non-discriminatoire toegang tot netwerken voor dienstaanbieders. Dat is wettelijk vastgelegd, zodat er geen wettelijk probleem is. Dat er in de praktijk een probleem is, daarover zijn wij het eens. Ik doe daarover straks ter afsluiting een voorstel.

De heer **Hessels** (CDA): Buiten het feit dat ik het jammer vind dat de energierichtlijn en de telefonie-richtlijn niet andersom zijn geregeld – de minister zal dat begrijpen van mij – vraag ik hem of ik het juist zie dat het verzoek in de motie volgens de Europese richtlijn wel mogelijk is. Als er aanmerkelijke marktmacht is, kan dat wat in de motie wordt gevraagd worden geregeld.

Minister **Brinkhorst**: Dan is dat door de toezichthouder af te dwingen. Dat is iets anders dan dat er nadere wetgeving nodig is.

Met de heren Hessels en Van Dam ben ik van mening dat wij maatregelen moeten treffen die zo snel mogelijk effect hebben. Mijn vrees is echter dat een wetgevingstraject verhindert dat wij nog voor 1 januari aanstaande maatregelen kunnen nemen. Dat is wat ik bedoelde met mijn opmerking ''inductief/deductief''. Ik wil liever een begaanbare weg hebben die zo snel mogelijk tot resultaat leidt, dan dat de sector zich ingraaft, waardoor het proces eerder wordt opgehouden. Zodra ik bericht heb van de NMa, zal ik een te volgen pad aangeven, zowel voor de tarieven als voor de conclusies uit het NMa-onderzoek. Verder zal ik ingaan op het antwoord van UPC. Casema heeft verklaard de tarieven vanaf 1 januari niet te zullen verhogen. We hebben dan een samenhangend pakket, dat ik de Kamer uiterlijk half oktober voor zal leggen. Het feit dat Kamer en regering gezamenlijk vinden dat er op deze markt wat moet gebeuren, geeft naar mijn gevoel voldoende druk op de Opta, de NMa en de kabelaars. Zij weten dan wat er boven hun hoofd hangt als er geen nadere maatregelen kunnen worden getroffen. De grote hoeveelheid moties geeft één ding duidelijk aan: de situatie die dreigt te ontstaan voor de consumenten is niet aanvaardbaar. We moeten niet vergeten dat Nederland het enige land binnen de EU is met een dichtgeschroeide kabelmarkt en een parallelsysteem, zoals dat van KPN. De verhalen die de leden nu houden over de kabel, hadden zij een tijdje geleden kunnen houden over KPN, maar dat is toen niet gebeurd. Wij moeten ervoor zorgen dat er een balans blijft bestaan.

De beraadslaging wordt gesloten.

De **voorzitter**: Ik stel voor, de dinsdag na prinsjesdag te stemmen over de ingediende moties.

Daartoe wordt besloten.

De vergadering wordt van 16.45 uur tot 19.00 uur geschorst.

Aan de orde is de 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).**

De algemene beraadslaging wordt geopend.

□

Mevrouw **Gerkens** (SP): Voorzitter. Sommigen gaat de cyberwereld de pet te boven. Toch is er niets nieuws onder de cyberzon, ook niet op het gebied van de criminaliteit. Het zou naïef zijn om te denken dat criminelen niet digitaliseren en de rest van de wereld wel. De SP is er dan ook blij mee dat wij vandaag over de implementatie van het verdrag kunnen spreken.

Ik onderscheid drie verschillende vormen van cybercrime: oude wijn in nieuwe zakken, oude wijn met behulp van nieuwe zakken en nieuwe wijn. Bij de oude wijn in nieuwe zakken zien wij de bekende criminaliteit digitaal uitgevoerd. Hieronder versta ik zaken zoals fraude, fishing, oplichting, afpersing en dergelijke. Oude wijn met behulp van nieuwe zakken is criminaliteit waarbij gebruik wordt gemaakt van ICT. Ik denk hierbij aan kinderporno en terrorisme, maar ook aan bouwfraude-zaken, et cetera. De nieuwe wijn is direct gerelateerd aan ICT. Ik geef hierbij hacking en DOS attacks als voorbeeld. Criminele activiteiten mogen niet, ook niet op het internet, een gewone pc of een Macie. Wij moeten dat dus aanpakken en onze wetgeving hierop aanpassen.

Ik ben blij dat de implementatie van het verdrag nu eindelijk voorligt. Het zou een eufemisme zijn om te zeggen dat het even heeft geduurd, want het heeft veel te lang geduurd. Als gevolg daarvan lopen wij dan ook achter de feiten aan. Niet alleen wij, maar ook de mensen in Nederland die geconfronteerd worden met computercriminaliteit, zijn daar de dupe van. Daar zit mijns inziens een vreemde discrepantie met het streven een digitale samenleving te zijn. Aan de ene kant promoten wij breedband en on line zijn van jong tot oud, maar aan de andere kant geven wij ruim baan aan de criminele randverschijnselen van dit instrument. Zo kunnen jonge kinderen onwetend begluurd worden door hun webcam, krijg ik nog steeds mailtjes van verontwaardigde vaders die als resultaten van googlen op het woord ''poesjes'' ten behoeve van een spreekbeurt van de dochter meer zien dan alleen de katachtigen en lopen de pc's van de ouderen vast door spyware, virussen en pop-offs. Daarnaast komen er steeds vaker berichten over het hacken van de Wehkampgegevens of, zoals onlangs, van ziekenhuisinformatie en over diefstal van creditcardgegevens. Ook ik heb ze gehad: de IB- en Postbank-fishmails, evenals de gewonnen cruise op mijn antwoord-apparaat. En u ziet het: ik ben nog niet op vakantie.

De toename van dit soort incidenten geeft aan dat wij achter de feiten aanlopen, maar draagt ook het risico in zich dat het vertrouwen in de digitale samenleving afneemt en dat is niet bevorderlijk voor de ontwikkeling ervan. Strafbaar stellen is goed, maar een regelmatige herziening van de wet zal nodig blijven om bij te blijven, net zoals het essentieel blijft om mensen te informeren over deze gevaren, zodat zij zich kunnen weren. Ik vind dat die verantwoordelijkheid ook bij de gebruiker van de cyberspace zelf ligt. Aan die informatie schort het. Ik vind dat dit kabinet veel te weinig verantwoordelijkheid neemt voor het informeren van gewone gebruikers van internet over de gevaren die er zijn. Ik heb daar meermalen bij het kabinet op aangedrongen. Ik zie de minister kijken. De vragen zijn in het verleden natuurlijk aan zijn collega van Economische Zaken gesteld. Mijn fractie is van mening dat de overheid aan de burgers op dit moment te weinig informatie geeft

over de manieren waarop zij zich kunnen weren tegen criminele activiteiten en het veilig maken van hun computer. Het is een tijdelijk gat dat wij moeten dichten. Ik besef terdege dat nu een nieuwe generatie opgroeit die waarschijnlijk meer weet dan wij allen in deze Kamer bij elkaar. Als je wilt dat ouders jongeren goed begeleiden, is het goed om ervoor te zorgen dat de ouders weten wat hun kinderen tegen kunnen komen als ze gaan googlen op een woord als ''poesjes''. Gaat het kabinet die verantwoordelijk nu eindelijk nemen?

Bij het actualiseren van onze wetgeving moeten wij ook ons opsporingsapparaat updaten. Wij moeten ervoor zorgen dat wij net zo slim zijn als degenen die de wet overtreden, of liever nog slimmer, maar daar schort het aan. Ik heb de minister meermalen schriftelijk gewezen op de bijzonder trage wijze waarop de vervolging van de DDoS-aanval op de overheidssites heeft plaatsgevonden. Een ander voorbeeld, dat onlangs in het nieuws was, is de aanval op de chat van Máxima en Willem-Alexander.

Dit zijn de meest zichtbare gevallen, maar wij weten dat er veel meer in cyberspace gebeurt dan wij op dit moment kunnen volgen en vervolgen. Wij hebben de regering er meermalen op aangesproken dat de opsporing beter kan en moet. Er is onvoldoende aandacht voor de grote schade die door computercriminaliteit wordt aangericht. Ik denk dan niet alleen aan die DDoS-aanvallen, maar ook aan phishing, creditcard-fraude of hackers die samenwerken met criminelen.

Heeft de minister cijfers over de oplossingspercentages van dergelijke criminaliteit? Klopt het dat er een aanzienlijke stijging is van deze criminaliteit, maar dat deze onvoldoende wordt geregistreerd? Sterker nog, dit wordt nauwelijks erkend als echte criminaliteit. Ik heb een voorbeeld van iemand die was opgelicht op internet en die naar de politie ging, maar daar kon de aangifte niet worden opgenomen, omdat fraude op internet niet bestaat. Dat moet echt niet kunnen. Wie doet er aangifte, als hij of zij een virus krijgt? Wie heeft er ooit geld verloren door geld te storten naar aanleiding van een mail van een prins uit Afrika?

Projecten zoals het National High-Tech Crime Center verdienen meer ondersteuning en de expertise bij de politie op dit vlak dient sterk verbeterd te worden. De minister van Justitie, met wie wij de implementatie van het Cybercrimeverdrag en andere maatregelen voor het bestrijden van cybercriminaliteit bespreken, heeft naar de mening van de SP nog zeer veel in te halen op dit vlak. Graag hoor ik vandaag van de minister hoe de opsporing en vervolging van deze criminaliteit wordt vormgegeven.

De daadwerkelijke opsporing en vervolging van cybercriminelen, zoals fraudeurs, hackers en dossers, moet worden opgevoerd. Er wordt een imposante lijst van nieuwe bevoegdheden gecreëerd, maar de minister heeft nog niet laten zien dat hij de bestaande mogelijkheden effectief gebruikt. Komt er meer expertise op het gebied van cybercrime bij de politie? Wordt het National High-Tech Crime Center na dit jaar gecontinueerd? Wordt de opsporing en vervolging van cybercrime, die eind vorig jaar bij het ministerie van EZ was ondergebracht, in het vervolg wel aangepakt? Kan de minister hierop ingaan?

Bij de wet zelf is het eerste punt de bevriezing van de gegevens. Het voorstel is dat de officier van justitie kan vorderen dat de gegevens een tijd worden vastgehouden, tot maximaal 90 dagen, als er een redelijke verdenking tegen iemand is. Mijn partij heeft in eerdere debatten met de minister voorgesteld om dit te zien als een alternatief voor de bewaarplicht, waartegen in de Tweede Kamer en in het Europees Parlement heel veel verzet is. Terwijl de bewaarplicht inhoudt dat gegevens van 450 miljoen merendeels onschuldige burgers worden opgeslagen, kunnen bij de bevriezingsorder selectief gegevens worden gepakt die alleen betrekking hebben op verdachten. De minister is hierover niet enthousiast. Hij zegt dat hij niet zoveel heeft aan een bevriezingsmaatregel. Mijn vraag is waarom hij deze dan wel in wetgeving wil omzetten. Het is onzinnig om allerlei maatregelen voor te stellen, te bespreken en tot wet te verheffen, als zij onbruikbaar zijn. Graag hoor ik hierover wat uitleg.

Ik worstel in het bijzonder met de omschrijving van het begrip ''georganiseerde misdaad'' in het wetsvoorstel. Toen ik sprak van oude wijn met behulp van nieuwe zakken, duidde ik onder andere op dit probleem. Door de digitalisering van de criminaliteit is het steeds eenvoudiger om wereldwijd met één persoon te doen waar vroeger een heel netwerk voor was. In de virtuele wereld is de term ''georganiseerd'' een achterhaald begrip voor de opsporing. Ziet de minister dit dilemma ook? Hoe denkt hij daarmee om te gaan? Gelden de bijzondere opsporingbevoegdheden bij het onderzoek naar een georganiseerd verband ook wanneer een zwaar misdrijf door één persoon wordt gepleegd? Ik denk dat wij de term ''georganiseerde misdaad'' in de digitale omgeving wellicht moeten herdefiniëren. Ik hoor daar graag een reactie op van de minister.

Voordat ik inga op een aantal kleine technische vragen, maak ik een opmerking over iets waarnaar ik al vaker heb gevraagd. Wij hebben te maken met een toename van pogingen tot diefstal van gegevens van bedrijven, overheid en organisaties. Ik ben van mening dat iedereen het recht moet hebben om op de hoogte gesteld te worden, wanneer zijn of haar gegevens zijn gestolen. Als wij dat wettelijk vastleggen, zullen bedrijven zich verantwoordelijk voelen voor de gegevens, want dat doen zij nog steeds veel te weinig. Het kan voor een bedrijf immers behoorlijk wat schade aanrichten als het iets dergelijks aan zijn klanten bekend moet maken. Dat bedrijf zal dus ook voorzichtiger met die gegevens omgaan. Daarnaast kan de persoon wiens gegevens zijn gestolen, beter controleren op welke wijze hiervan misbruik wordt gemaakt. Vervolgens heeft hij de mogelijkheid om adequaat te handelen. Het is bijvoorbeeld mogelijk om de creditcard te blokkeren op het moment dat er een mailtje binnenkomt met de mededeling dat zijn gegevens zijn gekraakt. Als bijvoorbeeld duidelijk is dat zijn bankrekeningnummer bij bepaalde personen bekend is, kan hij de automatische afschrijvingen beter in de gaten houden. Ik vraag de minister nogmaals om wetgevingsvoorstellen aan de Kamer voor te leggen, zoals die in de VS.

De SP-fractie is van mening dat de provider niet mag worden vervolgd voor het verspreiden van virussen door anderen via zijn server. Hetzelfde geldt als hackers voor hun werkzaamheden gebruikmaken van zijn server en ook voor andere

overtredingen waarin hij feitelijk geen aandeel heeft. Als een moordenaar een moord pleegt met een wapen uit een bepaalde winkel, treft de winkeleigenaar ook geen blaam, tenzij laatstgenoemde incorrect heeft gehandeld bij de verstrekking daarvan. Is dat overeenkomstig dit wetsvoorstel, of moeten providers hun klanten scannen?

Hoe stelt de minister zich opsporingsonderzoek voor zonder toestemming van de eigenaar van de server of netwerker? Er is een voorstel gedaan om het mogelijk te maken om IP-nummers mondeling door te geven. Komen die nummers wel goed over via de telefoon, of is dat een kwestie van wachten op fouten? Zouden wij dat niet anders moeten doen?

De voorgestelde dwangmiddelen staan los van de strafmaat. Waarom kiest de minister er juist voor om in deze gevallen mensen beter en langer vast te houden? Zijn hackers dan buitengewoon vluchtgevaarlijk?

Voorziet artikel 139b ook in de situatie waarin de pleger het werk door andere personen, bijvoorbeeld opdrachtgevers, of computernetwerken laat doen? In artikel 232 wordt ingegaan op het gebruik van passen. Op welke passen doelt de minister, behalve de betaalpassen? Moeten wij die passen niet uitbreiden met chips en biometrische gegevensdragers? Die vraag stelt mijn fractie ook ten aanzien van andere specifieke omschrijvingen van de technieken en de apparatuur. Wij maken die wetgeving op die manier enorm gevoelig voor de tijdgeest. Daardoor wordt de kans groter dat wij steeds meer achter die feiten aanlopen. Wil de minister het wetsvoorstel nog eens bestuderen op die specifieke tijdgevoelige gegevens en met verbetervoorstellen komen?

Ik heb een amendement ingediend om ervoor te zorgen dat ook personen strafbaar zijn die werkzaam zijn bij financiële instellingen en die gegevens doorgeven. In het wetsvoorstel staat dat dit alleen zal gelden voor telecomorganisaties. Wij constateren dat er in de wereld sprake is van een toename van identiteitsdiefstal. Dat is zeker het geval als het om creditcards gaat. Financiële instellingen zijn daarvoor ook heel gevoelig. Ik vermoed dat Nederland wat dat betreft niet zal achterblijven, als het daaraan al niet meedoet.

Kort gezegd, komt het erop neer dat de SP-fractie van mening is dat wij criminaliteit geen voorsprong moeten geven. Op het internet dreigt dat echter wel te gebeuren. Justitie en politie zullen hun achterstand snel moeten inhalen om te voorkomen dat dit voorstel tot wetswijziging een papieren tijger zal zijn. Wij staan al op achterstand en geven daarmee zowel binnen als buiten de virtuele wereld te veel ruimte aan oplichters, bedriegers en zware misdadigers. Na vandaag is het werk niet afgelopen. Ik verzoek de minister met klem om de vinger aan de pols te houden en de wet regelmatig aan te passen aan de actualiteit. Onze samenleving verandert snel en criminelen maken graag gebruik van mazen in de wet. Het is de taak van de minister om die mazen zo snel mogelijk te dichten. Daarnaast is het de taak van de overheid om mensen te informeren, zodat zij zelf snel de nodige maatregelen kunnen nemen. Mensen hebben nog te vaak het idee dat cybercriminelen stoute jongetjes zijn die willen laten zien hoe goed zij kunnen hacken en dat het downloaden van muziek nu eenmaal iets is van deze tijd. Deels is dat waar, maar zij beseffen te weinig dat er grote criminelen naast hen zitten die daarmee geld verwerven voor heel andere zaken, ook bij de piraterij. Als wij misdadigers, kinderporno, terrorisme en fraude echt willen aanpakken, kunnen wij niet meer om die cyberwereld heen. Die wereld is nu eenmaal anders dan de wereld die wij kennen. Die vraagt om een andere benadering en om veel creativiteit. Ik geef de Kamer en het kabinet dan ook mee dat het noodzakelijk is om steeds opnieuw aandacht te besteden aan de vraag welke wijn wij uit welke zak drinken en hoe die smaakt. Dat is de enige manier om met dit dilemma te kunnen omgaan.

