Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2004–2005

26 671 Wijziging van het Wetboek van Strafrecht, het Wetboek van Strafvordering en enige andere wetten in verband met nieuwe ontwikkelingen in de informatietechnologie (computercriminaliteit II)

Nr. 10

NOTA NAAR AANLEIDING VAN HET VERSLAG

Vastgesteld 2 mei 2005

Onlangs heb ik aan de Tweede Kamer de tweede nota van wijziging bij het onderhavige wetsvoorstel aangeboden (Kamerstukken II 2004/05, 26 671, nr. 7), die strekt tot implementatie van het op 23 november 2001 te Boedapest tot stand gekomen Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken (Trb. 2002, nr. 18, en Trb. 2004, nr. 290), hierna aan te duiden als het Cybercrime Verdrag. In de toelichting bij die nota van wijziging heb ik onder meer aangegeven om welke reden de voortgang van de schriftelijke behandeling van het wetsvoorstel geruime tijd had stilgelegen en ben ik uitgebreid ingegaan op het verband met het Cybercrime Verdrag. Het voorstel van rijkswet houdende goedkeuring van dat verdrag is inmiddels ook bij de Tweede Kamer ingediend (Kamerstukken II 2004/2005, 30 036, nr. 1). Zoals toegezegd doe ik hierbij de beantwoording toekomen van de vragen van de vaste commissie voor Justitie, gesteld in het verslag bij het onderhavige wetsvoorstel.

In deze nota is voor de overzichtelijkheid zoveel mogelijk de volgorde aangehouden van het verslag, zij het dat voor specifieke kwesties soms wordt verwezen naar een andere paragraaf dan waarin de vraag was gesteld.
Sinds het verslag werd vastgesteld zijn er ruim vier jaren verstreken, waarin zich vele gebeurtenissen hebben voorgedaan die ook van belang zijn voor het onderwerp van dit wetsvoorstel. Daarnaast is ook de wetgeving op een aantal punten ingrijpend gewijzigd. Zo zijn in het Wetboek van Strafvordering bevoegdheden geïntroduceerd terzake van onderzoek van telecommunicatiegegevens (Stb. 2004, 105) en onderzoek van gegevens bij financiële dienstverleners (Stb. 2004, 109). Bij de Eerste Kamer is inmiddels in behandeling het voorstel tot wijziging van het Wetboek van Strafvordering en enkele andere wetten in verband met de regeling van bevoegdheden tot het vorderen van gegevens (bevoegheden vorderen gegevens) (Kamerstukken I 2004–05, 29 441, A). Ook is nieuwe wetgeving in werking getreden terzake van de aansprakelijkheid van tussenpersonen, waardoor de destijds over dat onderwerp gestelde vragen aan belang hebben ingeboet. Aan de andere kant zijn er vragen gesteld die door de geschetste ontwikkelingen juist aan relevantie hebben gewonnen, zoals de vragen over de bij politie en justitie aanwezige expertise op het terrein van computercriminaliteit. Bij de onderstaande beantwoording van de

KST86350
0405tkkst26671-10
ISSN 0921 - 7371
Sdu Uitgevers
's-Gravenhage 2005

vragen heb ik getracht zoveel mogelijk recht te doen aan deze omstandigheden. En tenslotte zijn er veel vragen gesteld die beantwoord kunnen worden met een verwijzing naar de tweede nota van wijziging respectievelijk met een verwijzing naar (de memorie van toelichting bij) het hiervoor bedoelde voorstel voor de Goedkeuringswet inzake het Cybercrime Verdrag.

1. Algemeen

Tot mijn genoegen constateer ik dat de leden van de aan het woord zijnde fracties op hoofdlijnen konden instemmen met de in het wetsvoorstel gedane voorstellen.
Het belangrijkste punt van zorg bij de meeste fracties betrof het feit dat, op het moment waarop het verslag tot stand kwam, de regeling van de strafrechtelijke aansprakelijkheid van tussenpersonen uit het wetsvoorstel was geschrapt terwijl er nog geen zicht bestond op een nieuwe regeling. Zoals bekend, is deze materie inmiddels geregeld in het kader van de Aanpassingswet richtlijn elektronische handel (Stb. 2004, 210), waarmee de lacune die inderdaad in het wetsvoorstel Computercriminaliteit-II was ontstaan, werd opgevuld. In paragraaf 2 ga ik nader in op het onderwerp aansprakelijkheid.

De leden van de PvdA-fractie vroegen aandacht voor de reikwijdte van de Nederlandse rechtsmacht in relatie tot de internationale context van computercriminaliteit. Juist op dit punt is de totstandkoming van het Cybercrime Verdrag van groot belang. De bij het Verdrag aangesloten landen dienen de daarin aangeduide feiten in hun wetgeving strafbaar te stellen en de noodzakelijke bevoegdheden in hun wetgeving te introduceren; daarnaast voorziet het Verdrag zelf in de nodige aanvullende bepalingen inzake internationale rechtshulp. De door deze leden bedoelde belemmeringen vallen hiermee voor een belangrijk deel weg.

De leden van de PvdA-fractie vroegen in dat verband ook, hoe de regering het gegeven beziet dat internet service providers steeds grootschaliger en dus internationaler zijn gaan opereren. Zij vroegen welke gevolgen deze ontwikkelingen hebben voor de nationale opsporingspraktijk.
Bij de opsporing van strafbare feiten richten de opsporingsinstanties zich op activiteiten (bijvoorbeeld op websites) die gericht zijn op de Nederlandse markt, ook al staat de informatie op buitenlandse servers. Als gericht op Nederland kunnen bijvoorbeeld worden aangemerkt de sites waarop de Nederlandse taal gekozen kan worden (hoewel ook de Engelse taal algemeen wordt aanvaard als de algemeen erkende en gebruikelijke computertaal), sites waarop een Nederlands contact wordt opgegeven, sites die in Nederland zijn te bezoeken zodat de daarop aangeboden goederen in Nederland te koop worden aangeboden en dergelijke. Daarnaast is van belang dat service providers die kunnen worden aangemerkt als openbare telecommunicatiedienst in de zin van de Telecommunicatiewet, moeten voldoen aan de bepalingen van hoofdstuk 13 van de Telecommunicatiewet betreffende het aftappen van telecommunicatie en het verstrekken van informatie. In die zin heeft het internationale karakter van internet service providers voor de opsporing geen gevolgen. Internet service providers kunnen evenwel eenvoudig vanuit het buitenland diensten aanbieden in Nederland. Dat leidt ertoe dat in het kader van de opsporing van strafbare feiten, indien niet kan worden volstaan met het raadplegen van open bronnen, veelal een beroep gedaan moet worden op de medewerking van buitenlandse justitiële autoriteiten of opsporingsinstanties. Verschillen tussen de landen in strafvorderlijke bevoegdheden of strafbaarstellingen kunnen daarbij belemmerend werken. Maar juist het Cybercrime Verdrag draagt bij aan het wegnemen van dergelijke belemmeringen, doordat bevoegdheden en strafbaarstellingen worden gehar-

moniseerd en doordat samenwerking bij de opsporing en wederzijdse rechtshulp worden vergemakkelijkt. In dat verband noem ik ook in EU-verband het Kaderbesluit 2005/222/JBZ van de Raad van 24 februari 2005 over aanvallen op informatiesystemen (PbEG L 69 van 16/03/2005, blz. 67–71).
Door de implementatie van het Cybercrime Verdrag wordt ervoor gezorgd dat adequate strafvorderlijke bevoegdheden ter beschikking komen; ik verwijs naar hetgeen daarover wordt opgemerkt in de toelichting bij de tweede nota van wijziging bij het onderhavige wetsvoorstel. Een belangrijk aspect is, dat aanvullende bevoegdheden worden opgenomen voor die activiteiten die als communicatie voor de opsporing relevant zijn, maar die niet vallen onder het begrip «openbare telecommunicatiedienst» uit de Telecommunicatiewet.

De leden van de PvdA-fractie stelden een vraag over de harmonisatie van wetgeving in de Europese Unie. Inmiddels is tot stand gekomen het hiervoor genoemde Kaderbesluit van de Raad over aanvallen op informatiesystemen. Dit Kaderbesluit betreft een minder omvangrijk aantal onderwerpen dan het Cybercrime Verdrag, maar het stelt op een enkel punt een strakkere eis. Ik moge verwijzen naar hetgeen daarover specifiek is opgemerkt in de toelichting bij de tweede nota van wijziging (nr. 7, blz. 31–32).

Wat betreft het Cybercrime Verdrag verwijs ik naar het voorstel voor een goedkeuringswet terzake. De Nederlandse regering kon en kan zich geheel vinden in de in dat Verdrag gehanteerde uitgangspunten. Waar nodig wordt de Nederlandse wetgeving aan de eisen van het Verdrag aangepast. Ik verwijs naar de tweede nota van wijziging bij het onderhavige wetsvoorstel (nr. 7, blz. 22–26).

De vragen van de leden van de PvdA-fractie over de toerusting van opsporingsambtenaren op het gebied van «cybercrime» en over het functioneren van de bureaus digitale expertise behandel ik graag in het bredere verband van de handhaving. Daarom zal ik op deze vragen uitvoerig ingaan in paragraaf 9, die specifiek aan handhaving is gewijd.
Deze leden vroegen ook aandacht voor wat zij noemden de onwil bij het bedrijfsleven om computercriminaliteit bij bevoegde instanties te melden. In antwoorden op vragen van het lid Gerkens van 2 november 2004 (Aanhangsel Handelingen II 2004/05, nr. 645; zie ook de antwoorden op andere kamervragen terzake onder de nrs. 383, 553, 554 en 1332) heb ik aangegeven dat de aangiftebereidheid van computercriminaliteit onder bedrijven inderdaad relatief laag is. Eén van de redenen voor deze lage aangiftebereidheid is de vrees van bedrijven voor imagoschade. Zoals ik in de bedoelde antwoorden aangaf, is door het Nationaal Platform Criminaliteitsbeheersing inmiddels een project Aanpak Cybercrime gestart dat onder andere tot doel heeft het een betere vertrouwensrelatie tussen opsporingsinstanties en bedrijfsleven te bewerkstelligen ter verbetering van de onderlinge samenwerking. Ik ga ervan uit dat daardoor bij het bedrijfsleven de bereidheid zal toenemen om aangifte te doen.
De leden van de PvdA-fractie constateerden terecht, dat het geringe aantal aangiften ertoe leidt dat een zeker leereffect verloren gaat. Om in dat tekort te voorzien is inmiddels onder andere het project National High Tech Crime Centre (NHTCC) gestart. Het is de taak van dit NHTCC (zie ook de antwoorden op de hiervoor vermelde kamervragen) om in samenspraak met het bedrijfsleven te komen tot een adequaat kennisniveau inzake ICT en om advies te geven over de wijze waarop specifieke vormen van High Tech Crime dienen te worden aangepakt.

De leden van de PvdA-fractie stelden vragen over cyberterrorisme; de leden van de D66-fractie memoreerden dat tijdens een hoorzitting in 1999 in de Tweede Kamer door enkele sprekers naar voren was gebracht dat

het wetsvoorstel onvoldoende houvast bood om «cyberterreur» en sabotage via internet aan te pakken.
Ook op dit punt is van belang dat inmiddels het Cybercrime Verdrag tot stand is gekomen en dat met het oog op de implementatie daarvan het wetsvoorstel Computercriminaliteit-II wordt gewijzigd door middel van de tweede nota van wijziging. Het Verdrag voorziet in specifieke, snelle vormen van rechtshulp die kunnen worden ingezet ter bestrijding van computercriminaliteit. Wat de vragenstellers aanduiden als «cyberterreur», zal doorgaans de gedaante aannemen van strafbare feiten waarbij gebruik wordt gemaakt van telecommunicatie- of computernetwerken. Op dergelijke strafbare feiten is het Verdrag van toepassing. Indien het vermoeden van een zodanig strafbaar feit bestaat, kunnen de daarop toegesneden bevoegdheden van het Wetboek van Strafvordering worden ingezet. In dit verband verdient voorts aandacht dat sinds de aanslagen van 11 september 2001, mede ter implementatie van diverse internationale instrumenten, de nodige wetswijzigingen met het oog op een adequate bestrijding van terrorisme tot stand zijn gekomen. Te wijzen valt onder meer op de goedkeurings- en uitvoeringswetgeving betreffende het Protocol bij de EU-Overeenkomst inzake rechtshulp in strafzaken (Stb. 2004, 108), de goedkeurings- en uitvoeringswetgeving inzake het VN-verdrag ter bestrijding van de financiering van terrorisme (Stb. 2001, 675), de Overleveringswet (Stb. 2004, 195) en de Wet terroristische misdrijven (Stb. 2004, 290). Binnen het bestek van deze nota is van belang te vermelden dat deze wetswijzigingen de strafrechtelijke aansprakelijkheid voor diverse terroristische gedragingen hebben verruimd en tevens voorzien in nieuwe opsporingsbevoegdheden. Het Kabinet heeft bovendien in zijn brief van 10 september 2004 aan de Tweede Kamer inzake terrorismebestrijding aangekondigd dat verdere voorstellen worden voorbereid tot verruiming van bevoegdheden in verband met het voorkomen van terrorisme (Kamerstukken II 2003/04, 29 754, nr.1). In het naar aanleiding daarvan opgestelde wetsvoorstel tot wijziging van het Wetboek van Strafvordering, het Wetboek van Strafrecht en enige andere wetten ter verruiming van de mogelijkheden tot opsporing en vervolging van terroristische misdrijven – dat thans aanhangig is bij de Raad van State – is mede aansluiting gezocht bij het Cybercrime Verdrag en de ter implementatie daarvan voorgestelde wetswijzigingen. De wetgeving biedt daarmee voldoende grondslag voor een adequate bestrijding van terrorisme.

De leden van de PvdA-fractie hebben vragen gesteld over de verhouding tussen het wetsvoorstel Computercriminaliteit-II en de – destijds – voorziene grondwetswijziging. Voor de beantwoording verwijs ik naar paragraaf 6 hierna, dat geheel aan e-mail is gewijd.

De leden van de CDA-fractie vroegen, welke onderwerpen in de naaste toekomst regeling zouden behoeven op grond van ontwikkelingen die – destijds – nog niet uitgekristalliseerd waren. Het betreft in feite de onderwerpen die inmiddels hun neerslag hebben gevonden in het Cybercrime Verdrag en ten aanzien waarvan wordt voorgesteld deze te implementeren in het Wetboek van Strafvordering en het Wetboek van Strafrecht. Verwezen wordt naar de daarop betrekking hebbende stukken.

Voor de beantwoording van de vraag van de leden van de CDA-fractie over het Cybercrime Verdrag verwijs ik naar de toelichting op de tweede nota van wijziging (nr. 7) en naar de memorie van toelichting bij de goedkeuringswet terzake van het Cybercrime Verdrag.

