Holdijk

In de commissie hebben onze fracties via het voorlopig verslag uitdrukking gegeven aan hun twijfels in hoeverre de rechtszekerheid van partijen door dit voorstel wordt bevorderd. Eén ding is volstrekt duidelijk: er wordt meer geregeld dan bij het bestaande concurrentiebeding, zoals de al genoemde verplichte vergoeding, de geldigheidsduur en de verplichte beschrijving van de werkzaamheden. De regering spreekt van een aanscherping van de regelgeving. In elk geval is sprake van een meer gedetailleerde regeling. Maar het is, zo denk ik, een algemeen gegeven dat meer regels per saldo niet altijd tot meer duidelijkheid en grotere zekerheid leiden. Elke nieuwe regel kan immers weer zijn eigen vragen doen rijzen.

Het vanmiddag al veel genoemde lid 8 van artikel 653, dat zijn ontstaan te danken heeft aan een amendement van de Tweede Kamer, is in de commentaren het meest bekritiseerd; het heeft althans de meeste discussies opgeroepen. Het amendement plus de daarbij behorende toelichting heeft, zo lijkt het, een heldere bepaling opgeleverd die aan veel discussie een einde moest maken: het verbod voor de ex-werknemer om klanten van de ex-werkgever te benaderen, een relatiebeding, valt niet onder de regeling van het concurrentiebeding. Het wezenlijke verschil dat de regering thans ziet tussen het concurrentiebeding en het relatiebeding zou, als het wezenlijk is, uiteraard voor iedereen duidelijk moeten zijn. Dat blijkt echter niet het geval. Volgens een van de auteurs die kritiek leveren op de stelling van de regering dat het relatiebeding niet valt onder het concurrentiebeding, dankt het amendement zijn bestaan aan het eigen gebrek aan kennis bij de meest betrokkenen gedurende de behandeling van het wetsvoorstel in de Tweede Kamer over de vraag wat nu precies een concurrentiebeding is. Ik kreeg de indruk uit de bijdrage van mevrouw De Wolff dat zij zich in die opmerking kon verplaatsen. Hoe dit ook zij, voorgaande sprekers in deze Kamer mogen toch geacht worden over voldoende kennis en ervaring uit eigen praktijk te beschikken. Wat daarvan vervolgens weer moge zijn, zélf heb ik de sterke indruk dat ons met name de vage, multi-interpretabele omschrijving in het eerste lid van artikel 653, bestaande in de aanduiding ''op zekere wijze werkzaam zijn'', parten speelt.

De SER is de mening toegedaan dat de door de regering gekozen definitie van het relatiebeding een tamelijk willekeurige is. Volgens de raad kan worden gesteld dat het voorgestelde lid 8 van artikel 653 in de gekozen opzet in ieder geval geen einde zal maken aan de lopende discussies. Hij meent dat de gekozen definitie het risico in zich draagt dat bedingen die qua strekking het relatiebeding lijken te benaderen, bij letterlijke interpretatie ervan door de rechter toch niet als zodanig zullen worden uitgelegd. Er kan dan gedurende lange tijd onzekerheid blijven bestaan of het ''relatiebeding'' ook daadwerkelijk een relatiebeding is. De regering heeft schriftelijk gereageerd op de stelling van de raad, maar nauwelijks iets toegevoegd aan hetgeen in beide memories al naar voren was gebracht. De centrale vraag is, hoe de regering denkt dat, met een niet in de wet omschreven definitie van een relatiebeding en met de vage omschrijving van het concurrentiebeding, de rechter in het door haar bedoelde spoor te houden. Dit allemaal in het licht van het feit dat één van de belangrijkste doelen van het wetsvoorstel toch was het bevorderen van de rechtszekerheid, het voorkomen van rechtsvragen en procedures. Op deze centrale vraag zal in dit debat een afdoende antwoord moeten komen om dit wetsvoorstel voluit te kunnen omarmen.

Wij zien met belangstelling naar de reactie van de regering uit.

De beraadslaging wordt geschorst.

Aan de orde is de gezamenlijke behandeling van:

- **het wetsvoorstel Wijziging van het Wetboek van Strafrecht, het Wetboek van Strafvordering en de Telecommunicatiewet in verband met nieuwe ontwikkelingen in de informatietechnologie (computercriminaliteit II) (26671);**
- **het wetsvoorstel Goedkeuring van het op 23 november 2001 te Boedapest tot stand gekomen Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken (Trb. 2002, 18) (30036, R1784).**

De beraadslaging wordt geopend.

□

De heer **Franken** (CDA): Voorzitter. Ik mag u meedelen dat ik mijn inbreng mede mag leveren namens de fractie van de PvdA.

Nog niet zolang geleden was er in Friesland een jongeman die de tennisster – of is het tennisstér? – Anna Kournikova zeer bewonderde. Ik kan mij daar overigens best wat bij voorstellen! Bovendien had deze jongeman een bijzondere affiniteit met computervirussen. Hij heeft dan ook een naar deze dame genoemd computervirus in omloop gebracht. Er ontstond op grond daarvan grote opschudding, omdat dit virus een enorme schade kon teweegbrengen en er kwam veel aandacht in de media voor deze daad. De aandacht werd daarbij vooral getrokken door de burgemeester van de woonplaats van de dader, die zich voor de televisie trots betoonde over het feit dat ''zijn gemeente nu wereldwijd op de kaart was gezet'' en hij bood daarom zijn slimme plaatsgenoot publiekelijk een baan aan in gemeentedienst.

Nu is het natuurlijk bijzonder kwalijk wanneer een burgemeester publiekelijk een strafbare en bovendien zeer schadelijke handeling als een soort heldendaad ophemelt, maar het getuigt ook van een grenzeloze naïviteit wanneer iemand nog denkt, dat het verspreiden van een virus of het inbreken in computersystemen een onschuldige bezigheid is van een enkele ''nerd'' of een soort Robin Hood, die alleen rijken besteelt ten bate van de armen. Het misbruiken van informatie door de inhoud te veranderen, de overdracht te storen of de vertrouwelijkheid te schaden, levert inmiddels veel nadelen en economische schade op voor onze samenleving. Oude vormen van criminaliteit als oplichting en verduistering kunnen op veel groter schaal gevolgen hebben dan vroeger het geval was, terwijl nieuwe vormen van schadelijk gedrag, zoals het verspreiden van virussen of spam, het plaatsen van Trojaanse paarden, het cracken van informatiesystemen en allerlei vormen van denial of service attacks in bedrijven en huisgezinnen een hoop narigheid kunnen veroorzaken. Concrete schadebedragen zijn moeilijk te noemen, maar het loopt wereldwijd in vele honderden miljarden en de stijging is er nog lang niet uit. Het beveiligingsbedrijf Symantec heeft bijvoor-

beeld in het tweede halfjaar van 2005 10.992 nieuwe varianten van virussen gedetecteerd en ook in Nederland zouden per maand meer dan 350 pogingen tot phishing worden gedaan, waarmee de identiteitsfraude zich ontwikkelt tot een levensgroot gevaar. Het mag duidelijk zijn dat het strafrecht ter bestrijding van dit misbruik een rol krijgt.

