Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2004–2005

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

Nr. 3

MEMORIE VAN TOELICHTING

1. Algemeen

1.1. Inleiding

Het onderhavige voorstel van Rijkswet strekt tot goedkeuring van het Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken (Trb. 2002, 18, en Trb. 2004, 290), hierna ook wel kortweg aangeduid als het Verdrag of, naar zijn Engelse titel, als het Cybercrime Verdrag. Nederland kan pas aan het Cybercrime Verdrag gebonden worden als de nationale wetgeving daarmee in overeenstemming is gebracht. Voor een belangrijk deel is dat reeds het geval, maar voor een deel moet de wetgeving nog worden aangepast. Daarom wordt gelijktijdig met de indiening van dit wetsvoorstel een nota van wijziging aangeboden bij het wetsvoorstel Computercriminaliteit II (Kamerstukken II 1998/99, 26 671 nr. 1–2), waarmee het Wetboek van Strafrecht (Sr), het Wetboek van Strafvordering (Sv) en enige andere wetten in overeenstemming worden gebracht met de eisen die uit het Verdrag voortvloeien.

1.2. De totstandkoming van het Verdrag

Het Cybercrime Verdrag is totstandgekomen in het kader van de Raad van Europa. De onderhandelingen over het Verdrag zijn in april 1997 gestart en hebben gelopen tot in het najaar van 2001. Een belangrijke basis voor het Verdrag werd gelegd door een rapport dat door prof. dr. H.W.K. Kaspersen op verzoek van het European Committee on Crime Problems van de Raad van Europa (CDPC) werd opgesteld. Prof. Kaspersen trad namens Nederland ook op als voorzitter van de werkzaamheden die tot het Verdrag leidden. De Tweede Kamer is over het verloop van de onderhandelingen door de Minister van Justitie bij brief van 23 december 1999 tussentijds geïnformeerd.[1] De Vaste Commissie voor Justitie heeft daarop de Minister een lijst van 65 vragen voorgelegd die op 27 november 2000 schriftelijk zijn beantwoord. De Tweede Kamer heeft destijds volstaan met deze schriftelijke beantwoording.[2] Tussen de definitieve verdragstekst en het voorlopige onderhandelingsresultaat uit het jaar 2000 bestaan overigens slechts zodanige geringe verschillen dat hier met onderstaande toelichting op het Verdrag kan worden volstaan. In de toelichting bij de nota van wijziging bij het wetsvoorstel Computercriminaliteit II wordt op

[1] Kamerstukken II 1999–2000, 23 530, nr. 40.
[2] Kamerstukken II 2000–2001, 23 530, nr. 45.

KST85025
0405tkkst30036R1784-3
ISSN 0921 - 7371
Sdu Uitgevers
's-Gravenhage 2005

een enkele plaats aangegeven waarom een andere oplossing wordt gekozen dan destijds door de ambtsvoorganger van de eerste ondergetekende.

Het Verdrag werd door de betrokken Staten op 23 oktober 2001 te Boedapest ondertekend. Het Verdrag kent een zogenaamd *Explanatory Memorandum*[1] dat door het Comité van Ministers van de Raad van Europa op 8 november 2001 is aanvaard. De tekst van het Verdrag en het *Explanatory Memorandu*m zijn in het Engels en het Frans beschikbaar op de website van het Treaty Office van de Raad van Europa (*http://conventions.coe.int*) onder nummer ETS 185. Van de huidige 45 lidstaten van de Raad van Europa is het Verdrag door 28 lidstaten ondertekend, waaronder alle vijftien toenmalige lidstaten van de Europese Unie. Nog niet alle nieuwe leden van de Europese Unie hebben het Verdrag getekend, maar dit zal naar verwachting op korte termijn geschieden. Op grond van het Statuut van de Raad van Europa en de Statutory Resolution van 1993 kunnen ook waarnemers tot de onderhandelingen voor een verdrag worden toegelaten en daarbij partij worden. Van deze mogelijkheid is gebruik gemaakt door Canada, Japan, de Verenigde Staten van Amerika en Zuid-Afrika. Op 18 maart 2004 was het Verdrag door vijf lidstaten geratificeerd, zodat het krachtens artikel 31, derde lid, van het Verdrag per 1 juli 2004 voor die partijen in werking is getreden.
Toetreding van andere dan de hiervoor genoemde Partijen wordt geregeld door artikel 37 van het Verdrag en vereist een unaniem besluit van de zittende verdragspartijen.

2. Doel, strekking en inhoud van het Verdrag

2.1 Doel van het Verdrag

Het Verdrag heeft ten doel de vergroting van de mogelijkheden ter bestrijding van misdrijven die met behulp van computertechnologie worden begaan of die gericht zijn tegen de beoogde werking van computersystemen ennetwerken. Het Verdrag beoogt deze doelstelling langs verschillende wegen te bereiken.
Allereerst wordt een zekere harmonisatie beoogd van de bepalingen van materieel strafrecht in verband met gedragingen die in de Engelse titel van het Verdrag worden aangeduid als «*cyber crime*», een term die overigens ook in het hierna volgende zal worden gehanteerd omdat deze korter en krachtiger is dan de term die in de Nederlandse titel van het Verdrag is gehanteerd, te weten «strafbare feiten verbonden met elektronische netwerken».
Het Comité van Ministers van de Raad van Europa heeft in 1989, ook met het doel van een zekere harmonisatie, een aanbeveling doen uitgaan tot strafbaarstelling van gedragingen onder de noemer computergerelateerde criminaliteit.[2] Met de wet van 24 december 1992 (Wet Computercriminaliteit[3]) heeft Nederland aan deze aanbeveling voldaan. Andere lidstaten van de Raad van Europa hebben deze aanbeveling in hun wetgeving niet of slechts ten dele gevolgd. Met de opkomst van internationale, voor het grote publiek toegankelijke communicatienetwerken is niet denkbeeldig dat plegers van strafbare feiten waarvan burgers van de ene staat het slachtoffer zijn, zich aan vervolging onttrekken door deze feiten te plegen op het grondgebied van lidstaten die hun wetgeving niet hebben aangepast. Een krachtige, gezamenlijke aanpak in de vorm van een verdrag werd daarom nodig geacht. Hierbij is in aanmerking genomen dat de ontwikkeling van de informatie- en communicatietechnologie (ICT) met de opkomst van het internet tot een bijstelling van de inzichten van 1989 noopte.
Een tweede doelstelling die met het Verdrag wordt nagestreefd betreft een zekere ondergrens in de harmonisatie van opsporingsbevoegdheden,

[1] Ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer.
[2] Aanbeveling van het Comité van Ministers van de Raad van Europa d.d. 13 september 1989 R (89) 9.
[3] Stb. 1993, 33.

nodig om in een elektronische omgeving opsporing van strafbare feiten te kunnen verrichten. Uit voorafgaand onderzoek bleek dat de wetgeving van een belangrijk aantal lidstaten niet voorzag in de bevoegdheden tot het doen van strafrechtelijk onderzoek in computersystemen of computernetwerken. Het Comité van Ministers van de Raad van Europa bracht daarom in 1995 een aanbeveling uit met betrekking tot deze bevoegdheden.[1] Aanstonds bleek dat invoering van de aanbevolen maatregelen niet of slecht in beperkte mate zou worden uitgevoerd, reden waarom ook op dit onderdeel voor een krachtiger instrument in de vorm van een verdrag werd gekozen.
De bedoelde doelstellingen staan op zichzelf maar vormen tegelijkertijd een belangrijke bijdrage aan de internationale samenwerking ter opsporing van *cyber crime*, niet alleen zoals bedoeld in het Verdrag maar ook van andere delicten voor de opsporing waarvan onderzoek in computersystemen ennetwerken nodig is. Met het vergroten van de mogelijkheden tot internationale samenwerking wordt de veiligheid van internationale communicatienetwerken bevorderd en de rechtshandhaving versterkt.
De laatste doelstelling van het Verdrag is de regeling van de rechtshulp zelf. Het Verdrag voorziet – althans met betrekking tot de onderwerpen die het Verdrag regelt – in meer flexibele en daardoor meer efficiënte procedures dan die gebruikelijk is in de rechtshulppraktijk. Het Verdrag past daarmee in de trend ter versterking van de internationale samenwerking, zoals in Europa belichaamd in een aanzienlijk aantal verdragen en protocollen. Het Cybercrime Verdrag heeft evenwel niet alleen betekenis tussen Europese staten maar slaat een brug met niet-Europese staten die mede als richtinggevend kunnen worden beschouwd waar het de ontwikkeling van de informatiemaatschappij betreft.

