Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2005–2006

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

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

C

VOORLOPIG VERSLAG VAN DE VASTE COMMISSIE VOOR JUSTITIE[1]

Vastgesteld 20 december 2005

Het voorbereidend onderzoek geeft de vaste commissie voor Justitie aanleiding tot het maken van de volgende opmerkingen en het stellen van de volgende vragen.

De leden van de commissie hebben met veel belangstelling kennisgenomen van zowel de wijziging van het Wetboek van Strafrecht, het Wetboek van Strafvordering en enige andere wetten in verband met nieuwe ontwikkelingen in de informatietechnologie (computercriminaliteit II), nr. 26 671, (hierna aan te duiden als CCII), als de voorgestelde goedkeuring van het op 23 november 2001 te Boedapest totstandgekomen Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken (Trb. 2002, 18), nr. 30 036 (R 1784), (hierna aan te duiden als het Verdrag).
De leden van de fractie van het **CDA** stelden vast, dat het Verdrag een minimum karakter heeft, hetgeen betekent, dat het voorziet in een aanduiding van bevoegdheden waarover de betrokken staten in ieder geval dienen te beschikken. De meeste van deze bevoegdheden zijn al eerder in de Nederlandse wetgeving ingevoerd en met name bij de inwerkingtreding in 1993 van de Wet Computercriminaliteit I (Stb. 1993, 33). De leden kunnen zich erin vinden, dat de voor de implementatie nog nodige wetswijzigingen niet in een apart wetsvoorstel zijn opgenomen, doch dat daartoe is aangesloten bij het reeds aanhangige wetsvoorstel CCII. Het ligt dan ook voor de hand het commentaar op het ontwerp dat strekt tot goedkeuring van het Verdrag en de vragen c.q. opmerkingen over het ontwerp CCII te combineren.
De fractie van **D66** acht het van essentieel belang, waar de technologische ontwikkelingen steeds sneller lijken te gaan, dat het strafrecht daar niet bij achterblijft. Het kan niet zo zijn dat het Wetboek van Strafrecht en het Wetboek van Strafvordering alleen met kunstmatige ingrepen en extensieve interpretatie aansluiting blijven vinden bij de hedendaagse maatschappij. Om deze reden is het voorliggende voorstel tot moderni-

[1] Samenstelling:
Leden: Holdijk (SGP), Wagemakers (CDA), Witteveen (PvdA), De Wolff (GL), Van de Beeten (CDA) (voorzitter), Broekers-Knol (VVD), De Graaf (VVD), Kox (SP), Westerveld (PvdA), Engels (D66) en Franken (CDA).
Plv. Leden: Schuurman (CU), Pruiksma (CDA), Jurgens (PvdA), Thissen (GL), Dölle (CDA), Rosenthal (VVD), Biermans (VVD), Van Raak (SP), Tan (PvdA), Schuyer (D66) en Russell (CDA).

KST93348
ISSN 0921 - 7363
Sdu Uitgevers
's-Gravenhage 2005

sering toe te juichen.

Artikel 138a Sr

De commissie wil om te beginnen de aandacht vestigen op de breed levende twijfel omtrent de wenselijkheid van de nieuwe redactie van artikel 138 a Sr. De commissie onderstreept dat zij voorstander is van een zo strikt mogelijke implementatie van internationaal gemaakte afspraken, zoals dat ook geldt bij implementatie van Europese regelgeving. De vraag rijst of de gekozen formulering van computervredebreuk, zoals opgenomen in artikel 138a Sr., in de verschillende verdragsluitende staten niet zeer zal gaan uiteenlopen, vooral ook omdat de Franse en de Engelse tekst van het Verdrag dienaangaande verschillend zijn.