□

De heer **Van der Staaij** (SGP): Voorzitter. In hoofdlijnen kan mijn fractie zich prima vinden in het wetsvoorstel dat wij vandaag behandelen. Het is een vervolg op de Wet computercriminaliteit en omvat een aanpassing van het Wetboek van Strafrecht en het Wetboek van Strafvordering aan de nieuwe ontwikkelingen in de informatietechnologie. Ik zeg direct maar in het begin dat mijn bijdrage veeleer een welwillende steunbetuiging dan een heel kritische bevraging van het wetsvoorstel zal bevatten.

Het wetsvoorstel heeft inmiddels een lang traject achter zich. Het oorspronkelijke wetsvoorstel is al in 1998 ingediend. De behandeling schoot echter in de vertraging, omdat een bepaling over de aansprakelijkheid van internetproviders volgens de Europese Commissie in strijd was met een richtlijn. Dat belangrijke onderdeel is er toen uit gehaald en is aangehangen bij de Aanpassingswet richtlijn inzake elektronische handel. Vervolgens ontstond verdere vertraging door de beslissing om noodzakelijke wijzigingen ten gevolge van het Cybercrimeverdrag mee te nemen, maar ik zeg daar direct bij dat wij met de tweede en derde nota van wijziging een wetsvoorstel hebben gekregen dat wel degelijk bij de tijd is gebracht. Je kunt dus bepaald niet zeggen dat het sinds 1998 helemaal stil is geweest. Die vertraging is dus niet voor niets geweest. Het wetsvoorstel bevat ook de belangrijke implementatie van het Cybercrimeverdrag.

Ik vestig nog wel even de aandacht op het feit dat de goedkeuringswet van het Cybercrimeverdrag eigenlijk niet bij deze plenaire behandeling is geagendeerd, maar later in de week als hamerstuk op de agenda staat. Er is echter natuurlijk wel een inhoudelijke nauwe samenhang. Zaken die nu hier spelen, raken nadrukkelijk ook de inhoud van het Cybercrimeverdrag en de goedkeuring daarvan, zoals ik ook merkte bij bepaalde punten die mevrouw Gerkens aan de orde stelde. Ik hecht eraan om duidelijk te maken dat de SGP-fractie zeer positief staat tegenover de goedkeuring van het Cybercrimeverdrag, omdat daarmee een belangrijke stap wordt gezet in de internationale samenwerking die nodig is om de high-techcriminaliteit op een effectieve manier aan te kunnen pakken.

''Een stap ter hemel en een stap ter hel'' werd gezegd na de uitvinding van de boekdrukkunst. Hetzelfde zou je ook kunnen zeggen van de huidige digitalisering van onze samenleving. Enerzijds is er een snelle en massale informatie-uitwisseling door het verspreiden en delen van kennis en wetenschap via

internet. Dat zijn dus allerlei heel nuttige toepassingen. Anderzijds zijn er heel veel pulp, opruiend materiaal en cyberterrorisme. Dit wetsvoorstel bevat een aantal zeer bruikbare handvatten om de negatieve kanten van de digitalisering in te dammen. Dat vinden wij een goede zaak.

Ik wil nu geen uitvoerige beschouwingen wijden aan de bestrijding van hightechcriminaliteit en alles wat daarvoor nodig is. Dan heb ik het zowel over de misdaden met ICT als doelwit als over meer traditionele misdaden die worden verricht met ICT. Het is duidelijk dat het door de combinatie van de technische complexiteit, het internationale karakter, de snelheid en variëteit van bepaalde vormen van de hightechcriminaliteit, maar ook de veelvuldigheid van bepaalde vormen een grote opgave is om deze vorm van criminaliteit effectief aan te pakken en dus om waar te maken wat ooit, ongeveer zeven jaar geleden, in het debat over wetgeving op de elektronische snelweg in deze Kamer als eenvoudige vuistregel werd geformuleerd: ''wat off line geldt, moet ook on line gelden''; de wetgeving en de handhavingsinzet moeten daarop gericht zijn.

Een geregelde aanvulling van de gereedschapskist om de digitale criminaliteit aan te pakken is hard nodig, maar voor een effectieve aanpak is veel meer nodig. Het is ook van groot belang dat er voortdurend wordt geïnvesteerd in het verkrijgen van een helder beeld van vorm en omvang van digitale criminaliteit en dat bijvoorbeeld ook sprake is van een proactieve surveillance, zodat niet alleen wordt gereageerd op zaken die aan het licht worden gebracht door anderen dan politie en justitie. Ik beklemtoon dat ICT niet alleen een probleem is, maar ook kan helpen bij de oplossing. Bijvoorbeeld bij de bestrijding van terrorisme is het van groot belang dat, juist met gebruikmaking van ICT-middelen, vroegtijdig gesignaleerd kan worden wanneer internet gebruikt wordt voor communicatie, informatie-uitwisseling, planning, training, fondsenwerving en dergelijke. Het is dus ook van belang om juist de mogelijkheden van ICT goed te benutten in het kader van opsporing en vervolging.

Na deze algemene opmerkingen keer ik terug naar de inhoud van het wetsvoorstel. Op zichzelf heb ik daar niet veel opmerkingen over. Ik zal alleen over een paar punten wat vragen stellen, om te beginnen het hacken. In ons rechtsbestel zijn wij doorgaans niet zo royaal met de strafbaarstelling van voorbereidingshandelingen als zodanig. Bij de computervredebreuk gebeurt dat nu wel en gelet op het belang dat hiermee wordt gediend, is dat wat ons betreft zonder meer gerechtvaardigd. Het wetsvoorstel geeft een andere invulling aan het begrip ''hacken''. In de huidige definitie is het een vereiste dat de hacker een beveiliging doorbreekt, maar dat is nu geschrapt. Ieder opzettelijk en wederrechtelijk binnendringen in een computer is strafbaar. Wij kunnen ons vinden in de argumentatie die daarvoor in de stukken wordt gegeven, maar ik heb daar nog wel wat vragen bij. Hoe pakt deze delictsomschrijving precies uit wanneer het onduidelijk is of de ''eigenaar'' zijn computernetwerk opzettelijk of per ongeluk heeft opengezet? Kan het nadeel van deze wijze van strafbaarstelling niet zijn dat het signaal wordt uitgezonden aan beheerders van computersystemen dat er wel iets gemakkelijker kan worden omgesprongen met het beveiligen hiervan?

Bij het ontoegankelijk maken van gegevens, eventueel gevolgd door vernietiging ervan, vindt een uitbreiding van bevoegdheden plaats. Dat lijkt een zinvolle stap, waarmee strafbare feiten adequaat beëindigd of voorkomen kunnen worden. Ik zie nog wel wat interpretatieproblemen bij de vraag wanneer er nu sprake is van een besloten communicatie ofwel een openbare uiting. Dat kan soms erg dicht bij elkaar liggen. Het zou wat dat betreft ook niet verkeerd zijn als de al dan niet verwerpelijke inhoud van de betreffende berichten meer centraal zou komen te staan in plaats van de samenstelling van de groep van geadresseerden.

Positief zijn wij ook over de verbeterde mogelijkheden om spam, e-bombing en dergelijke aan te pakken. Wat dat aangaat, hebben wij maar weinig kritische noten. Ik heb wel nog de vraag in hoeverre de doelstellingen adequaat gehaald kunnen worden. Is de handhaving scherp en voldoende? Die gereedschapskist wordt dan wel beter gevuld met dit wetsvoorstel, maar ik kijk ook even naar de hoeveelheid ondeugdelijk materiaal die nog steeds op internet te vinden is. Ondanks de successen die er al geboekt zijn, is hier nog wel een enorme opgave te verrichten. In ieder geval kan er voor de tactische kant van digitaal opsporen nog wel de nodige winst worden behaald. Wij zijn goed te spreken over de plannen en de opleidingstrajecten die al worden uitgezet. In hoeverre kan de digitale slagkracht met meer inzet van mensen en middelen verder verstevigd worden? Lopen wij nu al aan tegen het probleem dat wij nauwelijks over meer mensen kunnen beschikken, gelet op alle opleidingstrajecten die ervoor nodig zijn? Of zou een grotere personele investering een steviger digitale slagkracht kunnen leveren? Zou dat nog meer zaken boven water kunnen halen?

Dit wetsvoorstel krijgt van ons een welwillende bejegening. Het is goed dat die gereedschapskist beter wordt gevuld. Ik deel van harte de analyse van mevrouw Gerkens dat je gelet op alle veranderingen die optreden op het gebied van informatie- en communicatietechnologie niet snel kunt zeggen dat de zaken voorlopig wel op orde zijn. Is er ook nog een wetgevingsagenda voor de toekomst op dit punt? Is Justitie al aan het broeden op terreinen waarop nog een stap gezet moet worden?

□

De heer **Van Fessem** (CDA): Voorzitter. Niet één gordiaanse knoop, maar diverse knopen heeft de minister met dit wetsvoorstel doorgehakt. De tegenslagen, oponthouden en dubbelingen zijn genoegzaam omschreven in de memorie van toelichting van 22 maart jongstleden. Het is ongebruikelijk, maar ik spreek graag mijn waardering uit voor het ingewikkelde werk dat de ambtenaren hebben verricht. Goed, het is hun vak, maar zo erg als in dit wetsvoorstel valt te lezen, zal het niet vaak voorgekomen zijn.

Dit wetsvoorstel gaat over aanpassing aan de snelle ontwikkelingen van deze cybertijd en aan de steeds weer nieuw opduikende euvele daden, die velen van ons aan den lijve ondervinden, zoals virussen en spam. Daarnaast is rond elf-negen ook de aantrekkingskracht van het wereldwijde web op terroristen en potentiële terroristen scherp naar voren gekomen. De CDA-fractie is van oordeel dat politie, openbaar

ministerie en andere diensten met dit wetsvoorstel weer een tijd vooruit kunnen. Nieuwe bevoegdheden vloeien direct voort uit het Cybercrimeverdrag. Deze nieuwe bevoegdheden, maar ook alle reeds bestaande bevoegdheden, zijn omgeven met voldoende waarborgen als bedoeld in artikel 8 EVRM.

Onzes inziens is onder andere artikel 126m van het Wetboek van Strafvordering cruciaal. Voorheen konden alleen telefoonmaatschappijen worden benaderd, maar nu is de uitbreiding van de omschrijving van de aanbieders compleet, zodat ook service providers daaronder vallen. Het is duidelijk dat dan de gegevens moeten worden bewaard om terug te kunnen zoeken in de tijd. Vroeger kwam de politie even langs voor een printje van de verbindingsgegevens van de PTT van twee of drie weken daarvóór. Dat betrof de telefoon, een communicatiemiddel. Wij vinden ook internet niet meer of minder dan een communicatiemiddel. Het is merkwaardig dat er zoveel verzet is tegen het bewaren van internetgegevens. Het is bijna tegenovergesteld aan wat vroeger gebruikelijk was. De televisie werd vooral in onze kringen beschouwd als het oog van de duivel; Kamer en regering moesten er goed op letten dat de uitzendingen van tevoren werden gecontroleerd. Internet lijkt echter even heilig te zijn als de televisie destijds verderfelijk was.

Het Cybercrimeverdrag definieert het desbetreffende begrip, en in navolging daarvan doet ook het Wetboek van Strafvordering dit. Alle tot 22 maart bekende begrippen op dit gebied lijken er nu onder te vallen. Is er sedertdien al sprake van nieuwe ontwikkelingen? De ontwikkelingen gaan immers razendsnel. Is dit wetsvoorstel voldoende techniekonafhankelijk opgesteld? Hoe gaat de minister om met de beroepsgroepen? Getuige de felle discussies in Europees verband over de bewaartermijn van computerverkeersgegevens, zit de beroepsgroep er bovenop. Kan de minister vertellen hoe dit wetsvoorstel ''Computercriminaliteit II'' bij de beroepsgroep is gevallen? Na alle verbeteringen komen er nog de nota's en de take down, en dan zijn wij een heel eind op weg.

Het nieuwe artikel 138a van het Wetboek van Strafrecht gaat het hacken strafbaar stellen, en dat is een uiterst goede zaak. Artikel 138b doet dat met de verstoring. Als voorbeeld daarvan worden virussen genoemd, en dat is ook een prima zaak. Wat is hiermee vergeleken de positie van de spam? Wordt dit beschouwd als een nog lichtere vorm van verstoring? De minister spreekt van bombarderen, zodat de toegang wordt belemmerd. Wat is hierin de juiste balans voor de opsporing? Iedereen zou graag van de hinderlijke spam af willen, maar wij kunnen moeilijk allemaal aangifte doen, want de opsporingscapaciteit is beperkt. Wat de vindt de beroepsgroep hiervan? Hoe verhoudt deze wet zich tot de inmiddels geïmplementeerde Richtlijn elektronische handel, die ten tijde van het indienen van dit wetsvoorstel nog niet eens was aangenomen?

Artikel 273d houdt het verbod in op inbreuk in een besloten netwerk. Zal dit artikel verdere arbeidsrechtelijke consequenties met zich brengen? Mogen als gevolg hiervan extra eisen worden gesteld aan een arbeidscontract?

Als voorbeeld van voorbereidingshandelingen tot indringen of onderscheppen zijn hackprogramma's genoemd. Er wordt dan gezegd: wie zoiets thuis heeft, is weinig goeds van plan. De minister geeft vriendelijk aan dat men zo'n programma thuis kan hebben om te testen of het eigen systeem hackbestendig is. Afgezien van deze smoes, want dat is het in onze ogen: hoe staat de minister tegenover winkels die dit soort programma's in voorraad hebben? Worden die programma's allemaal verkocht om te testen? Is hierover met de branche gesproken?

Het nieuwe artikel 126ni is echt nieuw. Het behandelt de mogelijkheid dat de officier van justitie bevriezing van gegevens voor korte tijd vordert; volgens het Cybercrimeverdrag maximaal 90 dagen. Hoe verhoudt deze bevoegdheid zich tot het gegeven dat de telecommunicatieaanbieders sowieso verkeersgegevens bewaren? Wat wordt bedoeld met ''gegevens die vatbaar zijn voor verlies of wijziging''? Wordt er niet van tevoren een excuus ingebouwd door gegevens zo te kwalificeren? De provider kan immers zeggen: de gegevens zijn al verloren gegaan, en dat wist u, want zij zijn vatbaar voor verlies. Op vragen van het OPT hierover antwoordt de minister weliswaar dat extra kosten hiervoor vergoed kunnen worden, maar zijn de providers verplicht om gegevens die vatbaar zijn voor verlies, toch te bewaren? Als dat zo is, hoeft ook die categorie niet te worden benoemd. Kan de minister hierover duidelijkheid geven? Hoe verhouden deze regels zich tot de Europese discussie die momenteel woedt over het bewaren van verkeersgegevens in verband met terrorismebestrijding en de bestrijding van andere zware misdrijven?

Dit wetsvoorstel vormt een goede en broodnodige aanpassing aan de eisen des tijds, en daarmee aan de eisen van het Cybercrimeverdrag. Het is goed dat die twee samenvallen. Wij gaan ervan uit dat aanpassingen aan de voortschrijdende ontwikkelingen in de toekomst sneller zullen leiden tot wetsaanpassingen. Die wens is hiermee dan in ieder geval uitgesproken.

□

De heer **Weekers** (VVD): Voorzitter. Koops en Schellekes verzuchtten in het Nederlandse Juristenblad in 1999: de boeven zijn er, nu de wet nog. De wet is er nu, anno 2005, nog steeds niet. Snelle invoering is wat dat betreft geboden. Als ik kijk naar de zaken die aangepakt worden in deze wet – hacking, DDoS, virusverspreiding, afluisteren, vernielen van geautomatiseerd werk, vernielen van computergegevens, valse betaalpas – dan zijn dat zaken die wij moeten kunnen aanpakken met ons strafrecht. Dat wordt geregeld. Als ik dan kijk naar wat er in het kader van dit wetsvoorstel is gebeurd, dan hebben wij dit jaar een tweede nota van wijziging gekregen en die was zeer omvangrijk. Het Cybercrimeverdrag wordt nu geïmplementeerd, bepalingen rondom het vorderen van gegevens zijn overgebracht naar een ander wetsvoorstel en ook de aansprakelijkheid voor tussenpersonen wordt nu elders geregeld. Het zijn zoveel wijzigingen bij elkaar dat er gesproken kan worden van een wetsvoorstel computercriminaliteit III.

