gebruik wordt niet vastgelegd omdat het diensten betreft die buiten de wet vallen.

De heer **Franken** (CDA): Er is dus wel communicatie mogelijk?

De heer **Van den Boom**: Inderdaad.

De **voorzitter**: Nog even heel specifiek. Ik ben advocaat en ik werk via mijn laptop met een VPN-verbinding met kantoor. Andere collega's doen dat ook. Ik communiceer via die VPN met hen thuis door middel van een mailtje. Wordt dat wel of niet geregistreerd?

De heer **Van den Boom**: In dit geval valt het buiten de wet omdat het binnen het kantoornetwerk valt. Het wordt niet geregistreerd. Als u via uw privéadres mailt naar kantoor, wordt het wel geregistreerd.

De heer **Niesen**: Het wordt niet geregistreerd omdat het niet openbaar is. Het wordt ook niet geregistreerd omdat het encrypted is. Alleen is duidelijk dat een verbinding openstaat, maar wat door de tunnel gaat, is niet helder.

Mevrouw **Broekers-Knol** (VVD): Als je een communicatie wilt zonder dat die geregistreerd wordt, heb je zo'n tunnel nodig? Dus boosaardige types hebben een tunnel? Ik zeg het eenvoudig, maar dan begrijp ik het beter.

De heer **Niesen**: Het causale verband is wat mij betreft niet helemaal juist. Boosaardige types zouden een tunnel kunnen hebben, maar er zijn boosaardige types die veel makkelijkere manieren weten om hier buitenom te gaan dan door tunnels te bouwen. Dat komt aan de orde in de vragen 16 en 17.

De **voorzitter**: Wij zijn nu ongeveer op de helft van de vragen. Ik zal proberen mij een beetje in te houden.

De heer **Niesen**: Ik vraag mij af, of vraag 9 hiermee ook niet voldoende beantwoord is.

De heer **Van den Boom**: Vraag 10 betreft het onderscheid tussen telefonie en internet. Gevraagd wordt in feite of de kosten voor ISP aanzienlijk groter zijn dan voor de telecomproviders. Wij hebben daarstraks al gezegd dat de telecomproviders al gewend zijn aan het registreren van de gevraagde gegevens, terwijl de ISP's dit in veel gevallen nog moeten opbouwen.

De heer **Niesen:** Vraag 11 bestaat eigenlijk uit vier vragen. Ik ben geen opsporingsexpert maar zou mij kunnen voorstellen dat de gegevens die langs deze weg geanalyseerd worden, hooguit als ondersteunend bewijs kunnen dienen. De gegevens kunnen namelijk nooit getraceerd worden naar een persoon maar alleen naar een device.

De **voorzitter**: Voor uw duidelijkheid, de minister zegt in de stukken dat verkeersgegevens een aanwijzing kunnen vormen die vervolgens een opstart kunnen geven aan een opsporingsonderzoek en dat ook niet valt te verwachten dat zij uiteindelijk een doorslaggevend bewijs zullen leveren in het kader van bewijsvoering voor de strafrechter. De minister is zich daarvan bewust.

De heer **Niesen**: Het is inderdaad best mogelijk om onjuiste conclusies te trekken. Ik geef een voorbeeld. Veel internetverbindingen, bijvoorbeeld wifi en hotspot, zijn vrij toegankelijk. Er zijn veel voorbeelden te geven van gevallen waarin een huiscomputer gehackt wordt, waardoor het lijkt alsof iemand iets gedaan heeft dat hij eigenlijk niet gedaan heeft: IP-spoofing. Er zijn veel redenen die onderbouwen dat het mogelijk is om onjuiste conclusies te trekken.
E-mail werkt alsof je iets op de brievenbus doet. Bij telefoneren is er een connectie van A naar B. Op het moment dat iemand aan de andere kant van de lijn opneemt, weet je zeker dat je contact hebt met degene die je belt. Hier is dat niet zo. Je weet nooit zeker of de communicatie echt wordt ontvangen aan de andere kant. De protocollen die daarvoor gebruikt worden, voorzien niet in de mogelijkheid dat je een bericht terugkrijgt als de communicatie is aangekomen. Dat is wel het geval als je een brief aangetekend verstuurd met bericht van ontvangst. Er zijn veel voorbeelden dat men wel iets heeft verstuurd maar dat het nooit is aangekomen.

De **voorzitter**: Daar hebben wij allemaal ervaring mee.