In 1987 is de basis gelegd voor de huidige Wet computercriminaliteit door een door de regering ingestelde commissie, die twee belangrijke uitgangspunten heeft vastgesteld voor de bestrijding van strafbaar gedrag met behulp van de nieuwe middelen van de informatietechnologie. Ten eerste: de wet moet zo veel mogelijk techniekonafhankelijke formuleringen gebruiken, want anders zal de wet op korte termijn door de technische ontwikkelingen zijn achterhaald, en ten tweede: het strafbare gedrag moet worden geformuleerd in termen die niet zozeer specifieke handelingen betreffen, maar aangeven welke rechtsbelangen door dit gedrag zijn geschaad. Daarmee zijn er algemene beginselen voor behoorlijk gebruik van informatietechnologie geformuleerd naar analogie van algemene beginselen van behoorlijk bestuur en algemene rechtsbeginselen in het strafrecht en civiele recht.

De WCCI van 1993 is dan ook geschreven op de beginselen ''beschikbaarheid'',''integriteit''en ''vertrouwelijkheid'', die de basis vormen voor de delictsomschrijvingen in het Wetboek van Strafrecht. Het aardige is nu, dat bij het opstellen van het Cybercrimeverdrag op deze in de Nederlandse wetgeving gehanteerde beginselen is voortgebouwd, zodat ten aanzien van het materiële recht daarin voor Nederland niet zoveel nieuws meer is te vinden. Wel wordt daarin veel aandacht gegeven aan politiële en justitiële samenwerking. En dat is terecht, want criminaliteit met behulp van de middelen van ICT is niet aan grenzen gebonden, terwijl dat wel geldt voor de politiële en justitiële bevoegdheden. Met dit verdrag zetten we daarom een goede stap vooruit.

De aanpassing van de Wet computercriminaliteit I in het thans voorliggende wetsvoorstel wordt ingegeven door een door de minister noodzakelijk geachte hardere aanpak van computercriminaliteit. Bij de indiening van het voorstel speelde ook nog een rol de noodzakelijk geachte regeling van de strafrechtelijke aansprakelijkheid van internet service providers. Er was in het voorstel op een goede wijze aangesloten bij de regeling van de vervolgingsuitsluitingsgronden die gelden voor de drukker en de uitgever. Helaas is dit voorstel vanuit Brussel getorpedeerd en vervangen door de regeling, die wij nu via de e-commerce richtlijn vinden in artikel 54a van het Wetboek van Strafrecht. Dat is jammer, omdat er nu in de wet een technische omschrijving is opgenomen aangezien het gaat om ''doorgifte'' of ''opslag''. Deze kan al tot interpretatieproblemen leiden. De vraag aan de minister is dan ook of hij in Brussel zijn voelhorens uitsteekt om te bezien of het mogelijk is om deze bepaling te laten vervangen door een formulering die onafhankelijk is van de techniek.

Bovendien leg ik de vraag voor hoe de spanning het beste kan worden opgevangen waarin de internet service providers verkeren, wanneer een partij stelt dat een publicatie onrechtmatig is, terwijl de klant die de publicatie door toedoen van de ISP heeft geplaatst, zich verzet tegen verwijdering ervan. Een kort geding is dan geen goede mogelijkheid, want deze is te kostbaar en te traag. Er is gepleit voor een notice and take-downprocedure, doch ik heb nog niet kunnen vernemen of daarmee vorderingen zijn gemaakt. Kan de minister aangeven of en, zo ja, hoe hij de internet service providers bij deze spagaat uit de problemen wil helpen?

Zoals gezegd, en zoals blijkt uit de stukken, kan mijn fractie zich vinden in het wetsvoorstel, alleen hebben wij nog een serieus probleem met het nieuw voorgestelde artikel over computervredebreuk: artikel 138a Wetboek van Strafrecht. Het wetsvoorstel laat de eis van beveiliging als een voorwaarde voor strafbaarheid vallen. De ratio van deze eis, die bij de behandeling van de Wet computercriminaliteit I op volle instemming mocht rekenen, is ten eerste de kenbaarheid voor de dader. Er moet een duidelijke grens of drempel worden overschreden, alvorens van een strafbaar feit sprake is. Hiermee samenhangend is ten tweede het bewijs van het feit makkelijk te leveren door aan te geven dat er een drempel is overschreden of een deur is opengemaakt. De wil van de gebruiker van het systeem die zich tegen binnendringen verzet, is daarmee aangegeven. Ten derde is het uit het oogpunt van criminele politiek van belang dat een gebruiker zelf ook zorgvuldig omgaat met zijn eigen systeem. Hij moet niet zomaar alle deuren laten openstaan.

In de stukken voor de Tweede Kamer wordt hiertegen ingebracht dat een aanscherping van de delictsomschrijving voor een verruiming pleit. In 2005 is daar een ander, extra argument bijgeschoven, te weten het kaderbesluit 2005/222/JBZ van de Raad. Dat kaderbesluit zou Nederland voor de keuze stellen tussen algehele strafbaarstelling van de opzettelijke en wederrechtelijke toegang tot een informatiesysteem of een systeem waarbij als enige voorwaarde voor strafbaarheid geldt dat er sprake is van een doorbreking van een beveiliging.

Naar mijn mening noopt noch het kaderbesluit, noch het Cybercrimeverdrag tot de voorgestelde wijziging. De nieuwe redactie heeft als enige voorwaarde voor strafbaarheid het opzet- en het wederrechtelijkheidsvereiste. Maar hoe kan dan de ''verklaarde wil'' van de gebruiker van het systeem worden bewezen? Een bordje ''verboden toegang'' is in de virtuele wereld volstrekt onvoldoende. Hoe moet men in de virtuele wereld zijn wil om een binnendringer tegen te houden anders verklaren dan door een technische maatregel te nemen, bijvoorbeeld door een toegangscode voor te schrijven, juist omdat men in de wereld van het internet steeds zijn best doet om klanten of gesprekspartners op zijn web- of mailadres binnen te halen? De minister heeft ons in het antwoord nog steeds niet overtuigd. Ik leg hem daarom deze vraag nog een keer voor.

Een volgende vraag betreft de ontsleutelplicht. De minister heeft toegezegd, eens te informeren hoe een en ander in Frankrijk en het Verenigd Koninkrijk is geregeld. Voorshands ga ik ervan uit dat de ontsleutelplicht niet wordt opgelegd aan de verdachte in verband met de nemo-teneturregel.

Dan heb ik nog een opmerking over de handhaving. Regels met sancties zonder garanties voor de uitvoerbaarheid hebben geen zin. Zij lijken misschien dienstbaar te zijn aan de rechtsorde, maar in werkelijkheid leiden zij tot rechtsbederf. Daarom heb ik hierover nog enige vragen.