2.2. ICT-specifiek en technologie-onafhankelijk

In de *terms of reference* opgesteld ten behoeve van het comité van experts dat de taak had de concepttekst van het Verdrag voor te bereiden, wordt veelvuldig verwezen naar begrippen als *information technology* (IT) en *Cyber space*.[2] In de tekst van de artikelen van het Verdrag wordt daaraan gerefereerd door het gebruik van het centrale begrippenpaar *computer system* en *computer dat*a. Uit de formulering van de *terms of reference* is evenwel duidelijk dat de ambitie van het Verdrag zich niet beperkt tot onderwerpen die als IT-specifiek kunnen worden aangemerkt. In het materieel-rechtelijk deel is naast de computerspecifieke delicten een aantal strafbare feiten gedefinieerd waarbij de computer als instrument wordt gebruikt of die in een elektronische omgeving kunnen worden begaan. De reden dat deze delicten in de verdragstekst zijn opgenomen, is dat het gebruik of misbruik van informatietechnologie van grote betekenis is voor de omvang en intensiteit van deze vormen van criminaliteit. Dat wil echter niet zeggen dat dergelijke delicten niet kunnen worden begaan met behulp van andere hulpmiddelen of in niet-elektronische omgevingen of omstandigheden. De verdragstekst beperkt zich tot de elektronische hulpmiddelen of de elektronische omgeving. Dat neemt niet weg dat in het Verdrag specifiek als computerdelict omschreven handelingen naar nationaal recht gedekt kunnen worden door technologieneutraal omschreven delicten. Een voorbeeld van een dergelijke benadering wordt gevormd door artikel 240b Sr (betreffende kinderpornografie), dat de Nederlandse wetgever vooruitlopend op de definitieve verdragstekst heeft aangepast en dat als technologieneutraal kan worden aangeduid. Op het gebied van het strafprocedurele recht wordt een ander voorbeeld gevormd door het wetsvoorstel Bevoegdheden vorderen gegevens (Kamerstukken II 2002/03, 29 441, nr. 2) dat een toepassing inhoudt van artikel 18 van het Verdrag alsmede de invoering van een overeenkomstige regeling voor niet-elektronische gegevens. Het Verdrag geeft een aantal voorzieningen die het verlenen van internationale rechtshulp vereenvou-

[1] Aanbeveling van het Comité van Ministers van de Raad van Europa d.d. 11 september 1995, R (95)13.
[2] Paragraaf 11 *Explanatory Memorandum*.

digen en versnellen. Deze maatregelen behoeven door de verdragsstaat slechts te worden ingevoerd voor zover de rechtshulp bestaat uit het toepassen van de computerspecifieke maatregelen. Een verdragsstaat kan overwegen of deze maatregelen niet ook voor rechtshulp ten aanzien van andere onderwerpen toepassing kan vinden.

2.3 Karakter van het Verdrag; uitleg van de verdragstekst

Voor de uitleg van het Verdrag is een uitgebreid toelichtend rapport beschikbaar, naar zijn Engelse aanduiding hier verder aangemerkt als «Explanatory Memorandum». De verdragspartijen zagen geen grond voor de oprichting van een onafhankelijk orgaan waartoe de verdragspartijen – dan wel de burgers van die staten – zich zouden kunnen wenden in geval van een geschil over de uitleg van de verdragstekst. De verdragspartijen worden in beginsel geacht hun geschillen door overleg op te lossen. Een specifiek voorbeeld is artikel 22, vijfde lid, dat in geval van een jurisdictiegeschil een consultatieprocedure voorschrijft. Artikel 45, tweede lid, nodigt de betrokken partijen uit in geval van een geschil in onderhandeling te treden. Indien zij dat wensen kan de European Committee on Crime Problems (CDPC) van de Raad van Europa als arbiter worden ingeschakeld of kan het geschil worden voorgelegd aan het Internationale Gerechtshof te Den Haag. Partijen dienen het CDPC krachtens artikel 45, eerste lid, te informeren over de uitleg en toepassing die partijen aan het Verdrag geven, zodat deze informatie ook voor andere partijen beschikbaar is.

Het Verdrag staat er niet aan in de weg dat een individuele verdragspartij bij implementatie in nationale wetgeving verder gaat dan de verplichting die uit de verdragstekst voortvloeit. Op geen enkele plaats wordt in de verdragstekst gesteld dat de verdragspartijen zich bij implementatie strikt tot de inhoud van de verdragsartikelen dienen te beperken. Bij een verdergaande implementatie mag echter geen strijd ontstaan met de inhoud en de geest van het Verdrag. Op grond van het op 23 mei 1969 te Wenen totstandgekomen Verdrag van Wenen inzake het Verdragenrecht (Trb. 1985, 79, hierna te noemen het Weens Verdragenverdrag) kan een verdragspartij zich evenmin op grond van het nationale recht onttrekken aan verplichtingen die hij in het kader van een verdrag is aangegaan. Zoals veel verdragen heeft het Cybercrime Verdrag daardoor het karakter van een minimumregeling met een potentieel bredere en meer innovatieve werking.

Raamwerkkarakter en flexibele wijzigingsprocedure

Het Verdrag is niet bedoeld als een eindpunt, maar als een formele vastlegging van een onderhandelingsresultaat voor een onbepaalde periode in de toekomst. De verdragspartijen hebben zich gerealiseerd dat de ontwikkeling van ICT onverminderd doorzet en dat nieuwe technologieën en nieuwe toepassingen daarvan veranderingen teweeg brengen in het maatschappelijk verkeer. Voorspellingen welke veranderingen zich op welk tijdstip in de samenleving zullen voordoen, laat staan op welke wijze de internationale en nationale wetgever daarop kunnen anticiperen, hebben in onze ondernemingsgewijze georganiseerde productiemaatschappij met vrije markten voor goederen en diensten slechts een betrekkelijke waarde. Bovendien is een belangrijke voorwaarde voor het internationale overleg dat men een gemeenschappelijke visie ontwikkelt als antwoord op de vraag met welke belangrijke kenmerken van de informatiemaatschappij men op korte en middellange termijn rekening dient te houden en welke eisen dat stelt aan de ontwikkeling van recht in het algemeen en het strafrecht in het bijzonder. De verdragspartijen hebben zich gerealiseerd dat de inhoud van het Verdrag niet anders is dan

een eerste stap. Het Verdrag kan dan ook mede de basis vormen voor verder internationaal overleg met als resultaat de aanpassing van het Verdrag aan de snel veranderende werkelijkheid.