De heer **Niesen**: Dynamische IP-adressering leidt alleen maar tot meer logging, maar technisch gezien is het wel mogelijk. Het betekent wel dat als een IP-adres wijzigt, je het opnieuw moest vastleggen. Dat zorgt dus voor extra logging.

De heer **Franken** (CDA) Dan moeten er wel veel meer gegevens bewaard worden. Het gaat er naar toe dat je niet als abonnee een vast IP-adres hebt, maar dat per boodschap een IP-adres wordt toegekend.

De heer **Niesen**: De curve van dit soort loggegevens gaat heel stijl omhoog. Als wij twee jaar verder kijken, is het zeer behoorlijk toegenomen. IP versie 6 zal tot nog veel meer gegevens leiden. Op basis van de huidige casuïstiek kan dat. Het leidt absoluut tot meer logging.

De heer **Franken** (CDA): En meer bewaren en meer terugzoeken.

De heer **Niesen**: Inderdaad.

Mevrouw **Van Bijsterveld** (CDA): Kun je bij die dynamische IP-gegevens wel vaststellen dat het bericht steeds van dezelfde afzender komt, ook al is hier sprake van een ander adres?

De heer **Niesen**: Het is geen ander adres. Er zijn ISP's die met vaste IP-adressen werken. Ik heb thuis een vast IP-adres. Er zijn ook ISP's die anders werken. Dat stamt uit het verleden. Toen je nog een connectie maakte met een telefoonlijntje, kreeg je een IP-adres. Dat betekent alleen dat een extra regel in het bestand moet worden opgeslagen en doorzocht moet kunnen worden. De systematiek is niet anders.

De **voorzitter**: Blijven die gegevens dan wel traceerbaar naar een locatie?

De heer **Niesen**: Ja, want er zit een timestamp op.

De heer **Franken** (CDA): Maar mijnheer Pietersen heeft niet meer één IP-adres. Als mijnheer Pietersen 1000 e-mails per dag verstuurt, heeft hij opeens 1000 adressen.

De heer **Niesen**: Dat klopt. Dat compliceert het doorzoeken.
Het antwoord op de laatste subvraag is dat het vrijwel nooit met zekerheid is aan te tonen dat communicatiegegevens wel of niet aan een contractant toebehoren. Het is zo gemakkelijk om in te breken of om je anders voor te doen dan je daadwerkelijk bent op het internet. De foutkans is voorspelbaar, zeker als mensen kwaadwillend zijn.

Mevrouw **Strik** (GroenLinks): Kunt u in percentages het risico aangeven dat het niet juist is?

De heer **Niesen**: In een van de latere vragen wordt terecht gesteld dat het leeuwendeel van de spamberichten niet afkomstig is van daadwerkelijke e-mailadressen. Dat is bijna 100%. Het merendeel van de georganiseerde misdaad weet hoe dit moet worden omzeild. Die mensen maken van dit soort systematiek gebruik om ervoor te zorgen dat zij niet te herleiden zijn.

De **voorzitter**: Als ik een brief verstuur en op de voorkant het adres van de geadresseerde zet en op de achterkant het adres van mevrouw Broekers bijvoorbeeld, is dat niet wezenlijk anders.

De heer **Niesen**: Ik denk dat het klopt.

De **voorzitter**: Niet dat ik ooit die aanvechting heb gehad, maar ik noem het puur als illustratie.

De heer **Van den Boom**: De volgende vraag is gericht op acceptabele beheerscriteria. De beheerscriteria van data zitten in eerste instantie in heldere afspraken. De timestamps waarover wij spraken, zijn natuurlijk niet bruikbaar als ISP 1 zijn klok anders heeft staan dan de andere ISP's. Als de klokken niet juist lopen, staan de registraties ook allemaal fout. Je moet controleren in de vorm van hashtotals. Je moet controleren of het verkeer dat in het systeem heeft plaatsgevonden, ook volledig in de opslag is meegenomen. Verder zijn er criteria voor de daadwerkelijke opslag, zoals het acceptabele uitvalpercentage. Er zijn ook standaarden op het gebied van informatiebeveiliging zoals de code voor informatiebeveiliging. Daarin worden de gebieden aangegeven die relevant zijn voor het beheer en de inrichting van beveiliging van gegevens. U moet daarbij denken aan vragen als: Hoe ga ik om met toegangverlening? Wat moet ik hebben geregeld op het vlak van back up en recovery, van uitwijken? Een

organisatie kan gebruikmaken van een scala aan richtlijnen om het beheer van de gegevens in te richten.

