Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2004–2005

30 036 (R 1784) Goedkeuring van het op 23 november 2001 te Boedapest totstandgekomen Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken (Trb. 2002, 18)

Nr. 7

NOTA NAAR AANLEIDING VAN HET VERSLAG

Ontvangen 15 juni 2005

Inleiding

Met genoegen hebben de Minister van Buitenlandse Zaken en ik vastgesteld dat de leden van de in het verslag aan het woord zijnde fracties met belangstelling kennis hebben genomen van het wetsvoorstel houdende goedkeuring van het Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, hierna verder aan te duiden als het Cybercrime Verdrag. In deze nota ga ik mede namens mijn ambtgenoot van Buitenlandse Zaken graag in op de in het verslag gestelde vragen en de daarin gemaakte opmerkingen. Daarbij houd ik de volgorde van het verslag aan.

Mét de leden van de CDA-fractie ben ik van mening dat internationale criminaliteit ook een internationale aanpak vergt. De leden van de PvdA-fractie merkten terecht op dat het Cybercrime Verdrag een bijdrage kan leveren aan de bestrijding van criminaliteit via internet. Zoals de leden van de fractie van de ChristenUnie opmerkten, zal het Cybercrime Verdrag inderdaad een bijdrage kunnen leveren aan het uitgangspunt dat in de virtuele wereld strafbaar moet zijn wat ook in de normale wereld strafbaar is.

Algemeen

De leden van de CDA-fractie merkten op dat het Verdrag door 28 lidstaten van de Raad van Europa is ondertekend alsmede door Canada, Japan, de Verenigde Staten en Zuid-Afrika, maar ik kan mededelen – ook in antwoord op de desbetreffende vraag van de leden van de SP-fractie – dat het Cybercrime Verdrag inmiddels door 42 landen is ondertekend, namelijk door 38 lidstaten van de Raad van Europa en door de vier genoemde landen van buiten de Raad van Europa. Deze toename acht ik verheugend. Het Verdrag voorziet inderdaad in de mogelijkheid dat ook andere landen van buiten de Raad van Europa partij worden bij het Verdrag, hoewel van die mogelijkheid tot nu toe nog geen gebruik is gemaakt. Eind april van dit jaar is bij het Elfde Congres van de Verenigde Naties inzake misdaadpreventie en strafrechtspraak de vraag aan de orde geweest of het niet wenselijk zou zijn om in het kader van de Verenigde Naties een Verdrag

KST87804
0405tkkst30036R1784–7
ISSN 0921 - 7371
Sdu Uitgevers
's-Gravenhage 2005

over het tegengaan van computercriminaliteit op te stellen, maar die vraag is – mede op Nederlands initiatief – ontkennend beantwoord aangezien nog pas zeer recent het Cybercrime Verdrag tot stand is gekomen, dat weliswaar is opgesteld in het kader van de Raad van Europa maar niettemin openstaat voor álle landen die zich met de inhoud kunnen verenigen. In de slotverklaring van het bedoelde congres (de Bangkok Verklaring van 25 april 2005, document A/CONF.203/L.5) werd dan ook opgeroepen tot uitvoering van bestaande instrumenten en tot versterking van de internationale samenwerking, ook op dit vlak.

In antwoord op de vraag van de leden van de fracties van CDA en SP merk ik op dat het met het oog op een zo krachtig mogelijke aanpak van computercriminaliteit inderdaad wenselijk is dat zoveel mogelijk landen, ook van buiten de Raad van Europa, zich aansluiten bij het Cybercrime Verdrag. Waar mogelijk zal de regering haar invloed aanwenden om bij andere landen aan te dringen op ondertekening en ratificatie van het Verdrag. Ten aanzien van landen die (nog) geen partij zijn bij het Verdrag, zal voor rechtshulpverzoeken moeten worden teruggevallen op minder specifieke verdragen terwijl bovendien de kans bestaat dat er een aanmerkelijk verschil bestaat ten aanzien van de als strafbaar aangeduide feiten; het Cybercrime Verdrag beoogt immers ook daarin enige harmonisatie te brengen.