Ten eerste houden naast Justitie ook Economische Zaken en Verkeer en Waterstaat zich bezig met computercriminaliteit. Wie doet wat en hoe staat het met de

kennis op dit gebied bij de opsporingsautoriteiten? Als ik het goed begrijp, heeft het departement van Economische Zaken het initiatief overgenomen bij de aanpak van de preventie door het Nationaal platform criminaliteitsbeheersing, waarin een groot aantal organisaties participeert. Daarnaast is Verkeer en Waterstaat verantwoordelijk voor het veiligheidsprogramma KWINT (Kwetsbaarheid op internet). En hoe zit het met de inbedding van de opsporing? Daarvoor draagt de minister van Justitie toch de verantwoordelijkheid? Er zijn specifieke deskundigen voor nodig, zoals auditors en webrechercheurs. Is die kennis aanwezig? Hoe is de opleiding en training georganiseerd? Wat is de verhouding tussen allerlei organisaties die zich hier melden, zoals Govcert, het National High Tech Crime Center en natuurlijk het Korps landelijke politiediensten? En dan hebben wij ook nog het Nederlands Forensisch Instituut, waar al heel wat kennis aanwezig is. Krijgen wij hier concurrerende instanties, met rivaliteit tussen de ambtenaren?

Ten tweede zit ik met het punt dat bij het aftappen veel fouten worden gemaakt, zoals blijkt uit onderzoek van Dialogic en de universiteit van Tilburg. Aftappen is een principiële inbreuk op een grondrecht en bovendien zeer kostbaar voor de providers. Van de kosten wordt maar een fractie vergoed. Er zijn diverse redenen om deze opsporingsbevoegdheid terughoudend en zorgvuldig te gebruiken. Graag hoor ik nog eens de visie van de minister op het beleid bij dit onderwerp. Ik heb het idee, en er is ook wel wat literatuur over, dat deze bevoegdheid nogal uit de losse pols wordt gebruikt. De minister zal weten dat een provider in het Verenigd Koninkrijk een tapverzoek kan laten toetsen door de Interception of Communication Commissioner. Overeenkomstig het voorstel van de provider XS4all zou men een geanonimiseerd statistisch overzicht kunnen publiceren om er enigszins achter te komen of nut en noodzaak de facto als doorslaggevende criteria worden gehanteerd. Het spreekt vanzelf dat de nakoming van de notificatieplicht bij dat oordeel ook een belangrijke rol speelt.

Ten derde is de vraag naar de rechtsmacht natuurlijk een heikel punt bij het onderwerp cybercrime. Wordt er inmiddels gewerkt aan een aanvulling op dit gebied, bijvoorbeeld door een aanvullend protocol op het Cybercrimeverdrag, om de werking uit te breiden?

Dan nog een persoonlijke noot tot besluit, gericht tot deze minister: ceterum censeo obligationem preservationis datorum informationis esse delendam.

□

Mevrouw **Broekers-Knol** (VVD): Mevrouw de voorzitter. Uit eigen ervaring is mij bekend dat deze minister er niet voor terugdeinst om straks in het Latijn te antwoorden.

Wij spreken vandaag over het wetsvoorstel Computercriminaliteit II en over het wetsvoorstel betreffende het zogeheten Cybercrimeverdrag. Dit verdrag is tot stand gekomen in het kader van de Raad van Europa. Computercriminaliteit II en het wetsvoorstel over het Cybercrimeverdrag zijn nauw aan elkaar verbonden. Om het Cybercrimeverdrag te kunnen ratificeren zijn enkele wijzigingen van met name het Wetboek van Strafrecht en het Wetboek van Strafvordering nodig. Die wijzigingen zijn door middel van een tweede nota van wijziging en in het wetsvoorstel Computercriminaliteit II ondergebracht.

Met het Cybercrimeverdrag en het wetsvoorstel Computercriminaliteit II wordt een belangrijke stap gezet in de richting van internationale samenwerking ter bestrijding van strafbare feiten verbonden met elektronische netwerken. Voor het overige worden door het wetsvoorstel Computercriminaliteit II de Wetboeken van Strafrecht en Strafvordering gewijzigd vanwege nieuwe ontwikkelingen in de informatietechnologie.

De wetsvoorstellen waarover wij vandaag spreken, zijn kwalitatief goede wetsvoorstellen. In de memorie van antwoord heeft de minister uitgebreid geantwoord op de in het voorlopig verslag gestelde vragen. Dank daarvoor. Namens de VVD-fractie heb ik dan ook slechts een enkele vraag.

In het voorlopig verslag is door mijn fractie de vraag gesteld of de definities van ''gegevens'' (artikel 80quinquies van het Wetboek van Strafrecht) en ''geautomatiseerd werk'' (artikel 80sexies van het Wetboek van Strafrecht) niet ook in de betekenissentitel van het Wetboek van Strafvordering zouden moeten worden opgenomen. De minister antwoordt daarop op pagina 6 van de memorie van antwoord dat hem uit de praktijk niet bekend is dat er problemen ontstaan doordat een aparte definitiebepaling in het Wetboek van Strafvordering ontbreekt. Dat moge zo zijn, maar zou het uit een oogpunt van wetsystematiek geen aanbeveling verdienen om de definities bij een eerstvolgende wijziging van het Wetboek van Strafvordering toch in dat wetboek op te nemen? Graag een reactie van de minister.

Op pagina 11 van de memorie van antwoord merkt de minister, naar aanleiding van een vraag van de CDA-fractie, op dat hij binnenkort de eindrapportage van het project NHTCC – het National High Tech Crime Center – verwacht. Kan de minister informatie geven of die eindrapportage inmiddels is uitgebracht en, zo ja, wat de conclusies zijn met betrekking tot het NHTCC? Uit de memorie van antwoord maken wij op dat het NHTCC wordt opgeheven en dat de werkzaamheden ervan worden ondergebracht bij de nationale recherche. Is die conclusie juist?

In het voorlopig verslag vroeg mijn fractie of het voorgestelde artikel 125o van het Wetboek van Strafvordering wel voldoende sluitend is en of niet aan de zittingrechter de bevoegdheid moet worden toegekend om de strafbare gegevens uit het systeem te laten verwijderen, voorafgaand aan de teruggaaf van een computersysteem. De reden om dit niet te doen is op efficiencygronden gebaseerd, zoals blijkt uit de memorie van antwoord. Op pagina 15 staat te lezen: ''Dit kost veel capaciteit van de betrokken opsporingsambtenaren.'' Mijn fractie heeft daar begrip voor. Het is de verdienste van de beantwoording in de memorie van antwoord dat voor de efficiencygronden ook nog een juridisch steekhoudende motivering kan worden gegeven. Ik citeer: ''Als inbeslagneming van de gegevensdrager proportioneel was, dan zal onttrekking aan het verkeer niet snel disproportioneel zijn.'' De vraag of de vraag van mijn fractie daarmee voldoende ''sluitend'' beantwoord is, blijft echter open.

Nog geen uur geleden kwam ik, zonder daarvoor enige moeite te doen en, afgezien van het verstrekken van mijn nieuwe password, zonder opzet in de e-mailbox van GroenLinks terecht. Mijn vraag is: ben ik nu een computercrimineel?

