Agendapunt 3
162

ONTWERP

Aan: de Voorzitter van de Tweede Kamer der Staten-Generaal

Betreft: Verdrag Cybercrime

Met deze nota stel ik u op de hoogte van de stand van zaken met betrekking tot het ontwerp van het Verdrag dat in de wandelgangen wordt aangeduid als 'Crime in cyberspace' of 'cybercrime'. Er is nog geen officiële naam voor. Daar het Verdrag ingrijpende gevolgen kan hebben voor de verdere ontwikkeling van het Nederlandse recht op het gebied van informatiecriminaliteit lijkt het dienstig Uw Kamer in de gelegenheid te stellen een debat te hebben over de Nederlandse inzet bij het Verdrag.

1. Voorgeschiedenis

Het internationale overleg over wat aanvankelijk computercriminaliteit heette, dateert van begin van de jaren tachtig. In eerste aanleg stelden de Verenigde Staten het onderwerp aan de orde in de Organisatie voor Economische Samenwerking en Ontwikkeling (OESO). Met het oog op de binnen de industriële landen van de wereld zich ontwikkelende informatietechnologie, leek het dienstig de daarmee parallel zich voltrekkende rechtsontwikkeling in de betrokken landen vanuit een aantal uitgangspunten te sturen. De OESO heeft in haar rapport 'Computer-related crime:, analysis of legal policy' van 1986 aanbevolen een aantal gedragingen in de betrokken landen strafbaar te stellen. De meest in het oog springende was het kraken van computers. De Raad van Europa heeft deze Aanbeveling opgenomen en nader uitgewerkt in de Aanbeveling R (89) 9 waarin meer precies op het gebied van het materiële strafrecht een aantal strafbaar te stellen gedragingen zijn omschreven. Vervolgens heeft de Raad van Europa in 1995 een tweede rapport over het formele strafrecht uitgebracht getiteld 'Problems of criminal procedural law connected with information technology' dat is gevoegd bij de Aanbeveling R (95) 13. Het rapport constateerde de dringende behoefte aan een Verdrag. Uitvoering gevend hieraan heeft het Comité van Ministers ingestemd met de instelling van een ad hoc Comité van experts dat tot opdracht heeft een Verdrag op te stellen over zowel het materiële als het formele strafrecht. De opdracht aan het Comité is als bijlage bijgevoegd. Als de aanvankelijke einddatum van de werkzaamheden was genoemd eind 1999. Deze termijn is verlengd tot eind 2000. Het Comité zal dan een ontwerp van een Verdrag aan de plenaire Stuurgroep criminele vraagstukken dienen voor te leggen.

Voor een volledig beeld lijkt het dienstig ook de nationale ontwikkelingen kort aan te duiden. Naar aanleiding van het rapport van de OESO en tegen de achtergronden van het overleg dat inmiddels in de Raad van Europa plaatsvond, heeft in 1985 de toenmalige Minister van Justitie de Commissie computercriminaliteit, onder leiding van prof mr H. Franken, ingesteld met de opdracht voorstellen te doen tot aanpassing van de Nederlandse strafwetgeving. Het rapport 'Informatietechniek en strafrecht' van april 1987 deed voorstellen tot aanpassing van het Wetboek van Strafrecht en het Wetboek van Strafvordering. Op basis daarvan is de Wet computercriminaliteit opgesteld die in 1993 (Stb. 1993, 33) in werking trad. De materieel-strafrechtelijke bepalingen sloten nauw aan bij de inmiddels internationaal gegroeide opvattingen.

De strafvordelijke bepalingen waren echter nieuw en trokken internationaal de aandacht.

Vooral de nieuwe bevoegdheid tot netwerkzoeking in artikel 125k die in samenhang met een huiszoeking kan worden uitgevoerd, riep de vraag op naar de juridische gevolgen van daarbij mogelijk in buitenlandse computers aangetroffen gegevens. Daar computernetwerken zich niet aan landsgrenzen storen, is het mogelijk dat daarbij buitenlandse computers op hun inhoud worden onderzocht. Het Nederlandse Wetboek van Strafvordering op dit punt was mede aanleiding tot de Aanbeveling R (95) 13. In het wetsvoorstel computercriminaliteit II (kamerstukken II 1998/99, 26 671) zijn reeds een aantal gedachten uit de Aanbeveling (95) 13 overgenomen.