De verdragspartijen hebben er ook rekening mee gehouden dat het Verdrag regelmatig aan de internationale werkelijkheid dient te worden aangepast. De belangrijkste voorziening daartoe is de instelling van een Conferentie van Partijen, waarbij periodiek alle verdragspartijeen bijeenkomen. Dit lichaam heeft de taak het effectieve gebruik en de implementatie van de verdragstekst te bevorderen, informatie uit te wisselen over juridische, politieke en technologische ontwikkelingen op het terrein van het Verdrag en eventueel het doen van voorstellen ter aanvulling of wijziging van de verdragstekst. De CDPC speelt hierbij een faciliterende en uitvoerende rol. Het is in artikel 46, derde lid, aan de CDPC opgedragen om ten hoogste drie jaar na de inwerkingtreding van het Verdrag – dat is derhalve vóór 1 juli 2007 – een analyse te maken van alle bepalingen in het Verdrag en daarvoor eventueel wijzigingen voor te stellen. Ook individuele partijen zijn bevoegd tot het voorstellen van wijzigingen. Wijzigingsvoorstellen van verdragspartijen of van de CDPC worden vervolgens in procedure gebracht, een en ander zoals geregeld in artikel 44. Dat laatste artikel verplicht o.m. het Comité van Ministers van de Raad van Europa de niet-Europese verdragstaten, die immers geen zitting hebben in de CDPC, over de voorgenomen wijzigingen te raadplegen.

2.4 Het materieel-strafrechtelijke deel van het Verdrag

Afdeling 1 van hoofdstuk II is onderverdeeld in een vijftal verschillende titels. De titels 1 tot en met 4 weerspiegelen de categorisering van «*cyber crime*s» zoals deze in het Verdrag wordt gemaakt. Uitgangspunt voor Afdeling 1 vormde de Aanbeveling van 1989. Deze kenmerkt zich door een zogenaamde lijstbenadering, een opsomming van strafbaar te stellen feiten zonder nadere inhoudelijke indeling. Het Cybercrime Verdrag bevat wel een categorisering van «*cyber crimes*». Titel 1 omvat de gedragingen die als *cyber crime* in enge zin kunnen worden opgevat, terwijl de gedragingen ondergebracht in de titels 2 tot en met 4 als *cyber crime* in ruime zin kunnen worden aangemerkt. Titel 5 tenslotte bevat enkele accessoire bepalingen. Een aantal bepalingen van de lijst van 1989 zijn als zelfstandige strafbaarstelling niet in het Verdrag opgenomen, terwijl nieuwe strafbaarstellingen zijn toegevoegd, bestaande zijn uitgebreid of aan de jongste inzichten zijn aangepast.

Titel 1 bevat de zogenaamde «c.i.a.-delicten», strafbare handelingen gericht tegen de vertrouwelijkheid (*confidentiallity*), de integriteit (*integrity*) en de beschikbaarheid (*availability*) van computergegevens en gegevensverwerkende systemen. De benaming en inrichting van deze delicten ter bescherming van aan een geautomatiseerde gegevensverwerking inherente belangen wijkt niet wezenlijk af van de Nederlandse benadering, zoals gevolgd bij de totstandkoming van de Wet Computercriminaliteit I (Stb. 1993, 33), zodat uitvoerige bespreking hiervan bij dit onderdeel achterwege kan blijven.

Titel 2 bevat bepalingen waarbij de strafbare handeling niet gericht is tegen (het resultaat) van een geautomatiseerde gegevensverwerking, maar de strafbare handeling het resultaat is van het al dan niet bevoegde gebruik van een geautomatiseerde gegevensverwerking. Deze bepalingen strekken tot de bescherming van rechtsbelangen waarvan de aantasting onder nationale wetgeving veelal al met straf bedreigd zal zijn indien de aantasting ervan met behulp van traditionele hulpmiddelen wordt ondernomen. Deze bepalingen, aangeduid als computer-gerelateerde valsheid

en computer-gerelateerde fraude, kan men samennemen onder de gemeenschappelijke noemer van computer-gerelateerde delicten.

Titel 3 is gereserveerd voor de zogenaamde inhoudgerelateerde delicten. Het gaat hierbij vooralsnog om de verspreiding van strafbare inhoud door middel van computersystemen en -netwerken. De titel bestrijkt op dit moment één onderwerp: de productie en verspreiding van kinderporno door middel van computersystemen en -netwerken. Over een vergelijkbare bepaling met betrekking tot racistische, xenophobe en discriminatoire uitlatingen kon in de context van het Verdrag geen overeenstemming worden bereikt. Daarom is besloten tot het op 28 januari 2003 te Straatsburg totstandgekomen Aanvullend Protocol bij het Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, betreffende de strafbaarstelling van handelingen van racistische of xenofobische aard verricht via computersystemen (Trb. 2003, 60). In beginsel staat dit Aanvullend Protocol open voor ondertekening door iedere partij bij het Cybercrime Verdrag, maar in de praktijk zullen niet al die staten partij worden bij dit Protocol. Het Koninkrijk heeft dit Protocol op genoemde datum ondertekend. Na de goedkeuring van het Verdrag zal een wetsvoorstel ter goedkeuring van dit Protocol worden ingediend.

Titel 4 richt zich op de bepalingen die inbreuken op het auteursrecht en naburige rechten strafbaar stellen. Anders dan bij de Aanbeveling van 1989 het geval was, beperkt de strafbaarstelling zich niet tot computerprogramma's maar sluit in beginsel ieder werk of prestatie zoals bedoeld in de Auteurswet of de Wet op de naburige rechten in, mits de verveelvoudiging of openbaarmaking geschiedt door middel van een computersysteem of -netwerk.

Titel 5 bevat enkele accessoire bepalingen.

Het Verdrag laat de mogelijkheid open dat de verdragspartijen meer of andere verwante gedragingen strafbaar willen stellen dan in de verdragstekst is voorzien. Zij zijn daartoe bevoegd, zolang geen strijd met de verdragstekst ontstaat. Zo is het toegestaan, gekwalificeerde vormen van een delict afzonderlijk of met een zwaardere sanctie strafbaar te stellen, zoals bijvoorbeeld het geval is in artikel 138a, tweede, derde en vierde lid, en in artikel 161sexies, tweede, derde en vierde lid, van het Wetboek van Strafrecht.

Gemeenschappelijke bestanddelen

In de Engelse tekst van het Verdrag worden enkele gemeenschappelijke begrippen gehanteerd, die van belang zijn voor het begrip van de meeste strafbepalingen. Het betreft de begrippen «intentionally» en «without right». Voor de omzetting van de verdragstekst in de Nederlandse strafwet kunnen hiervoor de bekende delictsbestanddelen «opzettelijk» en «wederrechtelijk» worden gebruikt. De achterliggende bedoeling van het Verdrag is het bereiken van een zekere harmonisatie van materiële bepalingen. Die harmonisatiedoelstelling strekt zich niet uit tot algemene begrippen en beginselen waarvan de verdragspartijen zich in hun strafwet bedienen. Met de verdragstekst wordt aanvaard dat de genoemde begrippen niet in alle staten op een zelfde wijze worden gebezigd en dat daardoor (geringe) onderlinge afwijkingen in strafbaarheid van bepaalde gedragingen kunnen optreden. Zo mag het bestanddeel «intentionally» worden uitgelegd als mede omvattend «voorwaardelijk opzet», zoals naar Nederlands recht gebruikelijk is.
«Without right» is een eigensoortige term om aan te geven dat de betekenis van dit bestanddeel breder is dan «unlawful» of «illegal» en net als het Nederlandse wederrechtelijk zowel inhoudt het handelen in strijd met

de wettelijke norm als het handelen zonder eigen recht, het hebben van toestemming daaronder begrepen.