Wij vernemen graag de antwoorden van de minister op de enkele vragen die wij gesteld hebben. Ik kan echter

reeds nu zeggen dat de VVD-fractie instemt met beide wetsvoorstellen.

Mevrouw **De Wolff** (GroenLinks): Ik kan mevrouw Broekers meteen geruststellen: ik ontken het wederrechtelijke karakter van haar inbreuk in onze e-mailbox.

Mevrouw **Broekers-Knol** (VVD): Dank u.

□

Mevrouw **De Wolff** (GroenLinks): Voorzitter. Ik voel mij gelukkig nooit onveilig op straat. Er is slechts één weg waar ik mij wel regelmatig onveilig voel, en dat is de elektronische snelweg. Dat dateert al van voor de rampen die ons twee weken geleden hier in de Eerste Kamer troffen, toen duidelijk werd dat in onze eigen computer in de Johan de Wittzaal een worm huist. Het blijkt niet eenvoudig te zijn om die worm te verwijderen. Ook los daarvan bekruipt mij regelmatig een gevoel van grote onveiligheid wanneer ik mij op de elektronische snelweg begeef, of dat nu is als advocaat die correspondentie wil verzenden, als toerist die een hotel wil betalen met een creditcard of als consument die gewoon wil internetbankieren. Daarom is het goed dat wij vandaag het cybercrimeverdrag aanvaarden en dat wij het wetsvoorstel tot implementatie van dat verdrag gaan aanvaarden. Er zitten een aantal elementen in die een betere aanpak van computercriminaliteit mogelijk maken, maar ik heb met mevrouw Broekers en de heer Franken een aantal vragen.

Mijn eerste serie vragen betrof artikel 138a van het Wetboek van Strafrecht, waarover ik met de heer Franken grote aarzeling heb omdat ik meen dat computergebruikers hun spulletjes afdoende moeten bewaken. Als iemand bewust of onbewust binnentreedt in andermans computer, zoals mevrouw Broekers vandaag kennelijk is overkomen, moet er geen sprake zijn van strafbaarheid. Ik refereer ook aan een in ieder geval voor mij begrijpelijk artikel van Frank Kuitenbrouwer in de NRC Next van 16 mei jongstleden. De minister moet dat artikel kennen, want het zat in de knipselkrant die wij dagelijks van het ministerie van Justitie ontvangen. Ik hoor van de minister graag een overtuigende weerlegging van de kritiek op dat artikel.

Een andere serie vragen die ik niet zal herhalen, had betrekking op de handhaving, maar daar is mevrouw Broekers al uitvoerig op ingegaan. Ik sluit mij op dat punt kortheidshalve bij haar aan.

Mijn laatste vraag, die een meer materiële aard heeft, betreft de spulletjes die in hoofdzaak zijn ontworpen om computermisdrijven mee te plegen. Ik begrijp niet helemaal wat dat voor spulletjes moeten zijn. De wet is daar onduidelijk over en de toelichting die de minister op 13 september in de Tweede Kamer heeft gegeven, maakt het er allemaal niet duidelijker op. Ik refereer aan een debatje met het lid Van Fessem over hackprogramma's en de verkoop daarvan in de winkel. De minister zei toen, blijkens pagina 6361 van de Handelingen: ''De winkelier die een dergelijk programma verkoopt, weet heel goed dat hij een programma verkoopt waarmee een strafbaar feit kan worden gepleegd. Het is wat anders dan het in huis hebben van een hackprogramma. Dan is niet per definitie die opzet aanwezig.'' Er zijn dus kennelijk artikelen, programma's en apparatuur die in hoofdzaak zijn bestemd voor het plegen van computercriminaliteit, maar of er sprake is van strafbaarheid, hangt kennelijk af van wie die artikelen voorradig heeft, verkoopt, verhandelt of onder zich heeft. Dat was mij allemaal niet op voorhand duidelijk. Ik kan mij ook niet veel voorstellen bij de afgrenzing van het type apparaat of programma dat in hoofdzaak is bestemd voor het plegen van computercriminaliteit. Als de minister daar een verduidelijkende toelichting op zou willen geven, ben ik in ieder geval tevreden.

De vergadering wordt van 14.50 uur tot 15.25 uur geschorst.

□

Minister **Donner**: Voorzitter. Ik dank de leden voor de waarderende woorden die zij gesproken hebben en voor de steun die zij hebben uitgesproken voor de wetsvoorstellen. Ik hoop nu de laatste vragen te beantwoorden, opdat wij dit traject op bevredigende wijze kunnen afsluiten. De heer Franken is uitvoerig ingegaan op de voorgeschiedenis van de Wet computercriminaliteit en het verschijnsel computercriminaliteit. Ik kan dat niet beter, dus ik laat dat achterwege.

De heer Franken heeft gevraagd of de formulering in artikel 54a Wetboek van Strafrecht, te weten doorgifte of opslag van gegevens, niet te techniekafhankelijk is gemaakt. Ik constateer dat er indertijd in het kader van de implementatie van de e-commercerichtlijn voor is gekozen om zo veel mogelijk te benadrukken dat de strafrechtelijke vrijwaring alleen opgaat voor gevallen waarin de tussenpersoon niets anders doet dan doorgeven of opslaan. Ik stel vast dat de term opslag ook in andere bepalingen van de Wetboeken van Strafrecht en Strafvordering voorkomt. Hetzelfde geldt voor de term doorgifte; die term komt ook voor in bijvoorbeeld de Wet bescherming persoonsgegevens. Het gaat dus niet om technisch afhankelijke termen, maar om een activiteit, namelijk het doorgeven of het opslaan van gegevens. Als geregeld zou zijn hoe wordt opgeslagen of hoe wordt doorgegeven, dan ben ik het met de heer Franken eens dat de wet te techniekafhankelijk wordt. Er is gekozen voor termen die een activiteit aanduiden. Ze zijn kennelijk zo duidelijk dat ze elders in de wetgeving ook voor andere technieken worden gebruikt. Dan kunnen ze hier dus ook gebruikt worden. Ik zie dan ook geen reden om dit in Brussel aan de orde te stellen.

Dan was de vraag hoe internetproviders moeten omgaan met de situatie waarin de officier van justitie hun beveelt publicaties of afbeeldingen te verwijderen, terwijl zij van de opdrachtgever te horen krijgen dat er geen sprake is van een strafbaar feit en dat die publicaties of afbeeldingen moeten blijven staan. Artikel 54a gaat alleen over het door de officier van justitie te geven bevel aan de tussenpersoon, die zich louter met doorgifte of opslag bezighoudt, en dan nog alleen met als strekking dat deze tussenpersoon als zodanig niet wordt vervolgd indien hij het bevel tot verwijdering opvolgt. Het gaat dus om een heel concrete situatie. Dat betekent dat het moet gaan om strafbare feiten en niet om afbeeldingen of publicaties die alleen in civielrechtelijke zin onrechtmatig kunnen zijn.