Hangende een internationale regeling moet worden aangenomen dat de enkele mogelijkheid dat bij een netwerkzoeking gegevens worden aangetroffen die (bij nader onderzoek) uit het buitenland afkomstig blijken, onvoldoende is om af te zien van het voornemen om een louter binnenlands bedoelde netwerkzoeking uit te voeren. Wel dienen daarbij de nodige voorzorgen te worden genomen dat geen buitenlandse computers worden onderzocht. Wanneer ondanks alle voorzorgsmaatregelen toch gegevens uit het buitenland bij het onderzoek blijken te zijn vergaard, lijkt het mij in beginsel uit een oogpunt van goede internationale verhoudingen dienstig contact op te nemen met de autoriteiten van het desbetreffende land teneinde te bezien of en zo ja in hoeverre het aldus verkregen materiaal als opsporinginformatie of als bewijs in een Nederlandse strafzaak kan worden aangewend.

Een Comité van experts (PC-CY genaamd), bestaande uit vertegenwoordigers van een beperkt aantal landen bereidt het ontwerp van een Verdrag voor. Het Comité staat onder voorzitterschap van prof H.W.K. Kaspersen van het Instituut voor Informatica en Recht van de Vrije Universiteit te Amsterdam. Op grond van een contract met het Ministerie van Justitie vertegenwoordigt hij daarin Nederland. Het Comité heeft tot taak uiterlijk eind 2000 een ontwerp van een Verdrag aan de stuugroep strafrechtelijke vraagstukken van de Raad van Europa voor te leggen. Naast de grote Europese landen als Frankrijk, Duitsland en Engeland, zijn niet-leden van de Raad nauw bij de werkzaamheden betrokken, zoals de VS en Canada. Vertegenwoordigers van Japan, Zuid-Afrika, de Europese Commissie, de OESO, de UNESCO en onafhankelijke wetenschappelijke experts nemen verder aan de beraadslagingen deel. De Raad van Ministers van de EU heeft op 27 mei 1999 een gemeenschappelijk standpunt vastgesteld over een aantal in het in voorbereiding zijnde Verdrag te regelen onderwerpen (PgEG van 5 juni 1999, L 142/1). De G8 vergaderen voortdurend parallel aan de PC-CY over een aantal verwante onderwerpen. De resultaten daarvan worden ingebracht door degenen die zowel aan G8 als aan de PC-CY deelnemen.

Ik kom dan nu aan een aantal onderwerpen die naar verwachting in het verdrag zullen worden geregeld. Het ontwerp gaat tot dusver in op materieel en formeel strafrecht op nationaal en internationaal niveau, alsmede enkele rechtshulpinstrumenten in aanvulling op bestaande multilaterale en bilaterale verdragen. Het belangrijkste multilaterale verdrag is het Verdrag inzake de wederzijdse rechtshulp in strafzaken van de Raad van Europa uit 1958 (Trb. 1965, 10). Een belangrijk bilateraal verdrag is het Verdrag met de VS aangaande de wederzijdse rechtshulp in strafzaken (Trb. 1981, 188). Voor het geval in de toekomst landen partij worden bij het Verdrag cy-

bercrime met wie nog geen enkel rechtshulpverdrag bestaat, dient het verdrag te voorzien in zelfstandige rechtshulpbepalingen. Het verdrag zal, evenmin als de genoemde verdragen, geen betrekking hebben op aangelegenheden die de staatsveiligheid aangaan.

2. Het materiële strafrecht

Het materiële strafrecht omschrijft een aantal gedragingen dat de landen in hun nationale wetgeving strafbaar dienen te stellen. Enerzijds gaat het om gedragingen die zich richten tegen de vertrouwelijkheid, de integriteit en de beschikbaarheid van computersystemen en de daarin opgeslagen en overgedragen gegevens. Onder computersystemen worden mede begrepen elektronische netwerken zoals het publieke Internet, maar ook private bedrijfsnetwerken. Wat betreft gegevens gaat het om informatie of computerprogramma's die in digitale vorm in computers zijn opgeslagen of over een netwerk via telecommunicatie worden getransporteerd. Deze gedragingen worden aangeduid als CIA-delicten (afgeleid van 'confidentiality, integrity and availability). Anderzijds betreft het inhoud-gerelateerde gedragingen. Het fundamentele recht op vrijheid van meningsuiting speelt daarbij een rol.

2.1 De CIA-delicten

Wat betreft de CIA-delicten is er in de eerste plaats het kraken van een computersysteem of een deel daarvan met doorbreking van veiligheidsmaatregelen of met een oneerlijke bedoeling. Deze bepaling komt overeen met het Nederlandse computervredebreuk, omschreven in artikel 138a van het Wetboek van Strafrecht. Met een deel van een computersysteem wordt mede gedoeld op directories waartoe de gebruiker van een netwerk niet-geautoriseerd is.