De leden van de PvdA-fractie vroegen waarom ervoor is gekozen om de goedkeuring van het Cybercrime Verdrag in dezelfde periode te laten plaatsvinden als de behandeling van de aan te passen wetgeving (in het kader van het wetsvoorstel Computercriminaliteit II), waardoor het risico bestaat dat de desbetreffende aanpassingswetgeving wel en het Verdrag niet wordt goedgekeurd. Het beleid van de regering is erop gericht de goedkeuringsprocedure van het Verdrag en de uitvoeringswetgeving zoveel mogelijk gelijk op te laten gaan, zodat het parlement in staat wordt gesteld om beide in samenhang te beoordelen. Het is vanzelfsprekend aan de Kamer om te bepalen op welk tijdstip de beide wetsvoorstellen worden behandeld. Wel moet bedacht worden dat ons land pas aan het Verdrag kan worden gebonden nadat de nationale wetgeving met het Verdrag in overeenstemming is gebracht. Door de thans gekozen aanpak kan de Kamer zelf de volgorde van behandeling bepalen. Denkbaar is bijvoorbeeld dat de wetsvoorstellen wel gelijktijdig openbaar worden behandeld maar dat de schriftelijke voorbereiding daarvan apart verloopt.

De leden van de PvdA-fractie hebben gevraagd vanuit welke landen de meeste internet-criminaliteit plaatsvindt en welke van deze landen het Verdrag ondertekend hebben. De herkomst van internet-criminaliteit is sterk wisselend; bovendien is internet-criminaliteit vaak niet tot de werkelijke bron te herleiden. Door gebruik te maken van zogenaamde proxyservers of gehackte computers van derden wordt de herkomst van internet-criminaliteit soms afgeschermd. Voor die landen die het Verdrag niet hebben ondertekend, gelden de normale regels en procedures van de internationale rechtshulp. Dat betekent in de praktijk dat moet worden teruggevallen op minder specifieke verdragen inzake wederzijdse rechtshulp of op rechtshulp op basis van vrijwilligheid.

Doel van het Verdrag

Graag geef ik, daartoe uitgenodigd door de leden van de CDA-fractie, een nadere toelichting op de doelstelling van het Cybercrime Verdrag om een zekere ondergrens te bereiken in de harmonisatie van opsporingsbevoegdheden, nodig om in een elektronische omgeving opsporing van strafbare feiten te kunnen verrichten. Voor een adequate opsporing van computercriminaliteit zijn enerzijds algemene strafvorderlijke bevoegd-

heden nodig, zoals de bevoegdheid tot het betreden van plaatsen en het inbeslagnemen van voorwerpen, maar anderzijds ook specifieke bevoegdheden zoals de bevoegdheid tot onderzoek in computersystemen en computernetwerken. Omdat het Cybercrime Verdrag in algemene zin ten doel heeft om de mogelijkheden tot bestrijding van computercriminaliteit te vergroten en de onderlinge samenwerking tussen aangesloten staten daarbij onontbeerlijk is, is het wenselijk dat alle aangesloten lidstaten in ieder geval over dergelijke bevoegdheden beschikken. Het Verdrag voorziet daarom in een aanduiding van de bevoegdheden waarover de betrokken staten in ieder geval dienen te beschikken. De meeste van de in het Verdrag opgenomen bevoegdheden zijn in de Nederlandse wetgeving al eerder ingevoerd, zoals bij de inwerkingtreding in 1993 van de wet Computercriminaliteit (Stb. 1993, 33).

Internationale rechtshulp

De leden van de CDA-fractie wezen op het feit dat bij de voorbereiding van het Verdrag geen overeenstemming kon worden bereikt over de instelling van een gemeenschappelijke opsporingsbevoegdheid in internationale elektronische communicatienetwerken, en zij vroegen wat dan de meerwaarde van het Verdrag is, nu men hier zal moeten terugvallen op de traditionele internationale rechtshulp.
De meerwaarde van het Verdrag is ten eerste gelegen in het feit dat de «traditionele» rechtshulp voor onderwerpen die onder de werking van het Verdrag vallen, wordt aangevuld met belangrijke nieuwe bevoegdheden en snel uitvoerbare procedures waardoor de beschikbaarheid van elektronisch bewijsmateriaal ten behoeve van de verzoekende staat in belangrijke mate kan worden verhoogd; ik verwijs naar de artikelen 25 en verder van het Verdrag, waarin bijvoorbeeld de informatieverstrekking op eigen initiatief, de zogenaamde spoedbewaring van opgeslagen computergegevens en de spoedverstrekking van vastgelegde verkeersgegevens zijn geregeld.
Ten tweede is de meerwaarde van het Verdrag dat nu voor twee situaties wél is vastgelegd dat een staat zich zonder toestemming van de andere staat toegang mag verschaffen tot computergegevens die zich bevinden in een andere staat:

– Een staat mag zich toegang verschaffen tot opgeslagen publiekelijk toegankelijke (open bron) computergegevens, ongeacht waar deze zich in geografische zin bevinden (artikel 32, onderdeel a, van het Verdrag); en
– Een staat mag zich via een computersysteem dat zich op zijn grondgebied bevindt, toegang verschaffen tot of de beschikking krijgen over opgeslagen computergegevens die zich in een andere staat bevinden, indien de rechtmatige en vrijwillige instemming wordt verkregen van de persoon die gerechtigd is de gegevens via dat computersysteem aan die staat te verstrekken (artikel 32, onderdeel b, van het Verdrag).

Of er mogelijkheden zijn het Verdrag op dit punt aan te vullen met verdergaande bevoegdheden, zal moeten worden bezien bij gelegenheid van het periodieke beraad dat in artikel 46 van het Verdrag is voorzien. Vooralsnog acht ik het echter van groot belang dat de thans in het Verdrag opgenomen bevoegdheden goede aanknopingspunten bieden voor een krachtige en efficiënte internationale samenwerking.

De leden van de CDA-fractie vroegen of er voor Europol en Eurojust bij de bestrijding van cybercrime een grotere rol wordt voorzien, indien het Verdrag wordt geratificeerd door meer landen. Uit het Verdrag zelf volgt niet een taak voor deze organisaties, zoals bijvoorbeeld wel het geval is voor Interpol (artikel 27 van het Verdrag). De bevoegdheden van Europol en Eurojust vloeien voort uit hun eigen regelingen; de daadwerkelijke inzet van beide organisaties hangt met name af van het door de Raad van

Ministers van de EU vast te stellen werkprogramma. Maar gelet op het feit dat cybercrime tot het mandaat van beide organisaties behoort, voor zover het gaat om grensoverschrijdende georganiseerde criminaliteit, kan zonder meer aangenomen worden dat zij hun werkzaamheden op dat punt beter en met meer effectiviteit zullen kunnen uitvoeren naarmate meer landen bij het Cybercrime Verdrag zijn aangesloten.

De koninkrijkspositie

De leden van de CDA-fractie vroegen of er inmiddels duidelijkheid is over de vraag of de Nederlandse Antillen medegelding van het Cybercrime Verdrag wensen. De regering van de Nederlandse Antillen heeft een eigen bevoegdheid in dezen en beraadt zich nog over de wenselijkheid van medegelding. De goedkeuring van het Verdrag als zodanig zal voor het gehele Koninkrijk gelden.

Toelichting op de artikelen van het Verdrag

De leden van de SP-fractie stelden dat zij in het verleden het Cybercrime Verdrag hadden aangedragen als alternatief voor een bewaar- of vergaarplicht voor telecomproviders; zij vroegen of ook de regering niet van mening is dat «deze methode» (ik neem aan het zogenaamde bevriezingsbevel van artikel 16 c.q. 29 van het Verdrag) meer proportioneel is voor wat betreft de inbreuk op de persoonlijke levenssfeer dan de vergaarplicht.
Tijdens het Algemeen Overleg van 1 december 2004, waarin onder andere aan de orde was het ontwerp-kaderbesluit inzake de bewaring van telecommunicatiegegevens (Kamerstukken II 2004–05, 23 490, nr. 355), heeft het lid van uw Kamer, mevrouw Gerkens, gevraagd waarom de mogelijkheid van bevriezing van gegevens, zoals voorzien in artikel 29 van het Cybercrime Verdrag, niet voldoende was om te voorzien in de behoefte van de politie. Ik ben daarop ingegaan in mijn brief van 14 februari 2005 (Kamerstukken II 2004–05, 23 490, nr. 360, blz. 6). Ook in de Eerste Kamer is deze kwestie aan de orde gesteld, waar de leden van de fracties van PvdA en CDA vragen hadden gesteld over de proportionaliteit tussen doel en middel in relatie tot artikel 8 EVRM; ik verwijs naar mijn brief van 6 april 2005 (Kamerstukken I 2004–05, 23 490, AM, blz. 10). Zoals ik daarin heb uiteengezet is de essentie van de in het ontwerp-kaderbesluit voorziene bewaarplicht, dat er op het moment van het bewaren van de gegevens geen wetenschap hoeft te bestaan van de later op te sporen strafbare feiten. Daarin onderscheidt een bewaarplicht («retention») zich van een verplichting tot bevriezing («preservation»). De doelstellingen van beide maatregelen verschillen dan ook zodanig, dat een vergelijking van de proportionaliteit van beide maatregelen niet opgaat.