Het Cybercrimeverdrag wordt geïmplementeerd met het voorliggende voorstel. Dat is winst. Het probleem dat wij bespreken, houdt zich immers niet aan landsgrenzen. En problemen die zich niet aan landsgrenzen houden, moeten in samenwerking tussen staten worden

opgelost. Het College Bescherming Persoonsgegevens merkte op dat het verdrag moet worden beschouwd als een maatgevend voorstel op het gebied van het opsporen van criminele gedragingen waarbij computernetwerken worden gebruikt. Wat mijn fractie betreft, slaat het CBP hiermee de plank volledig mis. De regering merkt immers terecht op dat het verdrag slechts die onderwerpen regelt waarover instemming is bereikt. Uitputtend is het geenszins. Naar mening van mijn fractie komt daar nog bij dat de snelle ontwikkeling van de ICT en de daarmee samenhangende criminaliteit met zich meebrengt dat welk verdrag dan ook nooit uitputtend kan zijn. Er zal altijd ruimte moeten zijn voor een reactie op nieuwe ontwikkelingen. De VVD-fractie vraagt de minister, die ruimte te houden.

Er zijn nieuwe ontwikkelingen en er was op tal van zaken ook in internationaal verband nog geen internationale afstemming. Welke initiatieven zijn er om te komen tot een Cybercrimeverdrag II? Ik meen dat deze vraag ook in het verlengde ligt van vragen die eerdere sprekers hebben gesteld. Ik heb de heer Van Fessem daarover horen spreken, maar ook de heer Van der Staaij. De vraag is al gesteld of de regering nog ergens op aan het broeden is. Die vraag geldt dus niet alleen internationaal, maar ook nationaal.

Voorzitter. Een ander punt dat ik aan de orde wil stellen, is spam. Spam is hinderlijk. Hinderlijk omdat er veel post in de brievenbus komt waarop mensen niet zitten te wachten, maar ook hinderlijk omdat er veel vunzigheid en schimmigheid in die post zit. De regering gaf eerder aan, geen rol voor het strafrecht te zien bij de aanpak van spam. Is dat inzicht inmiddels veranderd? Wat denkt de regering van de vaak gehoorde kwalificatie dat Nederland het spamparadijs zou zijn?

Ik las in de meest recente ICT-barometer van Ernst & Young dat de schade die wordt veroorzaakt door cybercrime gigantisch toeneemt.

De heer **Van Dam** (PvdA): Voorzitter. Wij moeten vanavond toch een beetje het idee krijgen dat wij een debat hebben en dat er af en toe geïnterrumpeerd wordt. Ik zag een kans, laat ik die grijpen. Het was destijds bij het debat over spam juist de VVD-fractie die zich aan alle kanten verzet heeft tegen de strafbaarheid van spam. Het kan gebeuren dat de heer Weekers nu na een jaar denkt dat dit misschien toch niet zo verstandig is geweest. Stelt de VVD-fractie haar standpunt hierover bij?

De heer **Weekers** (VVD): Voorzitter. Ik vind het in elk geval een vraagpunt dat wij opnieuw onder ogen moeten zien. Ik weet inderdaad dat mijn fractie zich destijds heeft verzet tegen een strafrechtelijke aanpak van spam. Ook onze Europese fractie zat op die lijn. Ook wij kunnen echter niet ontkennen dat de hinderlijkheid van spam een hoge vlucht neemt. Vandaar de vraag hoe de regering daar tegenaan kijkt.

De ICT Barometer van Ernst & Young laat zien dat de schade die wordt veroorzaakt door cybercrime gigantisch toeneemt. Zo ondervindt een derde van het aantal bedrijven hinder van illegale diensten en producten die via internet verspreid worden. Hoe gaan wij deze tendens keren, zo vraag ik de minister.

Ook verandert het karakter van cybercrime. Naarmate mensen en organisaties zich beter beveiligen tegen virussen verschuift het werkterrein van de criminelen. Gisteren las ik in de berichten van Webwereld over cybercrime het volgende citaat van een onderzoeker bij een beveiligingsbedrijf: de maffia heeft haar werkterrein naar internet verplaatst en afpersing is dan ook een groeiend probleem. Ook daartegen moet worden opgetreden.

De onderhavige wet lijkt hierop geen afdoende antwoord te bieden. Met alleen wetgeving komen wij er dus niet. Een antwoord is bijvoorbeeld wel, uiteraard met de wet in de hand, voldoende capaciteit bij politie en justitie voor de bestrijding van internetcriminaliteit. Hoe staat het daarmee? Graag verneem ik hierop een reactie van de minister.

□

De heer **Van Dam** (PvdA): Voorzitter. Begin juni kregen talloze Nederlanders een mailtje dat ogenschijnlijk van de Postbank kwam. Het was echter een phishing scam. De websites van de overheid werden verleden jaar plat gelegd met een DDoS-aanval, waarbij gebruik gemaakt werd van een leger van zombies. Script kiddies verspreiden dagelijks virussen, trojans en wormen om systemen te infecteren en te infiltreren. Achter lollige filmpjes zitten soms keyloggers die alles wat je typt, registreren, dus ook de gegevens van je creditcard. Langs die weg werd er verleden week bij talloze mensen € 9,95 van hun creditcard afgeschreven.

Verspreiders van kinderporno verschuilen zich achter proxies, encryptie en passwords. Hackers hacken niet alleen meer voor het heldendom, maar tegenwoordig ook voor het grote geld.

Ik zie de minister fronsen. Hij moet zich de hele dag zorgen hebben gemaakt over dit debat: hacking, phishing, scamming, DDoS, scripts, zombies, trojans, proxies ..., het klinkt allemaal spannend, maar eigenlijk gaat het om heel oude criminaliteit: inbreken, insluipen, saboteren, vernielen en stelen, heel echte criminaliteit, maar wel in een virtuele omgeving.

Het is goed dat Nederland het Cybercrimeverdrag ratificeert en nu implementeert. Zoals de heer Weekers al zei: cybercrime, criminaliteit op internet, is een internationaal probleem en dat kan je alleen aanpakken, als diverse landen criminaliteit op internet op dezelfde manier strafbaar stellen en vervolgen.

Wij hebben nogal lang moeten wachten totdat wij dit wetsvoorstel konden behandelen. Het ligt namelijk al zes jaar in de Kamer. In elk geval is er nu wel een voorstel waarvan wij hopen dat het de komende jaren geschikt is om de criminaliteit op internet echt te lijf te gaan. De Partij van de Arbeid staat dan ook vierkant achter dit wetsvoorstel.

Wij hebben nog ogenschijnlijk wat kleine verbeterpuntjes. Ik heb daartoe zojuist een aantal amendementen ingediend. Misschien zijn niet alle amendementen noodzakelijk; je kunt het maar beter zeker weten dan dat je over een jaar moet constateren dat je iets hebt opengelaten. Wij willen er dus zeker van zijn dat met deze wet de internetcriminaliteit nu en in de komende jaren effectief bestreden kan worden, zelfs op het moment dat de techniek voor criminelen weer nieuwe mogelijkheden creëert om zich te verschuilen of om hun daden weer langs nieuwe wegen uit te voeren.

Ik zal een aantal vragen stellen over die verbetermogelijkheden. De minister kan hierop ingaan aan de

hand daarvan en aan de hand van mijn amendementen. Daarna stel ik wat meer fundamentele vragen aan de orde.

Ik begin met het Wetboek van Strafrecht. Het wetsvoorstel regelt in de eerste plaats dat het binnendringen van een computer ook strafbaar wordt als daarvoor niet eerst een beveiliging is gekraakt. Dat lijkt logisch. Zelf als je immers niet beveiligd het internet opgaat, heeft niemand iets op je computer te zoeken. Je mag ook niet zomaar bij iemand zijn huis binnenwandelen, zelfs als hij zijn deur open heeft staan. Maar er is ook steeds meer software in omloop waarmee anderen toegang wordt gegeven tot een deel van de computer. Delen van bestanden zitten gewoon in Windows ingebakken, maar ook in allerlei andere software zoals Kazaa. U weet wel, dat is dat programma dat niemand gebruikt maar dat iedereen kent.

Voorzitter. Het valt voor een internetter niet altijd te controleren of iemand bewust toegang tot diens computer verleent of dat het per ongeluk gebeurt. Mijn vraag aan de minister luidt derhalve, hoe artikel 138a precies werkt in de gevallen dat men een computer binnengaat, waarvan in ieder geval kan worden vermoed dat bewust toegang wordt verstrekt, maar je het niet zeker weet.

Voorzitter. In artikel 138b wordt het verzenden van data strafbaar gesteld indien daarmee wordt beoogd om computers of een netwerk plat te leggen. In de praktijk wordt een zogenaamde denial-of-serviceaanval altijd uitgevoerd vanaf meerdere plaatsen. Daarom heet het dan een distributed denial-of-serviceaanval. Zou het daarom niet verstandig zijn om in artikel 138b niet alleen op te nemen dat het verzenden of aanbieden van gegevens onder de strafbaarstelling valt, maar ook het laten verzenden of laten aanbieden ervan. Ik heb daarover een amendement ingediend, waarop ik graag de reactie van de minister verneem.

Ook mevrouw Gerkens heeft al gesproken over artikel 232, waarin het vervalsen van een betaalpas en het gebruik daarvan strafbaar wordt gesteld. Het is de vraag of de strafbaarstelling beperkt moet blijven tot een betaalpas. Is het niet verstandiger om de strafbaarstelling alvast uit te breiden tot elke drager van identiteitsgegevens. Er komen immers steeds meer dragers van identiteitsgegevens in omloop die niet direct onder de definitie ''pas'' of ''kaart'' vallen.

Voorzitter. Een soortgelijke vraag moet worden gesteld ten aanzien van artikel 273d waarin een medewerker van een telecommunicatieaanbieder strafbaar wordt gesteld indien hij gegevens steelt. Zou een dergelijke strafbaarstelling niet moeten gelden voor elke werknemer van een organisatie waarin persoonsgegevens worden opgeslagen of verwerkt? Ook daarover heb ik een amendement ingediend.

Voorzitter. In het wetsvoorstel wordt het zogenaamde bevriezingsbevel geïntroduceerd in het Wetboek van Strafvordering. Daarmee kunnen gegevens van een verdachte gedurende drie maanden worden bevroren. Gezien de formulering van het betreffende artikel ga ik ervan uit dat dit slechts de gegevens betreft die providers toch al opslaan als onderdeel van de normale bedrijfsvoering. Ik zie de minister al knikken, dan hoeft hij dus niet meer te zeggen dat het klopt. Dat wilde ik echter wel graag zeker weten.

Voorzitter. Men kan zich de vraag stellen in hoeverre dit bevriezingsbevel de noodzaak van een bewaarplicht overbodig maakt. Daarover loopt de discussie nog. Is het niet verstandig om eerst ervaring op te doen met het bevriezingsbevel. Dat is immers zoveel als een tijdelijke bewaarplicht ten aanzien van iemand die tijdens een onderzoek in the picture komt. Ik verzoek de minister daarop wat nader in te gaan.

Voorzitter. In de artikelen 126nb en 126nb wordt de mogelijkheid gecreëerd om met behulp van nader te omschrijven apparatuur nummers van communicatieabonnees te achterhalen. Is het verstandig om dit zo beperkt te definiëren? Kan het niet beter ruimer worden gedefinieerd, zodat ook gebruik kan worden gemaakt van nieuwe vindingen? Ik denk bijvoorbeeld aan softwarematige vindingen, waarbij geen apparatuur meer nodig is.

Voorzitter. Tot zover mijn gedetailleerdere vragen over de teksten van dit wetsvoorstel. Ik kom toe aan een aantal in mijn ogen fundamentelere vragen die door dit wetsvoorstel worden opgeroepen. Criminaliteit op internet is, zoals ik al eerder zei, weliswaar heel gewone criminaliteit, maar verpakt in een nieuw jasje. Daardoor zijn de traditionele middelen niet altijd meer opgewassen tegen de voortschrijdende technieken. De themacommissie technologiebeleid heeft dit voorjaar een bijeenkomst georganiseerd waarop diverse deskundigen, waaronder een officier van justitie, vertelden hoe moeilijk het is geworden om slimme criminelen op internet te pakken te krijgen. Zij verbergen zich achter acht of negen lagen van beveiliging en versleuteling. De officier van justitie verzuchtte dat dergelijke criminelen eigenlijk alleen gepakt kunnen worden wanneer zware opsporingsmiddelen worden ingezet, zoals het installeren van software op de computer van de verdachte of van apparatuur in het huis van de verdachte. Dergelijke middelen zijn echter alleen toegestaan bij zware misdrijven waarop meer dan acht jaar gevangenisstraf staat. Het bezit of de verspreiding van kinderporno en economische delicten waarbij van het internet gebruik wordt gemaakt, vallen daar – als ik het goed beoordeel – dus niet onder. Zou het niet verstandig zijn om ons te beraden over de vraag of dergelijke opsporingsmiddelen specifiek voor dit soort zaken ingezet zouden kunnen worden. Ik hoor graag hoe de minister daar tegenaan kijkt. Ook hoor ik uit betrouwbare bron dat regelmatig wordt gehuiverd voor de inzet van bevoegdheden die behoren bij de opsporing van misdrijven in georganiseerd verband. Ik begrijp het wel. Een paar jochies met veel verstand van computers die elkaar niet eens kennen, laat staan hun opdrachtgevers, beantwoorden niet aan ons beeld van georganiseerde criminaliteit. Als die jochies echter vanuit Rusland of andere landen worden aangestuurd, is dat wel degelijk georganiseerde criminaliteit. Kan de minister uiteenzetten hoe in de praktijk met dergelijke gevallen en bepalingen wordt omgegaan?

Veel van de misdrijven die op internet worden gepleegd zijn moeilijk op te lossen. Daaraan werken dagelijks tientallen digitale rechercheurs. Voorkomen is beter dan genezen en ook op internet moet dus worden gesurveilleerd. Ik heb begrepen dat dat nauwelijks gebeurt. Naar verluidt zijn daarbij minder dan twintig rechercheurs betrokken. Klopt het dat er maar zo weinig agenten actief op internet zoeken naar criminaliteit en potentiële kwetsbaar-

heid? Is de minister van plan deze capaciteit fors uit te breiden?

Momenteel is het verboden om binnenshuis heimelijk foto's van iemand te maken en eveneens om dergelijke foto's te publiceren. Vandaag de dag loopt vrijwel iedereen continu rond met een camera en een microfoon, die namelijk standaard op elke telefoon zitten. Je kunt dus ongestraft in de openbare ruimte foto's en opnamen van iedereen maken en die zeer eenvoudig op internet publiceren. Wij weten inmiddels dat het internet niets vergeet. Het kan een flinke inbreuk op de privacy van mensen vormen als een afbeelding of opname van hen, gemaakt in de openbare ruimte, wordt gepubliceerd op internet. Dat is gewoon toegestaan. Dan zwijg ik nog van jonge meisjes die zich vrijwillig ontkleden voor de webcam en nog jaren later hun foto's op internet tegenkomen. Het is tijd om tegen dergelijke zaken op te treden. Ik nodig de minister uit, daarop zijn licht te laten schijnen. Het maken van foto's op straat kan niet worden verboden, maar de burger zou zich moeten kunnen verweren tegen het publiceren van foto's of opnamen, zelfs als die met instemming van de betrokkene zijn gemaakt. Zodra je op internet verschijnt, kom je er nooit meer vanaf. Diverse landen hebben inmiddels richtlijnen over het gebruik van camerafoons en ik denk dat ook in Nederland een discussie nodig is over bescherming van de privacy tegen de alom aanwezige camera's.

New York heeft onlangs in navolging van onder meer California een wetsvoorstel aangenomen waarin overheden, bedrijven en andere organisaties verplicht worden hun klanten – burgers en bedrijven – te informeren als zij zijn gehackt of als bij een inbraak in de systemen identiteitsgegevens zijn ontvreemd. Dat voorstel vind ik interessant. Ten eerste hebben burgers en bedrijven het recht om het te weten als hun gegevens in verkeerde handen terecht zijn gekomen. Ten tweede stimuleert een dergelijke verplichting bedrijven om hun beveiliging op orde te hebben. Ik hoor graag van de minister of hij bereid is om wetgeving op dat punt voor te bereiden.