Een tweede strafbaar te stellen gedraging is het afluisteren van data via telecommunicatie gestuurd naar of afkomstig van een computersysteem. Dit is in Nederland reeds strafbaar onder artikel 139c van het Wetboek van Strafrecht. Deze verdragsbepaling brengt met zich mee dat de deelnemende landen in hun wetgeving uitdrukkelijk bevoegdheden zullen moeten hebben tot het opnemen van dergelijke communicatie als strafuitsluitingsgrond op deze strafbepaling.

Een derde bepaling heeft betrekking op geautomatiseerd opgeslagen gegevens. De wijziging of vernietiging daarvan dient strafbaar te zijn. In Nederland is dit omschreven in artikel 350a van het Wetboek van Strafrecht. In het wetsvoorstel computercriminaliteit II is daarenboven opgenomen de wijziging van gegevens die gedurende telecommunicatie worden overgedragen.

Verder is voorwerp van overleg een tweetal gedragingen die stoornis veroorzaken enerzijds in het functioneren van een computersysteem, anderzijds in iemands mogelijkheden om ongestoord via de elektronische snelweg te kunnen communiceren. De eerste gedraging is verwant aan het in artikel 161sexies van het Wetboek van Strafrecht strafbaar gestelde gedrag, doch breidt deze tevens uit tot private netwerken. De tweede komt in de Nederlandse wetgeving nog niet voor. Nederland steunt de strafbaarstelling van de twee genoemde gedragingen. Tot op zekere hoogte zou met de voorgestelde strafbaarstelling het z.g. spammen worden bestreden: het op grote schaal verspreiden via e-mailboxen van berichten voor commerciële of ideolo-

gische doeleinden, namelijk in die gevallen dat die handelwijze is gericht op het veroorzaken van een dergelijke stoornis. Hieronder wordt mede begrepen de voorwaardelijke opzet: het willens en wetens nemen van het geenszins denkbeeldige risico dat deze stoornis ontstaat. Vaak is deze opzet echter niet aanwezig. Een voorstel om nog verder te gaan en ook gedragingen die onbedoeld dit gevolg hebben, daaronder te laten vallen, vond weinig steun. Er werd aangevoerd dat het een fundamenteel recht betreft om zijn mening te uiten, ook op grootscheepse schaal en ook tegenover mensen die daar niet om hebben gevraagd. Het toezenden van ongevraagde reclame via de e-mail wordt overigens buiten de sfeer van het strafrecht in verschillende (ontwerp)richtlijnen van de EU behandeld, zoals in die over (1) de elektronische handel, (2) de verkoop op afstand en (3) de bescherming van persoonsgegevens.

Een laatste gedraging is de handel in passwords en toegangscodes. In sommige landen is het een groot euvel dat op Internetsites omvangrijke lijsten van toegangscodes tot computersystemen al dan niet tegen betaling ter beschikking worden gesteld.

Tot slot is er een bepaling die verplicht tot een algemene strafbaarstelling van de volgende voorbereidingshandelingen: het vervaardigen, het beschikbaarstellen en de verspreiding van instrumenten die geschikt zijn om de eerder genoemde gedragingen te plegen. Onder instrumenten (devices) wordt zowel hardware als software begrepen. Tot zover de CIA-delicten die thans voorwerp van discussie zijn.

2.2 Inhoudgerelateerde delicten: kinderpornografie

Wat betreft de inhoud-gerelateerde delicten bestaat eigenlijk alleen overeenstemming over de strafbaarstelling van kinderpornografie. Het is duidelijk dat geen overeenstemming kan worden bereikt over het aanzetten tot rassenhaat of de verspreiding van pornografie. Waar in de traditie van veel Europese landen het aanzetten tot rassenhaat strafbaar is, stuit de codificatie daarvan in het Verdrag af op het First Amendment van de VS. De vrijheid van meningsuiting in de VS vindt pas zijn grenzen indien daadwerkelijk individuele personen worden bedreigd. Daar staat tegenover dat de VS (en andere landen) erkennen dat verschillende Europese landen van mening zijn dat er niet of nauwelijks een rol voor de overheid is weggelegd in het weren van pornografisch materiaal. Sommigen zullen deze stand van zaken teleurgesteld aanvaarden als een beperking inherent aan internationaal overleg. Anderen zullen het duiden als een behoud van culturele diversiteit op transnationale netwerken. Een samenleving waarin op dergelijke netwerken slechts de informatie beschikbaar is die de toets kan doorstaan van de gezamenlijke wetgevingen die daarop van toepassing zijn, zou volgens deze aan kleur kunnen verliezen. Wat daarvan zij, een verdergaande harmonisatie van inhoud-gerelateerde delicten lijkt niet vooralsnog niet in het verschiet te liggen. Dit laat onverlet dat in Nederland op nationaal niveau zal blijven worden opgetreden tegen personen die hier te lande meewerken aan de verspreiding van racistische informatie in de zin van artikel 137c van het Wetboek van Strafrecht, ook al is deze verspreiding legaal in het land van oorsprong, Ik verwijs naar mijn brief aan de Voorzitter van de Tweede Kamer van 7 september j.l over de aansprakelijkheid van tussenpersonen.