Artikelsgewijs

Artikel 4

De leden van de SP-fractie vroegen ons, in te gaan op het standpunt van de organisatie Bits of Freedom, dat «de voorgestelde uitbreiding» potentieel kan leiden tot een toename in de aangiften door consumenten met slecht beveiligde Pc's. Naar ik aanneem heeft deze vraag betrekking op artikel 2 van het Verdrag, dat handelt over het verbod van wederrechtelijke toegang tot computersystemen, en wordt met «de voorgestelde uitbreiding» gedoeld op de wijziging van het verbod van computervredebreuk (*hacken*) in artikel 138a Wetboek van Strafrecht, zoals voorgesteld in de tweede nota van wijziging bij het wetsvoorstel Computercriminaliteit-II (Kamerstukken II 2004–05, 26 671, nr. 7, onderdeel 2, toege-

licht op blz. 31 en 32). Graag ga ik daarop in. Artikel 2 van het Verdrag biedt de verdragsluitende partijen de mogelijkheid om hetzij een algemeen verbod van computervredebreuk in te stellen, hetzij een verbod waarbij aanvullende eisen aan de strafbaarheid van computervredebreuk worden gesteld, in die zin dat een staat mag bepalen dat computervredebreuk slechts strafbaar is als het feit wordt gepleegd (1) door een beveiligingsmaatregel te doorbreken, (2) met het oogmerk om computergegevens te verkrijgen of (3) met een andere «oneerlijke bedoeling» («*dishonest intent*»). Het thans geldende artikel 138a Sr kent dergelijke aanvullende eisen. Maar er moet ook rekening worden gehouden met artikel 2 van 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). Ook dat artikel schrijft voor dat maatregelen worden getroffen om opzettelijke onrechtmatige toegang tot een informatiesysteem of enig onderdeel daarvan strafbaar te stellen. Maar het Kaderbesluit laat niet dezelfde vrijheid aan de lidstaten bij de inrichting van de strafbepaling als het Cybercrime Verdrag. Artikel 2 van het Kaderbesluit laat de lidstaten immers slechts de keuze tussen een algehele strafbaarstelling zonder enige beperking en een strafbaarstelling waarbij alleen de beperking wordt aangebracht dat het feit dient plaats te vinden door een doorbreking van een beveiliging. Deze laatste modaliteit acht ik – zoals uiteengezet in de toelichting op de tweede nota van wijziging bij het wetsvoorstel Computercriminaliteit-II (zie vindplaats hierboven) – ongewenst, omdat daarmee de strafrechtelijke bescherming tegen computervredebreuk zou worden verminderd ten opzichte van het huidige artikel 138a Sr, waarin naast de doorbreking van een beveiliging ook andere elementen worden genoemd die kunnen leiden tot strafbaarheid van computervredebreuk, namelijk een technische ingreep, valse signalen, een valse sleutel of het aannemen van een valse hoedanigheid. De in de nota van wijziging bij Computercriminaliteit-II gekozen oplossing houdt in, dat deze elementen gehandhaafd blijven, zij het als voorbeelden van gevallen waarin wordt «binnengedrongen» in een geautomatiseerd werk. Daarmee wordt voor de jurisprudentie ruimte geschapen om ook andere methoden waarmee toegang wordt verworven, als binnendringen aan te merken. Ik verwacht evenwel niet dat dit een substantiële toename van aangiften van computervredebreuk tot gevolg zal hebben.