De commissie heeft bedenkingen ten aanzien van het vervallen van de beveiligingseis en het vervallen van de eis dat de opzet gericht moet zijn op de wederrechtelijkheid, welke door de fracties van **CDA, VVD** en **PvdA** als volgt verwoord zijn:
De leden van de **CDA**-fractie hebben bedenkingen bij het laten vervallen van de beveiligingseis als noodzakelijke voorwaarde voor strafbaarheid. De ratio daarvan is immers, dat gebruikers van de middelen van communicatie- en informatietechniek zelf de verantwoordelijkheid dragen voor het zorgvuldig omgaan met de hen ten dienste staande middelen. In het civiele recht is dat een vanzelfsprekendheid. Niemand kan zijn inboedel verzekeren als hij er niet voor zorgt, dat zijn woning deugdelijk is afgesloten. In de uitzending van NOVA op 19 november 2005 is nog eens gewezen op het gevaar, dat gebruikers van ICT-middelen lopen, wanneer zij onbeveiligde middelen van ICT gebruiken. Zou zelfs niet mogen worden gezegd, dat deze gebruikers door dusdanige handelingen het risico hebben aanvaard van schade door hacking of phishing-expedities?
De leden van de fracties van **VVD** en **PvdA** merken op dat zowel het Verdrag als het Kaderbesluit van de Raad van Europa inzake Aanvallen op informatiesystemen de wetgever ruimte laat de strafbaarstelling van computervredebreuk te beperken tot gevallen waarin het feit wordt gepleegd door inbreuk te maken op beveiligingsmaatregelen. In het onderhavige wetsvoorstel wordt deze bepaling echter zodanig aangepast dat het doorbreken van een beveiliging slecht als voorbeeld van binnendringen wordt genoemd en niet meer als voorwaarde voor strafbaarheid geldt. Kennelijk meent de minister dat er ook kan worden binnengedrongen in een computersysteem, zonder enige beveiliging te doorbreken (dan wel gebruik te maken van een valse hoedanigheid, valse signalen enz.). Zou de minister voorbeelden kunnen noemen van situaties waarin wel gesproken kan worden van opzettelijk wederrechtelijk binnendringen zonder dat daarbij tevens enige beveiliging wordt doorbroken c.q. omzeild? Is er naar de mening van de minister bij het enkele passeren van een mededeling (een virtueel bordje «verboden toegang») dat verdere toegang tot een systeem verboden is, mogelijk al sprake van opzettelijk wederrechtelijk binnendringen? Een van de redenen waarom de wetgever van 1993 (computercriminaliteit I) koos voor het opnemen van de huidige beveiligingseis in art 138a Sr. was gelegen in de kenbaarheid voor de potentiële dader. Het moeten doorbreken/omzeilen van enige beveiliging werpt een duidelijke drempel op; de potentiële dader weet hierdoor dat hij zich op verboden terrein gaat begeven. Gaat het laten vallen van deze beveiligingseis niet te zeer ten koste van de kenbaarheid waardoor te snel het risico ontstaat dat personen tijdens het surfen (door bijvoorbeeld een «deep link» te volgen) op verboden plaatsen terecht komen en zich deswege vervolgd slechts (moeizaam) kunnen verweren met het argument dat de opzet ontbrak? Is het niet beter dit soort situaties te voorkomen door de huidige redactie te handhaven?

De leden van de **CDA**-fractie merken verder op dat door de toevoeging van het woordje «en» tussen de woorden «opzettelijk wederrechtelijk» in art. 138a Sr. wordt weggenomen, dat de opzet op de wederrechtelijkheid moet zijn gericht. De in de memorie van toelichting gegeven motivering tot deze wijziging blijkt niet concludent. In het gegeven voorbeeld is duidelijk, dat het opzet op de wederrechtelijkheid is gericht, zodat daar geen sprake is van een onnodig zware eis. Zou het niet de voorkeur verdienen vanuit een oogpunt van criminele politiek om juist hier de gevallen van onhandige gebruikers, die toevallig een verkeerd nummer intoetsen en dan in het systeem van een onbeveiligde gebruiker binnenkomen buiten de sfeer van het strafrecht te laten?

Nu het verdrag niet noodzaakt tot een dergelijke formulering en de commissie twijfels heeft omtrent de redactie van dit artikel, wil de commissie graag de reactie van de minister vernemen op de suggestie van de commissie om, met gebruikmaking van artikel V van wetsvoorstel CCII (dat inwerkingtreding op een bij koninklijk besluit te bepalen tijdstip regelt, dat voor de verschillende artikelen of onderdelen daarvan verschillend kan worden vastgesteld) het gewijzigde artikel 138a Sr niet in werking te laten treden.