De heer **Niesen**: De volgende vraag betreft het onderscheid tussen netwerkaanbieders en dienstenaanbieders. Die kunnen elkaar overlappen, maar dat hoeft niet zo te zijn en dat compliceert de zaak inderdaad aanzienlijk. Als daarover geen zeer goede afspraken gemaakt worden, loop je inderdaad de kans dat zaken op verschillende plekken worden opgeslagen en niet duidelijk is wie precies verantwoordelijk is voor welke data. Ik denk dat ik deze vraag aan de heer Van den Boom doorgeef.

De heer **Van den Boom**: Er zijn partijen die als dienstenleverancier volledig hun diensten leveren. Vergelijkbare diensten kunnen ook volledig zijn uitbesteed. Bij de Rabomobiel heeft de Rabo niet zelf de infrastructuur staan om die mobiele dienst te leveren. De Rabo maakt hier gebruik van KPN. Het klantbeheersysteem zit bij de Rabo, maar verder vindt de hele afhandeling van de telefoongesprekken plaats bij KPN. In dit geval zou aan de netwerkkant, dus aan de KPN-zijde, de registratie moeten plaatsvinden. Het is een kwestie van het maken van eenduidige afspraken over waar de verantwoordelijkheid neergelegd wordt. Ik zou mij goed kunnen voorstellen dat men afspreekt, de verantwoordelijkheid te leggen aan de dienstenkant. Bij modellen waarbij een netwerkbeheerder een dienst aanbiedt aan een dienstaanbieder, moet de dienstaanbieder in zijn contract afspreken dat het leveren van die dienst zowel inhoudt dat de klant kan bellen als het registreren conform de wet- en regelgeving. Als je daarover geen heldere afspraken maakt, loop je het risico dat er dubbele registratie plaatsvindt of dat er geen registratie plaatsvindt. Het maken van afspraken is heel belangrijk. In het geval van de Rabo en KPN is het heel helder. Er zijn ook allerlei hybride modellen waarbij op verschillende fronten sprake is van overlap. Hoe ga je daarmee om?

De heer **Niesen**: Ik heb het niet helemaal uitgefilosofeerd, maar ik zou mij kunnen voorstellen dat je de dienstaanbieder in dezen leading laat zijn. Indien hijzelf niet het netwerk beheert, moet hij vervolgens als een soort onderaannemer met de desbetreffende netwerkaanbieder afspreken dat die het moet vastleggen. De bal moet primair bij de dienstaanbieder gelegd worden. Andersom werkt het in ieder geval niet, dat is duidelijk.

De **voorzitter**: Betekent dit niet dat om traceerbaar te zijn, ook iedere transactie met een simkaart geregistreerd en vastgelegd zou moeten worden? Wij hebben geen telefoonkaarten meer. Daarmee kon je volstrekt anoniem op alle mogelijke plaatsen bellen. Je koopt een telefoon, maar er wordt niet geregistreerd aan wie die telefoon verkocht wordt. Als ik de simkaart vervolgens aan u geef, kunt u daarmee doen wat u wilt en is naar mij geen enkele link te leggen.

De heer **Niesen**: Dat is inderdaad correct. Die situatie wordt niet veranderd door deze bewaarplicht.

De heer **Van den Boom**: Er valt niet te herleiden wie de beller is. De rest van de registratie vindt wel plaats in dit geval. Het zijn prepaid services.

De heer **Niesen**: Wat mij betreft, slaat vraag 14 terug op vraag 1. Ik stel voor dat wij die overslaan.
In vraag 15 staat dat niet wordt beoogd om de inhoud van de communicatie vast te leggen. Dat is inderdaad duidelijk.
Er hoeft geen sprake te zijn van overlap, maar het kan wel. Ik zal proberen dit aan de hand van een voorbeeld duidelijk te maken. Als een e-mailtje verstuurd wordt van buiten de Europese Unie naar Nederland, gaat het langs een aantal hubjes. Het is niet van te voren vast te leggen langs

welke hubjes hij gaat, maar uiteindelijk komt hij bij de ISP terecht. De ISP ziet alleen het laatste stukje van de weg. De wet beoogt natuurlijk de originele afzender te kunnen zien, maar die informatie zit in de enveloppeheader van het berichtje en dat wordt gezien als inhoud van het mailbericht. Het klopt dat als e-mailtjes verschillende bruggetjes over moeten en sluisjes door moeten, je eigenlijk in de inhoud moet kijken om het gehele pad te zien en dat kan niet. In dat geval kan de ISP alleen zeggen: het bericht komt van de Amsterdam Exchange of van KPN.