Artikel 5

De leden van de SP-fractie vroegen de regering naar de mogelijkheid om het Cybercrime Verdrag te koppelen aan een beperking van *spam* die via het Internet verspreid wordt. Zoals in de memorie van toelichting is uiteengezet (Kamerstukken II 2004–05, 30036, nr. 3, blz. 18), zagen de verdragspartijen geen aanleiding voor een zelfstandige strafbaarstelling van *spam* als zodanig. Artikel 5 van het Verdrag betreft het verbod om opzettelijk en wederrechtelijk de werking van een computersysteem te belemmeren. Indien degene die *spam* verstuurt de opzet heeft (wat ook de gedaante kan aannemen van zgn. voorwaardelijk opzet, dat wil zeggen dat de betrokkene de aanmerkelijke kans heeft aanvaard dat het bewuste gevolg zou intreden) om daarmee de werking van een computersysteem te belemmeren, komt dit artikel vanzelfsprekend weer wel in beeld. In het wetsvoorstel Computercriminaliteit-II wordt een nieuw artikel 138b Sr voorgesteld waarmee strafbaar wordt 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. De tekst van artikel 5 van het Verdrag spreekt in zijn Engelse tekst over «serious hindering» van het functioneren van een computersysteem en artikel 3 van het hiervoor aangeduide Kaderbesluit spreekt over «het ernstig hinderen of het onderbreken van de werking van een informatiesysteem». Het moet dus gaan om ernstige vormen van hinder voor de

gebruiker. Gedacht kan worden aan het toezenden van gegevens aan een computer(systeem) in een zodanige vorm of omvang of met een zodanige frequentie dat dit een significant nadelig effect heeft op de mogelijkheid van de eigenaar of gebruiker om de computer (of het computersysteem) te gebruiken of te communiceren met andere systemen. Ik verwijs verder naar de toelichting bij de tweede nota van wijziging bij het wetsvoorstel Computercriminaliteit-II, waarin op deze materie nader is ingegaan (Kamerstukken II 2004–05, 26 671, nr. 7, blz. 33 en 34).

De leden van de SP-fractie hebben ook nog gevraagd of er op het gebied van *spyware* maatregelen kunnen worden getroffen met gebruikmaking van het Cybercrime Verdrag. Deze vraag beantwoord ik bevestigend. Weliswaar bestaan er tussen de diverse vormen van *spyware* verschillen in verschijningsvorm, werking en dergelijke, maar in de meeste gevallen zal het installeren of versturen van *spyware* gepaard gaan met overtreding van een of meer van de specifiek op computercriminaliteit toegesneden artikelen van het Wetboek van Strafrecht, zoals gewijzigd met inachtneming van het Cybercrime Verdrag. Te wijzen valt op het verbod van computervredebreuk (artikel 138a Sr), het hierboven vermelde (nieuwe) verbod van artikel 138 Sr; het aftap- en opneemverbod van gegevens zoals voorzien in het voorgestelde nieuwe artikel 139c Sr en het verbod van artikel 350a Sr om gegevens te veranderen, te wissen, onbruikbaar of ontoegankelijk te maken dan wel daaraan andere gegevens toe te voegen. In de toelichting op de tweede nota van wijziging bij het wetsvoorstel Computercriminaliteit-II (Kamerstukken II 2004–05, 26 671, nr. 7, blz. 38 en 39) is aangegeven waarom dit laatste element (het toevoegen van gegevens) strafbaar dient te blijven met het oog op de strafbaarheid van het opzettelijk en wederrechtelijk (bijvoorbeeld zonder toestemming van de geadresseerde) meezenden van (verborgen) gegevens over de e-mail.

De leden van de fractie van de ChristenUnie vroegen of nader kan worden toegelicht waarom het versturen van *spam* niet zelfstandig strafbaar wordt gesteld, gelet op het feit dat *spam* in veel gevallen toch ernstige hinder kan veroorzaken. Zoals hiervoor uiteengezet zal het toezenden van *spam*, indien er sprake is van «ernstige hinder» voor de gebruiker, wel degelijk strafrechtelijk relevant kunnen zijn, bijvoorbeeld indien gegevens worden toegezonden in een zodanige vorm of omvang of met een zodanige frequentie dat dit een significant nadelig effect heeft op de mogelijkheid om de computer of het computersyteem te gebruiken of te communiceren met andere systemen. Het enkele toezenden van ongevraagde e-mail, indien het niet de hiervoor bedoelde effecten heeft, wordt niet strafbaar gesteld te worden, zoals ook eerder is uiteengezet in het kader van de Aanpassingswet richtlijn inzake elektronische handel (28 197) en bij de wijziging van de Telecommunicatiewet (28 815).