Onder kinderpornografie wordt gedacht de realistische uitbeelding van een kind dat deelneemt aan seksueel gedrag ongeacht of bij de vervaardiging daarvan daadwerkelijk kinderen zijn betrokken. Ook gevallen waarin volwassen acteurs een kind uit-

beelden en kinderpornografie vervaardigd via computeranimatie, vallen hieronder. Tekenfilmpjes waarbij duidelijk het niet-realistische karakter blijkt, vallen hier niet onder. Ieder land kan zelf de leeftijdsgrens vaststellen. De verdragsrechtelijke ondergrens is voorlopig gelegd op veertien jaar. Bij ons is die grens blijkens artikel 240b van het Wetboek van Strafrecht zestien jaar. De voorgestelde bepaling zou voor Nederland tot op zekere hoogte een verschuiving impliceren in het object van strafrechtelijke bescherming. Vindt de Nederlandse bepaling zijn oorsprong in de gedachte dat een kind moet worden beschermd tegen medewerking aan de vervaardiging van dergelijk materiaal, de voorgestelde bepaling beschermt veeleer het kind meer in het algemeen tegen iedere uitbeelding als seksueel begerenswaardig subject. Daarbij is de betrokkenheid van kinderen bij de vervaardiging van dergelijk materiaal niet meer relevant. Gelet op de breed gedragen internationale consensus hierover, komt mij voor dat Nederland zich hierbij kan aansluiten.

3. Het formele strafrecht

Wat betreft het formele strafrecht lijkt tot dusver vergaande overeenstemming te bestaan over een aantal zaken.

3.1 E-mail

In het voetspoor van de Aanbeveling R (95) 13 wordt vastgehouden aan de juridische relevantie van het moment waarop een strafvorderlijke bevoegdheid wordt gebruikt in verband met de vergaring van gegevens. Gaat het bijvoorbeeld om gegevens die op dat moment reeds zijn opgeslagen dan wordt aansluiting gezocht bij het regime voor de uitlevering van voorwerpen of huiszoeking. Gaat het daarentegen om gegevens die na dat moment zullen ontstaan dan is er meer verwantschap met het aftappen van telecommunicatie. Bij de uitlevering en huiszoeking gaat het in beginsel om een kortdurende actie waarbij selectief de gegevens worden vergaard die nodig worden geacht voor de waarheidsvinding. Er is een plicht van in beginsel iedere burger tot wie het desbetreffende bevel wordt gericht, om mee te werken. Deze plicht beperkt zich echter tot het verstrekken van de gevraagde gegevens of het dulden van de huiszoeking. De plicht kan echter niet zover gaan dat de burger wordt opgedragen zelf bestanden volgens bepaalde criteria te doorzoeken of anderszins als onbezoldigd opsporingsambtenaar op te treden. Na afloop van de vergaring van de gegevens is er ook in beginsel geen geheimhoudingsplicht van de persoon tot wie het bevel is gericht. Wel zullen de opsporingsinstanties onder omstandigheden vragen vertrouwelijkheid te bewaren wanneer dat nodig is om het onderzoek niet te schaden. Deze bevoegdheid kan worden gecontrasteerd met die inzake toekomstige gegevens: daarbij worden ongericht gedurende een bepaalde tijd in de orde van grootte van weken gegevens vergaard. Het bevel richt zich tot private personen die bepaalde werkzaamheden verrichten, tot dusver slechts aanbieders van telecommunicatiediensten. Deze dienen daartoe ook bepaalde voorzieningen te onderhouden. Zij zijn gehouden gedurende de uitvoering van gegevensvergaring daarover geheimhouding te betrachten, daar bekendheid bij de personen die voorwerp zijn van onderzoek, een negatieve invloed zal hebben op de gegevens die ter beschikking komen. Dat betekent dat het bij het vergaren van toekomstige gegevens gaat om de uitoefening van een geheime opsporingsbevoegdheid, althans gedurende enige tijd geheim op het moment van de uitvoering van die bevoegdheid tegenover degene die voorwerp is van onderzoek. Voor de introductie in 1971 van de bevoegdheid telefoongesprek-