De heer **Van den Boom**: In vraag 16 wordt gevraagd, hoe gemakkelijk het is voor gebruikers om de bewaarplicht te omzeilen. Welke mogelijkheden zijn er om te communiceren via telefonie of e-mail, zonder dat van dat verkeer bruikbare verkeersgegevens worden bewaard? Zojuist hebben wij al gezegd dat er diverse mogelijkheden zijn om dat te doen, bijvoorbeeld van internettelefoondiensten en mailverkeer via buitenlandse providers zoals Hotmail en Gmail. Dat zijn veel gebruikte webmailprogramma's. Het kan ook op andere wijze. Op internet zijn allerlei uitwisselsystemen en social netwerkprogramma's, bijvoorbeeld een fotouitwisselprogramma. Er zijn heel veel internettoepassingen waarmee gegevens kunnen worden uitgewisseld zonder dat die geregistreerd worden.

De heer **Niesen**: Of foutief geregistreerd worden.

Mevrouw **Broekers-Knol** (VVD): Dat betekent eigenlijk dat alleen recht op en neer e-mailberichten geregistreerd worden en dat iemand uit het zicht is zodra hij iets kunstzinniger aan de slag gaat?

De heer **Van den Boom**: Dat klopt.

Mevrouw **Strik** (GroenLinks): Dit is voor de echte domme boeven.

De heer **Franken** (CDA): U geeft hiermee ook aan dat er niet veel kosten gemaakt hoeven te worden om het te omzeilen en er nauwelijks technische kennis voor nodig is. Die programma's worden gratis aangeboden. Skype komt bij mij drie keer per dag langs met de vraag of ik het wat uitgebreider wil nemen. Dat is dus bij iedereen bekend.

De heer **Van den Boom**: Ja, bovendien heeft een programma als Skype op dit moment meer dan 370 mln. gebruikers wereldwijd. Het zijn geen exoten meer.

De heer **Franken** (CDA): Dus meer dan 370 mln. mensen vallen al buiten de bewaarplicht?

De heer **Van denBoom**: Maar niet binnen Nederland.

De **voorzitter**: Hoeveel zijn het er in Nederland?

De heer **Niesen**: Het aantal is snelgroeiend. Ik denk dat bij de doelgroep van deze wetgeving het percentage aanzienlijk hoog ligt. Als wij het kunnen bedenken, kunnen zij dat ook. Alle MSN-verkeer valt hier ook niet onder.

Mevrouw **Broekers-Knol** (VVD): MSN is hetzelfde als sms?

De heer **Niesen**: Nee, het is eigenlijk een soort sms maar dan via de computer. Je ziet in het schermpje «hallo» en tikt dan iets terug. Er is wel een directe communicatie.
Het wordt heel erg toegespitst op e-mail, maar surfgedrag valt daar dus niet onder. Er zijn veel websites zoals i Google, dat zijn combinatiesites

waarop berichtenverkeer kan worden uitgewisseld dat door de provider zal worden gezien als webverkeer en niet zal leiden tot opslag van enige gegevens.

De **voorzitter**: Bij verkeersgegevens praat je dus eigenlijk over die gegevens die in zekere zin ook voor facturatie van belang zijn, terwijl bij alle diensten die gratis worden aangeboden er geen enkel belang is om dergelijke verkeersgegevens te registreren, anders dan statistische gegevens om adverteerders te verleiden tot het plaatsen van advertenties op sites en dergelijke?

De heer **Van den Boom**: Nee. Het normale e-mailverkeer via een serviceprovider in Nederland valt wel onder de wet. Qua karakter is het vergelijkbaar met de webmail. MSN is qua karakter een heel andere manier van communicatie. Het daaraan koppelen van reclame et cetera is wat mij betreft iets heel anders.

De heer **Niesen**: Bij een telecomprovider bel je van A naar B en dat leidt tot een factuurregel. Bij ISP's werkt dat niet zo. Die systemen zijn ook niet ingericht om dat soort gegevens vast te houden. Dat compliceert de zaak wel, want deze operationele gegevens zijn per definitie niet aanwezig bij dit soort clubs. Die zullen dat alsnog moeten realiseren.

Mevrouw **Westerveld** (PvdA): Bent u van mening dat al de aspecten die niet geraakt worden door die wet, niet geraakt worden omdat er niet aan gedacht is of omdat het zo ontzettend ingewikkeld wordt dat het eigenlijk niet te doen is?