Aanvullend op deze vragen hebben de leden van de fracties van het **CDA**, de **VVD**, de **PvdA** en **D66** nog enkele andere vragen. De leden van de **VVD**-fractie hebben bij de voorbereiding voor het voorlopig verslag, evenals de leden van de **PvdA**-fractie, profijt gehad van het proefschrift van mr. dr. F. P. E. Wiemans van de Universiteit van Tilburg, «Onderzoek van gegevens in geautomatiseerde werken», Wolf Legal Publishers, Nijmegen 2004.

Enkele definitievragen

De leden van de **D66-**fractie vragen zich af of het onderscheid tussen stromende en opgeslagen gegevens nog wel noodzakelijk is. Aan de ene kant levert het een bijdrage aan de precisering van de bevoegdheden van de opsporingsautoriteiten. Aan de andere kant kan men zich afvragen of met de toenemende integratie van telefonie en internet het onderscheid nog wel nut heeft. Is een sms-chatsessie stromend of gaat het hierbij om telkens opnieuw opgeslagen gegevens?

Over de definitie van het begrip e-mail vragen deze leden zich af wat daar nu allemaal onder valt. Is het in de ogen van de minister correct dat daar ook SMS berichten ondervallen? En hoe zit het met instant messenger berichten, zoals bij MSN messenger en de hele opgeslagen geschiedenis daarvan.

In het onderhavige wetsvoorstel worden terecht de definities van «gegevens» (art. 80quinquies Sr.) en «geautomatiseerd werk» (art. 80sexies Sr.) verbeterd, zo stellen de leden van de fracties van **VVD** en **PvdA**. De betreffende definities zijn echter nog steeds alleen opgenomen in de betekenissentitel van het Wetboek van Strafrecht. De begrippen «gegevens» en «geautomatiseerd werk» komen ook voor in diverse bepalingen in het Wetboek van Strafvordering. Vanuit het oogpunt van legaliteit is van belang de toepasbaarheid en reikwijdte van de strafvorderlijke bepalingen waarin deze begrippen voorkomen zo nauwkeurig mogelijk te kunnen vaststellen. Vergelijk ook de definities van de begrippen «tijd en plaats» en «misdrijf» die telkens in beide wetboeken worden omschreven (resp. de art. 88 Sr. en 136 Sv.; art. 78 Sr. en 129 Sv.). Moeten de definities van «gegevens» en «geautomatiseerd werk», zo vragen de leden van de fracties van **VVD** en **PvdA**, niet ook in de

betekenissentitel van het Wetboek van Strafvordering worden opgenomen?

Vragen m.b.t. bevoegdheden

De leden van de **CDA**-fractie hebben met instemming kennisgenomen van een passage in de Tweede Nota van Wijziging over een toetsing van de nieuwe bevoegdheden aan art.8 EVRM. Zij zouden echter graag zien, dat de minister ook aangeeft waarom slechts bij een gedeelte van de nieuwe bevoegdheden tot het uitoefenen van dwangmiddelen sprake is van toezicht op het gebruik daarvan door de rechter-commissaris. Dit laatste blijkt slechts het geval bij de bevoegdheden, die zijn genoemd in de artikelen 126m en 126t Sv., doch niet bij de reeks overige toch vaak vergaande bevoegdheden. Gelet op het bepaalde in art.15 Verdrag wordt een redengeving voor deze keuze gaarne tegemoet gezien.
Deze leden vroegen zich daarbij tevens af of het niet valt te vrezen, dat in de praktijk de officier van justitie zijn zelfstandige bevoegdheden (in vergaande mate) zal delegeren, zodat deze bevoegdheden de facto door hulpofficieren of zelfs via subdelegatie door lagere politiefunctionarissen zullen worden uitgevoerd.