De leden van de CDA-fractie hebben aandacht gevraagd voor de snelle convergentie tussen telecommunicatiediensten en informatiediensten op bijvoorbeeld het internet. In antwoord op de in dat verband gestelde vragen merk ik op dat de Telecommunicatiewet beperkt is tot die instel-

lingen en diensten die voldoen aan de in dát kader relevante omschrijvingen en definities. Het betreft de openbare telecommunicatienetwerken en -diensten. Voor de bevoegdheden die nodig zijn voor het onderzoek naar strafbare feiten wordt thans in enkele bepalingen van het Wetboek van Strafvordering nog aangesloten bij het begrippenkader van de Telecommunicatiewet. Dit acht ik echter niet meer toereikend, mede in het licht van het Cybercrime Verdrag dat de aangesloten lidstaten noopt tot het introduceren van bevoegdheden ten opzichte van instellingen die heel in het algemeen de mogelijkheid bieden om te communiceren met behulp van computers c.q. computersystemen. Daarom wordt in dat verband ook wijziging aangebracht in de betrokken bepalingen van het Wetboek van Strafvordering. Ik moge verwijzen naar de tweede nota van wijziging, waarin de zevende afdeling van titel IVa van Boek I qua reikwijdte aanmerkelijk wordt uitgebreid.

De leden van de CDA-fractie vroegen waarom in het wetsvoorstel het inbreken in computernetwerken – *hacken* – niet strafbaar wordt gesteld. De achtergrond daarvan is eenvoudig, namelijk dat dergelijk handelen in de huidige wetgeving al strafbaar *is* gesteld. In artikel 138a van het Wetboek van Strafrecht wordt strafbaar gesteld het wederrechtelijk binnendringen in een geautomatiseerd werk voor de opslag of verwerking van gegevens. Overeenkomstig artikel 80sexies van het Wetboek van Strafrecht wordt onder geautomatiseerd werk voor de opslag of verwerking van gegevens verstaan iedere inrichting die bestemd is om langs elektronische weg gegevens op te slaan of te verwerken. Daarmee vallen niet alleen computers in de meer gangbare betekenis onder het begrip geautomatiseerd werk, maar ook computernetwerken en geautomatiseerde inrichtingen voor telecommunicatie, zoals telefoon en telefax.

De leden van de fracties van CDA en D66 hebben vragen gesteld over het mogelijk invoeren van een «kenteken» ter bestrijding van computercriminaliteit, waarbij iedere internetgebruiker een kenteken zou moeten krijgen, een en ander kennelijk met als doelstelling dat men op het internet niet langer anoniem zou kunnen blijven.
Nog afgezien van de vraag of een dergelijk systeem wel verenigbaar zou zijn met de uitgangspunten van onze open westerse democratie, is het, alleen al gelet op de technische ontwikkelingen terzake en op het grensoverschrijdende karakter van internetverkeer, niet realistisch te veronderstellen dat op nationaal niveau een waterdicht systeem van kentekens voor internetgebruikers zou kunnen worden ingevoerd en gehandhaafd, laat staan dat een dergelijk systeem ertoe zou leiden dat individuen niet meer anoniem aan internetverkeer zouden kunnen deelnemen. Een dergelijk systeem is bovendien voor opsporingsdoeleinden niet nodig. Aan de hand van *IP-adressen*, e-mailadressen en aliassen die plegen te worden vastgelegd in de zogenaamde *loggings* van computersystemen kan over het algemeen de herkomst of de bron van bepaalde informatie of berichten worden achterhaald. Langs deze weg zijn diverse computerdelicten succesvol opgespoord en vervolgd.
De leden van de D66-fractie vroegen of de ontwikkeling van de techniek met wetgeving wel valt bij te houden. Het is zeker zo dat de ontwikkeling van de techniek snel gaat. Juist daarom is het van groot belang dat de wetgeving, zeker degene die betrekking heeft op computercriminaliteit, zoveel mogelijk onafhankelijk van de techniek wordt geformuleerd. Dat uitgangspunt lag niet alleen ten grondslag aan de nota «wetgeving op de digitale snelweg» maar wordt ook daadwerkelijk toegepast bij de wettelijke bepalingen op dit vlak. In de volgende paragraaf ga ik op deze materie ook in naar aanleiding van de desbetreffende vraag van de fracties van (destijds) RPF en GPV.

Voor de vraag van de leden van de D66-fractie over de kennis en de technologische stand van zaken bij politie en justitie moge ik verwijzen naar de daarop specifiek toegespitste passage in paragraaf 9 hierna.

Deze leden vroegen aandacht voor nieuwe technieken die door criminelen worden toegepast en die, zo stelden deze leden, door politie en justitie zelden zouden worden opgespoord dan wel vervolgd. Deze leden hadden daarbij het oog op het kopen van goederen via het internet of het betalen via mobiele telefoon.
Het tot stand brengen van koopovereenkomsten door middel van internet is inmiddels gemeengoed geworden; voor het verrichten van betalingen via de mobiele telefoon geldt dat in mindere mate. Er is door het bedrijfsleven veel aan gedaan om betalingen via internet en betalingen van via internet aangeschafte goederen zo veilig mogelijk te kunnen laten verlopen. Indien goederen wel worden betaald maar niet worden geleverd, of wel worden geleverd maar niet betaald, is dat in beginsel een civielrechtelijke aangelegenheid zodat ook de civielrechtelijke weg zal moeten worden bewandeld om nakoming c.q. betaling te effectueren. Het strafrecht is hierbij ultimum remedium dat aan de orde kan komen (en ook daadwerkelijk wordt ingezet) als bijvoorbeeld stelselmatig of op grote schaal mensen worden opgelicht met koopovereenkomsten die via internet tot stand worden gebracht. Een verwante handelwijze, waarvoor het strafrecht ook daadwerkelijk is ingezet, was de oplichtingspraktijk die bekend is geworden als *advance fee fraude* en ook wel als de «*Nigerian money scam*»: daarbij werden vanuit internetcafés tal van e-mails verzonden waarin werd gevraagd geld te storten ter bemiddeling voor een zogenaamd afgezet Afrikaans staatshoofd. Politie en justitie hebben hierop adequaat gereageerd.

Ten aanzien van de vragen van de genoemde leden over het functioneren van de interregionale bureau's digitale recherche, de mate van specialisatie en daarmee samenhangende onderwerpen moge ik verwijzen naar paragraaf 9 hierna.

In antwoord op de vraag van de leden van de D66-fractie kan ik mededelen dat door middel van de tweede nota van wijziging wordt voorgesteld de strafmaat voor het eenvoudige «hacken», dat wil zeggen de computervredebreuk van artikel 138a, eerste lid, WvSr, die thans nog is gesteld op zes maanden gevangenisstraf, te verdubbelen tot een jaar gevangenisstraf. Indien de dader vervolgens opgeslagen gegevens overneemt en vastlegt, is de maximaal bedreigde straf nu overigens al vier jaar gevangenisstraf (artikel 138a, tweede lid). In het door de vragenstellers aangegeven geval is bovendien sprake van ernstige schade, zodat ook artikel 350a WvSr van toepassing is, dat een strafmaat kent van maximaal twee jaar (eerste lid) tot maximaal vier jaar (tweede en derde lid), te verhogen met maximaal een derde indien dat feit met «arglist» wordt gepleegd (artikel 354 Sr). Indien ook sprake is van een feit als bedoeld in artikel 161sexies, sub 2* (dat wil zeggen: opzettelijke vernieling of beschadiging van geautomatiseerde werken, indien daarvan gemeen gevaar voor goederen of de verlening van diensten te duchten is), sub 3* (idem, indien daarvan levensgevaar voor een ander te duchten is) of sub 4* (idem, indien het feit iemands dood ten gevolge heeft), is de maximale strafbedreiging zelfs zes respectievelijk negen of vijftien jaar gevangenisstraf.

De leden van de D66-fractie stelden vragen over de voorbereidingen die de overheid treft om aanvallen door hackers op bijv. websites van bedrijven te voorkomen en over de voorlichting die de overheid in het algemeen aan het publiek geeft over computercriminaliteit.

Het ministerie van Economische Zaken heeft in 2001 de voorlichtingscampagne Surf op Safe gestart (*www.surfopsafe.nl*), om zowel particuliere als (kleine) zakelijke internetgebruikers meer bewust te laten worden van de risico's op internet en de kwetsbaarheid van hun systeem voor dergelijke praktijken indien dit niet afdoende is beveiligd. In 2003 is de Waarschuwingsdienst ingericht (*www.waarschuwingsdienst.nl*). De Waarschuwingsdienst waarschuwt burgers en MKB voor actuele dreigingen van virussen en, veel belangrijker, voor nieuw ontdekte veiligheidsproblemen («gaten») in software die misbruikt kunnen worden om toegang te krijgen tot hun computers. Hoe sneller gebruikers deze gaten dichten, hoe kleiner de kans dat hun pc wordt misbruikt voor illegale of criminele doeleinden. Deze beide initiatieven hebben reeds geresulteerd in een betere bekendheid van de noodzaak zich goed te beveiligen en een toenemend aantal internetgebruikers dat een virusscanner en een firewall installeert op hun pc.
Vervolgens kan ik wijzen op de activiteiten van het Platform criminaliteitsbestrijding, waarover ik recentelijk Uw Kamer heb geïnformeerd. Tenslotte kan ik melden dat in het kader van het Safer Internet Actionplan – met subsidie vanuit de Europese Unie – het eerder genoemde Surf op Safe zal gaan optreden als *national awareness mode* voor veilig internetten. In 2005 zal de campagne aanzienlijk worden geïntensiveerd. De website wordt volledig vernieuwd; de campagne zal meer focussen op de risico's van misbruik en criminele praktijken en er zal een aantal doelgroepspecifieke projecten worden gestart. Eén van de doelgroepen die met vernieuwde intensiviteit zullen worden benaderd, is het MKB. Ik ben van mening dat deze nieuwe, intensievere voorlichting voldoende zal zijn om bedrijven te wijzen op de gevaren van internetcriminaliteit.

De leden van de D66-fractie stelden vragen over Echelon. Inmiddels is met de Kamer een uitgebreide discussie gevoerd over het Echelon netwerk, of beter gezegd het grootschalig afluisteren van communicatiesystemen. Ik moge verwijzen naar de brief van de minister van Defensie van 19 januari 2001 (Kamerstukken II 2000–2001, 27 591, nr. 1), de lijst met vragen en antwoorden van 14 juni 2001 (Kamerstukken II 2000–2001, 27 591, nr. 2), de brief van de minister van Binnenlandse Zaken en Koninkrijksrelaties van 4 april 2002 (Kamerstukken II 2001–2002, 27 591, nr. 4) en het naar aanleiding daarvan gevoerde overleg met de Kamer.

De leden van de GroenLinks-fractie betreurden dat de onderdelen van het wetsvoorstel die betrekking hadden op de aansprakelijkheid van tussenpersonen, waren vervallen. Zoals hiervoor al werd gememoreerd, is de aansprakelijkheid van tussenpersonen inmiddels geregeld; ik verwijs ook naar paragraaf 2 hierna.

De leden van de SP-fractie vroegen aandacht voor de positie van systeembeheerders van grotere bedrijven, instellingen etc., die in hun hoedanigheid nagenoeg onbeperkt toegang hebben tot bestanden, gebruikerscodes en passwords. Deze positie wordt voor een belangrijk deel bepaald door de Wet bescherming persoonsgegevens en door voorschriften die gelden in het kader van de arbeidsverhouding tussen degenen die werkzaam zijn bij de betrokken instelling. Daarnaast wijs ik op de tweede nota van wijziging, waarin de strafbaarheid zoals voorgesteld in artikel 273d Sr (strafbaarheid van de persoon, werkzaam bij een aanbieder van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst, die opzettelijk en wederrechtelijk kennisneemt van gegevens die niet voor hem zijn bestemd) wordt uitgebreid tot degenen die werkzaam zijn bij aanbieders van niet-openbare telecommunicatienetwerken en – diensten.

2. De aansprakelijkheid van tussenpersonen

In paragraaf 2 van het verslag werden veel vragen gesteld over het destijds door middel van een nota van wijziging laten vervallen van de onderdelen A, T en U van het wetsvoorstel, die betrekking hadden op de aansprakelijkheid van tussenpersonen. Veel vragen werden gesteld over de termijn waarop een nieuwe regeling kon worden verwacht en over de inhoud van zo'n nieuwe regeling. Deze vragen zijn inmiddels beantwoord doordat ter uitvoering van richtlijn nr. 2000/31/EG van het Europees Parlement en de Raad van de Europese Unie van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt (PbEG L 178) wetgeving tot stand is gekomen. Deze wet, de Aanpassingswet richtlijn elektronische handel (Stb. 2004, 210) is met ingang van 30 juni 2004 (Stb. 285) in werking. Daarmee is in het Wetboek van Strafrecht een nieuw artikel ingevoegd, te weten artikel 54a. Dit artikel houdt in dat de tussenpersoon die een telecommunicatiedienst verleent bestaande in de doorgifte of opslag van gegevens die van een ander afkomstig zijn, als zodanig – dat wil zeggen in zijn functie als tussenpersoon – niet wordt vervolgd indien hij voldoet aan een bevel van de officier van justitie, na schriftelijke machtiging op vordering van de officier van justitie te verlenen door de rechter-commissaris, om alle maatregelen te nemen die redelijkerwijs van hem kunnen worden gevergd om de gegevens ontoegankelijk te maken.
Volledigheidshalve moge ik verwijzen naar de toelichtende stukken op deze aansprakelijkheidsregeling (Kamerstukken II 2001–02, 28 197, nr. 3, blzz. 25–28 en 61–67). Ik meen dat daarmee een groot aantal vragen van paragraaf 2 van het verslag als beantwoord kan worden beschouwd. De nog overblijvende vragen zal ik hieronder beantwoorden.

De leden van de VVD-fractie vroegen een overzicht van de richtlijnen, verdragen, afspraken, onderhandelingen en andere voorzieningen die zich richten op het terrein van de internationale aanpak van computercriminaliteit. Het aantal voorzieningen dat zich specifiek richt op de internationale aanpak van computercriminaliteit is beperkt. Als eerste noem ik het Cybercrime Verdrag (Trb. 2002, nr. 18, en Trb. 2004, nr. 290) en het daaraan toegevoegde (eerste) Aanvullend Protocol, betreffende de strafbaarstelling van handelingen van racistische of xenophobische aard verricht via computersystemen (Trb. 2003, nr. 60, en Trb. 2005, nr. 46). Denkbaar is dat in de komende jaren nog andere protocollen worden toegevoegd. In Europees verband is inmiddels tot stand gekomen het hiervoor genoemde Kaderbesluit over aanvallen op informatiesystemen. Daarnaast bestaan in EU-kader diverse rechtsinstrumenten die niet specifiek zijn gericht op computercriminaliteit, maar waarbij doorgaans wel rekening is gehouden met het gebruik van computers of computersystemen.

De leden van de VVD-fractie vroegen de regering hoe er wordt omgesprongen met het opsporen van daders van strafbare handelingen en met name in hoeverre tussenpersonen bereid zijn vrijwillig hun medewerking te verlenen aan het opsporen van bijvoorbeeld verspreiders van kinderporno.
Met deze vraag refereerden deze leden aan een probleem dat destijds bestond omdat enkele internetproviders weigerden de voor nader onderzoek vereiste persoonsgegevens (zogenaamde NAW-gegevens) te verstrekken. Ik verwijs in dit verband op de antwoorden op vragen van het lid Van der Staaij van 12 december 2001 over problemen tussen justitie en providers bij kinderporno-onderzoek (Aanhangsel Handelingen II 2001/02, nr. 511). Met de inwerkingtreding van artikel 126na van het Wetboek van Strafvordering behoort deze problematiek tot het verleden, omdat daarbij

een wettelijke basis is gecreëerd voor het verplicht verstrekken van NAW-gegevens.