Artikel 9

De leden van de fractie van de ChristenUnie merkten op dat in de toelichting op dit artikel vermeld was dat deze bepaling ook strafbaar stelt het als maatschappelijk aanvaardbaar voorstellen van kinderpornografie en aanverwante zaken, maar dat zij dié strekking van het artikel niet zo gemakkelijk in het artikel zelf konden terugvinden, hoewel zij zich de wenselijkheid daarvan als zodanig goed konden voorstellen. Graag licht ik dit punt nog eens toe. De strafbaarstelling van de verschillende in artikel 9 vermelde gedragingen strekt primair tot bescherming van minderjarigen tegen misbruik. Kinderpornografie wordt in artikel 9, tweede lid, onderdeel a, van het Verdrag immers omschreven als pornografisch materiaal dat visueel een minderjarige uitbeeldt, die betrokken is bij expliciet seksuele handelingen. Maar onderdeel c van dat artikellid bepaalt dat ook

realistische afbeeldingen, voorstellende een minderjarige die betrokken is bij expliciet seksuele handelingen, als kinderpornografie worden aangemerkt. En onderdeel b maakt duidelijk dat het ook kan gaan om de uitbeelding van iemand met het *voorkomen van een minderjarige*. In beide gevallen staat niet de bescherming van individuele minderjarigen tegen misbruik voorop, maar de bescherming van minderjarigen in het algemeen tegen de vervaardiging en verspreiding van kinderpornografisch materiaal: in beide gevallen is de betrokkenheid van kinderen bij de vervaardiging van dergelijk materiaal niet relevant. Ik verwijs ook naar de brief van 23 december 1999 van de toenmalige Minister van Justitie aan de Tweede Kamer, waarin hij inging op de betekenis van het betrokken verdragsartikel voor de Nederlandse wetgeving (Kamerstukken II 1999–2000, 23 530, nr. 40, blz. 4–5). Inmiddels is in het kader van de partiële wijziging van de zedelijkheidswetgeving artikel 240b van het Wetboek van Strafrecht in overeenstemming gebracht met artikel 9 van het Verdrag (Wet van 13 juli 2002, Stb. 388), waardoor het sindsdien niet meer noodzakelijk is dat wordt bewezen dat een echt kind bij de vervaardiging van kinderpornografie is betrokken; bij de totstandkoming van het desbetreffende wetsvoorstel werd wel de term «virtuele kinderporno» gebruikt. Ik moge verwijzen naar de passages in de wetsgeschiedenis die daarop betrekking hebben (Kamerstukken II 2000/01, 27 745, nr. 3, blz. 4–5, idem 2001/02, nr. 6, blz. 8, 11 en 15).

De leden van de fractie van de ChristenUnie vroegen in dit verband ook, of de in het Verdrag opgenomen leeftijdsgrens van 18 jaar een wijziging of verduidelijking brengt van de grenzen die totdusver in Nederland worden gehanteerd. In het kader van de hiervoor gememoreerde partiële wijziging van de zedelijkheidswetgeving is óók de leeftijdsgrens in overeenstemming gebracht met het (toen nog: concept-) Verdrag, zodat voor kinderpornografie ook naar Nederlands recht sinds 2002 reeds een leeftijdsgrens van 18 jaar geldt. Naar ik meen kan voor de in dit kader nog gestelde vragen worden verwezen naar de totstandkoming van de bedoelde wetswijziging.

Artikelen 29 en 30

De leden van de SP-fractie vroegen naar aanleiding van de introductie van het zogenaamde bevriezingsbevel, aan te geven welke informatie kan leiden tot zo'n bevriezingsbevel. Deze leden meenden dat er toch bepaalde aanwijzingen zullen moeten zijn alvorens aan een telecomprovider opgedragen kan worden om dataverkeergegevens te bevriezen. Inderdaad moeten er bepaalde aanwijzigingen zijn voordat de bevoegdheid, die door middel van het Wetsvoorstel Computercriminaliteit-II in het Wetboek van Strafvordering zal worden ingevoegd als artikel 126ni, mag worden toegepast. De bevoegdheidstoepassing is gebonden aan beperkingen en voorwaarden, die naar aanleiding van de uitgebrachte adviezen nog zijn aangescherpt. De bevriezingsbevoegdheid (dat wil zeggen: de bevoegdheid te vorderen dat bepaalde gegevens worden bewaard en beschikbaar gehouden) mag op grond van het voorgestelde artikel 126ni Sv alleen worden toegepast indien er een verdenking van een misdrijf bestaat, en dan nog wel 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. Een extra voorwaarde is, dat de vordering tot het bewaren en beschikbaar houden van gegevens slechts mag worden gedaan indien het belang van het onderzoek dat dringend vordert. Zoals in de toelichting op de desbetreffende bevoegdheid is vermeld, (Kamerstukken II, 2004–05, 26 671, nr. 7, blz. 45) mag geen onevenredige inspanning worden verlangd van degene tot wie de vordering is gericht. Dit alles maakt ook duidelijk dat niet zomaar tot iedereen de vordering kan worden gedaan