Het voorstel creëert de mogelijkheid om gegevens die tijdens een doorzoeking worden aangetroffen op een geautomatiseerd werk in beslag te nemen voor zover die zijn gebruikt voor het plegen van een strafbaar feit of op zichzelf een strafbaar feit opleveren. Gegevens uit een geautomatiseerd werk kunnen ook in beslag worden genomen om toekomstige strafbare feiten te voorkomen. In de ogen van de leden van de **D66**-fractie is het een goede stap dat deze gegevens nu in beslag kunnen worden genomen. Maar aan deze vormgeving kleven nog wel enkele bezwaren. Ten eerste gaat het om een discretionaire bevoegdheid van de Officier van Justitie (OvJ) en van de rechter-commissaris. Inbeslagname zal niet altijd eenvoudig zijn omdat de gevonden gegevens onderdeel kunnen uitmaken van het netwerk of besturingssysteem en het in beslag nemen kan leiden tot het niet meer normaal functioneren van het geautomatiseerde werk. Is het te verwachten dat het Openbaar Ministerie ten aanzien van deze bevoegdheid interne beleidsregels opstelt om willekeur in het gebruik te voorkomen en duidelijke regels te scheppen over wanneer het proportioneel is om bijvoorbeeld de gehele harde schijf mee te nemen of alleen de strafbare gegevens. En zo ja, kan de minister aangegeven hoe die regeling er in grote lijnen uit komt te zien?
Verder vragen deze leden zich af of het wel in het taken pakket van de rechter-commissaris valt om strafbare feiten te voorkomen?

Bevriezing

Hoe denkt de minister met betrekking tot de bevoegdheid tot bevriezing te kunnen (doen) waarborgen, dat de integriteit van de betreffende gegevens tijdens de bevriezingsperiode niet zal worden aangetast, zo vragen de leden van de **CDA**-fractie?

Onder invloed van het Verdrag zijn er enkele veranderingen in dit voorstel opgenomen waarvan er een de aandacht van de **D66**-fractie heeft getrokken. Er wordt een nieuwe bevoegdheid gecreëerd die het mogelijk maakt dat de officier van justitie de bevriezing van gegevens kan bevelen van een telecommunicatie- of internetaanbieder. Dit is naar ons oordeel een inventieve maatregel die geen inbreuk maakt op de privacy van alle burgers, maar alleen op die waarvan het vermoeden bestaat dat zij zich schuldig maken aan een strafbaar feit. Denkt de minister dat deze nieuwe bevoegdheid een betere oplossing is dan het plan om een algemene bewaarplicht van een of twee jaar te creëren?

Encryptie

Een ander onderdeel is de medewerkingsplicht voor mensen die kennis dragen van de gebruikte encryptiesleutel van de gevonden gegevens. De leden van de D66-fractie willen graag van de minister vernemen wat voor invloed het feit heeft dat gegevens alleen door een derde zijn te ontsleutelen op de geldigheid van het bewijs? Hoe kunnen de opsporingsambtenaren zeker weten dat de gegevens juist zijn ontcijferd en wie zegt dat de derde die meewerkt niet een medeverdachte is? Hoe kan de advocaat van de verdachte nagaan of de gegevens wel juist zijn ontcijferd?

Met een beroep op het Saunders-arrest van het EHRM wordt aangenomen, dat een ontsleutelplicht niet aan de verdachte kan worden opgelegd. De leden van de **CDA**-fractie vragen of de minister kan meedelen welke positie de meeste EU-landen te dien aanzien innemen. Welke standpunten worden met name door Frankrijk en het Verenigd Koninkrijk gehanteerd?

Handhavingsaspecten

De leden van de **CDA**-fractie achten het van groot belang, dat de bestrijding van computercriminaliteit ten aanzien van het hele pakket van mogelijkheden, zowel waar het «oude delicten» met nieuwe kansen (te denken valt bijvoorbeeld aan vormen van fraude en oplichting als «phishing»), als «nieuwe» vormen van criminaliteit betreft, over de volle breedte zowel nationaal als internationaal ter hand wordt genomen. Gelet op de toenemende omvang van dit soort criminaliteit en de zeer omvangrijke schade, welke daardoor kan worden veroorzaakt, is verhoging van de strafmaat van diverse delicten en met name van computervredebreuk van belang. Hierbij past de opmerking, dat de capaciteit voor handhaving veel aandacht verdient. Enerzijds zullen niet of nauwelijks handhaafbare bepalingen niet bijdragen aan de kwaliteit van de rechtsorde, anderzijds dienen de kwalitatief juiste aan politie en justitie toegekende bevoegdheden ook daadwerkelijk te kunnen worden uitgeoefend. Deze leden vroegen zich daarom af of met de start van het National High Tech Crime Centre, de mogelijke inbreng van het Nederlands Forensisch Instituut en de aanwezige kennis bij de politieorganisatie zelf voldoende wordt bijgedragen aan de ontwikkeling van de daadwerkelijke bestrijding van de computercriminaliteit. Daarbij kwam de vraag op of er ook met enig succes wordt gewerkt aan de toename van de aangiftebereidheid van slachtoffers.