ken af te luisteren in het Wetboek van Strafvordering, bestonden dergelijke bevoegdheden niet. Gelet op het systeem van dit wetboek en op de uitgangspunten van de wet bijzondere opsporingbevoegdheden, ga ik ervan uit dat met de uitbreiding van geheime opsporingsmethoden terughoudendheid moet worden betracht.

Deze benadering kan vragen oproepen over de behandeling van elektronische post (e-mail). De technische ontwikkelingen leiden ertoe dat feitelijk steeds moeilijker valt vast te stellen of er sprake is van opslag of aftappen. Een e-mailbericht via Internet wordt tijdens het transport soms gedurende langere tijd opgeslagen op één van de aan het netwerk deelnemende computers wegens verstopping van het netwerk, dan dat het op de computer van een Internet Service Provider ter beschikking staat van de geadresseerde abonnee om te worden opgehaald. De technische feitelijkheid is dan echter minder relevant dan de maatschappelijke functionaliteit. De gegevens die wachten op (verder) transport zijn afhankelijk van techniek, het bericht in de e-mailbox is afhankelijk van menselijk ingrijpen. Dat lijkt mij bepalend voor de vraag of er sprake is van transport of van opslag. Bij transport is het nodig dat wordt afgetapt, bij opslag is nodig een bevel uitlevering gegevens of huiszoeking. De juridische zuiverheid lijkt mij zwaarder te moeten wegen dan het bezwaar dat voor e-mailberichten aldus een gedifferentieerd regime geldt, afhankelijk van het stadium waarin het bericht zich bevindt op de weg van de afzender naar de geadresseerde. Daarvan is ook uitgegaan in het wetsvoorstel computercriminaliteit II (kamerstukken II 1998/99, 26 671). Voor deze benadering lijkt in ieder geval een meerderheid te bestaan. Het staat nog niet vast of dit haalbaar zal blijken te zijn.

3.2 Grensoverschrijdende effecten van de uitoefening van strafvorderlijke bevoegdheden

Bij de vergaring van gegevens die langs elektronische netwerken beschikbaar zijn dan wel hun weg over de wereld zoeken, doemt onvermijdelijk, indien daarbij gebruik wordt gemaakt van strafvorderlijke bevoegdheden, de vraag op naar het verband met de traditioneel in hoofdzaak territoriaal afgegrensde rechtsmacht van staten. Er lijkt zich zich overeenstemming af te tekenen dat in beginsel dergelijke strafvorderlijke bevoegdheden niet grensoverschrijdend zouden moeten worden gebruikt. De landen blijven aangewezen op de traditionele instrumenten van rechtshulp: een rogatoire commissie waarbij het verzoekende land aan het aangezochte land vraagt om bepaalde bevoegdheden aan te wenden ten behoeve van de strafvordering in het verzoekende land. Daar in geval van cybercrime soms met grote spoed rechtshulp is vereist, wordt voorzien in nationale contactpunten die vierentwintig uur per dag zeven dagen per week met deskundig personeel zijn bemand. Veel landen, waaronder Nederland, zoeken daarbij aansluiting bij hun contactpunt voor Interpol. In Nederland is dat de CRI. Deze contactpunten moeten in staat zijn snel de justitiële autoriteiten te bereiken die moeten worden ingeschakeld voor de gevraagde uitoefening van bevoegdheden. Wanneer strafvorderlijke bevoegdheden in een ander land moeten worden uitgeoefend is dit dus in beginsel de weg.

Er is een scala van mogelijkheden om gegevens in een ander land te bereiken. Er zijn gegevens die op een website op Internet publiek toegankelijk zijn. Zoals iedere wereldburger, kan ook de politie, deze gegevens raadplegen. Bijzondere bevoegdheden zijn hiervoor niet nodig. Daarnaast zijn personen geautoriseerd om toegang te hebben tot gegevens die zijn opgeslagen op een centrale computer in een ander

land. Zo kan een bank in één van onze buurlanden een dépendance in ons land hebben en personeel op die dépendance autoriseren om toegang te hebben tot het centrale computersysteem en de daar opgeslagen gegevens in het land van het hoofdkantoor. Wanneer in ons land dergelijk geautoriseerd personeel vrijwillig de politie gegevens verstrekt uit het andere land of vrijwillig de politie toegang verleent tot de onderdelen van het computersysteem waartoe het in Nederland zich bevindende personeel bevoegd is, wordt er tot dusver evenzeer vanuit gegaan dat er geen sprake is van enige grensoverschrijdende bevoegdheidsuitoefening.