De leden van de SP-fractie vroegen de regering toe te lichten of de mogelijkheden verruimd moeten worden om muziek van extreemrechtse aard en de verspreiding daarvan via Internet (zoals nordisc) tegen te gaan. Ook vroegen zij welke prioriteit de regering legt bij de bestrijding van dergelijke uitingen, ook in internationaal verband. In dat verband wezen zij erop dat er wel voor is gewaarschuwd dat Nederland een vrijplaats zou dreigen te worden voor distributeurs.
De regering stelt zich op het standpunt dat het huidige instrumentarium voor de bestrijding van racisme en discriminatie in beginsel voldoende mogelijkheden biedt om (de verspreiding van) muziek van extreemrechtse aard via internet tegen te gaan. Aan de bestrijding van de verspreiding van extreem-rechtse muziek wordt dezelfde aandacht gegeven als aan de bestrijding van overige discriminatoire uitingen. De Aanwijzing Discriminatie van het College van procureurs-generaal is hierop onverminderd van toepassing. Deze aanwijzing geeft aan dat snel en adequaat optreden tegen discriminatie in alle gevallen aangewezen is. Het Meldpunt Discriminatie Internet heeft mij desgevraagd aangegeven, dat het aantal klachten over de verspreiding van extreemrechtse muziek via het internet verhoudingsgewijs gering is, evenals de openlijke verspreiding van dit soort materiaal via het Nederlandse deel van het internet. De meeste handel in extreem-rechtse muziek vindt plaats buiten het Internet om en richt zich voornamelijk op de buitenlandse afzetmarkt. Dat Internet een communicatiemiddel is dat bij deze handel wordt gebruikt lijkt wel vast te staan.
Voor de aanpak in internationaal verband van de internethandel in rechtsextremistische muziek staat het algemeen instrumentarium voor internationale strafrechtelijke samenwerking ter beschikking van politie en openbaar ministerie. Waar nodig vindt overleg en afstemming plaats met politie in andere landen en wordt dit instrumentarium ingezet. Wanneer buitenlandse distributeurs zich bedienen van in Nederland gevestigde distributeurs om (al dan niet via Internet) dergelijke muziek te verkopen, kunnen de in Nederland gevestigde distributeurs uiteraard worden aangepakt.

In antwoord op de desbetreffende vraag van de leden van de fracties van (destijds) RPF en GPV – in de vorige paragraaf kwam deze kwestie ook aan de orde naar aanleiding van een vraag van de D66-fractie – meen ik te kunnen stellen dat de wetgeving inderdaad zoveel mogelijk «techniekneutraal» is geformuleerd. Dat neemt niet weg dat zich door de voortschrijding en bredere toepassing van de techniek ontwikkelingen kunnen voordoen die nopen tot aanpassing van de wetgeving. Ik noem als voorbeeld de regeling van de pseudokoop in artikel 126i Sv. Daarbij is met name gedacht aan fysieke handelingen zoals het afnemen van drugs en het verlenen van transportdiensten. Op Internet zijn echter opsporingshandelingen denkbaar die erg op de genoemde lijken en dezelfde strekking hebben, maar waarvan het de vraag is of zij zonder meer onder de werking van 126i Sv gebracht kunnen worden. Denk aan onderzoek naar de handel op Internet in illegale uitingen of programmatuur. Het kan daarbij wenselijk zijn dat een politie-ambtenaar op een bepaalde aanbieding ingaat en de betrokken gegevens afneemt. Daarom is in het wetsvoorstel voorgesteld artikel 126i Sv (evenals artikel 126q Sv) in deze zin uit te breiden.

Deze leden hebben ook gevraagd op welke onderwerpen de regering doelde, die in de toekomst regeling zouden behoeven, en op welke termijn een dergelijke regeling tegemoet gezien zou kunnen worden. Met dit laatste werd vooral gedoeld op de onderwerpen die naar verwachting

in het Cybercrime Verdrag geregeld zouden worden en in de Nederlandse wetgeving overgenomen zouden moeten worden. Te denken valt bijvoorbeeld aan de introductie van de zogenaamde bevriezingsbevoegdheid en aan de aanscherping van een aantal specifieke computerdelicten. Ik volsta met een verwijzing naar de tweede nota van wijziging bij het onderhavige wetsvoorstel, waarmee de wetgeving wordt aangepast aan het Cybercrime Verdrag.

De leden van de fracties van (destijds) RPF en GPV konden zich er in vinden dat de bescherming dat het briefgeheim met het wetsvoorstel werd doorgetrokken naar de bescherming van e-mail. Wel vroegen zij zich af of de context van het medium niet zou moeten leiden tot een zekere risicoaanvaarding, er vanuit gaande dat het briefgeheim op de elektronische snelweg op papier wel geregeld kan worden maar praktisch gezien de nodige voeten in de aarde heeft. Zo wilden de leden van deze fracties weten tot hoever de verantwoordelijkheid van een provider strekt om gegevens te beschermen tegen hackers.
Het aanbieden van een e-maildienst geschiedt in de regel door partijen die gelden als aanbieders van openbare elektronische communicatiediensten en netwerken in de zin van artikel 1 van de Telecommunicatiewet. Als uitwerking van artikel 13 van de Grondwet legt de Telecommunicatiewet aan deze aanbieders de verplichting op hun systemen te beveiligen, zodat onbevoegden niet eenvoudig kennis kunnen nemen van het door middel van die systemen onderhouden verkeer. De mailboxen van individuele e-mailabonnees maken onderdeel uit van de computersystemen van die dienstenaanbieders. Voor zover genoemde beveiligingsverplichting zich niet al reeds tot deze mailboxen uit zou strekken, mag er vanuit worden gegaan dat providers een zelfstandige behoefte hebben tot het beveiligen van hun systemen teneinde de integriteit en continuïteit van hun dienstverlening te waarborgen. Absolute zekerheid dat onbevoegden nooit kennis kunnen nemen van e-mailverkeer kan daarbij niet worden gegeven, aangezien de mate waarin beveiligingsmaatregelen toepassing vinden, mede afhangt van de door de individuele provider te maken afweging van het te beschermen belang en de grootte van het te bestrijden risico, nog daargelaten de mogelijkheid van het optreden van menselijke fouten.

De leden van de genoemde fracties vroegen zich verder af of een ISP niet kennis van de inhoud van een e-mailbericht zou moeten nemen indien blijkt dat dit niet kan worden afgeleverd.
Indien bij het traditionele postverkeer een poststuk niet kan worden afgeleverd omdat het bestemmingsadres onjuist of onvolledig is en de afzender ontbreekt of dit adres eveneens onjuist of onvolledig is, kan het nodig zijn om het poststuk voor nader onderzoek te openen teneinde aflevering of terugzending mogelijk te maken, zoals geregeld in de Postwet. Het internet e-mailprotocol is zo ingericht dat uitgaande berichten automatisch worden voorzien van het e-mailadres van de afzender. Indien het bestemmingsadres niet geldig is, wordt het bericht aan de afzender teruggezonden. Indien het e-mailadres van de geadresseerde wel geldig is maar aan een ander toebehoort dan de door de afzender bedoelde persoon, zal deze laatste het bericht in zijn mailbox ontvangen. Zolang een e-mailbericht een geldig bestemmingsadres of afzenderadres bevat beperkt de taak van de provider zich tot het transport van het bericht. In sommige gevallen wordt het afzenderadres gemanipuleerd en vervangen door een niet bestaand adres waarmee de verzender voorkomt dat berichten die niet kunnen worden afgeleverd in zijn mailbox terugkeren; deze techniek («*spoofing*») wordt wel aangetroffen bij het zogenaamde *spammen*. Het kan voorkomen, dat dergelijk e-mailverkeer niet in een mailbox wordt opgeslagen maar enige tijd in het netwerk heen en weer gaat. In veel gevallen wordt dit uiteindelijk door de provider onderdrukt. Onderzoek van deze berichten teneinde tot aflevering te

geraken zal niet nodig zijn, aangezien de afzender er kennelijk geen prijs op stelt deze terug te ontvangen.

3. Vernietiging van computergegevens

In paragraaf 3 van het verslag waren de vragen samengebracht in verband met de in het wetsvoorstel in artikel 125o Sv voorgestelde bevoegdheid tot het ontoegankelijk maken van gegevens, eventueel gevolgd door de in artikel 354 Sv voorgestelde vernietiging. Ook in paragraaf 7 van het verslag waren nog enkele vragen (met name van de SGP-fractie) over dit onderwerp opgenomen. Deze vragen worden in het onderstaande zoveel mogelijk per onderwerp gegroepeerd beantwoord.

De leden van de fractie van de PvdA juichten de voorgestelde uitbreiding van bevoegdheden toe. Wel vroegen zij of het wel juist is, zoals gesteld in de toelichting, dat de vermogenswaarde van gegevens vaak ontbreekt dan wel moeilijk te kwantificeren is. In het economisch verkeer neemt de waarde van bijvoorbeeld klantgegevens toch steeds meer toe?
Met deze leden ben ik eens dat gegevens wel degelijk een economische waarde kunnen vertegenwoordigen. De passage in de memorie van toelichting waar deze leden op doelden (blz. 20), beoogde slechts aan te geven dat het niet nodig is voor gegevens de strafrechtelijke maatregel van «onttrekking aan het verkeer» in het leven te roepen. De argumentatie daarvoor moet inderdaad niet zozeer worden gevonden in het ontbreken van een waarde van gegevens of het moeilijk kunnen vaststellen van die waarde, als wel in het onstoffelijke karakter van gegevens en het feit dat met ontoegankelijkmaking en vernietiging hetzelfde doel kan worden bereikt, zodat niet een geheel parallel systeem als voor stoffelijke objecten tot stand hoeft te worden gebracht.

De leden van de PvdA-fractie wezen erop dat van één e-mailbericht verschillende exemplaren kunnen bestaan, bijvoorbeeld indien het bericht naar verschillende adressen tegelijk wordt doorgezonden of indien het bericht door de ontvanger vervolgens weer aan anderen wordt doorgezonden. Zij vroegen of dan de voorwaarden voor ontoegankelijkmaking c.q. vernietiging nog wel gelden.
De voorwaarde om te kunnen overgaan tot ontoegankelijkmaking op de voet van artikel 125o Sv – hetzelfde geldt voor vernietiging conform artikel 354 Sv – is dat dit noodzakelijk is ter beëindiging van een strafbaar feit of ter voorkoming van nieuwe strafbare feiten. De bedoeling van de maatregel is om de voortzetting of de herhaling van het strafbare feit door de houder of de gebruiker van het desbetreffende computersysteem te verhinderen of in ieder geval daaraan bij te dragen. Dat dezelfde of soortgelijke gegevens ook elders kunnen worden aangetroffen, doet daaraan niet af. Wel zal het, indien blijkt dat de desbetreffende gegevens vanuit dat of een ander geautomatiseerd werk verdere verspreiding hebben gevonden, voor de hand liggen dat het opsporingsonderzoek zich niet tot dat eerste geautomatiseerde werk beperkt.

De leden van de VVD-fractie vroegen, of de voorgestelde bepalingen in voldoende mate de lacune afdichten die bestaat in de beslagleggingsbevoegdheden waar het gaat om gegevens die deel uitmaken van een strafbaar feit of met behulp waarvan het strafbare feit is begaan. Ik kan deze vraag bevestigend beantwoorden. Het wetsvoorstel voorziet in deze lacune door in de artikelen 125o en 354 Sv de mogelijkheid te openen om computergegevens met betrekking waartoe of met behulp waarvan een strafbaar feit is gepleegd, bij wijze van voorlopige maatregel ontoegankelijk te maken c.q. – bij de einduitspraak over het feit of bij afzonderlijke beschikking – door de rechter te doen vernietigen.

De leden van de VVD-fractie vroegen, welke gegevens die bij onderzoek van geautomatiseerde systemen zijn vastgelegd, niet behoeven te worden vernietigd nadat zij niet meer van betekenis zijn voor het onderzoek. Deze vraag had, als ik het goed zie, betrekking op de vernietiging van bij het onderzoek vastgelegde gegevens op de grondslag van het in het wetsvoorstel voorgestelde artikel 125q Sv. Dit artikel is bij de tweede nota van wijziging vervallen, zodat het thans geldende artikel 125n Sv gehandhaafd blijft. Dat artikel bepaalt dat gegevens die van geen betekenis zijn voor het onderzoek, worden vernietigd en geeft – zoals hierna aan de orde komt – in het derde lid uitzonderingen op deze regel. De genoemde leden vroegen of bij zo'n onderzoek ook kopieën kunnen worden gemaakt voor andere doeleinden. Gegevens die in een bepaald onderzoek zijn vastgelegd, dienen in beginsel alleen voor dat onderzoek te worden gebruikt. Deze materie wordt beheerst door de Wet politieregisters en door het genoemde artikel 125n Sv. In het derde lid van artikel 125n Sv is vastgelegd dat de officier van justitie kan bepalen dat vastgelegde gegevens (a) kunnen worden gebruikt voor een ander *strafrechtelijk* onderzoek dan waartoe de bevoegdheid is uitgeoefend of (b) kunnen worden opgeslagen in een *register zware criminaliteit*, indien het gegevens betreft omtrent een persoon als bedoeld in artikel 13a, eerste lid, onderdeel a tot en met c, van de Wet politieregisters. Het vierde lid bepaalt dat alsdan de desbetreffende gegevens niet behoeven te worden vernietigd, ook al zijn zij niet van betekenis in het onderzoek waarvoor zij zijn vastgelegd. In hoeverre voor andere doelen gegevens uit een politieregister mogen worden verstrekt, wordt bepaald door de Wet politieregisters, die een gesloten verstrekkingenregime kent. In bepaalde gevallen kunnen gegevens worden verstrekt aan ontvangstgerechtigden, zoals bijzondere opsporingsambtenaren, indien zij deze, bij het onderzoek waarbij zij zijn betrokken, nodig hebben voor de opsporing van strafbare feiten.