De vraag is hoe de internetprovider zich moet opstellen als zo'n bevel komt en zijn klant zich tegen de verwijdering verzet. Ik stel vast dat het OM een dergelijk bevel pas zal geven als er feitelijk bijna geen twijfel

bestaat over het strafbare karakter. De claims van degenen die de opdracht gegeven hebben, zullen moeten berusten op onrechtmatige daad of wanprestatie als de internetprovider de publicatie of de beelden verwijdert. Die claims zullen stuiten op de verdediging dat men handelde in opdracht van het Openbaar Ministerie. Kortom, als de claims al gegrond zijn, dan zullen zij zich richten tegen de Staat. De internetprovider zal zich dus op die wijze kunnen verdedigen. Nogmaals, ik acht het weinig waarschijnlijk dat die situatie zich zal voordoen, omdat het OM niet lichtvaardig zal overgaan tot het geven van zo'n bevel.

In het kader van de samenwerking tussen alle betrokken partijen wordt gezocht naar modaliteiten om er los van het bevel op basis van artikel 54a voor te zorgen dat onwenselijke publicaties worden verwijderd. Er is inderdaad nog geen alles overkoepelende notice en take-downprocedure. Er is samen met een aantal internetproviders gezocht naar een opzet voor een dergelijke procedure. Dat is niet gelukt, omdat internetproviders meer garanties willen op het gebied van hun aansprakelijkheid in een dergelijke situatie. Daarbij komt dat de steeds groeiende markt van providers het lastig maakt om tot sluitende afspraken te komen op dit terrein. Daarom is er nu voor gekozen om werkendeweg, via meldingen die binnenkomen bij het Meldpunt Cybercrime, een structuur te ontwikkelen.

De heer **Franken** (CDA): De minister zegt dat het OM diligent zal zijn. Dan neem ik aan dat het niet alleen de gewone overtredingen betreft die in het Wetboek van Strafrecht zijn geformuleerd, maar bijvoorbeeld ook inbreuken op het auteursrecht. U weet dat daarin ook strafbare feiten worden vermeld. Dat is niet bepaald iets waar het OM kennis van draagt en actief in optreedt. Juist dan komt zo'n ISP in die spagaat terecht met mogelijke schadeclaims.

Minister **Donner**: Óf het is een situatie die zich buiten het Openbaar Ministerie en het strafrecht om afspeelt. Dan kan inderdaad die spagaat ontstaan. Dan zullen wij aan de hand van de praktijk moeten bezien welke structuur daar het meest geschikt voor is. Óf het gaat wel om strafbare feiten maar het behoort niet tot het actieve opsporingsbeleid van het OM of de politie. Dan kan het door aangifte onder de aandacht van het OM worden gebracht. In die situatie is het denkbaar dat het OM van zijn bevoegdheid gebruik maakt. Dan zal hetzelfde argument gelden voor de internetprovider: er is een bevel van de overheid. Dan richten de claims zich tegen de overheid. Dat zijn wij wel gewend. Dat gebeurt regelmatig.

Voorzitter. Dan kom ik bij de opmerkingen over de formulering van artikel 138a Wetboek van Strafrecht. Dit is een bekend en al ouder punt. De formulering waarvoor gekozen wordt, is ruimer dan de formulering die nu in de wet staat. De huidige wet concentreert zich overigens niet alleen op het doorbreken van de beveiliging. Die indruk kreeg ik even door de woorden van de heer Franken, maar ik vermoed dat hij het niet zo bedoelde. Nu al staan er in de wet drie andere mogelijkheden van computervredebreuk, namelijk door een technische ingreep, een valse sleutel of het aannemen van een valse hoedanigheid. Tegen de achtergrond van die situatie is gekozen van de huidige formulering in het wetsvoorstel. Wellicht laat het Cybercrimeverdrag ons de mogelijkheid van de huidige invulling in de Nederlandse wetgeving, maar het Kaderbesluit maakt in artikel 2 heel duidelijk dat er ofwel voor dient te worden gekozen om alle vormen van hacken strafbaar te stellen, dus iedere vorm van het opzettelijk en onrechtmatig toegang verwerven – in reactie op mevrouw Broekers zeg ik: behoudens wanneer zulks onbeduidend is; het per ongeluk bij GroenLinks binnenlopen is wellicht onbeduidend als men daar niet blijft – ofwel voor het, volgens het tweede lid, strafbaar stellen van de inbreuk op beveiligingsmaatregelen en zodoende het plegen van computervredebreuk. Ten opzichte van de bestaande bepaling zou dit laatste derhalve een beperking opleveren.

Om die reden is voor deze verruiming gekozen: in het algemeen het opzettelijk en wederrechtelijk toegang krijgen tot een computer, met de enumeratieve opsomming dat in ieder geval de bestaande situaties daaronder moeten worden begrepen. Daarmee is voldaan aan het tweede beginsel van de Commissie Computercriminaliteit: de bepaling is minder techniekafhankelijk gemaakt, dus niet uitsluitend afhankelijk gemaakt van het doorbreken van beveiliging; in wezen vallen daaronder alle situaties van het opzettelijk en wederrechtelijk toegang verwerven tot een computer. Uiteraard kan dit bewijsrechtelijke problemen opleveren, maar dit is deels opgelost door in ieder geval de vier bestaande mogelijkheden te noemen. Deze systematiek is niet wezenlijk anders dan die de wet kent in het geval van huisvredebreuk. Natuurlijk bestaat die ook uit het opzettelijk en wederrechtelijk toegang verkrijgen, maar de aparte bepalingen over braak treden in werking als daarvan sprake is. Die systematiek is dus niet wezenlijk anders en deze bestaande bepalingen leken mij de juiste vorm om bij aan te sluiten. Ik geef toe dat bij gewone huizen een bord met ''Verboden toegang'' kan worden gezet en dat dit in dit geval moeilijk is. Maar ikzelf heb ook niet zo'n bordje op mijn voordeur en toch zal iemand die wederrechtelijk en opzettelijk door mijn geopende deur naar binnen komt, huisvredebreuk plegen. Hij pleegt geen braak, maar wel huisvredebreuk; hij doet dit immers opzettelijk en weet dat hij er niet in mag. Ik ben het eens met het uitgangspunt dat we niet de kat op het spek moeten binden, maar ik vind het te ver gaan om de regel om te keren en te stellen dat iedereen vrijelijk naar binnen mag als er geen beveiligingsmaatregelen zijn genomen; dat dit niet strafbaar is, zou immers de consequentie zijn. Ik meen de casus in dezen van mevrouw Broekers dus af te kunnen doen als onbeduidend; mevrouw De Wolff gaf al aan dat zij het niet als wederrechtelijk beschouwt omdat men daar welkom is.