De eerste vragen beginnen wanneer personen die zich op Nederlands territoir bevinden via strafvorderlijke bevoegdheden, bijvoorbeeld tot uitlevering van gegevens, zouden worden gedwongen gebruik te maken van hun autorisaties om toegang te nemen tot in het buitenland opgeslagen gegevens. Sommige landen beschouwen dit als een grensoverschrijdende bevoegdheidsuitoefening die niet zonder hun instemming kan plaatsvinden. Andere landen menen dat een dergelijke autorisatie van de in het voorbeeld private rechtspersoon aan personen in dépendances in een ander land, met zich meebrengt dat daarmee ook de gegevens die overeenkomstig de autorisatie in dat andere land toegankelijk zijn, voorwerp kunnen zijn van de toepassing van strafvorderlijke bevoegdheden ingevolge het publieke recht in dat andere land. Ik neig tot deze laatste opvatting. Dat zou betekenen dat Nederland bereid is mee te gaan, wanneer zou blijken dat de algemene opvatting die kant opgaat, met een verdrag waarbij de politiële en justitiële autoriteiten van andere Partijen bij dat verdrag gerechtigd zijn overeenkomstig hun eigen recht, zonder medeweten van de Nederlandse autoriteiten, kennis te nemen van gegevens die zijn opgeslagen in computers op Nederlands territoir voor zover de rechthebbende op die gegevens in Nederland personen in het buitenland heeft geautoriseerd gebruik te maken van die gegevens.

Minder twijfels zijn er over meer ingrijpende vormen van bevoegdheidsuitoefening waarbij toegang wordt verkregen op in het in buitenland opgeslagen gegevens zonder dat in dat andere land ooit autorisatie of toestemming is gegeven van die gegevens kennis te nemen. Het ziet ernaar uit dat het Verdrag impliciet of expliciet dit zal verbieden. De autoriteiten in het ene land zullen dus voor de opsporing van strafbare feiten niet in computers op het territoir van een andere Verdragspartij kunnen zoeken zonder toestemming. Dit lost echter niet het probleem op dat bij de uitoefening op nationaal niveau van enige bevoegdheid in verband met grensoverschrijdende netwerken, waarbij ook alle redelijke maatregelen zijn genomen om grensoverschrijdend onderzoek uit te sluiten, toch gegevens uit het buitenland worden meegenomen. Dit kan blijken op het moment zelf van de uitoefening van de bevoegdheid of later bij het onderzoek van de daarbij verkregen gegevens. Wel is duidelijk dat het Staten niet kan worden verboden nationale bevoegdheden uit te oefenen uitsluitend omdat nimmer de mogelijkheid kan worden uitgesloten dat daarbij gegevens uit het buitenland worden verkregen. Sommige staten menen evenwel dat gegevens die overeenkomstig eigen strafvorderlijke bevoegdheden zonder medewerking van de autoriteiten van andere landen kunnen worden verkregen, zonder meer voor opsporing of als bewijs in een strafzaak in het eigen land kunnen worden gebruikt. Andere landen claimen een vetorecht op een dergelijke gebruik van zulke gegevens. Een intermediaire positie nemen die landen in die wel claimen dat in dergelijke gevallen mededeling wordt gedaan, doch dat de vraag naar het verdere gebruik van die gegevens in een strafzaak afhankelijk is van ad hoc overleg tussen de betrokken Partijen. Ik meen dat Nederland in beginsel voorstander zou dienen te zijn van een vetorecht op aldus

verkregen gegevens. Wanneer dat nodig is om consensus te bereiken zou evenwel kunnen worden ingestemd met een consultatieprocedure. Het komt mij voor dat zonder nader overleg met het parlement Nederland niet dient in te stemmen met een verdragstekst die gebruik van dergelijke gegevens voor opsporing en vervolging toelaat zonder dat het land waarvan de gegevens afkomstig zijn, daarover ten minste wordt geïnformeerd.