2.5 De processuele bepalingen van het Verdrag

Voor welke delicten?

Artikel 14 van het Verdrag geeft een heldere opsomming van de strafbare feiten waarvoor de bevoegdheden van afdeling 2 bedoeld zijn.

- In de eerste plaats betreft dat de materiële delicten zoals die in het Verdrag in hoofdstuk 2 in de artikelen 2 tot en met 11 zijn gedefinieerd, waaronder mede begrepen poging, medeplichtigheid en uitlokking.
- In de tweede plaats zijn de bevoegdheden bedoeld voor andere strafbare feiten die door middel van een computersysteem worden begaan, d.w.z. strafbare feiten voor de uitvoering waarvan gebruik is gemaakt van (de mogelijkheden) van een computersysteem. Deze strafbare feiten kunnen onder omstandigheden tevens onderdeel uitmaken van de in hoofdstuk 2 genoemde delicten. In het Nederlandse strafrecht en ook in het strafrecht van veel andere landen, zijn strafbaarstellingen veelal geformuleerd naar het gevolg dat door bepaald handelen of nalaten wordt veroorzaakt. Voor de uitvoering van deze delicten door middel van een computersysteem ofprogramma zal in de regel dan ook geen aparte strafbaarstelling nodig zijn. Voor de opsporing van die strafbare feiten zal het veelal wel nodig zijn om het elektronische bewijs van het feit aan het gebruikte computersysteem te ontlenen.
- In de derde plaats zijn de bevoegdheden bedoeld voor de opsporing van strafbare feiten die naar hun aard of naar hun uitvoering weliswaar niet als een computerdelict kunnen worden aangemerkt, maar waarvoor het bewijs – in elektronische vorm – in een computersysteem of op een elektronische gegevensdrager kan worden aangetroffen. Dat bewijs kan door de dader ter bewaring zijn vastgelegd of ingevoerd – bijvoorbeeld in de vorm van de elektronische administratie van een frauderende bouwonderneming in de bedrijfscomputer of een lijst met telefoonnummers van dealers in de palmcomputer van een drugshandelaar – of, al dan niet bewust, zijn achtergelaten in elektronische communicatiesystemen of computersystemen met behulp waarvan bepaalde diensten worden verricht, zoals de verkeersgegevens van alle communicaties in het centrale computersysteem van een aanbieder van telecommunicatiediensten of zogenaamde *log files* met betrekking tot de handelingen van bezoekers van een bepaalde website. Bij deze laatste groep zijn de aard en de uitvoering van het strafbare feit irrelevant. Het gaat immers om de vergaring van elektronisch materiaal dat zo mogelijk als bewijs kan worden gebruikt. Deze laatste groep geeft aan de toepassingsmogelijkheden van de bevoegdheden een aanzienlijke uitbreiding.

Onderscheid tussen dataopslag en dataflows

Onderwerp van de opsporingsbevoegdheden zijn gegevens die voorwerp zijn van een geautomatiseerde gegevensverwerking. Die verwerking kan bestaan uit het uitvoeren van geprogrammeerde instructies met betrekking tot die gegevens (bijvoorbeeld een berekening of een mutatie) of uit de overdracht of het transport van die gegevens (bijvoorbeeld de overdracht ten behoeve van al dan niet ter verdere verwerking aan het centrale geheugen, aan de randapparatuur of aan een ander aangesloten computersysteem). Gegevens in een computersysteem of -netwerk kunnen zich derhalve in twee verschillende aggregatietoestanden bevinden: in een statische en een dynamische. In de statische toestand zijn zij op een met het systeem verbonden gegevensdrager vastgelegd, zoals bijvoorbeeld een vaste schijf. De gegevens worden in deze toestand

ter beschikking gehouden voor raadpleging of verdere verwerking. Uitschakeling van het computersysteem heeft geen gevolgen voor de gegevensbestanden die op een gegevensdrager zijn vastgelegd. Deze blijven in stand en kunnen bij opnieuw inschakelen van het systeem worden benaderd. In de dynamische toestand vindt verplaatsing van de gegevens plaats. Een gegevensoverdracht kan plaats vinden binnen de grenzen van een enkel computersysteem, maar ook in de vorm van elektronische communicatie binnen een computernetwerk, een telecommunicatienetwerk daaronder begrepen. Ten behoeve van die overdracht vindt weliswaar vastlegging van die gegevens plaats, maar deze is slechts zeer kortstondig en niet bestemd om die gegevens voor andere bewerkingen beschikbaar te houden, dit in tegenstelling tot de opslag van gegevens, die in beginsel permanent is.

Het Verdrag maakt bij de behandeling van opsporingsbevoegdheden een onderscheid tussen opgeslagen gegevens en gegevensstromen. De strafvorderlijke bevoegdheden om opgeslagen gegevens te verkrijgen worden onderscheiden van de bevoegdheden tot het vergaren van gegevensstromen. Dit onderscheid sluit aan bij het bestaande onderscheid in de traditionele wetgeving met betrekking tot de verkrijging van voorwerpen en de bevoegdheden die de toegang tot en de registratie van telecommunicatie tussen personen tot onderwerp hebben. De voorwaarden en waarborgen, onder de nationale wetgeving op deze typen van bevoegdheden van toepassing, kunnen aanzienlijk verschillen naar gelang de indringendheid van de betreffende bevoegdheid. Een maatregel als inbeslagneming kenmerkt zich door de relatieve openheid ervan, terwijl het afluisteren van bepaalde (tele)communicatie slechts succesvol kan geschieden indien de betrokkenen geen kennis dragen van het feit dat de maatregel wordt toegepast. In het laatste geval zal kennisgeving van de maatregel aan de betrokkene(n) eerst in een later stadium kunnen geschieden.
De artikelen 16 tot en met 19 van het Verdrag betreffen bevoegdheden ten aanzien van reeds opgeslagen gegevens. Deze bepalingen vormen met betrekking tot computergegevens min of meer een uitwerking van de traditionele zoek- en inbeslagnemingsbepalingen ten aanzien van voorwerpen, zij het dat de spoedmaatregelen van de artikelen 16 en 17, gelet op het specifieke karakter daarvan, feitelijk geen pendant in de fysieke wereld kennen.
De artikelen 20 en 21 betreffen bevoegdheden die er juist op gericht zijn dat bepaalde gegevens worden vergaard of vastgelegd. Artikel 20 richt zich op het ten behoeve van het opsporingsonderzoek in *real-time* vergaren of vastleggen van de zogenaamde verkeersgegevens met betrekking tot elektronische communicaties. De bevoegdheden van artikel 21 kunnen door de opsporingsautoriteiten worden aangewend om in *real-time* toegang te verkrijgen tot specifieke elektronische communicaties teneinde de inhoud daarvan te kunnen registreren.