De heer Franken vroeg naar de situatie in Frankrijk. Ook na onderzoek kan niet worden vastgesteld of Frankrijk een ontsleutelplicht heeft opgenomen op de wijze waarop wij dit doen. Ik weet wel zeker dat dit in het Verenigd Koninkrijk niet het geval is; daar komt men via een andere systematiek op hetzelfde resultaat uit. Ik ga er met de Kamer van uit dat de ontsleutelplicht niet wordt opgelegd aan de verdachte. Dat berust op artikel 19, vijfde lid van het Cybercrimeverdrag, dat uitdrukkelijk bepaalt dat de implementatie van de in het verdrag bedoelde bevoegdheden de waarborgen van onder andere artikel 15 van het verdrag in acht moet nemen. Een en ander betekent onder meer dat er een adequaat niveau van bescherming van mensenrechten moet zijn. In de toelichting op het verdrag is zelfs uitdrukkelijk vermeld dat dit onder meer het verbod van zelfincrimina-

tie betreft. Ik ga ervan uit dat in de andere Europese landen dus ook geen medewerkingverplichting kan worden opgelegd. Dit is echter niet altijd op dezelfde wijze gedaan als in Nederland, met zijn bepaling in de wet.

Verder werd uit het Dialogicrapport onterecht geconcludeerd dat er bij het tappen veel fouten worden gemaakt. De minister van Economische Zaken heeft mede namens de minister van Binnenlandse Zaken en mijzelf dit rapport aan de Tweede Kamer gezonden, voorzien van een reactie. In dit rapport wordt niet gesteld dat er veel fouten worden gemaakt; nee, in een voetnoot wordt geconstateerd dat er fouten worden gemaakt, vooral fouten die berusten op slordigheden. Het gaat immers om mensenwerk, er moeten nummers worden ingetikt, daarbij worden wel eens fouten gemaakt en wordt per ongeluk de verkeerde afgeluisterd. Mede omwille van het terugdringen van dit soort fouten proberen wij meer techniek toe te passen. Ik bestrijd echter dat in het rapport wordt vastgesteld dat er veel fouten worden gemaakt. Men heeft het van zegslieden en geeft uitdrukkelijk aan dat het niet verder is onderzocht. Het gegeven dat dit soort fouten worden gemaakt, is inderdaad reden om terughoudend om te gaan met het middel van afluisteren. Dat wordt dan ook gedaan. Het Openbaar Ministerie heeft de taak om hierin keuzes te maken. De bevoegdheid voorziet in voorwaarden voor de toepassing: zo dient er sprake te zijn van een misdrijf dat een ernstige inbreuk maakt op de rechtsorde, dient het belang van het onderzoek de toepassing hiervan dringend te vorderen en is een machtiging van de rechter-commissaris vereist. Ik zie geen reden om het beleid in dezen ten principale te veranderen. Nut en noodzaak van de bevoegdheid staan ook niet ter discussie. In de brief van 31 maart staat ons standpunt dat de interceptie van telecommunicatie van groot belang is voor de opsporing.

Wordt er gewerkt aan een aanvulling op het gebied van de rechtsmacht? Ik ben in eerlijkheid van mening dat de rechtsmacht op dit moment toereikend is geregeld. Er lijkt mij aanleiding voor aanvullingen van de rechtsmacht als er sprake van nieuwe technische ontwikkelingen zou zijn. De vraag naar de ontwikkelingen omtrent NHTC komt weldra aan de orde bij de beantwoording van de vragen van mevrouw Broekers, die daarover ook vragen stelde.

Mevrouw Broekers, u vroeg allereerst naar de wenselijkheid om termen als ''gegevens'' en ''geautomatiseerd werk'', gedefinieerd in het Wetboek van Strafrecht, ook in het Wetboek van Strafvordering te definiëren. Welnu, de oorzaak van de discrepantie is het feit dat de begrippen indertijd bij amendement in het Wetboek van Strafrecht zijn opgenomen, zonder dat het Wetboek van Strafvordering aan de orde was. Het hoeft evenwel geen problemen op te leveren. In de stukken gaf ik al aan dat het mij niet bekend is dat er problemen zijn ontstaan door het ontbreken van een aparte definitiebepaling in het Wetboek van Strafvordering. De begrippen worden kennelijk gehanteerd in de betekenis zoals die in het Wetboek van Strafrecht wordt gegeven. Tegelijkertijd ben ik het met u eens dat wij met oog op de systematiek moeten bezien of het nodig is om een gelijkluidende definitie op te nemen in het Wetboek van Strafvordering. Mag ik u toezeggen dat wij bij de algemene herziening van het Wetboek van Strafvordering zullen bezien of hiervoor aanleiding is en, zo ja, hoe het opgelost kan worden?

Er is veel kennis van zaken bij politie en justitie nodig om adequaat te kunnen optreden op dit terrein. De ontwikkeling van het internet gaat zo snel dat het langzamerhand een wezenlijk terrein van het maatschappelijk verkeer is geworden en dat betekent dat de politie en justitie over de nodige deskundigheid moeten beschikken om op te kunnen treden. Daarvoor is vooral nodig dat de kennis en vaardigheden van de recherche op orde worden gebracht om veel voorkomende vormen van ICT-criminaliteit te kunnen aanpakken. Daarnaast worden specialisten opgeleid voor ingewikkelder vormen van deze criminaliteit. Deze opleiding wordt verzorgd in het kader van het door de raad van hoofdcommissarissen opgestarte project Digitaal opsporen. Het is de bedoeling dat dit project in 2008 is afgerond. Door deze aanpak zal de politie steeds beter in staat zijn om bestaande en nieuwe vormen van criminaliteit op dit terrein op te sporen.

In antwoord op schriftelijke vragen van mevrouw Gerkens is de Tweede Kamer aangegeven dat ongeveer 190 gespecialiseerde rechercheurs bij de regionale korpsen werkzaam zijn en dat het KLPD beschikt over 56 digitale rechercheurs. De Politieacademie zal verder digitaal opsporen als een vast onderdeel opnemen in het onderwijs. Bij het Openbaar Ministerie en de rechterlijke macht blijven investeringen in kennis, deskundigheid en menskracht nodig. Dat is een continu proces, ook omdat de ontwikkelingen in ICT-techniek steeds verder voortschrijden. De verbreding en verdieping van de kennis van de politie is bij het Openbaar Ministerie en de rechterlijke macht ingezet als een onderdeel van de financiering van kennisontwikkeling in de begroting.

Op 18 mei heeft de staatssecretaris van Economische Zaken, mede namens de minister van Binnenlandse Zaken en mij, het eindadvies over de projecten NPAC en het National High-Tech Crime Center en de kabinetsreactie daarop naar de Kamer gestuurd. Onze drie departementen zullen dus gezamenlijk optreden. Zoals in de kabinetsreactie vermeld wordt het NHTCC als pilot afgesloten en de activiteiten daarvan bij het KLPD ondergebracht. In lijn met het uitgebrachte advies wordt een effectieve aanpak van cybercrime gevolgd langs de lijn van het ontwikkelen van een nationale infrastructuur voor het bestrijden van cybercrime. Daardoor moet er meer samenhang komen bij de bestrijding ervan. Uiteraard vereist dat niet alleen kennis, maar ook een professionele aanpak. Verder zal de samenhang tussen lokale, regionale, bovenregionale en nationale aanpak moeten worden versterkt. Voor een uitgebreidere toelichting op de door ons voorgestane aanpak verwijs ik naar de brief.