□

Mevrouw **Vos** (GroenLinks):

Voorzitter. Het wetsvoorstel Computercriminaliteit II heeft een lange voorgeschiedenis. Het is in 1998 ingediend en na sluiting van het Cybercrimeverdrag aanmerkelijk gewijzigd. Het wetsvoorstel probeert een aantal verplichtingen voor de informatiesector en een aantal onderzoeksbevoegdheden voor Justitie te scheppen, die de komende onvoorzienbare technologische ontwikkelingen kunnen doorstaan. Dit kabinet vindt informatietechnologie belangrijk. Toekomstige kansen en risico's van de ontwikkelingen op dit gebied zijn lastig in te schatten. Twintig jaar geleden hield nog niemand het überhaupt voor mogelijk dat een Nederlandse hacker andermans computerbestanden in Amerika zou kunnen plunderen. Er zijn dus risico's, maar ook kansen. Dezelfde technologische ontwikkelingen zorgen ervoor dat elektronische data in een fractie van een seconde waar dan ook ter wereld bezorgd kunnen worden. Dit geeft ook de sociale en economische ontwikkelingen een gigantische boost. Het delen van kennis is inmiddels ondenkbaar zonder deze technologie.

Het is belangrijk om een zekere mate van veiligheid op de digitale snelweg te bieden, en daarbij passen strafbepalingen. Van andermans eigendommen behoor je doorgaans af te blijven, en het is niet in te zien waarom dit niet voor andermans digitale spulletjes zou moeten gelden. Het blijft alleen de vraag of wetswijzigingen gezonde technologische ontwikkelingen niet in de weg staan. Het College Bescherming Persoonsgegevens heeft hierover zijn zorgen geuit bij brief van 20 februari 2004. De onderlinge samenhang en de consistentie van bestaande wettelijke bepalingen en lopende wetgevingstrajecten baarde het college grote zorgen. Het constateerde dat veel bedrijven en instellingen in de telecommunicatiesector niet meer weten welke verplichtingen zij hebben en wat zij uiteindelijk aan moeten met het aanzienlijke complex van regels.

Deze kritiek klemt te meer nu deze materie raakt aan het grondwettelijke brief-, telegraaf- en telefoongeheim, dat behoudens strikt wettelijke uitzonderingen geëerbiedigd moet worden. Dit vergt bijzondere voorzichtigheid van de wetgever. Ik zie in dit wetsvoorstel een aantal diep ingrijpende bevoegdheden tot het gebruik van dwangmiddelen en een uitbreiding van de strafbaarheid. Voor een aantal ervan geldt de vraag of ze werkbaar zijn. De bevoegdheden waarin voorzien wordt, bestaan uit het ontoegankelijk maken van gegevens voor zover dit noodzakelijk is ter beëindiging van strafbare feiten of nieuwe strafbare feiten, artikel 125o, het maken van opnamen van niet voor het publiek bestemde communicatie, artikel 126, eerste lid, onderdeel a, het verstrekken van gegevens over een gebruiker van een communicatiedienst, artikel 126n, het bevriezen van gegevens voor maximaal 90 dagen, artikel 126ni, en het onderzoek aan netwerken, eventueel zonder de medewerking van providers, artikel 126n, vierde lid.

Het ontoegankelijk maken van gegevens roept toch wel een aantal fascinerende vragen op, want op welk moment kan hiertoe worden overgegaan? Gaat het erom dat de officier van justitie een strafbaar feit constateert en kan men dan al tot het in feite blokkeren van gegevens? Of kan dit pas als de rechter uiteindelijk een veroordeling heeft uitgesproken? Hoe verhoudt dit zich tot het apologieverbod? Daarover komen wij nog met de minister te spreken, maar ik vraag me af of de situatie kan ontstaan dat een op internet geuite onsmakelijke mening die onder de strafbaarstelling van apologie kan vallen, tot blokkering van die boodschap kan leiden. Dan zou er heel wel sprake zijn van aantasting van de vrijheid van meningsuiting. Er kan ook sprake zijn van economische schade, als het gegevens betreft die essentieel zijn voor het voortbestaan van een onderneming. Hoe gaat men daarmee om? Dus graag meer duidelijkheid over het moment waarop hiertoe kan worden besloten.

Dan het voorstel om zonder de tussenkomst van providers netwerken te onderzoeken. Mijn fractie vindt dit een tamelijk eng voorstel, want betekent dit nu volstrekte carte blanche om naar hartelust in gegevensbestanden te zoeken? Betekent dit eigenlijk niet dat justitie oncontroleerbaar al die gegevensbestanden kan inzien en dat wij maar moeten afwachten, hoe en waar zij dit doet? Controle hierop lijkt mij zeer lastig, dus justitie zou hiermee wel eens hetzelfde kunnen doen als datgene wat als computervredebreuk strafbaar wordt gesteld. Graag meer duidelijkheid over hoe dit wordt

Mevrouw Vos (GroenLinks)

© M. Sablerolle – Gouda

vormgegeven. Hoe is er controle op dit punt mogelijk?

De strafbepaling voor computervredebreuk en voor een poging daartoe wordt op de schop genomen, maar de formulering die de minister nu voorstelt, vind ik eerlijk gezegd onwerkbaar. Het lijkt erop dat het Openbaar Ministerie computervredebreuk voortaan gaat bewijzen aan de hand van de begrippen opzet en wederrechtelijkheid. Enerzijds vraagt dat nogal wat. Justitie moet dan de opzettelijke intentie van de hacker voor de rechter aantonen. Ik stel mij voor dat daarin door de raadslieden snel gaten kunnen worden geschoten. Anderzijds wordt inbraak blijkbaar altijd strafbaar gesteld, ook als de eigenaar van de computer geen maatregelen heeft genomen om dat te voorkomen. In de huidige praktijk is niet altijd duidelijk of de eigenaar van de computer opzettelijk of per ongeluk de computer ''open'' heeft gezet. Graag een verduidelijking van de minister.

Ik kom toe aan het strafbaar stellen van voorbereidingshandelingen in artikel 139d van het Wetboek van Strafvordering, een voorstel dat mijn fractie echt te ver gaat. Op de markt zijn ongelooflijk veel programma's te koop en te downloaden, die uitwisseling van gegevens mogelijk maken. Daar kun je uiteraard misbruik van maken. In het artikel zit het oogmerk ''plegen van computermisdrijven'' ingebakken, maar ook hier vraag ik mij of af dit werkbaar is, en of de kans niet groot is dat onschuldige, bonafide softwaremakers en -leveranciers de dupe worden.

De officier van justitie kan internetproviders bevelen, bepaalde gegevens tijdelijk, voor maximaal 90 dagen, beschikbaar te houden in afwachting van een definitieve vordering om de gegevens uit te leveren. Dat zou wel eens een uitstekend alternatief kunnen zijn voor de vermaledijde bewaarplicht, omdat het hier gaat om een bevel dat doelgericht kan worden ingezet op personen die tijdens een onderzoek in beeld komen, maar waarvan de verkeersgegevens mogelijk later gevorderd worden. Ziet de minister dit ook als een mogelijk alternatief voor deze bewaarplicht?

De heer **Van Fessem** (CDA): Maar het gaat toch vaak om gegevens die nodig zijn voordat het delict is gepleegd, en niet als het al is gepleegd? Immers, de verdachte zal dan niet meer bellen, want dan zit hij vast. Ik noem als voorbeeld de moord op de drie Hells Angels, die is opgelost door terug te gaan in de tijd.

Mevrouw **Vos** (GroenLinks): Er zal ook worden onderzocht als men bepaalde personen verdenkt van het voorbereiden van een of meerdere aanslagen. Ik kan mij voorstellen dat ook in dat geval het bevriezingsbevel een rol kan spelen. Wanneer die personen opduiken in het onderzoek, kan doelgericht worden gezegd dat de gegevens van die personen moeten worden bewaard, zodat ze eventueel later gevorderd kunnen worden.

Ik heb nog een vraag over een stokpaardje van mij, de notificatieplicht ex artikel 126bb van het Wetboek van Strafvordering. Heb ik het goed gelezen dat de notificatieplicht van toepassing zal zijn op deze voorgestelde bevoegdheden? Zo ja, dan verheugt mij dat zeer, maar dan vraag ik de minister op welke wijze naleving zal worden afgedwongen. De notificatie bij het belverkeer laat op dit moment namelijk ernstig te wensen over.

De heer **Van der Staaij** (SGP): Wat is de opvatting van de fractie van GroenLinks over het Cybercrimeverdrag? Kan het wetsvoorstel terzake onverkort worden goedgekeurd?

Mevrouw **Vos** (GroenLinks): Mijn fractie is in principe van mening dat dit goedgekeurd moet worden. Wij hebben kritische vragen over het aan de orde zijnde wetsvoorstel.

De heer **Van der Staaij** (SGP): U sprak over elementen uit de tweede nota van wijziging en die betreffen voor een groot deel de implementatie van het Cybercrimeverdrag.

Mevrouw **Vos** (GroenLinks): Daar heeft u gelijk in. Wij zullen moeten afwegen of wij akkoord kunnen gaan met dit wetsvoorstel en met hetgeen via het Cybercrimeverdrag wordt geïmplementeerd. Op een aantal punten hebben wij forse bezwaren. Na de reactie van de minister zullen wij onze afweging maken.

De vergadering wordt van 20.05 uur tot 20.25 uur geschorst.

Voorzitter: Ten Hoopen

□

Minister **Donner**: Voorzitter. Ik dank de Kamer voor de bespreking van dit onderwerp en voor bereidheid om hier voortvarend mee om te gaan. Naar ik meen, heeft het wel tot

gevolg gehad dat wij over de tweede nota van wijziging geen echte schriftelijke ronde hebben gehad, zodat die nu in wezen in één klap mondeling wordt ingehaald. Ik verzoek de Kamer dan ook vriendelijk om niet al te ver door te vragen over een aantal verschijnselen die hierop betrekking hebben, zoals DDoS-attacks en dat soort zaken, omdat dan onmiddellijk blijkt dat ik daar geen parate kennis over heb.

Ik deel de Kamer mee dat ik nog een vierde nota van wijziging naar de Kamer heb gestuurd. Die nota heeft betrekking op een onderdeel van een eerdere nota van wijziging, namelijk op de wijziging van artikel 126ee. Daarbij gaat het inderdaad om de mogelijkheid om te tappen zonder tussenkomst van de provider. Daarin is de bepaling opgenomen dat dit alleen maar kan als de apparatuur die wordt gebruikt, voldoet aan bepaalde technische vereisten. Per abuis is die bepaling uitgebreid voor de gevallen waarin wordt getapt via de provider. Daarvoor gelden andere regels. Daarom wordt de reikwijdte van artikel 126ee technisch teruggedraaid. Deze nota van wijziging is naar de Kamer gestuurd. Ik heb een ondertekend exemplaar bij me. Dat kan ik nu afgeven, maar ik weet niet of dat van de postkamer wel zo mag.

Ik meen dat wij tevreden mogen zijn over het feit dat de teneur van het wetsontwerp in de Kamer breed wordt gesteund. Mevrouw Vos had volgens mij nog de meest kritische vragen op dit terrein. Zij heeft zich overigens geëxcuseerd, want zij had een verplichting elders. Uiteraard blijft dat wij op dit terrein met een aantal verschijnselen zitten waarbij wij in feite nog maar tastend proberen om vooruit te komen. Toch wil ik voor iets waarschuwen en dat is voor het beeld dat wij hierbij te maken hebben met een aantal zaken dat wij al langer kennen. Uiteraard, voor een deel is dat waar. Diefstal van informatie is in wezen diefstal in de zin van ''iets wegnemen'', zoals dat vroeger werd genoemd. Wij beginnen ons pas geleidelijk aan te realiseren dat het fundamentele gegeven van internet is dat wij met internet het onderscheid tussen binnen en buiten opgeheven hebben. De private ruimte en de openbare ruimte lopen daardoor in elkaar over. Daarom worden ook vragen gesteld over het wederrechtelijk toetreden. Bij huizen maken wij dat onderscheid ook altijd. Het gaat om diefstal met braak of om diefstal. Dat is al een oud onderscheid. Als ik een huis binnenkom terwijl de voordeur openstaat, kan dat huisvredebreuk opleveren, maar dan zal primair aangetoond moeten worden dat ik kon beseffen dat ik daar niet binnen hoorde te komen. Dat is anders als ik met een koevoet iemands voordeur openbreek. Dan wordt verondersteld dat ik begrijp dat ik daar niet binnen mag komen.

In wezen zit ik ook op dit terrein met die vragen. Dat proberen wij in het wetsontwerp op te vangen, met name door het begrip ''wederrechtelijk'', dat inderdaad in den brede de situaties moet dekken waarbij de rechter steeds in het concrete geval zal moeten vaststellen of het nu wel of niet duidelijk was of iemand binnen mocht komen. Dat probleem ontstaat met name wanneer geen duidelijke wil tot uitdrukking is gekomen. Als ik op de straat loop en een voordeur open zie staan, betekent dat niet per definitie dat ik daar welkom ben, maar zie ik een winkeldeur openstaan, dan mag ik aannemen dat ik daar wel welkom ben. Dan ligt de bewijslast bij de winkelier, die dan moet aantonen dat ik wederrechtelijk de winkel binnengetreden ben. Kortom, dat zijn vragen die niet algemeen bij wetgeving beantwoord kunnen worden. Zo speelt door dit hele wetsontwerp een groot aantal punten. Voor een deel zullen die door jurisprudentie in de rechtspraak gepreciseerd moeten worden.

Er is een aantal vragen gesteld over het onderwerp dataretentie. Dat is eigenlijk het meest klassieke onderwerp, want dat gaat over gegevens van telefonieverkeer die wij allang hadden, en over het internetverkeer. Verder hebben wij niet veel nieuwe voorstellen. Er is voortdurend discussie over het gebruik van internet bij terroristische aanvallen en op het terrein van radicalisering. De vragen daarbij zijn in wezen niet anders dan de vraag waarmee wij hier bezig zijn: wanneer en hoe kan ik effectief ingrijpen om bepaalde berichtgeving stop te zetten. Daarbij zijn geen fundamenteel nieuwe dimensies.

Ik kan de Kamer op dit punt volstrekt geen garantie geven, zoals de heer Weekers ook duidelijk heeft aangegeven. In het verdrag zijn de punten opgenomen waarover wij het internationaal eens kunnen zijn. Het is niet zomaar een begin, maar het is ook niet uitputtend. Ik denk dat het verdrag wezenlijk is voor de bestrijding van de cybercriminaliteit. Om die reden zijn wij niet doorgegaan met het oorspronkelijke wetsvoorstel om vervolgens los daarvan het verdrag uit te voeren. Op dit terrein moeten wij het juist primair hebben van internationale samenwerking. Het verdrag is van wezenlijke betekenis door de regeling van uniforme definities en van bevoegdheden waarvan ieder zich moet voorzien. Verder kan er rechtshulp worden geleverd onder het verdrag.

Alleen zo kan ik op eenvoudige wijze optreden bij een internationaal verschijnsel als internet, omdat ik weet dat de bevoegdheid die ik hier heb, ook aan de andere kant bestaat. Het belang van de bepaling over bevriezing is dat ik niet alleen weet dat ik die bevoegdheid heb, maar ook dat ik bij alle landen die partij zijn bij het verdrag, een dergelijk bevriezingsbevel kan vragen. Dat is wezenlijk bij dit verschijnsel.

De vraagstelling bij deze voorstellen ligt dan ook iets anders. Men kan zeggen dat men het nationaal misschien iets anders zou definiëren of opzetten, bijvoorbeeld door bepaalde opsporingsbevoegdheden te koppelen aan de strafmaat. De nu gekozen opzet vloeit voort uit het verdrag, waarin duidelijk is bepaald dat die koppeling niet gelegd moet worden. Dan is de uniformiteit die met het verdrag wordt gerealiseerd, belangrijker dan het specifieke, eigene van onze wetgeving op deze terreinen.

Dan wil ik wat meer stelselmatig ingaan op de gestelde vragen. Ik heb al een aantal punten van mevrouw Gerkens genoemd in mijn algemene overwegingen. Zij stelde de vraag of de regering meer aandacht moet besteden aan het voorlichten van gewone gebruikers over de risico's. Er is een voorlichtingsprogramma van Economische Zaken, met de naam ''surf op safe''. Dat loopt al een aantal jaren. Je kunt erover discussiëren of het uitgebreid moet worden.

De overheid heeft in beginsel een verantwoordelijkheid bij de voorlichting van gebruikers. Ik denk dat deze eerder in de sfeer zit van voorlichting aan consumenten of gebruikers dan over de gevaren in de justitiële sfeer. Daarom zit het ook bij Economische Zaken. Overeind blijft

dat de aard van het instrument met zich meebrengt dat daarin niet een bepaald vertrouwen kan worden gesteld, hoewel er sprake is van gewenning en hoewel wij dit gelijkstellen aan de openbare weg. Wij kunnen er niet op vertrouwen dat dit instrument niet uitvalt en het is evenmin zeker dat bepaalde informatie niet wordt gebruikt. Het aloude beginsel van het recht is daarop van toepassing: ''Men moet zijn vertrouwen vinden waar men het gelaten heeft.''