De leden van de VVD-fractie hebben de vraag gesteld of het uit een oogpunt van proportionaliteit aanvaardbaar zou zijn indien een harde schijf in beslag zou worden genomen met het oog op de daarop opgeslagen gegevens, en of het daarbij van belang zou zijn of de harde schijf tevens het besturingsprogramma en/of applicaties bevat.
Indien voor het onderzoek de beschikbaarheid van bepaalde gegevens nodig is, zal de opsporingsambtenaar steeds moeten afwegen op welke wijze in het concrete geval invulling moet worden gegeven zowel aan het proportionaliteits- als aan het subsidiariteitsbeginsel, waarbij ook de effectiviteit van de te kiezen maatregel van belang is. De minst inbreuk makende bevoegdheid zal doorgaans bestaan in de vordering om bepaalde gegevens te verstrekken, zoals voorzien in de artikelen 126nc en 126nd Sv, voorgesteld in het eerder gememoreerde Wetsvoorstel Bevoegdheden vorderen gegevens (29 441). Als dat niet mogelijk is, bijvoorbeeld omdat niet op voorhand bekend is welke gegevens nodig zijn, kan gedacht worden aan hetzij inbeslagneming van het voorwerp waarmee de gegevens verbonden zijn, hetzij vastlegging van de gegevens zelf. In de memorie van toelichting bij genoemd Wetsvoorstel Bevoegdheden vorderen gegevens (29 441, nr. 3, blz. 18) is een situatie besproken waarin vooraf vaststaat dat inbeslagneming van het voorwerp niet nodig is omdat volstaan kan worden met het ter plekke inzien van de computer en het vervaardigen van kopieën van de gezochte gegevens door deze op een gegevensdrager vast te leggen. Dit laatste is ten opzichte van de inbeslagneming van de harde schijf minder belastend voor degene die op de plaats van de doorzoeking dagelijks van de computer gebruik maakt, zeker wanneer de computer deel uitmaakt van een netwerk. In dat geval dient volstaan te worden met een doorzoeking ter vastlegging van gegevens op grond van artikel 125i Sv. In bepaalde gevallen kan het niettemin noodzakelijk zijn om toch de harde schijf in beslag te nemen, bijvoorbeeld indien deze alleen adequaat kan worden onderzocht met behulp van appa-

ratuur die elders aanwezig is. Indien de voor het onderzoek benodigde gegevens zich op een schijf bevinden die op eenvoudige en veilige wijze kan worden verwijderd, zou het evenwel disproportioneel zijn om het gehele systeem in beslag te nemen. Op overeenkomstige wijze zou het disproportioneel zijn om een volledige schijf in beslag te nemen indien de benodigde gegevens slechts een beperkt deel van de informatie-inhoud van het geheel zouden uitmaken. In dat laatste geval kan men zich voorstellen dat het overnemen en vastleggen van de benodigde gegevens de voorkeur verdient. Deze regel heeft echter geen algemene geldigheid, omdat omstandigheden kunnen dwingen tot andere keuzes. Indien de desbetreffende gegevens niet langs betrouwbare weg kunnen worden veiliggesteld, bijvoorbeeld omdat vermoed wordt dat het computersysteem niet betrouwbaar functioneert, kan de inbeslagneming van de schijf of zelfs van het gehele systeem niet als disproportioneel worden aangemerkt. Ook kan het nodig zijn om naast gegevens tevens bepaalde programmatuur veilig te stellen indien deze nodig is om toegang tot de veiliggestelde gegevens mogelijk te maken. Steeds is derhalve in concreto een beoordeling van de feiten en omstandigheden nodig om te komen tot die inzet die het meest in aanmerking komt in het licht van de effectiviteit van de maatregel en de eisen van proportionaliteit en subsidiariteit.

De leden van de VVD-fractie hebben gevraagd of de maatregelen van ontoegankelijkmaking en vernietiging van gegevens ook kunnen worden toegepast op computers in het buitenland of dat de toepassing zich beperkt tot Nederlandse computers, ongeacht of deze systemen zich in een nationaal of internationaal netwerk bevinden.
De toepassing van strafvorderlijke bevoegdheden wordt begrensd door het volkenrecht en het interregionale recht, zoals geformuleerd in artikel 539a, derde lid, Sv. Het volkenrecht erkent rechtsmacht van de nationale staat binnen het eigen territorium, eventueel uit te breiden met het continentale plat en aan boord van schepen en vliegtuigen onder nationale registratie. Onder de plaats waar een computersysteem zich bevindt dient te worden verstaan de fysieke locatie waar het systeem is opgesteld of – indien het systeem uit verschillende componenten bestaat – de plaats waar een of meer van die componenten zich bevinden. Toepassing van de bevoegdheid tot ontoegankelijkmaking is derhalve alleen mogelijk ten aanzien van gegevens die zijn opgeslagen in computersystemen die zich bevinden binnen het Nederlandse territorium, op het continentaal plat of aan boord van een vaar- of luchtvaartuig dat onder Nederlandse vlag is geregistreerd. Voor toepassing van de maatregel van ontoegankelijkmaking in computersystemen die zich buiten de Nederlandse rechtsmacht bevinden, zal derhalve een beroep moeten worden gedaan op internationale rechtshulp, ten behoeve waarvan het Cybercrime Verdrag tot stand is gebracht. Ik verwijs ook naar het gestelde hieronder in paragraaf 7 over opsporingsonderzoek op openbare computernetwerken.

De leden van de VVD-fractie hebben vervolgens gevraagd hoe in praktische zin gegevens voor de netwerkbeheerder ontoegankelijk kunnen worden gemaakt, anders dan door fysieke verwijdering, nu deze netwerkbeheerder uit hoofde van zijn functie volledige toegangsrechten kent.
De maatregel van ontoegankelijkmaking kan worden uitgevoerd hetzij door de gegevens tijdelijk van de betrokken gegevensdrager te verwijderen, hetzij door de gegevens in het systeem te laten maar deze feitelijk ontoegankelijk te maken. Een methode waarop gegevens feitelijk ontoegankelijk gemaakt kunnen worden, is de versleuteling van de gegevens.
De maatregel van ontoegankelijkmaking strekt ertoe dat zowel de raadpleging als het gebruik van die gegevens niet langer mogelijk is, zodat het strafbare feit wordt beëindigd of nieuwe strafbare feiten worden voorkomen. Indien de gegevens ontoegankelijk worden gemaakt door versleu-

teling, treft deze gebruiksbeperking een ieder, dus ook de systeembeheerder.
Deze leden hebben nog aandacht gevraagd voor de situatie waarin ontoegankelijkmaking gevolgen heeft voor het functioneren van het desbetreffende netwerk. Bij de keuze van de wijze waarop de gegevens ontoegankelijk worden gemaakt, gelden vanzelfsprekend de eisen van effectiviteit, subsidiariteit en proportionaliteit. Het ligt voor de hand dat bij deze keuze rekening wordt gehouden met belangen van derden. Indien voor de ontoegankelijkmaking gekozen kan worden tussen een methode die wel, en een methode die geen gevolgen heeft voor het functioneren van een netwerk, zal – indien er geen andere relevante verschillen zijn – natuurlijk voor die laatste methode gekozen worden.

Voor de vragen van de leden van de VVD-fractie over de organisatie, uitrusting en opleiding van de politie verwijs ik naar paragraaf 9 hierna.

De leden van de VVD-fractie vroegen, welke garanties het wetsvoorstel biedt voor de vertrouwelijkheid van het onderzoek. Voor opsporingsambtenaren geldt vanzelfsprekend een met hun functie samenhangende algemene geheimhoudingsplicht. Voor zover bij het onderzoek derden worden betrokken zullen terzake doorgaans afspraken worden gemaakt over de in acht te nemen vertrouwelijkheid voor een daarbij te bepalen termijn. De betrouwbaarheid van de bij het onderzoek te betrekken personen zal doorgaans een belangrijk criterium zijn bij de keuze van de personen. Tenslotte biedt artikel 126bb, vijfde lid, een bijzondere wettelijke geheimhoudingsplicht voor de categorie van personen tot wie een vordering wordt gericht inzake de verstrekking van gegevens.

De leden van de VVD-fractie vroegen of het niet wenselijk is om het bevel te kunnen uitvaardigen dat iedere vorm van bewerking, opslag of overdracht van gegevens wordt gestaakt, zodra is beslist dat de gegevens ontoegankelijk worden gemaakt. Deze leden zullen daarbij de situatie op het oog hebben gehad, waarin er enig tijdsverloop zit tussen het moment waarop wordt beslist dat gegevens ontoegankelijk worden gemaakt en het moment van uitvoering van de maatregel, waardoor het mogelijk is om de gegevens aan de controle van politie en justitie te onttrekken.
Het door deze leden bedoelde bevel kan inderdaad nuttig en zelfs noodzakelijk zijn en de wet biedt daarvoor ook een grondslag in artikel 125 Sv. Het onderzoek van computersystemen in de zin van de zevende afdeling zal doorgaans immers plaatsvinden in het kader van een doorzoeking, zoals geregeld in artikel 125i Sv. Op grond van artikel 125 Sv kan de bevoegde ambtenaar onder meer «de nodige maatregelen tot bewaking of afsluiting nemen». Dat betekent dat de opsporingsambtenaar de maatregelen kan nemen die redelijkerwijs nodig zijn om te voorkomen dat ontoegankelijkmaking niet meer mogelijk is.

De leden van de VVD-fractie vroegen aandacht voor de passage in de memorie van toelichting (nr. 3, blz. 23) waarin was vermeld dat het aantreffen van een racistische uiting in een e-mailbox op zich zelf nog geen grond is voor ontoegankelijkmaking. Zij vroegen of dit anders is, indien de uiting is verzonden aan een groep van personen of aan een openbare mailinglist.
Zoals hierboven aangegeven strekt de maatregel van ontoegankelijkmaking ter beëindiging van het strafbare gedrag of ter voorkoming van eenzelfde strafbare feit. In geval van een racistische uiting, bijvoorbeeld in de zin van artikel 137d of 137e Sr, ontstaat eerst strafbaarheid indien de uiting in het openbaar wordt gedaan. Het uitwisselen van racistische uitingen per brief of op elektronische wijze per e-mail tussen individuele personen voldoet niet aan dit openbaarheidscriterium en wordt als vorm van besloten communicatie beschermd onder artikel 13 Grondwet. Dit kan

anders zijn indien de bestemming van een dergelijke racistische uiting niet een individuele persoon betreft maar verschillende personen. Of dan nog van een besloten communicatie kan worden gesproken hangt af van de vraag of de groep geadresseerden kan worden beschouwd als een gesloten groep. Dit hangt af van verschillende factoren, zoals de grootte van de groep, de gemeenschappelijke achtergrond van de leden van de groep, de wijze van samenstelling van de groep en de aanwezigheid van een gemeenschappelijk doel. Het zenden van eenzelfde racistische e-mailbericht aan een willekeurig aantal geadresseerden zal kunnen gelden als de verspreiding van een dergelijke uiting in het openbaar en zal derhalve strafbaar zijn onder genoemd artikel 137d of 137e Sr. Of het verzenden per e-mail van een racistisch bericht aan personen die op een openbare mailinglist staan aan het openbaarheidscriterium voldoet, naast bovengenoemde criteria, hangt tevens af van vraag in welke relatie de verzender tot de betrokken personen staat.

De leden van de CDA-fractie hebben een vraag gesteld over artikel 125n zoals in het wetsvoorstel opgenomen. Zoals hiervoor al werd aangegeven, is dat artikel door middel van de tweede nota van wijziging uit het wetsvoorstel geschrapt.

De leden van de fracties van CDA en D66 hebben gevraagd of het wel juist is dat de rechter-commissaris zeggenschap krijgt over het beëindigen of voorkomen van strafbare feiten. Voorop staat dat het hierbij gaat om een maatregel die onlosmakelijk verbonden is met het doorzoeken van een geautomatiseerd werk. Indien dat doorzoeken plaatsvindt onder verantwoordelijkheid van de rechter-commissaris – en dat is het geval bij een gerechtelijk vooronderzoek – dan dient deze ook verantwoordelijkheid te kunnen dragen voor de maatregel van ontoegankelijkmaking van gegevens, al was het maar omdat die maatregel invloed kan hebben op het onderzoek zelf. Met de in artikel 125o voorgestelde regeling wordt dan ook aangesloten bij de toedeling van bevoegdheden tijdens een gerechtelijk vooronderzoek. De leden van genoemde fracties hebben wel in die zin gelijk dat het voorkomen en beëindigen van strafbare feiten niet tot de reguliere taken van de rechter-commissaris behoort. Verwacht mag dan ook worden dat de rechter-commissaris niet op eigen initiatief maar op voorstel van de officier van justitie komt tot een beslissing tot ontoegankelijkmaking.

De leden van de CDA-fractie hebben gewezen op de risico's voor buitenproportionele schade die kan optreden indien onoordeelkundig gebruik wordt gemaakt van bevoegdheden bij onderzoek in complexe geautomatiseerde omgevingen. Volgens deze leden dienen de verantwoordelijke autoriteiten zich bij hun beslissing of tot onderzoek moet worden overgegaan weliswaar rekenschap te geven van de beginselen van proportionaliteit en subsidiariteit, maar zou de wetgever hierbij speciale waarborgen dienen te creëren.
Inderdaad kunnen zich, bij een onoordeelkundig gebruik van de bevoegdheden in het kader van onderzoek in complexe geautomatiseerde omgevingen, grote risico's voordoen voor het optreden van aanzienlijke schade. Dit moet vanzelfsprekend zoveel mogelijk worden voorkomen. Maar ik meen dat het niet juist zou zijn hiertoe speciale wettelijke waarborgen in het leven te roepen. Bij alles wat politie en justitie doen moeten zij met voldoende kennis van zaken optreden en moeten zij zich rekenschap geven van – onder andere – de beginselen van proportionaliteit en subsidiariteit. Daarbij moet worden zorggedragen voor een adequaat kennisniveau zowel van de geautomatiseerde omgevingen als van de invloed van onderzoeksmaatregelen daarop; ik verwijs in algemene zin naar paragraaf 9 hierna, waarin wordt ingegaan op het kennisniveau terzake. Het is natuurlijk van belang dat het onderzoek wordt uitgevoerd door opsporings-

ambtenaren die kennis hebben van de mogelijkheden en werking van ICT en van het te onderzoeken geautomatiseerde systeem in het bijzonder. Indien bij het onderzoek blijkt dat specifieke expertise benodigd is, kunnen zodanige maatregelen worden getroffen dat het onderzoek op een later tijdstip door specifieke deskundigen kan worden uitgevoerd. Maar daar komt nog iets bij. Ter voorbereiding van maatregelen die in het kader van onderzoek in een bepaald geautomatiseerd systeem zullen worden genomen, zal doorgaans een analyse worden gemaakt van alle relevante factoren. Van grote betekenis daarbij is de rol van de systeembeheerder. Deze zal doorgaans bereid zijn vrijwillig medewerking te verlenen, enerzijds omdat hij belang heeft bij het voorkomen van schade aan zijn systeem en anderzijds omdat het ook in zijn belang is dat strafbare feiten worden beëindigd en/of voorkomen.

De leden van de D66-fractie hebben gevraagd of en, zo ja, wanneer de beheerder van een geautomatiseerd werk aanspraak kan maken op een vergoeding op basis van de Wet tarieven in strafzaken. In de memorie van toelichting (nr. 3, blz. 21) was terzake van ontoegankelijkmaking het volgende gemeld: «... In iedere situatie zal moeten worden beoordeeld welke maatregel het meest effectief is. Daarbij moeten uiteraard de eisen van proportionaliteit en subsidiariteit in acht worden genomen. Dit vereist in het bijzonder in netwerkomgevingen voorzichtigheid, opdat niet onnodig schade wordt toegebracht aan gegevens of systemen. Soms zal het daarom in de rede liggen om de medewerking van de netwerkbeheerder te vragen. Deze kan daarvoor eventueel een vergoeding krijgen op grond van de Wet tarieven in strafzaken.». Deze laatste volzin is onjuist. Slechts indien sprake is van afgedwongen medewerking, biedt de wet een grondslag voor vergoeding. Een dergelijke medewerkingsplicht voor de systeembeheerder bij de ontoegankelijkmaking wordt door het wetsvoorstel niet in het leven geroepen. Er is dan ook geen aanspraak op een vergoeding, tenzij in een individueel geval een vergoeding wordt overeengekomen.