De heer **Niesen**: Ik denk dat er twee antwoorden mogelijk zijn. Inderdaad zijn er heel veel manieren om het te omzeilen. Is het überhaupt effectief? Natuurlijk gaat het heel erg snel. Ik noem twitteren. Dat is een soort hybridevorm van aan de ene kant SMS-verkeer en aan de andere kant een computer. Valt dit er wel of niet onder? Ik denk gedeeltelijk. Volgend week wordt er weer iets anders uitgevonden. Er moet altijd een inhaalslag gemaakt worden om de bozerikken bij te blijven.
Als het wereldwijd georganiseerd wordt en de Amerikanen doen het op dezelfde manier, dan pakken zij het stukje Hotmail en zou je samen misschien wel alle gegevens krijgen waarmee het probleem kan worden opgelost.

De heer **Franken** (CDA): Amerika kent geen bewaarplicht.

De heer **Niesen**: Nederland op dit moment ook nog niet.

De heer **Van den Boom**: Wij spraken over Skype en 370 mln. gebruikers wereldwijd. Uit onderzoek van het Webmagazine blijkt dat 30% van de Nederlanders wel eens gebruikmaakt van een dergelijke communicatievorm. In de leeftijdscategorie van 12 tot 25 jaar de helft. Dat geeft een indicatie.

De **voorzitter**: Mijnheer Niesen, eigenlijk zegt u dat het dichten van de lekken alleen maar mogelijk is door wereldwijd afspraken te maken?

De heer **Niesen**: Als het beperkt wordt tot Nederland, zie ik zoveel lekstromen dat het bijna onmogelijk is. Dat zie je ook in het rapport. Slechts een beperkt aantal dossiers had betrekking op internetgegevens. In al die dossiers was een link met Hotmail of Gmail. Als dat bekeken zou worden vanuit de gedachte van deze wetgeving, zou je het dossier niet rond krijgen.

De **voorzitter**: Met wereldwijd maken, dek je het e-mailverkeer af. De andere diensten blijven buiten scope. Hotmail en Gmail worden daarmee dus wel afgedekt?

De heer **Niesen**: Onder 17 wordt gevraagd, hoe moeilijk het is om (al dan niet opzettelijk) te bewaren gegevens te genereren die een verkeerd beeld geven over de communicatie. Er worden zeer treffende voorbeelden genoemd die inderdaad breed worden toegepast. Er wordt iets gestuurd maar de afzender is niet juist; de IP-spoofing-achtige dingen. Dat lijkt heel erg technisch maar is relatief simpel. Een ander voorbeeld: er is wel communicatie maar degene die je denkt dat het stuurt, is niet degene die het stuurt. Er wordt gebruikgemaakt van het netwerk van iemand anders. Dat komt veel voor. Wat hier staat, klopt wel.

De heer **Franken** (CDA): Identiteitsfraude is dus heel gemakkelijk te realiseren? Iemand kan als verdachte worden aangemerkt terwijl hij er helemaal niets mee te maken heeft?

De heer **Niesen**: Dat is zeer wel mogelijk. Volgens mij biedt Hotmail zelfs de mogelijkheid om het Van-veld aan te passen. Je kunt gewoon zeggen dat het van iemand anders komt, terwijl jij het wel verstuurt.
Alle spam komt niet van het adres dat erop staat.

De heer **Van den Boom**: Daarbij komen wij bij vraag 18. Is het juist dat SMTP-servers niet controleren of de afzendergegevens juist zijn? Dat klopt inderdaad. Een van de beperkingen van het SMTP-mailverkeer is juist dat de afzender niet vaststaat. Daardoor is het heel gemakkelijk om spamverkeer te genereren en een onjuiste afzender mee te geven.

De heer **Niesen**: Het antwoord op vraag 19 is: bijzonder weinig.
Technisch gezien kan spam niet onderscheiden worden van gewone gegevens.

De heer **Kox** (SP): Het is fascinerend dat de hele wereld bezig is met het weggooien van dingen die men niet wil hebben en dat wij nu een systeem ontwikkelen om gegevens te bewaren. De conclusie is dat wij spam bewaren plus nog enkele andere zaken?

De heer **Niesen**: Wij bewaren gegevens over spam. Het bericht zelf wordt weggegooid.

De heer **Kox** (SP): Heeft u daar een oordeel over?

De **voorzitter**: Het oordeel is voorbehouden aan de Kamer. Daarover hoeven de experts zich niet uit te laten.

De heer **Kox** (SP): Ik vraag geen politiek oordeel. Ik vraag of dit een logische manier van gegevens bewaren is.