Mevrouw **Gerkens** (SP): Ik ga in dit geval mee met de redenering van de minister, maar het zal niemand bevreemden dat ik niet tevreden ben met de campagne die het ministerie van Economische Zaken op dit terrein voert. Die discussie kan ik echter niet voeren met de minister van Justitie. Wel vraag ik hem om daarover in wat bredere zin zijn gedachten te laten gaan. Ook van de politie kennen wij campagnes onder de titel ''Op slot, buit eruit'' om te voorkomen dat er diefstal wordt gepleegd. De minister heeft zojuist een goede analogie gebruikt: ''De deur wagenwijd open of een koevoet ertussen.'' Wij zouden mensen ook op die gevaren moeten wijzen. Voor inbraak is dat niet meer nodig. Iedereen weet immers dat het keurmerk Veilig Wonen beter is dan een slot met een loper. Het lijkt mij goed om ook op dit terrein iets dergelijks te ontwikkelen. Kan het kabinet daarover zijn gedachten laten gaan?

Minister **Donner**: Op dat punt ben ik het met mevrouw Gerkens eens. Zij heeft ook aangegeven wat onder bepaalde trefwoorden kan worden gevonden op het moment dat men gebruikmaakt van sommige zoekmachines. Het is wel belangrijk om na te gaan op welke wijze dat moet worden opgezet, omdat het niet mogelijk is om allerlei verantwoordelijkheden van de overheid over te nemen. Ik zal dit punt in ieder geval bij de minister van Economische Zaken aan de orde stellen en dat eventueel breder in het kabinet inbrengen.

Mevrouw Gerkens heeft een vraag gesteld over de handhaving en de opsporing op dit terrein. Veel andere Kamerleden hebben daarop voortgeborduurd. Dit is één van de redenen om te komen met een voorstel tot wijziging van het politiebestel. Zodoende is het mogelijk om de opsporing en de handhaving op dat terrein wat effectiever te organiseren. Op dit moment zit er een dienst bij het KLPD en ook bij alle verschillende korpsen zijn afzonderlijke diensten ondergebracht. Ik zal niet de precieze aantallen noemen om te voorkomen dat die in de kranten verschijnen. Bij de politie is er een capaciteit van ongeveer 150 mensen die met deze zaken bezig zijn. Bij het OM wordt de capaciteit geleidelijk uitgebreid met mensen die daadwerkelijk deskundig zijn en met een algemene cursus wordt geprobeerd om de officier van justitie zo veel mogelijk met deze zaken bekend te maken. Daarnaast is er een landelijk project van de Raad van Hoofdcommissarissen onder de titel ''Digitaal opsporen''. Dat project heeft voorstellen gedaan voor de opleidingsorganisatie die zich bezighoudt met digitaal opsporen. Die voorstellen zijn inmiddels ook door de Raad van Hoofdcommissarissen aanvaard en worden uitgevoerd met als doel dat in 2008 alle tactisch rechercheurs aanvullend zijn opgeleid. Ten slotte kennen wij het NHTCC, het National High-Tech Crime Center. Ook dat is op zichzelf een belangrijke verbetering voor het internet. Desondanks moet de Kamer niet de illusie hebben dat wij op het internet kunnen surveilleren zoals dat op straat mogelijk is.

De heer **Van Dam** (PvdA): Dit lijkt mij bij uitstek een kwestie die losstaat van de discussie over het politiebestel. De activiteiten op het internet lijken mij de verantwoordelijkheid van het KLPD.

Minister **Donner**: Het aardige is dat die niet decentraal zijn.

De heer **Van Dam** (PvdA): Als ik goed ben geïnformeerd, doen de digitale rechercheurs aan opsporing op het moment dat er sprake is van een aangifte. Zij gaan terugzoeken naar sporen en proberen op die manier een verdachte te traceren. Daarnaast zijn er de zogenaamde internetrechercheurs. Ik neem aan dat die terminologie klopt. Ik heb begrepen dat er slechts een aantal internetrechercheurs zijn. Die rechercheurs surveilleren en betrappen op heterdaad. Op basis van wat zij op heterdaad waarnemen, proberen zij om daders te achterhalen. Op internet kun je er het beste bij zijn op het moment waarop zaken gebeuren. Als je het allemaal achteraf terug moet zoeken, is dat erg lastig, zeker bij het soort slimme hackers waarover wij het meestal hebben. Is die capaciteit van die internetrechercheurs, die moeten surveilleren op internet, wel voldoende? Ik snap natuurlijk dat je niet evenveel agenten op internet hebt als op straat, maar ik heb gehoord dat er voor heel Nederland minder dan twintig internetrechercheurs zijn. Dat lijkt mij wel heel erg beperkt.

Minister **Donner**: Daar kan ik niet precies op antwoorden, omdat u nu een definitie gebruikt die niet correspondeert met mijn definitie. Ik ben mij er zeker van bewust dat in de afgelopen tijd een vrij snel expanderend aantal mensen hiermee bezig is. Daarom zal eind deze maand nog verdere besluitvorming plaatsvinden over het National High-Tech Crime Center en de capaciteit daarvan, maar in het licht van de omvang van het probleem, zal dat waarschijnlijk nog tekortschieten. Ik neem uw zorg en de zorg van de Kamer in het algemeen over dit punt dus mee. Ik beluister immers in wezen bij u allen dat u het wel aardig vindt om de wetgeving nu te aanvaarden, maar ook vraagt hoe het zit met de handhaving.

De heer **Van Dam** (PvdA): Ik neem aan dat wij, op het moment dat die besluitvorming plaatsvindt, daarover nader worden geïnformeerd. Dan kunnen wij daar ook op terugkomen.

Minister **Donner**: Het komt vermoedelijk aan de orde zowel wanneer de minister van BZK en ik gezamenlijk de politieorganisatie bespreken als wanneer bij de begroting van het ministerie van Justitie de OM-begroting aan de orde is. Dat is al binnen twee maanden.

Mevrouw **Gerkens** (SP): Het zal u niet verbazen dat ik vragen stel over het project National High-Tech Crime Center, want de SP-fractie heeft al vaker, ook schriftelijk, vragen gesteld die erop gericht waren om dat project te continueren. U hebt toen gezegd dat dat project eindig is en tot 1 december 2005 loopt. U hebt ook gezegd dat u vindt dat het naar tevredenheid functioneert. Het is nu september. Het zou goed zijn om nu

al duidelijk te maken of wij verder gaan met dit project. Mijn fractie zou daar zeer voor zijn.

Minister **Donner**: Ik heb zojuist aangegeven dat die beslissing deze maand op de agenda staat. Die beslissing is niet alleen afhankelijk van mij, maar ook van de minister van BZK. Derhalve kan ik de Kamer daar volgende maand over inlichten. Op dit punt heb ik wel enige geruststellende woorden. De minister van BZK en ikzelf zijn er op bezoek geweest en waren zeer onder de indruk.

De tweede algemene vraag die door velen van u is gesteld, betreft de bevriezingsbevoegdheid: biedt die geen alternatief voor de bediscussieerde dataretentiemaatregel? Het antwoord daarop is ''nee''. De bevriezingsmaatregel is een specifieke bevoegdheid om met betrekking tot vluchtig materiaal – dat is er; dat was een van de vragen – te bevelen dat het bewaard wordt. In een onderzoek met betrekking tot zaken die ermee in verband gebracht kunnen worden, kan ik op dit moment naar de toekomst toe inderdaad bevriezen. Dataretentie biedt met name een mogelijkheid om terug te gaan in de tijd: als nu een misdrijf wordt gepleegd, kan in het verleden eventueel worden teruggevonden wat de gangen van de dader, het slachtoffer en eventuele betrokkenen zijn geweest. Het gaat dus om fundamenteel verschillende zaken. Dataretentie is ook niet gespecificeerd ten aanzien van een persoon. Het blijft wel zo dat de toegang voor de overheid beperkt blijft tot gevallen waarin door middel van de normale bevoegdheden ten aanzien van onderzoek besloten is dat men toegang krijgt tot het geheel. Op dat punt weet men dan dat die informatie er moet zijn. Dat is ook een verschil met het bevriezingsbevel. Een bevriezingsbevel heeft betrekking op specifieke informatie die er op het moment van het bevriezingsbevel is. De dataretentie regelt in de eerste plaats wat men moet bewaren en dat kan meer zijn dan men normaal zou bewaren. Dat is een onderdeel van de discussie. De essentie van dataretentie is dat het niet alleen een kwestie van de duur is, maar ook van de omvang. Als de dataretentie geregeld is, dan weet ik gelijk dat in alle landen die gegevens aanwezig moeten zijn voor die duur. Bij een bevriezingsbevel weet ik alleen dat een overheid die bevoegdheid heeft en dan moet ik nog maar hopen dat de gegevens die ik verwacht er ook daadwerkelijk zijn. Dat zijn twee zaken die niet met elkaar verward kunnen worden.

Een andere vraag die door verschillende woordvoerders is gesteld, is of het gebruik van georganiseerde misdaad een functie heeft voor internet. Ik denk dat dit in eerste instantie een kwestie is van de uitleg die de rechter zal moeten geven aan de definitie van georganiseerde misdaad. De essentie daarvan is dat ik niet meer voor ieder van de betrokkenen de volledige betrokkenheid moet aangeven, maar dat ik die door de combinatie kan construeren. De heer Van Dam kwam met het voorbeeld van een groep jongens die wordt aangestuurd vanuit Rusland. Ik denk dat dit onder bepaalde omstandigheden een vorm van georganiseerde misdaad zal geven, maar dat kan ik niet op voorhand zeggen. Niet iedere willekeurige groep op internet kan ik als georganiseerde misdaad definiëren, maar zodra men gezamenlijk optreedt, kan ik dat heel wel.

De vraag van mevrouw Gerkens was hoe het zit als één persoon actief is. Dan gelden de gewone bevoegdheden die ik heb. De bevoegdheden voor het georganiseerde verband zijn extra om onderzoek te kunnen doen naar het georganiseerde verband als geheel. Dat maakt het mij mogelijk om buiten de ene verdachte te treden op wie ik anders mijn aandacht en mijn bevoegdheden moet richten.

Mevrouw **Gerkens** (SP): U zegt dat het ook aan de rechter is om te bepalen hoe dat te interpreteren, maar daar zit volgens mij juist het probleem. Ik weet ook niet zo goed hoe wij dat hier kunnen oplossen, maar misschien kunnen dit debat en de uitleg van de wetgever daarbij helpen. Veel rechters-commissarissen denken nog niet in cybercrimetermen. Zij denken bij georganiseerde misdaad nog steeds aan een andere soort misdaad, zoals wij die in het dagelijkse leven kennen. Zij beseffen te weinig hoe die cyberwereld in elkaar zit. Ik zeg niet dat wij het begrip georganiseerde misdaad in de hele wetgeving moeten laten vervallen, want daar zou mijn fractie ook geen voorstander van zijn. Willen wij echter adequaat kunnen optreden, dan moeten wij rechters handvatten geven om verder onderzoek te doen naar misdaad die niet georganiseerd lijkt, maar dat wel is. Hoe gaan wij dat oplossen?

Minister **Donner**: Ook dat is een kwestie van opleiding. De zware cursus wordt zowel door de staande als zittende magistratuur gevolgd, ook om binnen de zittende magistratuur deskundigheid op dit terrein te ontwikkelen. Ik zal niet ontkennen dat het best mogelijk is dat op een goed moment een bepaalde rechter-commissaris of een bepaalde rechter bij gebrek aan kennis in eerste instantie zal zeggen dat het geen georganiseerde misdaad is. Dat is de klassieke situatie, waarbij wij eventueel door rechtspraak moeten komen tot een nadere invulling van wat daaronder valt. Voor het overige gaat het om de vraag wat het kenmerk van de georganiseerde misdaad is. Die bevoegdheden zijn nodig omdat ik dan buiten de ene persoon kan treden op wie ik mij anders dan bij een verdenking moet richten. Het zal dus aan het Openbaar Ministerie zijn om aan te tonen dat de misdrijven worden gepleegd in een georganiseerd verband. Derhalve kunnen die bevoegdheden ook worden uitgeoefend ten aanzien van andere personen, die op zichzelf genomen nog geen verdachte zijn. Georganiseerde misdaad geeft alleen maar een extra bevoegdheid bovenop de specifieke bevoegdheid ten aanzien van een verdachte.

Mevrouw **Gerkens** (SP): Misschien zou ik wel willen zeggen dat wij die extra bevoegdheden niet alleen bij georganiseerde misdaad moeten hebben, juist omdat het zo moeilijk is om bij ICT-gerelateerde misdaden aan te tonen dat er van georganiseerde misdaad sprake is. Misschien moeten wij de mogelijkheden bezien om de bijzondere bevoegdheden voor internetgerelateerde misdaden uit te breiden.

Minister **Donner**: Ik ken de instelling van uw fractie op dit terrein, en ik denk dat u nu te snel gaat. Stel dat er één internetverdachte is, ten aanzien van wie ik bevoegdheden heb, dan kan ik bepaalde bevoegdheden ook ten aanzien van andere personen uitoefenen, als ik kan aantonen dat er sprake is van georganiseerde misdaad. Ook wat

internet betreft zal ik dan toch bepaalde relaties moeten kunnen aantonen, want anders schep ik een bevoegdheid die tegen iedereen kan worden uitgeoefend.

Dan kom ik nu toe aan de vraag of een aanbieder zijn klanten moet scannen en of hij aansprakelijk is als zijn klanten een virus verspreiden. Het antwoord op die vraag kan zijn dat de aanbieder doorgaans niet aansprakelijk zal zijn voor het handelen van zijn klanten. Dat wordt anders als hij weet dat er strafbare handelingen plaatsvinden en dat hij gebruikt wordt om een virus door te geven. De officier van justitie kan een bevel geven aan de aanbieder om de site te sluiten. Als de aanbieder dat doet, is zijn strafrechtelijke aansprakelijkheid weg. Doet hij het niet, dan wordt hij door de mededeling strafrechtelijk aansprakelijk als vervolgens blijkt dat er strafbaar wordt gehandeld. Ik denk dat dit een zeer verantwoorde regeling is.

Er is ook gevraagd waarom opsporingsonderzoek plaatsvindt zonder dat de eigenaar toestemming heeft gegeven. Daarbij gaat het om artikel 126l van het Wetboek van Strafvordering. Het is nu al mogelijk om, zonder aankondiging vooraf, vertrouwelijke communicatie binnen besloten netwerken op te nemen met een technisch hulpmiddel. Daarbij kan het gaan om een ''bug'', een kevertje, in een computer, voor het registreren van toetsaanslagen en muisklikken. Daarnaast is het op grond van het huidige artikel 125j nu ook al mogelijk om, in het kader van een lopend onderzoek, vanaf de plaats waar de doorzoeking plaatsvindt elders aanwezig geautomatiseerd werk te onderzoeken. Het is dus niets nieuws. Het Cybercrimeverdrag verplicht ons echter om op dit punt de bewuste bevoegdheid te scheppen, ook op de terreinen waar het uitoefenen daarvan technisch gewoon nog niet mogelijk is. Aan de andere kant hoorde ik laatst ook dat de mogelijkheid al bestaat om in het enkele voorbijgaan telefoons leeg te vegen. Dit is een voorbeeld van wetgeving waarmee op de techniek vooruit wordt gelopen, maar het is niet principieel iets nieuws. De controles blijven dezelfde als bij de andere vormen van tappen. De technische mogelijkheid houdt echter in dat de last niet meer gericht is tot de provider. De politie en de andere opsporingsinstanties kunnen rechtstreeks tappen. De aangekondigde nota van wijziging gaat daarover en draait een gedeelte terug, in de zin dat wordt voorgesteld dat ten minste moet worden voldaan aan technische eisen, zodat wij niet de figuur krijgen dat aftappen op alle mogelijke manieren mogelijk is. De regeling is echter een gevolg van het aanvaarden van het Cybercrimeverdrag. Gevraagd is ook of artikel 138b – de heer Van Dam heeft er een amendement op ingediend – voorziet in het geval dat de pleger iemand anders is. Daar is artikel 47 Wetboek van Strafrecht op van toepassing, dat het doen plegen van een strafbaar feit gelijkstelt aan het plegen. Op dit moment is dus in het strafrecht geregeld dat de DDoS-aanval waar de heer Van Dam het over had – ik zou niet weten waar het over gaat – die gepleegd wordt door tussenkomst van een ander, daaronder valt.

De heer **Van Dam** (PvdA): Ik heb nog een verduidelijkende vraag. Misschien kan ik mijn amendement wel intrekken. Of misschien moet ik aan de minister uitleggen wat een DDoS-aanval is.