3.3 Het vastleggingsbevel

Een geheel nieuwe bevoegdheid die in de nationale wetten zou moeten worden opgenomen is het vastleggingsbevel (dit is een voorlopige vertaling van 'preservation order'). Het bevel houdt in dat een beheerder van een privaat netwerk of van een netwerk dat telecommunicatiediensten aan het publiek aanbiedt, voor een in het bevel gespecificeerd aansluitpunt de verkeersgegevens vastlegt die anders wellicht terstond of na korte tijd zouden worden vernietigd. Onder verkeersgegevens worden de gegevens verstaan die informatie geven vanaf welk aansluitpunt met wie, wanneer en hoelang is gecommuniceerd. Aanbieders van klassieke telefoondiensten plegen deze gegevens vast te houden teneinde op basis daarvan hun abonnees een rekening te kunnen sturen. Soms worden na betaling van de rekening de gegevens nog vastgehouden om mogelijke fraude te constateren. Het privacyrecht van de EU vereist dat de gegevens worden vernietigd zodra deze niet meer noodzakelijk zijn voor de bedrijfsvoering. Zie hiervoor artikel 6, eerste lid, van de richtlijn 97/66/EG van 15 december 1997, PbEG van 30 januari 1998, L 24/1. Deze bepaling is omgezet in het Nederlands recht in artikel 11.5 van de Telecommunicatiewet. Op deze regel kan een uitzondering worden gemaakt indien dat noodzakelijk is voor onder meer de opsporing van strafbare feiten en daarin is voorzien bij wet. Dit is gebeurd in artikel 13.4, tweede lid, van de Telecommunicatiewet dat bepaalt dat telecom dienstaanbieders bepaalde bij algemene maatregel van bestuur aan te wijzen verkeersgegevens gedurende drie maanden moeten bewaren, ook los van een concrete verdenking. Een bepaling als thans wordt overwogen in de Verdrag cybercrime zou met zich brengen dat het Wetboek van Strafvordering wordt aangevuld met een bepaling die de Justitie de bevoegdheid geeft in het concrete geval van een verdenking een netwerkbeheerder te gelasten daarmee verband houdende verkeersgegevens langer te bewaren dan nodig is voor de interne bedrijfsvoering. De bevoegdheid zou moeten gelden ongeacht de vraag of het gaat om een netwerkbeheerder die valt onder het regime van de Telecommunicatiewet dan wel een beheerder van een privaat netwerk, bijvoorbeeld van een concern of een hotelketen. Een dergelijke last heeft het karakter van een voorlopige maatregel om zeker te stellen dat de gegevens beschikbaar zijn wanneer daarom wordt gevraagd bij een bevel tot overdracht van gegevens ingevolge artikel 125i van het Wetboek van Strafvordering. Een dergelijke last brengt dus op zichzelf nog niet mee dat de Justitie ook al de beschikking krijgt over de vastgelegde gegevens.

Deze nationale bevoegdheid is echter incompleet zonder een internationaal complement. Zoals gebruikelijk kan een dergelijke nationale bevoegdheid ook altijd worden aangewend indien buitenlandse autoriteiten daarom ten behoeve van een eigen strafrechtelijk onderzoek vragen in het kader van een verzoek om rechtshulp. De ervaring leert echter dat dit waarschijnlijk niet snel genoeg zal gaan om de vereiste gegevens veilig te stellen. Daarom ligt het voorstel ter tafel dat voor beheerders van dergelijke netwerken, wanneer zij elkaar vrijwillig informeren over de grenzen van de

bij het Verdrag aangesloten staten heen, ook de verplichting wordt opgeheven om verkeersgegevens te vernietigen die niet meer voor de eigen bedrijfsvoering zijn vereist. Tevens zou de civielrechtelijke aansprakelijkheid moeten worden uitgesloten voor mogelijke schade die voortvloeit uit een aldus langer bewaren van verkeersgegevens. Op zichzelf is het een novum in het internationale recht dat het verzoek van de autoriteiten van het ene land rechtsgevolgen kunnen bewerkstelligen in een ander land zonder tussenkomst van de autoriteiten in dat andere land. Voor zover het zou gaan om het rechtsgevolg van een verplichting, wordt door een aantal landen een dergelijk grensoverschrijdend effect afgewezen. Het valt niet uit te sluiten dat het compromis kan worden bereikt in die zin dat het grensoverschrijdend rechtsgevolg weliswaar geen verplichting tot gevolg kan hebben om verkeersgegevens op te slaan, doch wel een bevoegdheid. Dit zou betekenen de ontheffing van een verplichting verkeersgegevens te vernietigen die bewijs kunnen bevatten, alsmede van de daaruit voortvloeiende ontheffing van civielrechtelijke aansprakelijkheid wegens het niet-nakomen van de vernietigingsplicht. Ik meen dat Nederland een dergelijk compromis zou kunnen ondersteunen. Zijn de gegevens vrijwillig overeenkomstig een dergelijk vastleggingsbevel vanuit het buitenland opgeslagen, dan vindt uiteraard de daadwerkelijke terbeschikkingstelling aan de buitenlandse autoriteiten weer plaats langs de klassieke weg van de wederzijdse rechtshulp met alle mogelijke uitzonderingen daarop die de bestaande rechtshulpverdragen kennen.