Geen verplichting tot opslag van verkeersgegevens

De beschikbaarheid van verkeersgegevens is van groot belang voor het strafvorderlijk onderzoek. De maatregelen die het Verdrag daartoe in het leven roept gaan uit van een stelsel dat een effectieve vergaring van deze gegevens mogelijk maakt. De basis van dit stelsel is dat bij of van de betrokken dienstverleners slechts verkeersgegevens worden verkregen, voor zover hij of zij daarover beschikt (historische verkeersgegevens) dan wel voor zover deze gegevens aan een specifieke elektronische communicatie kunnen worden ontleend (real-time vergaring van verkeersgegevens). Binnen de Europese Unie (EU) kan een dienstaanbieder verkeersgegevens slechts voor een korte tijd en voor bepaalde doelen bewaren, zoals ten onzent geregeld in hoofdstuk 11 van de (herziene) Telecommunicatiewet. Toepassing van de voorlopige maatregelen van de

artikelen 16 en 17 van het Verdrag draagt bij aan het beschikbaar blijven van dergelijke gegevens, terwijl toepassing van artikel 20 van het Verdrag zeker stelt dat verkeersgegevens vanaf een bepaald moment beschikbaar blijven. Zoals uiteengezet in het Explanatory Memorandum (paragraaf 151) worden deze maatregelen tot het beschikbaar maken en houden van verkeersgegevens alleen toegepast met betrekking tot een *specifieke* communicatie. Het Verdrag verplicht niet tot een systematische en volledige vastlegging van de verkeersgegevens van welke elektronische communicatie dan ook. Dit heeft mogelijk tot gevolg dat bij een dienstverlener niet altijd informatie beschikbaar is over elektronische communicaties in het verleden. Voor een belangrijk deel van de Verdragspartijen wogen de nadelen van een stelsel van volledige bewaring van verkeersgegevens voor de samenleving niet op tegen het voordeel dat de beschikbaarheid van historische verkeersgegevens de mogelijkheden tot identificatie van de dader van een strafbaar feit in bepaalde gevallen kan vergroten. Een en ander neemt niet weg dat er op termijn in ieder geval in Europees verband een maatregel tot stand kan worden gebracht inzake de verplichte opslag van verkeersgegevens. Ik verwijs naar de brief van de Staatssecretaris van Buitenlandse Zaken van 14 juli 20 044 (Kamerstukken TK 2003–2004, 22 112, nr. 331, blz. 3 tot en met 6), waarin is ingegaan op het «Ontwerp-kaderbesluit over de bewaring van gegevens die zijn verwerkt en opgeslagen in verband met het aanbieden van openbare elektronische-communicatiediensten of gegevens in openbare communicatienetwerken met het oog op het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten, daaronder begrepen terrorisme» en naar mijn brief, mede namens mijn ambtgenoot van Binnenlandse Zaken en Koninkrijksrelaties, van 14 februari 2005 (kenmerk 5 334 011/05) waarin nader op een aantal vragen omtrent het ontwerp-kaderbesluit, waaronder de verhouding tot het Cybercrime Verdrag, is ingegaan. Een verplichte opslag van verkeersgegevens als voorzien in het ontwerp-kaderbesluit, zal ertoe kunnen leiden dat een minder frequent gebruik behoeft te worden gemaakt van de maatregelen die het Verdrag ten aanzien van de vergaring van verkeersgegevens voorschrijft, maar maakt deze niet overbodig; zo beperkt het ontwerp-kaderbesluit zich bijvoorbeeld tot openbare diensten en netwerken.

2.6. Internationale rechtshulp

Grensoverschrijdende opsporingshandelingen en internationale rechtshulp

Een van de doelstellingen van het Verdrag was volgens de zogenaamde *terms of reference* tot overeenstemming te komen over het uitoefenen van opsporingsbevoegdheden in computernetwerken die zich geheel of gedeeltelijk op het grondgebied van een der andere verdragsstaten bevinden. Aan een dergelijke bevoegdheid kan behoefte bestaan indien tijd een belangrijke factor is voor het beschikbaar blijven van elektronisch bewijs. In de Nederlandse literatuur is deze figuur wel bekend als «internationale netwerkzoeking». In de toelichtende tekst van de hiervoor aangehaalde Aanbeveling van 1995 (zie noot 5) werd met zoveel woorden erkend dat het uitoefenen van opsporingsbevoegdheden in netwerken die zich op het grondgebied van een andere staat bevinden, in strijd kan komen met het internationale publiekrecht. Dergelijk opsporingsonderzoek dient daarom alleen met toestemming van die staat te geschieden, bijvoorbeeld vormgegeven als een internationale overeenkomst. Na langdurige onderhandelingen kwam vast te staan dat over de instelling van een gemeenschappelijke opsporingsbevoegdheid in internationale elektronische communicatienetwerken, dan wel het onder voorwaarden toestaan van grensoverschrijdende opsporingshandelingen in die

netwerken, tussen de betrokken Partijen vooralsnog geen overeenstemming kon worden bereikt.

In het Verdrag is daarom in artikel 32 vastgelegd in welke beperkte omstandigheden grensoverschrijdende opsporingshandelingen door de verdragspartijen niet worden beschouwd als een schending van de territoriale soevereiniteit van andere verdragspartijen. Deze geven hiermee invulling aan het internationale publiekrecht op dit punt. Gezien echter de beperkte mogelijkheden die artikel 32 open laat voor eigen opsporingshandelingen in internationale elektronische communicatienetwerken, zal voor het verkrijgen van elektronisch bewijsmateriaal uit andere verdragspartijen het middel van de internationale rechtshulp toepassing moeten vinden. Aangezien de bestaande rechtshulpinstrumenten qua procedure en maatregelen in veel gevallen niet toereikend zijn om elektronisch bewijs te vergaren, laat staan dit veilig te stellen en aan een verzoekende Partij uit te leveren, komt het Cybercrime Verdrag met belangrijke nieuwe bevoegdheden en snelle procedures waardoor de beschikbaarheid van elektronisch bewijsmateriaal ten behoeve van een verzoekende Partij in belangrijke mate kan worden verhoogd. Het Verdrag is gericht op een versterking van de internationale samenwerking en levert daarmee een belangrijke bijdrage aan de bestrijding van grensoverschrijdende criminaliteit.

Het Verdrag brengt in artikel 23 (hoofdstuk III, internationale rechtshulp) tot uitdrukking dat Partijen dienen te streven naar een zo breed mogelijke samenwerking in het algemeen ten behoeve van de opsporing van de delicten die in het Verdrag worden gedefinieerd en ten behoeve van de vergaring van elektronisch bewijs. In artikel 25, eerste lid, wordt deze aansporing herhaald met het oog op het verlenen van rechtshulp in het bijzonder. Hoewel aan deze verdragsbepalingen geen *concrete* verplichtingen kunnen worden ontleend, geven zij een duidelijke aanwijzing hoe de toepassing van het Verdrag is bedoeld; men vergelijke ook artikel 552k, eerste lid, van het Wetboek van Strafvordering. Een ander voorbeeld van de strekking van het Verdrag is de opname van artikel 26 dat verdragspartijen de bevoegdheid geeft, dit uiteraard binnen de grenzen door de eigen nationale wetgeving gesteld, om de opsporingsautoriteiten van andere verdragsstaten uit eigen beweging in het kader van een strafrechtelijk onderzoek vergaarde informatie te verstrekken indien dit de andere verdragsstaat in een lopend strafrechtelijk onderzoek of strafrechtelijke procedure van nut kan zijn, bijvoorbeeld door de wetenschap dat deze informatie of het onderliggende materiaal door middel van een rechtshulpverzoek kan worden verkregen. De verstrekkende staat is bevoegd tot het stellen van gebruiksbeperkingen aan de verstrekte informatie.

Verhouding met andere internationale overeenkomsten

Het Cybercrime Verdrag maakt het verlenen van rechtshulp mogelijk, in het bijzonder in verband met de specifieke bevoegdheden zoals deze in hoofdstuk II, afdeling 2, en in hoofdstuk III zijn opgenomen. In sommige gevallen behoeft het verlenen van rechtshulp niet op het Cybercrime Verdrag te worden gegrond, maar kan eenzelfde resultaat worden bereikt op basis van een ander rechtshulpverdrag dat tussen de verzoekende en de aangezochte Partij van kracht is. Bijvoorbeeld, indien een verzoekende Partij vraagt om elektronisch bewijs op een gegevensdrager veilig te stellen en aan de verzoekende Partij uit te leveren, kan dit resultaat worden bereikt door toepassing van de bijzondere bevoegdheid van artikel 19 maar wellicht ook door inbeslagneming en uitlevering van voorwerpen. Dit brengt de vraag mee wat de verhouding is tussen het Cybercrime Verdrag en andere rechtshulpinstrumenten en op welk verdrag in

de internationale rechtspraktijk het verzoeken en verlenen van rechtshulp kan worden gegrond.