De **voorzitter**: Misschien moeten wij het anders formuleren. Stel dat u de minister zou mogen adviseren om een aanpak te kiezen die wel tot een beter resultaat leidt dan wat u op dit moment beschreven hebt, wat zou er dan moeten gebeuren, ervan uitgaande dat de minister onverkort volhoudt dat dit niet ertoe leidt om bewijs rond te maken maar om aanknopingspunten te hebben voor het starten van enig verkennend onderzoek of zelfs een opsporingsonderzoek?

De heer **Niesen**: Ik denk dat het zowel kosteneffectief als tijdeffectief kan zijn om een soort uniforme aanpak voor te schrijven voor de wijze waarop

ISP's dit moeten gaan inrichten. Aan het begin van het gesprek hebben wij gezegd dat elke ISP anders is en dat geldt ook voor hun systemen. Als je de onderliggende gegevens op deze manier aan de ISP's zou geven, weet ik zeker dat je 300 verschillende implementaties zult zien. Zij zijn dus niet hetzelfde. De wet biedt heel veel ruimte voor interpretatie. Ik vrees dat het tot veel onnodige kosten leidt en ik ben ook bang dat de kwaliteit van de gegevens die uiteindelijk worden vastgelegd, eronder lijdt.

De **voorzitter**: Daarmee hebt u dan de eerste 10 vragen getackeld, maar nog niet de laatste vragen van dit rijtje. De ontwijkingsmogelijkheden hebt u immers nog niet getackeld? Daartoe ziet u ook geen mogelijkheden?

De heer **Van den Boom**: Ik denk dat het ontzettend lastig is om dat sluitend te krijgen, gezien de ontwijkingsmogelijkheden, het open karakter van het internet en de mogelijkheden die de technologie biedt. Dat geldt zowel voor de Nederlandse wetgeving als voor EU-wetgeving.

De heer **Niesen**: In het VKA-rapport is een datamodel opgesteld. Het VKA heeft het vaak over MAC-adressen in plaats van over IP-adressen. Een MAC-adres ligt eigenlijk onder het IP-adres. Een IP-adres is heel makkelijk aan te passen en een MAC-adres geeft iets meer zekerheid, maar geen 100%, zeker niet. Het zal de barrière ietsje groter maken. Het vervelende is dat mensen die kwaad willen, precies weten waar zij moeten zijn.

De **voorzitter**: Ook hier kun je een vergelijking maken met de brief. Alle brieven worden tegenwoordig alleen nog maar in Nieuwegein afgestempeld. Dus aan het poststempel kun je niet meer zien waar een brief vandaan komt. Als je per brievenbus een stempel erop zou zetten, zou je meer informatie hebben.

De **voorzitter**: Dames en heren, het is inmiddels kwart over zes geweest. Mag ik vragen of de leden nog bepaalde punten willen aanroeren en aan de heren vragen of zij nog dingen willen zeggen die wij niet gevraagd hebben en die relevant kunnen zijn voor onze beraadslaging?

De heer **Franken** (CDA): Mag ik iets heel praktisch vragen, voorzitter? Ik zie dat de deskundigen prachtige aantekeningen hebben gemaakt. Zou het handig zijn om die aan ons te overleggen, mits zij natuurlijk van die gegevens afscheid willen nemen?

De heer **Niesen**: Wat wij hier gezegd hebben, wordt stenografisch vastgelegd.

De **voorzitter**: Heren, hebt u nog iets te berde te brengen waarvan u denkt: daarmee zou de Eerste Kamer haar voordeel kunnen doen?

De heer **Van den Boom**: Nee, wat mij betreft zijn de punten die van belang zijn allemaal aan de orde gekomen.

De **voorzitter**: Dan dank ik u beiden hartelijk. Het was heel verhelderend. Wij hebben er veel van opgestoken. Er volgt eerst nog een schriftelijke gedachtewisseling met de minister over dit wetsvoorstel en daarna een plenaire behandeling. Wij zullen u daarvan graag op de hoogte houden. Het stenografisch verslag verschijnt eerst in conceptvorm. Wij hebben de mogelijkheid van correctie. Ik zal de griffie vragen om ook u het concept

toe te sturen, want er zijn termen gebruikt waarvan ik mij kan voorstellen dat zelfs de DVR zich deze nog niet eigen heeft gemaakt.
Zeer bedankt.