De minister van Binnenlandse Zaken en ik bezien op dit moment hoe het na 2006 op hoofdlijnen verder moet met het Veiligheidsprogramma. Cybercrime en de mogelijkheden van politie en justitie op het internet zullen daarvan een wezenlijk onderdeel uitmaken.

Mevrouw Broekers vroeg mij of het voorgestelde artikel 125o aan de zittingsrechter de bevoegdheid moet geven om strafbare gegevens uit het systeem te laten verwijderen. Ik ben blij dat zij al tijdens haar interventie instemde met het zowel praktische als juridische antwoord dat op dit punt gegeven is. Uit de reactie van het Openbaar Ministerie heb ik begrepen dat de gekozen opzet bevredigend kan werken, niet in de laatste plaats

omdat in noodgevallen de officier van justitie ook in de zittingsfase het bevel kan geven om gegevens te verwijderen.

Mevrouw De Wolff vroeg mij wat wordt bedoeld met: de spulletjes die gebruikt moeten worden bij de voorbereiding. Ik dacht dat er gesproken was van programma's of voorwerpen. De bepaling op dat terrein kent een dubbele sleutel. Het gaat daarbij vooral om computerprogramma's die hoofdzakelijk zijn bedoeld om mee te hacken. Het programma als zodanig moet daar echter niet alleen op gericht zijn, maar het moet ook het oogmerk van de verkoper zijn om een programma te verkopen dat gebruikt kan worden om te hacken. De verkoper mag dus niet zeggen: u moet het vooral niet doen, maar dit hackprogramma is wel heel leuk voor uw verzameling programma's die u nooit mag gebruiken. Daardoor zou de situatie kunnen ontstaan waarvoor geldt: dat is niet het oogmerk. In andere gevallen is er dus wel die dubbele sleutel.

De Hoge Raad is overigens in een vergelijkbare situatie met betrekking tot de uitleg van artikel 326c, tweede lid tot de conclusie gekomen dat degene die een stappenplan publiceert voor een succesvolle inbraak, strafbaar is, omdat voldaan is aan de omschrijving dat men het liet geworden, dan wel dat men het bevorderde. De term die nu wordt voorgesteld, houdt in dat daarmee een misdrijf als bedoeld wordt gepleegd. Als wij het terugdraaien van een kilometerteller strafbaar zouden stellen, dan zou een programma dat specifiek bedoeld is om de kilometerteller terug te draaien ook hieronder gebracht kunnen worden. Dat soort inbrekersmateriaal wordt op dit moment inderdaad soms verkocht.

Voorzitter. Ad finire. Ceterum censeo obligationes Unitatis Europeae esse implementanda. Pacta sunt servanda!

□

De heer **Franken** (CDA): Voorzitter. Ik bedank de minister voor zijn uitvoerige en duidelijke beantwoording.

De discussie over al dan niet techniekonafhankelijke formuleringen bij artikel 54a van het Wetboek van Strafrecht is nog lang niet afgelopen. De minister spreekt namelijk van ''doorgifte'' en ''opslag'' en dat lijken activiteiten te zijn. Dat zijn ze ook in de reële wereld, maar het internet is een virtuele wereld waar dergelijke onderscheiden eigenlijk niet meer gemaakt kunnen worden. Het probleem zit vooral in het civiele recht omdat de richtlijn voor e-commerce onderscheid maakt tussen de activiteiten ''mere conduit'', ''cashing'' en ''hosting''. Die lopen echter ook door elkaar, want deze verschillen vervagen. Het is geen urgent probleem, maar wij zullen hier wel diligent mee om moeten gaan omdat hier ook wat kan gebeuren.

Op het punt van de huisvredebreuk en de computervredebreuk hebben wij wat langs elkaar heen gesproken. Natuurlijk kunnen wij alleen maar denken in de reële wereld en is het voor een mens noodzakelijk om te denken in modellen om de gedachten te kunnen bepalen. Tegen die beperking lopen wij nu eenmaal aan. Huisvredebreuk is in dat opzicht een goed aanknopingspunt; als de deur openstaat, mag iedereen naar binnen behalve als, via een bordje of een persoonlijk woord, de toegang wordt ontzegd. Als de deur netjes gesloten is, dan kan men alleen door braak, tegen de verklaarde wil van de bewoner, naar binnen komen. Hoe staat het echter bij computervredebreuk? Het woord is modelmatig geënt op de realiteit. Waarom een beveiliging als voorwaarde voor strafbaarheid? Waarom is iemand alleen strafbaar als hij zich van een technische ingreep bedient zoals valse signalen of een valse sleutel, of als hij een valse hoedanigheid aanneemt? Die punten van a tot en met d, genoemd door de minister, zijn als voorwaarden voor strafbaarheid geformuleerd. Internet is in beginsel openbaar. Als iemand geen ongewenst bezoek in een deel van het systeem wil, dan moet hij zijn deur sluiten voor degenen die geen uitdrukkelijke toestemming hebben. Toegang verkrijgen kan alleen door het nemen van een technische maatregel. Het is onmogelijk om te zeggen: iedereen mag naar binnen, behalve mijnheer A. Er moet dan met toegangscodes worden gewerkt die aan geautoriseerden worden toegekend. Die valsheid is van belang om het omzeilen van een beveiligingsmaatregel strafbaar te stellen als een noodzakelijke aanvulling. Overigens zijn het aannemen van een valse hoedanigheid, het hanteren van een valse sleutel of het geven van valse signalen ook maatregelen om een beveiliging te doorbreken. Het lukt immers schijnbaar niet om zomaar binnen te komen; daarvoor moet een speciale handeling worden uitgevoerd. Als de deur niet op slot zit, dan is braak onnodig en is een valse sleutel niet aan de orde.

Natuurlijk kunnen wij dit wetsvoorstel niet amenderen. Ik zou het echter plezierig vinden als de minister de toezegging doet dat het Openbaar Ministerie in beginsel alleen computervredebreuk vervolgt als er een beveiliging wordt doorbroken of toegang wordt verworven door een technische ingreep met behulp van valse signalen, een valse sleutel of het aannemen van een valse hoedanigheid. Het gaat niet slechts om ''wilfull intent'' omdat die naar mijn mening in de virtuele wereld niet bewijsbaar is. Als dat wel het geval was, dan zullen er heel wat vrijspraken voorkomen wegens gebrek aan bewijs. Ik meen dat het voorkomen van veel vrijspraken slecht is voor de rechtsorde.

De minister stelt dat het punt van de rechtsmacht op dit moment toereikend geregeld is. Ik meen dat dat betrekkelijk is. Ik vraag de minister of hij de bevoegdheid van de Nederlandse rechter in dit verband via het ubiquiteitsvereiste wil laten lopen. Als iedere rechter zichzelf bevoegd mag achten, ontstaan er gevallen van dubbele strafbaarheid. Bovendien speelt dan de vraag welke rechter het eerst aan zet is, want zijn recht wordt toegepast en zijn straf wordt geëxecuteerd.

De minister is zijn beantwoording geëindigd met de verzuchting: ''pacta sunt servanda.'' Ik breng niet de lenigheid van geest op om daarop in het Latijn te variëren. De minister dient op een zeker moment met implementatie van dat pact te komen en mijn verzuchting duidde erop dat hij dat zo minimaal mogelijk moet doen.