In samenhang met het voorgaande vroegen deze leden zich af of de minister van mening is, dat de huidige en de voorziene bepalingen in het wetboek van strafvordering, totstandgekomen na een opeenstapeling van zes recentelijk voorafgegane wetswijzigingen, wel voldoende overzichtelijk en hanteerbaar zijn. De strafvordering moet immers een stelsel van concrete, uitvoerbare en voor wat betreft de wijze van uitoefening toetsbare bevoegdheden bevatten en mag volgens de aan het woord zijnde leden niet ontaarden in een mandarijnenwetenschap.

Het inbreken in computers, het platleggen van netwerken en het verspreiden van virussen en ernstige vormen *spam* kunnen heel verstorend zijn voor individuele burgers alsmede ook voor de samenleving als geheel. De voorgestelde strafverzwaring van deze daden is begrijpelijk gezien de soms ernstige aard van deze daden. Dit neemt echter niet weg dat strafbaarstelling en strafverzwaring alleen nooit criminaliteit volledig tegen gaan. Het vergroten van de pakkans werkt veel afschrikwekkender. Op dit punt heeft de **D66-**fractie enige zorg. Zou de minister in willen gaan op de vragen of er binnen de politie, het openbaar

ministerie en de rechterlijke macht wel voldoende kennis en mankracht aanwezig is voor een effectieve handhaving? Bij alle onderdelen van dit voorstel, van het opsporen tot het benutten van de nieuwe strafvorderlijke bevoegdheden, is het immers van essentieel belang dat er voldoende kennis aanwezig is, niet alleen voor een goede opsporing maar ook voor een proportionele toepassing van de bevoegdheden. De gecompliceerde cyberwereld vraagt maatwerk.

Artikelgewijs

Artikel 139d, lid 2 en 3 Sr/artikel 161sexies Sr:

Met betrekking tot de strafbaarstelling van voorbereidingshandelingen (art 6 Verdrag) is naast de reeds bestaande mogelijkheden in de artikelen 139d, 350a en 350b Sr. voor specifieke vormen en art. 46 Sr. voor een algemene bepaling nog een aanvulling voorzien ten aanzien van de artikelen 139d en 161sexies Sr. Voor de werking van deze aanvulling is bepalend of hier sprake is van opzet in de vorm van oogmerk. Zien de leden van de **CDA**-fractie het juist dan zal de bewijsbaarheid van dit delictsbestanddeel heel wat vraagtekens oproepen mede omdat er een verband zal moeten zijn met de in lid 2 sub a bedoelde elementen «technisch hulpmiddel» en «hoofdzakelijk geschikt gemaakt». Wat is de mening van de minister hierover?

De leden van de fracties van **VVD** en **PvdA** constateren dat aan het bestaande art. 139d Sr. na het eerste lid twee leden worden toegevoegd. Het nieuwe tweede lid stelt kort gezegd strafbaar het voorhanden hebben, verspreiden, verkopen enz. van technische hulpmiddelen of wachtwoorden enz. met het oogmerk dat daarmee de misdrijven van art. 138a (computervredebreuk), 138b (nieuw, denial of service attack) of 139c (afluisteren telecommunicatie) worden gepleegd. Dit lijkt een zinvolle bepaling. In het nieuw voorgestelde derde lid van art. 139d wordt echter (onder verhoging van het strafmaximum naar vier jaar) strafbaar gesteld «hij die het in het tweede lid bedoelde feit pleegt terwijl zijn oogmerk is gericht op een misdrijf als bedoeld in art.138a, tweede of derde lid». In het hier bedoelde tweede en derde lid van art. 138a gaat het om de gekwalificeerde vormen van computervredebreuk, dat wil zeggen het na voorafgaande computervredebreuk: a) kopiëren van gegevens (138a lid 2) of b) het met het oogmerk van wederrechtelijke bevoordeling gebruiken van verwerkingscapaciteit dan wel het verschaffen van toegang tot het systeem van een derde (138a lid 3).