Minister **Donner**: Het is handig als u dat eerst even uitlegt.

De heer **Van Dam** (PvdA): Bij een DDoS-aanval laat je niet zozeer anderen een strafbaar feit plegen, maar je laat computers een strafbaar feit plegen.

Minister **Donner**: Ja, maar nogmaals: óf je gebruikt een instrument zodat de uitleg is dat je het zelf pleegt, óf die computer wordt toegerekend aan een andere persoon en dan dóe je het plegen. Dat is hetzelfde als wanneer ik een instrument gebruik dat indirect werkt. Als ik dat redelijkerwijs mag verwachten van dat instrument, dan pleeg ik. Daarom ben ik ook de verantwoordelijke wanneer ik met een ricochetkogel iemand anders doodschiet, hoewel je strikt genomen kunt zeggen: dat kon ik niet uitrekenen.

Mevrouw Gerkens en anderen vroegen of wij de bepaling over de passen niet moeten uitbreiden. Het gaat hier om een bepaling in artikel 232: betaalpas, waardekaart of enig andere publieke kaart. Daaronder vallen ook chipkaarten, waarmee immers langs geautomatiseerde weg betalingen kunnen worden verricht. Het is wel een wijziging die al door uw Kamer is aanvaard, die al in de wetgeving is opgenomen. Dat is vrij recent gebeurd. De bepaling is een jaar oud. Daarom ben ik enigszins huiverig om deze bepaling nu verder uit te breiden. Je blijft uiteraard altijd zitten met de vraag of je voldoende onafhankelijk bent van techniek of dat je ergens mee de wetgeving techniekafhankelijk maakt. Tot nu toe is niet gebleken dat er op dit punt problemen ontstaan, maar deze bepaling is bij Staatsblad 204 opgenomen bij de wet handelend over de fraude met niet-chartaal geld.

Mevrouw **Gerkens** (SP): Voorzitter. Ik snap de bedenkingen van de minister, maar het gaat hier niet alleen over geld. Het gaat ook over fraude en misbruik van andere gegevens. Ik ben de laatste die zegt dat wij iedere dag alles maar moeten veranderen wat wij hebben, maar wij zitten wel met een enorme gevoeligheid van de tijdsgeest op het moment dat wij te specifiek alles omschrijven. Tegelijkertijd is dat de moeilijkheid bij wetgeving, want je moet het ook weer niet te ruim doen. Ik zou de minister toch willen vragen om nog eens te kijken of wij deze techniek niet iets moeten uitbreiden voordat wij weer achter de feiten aanlopen.

Minister **Donner**: Juist het gevaar van te techniekafhankelijke wetgeving loop ik bij die benadering. De omschrijving is nu vrij abstract. ''Betaalpas, waardekaart'' geeft aan in welke categorie ik moet denken, ''of enig andere voor het publiek beschikbare kaart bestemd voor het verrichten of verkrijgen van betalingen of andere prestaties langs geautomatiseerde weg''. Zodra ik technische specificaties ga opnemen, dreigt dat algauw een beperking te zijn ten opzichte van de bestaande bepaling. De discussie hierover heeft plaatsgevonden, daarom verwijs ik naar die andere wet. Ik zou willen voorkomen dat wij door een discussie hier de uitleg gaan wijzigen die de wetgever heeft gegeven aan die bepaling. Er is een voorbeeld gegeven over identificerende gegevens. Als ik dat zou opnemen, valt de chipkaart er niet meer onder. Een chipkaart bevalt namelijk geen

identificerende gegevens. Immers, het is plastic geld.

Mevrouw **Gerkens** (SP): Dat is de chipkaart niet, maar dat is een ander verhaal. Ik denk ook aan de mogelijkheid die bij sommige discotheken wordt toegepast: een chip die in een arm wordt ingebracht. Valt dat er ook onder?

Minister **Donner**: Tenzij ik mijn arm gebruik voor betaling of andere prestaties. Als ik mijn arm met zo'n chip ''in de muur'' kan steken, waarna er geld uitkomt vanwege die chip, valt het eronder. Ik hoop overigens dat ons dat voorlopig bespaard blijft.

Voorzitter. Ook de heer Van der Staaij heeft vragen gesteld over de handhavingscapaciteit. Daar ben ik dus al op ingegaan.

In verband met de vraag over artikel 138a of het open is, heb ik al aangegeven dat dit het geval is, wanneer niet duidelijk is dat het niet afgesloten is. Het is dus niet vereist dat de hacker een beveiliging buiten werking stelt. In dezelfde situatie als bij de open voordeur moet uit andere omstandigheden wel duidelijk zijn dat ik mijn computer geen publieke plaats maak. Dat kan op verschillende wijzen gebeuren. Dit heeft dan te maken met de ontwikkeling van de rechtspraak op dit terrein over de betekenis van ''wederrechtelijk''.

Over het algemeen ben ik ook van mening dat het vooral een zaak is van gedegen voorlichting over de risico's die men loopt, als men zo'n computer gaat gebruiken en daar gegevens op zet.

Naar aanleiding van de vraag over de wetgevingsagenda van de toekomst heb ik al geantwoord dat daar op dit moment geen specifieke punten op staan, behalve uiteraard de regeling van de dataretentie.

De primaire algemene vraag van de heer Van Fessem was ook, of het wetsontwerp wel voldoende bij de tijd is. Ik herhaal dat ik nu niet wil komen aan de definities die in het Cybercrimeverdrag zijn opgenomen. Een van de essenties daarvan is namelijk de gelijkheid van definities. Anders ontstaat er geleidelijk weer verwarring. Dit sluit uiteraard niet uit dat wij er steeds alert op moeten zijn of wij op dat punt wel bij de tijd zijn. Ik sluit als gevolg hiervan ook niet uit dat wij elkaar hierover weer zullen treffen.

De heer Van Fessem heeft ook een vraag gesteld over het strafbaar stellen van hacken. Daarop ben ik zojuist ingegaan in antwoord op de vragen daarover van de heer Van der Staaij.

Ook door de heer Weekers zijn er nog vragen gesteld over spam. Zo vroeg hij of ik op dat punt van mijn geloof was gevallen. Dat is niet het geval, want indertijd heb ik in de discussie over het wetsvoorstel inzake e-commerce al aangegeven dat ik er tegen was om dit punt in dat wetsvoorstel te regelen, omdat het in het onderhavige wetsvoorstel aan de orde zou komen. Het ligt besloten in artikel 138b dat ik niet per definitie strafrechtelijk tegen spam wil optreden. Ingevolge dat artikel ben ik wel tegen spam, indien het om het zodanig verzenden van spam gaat dat daardoor de toegang tot ''mijn'' computer wordt belemmerd dan wel wezenlijk verhinderd. Tegen deze achtergrond is dus niet iedere spam strafrechtelijk verboden. Nogmaals, er moet primair aangetoond worden dat de betrokkene die spam verstuurt, daarmee de opzet heeft om de werking van het ontvangende computersysteem te belemmeren. Dit is een uitwerking c.q. specificatie van de bestaande meer algemene bepaling inzake het verstoren van netwerken. Strafrechtelijke handhaving van een nog grotere specificatie is volgens mij niet realistisch. Daar is ook geen grond voor, omdat hierbij primair het uitgangspunt is, dat er in wezen opzettelijk geprobeerd wordt om ''mijn'' computer buiten werking te stellen dan wel wezenlijk te belemmeren. Dan kan al het geval zijn als daardoor de toegang tot mijn computer wordt vertraagd of als ik minder snel informatie kan oproepen. Het functioneren wordt dan immers ondergraven. Dit in antwoord op een van de vragen van de heer Van Fessem.

Hij vroeg ook naar de verkoop van hackprogramma's in de winkel. Dat zal strafbaar zijn. 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; de heer Van Fessem beschreef de situatie dat men zijn eigen computer wil testen of deze veilig is tegen hacken. Helaas is dat de beperking die hieraan is gesteld. De winkelier kan het echter slechts met de opzet van hacken verkopen is daarom ingevolge artikel 139d, tweede lid, strafbaar.

De heer **Van Fessem** (CDA): Het verhaal dat de minister nu vertelt, staat ook in de memorie van toelichting. Ik ben juist van mening dat het een smoes is, dat men het programma zou hebben om de eigen computer te kunnen hebben. Voor de volledigheid wil ik dat nogmaals gezegd hebben.

Minister **Donner**: Daar ben ik het mee eens, maar het is erg gevaarlijk om de enkele aanwezigheid van een hackprogramma op de computer direct in de sfeer van wederrechtelijkheid te plaatsen. Dan gaan wij erg ver in het strafrecht achter de voordeur.

De vraag over de aansprakelijkheid met betrekking tot artikel 273d is door een aantal leden gesteld. Mevrouw Gerkens en de heer Van Dam hebben over dit onderdeel een amendement ingediend, waarvan ik het aannemen moet ontraden omdat het in wezen de betekenis van artikel 273d verandert. Dit artikel is nu het equivalent van het briefgeheim, op internet. Dat geldt ook in termen van communicatiesystemen, doch in die gevallen is het afhankelijk van de afspraken die binnen de onderneming zijn gemaakt. Het artikel kan dus inderdaad gevolgen hebben voor de arbeidsrechtelijke verhoudingen. Als binnen een bedrijf een netwerk mede is bedoeld voor vertrouwelijke informatie, zal het onder deze bepaling vallen wanneer daarvan kennis wordt genomen. Daardoor kan ik het artikel niet uitbreiden tot financiële netwerken. Die zijn immers niet bestemd voor communicatie, maar voor mijn contact met de bank. Ik ben dan met iets geheel anders bezig. De bank leest mijn gegevens. Dat is ook de bedoeling, want zij zijn aan hem geadresseerd, tenzij hij als faciliteit een communicatienetwerk aanbiedt, maar dat valt dan weer wel onder deze bepaling. Met dit amendement zou de strekking van de bepaling dus worden verward. Ik herhaal het aannemen van dit amendement te ontraden.

De heer **Van Dam** (PvdA): Ik acht het zeer wel mogelijk dat dit wetstechnisch niet op de juiste plaats is ingevoegd. Ik had daarbij ook zelf al

wel stilgestaan. Misschien is er dan een andere uitweg. Ik ben daarom vooral benieuwd of de minister het wel eens is met het principe?

Minister **Donner**: Welk principe?

De heer **Van Dam** (PvdA): Ik doel op het principe dat net zoals bij een telecombedrijf wordt gesteld dat de communicatie tussen mensen geheim is en dus niet ontvreemd en gebruikt mag worden, dit ook zo zou moeten zijn wanneer het geen specifieke telecomdienst betreft, maar een aan internet gebonden dienst. Er worden immers steeds meer gegevens van mensen verwerkt en opgeslagen. Ook die gegevens moeten niet ontvreemd kunnen worden en er zou dezelfde strafbepaling op moeten staan. Ik meen dat mevrouw Gerkens met deze zelfde overweging haar amendement heeft ingediend.

Minister **Donner**: Dan hebben wij het toch over twee wezenlijk verschillende zaken. Het een is het creëren van een equivalent van het briefgeheim. Degene die het bericht transporteert behoort niet mee te kijken in de berichtgeving die langs komt. Het genoemde punt moet echter worden bezien in het kader van de geheimhoudingsplicht. De houder van een bestand is onder de privacywetgeving al verantwoordelijk voor het beperken van de toegang daartoe. Bij vertrouwelijke gegevens, zoals bankgegevens, gelden ook algemene strafbepalingen over geheimhouding en zal de houder beschermingsmaatregelen moeten nemen. Als dat onvoldoende is in het licht van de huidige mogelijkheden, moeten wij daarover praten, maar dat is een wezenlijk andere situatie.

Voorzitter. De heer Van Fessen vroeg naar aanleiding van het bevriezingsbevel naar de situatie waarin de provider de gegevens toch al bewaart. Ik ben het met hem eens dat een bevriezingsbevel dan misschien niet nodig is, maar ik heb niet de zekerheid dat de provider de gegevens 90 dagen bewaart. Het blijft zijn verantwoordelijkheid en vrijheid om deze al dan niet te wissen. Ook in dergelijke situaties kan het dus geen kwaad om een dergelijk bevel te geven.

Vluchtig betekent snel verdwijnend. Een boek kan bijvoorbeeld worden weggegooid, maar is minder vluchtig dan gegevens op een computer. De kosten kunnen inderdaad worden vergoed op grond van artikel 592 van het Wetboek van Strafvordering.

Ik meen dat het wetsvoorstel voldoende techniekonafhankelijk is. Er is zoveel mogelijk gekozen voor techniekneutrale omschrijvingen. In de bepaling die ik voorlas wordt bijvoorbeeld met enkele begrippen aangegeven over welke categorie het gaat, waarna de categorie zodanig wordt verbreed met techniekneutrale begrippen, dat vergelijkbare technieken er ook onder kunnen vallen. Ik denk dat wij hiermee even vooruit kunnen, maar kan daar mijn hand niet voor in het vuur steken.

Ik dank de heer Weekers voor zijn steun voor het wetsontwerp. Ik ben al ingegaan op zijn vragen over het KLPD en het NFI, hoewel men in dit verband eerder aan het National High-Tech Crime Center moet denken als opsporingsinstantie dan aan het NFI. De vraag over de verdediging tegen virussen betrof voornamelijk de capaciteit. De minister van Binnenlandse Zaken hoopt binnenkort met een notitie te komen over de bescherming van vitale netwerken, waarvan dit een aspect is.

De heer Van Dam stelde vragen over de punten waarover ook zijn amendementen gaan. Ik ben al ingegaan op zijn amendement over artikel 138b. Het ''doen plegen'' valt daar al onder via artikel 47.

Naar aanleiding van zijn vraag over een voor het publiek beschikbare kaart merk ik op dat de geschiedenis is vastgelegd in de wet die het chartale geldverkeer regelt. Ik denk dat dat voldoende is. De bepaling zou in onderlinge samenhang moeten worden geamendeerd, want wij moeten niet in het voorliggende wetsvoorstel met een andere definitie gaan werken dan in de genoemde wet. Blijkens de wetsgeschiedenis wordt in die wet dezelfde bepaling bedoeld. Daarom zou ik ook de aanneming van dit amendement willen ontraden.

De heer **Van Dam** (PvdA): Ik kan me voorstellen dat er bij een wet voor chartaal verkeer niet direct gesproken is over alle technische mogelijkheden op het vlak van dragers van identiteitsgegevens, maar zulke gegevens kunnen ook nu al willekeurig in diverse apparaten opgeslagen worden. Je kunt je identiteitsgegevens bij wijze van spreken gewoon in je telefoon opslaan en je kunt overigens je telefoon ook gebruiken om betalingen te verrichten. Volgens mij moet je dit wetsartikel niet al te rigide formuleren, juist om te voorkomen dat je over een halfjaar met zaken wordt geconfronteerd die je zou hebben kunnen aanpakken als het nu wat ruimer was geformuleerd.

Minister **Donner**: Dat ben ik met u eens, maar de omschrijving in het wetsvoorstel is ruimer dan die van uw amendement, want daarin wordt bepaald dat het moet gaan om een drager van identiteitsgegevens. De chipkaart is geen drager van identiteitsgegevens, hij valt wel onder de huidige bepaling, maar met uw amendement zou dat niet meer zo zijn.

De heer **Van Dam** (PvdA): Goed, maar als je de huidige tekst handhaaft en daaraan de tekst van het amendement toevoegt, heb je alles te pakken.

Minister **Donner**: Nogmaals, ik denk dat wij met de huidige tekst een zeer brede formulering hebben voor de functie van dit artikel. Wij moeten er nu niet alles onder gaan brengen, want het gaat om strafbepalingen; anders zal de rechter ze gewoon inperken. Het lijkt mij dus niet verstandig.

Op het voorstel tot wijziging van artikel 273d ben ik eigenlijk al ingegaan toen ik reageerde op het betoog van mevrouw Gerkens. Met dat amendement wordt de strekking van het artikel in wezen uitgebreid.

Bij het amendement op artikel 16 gaat het om het tappen zonder tussenkomst van de provider. De ruime bepaling van apparatuur in de formulering hebben wij deels ontleend aan het Cybercrimeverdrag. De technische hulpmiddelen waarmee dit mogelijk is, zijn er nog maar in beperkte mate. Een voorbeeld ervan is de IMSI-catcher, die het mogelijk maakt om identificatienummers te onderscheppen. De Telecommunicatiewet stelt grenzen aan het actief scannen van de ether en zolang wij niet duidelijk maken om welke hulpmiddelen het hierbij gaat, lijkt het mij onverstandig om deze bepaling maar gewoon uit te breiden. Het gaat hierbij om bevoegdheden die wij de overheid geven, dat moeten wij niet met bakken doen, zelfs niet als wij ze aan mij geven.