De leden van de GL-fractie gaven aan dat zij het tijdelijk onbruikbaar maken van de toegangspoort van een computer een te vergaande maatregel achtten. Deze vorm van ontoegankelijkmaking van gegevens is inderdaad zeer vergaand en zal pas in beeld kunnen komen als minder vergaande maatregelen onvoldoende soelaas bieden. Bij het kiezen van de meest in aanmerking komende vorm van ontoegankelijkmaking dient – het kwam hiervoor al meermalen aan de orde – niet alleen te worden gelet op de effectiviteit van de maatregel, maar ook op de eisen van proportionaliteit en subsidiariteit. In de memorie van toelichting (blz. 21) zijn naast deze vergaande vorm van ontoegankelijkmaking dan ook andere, minder vergaande en minder inbreukmakende modaliteiten genoemd. Maar in algemene zin zal ook het tijdelijk onbruikbaar maken van de toegangspoort als optie mogelijk moeten zijn.

De leden van de GL-fractie stelden een vraag over de notificatieplicht zoals opgenomen in het voorgestelde concept-artikel 125p. Bij de tweede nota van wijziging is dit artikel echter geschrapt, omdat in dit onderwerp wordt voorzien door het Wetsvoorstel bevoegdheden vorderen gegevens. De inhoud van het concept-artikel 125p is in grote lijnen overgenomen in artikel 125m zoals voorgesteld in bedoeld wetsvoorstel.

4. Medewerking aan de ontsleuteling van gegevens

Gevraagd is, hoe bevorderd kan worden dat derden over voldoende kennis beschikken om te ontsleutelen, en aandacht te besteden aan een zgn. sleuteldeponeringsplicht. In het kader van Nationaal TTP-project zijn de mogelijkheden onderzocht voor rechtmatige toegang tot versleutelde

elektronische berichten. Gelet op de resultaten en eindconclusies van het onderzoek zag het kabinet destijds geen aanleiding om over te gaan tot het invoeren van een zelfreguleringsmechanisme of een wettelijke verplichting voor Trusted Third Parties die vertrouwelijkheidsdiensten aanbieden tot het deponeren van sleutels. Het huidige kabinet onderschrijft de conclusie van destijds dat de dienstverlening van TTP's geen grote belemmeringen oplevert bij de opsporing door Justitie. Een sleuteldeponeringsplicht acht ik derhalve ook nu niet opportuun, gezien de vele bezwaren die blijkens het onderzoek aan een dergelijke plicht kleven. De bevoegdheid waarover de opsporingsdiensten op grond van artikel 125k Sv beschikken zijn in de praktijk afdoende gebleken voor een goede samenwerking met TTP's. Voor een uitvoerige bespreking van de resultaten en eindconclusies van het Nationaal TTP-project verwijs ik u graag naar de notitie «Rechtmatige Toegang: mogelijkheden ontcijferd» (Kamerstukken TK, 2002–2003, 26 581, nr. 2).

In antwoord op de vraag van de leden van de fracties van VVD, CDA en D66 kan ik bevestigen dat een weigerachtige derde die het bevel tot decryptie niet opvolgt, zich schuldig maakt aan het strafbare feit van art 184 Sr. De sanctie op overtreding van artikel 184 Sr – gevangenisstraf van ten hoogste drie maanden of een geldboete van € 2 250,- voor natuurlijke personen en € 4 500,- voor rechtspersonen – acht ik in verhouding tot de ernst van de overtreding. Ik zie geen dringende redenen om de weigering van een derde om mee te werken aan ontsleuteling als een ernstiger overtreding op te vatten dan het niet opvolgen van enig ander ambtelijk bevel, waarmee in veel gevallen ook grote belangen gemoeid kunnen zijn.

De leden van de VDD-fractie hebben de vraag opgeworpen of de medewerkingsverplichting onder omstandigheden afbreuk kan doen aan de bewijskracht van het ontsleutelde materiaal. Ik acht het niet aannemelijk dat bij de ontsleuteling andere informatie dan de oorspronkelijke informatie kenbaar zal worden gemaakt. Het doel van versleuteling is juist om manipulatie van gegevens te voorkomen en de authenticiteit van de informatie te garanderen. Indien bij ontsleuteling de informatie gemanipuleerd zou worden verliest de versleuteling ook iedere betekenis voor de oorspronkelijke gebruikers van de versleuteling.

Ik acht het dan ook niet noodzakelijk – dit in antwoord op de terzake door de leden van de fracties van VVD, CDA en D66 gestelde vragen – om een onafhankelijke deskundige partij te belasten met de ontsleuteling van gegevens. In het geval dat er vrees bestaat dat de derde bij ontsleuteling de gegevens zal manipuleren kunnen de opsporingsdiensten de nodige toezichtsmaatregelen treffen om manipulatie te voorkomen. Ook kan, als er een dergelijk risico bestaat, gevraagd worden om de kennis ter beschikking te stellen waarna door de politie zelf wordt ontsleuteld (artikel 125k, eerste lid, slot). De vraag naar de betrouwbaarheid van een derde speelt niet alleen bij het bevel tot ontsleuteling. Ook bij uitlevering van voorwerpen door derden op grond van artikel 96a Sv dienen de opsporingsdiensten zich te vergewissen van de betrouwbaarheid van de uitgeleverde voorwerpen.

De leden van de VVD-fractie stelden de vraag of de termijn waarin het bevel tot ontsleuteling kan worden gegeven wel in voldoende mate zal worden verruimd in de voorgestelde formulering «bij of terstond na een doorzoeking». Ik meen met deze leden, dat de gekozen terminologie een onwenselijke beperking inhoudt. In de praktijk zal in veel gevallen niet tijdens de doorzoeking of terstond daarna, maar pas bij het onderzoek in een geautomatiseerd werk duidelijk worden dat de gegevens beveiligd of versleuteld zijn. In het geval van grootschalige en complexe onderzoeken is het immers denkbaar dat het enkele dagen of zelfs weken duurt voordat

de beveiliging of versleuteling wordt ontdekt. De formulering «terstond na een doorzoeking» acht ik in dergelijke gevallen inderdaad niet adequaat. Door middel van een nota van wijziging zal de bepaling zodanig worden verruimd, dat het bevel tot ontsleuteling of het ongedaan maken van een beveiliging ook nog daarna kan worden gegeven. Een specifieke tijdsbegrenzing is overigens ook niet nodig.

De leden van de fracties van CDA, D66 en GroenLinks hebben vragen gesteld over het zogenaamde nemo tenetur-beginsel in relatie tot de verplichting voor betrokkenen om medewerking te verlenen aan decryptie.
In antwoord op de vraag van de leden van de CDA-fractie stel ik voorop dat het wetsvoorstel niet voorziet in een medewerkingsplicht voor de verdachte om gegevens te ontsleutelen. Expliciet wordt bepaald dat het bevel tot ontsleuteling niet aan de verdachte kan worden gericht, waarmee het zwijgrecht van de verdachte uitdrukkelijk wordt erkend en ongepaste dwang jegens de verdachte wordt voorkomen.
De leden van de D66-fractie wensen een nadere uiteenzetting ten aanzien van de vraag of een jegens de verdachte gedwongen afgifte van een wachtwoord in strijd zou zijn met het nemo tenetur-beginsel. Allereerst wil ik erop wijzen dat in het voorstel de systematiek ten aanzien van de ontsleutelplicht, zoals die nu reeds voor derden geldt op grond van artikel 125k, wordt gehandhaafd. Evenals bij artikel 125k zal ook voor het voorgestelde artikel 126m, zesde lid, gelden dat het bevel tot ontsleuteling niet tot de verdachte kan worden gericht.
Uit de beslissing van het Europese Hof van de rechten van de mens in de zaak Saunders (EHRM 17 december 1996, NJ 1997, 699) valt af te leiden dat het zwijgrecht en het recht zichzelf niet te beschuldigen besloten ligt in het «fair-trial» beginsel van artikel 6, eerste lid, EVRM. Het nemo tenetur-beginsel beschermt de verdachte tegen ongepaste dwang bij het vergaren van bewijsmateriaal. Dit betekent volgens het Hof echter niet dat de verdachte op geen enkele wijze kan worden gedwongen aan zijn eigen veroordeling mee te werken. In de gevallen dat het materiaal onafhankelijk van de wil van de verdachte bestaat kan de verdachte onder omstandigheden wel tot medewerking worden verplicht. Het Hof denkt hierbij aan het uitleveren van documenten of het afstaan van urinemonsters of lichaamsweefsel. De medewerking van de verdachte is in deze gevallen naar het oordeel van het Hof toelaatbaar, aangezien deze materialen zonder ongepaste dwang jegens de verdachte kunnen worden verkregen. In deze gevallen bestaat ook niet het gevaar dat de verdachte onder dwang valse informatie verstrekt die tot een justitiële dwaling aanleiding kan geven. Informatie die zich in het geheugen van de verdachte bevindt, zoals een wachtwoord of encryptiesleutel, kan evenwel niet worden gekwalificeerd als materiaal dat bestaat onafhankelijk van de wil van de verdachte. Het prijsgeven van deze informatie kan slechts plaats vinden met de wilsinstemming van de verdachte. Gelet op het oordeel van het Hof zal een verplichting voor de verdachte tot het prijsgeven van de encryptiesleutel die zich in zijn geheugen bevindt, ontoelaatbaar moeten worden geacht.
Naast het nemo tenetur-beginsel en het daaruit voortvloeiende zwijgrecht verzet overigens ook de onzekerheid of de verdachte daadwerkelijk nog over het wachtwoord beschikt, zich tegen een gedwongen afgifte van een encryptiesleutel door de verdachte (Zaak-Funke, EHRM 25 februari 1993, NJ 1993, 485).

De leden van de Groen-Links fractie hebben in dit verband nog gevraagd naar de reikwijdte van het nemo tenetur-beginsel, in het bijzonder wanneer een derde juist doordat hij medewerking verleent aan ontsleuteling, zelf (mede)verdachte wordt.

Het Hof heeft in de zaak Saunders de reikwijdte van het nemo tenetur-beginsel en het daaruit voortvloeiende zwijgrecht beperkt tot de verdachte. Naar het oordeel van het Hof kan er alleen een beroep op het zwijgrecht worden gedaan indien er sprake is van een «criminal charge» in de zin van artikel 6 EVRM. In het licht van de uitspraken van het Hof kan een niet-verdachte worden bevolen mee te werken aan de ontsleuteling van een aan hem gericht e-mail bericht. Ook in het geval dat uit de inhoud van het bericht zou kunnen blijken dat de niet-verdachte zich schuldig heeft gemaakt aan het plegen van een strafbaar feit. Er is geen strafrechtelijk beginsel dat een niet-verdachte ontslaat van zijn medewerkingsverplichting. Een beroep op het zesde lid van de artikelen 126m en 126t is derhalve slechts mogelijk door een verdachte en niet door een derde die zich mogelijkerwijs zelf zou kunnen incrimineren door het opvolgen van het tot hem gerichte bevel.
Voor een uitgebreide uiteenzetting over het nemo tenetur-beginsel verwijs ik overigens naar de notitie van de toenmalige Minister van Justitie over de verhouding tussen het nemo tenetur-beginsel en artikel 184 van het Wetboek van Strafrecht bij de toepassing van een maatregel in het belang van het onderzoek (Kamerstukken TK 2001–2002, 28 176, nr. 1).

5. Het onderscheid tussen opgeslagen en stromende gegevens

De leden van de fracties van CDA, PvdA, VVD en D66 hebben vragen gesteld over het onderscheid tussen opgeslagen en stromende gegevens. De vragen betroffen met name de praktische werkbaarheid van het onderscheid en de relatie tot het onderscheid tussen toekomstige en bestaande gegevens.

Het onderscheid tussen opgeslagen en stromende gegevens is vooral conceptueel van aard. Het dient ertoe een kader te bieden voor de definiëring van strafbare handelingen en het toepassingsbereik van strafvorderlijke bevoegdheden. Het onderscheidend criterium is inderdaad, zoals de fracties van CDA en D66 aangaven, of een gegeven op een door een mens te bepalen tijdstip is te raadplegen. Is dat het geval, dan kan gesproken worden van opgeslagen gegevens. Is dat niet het geval, dan betreft het stromende gegevens of gegevens in transport. Het onderscheid is aangebracht om de elementen van de delictsomschrijving goed onder woorden te kunnen brengen. De memorie van toelichting zegt daarover dat zonder een onderscheid naar opgeslagen en stromende gegevens, tot uiting gebracht in de woorden *zijn opgeslagen, worden verwerkt of overgedragen,* het niet mogelijk is de strafbepalingen en strafvorderlijke bevoegdheden voldoende precies te omschrijven. Zonder dit terminologisch onderscheid, dat dus als gezegd zijn basis vindt in het onderscheid tussen opgeslagen en stromende gegevens, zou teruggevallen moeten worden op alternatieve termen die alleen in ruimere en abstractere bewoordingen kunnen worden gevat.

Van bijzondere betekenis is het onderscheid bij de aftap- en opneemverboden (139a Sr) en -bevoegdheden (126m en t Sv). Dit houdt verband met de grondwettelijke bescherming van communicatie in de fase dat deze onder de verantwoordelijkheid berust van de transporteur (artikel 13 Grondwet). In het materiële strafrecht maakt het voor het overige niet uit of een bepaalde (strafwaardige) handeling plaatsvindt ten aanzien van opgeslagen of stromende gegevens.

Het onderscheid tussen bestaande en toekomstige gegevens staat los van het onderscheid tussen opgeslagen en stromende gegevens. Toekomstige gegevens zijn gegevens die op het moment van een verzoek of vordering nog niet bestaan. Een voorbeeld hiervan is de vraag gegevens te verstrekken over een transactie, bijvoorbeeld de overboeking van geld,

zodra die heeft plaatsgevonden. De voorgestelde bevoegdheid van artikel 126ne Sv in het Wetsvoorstel Bevoegdheden vorderen gegevens heeft hierop betrekking.

Terecht hebben de leden van de VVD fractie erop gewezen dat de algemene regel van niet-geheimhouding bij onderzoek naar bestaande gegevens, vaker dan in de geschetste gevallen doorbreking behoeft. In de praktijk worden daarover in voorkomende gevallen afspraken gemaakt. Ook is in artikel 126bb, vijfde lid, Sv bepaald dat degene tot wie een vordering tot het verstrekken van gegevens is gericht, in het belang van het onderzoek geheimhouding in acht neemt omtrent al hetgeen hem terzake van de vordering bekend is.