Bij de voorbereiding van het Verdrag zijn, in overeenstemming met het Weens Verdragenverdrag ten aanzien van nieuwe verdragen op het gebied van het strafrecht, de volgende uitgangspunten gehanteerd:

a) Het Cybercrime Verdrag heeft geen invloed op de rechten en verplichtingen van verdragspartijen bij bestaande verdragen over specifieke onderwerpen;
b) Partijen bij een toekomstig verdrag zijn bevoegd om over het onderwerp dat door het Cybercrime Verdrag wordt bestreken onderling eigen regelingen te treffen, teneinde de werking daarvan aan te vullen of te versterken;
c) Indien Partijen bij het Verdrag zich met betrekking tot het onderwerp van het Verdrag reeds van een bilaterale of multilaterale regeling hadden voorzien, zijn zij bevoegd deze regeling in hun onderlinge relatie toe te passen in plaats van het nieuwe verdrag, vooropgesteld dat de regeling het verlenen van rechtshulp toelaat.

Aangezien het Cybercrime Verdrag algemene regels ten behoeve van rechtshulp combineert met specifieke maatregelen, is aan deze uitgangspunten in artikel 39 een eigen uitwerking gegeven. In het eerste lid van deze bepaling wordt aangegeven dat het Cybercrime Verdrag bedoeld is als aanvulling op de bestaande internationale instrumenten die tussen de verdragspartijen bij het Cybercrime Verdrag van kracht zijn, zowel multilaterale als bilaterale. Tussen de lidstaten van de Raad van Europa zijn dit meestal multilaterale instrumenten, zoals het op 13 december 1957 te Parijs totstandgekomen Europese Verdrag betreffende uitlevering (Trb. 1965, 9), het op 20 april 1959 te Straatsburg totstandgekomen Europese Verdrag aangaande de wederzijdse rechtshulp in strafzaken (Trb. 1965, 10) en het bij dat laatste verdrag op 17 maart 1978 te Straatsburg totstandgekomen Eerste Aanvullende Protocol (Trb. 1979, 121). Het Tweede Aanvullende Protocol bij dat laatste verdrag (Trb. 2002, 30) is overigens niet in de verdragstekst vermeld aangezien dit pas ongeveer tegelijkertijd met het Cybercrime Verdrag tot stand is gekomen. Tussen de lidstaten van de Europese Unie worden de rechtshulpverhoudingen nader uitgewerkt in de regeling inzake het Europese arrestatiebevel, de Overeenkomst betreffende de wederzijdse rechtshulp in strafzaken tussen de lidstaten van de Europese Unie (Trb. 2000, 96) en het Protocol bij dit laatste verdrag (Trb. 2001, 187). Daarnaast bestaan er tussen individuele verdragspartijen bilaterale rechtshulpinstrumenten, met name die waarbij de niet-Europese verdragspartijen partij zijn. De verdragspartijen zijn op grond van het tweede lid van artikel 39 bevoegd om elkaar rechtshulp te verlenen op basis van andere overeenkomsten die tussen hen bestaan in plaats van het Cybercrime Verdrag, zelfs indien de inhoud van die overeenkomst af zou wijken van, of in strijd zou zijn met de inhoud van het Cybercrime Verdrag. Slechts indien verdragspartijen alsnog zouden overwegen om een overeenkomst aan te gaan rust op hen de verplichting om te voorkomen dat de inhoud daarvan strijd oplevert met het doel en de beginselen van het Cybercrime Verdrag. Het derde lid van artikel 39 drukt ten overvloede uit dat de inhoud van het Cybercrime Verdrag wordt geacht geen invloed te hebben op verplichtingen of rechten van een verdragspartij die voortvloeien uit andere internationale overeenkomsten.

Op grond van welk verdrag een verzoek tot rechtshulp wordt uitgevoerd is derhalve in beginsel afhankelijk van de verzoekende partij die daarvoor de meest geëigende procedure of het meest geëigende middel zal kiezen. Voor de specifieke maatregelen zoals voorzien in de artikelen 29 en volgende ligt een primair beroep op het Cybercrime Verdrag voor de hand. Het is echter niet uitgesloten dat andere rechtshulpinstrumenten tot

vergelijkbare resultaten leiden en dat de verzoekende staat zijn verzoek op dat instrument grondt. Een verdragspartij kan voor het doen van een rechtshulpverzoek echter ook kiezen voor een meer snelle en flexibele procedure, bijvoorbeeld volgens artikel 25, derde lid, dat voorziet in het gebruik van moderne elektronische communicatiemiddelen.

Indien tussen de verdragspartijen bij het Cybercrime Verdrag geen rechtshulpovereenkomst van kracht is, kan de verzoekende partij zijn beroep gronden op het Cybercrime Verdrag zelf. De artikelen 27 en 28 bevatten daartoe een beknopte, maar toereikende minimumregeling. De verdragspartijen zijn bevoegd om deze regeling geheel of gedeeltelijk toe te passen, ook indien tussen hen een regeling van kracht is. Een zodanige situatie kan zich voordoen indien deze bestaande regeling naar beider opvatting niet voldoet aan de moderne eisen van de internationale rechtspraktijk.

Samenvattend kan tussen de verdragspartijen bij het Cybercrime Verdrag rechtshulp worden verleend:

a. Op basis van het Cybercrime Verdrag, al dan niet in combinatie met een andere bestaande regeling. Wanneer de toepassing van bijzondere maatregelen nodig is, zoals die worden gegeven door het Cybercrime Verdrag, ligt het in de rede dit Verdrag toe te passen. Niettemin kan een verdragspartij zijn verzoek gronden op andere rechtshulpinstrumenten of daarin geregelde procedures. Indien tussen de verdragspartijen geen andere rechtshulpovereenkomst van kracht is, kan een rechtstreeks beroep op artikel 27 en 28 worden gedaan. Daarnaast kunnen de verdragspartijen overeenkomen aan het geheel of delen van artikel 27 en 28 toepassing te geven in plaats van de bestaande overeenkomst.
b. Op basis van een tussen Partijen bestaande andere regeling. Indien een bestaande regeling naar het inzicht van Partijen tot een toereikend resultaat leidt, kan de bestaande regeling worden toegepast. Het is aan Partijen te bepalen of zij toepassing aan het Cybercrime Verdrag geven.
c. Op basis van artikel 27 en 28 van het Cybercrime Verdrag. In geval van afwezigheid van een internationale overeenkomst tussen de betrokken verdragspartijen of indien zij de voorkeur geven aan het geheel of een deel van het in die artikelen bepaalde boven de voorzieningen in een bestaande overeenkomst.