De heer Van Dam en mevrouw Gerkens hebben de vraag van het informeren van de klant na een aanval van hackers aan de orde gesteld. Dit lijkt mij in eerste instantie een kwestie van privaatrechtelijke verhoudingen: de provider waarschuwt de klant als er ingebroken is. Als er al een reden was om dit wettelijk te regelen, zou het niet in het kader van de strafwetgeving moeten worden geregeld, maar in de aansprakelijkheidswetgeving. En ook daarbij geldt het beginsel dat men vertrouwen moet vinden waar men het gelaten heeft, dat is het privaatrechtelijke uitgangspunt. Ik denk dat dat zich geleidelijk aan ontwikkelt door zelfregulering, en op dit moment adequaat wordt gedekt. Dit is een punt dat in het kader van de consumentenbescherming aan de orde kan komen, en zeker niet moet worden afgedwongen via wetgeving.

De heer Van Dam heeft gevraagd of de bevoegdheden niet moeten worden verruimd, gelet op de misdrijven waarom het gaat. Daarbij gaat het om de bevoegdheid om te doorzoeken. Dat kan een onderzoeksmethode zijn die soelaas biedt bij het gebruik van versleuteling, maar de Wet bijzondere opsporingsbevoegdheden biedt nu al diverse andere bevoegdheden die met de huidige strafmaat kunnen worden ingezet. Het opnemen van vertrouwelijke communicatie is nu al bij kinderporno mogelijk, maar kan niet worden toegepast in een woning, omdat dan de strafmaat te laag is. Ik zou dan kijken of de strafmaat niet moet worden verhoogd, eerder dan doorbreking voor één specifiek delict.

De heer **Van Dam** (PvdA): Bij kinderporno kan ik mij nog iets voorstellen. Maar bij economische delicten is het wat raar om de strafmaat te verhogen. Een beetje slimme internetgebruiker weet zijn communicatie zodanig te versleutelen dat alle bevoegdheden ter wereld onvoldoende zijn om hen aan te pakken. Je kunt bij dit soort zaken de communicatie alleen bij de bron, dus op de computer, onderscheppen.

Minister **Donner**: Ik kom hier in tweede termijn op terug.

Mevrouw Vos heeft voorgesteld, het ontoegankelijk maken van gegevens pas mogelijk te maken nadat de zaak bij de rechter is geweest. Ik ben bang dat die bevoegdheid dan doorgaans te laat komt. De instanties die het bevel van het ontoegankelijk maken geven, zullen met recht aan moeten geven wat de strafbaarheid van het geheel is. Nogmaals, de rechtvaardiging om het toe te passen zit in de mate van strafbaarheid van wat er wordt aangetroffen. Dan moet de maatregel zo snel mogelijk kunnen worden toegepast, want we hebben hier te maken met zaken die zo weer verdwenen zijn.

De provider beoordeelt niet of de opsporingsinstanties terecht tappen. De normale bepalingen ter zake blijven van toepassing, ook als er zonder tussenkomst van de provider wordt getapt.

Willen wij de computercriminaliteit effectief kunnen bestrijden, dan zullen wij voorbereidingshandelingen, zoals het verkopen van hackerprogramma's, strafbaar moeten stellen. Doen wij dit niet, dan blijven wij achter de ontwikkelingen aanlopen.

Er is eerder gesproken over de notificatieplicht in verband met de onbevredigende toepassingen van soortgelijke bepalingen met betrekking tot telefonie. Naar aanleiding van die discussie is het OM bezig met het opstellen van een plan van aanpak om de naleving hiervan te verzekeren. Dit geldt ook voor de notificatieplicht in dit wetsvoorstel.

De heer Van Dam vroeg zich af of de bevoegdheden voor het opsporen van georganiseerde criminaliteit ook op dit terrein ingezet moeten worden. Bij het OM loopt op dit moment een onderzoek naar de toepassing van die bevoegdheden naar aanleiding van een artikel in de Nieuwe Revu. Ik wil graag eerst de uitkomsten van dat onderzoek afwachten alvorens een oordeel hierover te geven.

De heer **Van Dam** (PvdA): Wilt u nog ingaan op mijn vraag over het publiceren van foto's op internet?

Minister **Donner**: Dit valt primair onder het portretrecht. Ik weet dat er in de Duitse wetgeving hierover een bepaling is opgenomen. Ik wil dit niet in dit wetsvoorstel regelen, maar ik ben wel bereid om hier nog eens naar te kijken, mede in verband met de Duitse regels op dit terrein. Ik moet een duidelijk beeld hebben van de strafwaardige elementen en van de elementen die primair via het privaatrecht moeten worden afgedaan.

□

Mevrouw **Gerkens** (SP): Voorzitter. Ik dank de minister voor zijn uitgebreide beantwoording. Het was een interessant samenspel tussen de cyberkennis van de oppositie en de juridische kennis van de minister. Ik moet zeggen dat de minister zich kranig weerde in dit debat met zo veel vaktermen.

Ik ben blij met de toezegging dat de minister zich binnen het kabinet zal inzetten voor een publiekscampagne. Ik meen ook waarderende geluiden gehoord te hebben voor het National High-Tech Crime Center. Ik hoop dat dit uiteindelijk tot een positieve uitkomst zal leiden, maar ik wacht dat nog even af.

Ik kan nu niet precies overzien welke consequenties de beantwoording voor de ingediende amendementen heeft. Ik zal dit nog nagaan. De minister heeft duidelijk gemaakt dat heel veel punten nu eenmaal worden bepaald door het verdrag en dat wij het daarom zo doen.

Het signaal van de Kamer is duidelijk. Ik wil de minister vragen om echt te proberen door hetgeen wij nu maken, de achterstand in te halen en vooral actueel te blijven op dit gebied. Hoe wil de minister er in de toekomst voor zorgen dat wij niet weer achterlopen en ons strafrecht ook op dit punt actueel houden?

De Kamer en de minister vinden opsporing onontbeerlijk. De minister heeft een aantal zaken genoemd dat al plaatsvindt. Dat klinkt goed, maar het kan mijn fractie niet snel of gedegen genoeg gaan. Dit wetsvoorstel is een goede eerste stap. Wij moeten vooral blijven lopen. Ministerie, politie en justitie moeten zich blijven focussen op het actueel houden. Stilstand is hier echt achteruitgang. Dat kan ik niet genoeg benadrukken.

Wij hebben een kort debat gehad over het dilemma van de georganiseerde misdaad versus de ICT-misdaad en de organisatie daarvan. Ik ben erg blij met het debatje met de minister en ik ben tevreden met zijn antwoorden. Ik vraag hem na te blijven gaan of wij het probleem hiermee echt kunnen aan pakken dan wel of er uiteindelijk toch aanvullende wetgeving nodig is. Dit is immers iets wat zich zal moeten uitkristalliseren. Ik vertrouw erop dat

het apparaat dat achter de minister staat, dat op tijd signaleert.

Als wij zoiets als cybercrime in een wetboek willen omvatten, moeten wij gaan zoeken. Dat maakt dit debat wel duidelijk. Waar liggen dan de belangen buiten de cyberwereld en hoe kunnen wij een balans vinden zodat wij de criminaliteit op dat gebied toch kunnen aanpakken? Het besef dat de cybercrime anders is dan de criminaliteit buiten de cyberspace is vandaag in ieder geval behoorlijk duidelijk geworden. Dat moeten wij ook vasthouden. Ik vind dan ook dat mensen er echt recht op hebben om te weten dat hun gegevens gestolen kunnen zijn. Zo kunnen zij voorkomen dat daar voor hen schade uit voortvloeit. Hierbij wijs ik overigens ook op de eigen verantwoordelijkheid, die er absoluut is; we moeten niet de voordeur openzetten. De minister zegt dat wij dat niet in deze wet kunnen doen, maar dat misschien op een andere plek moeten regelen. Dat begrijp ik. Ik dien daarom samen met de heer Van Dam een motie in waarin ik de minister verzoek voorstellen te doen.

Motie

De Kamer,

gehoord de beraadslaging,

overwegende dat burgers en bedrijven het recht moeten hebben te weten dat hun gegevens in verkeerde handen terecht zijn gekomen of kunnen zijn gekomen;

verzoekt de regering, een voorstel uit te werken dat leidt tot de verplichting van bedrijven, overheden en andere organisaties om burgers en bedrijven te informeren dat hun gegevens ontvreemd zijn, of dat de systemen van de organisatie gehackt zijn en hiermee voor 1 juni 2006 naar de Kamer te komen,

en gaat over tot de orde van de dag.

De **voorzitter**: Deze motie is voorgesteld door de leden Gerkens en Van Dam. Naar mij blijkt, wordt zij voldoende ondersteund.

Zij krijgt nr. 18 (26671).

□

De heer **Van Dam** (PvdA): Voorzitter. Ik dank de minister, die vandaag ongetwijfeld ook andere dingen aan het hoofd had, maar zich in dit debat toch kranig heeft geweerd. Als ik zie hoe ik de afgelopen dagen geworsteld heb met het strafrecht, waar ik mij niet dagelijks mee bezighoudt, kan ik mij voorstellen dat de minister op dezelfde wijze geworsteld moet hebben met de terminologie die hier af en toe over tafel ging.

In mijn eerste termijn heb ik een aantal amendementen ingediend om het zekere voor het onzekere te nemen. Mij is uit de beantwoording van de minister gebleken dat de amendementen op de stukken nrs. 13 en 15 niet nodig zijn. Daarom trek ik die amendementen in.

De **voorzitter**: Aangezien de amendementen-Van Dam (26671, nrs. 13 en 15) zijn ingetrokken, maken zij geen onderwerp van beraadslaging meer uit.

De heer **Van Dam** (PvdA): Voorzitter. Op dat gebied ben ik in elk geval gerustgesteld.

Het amendement op stuk nr. 14 zal ik aanpassen. Ik heb nog enige twijfel over het amendement op stuk nr. 16. De minister zegt terecht dat wij niet bakken met bevoegdheden moeten overhevelen, terwijl wij niet zeker weten over welke bevoegdheden wij het hebben. Ik ben wel gevoelig voor die waarschuwing, maar ik wil hier niet over een jaar weer staan, omdat wij constateren dat er nieuwe mogelijkheden zijn die de politie niet kan gebruiken op basis van het artikel zoals het nu luidt. Als de minister mij kan geruststellen dat wij hier niet over een jaar weer staan, wil ik het amendement wel intrekken. Anders ga ik op zoek naar een formulering waarmee die bevoegdheden niet bij bakken worden overgeheveld, maar waarmee de deur ook niet op voorhand dicht wordt gezet.

Dat zijn de resterende punten bij dit wetsvoorstel, waarmee wij vooral snel aan de slag moeten gaan. De Kamer vraagt nogal vaak om rapportages, maar juist omdat er zoveel gebeurt op dit vlak, zou ik het op prijs stellen om een jaar na ingang een rapportage te krijgen van de minister in hoeverre deze wetswijziging bruikbaar is gebleken in de dagelijkse praktijk.

Minister **Donner**: Dat is de beste methode om te verzekeren dat wij hier over een jaar weer staan.

De heer **Van Dam** (PvdA): Bij goed nieuws hoeft u niet op te komen draven, dat weet u. Als u over een jaar een rapportage stuurt met goed nieuws, dan nemen wij die met veel enthousiasme voor kennisgeving aan.

Mevrouw Gerkens is in haar motie ingegaan op de verplichting aan bedrijven om kenbaar te maken dat zij zijn gehackt en dat daarbij mogelijk gegevens van burgers of bedrijven zijn ontvreemd. Ik vind het een recht voor burgers en bedrijven om te weten dat hun gegevens wellicht in verkeerde handen terecht zijn gekomen. Ik doe een beroep op de minister om die motie te omarmen.

Dan de opsporingsbevoegdheden. De minister zegt dat er een onderzoek loopt naar aanleiding van de publicatie in de Nieuwe Revu. Ik had niet het idee om deze kwestie vandaag op te lossen, want dat lijkt mij wat al te kort door de bocht. Het lijkt mij goed om dat onderzoek af te wachten. Als dat aanleiding geeft om opsporingsbevoegdheden uit te breiden, neem ik aan dat wij dat van de minister horen. De minister weet dat wij bereid zijn om daarover te spreken. Omdat bij deze specifieke kwesties alle andere opsporingsmiddelen niet toereikend zijn, zou je de stap moeten kunnen nemen om dergelijke zware opsporingsmethoden in te zetten.

Tot slot het publiceren van foto's. Het probleem is dat het portretrecht een civielrechtelijke kwestie is, zoals de minister al zei. Je kunt wel procederen, maar dan staat de foto of de opname al op internet en die krijg je er nooit, maar dan ook nooit meer af. Daarom doe ik een beroep op de minister om bij dit soort kwesties het strafrecht te kunnen inzetten. De minister kijkt hoe dat in Duitsland is geregeld. Ik meen dat er ook landen buiten Europa zijn die regelgeving op dit vlak in voorbereiding hebben. Ik hoop hierover nog nader van de minister te horen.

De heer **Van Fessem** (CDA): Mede namens de heer Weekers complimenteer ik de minister met hoe hij zich op deze dag door deze voor hem toch moeilijke materie heeft heengeslagen. Wij stellen dat zeer op prijs.

De **voorzitter**: Ik neem aan dat de minister dit breed uitgesproken compliment heeft ontvangen.

Van Dam

De vergadering wordt enkele minuten geschorst.

□

Minister **Donner**: Voorzitter. Ik dank de Kamerleden voor de complimenten die ik heb gekregen voor de wijze waarop ik deze materie heb behandeld. Ik verzeker u dat dit vandaag een prettige afleiding is geweest.

Ik huiver enigszins om op het voorstel van de heer Van Dam in te gaan dat inhoudt dat wij ons erop vastleggen om over een jaar te rapporteren. Op dit terrein ben ik het wel volledig met de Kamer eens dat wij ervoor moeten zorgen dat wij bij de tijd blijven. Dit probleem speelt voortdurend op allerlei terreinen. Het is dus niet zinvol om specifiek in dit kader te zeggen dat wij over een jaar bij de tijd moeten zijn. Alle Kamerleden hebben echter aangegeven dat wij met dit wetsvoorstel redelijk bij de tijd zijn en zij pleiten ervoor dat wij bij de tijd blijven. Daarmee ben ik het eens. Ik zeg toe dat wij de ontwikkelingen zullen monitoren. Wij zullen ons echter niet vastleggen op een rapportageplicht op bepaalde momenten. Ook bij de begroting van het ministerie van Justitie zal dit soort zaken aan de orde komen.

Ik ga ermee akkoord dat wij ingaan op het punt van de opsporingbevoegdheden in het licht van de ontwikkeling. Eerder ben ik ingegaan op het aspect van de foto's. Ik begrijp het probleem. Het heeft minder te maken met het punt van de rechtsrelatie. Met privaatrecht komt men echter niet ver, omdat niet duidelijk is wie aanspreekbaar is als zaken eenmaal op het internet staan. De enige die de bevoegdheid heeft om dergelijke zaken van het internet te halen, is de overheid. Zij beschikt namelijk over strafrechtelijke bevoegdheden. Er is wat dat betreft sprake van een breder probleem. Ik huiver er namelijk voor om dat specifiek met het strafrecht op te lossen. Dan moeten wij het immers steeds zoeken in het strafbare feit. Dit is een probleem van privaatrecht. Er zouden inderdaad bepaalde zaken moeten zijn waartegen men privaatrechtelijk zou kunnen optreden. Omdat niet duidelijk is wie men zou moeten aanpakken, verliest men zijn rechten. Dat is het vraagstuk. In die zin ben ik bereid om mijn gedachten daarover te laten gaan, ook in relatie tot die foto's. Het is echter een breder vraagstuk.

De heer **Van Dam** (PvdA): Misschien moet de minister even kijken naar artikel 139g van het Wetboek van Strafrecht, dat het openbaar maken van foto's strafbaar stelt voor zover die foto's binnenshuis en onder list of een kunstgreep zijn gemaakt. Mijn punt betreft het onderscheid op basis van waar die foto's gemaakt zijn. Gelet op de wijdverbreidheid van camera's in de openbare ruimte, vind ik dat onderscheid niet meer zo relevant. De strafbaarstelling is op zich dus geen nieuwigheid. Het gaat mij om de verbreding van de grondslag voor die strafbaarstelling.

Minister **Donner**: Dan bent u echt met een fundamenteel andere stap bezig. Camera's zijn er al een hele tijd in groten getale. Het fundamentele element is dat ik mij, wanneer ik de straat op ga, daarmee in wezen blootgeef aan anderen. Daardoor kan een ander mij op dat moment vastleggen. De bestaande bepaling verbiedt een ander om mij door kunstgrepen anders voor te stellen dan ik daadwerkelijk ben. De fundamentele keuze die gemaakt is, is dat ik nu geen recht heb om een ander te verbieden om het beeld van mij, zoals ik daar ben, op dat moment eventueel vast te leggen en eventueel op internet te plaatsen. Ik was immers zo op straat te zien. Binnen de woning is dat anders. Het opheffen van dat onderscheid is een brug te ver.