De leden van fracties van VVD en CDA hebben nog vragen gesteld over de uitvoerbaarheid van het onderscheid tussen het aftappen van e-mailverkeer en het bevel tot uitlevering van opgeslagen e-mail; de leden van de VVD-fractie vroegen daarbij of dat onderscheid geen verzwaring van de voorwaarden betekent ten opzichte van de situatie waarbij in zijn geheel zou worden aangesloten bij de systematiek van het aftappen van telecommunicatie.
Ik stel voorop dat zowel voor het aftappen van e-mailverkeer (op grond van een bevel krachtens artikel 126m Sv) als voor het vorderen van gegevens uit een e-mailbericht (op grond van artikel 126ng, tweede lid, Sv zoals opgenomen in het wetsvoorstel Bevoegdheden vorderen gegevens) een machtiging van de rechter-commissaris vereist is. In die zin is dus geen sprake van een onderscheid of van een verschil in procedure. Ook gelden dezelfde voorwaarden: in beide gevallen moet sprake zijn van een verdenking van een misdrijf als omschreven in artikel 67, eerste lid, Sv, dat gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert. Het enige verschil is dat de bevoegdheid om gegevens te *vorderen* beperkt is tot gegevens voorzover zij klaarblijkelijk van de verdachte afkomstig zijn, voor hem bestemd zijn, op hem betrekking hebben of tot het begaan van het strafbare feit hebben gediend of klaarblijkelijk met betrekking tot die gegevens het strafbare feit is gepleegd. Deze kwestie is aan de orde geweest bij het wetsvoorstel Bevoegdheden vorderen gegevens (Kamerstukken II, 2003–04, 29 441, nr. 3, blz. 14). In dat kader is ervoor gekozen om aan de gegevens betreffende de inhoud van een e-mail die is opgeslagen bij de internetaanbieder, dezelfde bescherming te bieden als aan de brief die is toevertrouwd aan de instelling van vervoer. Verwezen zij naar artikel 114 Sv.

6. Onderzoek van e-mail

De in deze paragraaf gestelde vragen over het onderzoek van e-mail zijn voor een belangrijk deel inmiddels achterhaald, doordat in het voorstel van wet Bevoegdheden vorderen gegevens, dat thans aanhangig is in de Eerste Kamer (Kamerstukken I 2004–2005, 29 441, A), specifieke regels worden gesteld over het onderzoek van e-mail. In de schriftelijke behandeling van dat wetsvoorstel door de Tweede Kamer is daarop ook ingegaan. In artikel 125la Sv, zoals voorgesteld in dat wetsvoorstel, wordt een regeling gegeven voor de doorzoeking ter vastlegging van gegevens bij aanbieders van openbare telecommunicatienetwerken of -diensten. Deze regeling betreft de gegevens in een e-mail die is opgeslagen bij een aanbieder en die niet voor de aanbieder bestemd is of van hem afkomstig is. Het gaat om de e-mails van de abonnees van de internetaanbieder. De regeling houdt in, zoals hiervoor al aan de orde kwam, dat van deze gegevens slechts kennis kan worden genomen voor zover de gegevens klaarblijkelijk van de verdachte afkomstig zijn, voor hem bestemd zijn of op hem betrekking hebben, of indien zij klaarblijkelijk tot het begaan van het

strafbare feit hebben gediend of klaarblijkelijk met betrekking tot die gegevens het strafbare feit is gepleegd. De term «klaarblijkelijk» betekent in dat verband dat alleen van die gegevens kan worden kennisgenomen waarvan van buitenaf, bijvoorbeeld aan de hand van de adressering of de herkomstgegevens van het bericht, eventueel mede gelet op andere uit het opsporingsonderzoek bekende gegevens, duidelijk is dat ze van de verdachte afkomstig zijn, voor hem bestemd zijn enz. De met opsporing belaste instantie kan bij de doorzoeking bij een internetaanbieder vooraf inzicht hebben in de gegevens die hij waarschijnlijk zal aantreffen. Ook is een extra waarborg nodig in de vorm van een voorafgaande machtiging van de rechter-commissaris. De in het bedoelde wetsvoorstel voorgestelde artikelen 126ng, tweede lid, en artikel 126ug, tweede lid, geven een regeling voor het vorderen van deze gegevens bij de aanbieder. In het in dat wetsvoorstel voorgestelde artikel 125m wordt bepaald dat van een vastlegging van gegevens aan de betrokkenen schriftelijk mededeling wordt gedaan, waarbij is aangesloten bij de notificatieplicht van artikel 126bb Sv.

Een aantal vragen dient niettemin nog beantwoord te worden omdat zij bij wetsvoorstel 29 441 niet aan de orde zijn gekomen en wel van belang zijn.

De leden van de PvdA vroegen in hoeverre e-mail in de toekomst kan worden onderscheiden van andere vormen van *content* die providers aangeboden krijgen ter verwerking. E-mail is een verzamelterm voor diensten waarbij elektronische berichten van een afzender naar een ontvanger worden getransporteerd. Deze diensten vallen naar de opvatting van de regering onder de bescherming van artikel 13 Grondwet, althans voorzover het berichtenverkeer aan de zorg van een provider is toevertrouwd. De opslag van e-mailberichten in de zogenaamde mailbox, waar de berichten aanwezig blijven totdat ze door de ontvanger worden geopend en door het e-mailprogramma naar diens computersysteem worden overgebracht, behoort tot deze transportfase. Providers vervoeren niet alleen e-mailberichten maar allerlei soorten berichten, bestanden, gegevens etc. die als vertrouwelijke communicatie moeten worden beschouwd. Het interactieve verkeer dat plaatsvindt tussen een internetgebruiker en een web-site komt evenzeer in aanmerking voor bescherming onder artikel 13 Grondwet als e-mailverkeer. Het verschil met e-mail is dat deze gegevensstromen niet tijdelijk ter aflevering in een e-mailbox worden opgeslagen maar direct aan de communicerende systemen worden doorgegeven. Naar mijn mening is er qua techniek wel, maar inhoudelijk geen verschil tussen e-mail en deze andere communicatievormen: beide behoren tot het domein van artikel 13 Grondwet. De Telecommunicatiewet heeft ter uitdrukking daarvan – en qua formulering vooruitlopend op de destijds aangekondigde wijziging van de Grondwet – in artikel 18.13 aangegeven dat de norm van artikel 13 Grondwet van toepassing is op de vormen van elektronische communicatie zoals bestreken door de Telecommunicatiewet. Zie ook artikel 11.2 Telecommunicatiewet ten aanzien van de verplichting tot beveiliging.

Deze leden vroegen aandacht voor het commentaar van de korpsbeheerders bij het oorspronkelijke wetsvoorstel Computercriminaliteit-II, dat er nogal wat zaken zouden stuklopen doordat zou moeten worden gewacht op de tussenkomst van de rechter-commissaris. Het voorbeeld waarop hier werd gedoeld betrof de medewerking van internet service providers bij het verstrekken van de zogenaamde NAW-gegevens (naam, adres en woonplaats). Dit probleem is inmiddels ondervangen door een wijziging van het Wetboek van Strafvordering (Vorderen gegevens telecommunicatie) die op 1 september 2004 in werking is getreden. Artikel 126na Sv bepaalt nu dat de opsporingsambtenaar in de daar bedoelde gevallen van de aanbieder van telecommunicatie identificerende gege-

vens kan vorderen, waarvoor derhalve niet meer de tussenkomst van de rechter-commissaris vereist is.

De leden van de fracties van VVD en SP vroegen zich af of de geadresseerde van een e-mailbericht achteraf kan zien of door een derde van de inhoud kennis is genomen. Dit hangt af van het desbetreffende e-mailprogramma. Zo zijn er programma's waarbij reeds gelezen e-mail kan worden aangemerkt als niet-gelezen, en programma's waarbij dat niet mogelijk is. In ieder geval is aan te bevelen een technische beveiliging zoals versleuteling toe te passen zodat onbevoegden van de inhoud geen kennis kunnen nemen.

De leden van de CDA-fractie vroegen waarom de regering bij de bescherming van e-mailberichten geen aansluiting heeft gezocht bij de artikelen 113 en 114 Sv. Voor de goede orde merk ik op dat artikel 113 Sv sinds 1 februari 2000 is vervallen bij de herziening van het gerechtelijk vooronderzoek (Stb. 1999, 243). Bij de strafvorderlijke regeling inzake e-mailberichten is in die zin bij artikel 114 Sv aangesloten, dat de tussenkomst van de rechter-commissaris vereist is en dezelfde beperkingen gelden; ik verwijs naar het hiervoor reeds gestelde.

De leden van de CDA-fractie vroegen om een reactie van de regering op het schrijven van het College van procureurs-generaal naar aanleiding van het wetsvoorstel, waarin erop gewezen werd dat het aftappen van gegevensverkeer niet gemakkelijk zal zijn, omdat berichten vaak in delen worden opgesplitst die langs verschillende wegen en technologische systemen naar het uiteindelijke doel worden geleid. Inmiddels zijn de ontwikkelingen zover gevorderd dat voldoende technische voorzieningen zijn ontwikkeld om hieraan het hoofd te bieden. Bovendien is voorzien in een kenniscentrum bij de Landelijke Interceptieorganisatie (het LIO), dat nieuwe aftapvoorzieningen faciliteert. De bevoegdheden die de met opsporing belaste organen ten dienste staan, met inbegrip van de bepalingen zoals opgenomen in het eerder gememoreerde wetsvoorstel Bevoegdheden vorderen gegevens (29 441), bieden voldoende aanknopingspunten voor een adequaat opsporingsonderzoek terzake.

Op het onderwerp dat door de leden van de CDA-fractie werd aangesneden over de vraag welke taak de internet service provider heeft indien e-mailberichten kennelijk onjuist zijn geadresseerd, ben ik reeds ingegaan aan het slot van paragraaf 2 hierboven, naar aanleiding van vragen van de leden van de fracties van (destijds) RPF en GPV.

De leden van de GL-fractie stelden een vraag over de betekenis van artikel 138a Sr binnen het netwerk van een bedrijf. De delen van een geautomatiseerd werk van de werkgever die door een werknemer worden gebruikt, worden op grond van artikel 138a Sr tegen de toegang door onbevoegde *derden* beschermd: verboden is immers het opzettelijk (en) wederrechtelijk binnendringen in het geautomatiseerde werk, veelal aangeduid als «hacken». De werkgever heeft in beginsel echter toegang tot zijn eigen geautomatiseerd werk. Wel kan de arbeidsverhouding – al dan niet geëxpliciteerd in de vorm van een reglement – met zich meebrengen dat beperkingen gelden bij de toegang van de werkgever tot (bepaalde) gegevens van de werknemer. Daarbij zal echter, gelet op het karakter van de betrokken rechtsverhouding, artikel 138a Sr niet snel toepassing vinden. Ik verwijs evenwel naar onderdeel 12 van de tweede nota van wijziging bij het wetsvoorstel (nr. 7), waarin de werking van het voorgestelde artikel 273d Sr wordt uitgebreid tot niet-openbare netwerken, inzake het opzettelijk en wederrechtelijk kennisnemen, overnemen, aftappen of opnemen van gegvens die niet voor de betrokkene bestemd zijn.

De vraag van de leden van de SP-fractie of de regering van mening is dat er richtlijnen of regelgeving zou moeten komen waarin het verplicht wordt gesteld om individuele computers in grote organisaties en netwerken beter te beveiligen, beantwoord ik ontkennend. Vanzelfsprekend is het van groot belang dat computers worden beveiligd, maar ik zie hierbij geen rol weggelegd voor de wetgever.

7. Opsporingsonderzoek op openbare computernetwerken

De in deze paragraaf aan de orde gestelde vragen hadden grotendeels betrekking op het onderzoek op openbare computernetwerken, maar enkele vragen betroffen het onderzoek naar besloten netwerken. Deze laatste vragen beantwoord ik eerst, waarna ik nader inga op het onderzoek op openbare netwerken.

De leden van de PvdA-fractie hebben gevraagd, of de Nederlandse rechtsmacht zich uitstrekt tot het onderzoek van computernetwerken van (mede) in Nederland gevestigde internationale organisaties of bedrijven. Als bij het onderzoek- dat bijvoorbeeld is aangevangen op de voet van artikel 96c Sv- blijkt dat de doorzochte computer in verbinding staat met andere computers binnen Nederland, mag slechts op grond van artikel 125j Sv in die andere computers worden gezocht. Een dergelijke netwerkzoeking mag slechts gericht zijn op gegevens die redelijkerwijs nodig zijn om de waarheid aan het licht te brengen. De oorspronkelijke personen die op de plaats van doorzoeking wonen, werken of verblijven, moeten overigens wel gemachtigd zijn om toegang te hebben tot die andere computers. Als een van de computers uit het te onderzoeken netwerk in het buitenland blijkt te staan (de formele plaats van vestiging van het bedrijf is daarbij derhalve minder relevant), is voorzichtigheid geboden. Een onderzoek in die computer betekent immers het verrichten van opsporingshandelingen buiten de landsgrenzen. Dit soort optreden is verdragsrechtelijk geregeld. In beginsel dient men in een rechtshulpverzoek aan het desbetreffende land om de gegevens te vragen. Men kan echter niet altijd van tevoren weten of een netwerkzoeking leidt tot een zoeking in een computer in het buitenland. In dat geval zijn de gegevens te gebruiken voor het onderzoek. Als men dit echter wel weet, ontdekt of zou behoren te weten, is internationale rechtshulp noodzakelijk.
Het voorgaande moet op twee punten worden genuanceerd. Ten eerste is binnen de Europese Unie voorzien in een specifieke regeling voor een bepaalde vorm van onderzoek, namelijk het onderzoek van telecommunicatie, en wel door middel van de op 29 mei 2000 te Brussel tot stand gekomen Overeenkomst betreffende de wederzijdse rechtshulp in strafzaken tussen de Lid-Staten van de Europese Unie. Deze is in de Nederlandse wetgeving geïmplementeerd door middel van de Uitvoeringswet EU-rechtshulpverdrag (Stb. 2004, 107). De daarop betrekking hebbende bepalingen worden door middel van de tweede nota van wijziging bij het onderhavige wetsvoorstel geplaatst in het nieuwe artikel 126ma Sv. Ten tweede – dit in antwoord op de desbetreffende vraag van de leden van de PvdA-fractie – voorziet het Cybercrime Verdrag in belangrijke mate in aanvullende bepalingen die hier van belang zijn. De artikelen 31 tot en met 34 van het Verdrag voorzien namelijk in een laagdrempelige vorm van rechtshulp. Zodra het Cybercrime Verdrag voor Nederland in werking treedt, betekent dat een aanzienlijke vereenvoudiging in de samenwerking bij het onderzoek in computerbestanden voor zover het de samenwerking betreft met andere Staten waarvoor het Verdrag in werking is getreden.

De leden van de PvdA-fractie hebben gevraagd of buitenlandse opsporingsambtenaren onderzoek mogen doen in Nederlandse computernetwerken. Hier geldt hetzelfde als wat geldt voor Nederlandse opsporingsambtenaren die onderzoek willen doen in «buitenlandse»

computernetwerken: voor zover sprake is van openbare bronnen is daartegen geen bezwaar, maar in andere gevallen moet in beginsel de weg van een rechtshulpverzoek worden bewandeld. Het Cybercrime Verdrag biedt daarvoor naast andere rechtshulpverdragen de grondslag.