De vraag kan rijzen of netwerkbeheerders ook verplicht dienen te worden om voorzieningen te treffen om verkeersgegevens vast te leggen teneinde uitvoering te kunnen geven aan een dergelijk vastleggingsbevel, c.q. in staat moeten zijn op vrijwillige basis daaraan te voldoen wanneer zij daarvan kennis nemen via een andere operator in de communicatieketen. Een dergelijke verplichting lijkt mij niet in de rede te liggen. In de meeste gevallen zullen dergelijke technische voorzieningen wel aanwezig zijn. Het is niet nodig dit feit te juridiseren.

3.4 Het aftappen van private netwerken

Het Verdrag zal waarschijnlijk ook voorzien in een verplichting van de Partijen bij het Verdrag om in hun wetgeving te voorzien in het aftappen van telecommunicatie. In Nederland bestaat al een dergelijke wettelijke voorziening in artikel 13.2 van de Telecommunicatiewet in verband met artikel 125g het Wetboek van Strafvordering (na inwerkingtreding van de Wet bijzondere opsporingsbevoegdheden op 1 februari 2000 zal dit zijn artikel 125m). Veel landen bepleiten deze bevoegdheid niet te beperken tot netwerken waarover telecommunicatiediensten aan het publiek worden aangeboden, doch ook uit te strekken tot private netwerken. Voor Nederland lijkt dit op het eerste gezicht iets nieuws te zijn. In ieder geval is er voor private netwerken geen algemene aftapbaarheidsplicht zoals die geldt voor de publieke netwerken ingevolge de Telecommunicatiewet. In Nederland zal de mogelijkheid van het aftappen van private netwerken besloten liggen in artikel 126l van het Wetboek van Strafvordering zoals dat luidt in de wet bijzondere opsporingsbevoegdheden: het opnemen van vertrouwelijke communicatie. Deze bepaling specificeert niet of het gaat om vertrouwelijke communicatie van mensen die in een zelfde vertrek met elkaar spreken zonder technisch hulpmiddel dan wel om personen die met elkaar communiceren via een privaat netwerk, dat zelfs een WAN (wide area network) kan zijn. Evenmin specificeert deze bepaling of het afluisteren met medewerking van de systeembeheerder dient te geschieden dan wel zonder zijn instemming en medeweten kan plaatsvin-

den. Al deze mogelijkheden staan open. De medewerking van een beheerder van een privaat netwerk kan niet worden afgedwongen. Zelfs een woning kan onder omstandigheden zonder medeweten van de rechthebbende worden betreden om een tap te plaatsen op een privaat netwerk.

Gelet op deze bepaling komt het mij voor dat Nederland zich in Straatsburg niet behoeft te verzetten tegen een verdragsrechtelijke verplichting ook telecommunicatie die wordt afgewikkeld via private netwerken te kunnen aftappen. Denkbaar is dat dit het gevolg heeft dat de desbetreffende netwerkbeheerders een medewerkingsverplichting in het Wetboek van Strafvordering zal worden opgelegd. Dit lijkt mij aanvaardbaar. Eventuele ad-hockosten komen dan voor rekening van Justitie. Een algemene aftapbaarheidseis van private netwerken lijkt mij echter vooralsnog niet wenselijk. In dit opzicht zou er dan een principieel verschil blijven met netwerken die telecommunicatie aanbieden aan het publiek.

Bestaat er eenmaal een dergelijke bevoegdheid op nationaal niveau, dan vloeit uit de bestaande rechtshulpverdragen voort dat een dergelijke bevoegdheid ook op verzoek van buitenlandse autoriteiten ten behoeve van hun strafrechtelijke onderzoeken kan worden aangewend.

4. Slot

Ik hoop met het bovenstaande enig inzicht te hebben verschaft in de positie van de Nederlandse regering en de Nederlandse inbreng. Gaarne zal ik desgewenst met de Tweede Kamer overleggen over aspecten hiervan.

De Minister van Justitie,