om bepaalde gegevens te bewaren. In het door de vragenstellers genoemde geval waarin gegevens kennelijk voor een ieder toegankelijk zijn via internet, zijn de gegevens dus ook toegankelijk voor de politie zelf. Gelet op de eisen van proportionaliteit, subsidiariteit en effectiviteit die hier vanzelfsprekend in acht genomen moeten worden, zal in zo'n geval dus niet van een willekeurige internetter gevorderd kunnen worden dat hij de betrokken gegevens «bewaart en beschikbaar houdt», nog daargelaten de vraag of die persoon wel beschikt over veilige opslagmogelijkheden.

Deze leden vroegen ook nog, op welke wijze de opdracht tot bevriezing zal worden doorgegeven, mede met het oog op het voorkomen van fouten. Dit is inderdaad een belangrijk punt. Tussen het openbaar ministerie, de politie en degene van wie bevriezing van de gegevens wordt gevorderd, zullen praktische afspraken gemaakt moeten worden om fouten zoveel mogelijk te voorkomen. De vordering mag mondeling (met een latere schriftelijke bevestiging) of schriftelijk worden gedaan. In beide gevallen zal ervoor gezorgd moeten worden dat de vordering terecht komt bij de bevoegde instantie én dat daarover geen verdere bekendheid ontstaat dan nodig is voor de uitvoering van de vordering.

Deze leden vroegen nog, waarom ervoor is gekozen om deze ingrijpende bevoegdheid te leggen bij de hulpofficier van justitie. Hier is kennelijk sprake van een misverstand. Naar aanleiding van de uitgebrachte adviezen is de onderhavige regeling ingrijpend herzien, onder meer ten aanzien van de bevoegde autoriteit. De bevoegdheid komt niet toe – zoals oorspronkelijk voorzien – aan de hulpofficier van justitie, maar aan de officier van justitie. Ook op andere punten, zoals door deze leden hier aan de orde gesteld, is de regeling herzien of van een nadere toelichting voorzien, onder meer naar aanleiding van het commentaar van de Nederlandse Vereniging voor Rechtspraak en de Nederlandse Orde van Advocaten.

Deze leden vroegen tenslotte in te gaan op de vraag, welke informatie als gevolg van dit wetsvoorstel (bedoeld zal niet zijn het wetsvoorstel tot goedkeuring van het Cybercrime Verdrag maar het wetsvoorstel Computercriminaliteit-II) bevroren kan worden. Een inhoudelijke aanduiding van de aard van de informatie kan in algemene zin echter niet worden gegeven. Het moet in ieder geval gaan om gegevens die zijn opgeslagen in een geautomatiseerd werk en waarvan redelijkerwijs kan worden aangenomen dat zij in het bijzonder vatbaar zijn voor verlies of wijziging, de zogenaamde vluchtige gegevens. In de toelichting op de betrokken wetsbepaling (Kamerstukken II 2004–05, 26 671, nr. 7, blz. 44) is het voorbeeld gegeven van een situatie waarin bij een schietincident met slachtoffers veel mogelijke betrokkenen op de plaats van het incident aanwezig waren en gegevens over deze betrokkenen wellicht beschikbaar zijn omdat zij in de buurt van het incident elektronische handelingen hebben verricht of gebruik van mobiele telecommunicatie hebben gemaakt. Denkbaar is dan dat gevorderd wordt om de zogenaamde «paalgegevens» van de mobiele telefonie tijdelijk te bewaren, evenals gegevens over elektronisch betaalverkeer dat in de buurt is verricht, teneinde de mogelijkheid te behouden om zonodig op die wijze getuigen en andere betrokkenen te kunnen achterhalen. Van belang is hierbij ook weer dat de eisen van proportionaliteit, subsidiariteit en effectiviteit in het oog worden gehouden.

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