Deze leden hebben ook gevraagd, hoe het onderzoek naar een strafbare inhoud op een *stand-alone* computer moet worden gezien en of het – om opsporing te voorkomen of te verhinderen – slechts noodzakelijk is dat dit apparaat de grens met België of Duitsland wordt overgebracht. Een *stand-alone* computer kan doorgaans zonder veel bezwaar in beslag worden genomen met het oog op onderzoek, maar ook is denkbaar dat – op basis van artikel 125i zoals dat komt te luiden na inwerkingtreding van het wetsvoorstel Bevoegdheden vorderen gegevens – de bevoegde autoriteit de computer ter plaatse doorzoekt en van (delen van) de inhoud bijvoorbeeld een copie maakt. Zodra het apparaat de grens over is, wil dat niet zeggen dat geen opsporing meer kan plaatsvinden maar moet daarvoor wel de (rechts)hulp van de betrokken Staat worden ingeroepen.

De leden van de VVD-fractie vroegen naar aanleiding van de passage in de memorie van toelichting over opsporingsonderzoek op openbare computernetwerken, of er een duidelijke grens is te trekken tussen bevoegdheden die opsporingsambtenaren altijd mogen uitoefenen en bevoegdheden die zij slechts uit hoofde van een specifieke grondslag mogen uitoefenen. In de memorie van toelichting (nr. 3, blz. 36) was vermeld dat zo'n aparte specifieke juridische grondslag nodig is wanneer het onderzoek een stelselmatig karakter krijgt. De bedoelde leden vroegen in dat verband wanneer daarvan sprake is.
Het begrip «stelselmatig» speelt een rol bij twee bijzondere opsporingsbevoegdheden, te weten de stelselmatige observatie (artikelen 126g en 126o Sv) en de stelselmatige inwinning van informatie (artikelen 126j en 126qa Sv). De observatie of de inwinning van informatie kan naar algemeen inzicht worden aangemerkt als stelselmatig indien deze systematisch en gericht plaatsvindt met als te verwachten resultaat dat daardoor een min of meer volledig beeld kan worden verkregen van bepaalde aspecten van iemands leven. Het criterium van de stelselmatigheid is echter een bijkomend criterium bij het karakter van de desbetreffende bevoegdheid. Alleen het stelselmatig volgen van een persoon of het stelselmatig waarnemen van diens aanwezigheid of gedrag vergt een specifieke wettelijke grondslag. Evenals het stelselmatig inwinnen van informatie over de verdachte zonder dat kenbaar is dat de opsporingsambtenaar als zodanig optreedt. Stelselmatig onderzoek in het algemeen vergt geen specifieke wettelijke grondslag; die is slechts vereist bij de toepassing van een opsporingsmethode die als zodanig een inbreuk op de persoonlijke levenssfeer kan opleveren. Zodra een onderzoek op een computernetwerk de vorm aanneemt van het stelselmatig inwinnen van informatie over een verdachte, bijvoorbeeld in een webforum op Internet waaraan ook de verdachte deelneemt, zonder dat de deelnemers aan dat webforum weten dat zich onder hen een opsporingsambtenaar bevindt, mag dat onderzoek dus slechts voortgezet worden met een bevel van de officier van justitie op de voet van artikel 126j Sv. Iets dergelijks geldt voor de situatie waarin het onderzoek de vorm aanneemt van het stelselmatig waarnemen van het gedrag van een verdachte: dan is een bevel inzake stelselmatige observatie nodig op de voet van artikel 126g Sv.
Daarnaast zijn er bijzondere opsporingsbevoegdheden waarbij het begrip stelselmatig geen rol speelt. Zo is een bevel van de officier van justitie op de voet van artikel 126h vereist indien het onderzoek de vorm aanneemt van infiltratie.

De leden van de VVD-fractie vroegen, of het toelaatbaar zou zijn dat voor opsporingsdoeleingen gebruik wordt gemaakt van autonome, geautoma-

tiseerde programma's zoals «*bots*». Dit zijn programma's die – meestal op onrechtmatige wijze – toegang proberen te verkrijgen tot computersystemen, teneinde daarop programma's te installeren waarmee bijvoorbeeld het gedrag van de computergebruiker wordt geregistreerd of waarmee de computer gemanipuleerd wordt. Het gebruik van dergelijke programma's is daarmee strafbaar, zodat alleen al daarom grote terughoudendheid geboden is bij het gebruik ter opsporing. Ik wijs evenwel op artikel 126l Sv betreffende het opnemen van vertrouwelijke communicatie met een technisch hulpmiddel. Ten behoeve daarvan kan de officier van justitie – na machtiging door de rechter-commissaris – bepalen dat een besloten plaats wordt betreden. Daarbij gelden dan wel twee eisen: het technisch hulpmiddel moet voldoen aan de eisen die – krachtens artikel 126ee Sv – gesteld worden; en voor de inzet is de machtiging van de rechter-commissaris vereist. Denkbaar is dat op enig moment voor opsporingsdoeleinden een programma wordt ontwikkeld dat kenmerken vertoont van een «*bot*» doch in functie beperkt is tot het opnemen van communicatie en daarnaast aan zodanige eisen voldoet dat het in bijzondere omstandigheden voor opsporingsdoeleinden gebruikt mag worden. Mét de leden van de VVD-fractie is de regering van mening dat politie en justitie moeten kunnen beschikken over adequate bevoegdheden voor onderzoek op bijvoorbeeld het internet, maar ik teken daarbij wel aan dat conform het stelsel van het Wetboek van Strafvordering voorzien moet worden in een adequate afweging van de aan de orde zijnde belangen. Juist daarom is het van belang dat zowel bij de ontwikkeling van dergelijke opsporingshulpmiddelen als bij de toepassing daarvan wordt voorzien in adequate toetsingsmomenten.

De leden van de VVD-fractie hebben erop gewezen dat in het wetsvoorstel bijzondere opsporingsbevoegdheden worden gecreëerd die kunnen worden gehanteerd ten aanzien van openbare netwerken en diensten en hebben de vraag gesteld of er geen reden is die bevoegdheden ook te kunnen toepassen op besloten netwerken. Dit laatste is inderdaad het geval. In de tweede nota van wijziging is met name de bevoegdheid zoals oorspronkelijk in concept-artikel 126m opgenomen aanmerkelijk uitgebreid, juist ook naar besloten netwerken. Ik moge naar de desbetreffende nota van wijziging, met inbegrip van de daarop gegeven toelichting, verwijzen.

De leden van de VVD-fractie vroegen, of opsporingsambtenaren net als gewone burgers gegevens mogen downloaden van buitenlandse sites. Ervan uitgaande dat dat handelen, met inachtneming van artikel 2 Politiewet en artikel 141 Sv, nodig is voor een goede uitvoering van de politie- of opsporingstaak, mogen opsporingsambtenaren inderdaad alles wat via open bronnen toegankelijk is bekijken en downloaden. Dit onderwerp wordt ook geregeld in artikel 32 van het Cybercrime Verdrag, waarin is aangegeven in welke gevallen dergelijk als «grensoverschrijdende zelfhulp» aan te merken handelen is toegestaan. Onderdeel a van artikel 32 betreft het geval waarin bepaalde elektronische informatie door middel van een computersysteem dat zich op het grondgebied van een andere staat bevindt, aan het publiek wordt aangeboden – bijvoorbeeld gegevens op een bepaalde website. In dat geval zijn de opsporingsautoriteiten van andere staten bevoegd om zich toegang tot die gegevens te verschaffen en een kopie daarvan te downloaden zonder dat daarvoor toestemming behoefte te worden gekregen. Onderdeel b van artikel 32 van het Verdrag komt erop neer dat ook geen toestemming van de andere staat nodig is indien computergegevens naar het territoir van een andere verdragspartij worden overgehaald met toestemming van de persoon die met betrekking tot die gegevens handelingsbevoegd is. De plaats waar deze persoon zich bevindt is hierbij irrelevant; hij kan zich op het grondgebied van een van beide verdragspartijen bevinden of zelfs in een derde staat, zolang hij

maar bevoegd is tot verstrekking. Deze bevoegdheid kan hij ontlenen aan de wet, aan een overeenkomst of aan zijn relatie met de gegevens. In andere situaties zal een rechtshulpverzoek uitkomst moeten bieden. Ik verwijs ook naar het hiervoor in paragraaf 3 gestelde over de toepassing van specifieke strafvorderlijke bevoegdheden en grenzen die het volkenrecht daaraan stelt.

De vraag van de leden van de VVD-fractie of het adres in het netwerk voldoende aanwijzing vormt over de locatie van de gegevens, moet ontkennend beantwoord worden. Domeinen met een .nl-aanduiding kunnen in het buitenland worden gehost en omgekeerd kunnen domeinen met een .com-aanduiding in Nederland worden gehost. Het land van registratie van het domein en het land waarin de site wordt gehost, hoeven kortom niet hetzelfde te zijn.

De leden van de VVD-fractie stelden enkele vragen over rechtsmacht. Als abusievelijk een opsporingsbevoegdheid is toegepast op een zich in het buitenland bevindendende computer, en de daarmee verkregen gegevens bijvoorbeeld van belang zijn voor het bewijs, zal in beginsel alsnog door middel van een rechtshulpverzoek erin moeten worden voorzien dat de gegevens als bewijs in de strafzaak mogen worden gebruikt. In de praktijk worden dergelijke gebreken ook wel hersteld, bijvoorbeeld door notificatie achteraf. Het Cybercrime Verdrag biedt aanknopingspunten voor een laagdrempelige voorziening terzake.

De leden van de fracties van VVD, D66, GroenLinks en (destijds) RPF en GPV hebben, naar aanleiding van de voorgestelde regeling van pseudokoop van gegevens, gevraagd waarom in het wetsvoorstel niet ook een regeling voor de zogenaamde *burgerpseudokoop* van gegevens is opgenomen. Indertijd is hiervoor gekozen omdat ervan werd uitgegaan dat de tussenkomst van een netwerk met zich meebracht dat het altijd mogelijk was om de politie zelf de pseudokoop te laten uitvoeren, zodat de burgerpseudokoop van gegevens niet nodig zou zijn. Op Internet is het immers betrekkelijk eenvoudig om de identiteit van een ander aan te nemen, dat wil zeggen met naam, (IP)-adres, bijnaam, e-mailadres e.d. Dit ligt echter lastiger indien er bijvoorbeeld visueel contact wordt gelegd, bijvoorbeeld met gebruikmaking van een webcam. Voor dergelijke gevallen kan in bijzondere situaties behoefte bestaan aan de inzet van burgerpseudokoop. Bij nota van wijziging zal het wetsvoorstel op dit punt worden uitgebreid.

De destijds nog door de fracties van VVD en D66 gestelde vraag of pseudokoop dient te worden opgevat als een vorm van infiltratie is inmiddels ontkennend beantwoord. Zoals bekend heeft de wetgever ervoor gekozen de pseudokoop apart te regelen naast de infiltratie, wat niet wegneemt dat er tussen beide bevoegdheden belangrijke overeenkomsten zijn aan te wijzen. Een bevel tot infiltratie kán onder omstandigheden overigens ook mede de bevoegdheid tot pseudokoop omvatten, mits uitdrukkelijk bepaald. Anders dan pseudokoop houdt infiltratie echter in dat wordt deelgenomen aan een groep van personen waarbinnen misdrijven worden beraamd of gepleegd.

De leden van de fracties van (destijds) RPF en GPV vroegen nog, waarom wel een wijziging van het Wetboek van Strafvordering nodig is voor de pseudokoop van gegevens en niet voor infiltratie. De reden daarvoor is dat de regeling van infiltratie ook in zijn huidige bewoordingen toegepast kan worden in een digitale omgeving (het deelnemen of medewerking verlenen aan een groep van personen waarbinnen naar redelijkerwijs kan worden vermoed misdrijven worden beraamd of gepleegd), terwijl dat

met de regeling van pseudokoop niet het geval is (het afnemen van goederen en het verlenen van diensten omvat niet de afname van gegevens).

Naar aanleiding van de vraag van o.a. de D66-fractie in verband met de beperkte reikwijdte van de Nederlandse rechtsmacht, of er al verdragen zijn die daaraan tegemoet beogen te komen, volsta ik ermee te verwijzen naar het Cybercrime Verdrag en het voorstel voor een goedkeuringswet terzake, en naar de tweede nota van wijziging van het onderhavige wetsvoorstel.

De leden van de VVD-fractie hebben gevraagd of het niet wenselijk is om ook *interne* systemen met betrekking tot stromende gegevens aftapbaar of monitorbaar te maken, en daartoe in artikel 125g Sv de toevoeging van de woorden «die wordt aangewend voor dienstverlening aan het publiek» te laten vervallen. Door middel van de tweede nota van wijziging is aan deze wens tegemoet gekomen door een aanzienlijke wijziging van (niet artikel 125g maar het daarvoor in de plaats getreden) artikel 126m Sv. Ik volsta met een verwijzing naar die nota van toelichting.

Deze leden vroegen ook naar de toegevoegde waarde die de term «heimelijk» in artikel 139b, tweede lid, Sr heeft naast de termen «opzettelijk en wederrechtelijk». De toegevoegde waarde van dit element zit daarin, dat het omschreven handelen alleen dan strafbaar is, indien het op een heimelijke manier plaatsvindt. Dit element van «heimelijkheid» is niet gesteld in artikel 139a, waar het gaat om het opnemen en aftappen in een woning. De wetgever heeft geoordeeld dat wederrechtelijk aftappen van gesprekken in een woning altijd strafbaar moet zijn en dat voor het aftappen van gesprekken in de openbare ruimte geen strafbaarheid bestaat als voor de «afgetapte» zichtbaar of op andere wijze kenbaar is dat het gesprek wordt afgetapt. Daarom is er wel degelijk een toegevoegde waarde van het element «heimelijk» naast de eis van opzet en wederrechtelijkheid. Ik wijs er overigens op dat in de tweede nota van wijziging de opbouw van de artikelen 139a tot en met 139d Sr is gewijzigd zodat deze beter inzichtelijk is. Het verschil tussen aftappen in een woning en in de openbare ruimte is evenwel gehandhaafd omdat dat nog steeds relevant is.

De leden van de SGP-fractie hadden in deze paragraaf nog een vraag gesteld over de ontoegankelijkmaking van gegevens (artikel 125o Sv). Zoals hiervoor in paragraaf 3 is uiteengezet, in aansluiting op de memorie van toelichting, gelden bij de ontoegankelijkmaking altijd de eisen van subsidiariteit en proportionaliteit maar zal ook steeds de effectiviteit van de maatregel in het oog gehouden moeten worden. De keuze van het moment waarop wordt overgegaan tot ontoegankelijkmaking hangt af van de specifieke omstandigheden van het geval. Wat betreft de vragen van deze leden over ondersteuning en opleiding van de opsporingsambtenaren, verwijs ik naar paragraaf 9 hierna. De vraag van deze leden over de in het wetsvoorstel voorgestelde wijziging van 125i Sv behoeft geen beantwoording meer, aangezien deze wijziging met de tweede nota van wijziging is vervallen. De wijziging van artikel 125i Sv heeft zijn beslag gekregen in het wetsvoorstel Bevoegdheden vorderen gegevens.