Denkt de minister, zo vragen de leden van de fracties van **VVD** en **PvdA**, dat in de praktijk bewezen zal kunnen worden dat iemand die betrapt wordt op het voorhanden hebben (etc.) van de in het tweede lid bedoelde technische middelen of wachtwoorden, deze middelen voorhanden (etc.) heeft (gehad) met het oogmerk (naaste doel) om gekwalificeerde computervredebreuk te gaan plegen? In de praktijk zal namelijk het tweede lid al moeilijk te bewijzen zijn. Er moet immers worden vastgesteld dat degene die de hulpmiddelen (etc.) voorhanden had (etc.) dit deed met het oogmerk om een van de drie genoemde misdrijven te gaan plegen. Is het zodoende al lastig om vast te stellen dat iemand bijvoorbeeld over een wachtwoord beschikt met het oogmerk om computervredebreuk te gaan plegen, hoe valt dan ooit aan te tonen dat betrokkene over een wachtwoord beschikt met het oogmerk (naaste doel) om gekwalificeerde computervredebreuk te gaan plegen? Uit het enkele voorhanden hebben (etc.) valt dit immers niet af te leiden? In feite wordt hier het bewijs van «oogmerk op oogmerk» gevraagd. Dat is een novum in het straf(proces)recht.

Indien ook de minister van mening is dat het openbaar ministerie met betrekking tot dit nieuwe derde lid van art. 139d voor (te) grote bewijsproblemen komt te staan, is het dan wel zinvol/wenselijk dit onderdeel van de bepaling in te voeren?

De voorgestelde strafmaat van art. 139d derde lid (vier jaar gevangenisstraf of geldboete van de vierde categorie) is gelijk aan die van een voltooide gekwalificeerde computervredebreuk. De eerdere motivering door de minister dat «degene die een instrument verkoopt of vervaardigt met specifiek het oogmerk dat daarmee het gekwalificeerde delict van art. 138a, tweede of derde lid, wordt gepleegd, (...) ook zelf (dient) te worden bedreigd met de daarbij passende hogere straf» overtuigt in het licht van de strafbaarstelling van poging (art. 45 Sr. – maximaal 2/3 van de maximum straf gronddelict) en strafbare voorbereiding van zeer ernstige delicten (art. 46 Sr. – maximaal de helft van de maximum straf gronddelict) niet (zonder meer). Kan de minister nog eens duidelijk aangeven waarom juist in dit geval het treffen van voorbereidingshandelingen net zo zwaar bestraft moet worden als het gekwalificeerde delict?

Artikel 125n Sv: In de versie van het wetsvoorstel zoals die na de tweede nota van wijziging luidt, wordt kennelijk het bestaande art. 125n Strafvordering gehandhaafd. Dit betekent, kort gezegd, dat de bij een onderzoek in geautomatiseerd werk vastgelegde gegevens, die van geen betekenis zijn voor het onderzoek, moeten worden vernietigd. In de eerdere versie van dit wetsvoorstel werd nog voorgesteld deze bepaling te vervangen door een nieuwe, art. 125q, waarin aansluiting werd gezocht bij de bepalingen 126cc en 126dd (ingevoerd bij de wet BOB) die juist uitgaan van een beperkte bewaarplicht.

Kan de minister aangeven, zo vragen de leden van de fracties van **VVD** en **PvdA**, waarom er met betrekking tot door Justitie bij onderzoek uit computersystemen vastgelegde gegevens op dit punt voor een wezenlijk ander regime wordt gekozen dan wanneer het gaat om gegevens die bijvoorbeeld door observatie of taps zijn verkregen?