3. De koninkrijkspositie

De Regering van Aruba heeft laten weten medegelding van het Verdrag wenselijk te achten. Wel dient nog de benodigde uitvoeringswetgeving te worden afgerond alvorens het Verdrag voor dat land in werking kan treden. De Arubaanse Regering is van mening dat, gelet op internationale ontwikkelingen op het gebied van de informatietechnologie, het Verdrag van groot belang is aangezien het daden, gericht tegen de vertrouwelijkheid, de integriteit en de beschikbaarheid van computersystemen, netwerken en computerdata, alsmede het misbruik van dergelijke systemen, netwerken en data, strafbaar stelt.
De Regering van de Nederlandse Antillen beraadt zich nog over de wenselijkheid van medegelding van het Verdrag.
Teneinde het mogelijk te maken dat, wanneer de benodigde uitvoeringswetgeving voor Aruba in werking is getreden en de Regering van de Nederlandse Antillen medegelding van het Verdrag voor dat land wenselijk acht, deze medegelding direct tot stand kan worden gebracht, wordt goedkeuring van het Verdrag voor het gehele Koninkrijk gevraagd.

4. Toelichting op de artikelen van het Verdrag

Artikel 1: De definities

De definities van artikel 1 gelden voor de gehele verdragstekst. Het *Explanatory Memorandum* geeft aan dat de verdragspartijen niet verplicht zijn om de letterlijke (vertaalde) tekst van deze definities onderdeel van hun wetgeving te maken. Voldoende is dat de nationale regelgeving op deze begrippen van toepassing is op een wijze die in overeenstemming is met de beginselen van het Verdrag en dat deze regelgeving een gelijkwaardig kader biedt voor de implementatie van het in het Verdrag bepaalde.

Artikel 1, onderdeel a, definieert een computersysteem. De kernfunctie van een computersysteem is de geautomatiseerde verwerking van gegevens. Geautomatiseerd wil zeggen zonder directe menselijke tussenkomst. Deze verwerking vindt plaats op basis van een computerprogramma en omvat de invoer, uitvoer, verwerking en opslag van deze gegevens of van de gegevens die het resultaat van die verwerking zijn. Een computersysteem bestaat uit apparaten (hardware) en computerprogramma's (software). Hardware kan worden onderscheiden in processor en randapparatuur die onder besturing van de centrale processor werkt. Het doel van de definitie is aan te geven dat een computersysteem in de zin van het Verdrag kan bestaan uit computersystemen met een zelfstandige betekenis – bijvoorbeeld een palmcomputer, organiser, laptop, main-frame – maar ook een computernetwerk, ongeacht op welke wijze de communicatieverbinding tussen de individuele systemen die het netwerk vormen, wordt onderhouden: door middel van kabels, radioverbindingen, infrarood of satellietcommunicatie. De definitie van geautomatiseerd werk in art. 80sexies Sr zoals deze komt te luiden na van kracht worden van de Wet Computercriminaliteit II voldoet aan de definitie in artikel 1, onder a, van het Verdrag.

Artikel 1, onderdeel b, definieert het begrip computergegeven. Een computergegeven is een gegeven dat zich in een zodanige vorm of codering bevindt dat het direct vatbaar is voor geautomatiseerde verwerking door een computersysteem in de zin van artikel 1, onderdeel a, van het Verdrag. Deze definitie is gebaseerd op de ISO-definitie van een gegeven. In die definitie wordt een gegeven aangemerkt als geschikt voor menselijke kennisname of geautomatiseerde verwerking. Het Verdrag beperkt zich tot gegevens die zich in digitale of elektronische vorm bevinden en derhalve onderwerp zijn van geautomatiseerde verwerking. De definitie in artikel 80quinquies Sr zoals deze komt te luiden na van kracht worden van de Wet Computercriminaliteit II gaat eveneens uit van genoemde ISO-definitie en sluit derhalve de definitie van artikel 1, onder b, van het Verdrag in.

Artikel 1, onderdeel c, definieert de *serviceprovider*. Hieronder wordt verstaan de natuurlijke of rechtspersoon, zowel van privaatrechtelijke als van publiekrechtelijke aard, die de gebruikers van zijn dienst de mogelijkheid biedt om met anderen gegevens uit te wisselen of te verwerken. Het is hierbij niet relevant of deze dienst tegen betaling wordt verricht of uitsluitend ten behoeve van een besloten groep gebruikers. Gelet op de specifieke betekenis van het woord is in de Nederlandse vertaling het woord «serviceprovider» gehandhaafd. Als serviceprovider wordt ook beschouwd de persoon of instelling die ten behoeve van deze dienstverlening gegevens opslaat of verwerkt. Gedacht kan bijvoorbeeld worden aan de aanbieders van webhostingdiensten en beheerders en eigenaren van websites. De Telecommunicatiewet richt zich op de aanbieders van openbare elektronische communicatienetwerken en elektronische communicatiediensten, nader uitgewerkt in artikel 1.1 onder letter e, f, g, h

en i van de Telecommunicatiewet.[1] Hieronder worden verstaan de klassieke aanbieders van openbare telecommunicatienetwerken en -diensten alsmede aanbieders van internettoegang. Het Verdrag maakt in de definitie geen onderscheid tussen openbare elektronische communicatiediensten en niet-openbare elektronische communicatiediensten en richt zich ook op die aanbieders die gebruik maken van deze netwerken om hun diensten aan te bieden, zoals de beheerders en eigenaren van websites en webhostingdiensten. Deze verschillen zijn aanleiding tot aanpassing van de strafvorderlijke bevoegdheden rond het vergaren van verkeersgegevens en het aftappen en opnemen van gegevensverkeer.

Artikel 1, onderdeel d, geeft een functionele definitie van verkeersgegevens. Verkeersgegevens ontstaan in de computersystemen van de serviceproviders in de zin van art. 1, onderdeel c, van het Verdrag. Serviceproviders gebruiken deze gegevens onder andere om hun abonnees te kunnen belasten voor het gebruik van de afgenomen dienst. Maar verkeersgegevens kunnen ook worden gebruikt om een inzicht te verkrijgen in het gebruik dat abonnees van de dienst maken (marketing) of voor andere doeleinden, zoals bijvoorbeeld het bestrijden van misbruik van die diensten. Binnen de Europese Unie wordt het gebruik en de bewaring van verkeersgegevens door dienstenaanbieders van openbare elektronische communicatiediensten geregeld door richtlijn nr. 2002/58/EG van het Europees Parlement en de Raad van de Europese Unie, waarvan de inhoud is opgenomen in Hoofdstuk 11 van de recent gewijzigde Telecommunicatiewet. Voor de goede orde zij er wel op gewezen dat het begrip «verkeersgegevens» in het Verdrag een ruimere betekenis heeft dan in de Telecommunicatiewet. In de Telecommunicatiewet is het begrip gedefinieerd als gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronisch communicatienetwerk of voor de facturering ervan. In het Verdrag betreft het alle computergegevens die verband houden met een met behulp van een computersysteem gevoerde communicatie, die worden voortgebracht door een computersysteem dat een onderdeel vormt van de communicatieketen en die de herkomst, de bestemming, de route, de tijd, de datum, de omvang, de duur of de aard van de betrokken dienst aanduiden. Een ander punt waar het Verdrag en het WvSv het begrip verkeersgegevens in een andere betekenis dan de Telecommunicatiewet hanteren, is dat zij de zogenaamde gebruikersgegevens meenemen, d.w.z. de gegevens betreffende naam, adres, woonplaats, nummer en soort dienst. In het Besluit vorderen gegevens telecommunicatie (Stb. 2004, 394) is bepaald, welke verkeersgegevens de officier van justitie op de voet van artikel 126n van het WvSv mag vorderen.