8. Overige wijzigingen

De strafrechtelijke aanpak van ernstige vormen van *spam*, in het bijzonder *e-mailbombing*, kan tot mijn vreugde op steun van de aan het woord zijnde leden rekenen. Van belang acht ik dat niet zonder meer iedere vorm van *spam* via het strafrecht wordt aangepakt maar wel de ernstiger vormen daarvan. Door middel van de tweede nota van wijziging is het

nieuw voorgestelde artikel 138b aangepast aan de eisen van het Cybercrime Verdrag, waardoor een verruiming wordt aangebracht in de gevallen die onder de strafbepaling komen te vallen.

De leden van de VVD-fractie vroegen of *e-bombing* – waarvoor een strafbedreiging van maximaal een jaar gevangenisstraf werd geïntroduceerd – een ernstiger feit is dan computervredebreuk (artikel 138a Sr), waarop – in de eenvoudige vorm daarvan – een strafbedreiging staat van maximaal zes maanden. Computervredebreuk kan in bepaalde gevallen ook ernstig zijn. In de tweede nota van wijziging heb ik daarom, naar aanleiding van een heroverweging van de strafmaxima, ervoor gekozen de maximumstraf voor computervredebreuk ook te verhogen tot een jaar. Indien zich strafverzwarende omstandigheden voordoen, is het maximum overigens aanmerkelijk hoger. Ik moge verwijzen naar de tweede nota van wijziging.

De leden van de fracties van VVD en SGP stelden ook een vraag over het feit dat strafvorderlijke bevoegdheden niet mogen worden toegepast bij computergerelateerde misdrijven waarvoor een lagere maximumstraf dan vier jaar is vastgesteld. Met deze leden ben ik van mening dat juist bij computergerelateerde misdrijven de nodige strafvorderlijke bevoegdheden toegepast moeten kunnen worden, in het bijzonder degene die juist kunnen bijdragen aan de opsporing van dergelijke strafbare feiten. Dit wordt bovendien voorgeschreven in het Cybercrime Verdrag. Daarom is bij de tweede nota van wijziging bij het onderhavige wetsvoorstel een wijziging aangebracht, inhoudende dat de typische computermisdrijven worden toegevoegd aan de lijst van artikel 67 Sv, waardoor de strafvorderlijke bevoegdheden mogen worden toegepast die slechts mogelijk zijn bij de verdenking van strafbare feiten als omschreven in artikel 67 Sv, onafhankelijk van de daarop ten hoogste gestelde straf.

De leden van de fracties van VVD, D66 en SGP hebben vragen gesteld over *spam*. In het nieuwe artikel 138b Sr, zoals gewijzigd door de tweede nota van wijziging, wordt strafbaar degene die opzettelijk en wederrechtelijk de toegang tot of het gebruik van een geautomatiseerd werk belemmert door daaraan gegevens aan te bieden of toe te zenden. Ernstige vormen van *spam worden daardoor strafbaar, namelijk die spam* waarmee wordt beoogd de toegang tot of het gebruik van een computer te belemmeren. Dit betekent een belangrijke verruiming van de werking van het strafrecht bij de bestrijding van *spam*. Andere, eenvoudiger en minder schadelijke vormen van *spam*, worden aangepakt langs privaatrechtelijke c.q. bestuursrechtelijke weg. Ik moge daartoe verwijzen naar de discussies die met Uw Kamer hebben plaatsgevonden in het kader van het wetsvoorstel Aanpassingswet richtlijn inzake elektronische handel (kamerstukken 28 197) en – door mijn ambtgenoot van Economische Zaken – in het kader van de wijziging van de Telecommunicatiewet inzake de implementatie van een van een nieuw Europees geharmoniseerd regelgevingskader voor elektronische communicatienetwerken en -diensten (het zgn. ONP-wetsvoorstel, kamerstukken 28 815).

Voor een beantwoording van de vragen over de inzet en expertise van politie en justitie verwijs ik naar paragraaf 9 hierna.

Van een leemte tussen de Wet bescherming persoonsgegevens en het Wetboek van Strafvordering op het punt van ongewenste e-mail, waarnaar door de leden van de VVD-fractie werd gevraagd, is mij niets bekend.

De leden van de GL-fractie vroegen een verheldering van het element «bestemd om diens toegang tot dat netwerk of die dienst te belemmeren» dat voorkwam in het voorgestelde artikel 138b Sr. Door middel van de tweede nota van wijziging is dat artikel zodanig gewijzigd dat het

bedoelde element daarin niet meer voorkomt. Op grond van de nieuwe formulering is vereist dat de toegang of het gebruik van het geautomatiseerd daadwerkelijk wordt belemmerd.

9. Handhaving

De leden van de fracties van CDA en D66 hebben – naar aanleiding van het advies van het College van procureurs-generaal – gevraagd of de regering ook heeft overwogen om in het buitenland gepleegde strafbare feiten door uitbreiding van artikel 4 Sr onder het bereik van de Nederlandse rechtsmacht te brengen. Het antwoord luidt ontkennend. Afgezien van enkele specifieke zeer ernstige delicten zoals de aanslag op het staatshoofd, wordt rechtsmacht overeenkomstig het universaliteitsbeginsel doorgaans slechts gevestigd ter uitvoering van verdragen die daartoe specifiek verplichten. Het inmiddels tot stand gekomen Cybercrime Verdrag noopt niet tot de vestiging van een dergelijke rechtsmacht, maar slechts tot de vestiging van rechtsmacht zoals deze ten onzent is geregeld in de artikelen 2, 3 en 5 Sr. Daarnaast is een zeer specifieke uitbreiding (niet van artikel 4 Sr maar) van artikel 5 Sr nodig. Daarin wordt voorzien in de tweede nota van wijziging bij het onderhavige wetsvoorstel. Voor het overige voorziet het Cybercrime Verdrag in de nodige instrumenten van onderlinge rechtshulp.

Leden van diverse fracties hebben, zowel in paragraaf 9 als verspreid over andere paragrafen van het verslag, vele vragen gesteld over de kennis van zaken op het gebied van computercriminaliteit bij degenen die belast zijn met de handhaving, over de samenwerking, de capaciteit en inzetbaarheid van de betrokken organen, de toerusting van opsporingsambtenaren op het gebied van cybercrime, over de interregionale bureaus digitale expertise en dergelijke. Ik hecht eraan deze vragen in samenhang te beantwoorden en daarbij een overzicht te geven van de stand van zaken tot nu toe op het gebied van de toerusting en opleiding van betrokkenen. Dat dit onderwerp sterk in de aandacht staat, wordt overigens ook weerspiegeld in de kamervragen die de afgelopen tijd over computercriminaliteit in brede zin zijn gesteld (zie Aanhangsel Handelingen 2003/04, nrs. 1783 en 2099; idem 2004/05, nrs. 227, 383, 553, 554, 645 en 1332).

De politie is sinds ongeveer acht jaar actief en structureel bezig met de invulling en vormgeving van digitaal opsporen. In 1996 werd de visienota «Op weg naar... digitaal rechercheren» aangeboden aan de Raad van Hoofdcommissarissen. Nadat binnen verschillende korpsen op zichzelf staande initiatieven op het terrein van digitaal opsporen waren ontplooid, zijn op interregionaal niveau samenwerkingsverbanden gesmeed. De ontwikkeling van digitaal rechercheren heeft zo in het recente verleden op interregionaal niveau een aanvang genomen met het opzetten van vijf ressortelijk ingedeelde Bureaus Computercriminaliteit (BCC). Alle operationele zaken met betrekking tot de bestrijding van digitale criminaliteit werden in die bureaus belegd. Alle kennis op dat terrein werd eveneens in die bureaus geconcentreerd.
In een later stadium zijn de korpsen overgegaan tot het inrichten van eigen Bureaus Digitaal Rechercheren (BDR). Op dit moment heeft nagenoeg ieder korps een BDR. Met de komst van de BDR's veranderde de positie van de BCC's. De operationele taken gingen naar de BDR's, terwijl de BCC's daaraan ondersteunend werden. Deze verschuiving werd in de naamsverandering van de BCC's geëxpliciteerd: zij werden vanaf dat moment Bureau Digitale Expertise (BDE). BDR's moesten beschikken over digitale expertise op MBO-niveau, BDE's op HBO-niveau. In feite werd hiermee een escalatiemodel gecreëerd, waarbij de meer complexe zaken op het interregionale niveau terechtkwamen en de eenvoudiger zaken bij de regiokorpsen bleven.

Na verloop van tijd is de Groep Digitaal Rechercheren (inmiddels het TDE, Team Digitale Expertise, ook wel aangeduid als de «Cybercops») opgezet als onderdeel van het KLPD. Het TDE fungeert vergelijkbaar met een BDE: er is sprake van bundeling van technische kennis die wordt aangeboden voor het uitvoeren van tactisch onderzoek. Het beroep dat vanuit de regionale korpsen wordt gedaan op het TDE, is beperkt. Het TDE voert zelfstandig operationeel onderzoek uit. Naar schatting 5% van de capaciteit van het TDE wordt aangewend voor ondersteuning van de regiokorpsen.

Op dit moment zijn er in dienst van de Nederlandse politie ongeveer 115 mensen werkzaam in de digitale recherche, inclusief 28 medewerkers in dienst van het KLPD. Zij zijn nagenoeg allemaal als technische onderzoekers werkzaam en ondergebracht in een ondersteunende functie. Voor het overgrote deel (84%) zijn deze mensen intern geworven en hebben zij een executieve achtergrond. Het kennisniveau bevindt zich op MBOen HBO-niveau.

Digitaal opsporen heeft tot op heden vooral in het teken gestaan van techniek; heel nadrukkelijk is hierop gefocust. Dat heeft tot gevolg gehad dat de aandacht vooral is uitgegaan naar de technisch ondersteunende zijde van digitaal opsporen. Een aantal van 115 technisch specialisten ter ondersteuning van het tactische opsporingswerk is heel behoorlijk, gelet ook op het niveau van de ondersteuning. De tactische kant van digitaal opsporen is echter in de afgelopen jaren verwaarloosd. Tactische opsporingsambtenaren zijn in het algemeen onvoldoende onderlegd in ICT, enerzijds om er gebruik van te maken in hun eigen voordeel en anderzijds om strafbare feiten waarin ICT een wezenlijke component vormt op te merken en adequaat strafrechtelijk af te handelen. Geconcludeerd kan dan ook worden dat de huidige wijze van werken nodig en vruchtbaar is gebleken, maar ook risico's en tekortkomingen kent.
Deze risico's zijn inmiddels door de Raad van Hoofdcommissarissen onderkend. De Raad is een Landelijk Project Digitaal Opsporen gestart dat verbetering in de situatie van het digitaal opsporen moet brengen. Uitgangspunt daarbij is een onderscheid tussen tactisch uitvoerend en technisch ondersteunend opsporingswerk. Het uitvoeren van werkzaamheden op het gebied van digitaal rechercheren dient in de visie van de Raad generiek te zijn: iedere opsporingsambtenaar (recherche of anderszins) moet worden toegerust om zijn of haar werk te kunnen doen, gegeven de digitalisering van de samenleving. Dat betekent een verbreding van de competenties van alle opsporingsambtenaren. Daarnaast is naar de mening van de Raad op het gebied van de technische ondersteuning een professionaliseringsslag nodig.

Bovenstaande visie heeft tot gevolg dat een aantal maatregelen zal moeten worden genomen, waarvan de belangrijkste zijn: het heroverwegen van het opleidingsaanbod en het heroverwegen van de gehanteerde structuur waarbinnen deskundigheid is georganiseerd. Er is voorzien in een opleidingstraject van alle zittende rechercheurs. Dit zal worden gerealiseerd in een periode van 4 jaar: van 2005 tot en met 2008. Tegelijkertijd zal de organisatie van de digitale recherche worden gewijzigd. De technische kennis wordt verdiept en samengevoegd met de forensisch technische expertise binnen de politie. De tactische kennis wordt door middel van de eerdergenoemde opleidingen verbreed en ingebed in de bestaande tactische opsporingsteams op regionaal, bovenregionaal en landelijk niveau.

Ook voor het Openbaar Ministerie is een opleiding op het terrein van het digitaal opsporen ontwikkeld. Hieraan wordt door alle parketten deelgenomen. Deze cursussen worden georganiseerd door de Stichting Studie-

centrum Rechtspleging in samenwerking met de OM-werkgroep computercriminaliteit.
Het is niet zo, dat strafzaken door gebrek aan kennis (zijn) blijven liggen. Met name op het terrein van de bestrijding van kinderpornografie zijn de afgelopen jaren enkele ernstige zaken opgespoord en vervolgd. Ook op andere terreinen zijn successen te melden. Ik noem bijvoorbeeld de veroordeling van de maker en verspreider van het Kournikova virus, de afpersingszaak bij Campina, en – recent – de aanhoudingen c.q. veroordelingen van de hackers van enkele overheidswebsites en van de e-mail postbus van een lid van het openbaar ministerie.

Al met al meen ik dat op het gebied van de handhaving adequate maatregelen zijn genomen om computercriminaliteit met de nodige voortvarendheid en deskundigheid aan te pakken. Tegelijkertijd is duidelijk dat de ontwikkelingen op dit gebied zo snel gaan, dat continu investeringen nodig zullen blijven zowel met het oog op het op peil houden van de noodzakelijke kennis als met het oog op de ontwikkeling van de benodigde instrumenten om deze vorm van criminaliteit te bestrijden en – waar mogelijk – te voorkomen.

De in deze paragraaf nog gestelde vragen over versleuteling zijn beantwoord in paragraaf 4, die daarover specifiek handelt.

ARTIKELSGEWIJS DEEL

Artikel I

C

De leden van de D66-fractie vroegen, te verduidelijken wat onder een geautomatiseerd werk dient te worden verstaan. Artikel 80sexies Sr, zoals dit wordt aangevuld door het onderhavige wetsvoorstel, definieert geautomatiseerd werk als een inrichting die bestemd is om langs elektronische weg gegevens op te slaan, te verwerken en over te dragen. Met dit begrip worden op zichzelf staande computers aangeduid, maar ook netwerken van computers en geautomatiseerde inrichtingen voor telecommunicatie. Van belang is wel dat de «inrichting» zowel gegevens kan opslaan als deze verwerken én overdragen.

K

De leden van de SGP-fractie stelden de vraag of de zinsnede «voor het publiek beschikbare» in het nieuw geformuleerde artikel 232, tweede lid, Sr geen heroverweging verdient. Ik meen dat zulks niet het geval is, omdat artikel 232 strekt tot bescherming van het maatschappelijk vertrouwen in betaalpassen en dergelijke en dit maatschappelijk vertrouwen niet in dezelfde mate in het geding is bij kaarten die louter in besloten kring worden gebruikt. In de door de vragenstellers naar voren gebrachte casus, waarin een toegangspas voor werknemers tevens betaalmogelijkheden in zich bergt, dient het vooral de zorg van de werkgever te zijn dat geen vervalsingen tot stand worden gebracht, bijvoorbeeld door ervoor te zorgen dat slechts een beperkt bedrag op de toegangspas gecrediteerd kan worden waardoor vervalsing niet snel zal lonen. Daarbij acht ik in beginsel geen taak voor de overheid weggelegd. Aan de andere kant moet het aan de rechtsontwikkeling worden overgelaten om te bepalen in welk geval wél sprake is van een kaart die «voor het publiek beschikbaar» is.

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