De voorzitter van de vaste commissie voor Justitie,
Van de Beeten

De griffier van de vaste commissie voor Justitie,
Van Dooren

Bijlage

Technische vragen ter voorbereiding op de expertbijeenkomst

1. Op de bijlage van het wetsvoorstel is aangegeven welke gegevens worden vastgelegd. Dit betreft iedere in- en uitgaande mail, in- en uitgaande internettelefoonoproep, in- en uitlog van de internet- of e-maildienst. Om hoeveel «communicaties» per dag zal het dan gaan?

2. Bestaat de hardware en software technologie en verwerkingscapaciteit om voor duizenden simultane communicaties «live» verschillende systemen te bevragen die tot op heden niet aan elkaar verbonden zijn (zoals de e-mail server, de telefonieserver, de facturatiesystemen etc.), daaruit alle informatie te extraheren die op de bijlage bij de wet staat vermeld en deze informatie weg te schrijven? Welke infrastructuur dient hiervoor te worden aangelegd en welke verwerkingscapaciteit is daarvoor nodig? Hoelang duurt het om daarmee de gewenste informatie te verkrijgen? Zijn er in de toekomst technische voorzieningen beschikbaar die de verwerkingstijd kunnen versnellen?

3. Stel dat het mogelijk zou zijn om de hiervoor bedoelde informatie van elke communicatie onmiddellijk bij elkaar te brengen en op te slaan, hoe zou dat dan worden opgeslagen? In een groot en immer groeiend tekstbestand, bijvoorbeeld per dag een nieuw tekstbestand en dan na een jaar het oudste dagbestand wissen, etc? Of zou het noodzakelijk zijn hiervoor een database te ontwerpen, te programmeren en bij te houden?

4. Stel u bent bij een middelgrote internetaanbieder verantwoordelijk voor de technische implementatie van de bewaarplicht. Kunt u concreet aangeven welke werkzaamheden u denkt dat er verricht zouden moeten worden en welke investeringen in tijd, menskracht en apparatuur hiervoor nodig zijn?

5. In hoeverre zal een langere bewaartermijn dan 6 maanden meer (werk-)belasting en kosten met zich meebrengen voor het bedrijfsleven en hoe is de verhouding van de verlenging van de bewaartermijn ten aanzien van de reeds gedane en bedrijfsmatig noodzakelijke investeringen?

6. Klopt het dat bij push e-mail diensten (zoals Blackberry, Microsoft Windows Mobile en iPhone) helemaal geen sprake is van in- of uitloggen, omdat deze diensten zich juist kenmerken doordat de klant zijn mail niet ophaalt maar dat de server deze naar hem toestuurt? Klopt het dat e-mail verkeer van en naar dergelijke apparaten dus buiten de bewaarplicht valt?

7. Is het technisch wel mogelijk om gegevens na precies 12 maanden te wissen zonder ook gegevens te wissen die juist nog bewaard moeten worden?

8. Is het juist dat veel servers en andere netwerkonderdelen worden gebruikt voor de levering van diensten van derden, die daarmee – buiten het gezichtsveld van de netwerkaanbieder – allerlei diensten kunnen aanbieden die als openbaar verkeer wel of als niet-openbaar verkeer niet onder de Telecomwet (Tw) vallen, zodat het voor de aanbieder ook niet kenbaar is of het daarmee gegeneerde verkeer onder de bewaarplicht valt?

9. Hoe zou een aanbieder zijn systemen moeten instellen om automatisch onderscheid te maken tussen openbaar en niet-openbaar verkeer dat over dezelfde netwerkdelen wordt vervoerd? Klopt het dat dat technisch onmogelijk is, zodat onvermijdelijk is dat ook verkeersgegevens van niet-openbaar telecommunicatieverkeer (bijv. verkeer binnen bedrijven, universiteiten en overheidsorganisaties) zullen worden opgeslagen en later door behoeftestellers doorzocht en bevraagd?

10. Onderscheid telefonie (bijlage onder A) en internet (bijlage onder B): voor telefonie betreft de bewaarplicht vooral het langer bewaren van gegevens die aanbieders toch al bewaren voor facturering en verrekening en ter nakoming van artikel 13.4 lid 2 Tw. Dit geldt niet voor de internetgegevens: die worden nu niet vergaard / bewaard, zodat de (complexiteit, kosten en overige bedrijfsmatige impact) van de vereiste maatregelen onvergelijkbaar groot zijn.