Een apart probleem is in hoeverre ik moet kunnen optreden tegen het eindeloos op internet zetten van foto's. Dat blijft naar mijn gevoel primair een zaak die in de privérelatie moet zitten, want primair moet iemand zich eraan ergeren voordat er kan worden opgetreden. Ik zie niet in hoe de overheid of een politieagent zou moeten weten wie zich wel of niet ergert om te bepalen of er moet worden opgetreden. Er zal dus een aangifte moeten zijn. Dan zouden wij de politie weer inzetten voor allerlei dingen, terwijl wij haar beter voor iets anders kunnen gebruiken. Het specifieke probleem is het verschijnsel dat een beeltenis op internet wordt gezet die je er niet meer af krijgt; je weet ook niet wie je moet aanspreken om die eraf te krijgen. Dat is een geldig probleem.

De heer **Van Dam** (PvdA): Volgens mij gaat het om twee kwesties, ten eerste om de foto of opname die in de openbare ruimte is genomen. Ten tweede is er het webcamvoorbeeld: mensen poseren op dat moment vrijwillig voor een webcam, maar komen er twee jaar later achter dat de foto nog steeds circuleert op internet. Ik denk dat het strafrecht het enige recht is dat een afschrikwekkende werking kan hebben. Als je dit privaatrechtelijk wilt aanpakken, krijg je de opname er immers niet meer af op het moment dat die eenmaal op internet staat. Dan kun je er wel privaatrechtelijk achteraan gaan, maar daarmee wordt het kwaad niet voorkomen. Ik denk dat het strafrecht wat dat betreft als afschrikking zou kunnen werken waarmee je het in een aantal gevallen misschien wel zou kunnen voorkomen.

Minister **Donner**: Mag ik voorstellen dat ik eerst even kijk naar artikel 139f? Ik word daar zojuist op gewezen. Dat is juist door de Tweede Kamer aanvaard, is pas vorig jaar in werking getreden en zou deze materie regelen, in ieder geval voor een deel.

De heer **Van Fessem** (CDA): De minister heeft het over het beter gebruiken van de opsporingscapaciteit van de politie. Bij een aangifte van iemand die zegt ''Mijn foto is door hem verspreid, want hij is de enige die die foto had'', gaat het echter meer om het opschrijven of constateren van een feit dan om de behoefte aan een opsporingsonderzoek.

Minister **Donner**: Ik bekijk nu even wat artikel 139f precies inhoudt. Dat is precies de bepaling waarnaar al werd verwezen. Die bepaling heeft betrekking op het probleem van het gebruik van ongeoorloofde foto's. Ik zou op dat punt geen uitbreiding van het strafrecht willen, want dan zal ik een opsporingsonderzoek moeten gaan doen. Waar zit de strafbaarheid in? Men zet een foto op internet en dan moet ik dat algemeen strafbaar gaan stellen. Het op internet plaatsen van een foto van anderen gaat de mogelijkheden van de overheid te buiten. Via internet worden voortdurend foto's doorgestuurd. Hele vakantieverslagen komen er langs. Die beeltenissen blijven staan en dat kan niet strafbaar gesteld worden. Over het specifieke punt hoe

je na verloop kunt optreden tegen foto's die ongewenst zijn, wil ik nog verder nadenken.

Mevrouw Gerkens heeft nog een vraag gesteld over georganiseerde criminaliteit. Wanneer ik daarop stuit, krijgt het de aandacht.

Dan kom ik bij de amendementen van de heer Van Dam. Wat betreft het amendement op stuk nr. 16 ligt het nog iets ingewikkelder. Dat amendement slaat ook terug op de regeling in de Telecomwet die de IMSI-catcher regelt. De Telecomwet maakt alleen de IMSI-catcher mogelijk. De bepaling die hier staat, geeft de opsporingsinstantie de bevoegdheid om dat middel te gebruiken. Een uitbreiding hier heeft dus geen effect, want dan zou eerst de Telecomwet moeten worden aangepast. Als dat gebeurt zonder dat men specifiek de apparatuur voor ogen heeft, krijgt de overheid een blanco cheque voor alle technische hulpmiddelen. Het is logisch om te discussiëren over de vraag wat er in het kader van de Telecomwet mogelijk is. Het gaat dan specifiek om het lokaliseren van een bepaalde mobiele telefoon. Als er andere apparatuur komt die dat mogelijk maakt, dan verwacht ik dat er vrij snel een wetsvoorstel komt om de bepalingen in de Telecomwet uit te breiden. Dit amendement heeft in ieder geval niet het door de heer Van Dam gewenste effect.

Ik denk dat er bij het amendement op stuk nr. 14 een verwarring is opgetreden. Het gaat om de bepaling van artikel 2.32. Die bepaling regelt nu in aansluiting op de wet op het chartale verkeer de strafbaarheid van ieder die door middel van een betaalpas of welke kaart dan ook probeert wederrechtelijk voordeel te verkrijgen. Dat is zo ruim dat ieder amendement op dat punt waarschijnlijk tot gevolg heeft dat de omschrijving wordt ingeperkt. Uit de discussie heb ik echter begrepen dat de heer Van Dam doelt op een ander probleem, namelijk het probleem van het gebruiken van identiteitsgegevens voor andere doeleinden, kortom het aannemen van een andere identiteit. Artikel 2.32 gaat echter heel specifiek over het gebruik van kaarten in het betalingsverkeer. Dat staat los van de vraag of die kaarten identiteitsgegevens bevatten. Ik moet aanneming van dit amendement dus ontraden. Dat zal namelijk niet leiden tot een verruiming. Bij de bredere vraag over identiteitsdiefstal hebben wij het over andere bepalingen dan deze.

Ten slotte ga ik in op de motie van mevrouw Gerkens.

De heer **Van Dam** (PvdA): In het wetsvoorstel wordt artikel 232 juist niet langer beperkt tot het betalingsverkeer, want daarin wordt ook gesproken van het verkrijgen van andere prestaties langs geautomatiseerde weg. Volgens mij wordt het een veel breder artikel, en dan ligt het volgens mij voor de hand om het artikel niet te beperken tot de fysieke kaarten, maar uit te breiden tot allerlei andere dragers van gegevens waarmee je toegang kunt krijgen tot prestaties langs geautomatiseerde weg. Voor mij is het een punt van zorg dat de werking van het artikel niet te veel wordt beperkt.

Minister **Donner**: Het gaat om de waardekaart, of enige andere voor het publiek beschikbare kaart. Er moet sprake zijn van de fysieke drager, want anders komen wij in een totaal andere sfeer, namelijk diefstal via internet, waarbij een rekening wordt leeggehaald. In dit geval gaat het specifiek om de bescherming van het betalingsverkeer via kaarten. De desbetreffende bepaling is nodig om de aansluiting op de Wet fraude niet-chartaal geldverkeer te realiseren. De vraag wat te doen met alle andere methoden waarop mensen eventueel wederrechtelijk voordeel kunnen verkrijgen, is een totaal andere vraag. Dan komen wij terecht in de sfeer van diefstal, fraude, oplichting, en dergelijke, of is er sprake van het gebruik van telebankieren op een andere wijze dan waarvoor dit is bedoeld. Een bijkomende overweging is dat de bepaling in de Wet fraude niet-chartaal geldverkeer de uitvoering betreft van een EG-richtlijn, en derhalve dient aan te sluiten op definities elders. Wij moeten dan niet in dit wetsvoorstel een verandering aanbrengen. De problematiek waarop u doelt is een andere dan die welke wij in dit wetsvoorstel regelen, te weten de specifieke figuur dat gebruik wordt gemaakt van de fysieke drager. Als er sprake is van niet-fysieke dragers, kom ik per definitie in een totaal andere sfeer terecht.

Wat de foto's betreft, is in artikel 35 van de Auteurswet al geregeld dat hij die zonder daartoe gerechtigd te zijn een portret in het openbaar ten toon stelt, bijvoorbeeld via internet, of op andere wijze openbaar maakt, strafbaar is.

Dan kom ik nu op de motie van mevrouw Gerkens over de mededelingsplicht van bedrijven dat gegevens via hacken zijn gestolen. Ik blijf van mening dat wij daarbij te maken hebben met een kwestie die primair in het gewone maatschappelijke verkeer moet worden geregeld. Men kan van bedrijven verlangen dat men die informatie krijgt, als onderdeel van de dienstverlening. Ik kan mij ook voorstellen dat bedrijven op dat punt onderling in de aanbieding van hun dienstverlening zullen concurreren. De invoering van een wettelijke plicht op dit punt brengt de zaak in de sfeer van de overheid. Ik vermoed dat wij het erover eens zijn, dat dit geen kwestie is van het strafrecht. Zolang ik niet weet dat gegevens via hacken in handen van een ander zijn gekomen, kan ik geen aangifte doen van het feit dat degene die mij had moeten waarschuwen, dat niet heeft gedaan. In alle gevallen bevinden wij ons in de sfeer van het privaatrecht. Deze kwestie wordt nu al in het economisch verkeer geregeld, namelijk via de gewone bescherming van de consument. Ik ontraad daarom de aanneming van de motie, op alle punten waarbij het er concreet om gaat om per 1 juni 2006 een wetsvoorstel aan de Kamer aan te bieden. Dan is het logischer om te zeggen: laten wij dat punt eens bespreken. Dan geef ik de wens door aan mijn collega van Economische Zaken om aan de Kamer een notitie aan te bieden over de wenselijkheid, de mogelijkheden en de ontwikkelingen op dit terrein.

Mevrouw **Gerkens** (SP): Ten aanzien van het laatste staat er in de motie ''het voorstel'' en niet ''het wetsvoorstel''. Wat dat betreft, kom ik u misschien nog tegemoet.

Ik ben het pertinent met u oneens waar u zegt dat marktwerking en concurrentievermogen dit eigenlijk zouden moeten regelen, want bedrijven kunnen op dit punt met elkaar concurreren. Feit is dat bedrijven er alle belang bij hebben om elkaar op dit punt vooral niet te beconcurreren. Als de een het doet, moet de ander het immers ook doen. Ik acht het juist van essentieel belang dat dit wel gebeurt, omdat ik er als burger recht op heb, te weten wanneer gegevens van mij gestolen

zouden kunnen zijn, waarbij er misbruik gemaakt zou kunnen worden van mijn gegevens. Het is nu al duidelijk dat dit soms gebeurt, dat gegevens gehacked worden. Ik heb geen mailtje gehad van Wehkamp dat derden bij mijn gegevens zijn geweest, terwijl daar wel misbruik van gemaakt kan worden. Ik acht het juist met het oog op de bescherming van persoonsgegevens een taak van de overheid om bedrijven op te dragen dat te gaan doen. Dat heeft als neveneffect dat het de druk op die bedrijven opvoert om ook hun gegevens te gaan beveiligen. Dat is ook wat ik in eerste termijn heb gezegd. Wij zien dat het hacken van systemen en het stelen van bedrijfs- of persoonsgegevens in toenemende mate gebeuren. Wij zien identiteitsdiefstal toenemen, met alle gevolgen van dien, maar bedrijven weigeren of verzuimen nog steeds, hun beveiliging op orde te brengen. Als wij zeggen dat wij het wetboek moeten aanpassen aan de actualiteit, dat wij moeten zorgen voor een betere opsporing en vervolging en dat daarvoor overheidsmiddelen worden ingezet, dan kan het niet zo zijn dat bedrijven niet de druk voelen om ook hun verantwoordelijkheid te nemen, namelijk in de beveiliging. Ik denk dat dit een goed middel zou zijn om het wel te doen.

Minister **Donner**: Op dat punt blijf ik gewoon met u van mening verschillen. Ik ben het erover eens dat het nu een vraag is of het wenselijk is om dit in de vorm van een recht te doen. Men heeft nog geen recht. U zegt te menen dat het een recht moet worden van burgers om daar kennis van te nemen. Ik zeg dat dit een ontwikkeling moet zijn in het maatschappelijke verkeer. Ik ontraad de aanneming van deze motie, omdat ik vrees dat wij anders iets in de overheidssfeer trekken wat daar niet hoort. Ik kan mij echter volledig voorstellen dat u een andere mening bent toegedaan, dus laten wij het daar op dit moment bij houden.

De algemene beraadslaging wordt gesloten.

De **voorzitter**: Ik stel voor, over de ingediende motie, de ingediende amendementen en het wetsvoorstel dinsdag over veertien dagen te stemmen.

Daartoe wordt besloten.

Sluiting 22.09 uur

□

Lijst van ingekomen stukken, met de door de Voorzitter terzake gedane voorstellen:

1. twee koninklijke boodschappen, de voorstellen van (rijks)wet:
Wijziging van enige sociale-verzekeringswetten in verband met de beëindiging van de verzekeringsplicht van in het buitenland wonende uitkeringsgerechtigden (30223);
Wijziging van de Rijksoctrooiwet 1995 ter implementatie van de richtlijn inzake handhaving van intellectuele-eigendomsrechten (Wijziging Rijksoctrooiwet 1995 in verband met implementatie richtlijn handhaving intellectuele-eigendomsrechten) (30222, R1797).

Deze koninklijke boodschappen, met de erbij behorende stukken, zijn al gedrukt en rondgedeeld;

2. de volgende brieven:
zeven, van de minister van Buitenlandse Zaken, te weten:
een, ten geleide van verslag bezoek aan Indonesië (26049, nr. 48);
een, ten geleide van Verdrag tussen het Koninkrijk der Nederlanden en de Bondsrepubliek Duitsland betreffende de aansluiting van de Nederlandse regionale weg N 297n en de Duitse rijksweg B 56 (30219);
een, ten geleide van Verdrag tussen het Koninkrijk der Nederlanden en de Bondsrepubliek Duitsland betreffende de aansluiting tussen de Nederlandse regionale weg N 280 en de Duitse autosnelweg A 52 (30221);
een, ten geleide van Verdrag tussen het Koninkrijk der Nederlanden en de Bondsrepubliek Duitsland betreffende de aansluiting tussen de Nederlandse autosnelweg A 74 en de Duitse autosnelweg A 61 (30224);
een, ten geleide van Verdrag tussen de Regering van het Koninkrijk der Nederlanden en de Regering van de Republiek Albanië tot het vermijden van dubbele belasting en het voorkomen van het ontgaan van belasting met betrekking tot belastingen naar het inkomen en het vermogen (Verdrag tussen de Regering van het Koninkrijk der Nederlanden en de Regering van de Republiek Albanië tot het vermijden van dubbele belasting en het voorkomen van het ontgaan van belasting met betrekking tot belastingen naar het inkomen en het vermogen, met Protocol) (30225);
een, inzake protocol vastgesteld overeenkomstig artikel 34 van het Verdrag betreffende de Europese Unie tot wijziging, wat betreft de vorming van een referentiebestand van onderzoeksdossiers op douanegebied, van de Overeenkomst inzake het gebruik van informatica op douanegebied (30266);
een, inzake Wijziging van het op 17 maart 1992 te Helsinki totstandgekomen Verdrag inzake de bescherming en het gebruik van grensoverschrijdende waterlopen en internationale meren (30227);
een, van de ministers van Buitenlandse Zaken en voor Ontwikkelingssamenwerking, ten geleide van brief Richtlijnen voor de Koninkrijksdelegatie (26150, nr. 30);
een, van de minister van Justitie, inzake reactie rapport Wie wat bewaart heeft wat (23490, nr. 388);
een, van de minister voor Vreemdelingenzaken en Integratie, inzake antwoord op vragen van de vaste commissie voor Justitie (19637, nr. 964);
twee, van de minister van Onderwijs, Cultuur en Wetenschap, te weten:
een, inzake Vaststelling van bekwaamheidseisen voor leraren in het basisonderwijs, het speciaal en voortgezet speciaal onderwijs, het voortgezet onderwijs en voor docenten educatie en beroepsonderwijs, alsmede houdende aanwijzing van vakken voor bekwaamheid als vakleerkracht in het primair onderwijs (Besluit bekwaamheidseisen onderwijspersoneel) (30230);
een, inzake Besluit tot intrekking van een aantal algemene maatregelen van bestuur en andere koninklijke besluiten op de beleidsterreinen van het Ministerie van Onderwijs, Cultuur en Wetenschap (30233);
een, van de staatssecretaris van Onderwijs, Cultuur en Wetenschap, over de toekomst van de publieke omroep (29800-VIII, nr. 260);
vier, van de minister van Financiën, te weten:
een, ten geleide van agenda voor de Ecofin Raad (21501-07, nr. 495);
een, ten geleide van agenda voor de vergadering van het IMFC (26234, nr. 45);
een, over kabinetsstandpunt af te zien invoering van een rijksbreed baten-lastenstelsel (28737, nr. 10);
een, over de knelpunten gevolg van btw bij PPS-projecten (28753, nr. 7);