□

Mevrouw **Broekers-Knol** (VVD): Voorzitter. Ik dank de minister voor zijn beantwoording van de vragen. De toezegging van de minister op de vraag van mijn fractie om de definitie van gegevens en geautomatiseerd werk ook op te nemen in het Wetboek van Strafvordering is in die zin gehonoreerd dat het punt wordt meegenomen bij de algehele herziening van het Wetboek van Strafvordering. Die toezegging is voor mijn fractie voldoende.

Broekers-Knol

Ten aanzien van de andere vraag van mijn fractie merk ik op dat de ontwikkeling van een nationale infrastructuur voor het bestrijden van cybercrime het vertrouwen geeft dat er hard wordt gewerkt om de deskundigheid op dit terrein bij de opsporing te optimaliseren. Dat is ook belangrijk.

Ik had gedacht dat ik vandaag mijn ''one moment of fame'' zou meemaken en dat ik geboeid dit gebouw zou verlaten als computercrimineel. Dan zou ik ook een keer in de krant zijn gekomen en dat was best heel aardig geweest. Helaas is mijn onopzettelijk elektronisch binnenlopen bij GroenLinks door de minister betiteld als onbeduidend. Hoewel mevrouw De Wolff het blijkbaar ook onbeduidend vond, had het veel erger kunnen aflopen. Ik heb echter geen handboeien om en zal rustig het pand kunnen verlaten.

De vergadering wordt geschorst van 16.02 uur tot 16.06 uur.

□

Minister **Donner**: Voorzitter. Ik dank u dat u mij even toestond om de zaal te verlaten.

De heer Franken is op twee punten teruggekomen, in de eerste plaats op het punt van doorgifte en opslag. Op zichzelf ben ik het met hem eens dat die twee activiteiten bij bepaalde technieken nauwelijks meer te onderscheiden zijn. Dat acht ik echter geen reden om te constateren dat de bepaling techniekafhankelijk geworden is. Nee, er is bewust voor gekozen om in die bepaling te spreken van zowel doorgifte als ook opslag, omdat er in de praktijk vaak niet meer te onderscheiden is, welke van de twee men bedoelt. Laat de heer Franken ervan verzekerd zijn dat wij tegen de achtergrond van die ontwikkelingen zullen nagaan of daardoor bepaalde begrippen zoals wij die in de wet hebben als het alleen over opslag gaat of alleen over doorgifte, niet hun betekenis verliezen. Dat is een terecht punt. Naar mijn mening is artikel 54 van de Wetboek van Strafrecht daar geen goed voorbeeld van, omdat daarin juist weer opslag én doorgifte worden gebruikt.

Ten aanzien van punt twee constateert de heer Franken terecht dat het gebruik van de analogie als zou inbreuk op internet vergelijkbaar zijn met huisvredebreuk en het onrechtmatig betreden van huizen net zoals iedere analogie zo zijn beperkingen kent. Ik zei al eerder dat de uitvoering van het kaderbesluit een van tweeën vergde: of een beperking tot het doorbreken van een beveiliging of via uitleg aangeven dat de vormen die wij eerder in de wet daarnaast onderscheiden hebben, daaronder begrepen waren. Naar mijn mening was dat een veel moeilijkere operatie geweest dan de oplossing die wij nu gekozen hebben, namelijk constateren dat het gaat om het brede verschijnsel van de opzettelijk en wederrechtelijke betreding. Ik ben het met de heer Franken eens dat de bewijslast zeer hoog is als het OM, los van de vier gevallen waarin er per definitie sprake is van computervredebreuk, moet bewijzen dat die vier figuren zich niet voordoen en er dan toch sprake is van opzettelijk en wederrechtelijk betreden van de computer. Ik kan echter niet op voorhand uitsluiten dat die figuren zich mede door ontwikkelingen in de techniek kunnen gaan voordoen. Er is nu gekozen voor de minder techniekafhankelijke oplossing om het mee te nemen, maar het OM zit echt niet te wachten op werk en het gaat echt niet regelmatig over tot vervolging in gevallen waarin het weet dat het in bewijsmoeilijkheden zal komen. Als het OM dat een keer doet om een proefproces uit te lokken en het krijgt nul op rekest, dan gaat het echt niet systematisch door met precies hetzelfde. Ik wil dan ook niet toezeggen dat ik het OM een aanwijzing geef voor dit soort specifieke gevallen. Ik ga ervan uit dat men bij het OM zijn verstand gebruikt en tot nu toe ben ik niet beschaamd in dat vertrouwen.

Verder wijst de heer Franken op het probleem van de rechtsmacht. Zoals het nu geregeld wordt – dat is in wezen de substantie van wat ik heb willen zeggen – is de regeling bevredigend. Dat betekent niet dat in de huidige situatie met het verschijnsel internet meer staten rechtsmacht kunnen claimen. Binnen de Europese Unie en breder zijn wij ideeën aan het ontwikkelen over de vraag wat de meest passende jurisdictie is om bepaalde vergrijpen aan te pakken. Als het gaat om internet, heb ik liever een situatie waarin er gelijktijdig meerdere staten bevoegd zijn, dan dat er eerst gestreden moet worden over de vraag welke staat bevoegd is en dat er vervolgens maar afgewacht moet worden of de staat die bevoegd is, ook tot vervolging overgaat. In dat opzicht is een zekere overkill – als ik mij deze Engelse term mag permitteren – mijns inziens beter om misbruik van internet tegen te gaan dan andersom. Als het aan de orde komt, neem ik het gaarne mee. Op dit moment is de vraag eerder hoe wij ervoor kunnen zorgen dat alle staten in gelijke mate aandacht besteden aan het gebruik van internet. Het is niet zo dat ik een gedrang constateer van overheden die allemaal hun eigen jurisdictie willen toepassen.

Ik geloof dat mevrouw Broekers mij geen vragen meer stelde, maar zaken constateerde. Zij aanvaardde mijn toezegging om het punt van de definities mee te nemen bij de algemene herziening en vond het jammer dat ik haar casus helaas onbeduidend vond. Als zij het een paar keer herhaalt, wil ik best bekijken of ik het serieuzer kan nemen.

Ten slotte beantwoord ik de slotopmerking van de heer Franken met ''pacta sunt servanda non solum litterae sed in spiritu''.

De beraadslaging wordt gesloten.

De wetsvoorstellen worden zonder stemming aangenomen.

De vergadering wordt van 16.15 uur tot 17.30 uur geschorst.

Aan de orde is de voortzetting van de behandeling van:
- **het wetsvoorstel Wijziging van artikel 7.10 (arbeidsovereenkomst) van het Burgerlijk Wetboek met betrekking tot het concurrentiebeding (28167).**

De beraadslaging wordt hervat.

□

Minister **Donner**: Voorzitter. Er is veel gezegd door verschillende leden over dit wetsontwerp. Er is zelfs enigszins gezinspeeld op een mogelijke uitkomst van de besluitvorming op dit punt. Toch wil ik proberen om de