11. De meeste van in de bijlage B genoemde diensten worden, anders dan doorgaans bij telefonie het geval is, geleverd zonder sluitende identificatie van abonnees, laat staan gebruikers. Registratie van contractanten is beperkt en voor gebruikers wordt nagenoeg niets geregistreerd. Deze feiten waren bekend bij het opstellen van de Wet, op welke wijze kan toch de doeltreffendheid voor de opsporing hier geborgd zijn? Klopt het dat de kans op opslag van onjuiste gegevens – en dus, in de opsporingsfase, onjuiste conclusies en onschuldige slachtoffers – bij internetgegevens dus aanzienlijk groter is dan bij telefonie? Is het technisch haalbaar om bij gebruik van dynamische IP adressering zoals door netwerkaanbieders wordt gehanteerd, op elk moment vast te stellen aan welke contractant een communicatie moet worden toegerekend? Is op enigerlei wijze achteraf aan te tonen dat communicatiegegevens aan een ander dan de vastgelegde contractant toe te rekenen zijn?

12. Als de in bijlage B genoemde gegevens vóór de invoering van de wet niet worden opgeslagen wat zijn dan acceptabele beheerscriteria voor het opslaan van deze gegevens (acceptabele uitval percentages, backup systemen etc.) in het kader van de bewaarplicht?

13. Onderscheid netwerkaanbieders en dienstaanbieders: de bewaarplicht is van toepassing op zowel netwerkaanbieders als dienstaanbieders. Kunt u aangeven welke van de in de bijlage onder B genoemde gegevens relevant is voor welke van deze groepen? Is daarmee duidelijk welke gegevens door wie moeten worden opgeslagen zodat met name de in bijlage B genoemde gegevens niet onnodig (inefficiënt, onnodig kostenverhogend en onnodig privacybeperkend) meerdere keren door meerdere partijen moeten worden opgeslagen?

14. Welke investeringen zijn noodzakelijk om relaties te kunnen leggen tussen de opgeslagen data om te kunnen voldoen aan informatieverzoeken van behoeftestellers ten aanzien van individuele communicaties of gebruikers?

15. Er wordt niet beoogd de inhoud van de communicatie vast te leggen. Is er niet altijd sprake van een overlap, d.w.z. dat verkeersgegevens, locatiegegevens en persoonsgegevens niet volledig kunnen worden gescheiden (met name door de aanwezigheid van headers)?

16. Hoe gemakkelijk is het voor gebruikers om de bewaarplicht te omzeilen? Dat wil zeggen: welke mogelijkheden zijn er om te communiceren via (internet)telefonie of e-mail zonder dat er van dat verkeer bruikbare verkeersgegevens worden bewaard, zoals geldt voor de onderstaande voorbeelden?
    - Bericht via webmail interface opstellen maar niet verzenden. Ontvanger logt in op zelfde webmail interface en leest bericht uit de folder «Te verzenden berichten»
    - Instant messaging
    - VOIP-applicaties zoals Skype, die geen openbare telecommunicatiedienst zijn en dus niet onder Tw vallen (en overigens ook instant messaging en sms diensten mogelijk maken die evenmin onder de bewaarplicht vallen)
    - Gebruik van bedrijfs e-mail en internationale webmaildiensten zoals Hotmail en GMail die volgens de minister niet onder de Tw vallen
    - IPv6 dan wel veel wisselende IP-adressen
    - Het gebruik van proxyservers

17. Hoe moeilijk is het om (al dan niet opzettelijk) te bewaren verkeersgegevens te genereren die een verkeerd beeld geven over de communicatie? Kunt u daar voorbeelden van geven?
    - Gebruiken van andermans wifi verbinden
    - Nepafzendergegevens
    - IP-spoofing
    - Een DDoS/DoS aanval die een aanbieder overspoelt met potentieel on-juiste data w.o. log-on/log-off verzoeken (RADIUS, email, etc)

18. Is juist dat SMTP servers (voor uitgaande mail) niet controleren of de afzendergegevens (naam, e-mail adres) juist zijn en dat het afzenderadres van een e-mail bericht op eenvoudige manier is te manipuleren? Maakt dit dat de identiteit van gebruikers gemakkelijk kan worden verward?

19. Hoeveel afzenders van spamberichten gebruiken naar Uw ervaring correcte afzendergegevens (naam, e-mailadres?)

20. 98% Van het e-mailverkeer is spam. Veelal wordt spam bij de toegangspoort van de ISP tegengehouden danwel weggegooid. Wat is het nut van het bewaren van alle gegevens die betrekking hebben op spam? **NB**. Het gaat niet alleen om inkomende maar ook uitgaande spam, door criminele bendes verzonden met gebruikmaking van computers van klanten die zonder het te weten geïnfecteerd zijn met kwaadaardige software (botnets, trojans, etc.).