Artikel 125o Sv: Het voorgestelde art. 125o Sv., dat ziet op het ontoegankelijk maken van gegevens met een verboden karakter, is een nuttige bepaling die goed aansluit bij problemen die zich in de praktijk op dit punt voordoen. In de gevallen bedoeld in de eveneens nieuw voorgestelde artikelen 354 en 552fa Sv. dient de zittingsrechter een beslissing te nemen met betrekking tot de door de OvJ of de rechter-commissaris eerder ontoegankelijk gemaakte gegevens. De rechter kan dan teruggave of vernietiging van de ontoegankelijk gemaakte gegevens bevelen. Dit systeem is niet geheel sluitend. Wat ontbreekt is een zelfstandige beslissingsbevoegdheid van de zittingsrechter om gegevens ontoegankelijk te maken en te vernietigen. Dit probleem doet zich voor indien de OvJ of de rechter-commissaris niet al eerder gebruik hebben gemaakt van de mogelijkheid om ex art. 125o Sv. (nieuw) gegevens ontoegankelijk te maken, bijvoorbeeld omdat de noodzaak daartoe ontbrak omdat een heel computersysteem (inclusief de verboden gegevens) in beslag was genomen. Indien zo'n systeem (bijvoorbeeld na vrijspraak van de verdachte) moet worden teruggegeven, ontbreekt formeel de bevoegdheid voor de zittingsrechter om de desbetreffende gegevens voorafgaand aan de teruggaaf van het systeem te doen verwijderen.
Is de minister het eens met de opvatting dat het nuttig zou zijn de zittingsrechter een zelfstandige beslissingsbevoegdheid met betrekking tot het ontoegankelijk maken c.q. vernietigen van gegevens te verlenen?

Inwerkingtreding artikel 273d, lid 2 Sr

Het voorgestelde art. 273 d lid 2 Sr. breidt de strafbaarstelling van de schending van het telefoongeheim terecht uit naar niet-openbare telecommunicatienetwerken en -diensten. De minister wil deze bepaling op een later tijdstip doen ingaan dan de andere delen van het voorstel. Leidt dit niet tot verwarring voor de justitiabelen, zo vragen de leden van de **CDA**-fractie? De aangegeven reden om een enkele bepaling uit het hele pakket van nieuwe strafbaarstellingen en bevoegdheden te halen lijkt op voorhand niet overtuigend.

Toekomstige ontwikkelingen

Met het Verdrag en de CC II wordt een belangrijke stap gezet in de richting van internationale samenwerking ter bestrijding van strafbare feiten verbonden met elektronische netwerken, doch deze vormen geen finale oplossing, zo merken de leden van de **VVD**-fractie tenslotte nog op. De ontwikkelingen staan niet stil. Prof. mr. H. W. K. Kaspersen merkt hierover op in zijn artikel «Bestrijding van Cybercrime en de noodzaak van internationale regelingen», Justitiële verkenningen 30(8): 58–75, 2004: «Het internationale karakter van internet dwingt tot verdergaande internationale samenwerking bij de opsporing van strafbare feiten. (...) Hiervoor zijn en blijven internationale verdragen nodig, bij voorkeur in de vorm van een Aanvullend Protocol bij het Cybercrime verdrag.» Kan de minister aangeven of thans in de internationale context ontwikkelingen gaande zijn om tot verdere harmonisatie van cybercrime strafbepalingen te komen?

Tenslotte

Op 21 juni 2005 heeft het VNO/NCW een brief aan de Voorzitter van de Tweede Kamer gezonden met een aantal vragen, die de thans aan de orde zijnde materie betreffen. Het is de leden van de **CDA**-fractie niet duidelijk of, en zo ja hoe, tijdens de behandeling van de wetsontwerpen op de gestelde vragen is ingegaan. Kan de minister hieromtrent opheldering geven en met name enige uitleg vertrekken met betrekking tot het zonder aankondiging vooraf verrichten van onderzoek in gesloten netwerken? Is het niet geëigend hiertoe afspraken te maken met de leiding van ondernemingen c.q. branches om te voorkomen, dat er «overheids-hackers» in bedrijfsnetwerken van bonafide ondernemingen binnen-dringen?

De leden van de vaste commissie voor Justitie zien met belangstelling uit naar de antwoorden van de minister.

De voorzitter van de commissie,
Van de Beeten

De wnd. griffier van de commissie,
Van Dooren