De beschikbaarheid van verkeersgegevens, met name wanneer de communicatieketen zich uitstrekt over meerdere dienstenaanbieders, kan buitengewoon belangrijk zijn voor het strafrechtelijk onderzoek. In het bijzonder kan met behulp van die verkeersgegevens de bron van een elektronische communicatie worden achterhaald. Met dat gegeven in handen is het mogelijk verder bewijs van het onderzochte strafbare feit te achterhalen. Verkeersgegevens zijn echter gegevens die of op grond van wettelijke verplichtingen of op praktische gronden slechts korte tijd worden bewaard. Een belangrijk deel van de bevoegdheden in het Verdrag richt zich op het op snelle en effectieve wijze beschikbaar krijgen van verkeersgegevens ten behoeve van strafrechtelijk onderzoek.

Verkeersgegevens kunnen uit vele elementen en onderdelen bestaan. De definitie van het Verdrag geeft de categorieën van gegevens die nodig zijn om een elektronische communicatie tot zijn oorsprong te kunnen terugvoeren. Afhankelijk van de technische omgeving van het onderzoek, zullen deze categorieën gegevens niet altijd beschikbaar zijn of steeds nodig om

[1] Wet van 22 april 2004, Stb. 2004, 189, in werking 19 mei 2004.

de oorsprong van de communicatie te achterhalen. De verdragstekst verhindert niet dat verdragspartijen in hun nationale wetgeving aan deze definitie andere bestanddelen of categorieën toevoegen. Voor Nederland wordt verwezen naar het hiervoor genoemde Besluit vorderen gegevens telecommunicatie.

Artikel 2: Wederrechtelijke toegang

Artikel 2 stelt strafbaar het zich opzettelijk en wederrechtelijk toegang verwerven tot het geheel of tot een deel van een computersysteem in de zin van artikel 1 van het Verdrag. De bepaling heeft ten doel de gevaarlijke bedreiging van of de aanval op de werking of inhoud van een computersysteem strafbaar te stellen. Gebruikers van computersystemen hebben een legitiem belang bij een ongehinderd en onverstoord gebruik van die systemen. Het meest doeltreffende middel om onbevoegde toegang te voorkomen is weliswaar de ontwikkeling en toepassing van beveiligingsmaatregelen, maar ook de mogelijke toepassing van het strafrecht kan daaraan een belangrijke aanvullende bijdrage leveren, mede omdat artikel 2 in een vroege fase van uitvoering strafrechtelijke aansprakelijkheid kan doen ontstaan.

Onder het verwerven van toegang tot een systeem – of een deel daarvan – moet worden verstaan het binnengaan in het geheel of enig deel van daarvan. Dit sluit niet alleen de hardware en hardwareonderdelen in, maar ook de gegevensstructuren en de gegevens die zich binnen het systeem bevinden. Toegang tot een systeem kan ook worden verkregen door middel van een ander computersysteem dat door middel van een openbaar telecommunicatienetwerk is verbonden, of met die computer onderdeel van een netwerk uitmaakt. De techniek die wordt gebruikt om zich toegang te verwerven – ter plaatse, door middels van een kabelverbinding, draadloos – is hierbij irrelevant.

Niet als het verwerven van toegang tot een systeem wordt beschouwd het enkele toezenden van een e-mail of het aanbieden ter verwerking van een bestand, omdat de verzender hierdoor geen controle verkrijgt over enige functie van het ontvangende computersysteem.

Wederrechtelijk houdt in het kader van artikel 2 in, dat door de houder of rechthebbende van het computersysteem – of deel daarvan – geen toestemming is verleend. Niet wederrechtelijk is het zich toegang verschaffen tot computervoorzieningen die onder betaling aan het publiek worden aangeboden, zoals bijvoorbeeld een web-site of een publieke databank. Gebruik van bepaalde technische voorzieningen die tot toegang leiden, zoals bijvoorbeeld een hyperlink die naar een web-pagina verwijst, of het plaatsen van zogenaamde cookies dient niet als wederrechtelijk te worden aangemerkt, indien kan worden aangenomen dat de rechthebbende van het computersysteem het gebruik en de effecten van die voorzieningen aanvaardt. Zie voor de Nederlandse situatie bijvoorbeeld het Besluit universele dienstverlening en eindgebruikersbelangen (Stb. 2004, 203), dat strekt ter implementatie van artikel 5, derde lid, van de hiervoor genoemde richtlijn nr. 2002/58/EG. Het plaatsen van cookies, spyware en dergelijke is alleen onder bepaalde wettelijk gestelde voorwaarden toelaatbaar.

Ten behoeve van de verdragspartijen die het strafbaarstellen van het enkele feit van wederrechtelijke toegang niet in kunnen passen in hun criminele politiek of wetgevingstraditie, noemt de verdragstekst een drietal elementen waarvan een verdragspartij bevoegd is er een in de nationale bepaling op te nemen als voorwaarde van strafbaarheid. Deze keuze dient krachtens artikel 40 van het Verdrag bij ratificatie aan de

Secretaris-Generaal kenbaar te worden gemaakt. De elementen zijn: het feit wordt begaan door het doorbreken van veiligheidsmaatregelen; het feit wordt begaan met het oogmerk computergegevens te verkrijgen of het oogmerk van andere oneerlijke bedoelingen; het feit wordt begaan met betrekking tot een computersysteem dat met een ander computersysteem is verbonden. Nederland kan artikel 2 zonder toevoeging van deze elementen implementeren.

Artikel 3: Wederrechtelijke onderschepping

Artikel 3 strekt tot bescherming van de persoonlijke levenssfeer in verband met data communicatie op eenzelfde wijze als de bescherming van traditionele telefoongesprekken tussen personen tegen aftappen en opnemen is geregeld. Artikel 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM) beschermt het recht van vertrouwelijkheid van «correspondence». Artikel 3 breidt dit uit tot alle vormen van elektronische gegevensoverdracht, door middel van de telefoon, fax, e-mail of overdracht van bestanden.

De beschermde elektronische gegevensoverdracht kan plaats vinden als intern gegevenstransport binnen een computersysteem (bijvoorbeeld van centrale besturingseenheid naar randapparatuur), tussen twee computersystemen van eenzelfde persoon, maar ook tussen computersystemen onderling, of tussen een persoon en een computersysteem (bijvoorbeeld door middel van het toetsenbord) en omgekeerd. De bepaling strekt zich eveneens uit tot elektromagnetische emissies die door de computer of onderdelen daarvan als resultaat van het gegevensverwerkende proces met toepasselijke technieken kunnen worden waargenomen.

Voorwerp van bescherming in artikel 3 is de gegevensoverdracht met een niet-openbaar karakter. Hiertoe wordt ook gerekend de gegevensoverdracht aan abonnees van een informatiedienst, bijvoorbeeld betaal-tv, als ook de gegevensoverdracht tussen of met werknemers van een onderneming (zie bijvoorbeeld Europees Hof van de Rechten van de Mens (EHRM) d.d. 25 juni 1997, Halford vs UK, 20605/92).

Bestanddeel van het delict is het gebruik van een technisch middel. Niet strafbaar is derhalve onder artikel 3 de enkele kennisname van een gegevensoverdracht. Onder het onderscheppen met behulp van een technisch middel moet worden verstaan het afluisteren, monitoren, waarnemen van de inhoud van de gegevensoverdracht, maar ook de registratie van de gegevensstroom, direct door middel van toegang of gebruik van het computersysteem waardoor of waarbinnen de gegevensoverdracht plaatsvindt, of indirect door middel van elektronische afluister- en onderscheppingsapparatuur. Een technisch middel beperkt zich niet tot vaste communicatieverbindingen maar kan ook worden aangewend bij draadloze toepassingen.

Artikel 3 verplicht de verdragsstaten niet, indien de gegevensoverdracht mede plaats door middel van radioverbindingen, het onderscheppen van dit radioverkeer strafbaar te stellen, indien het als onderdeel van de vrije ether moet worden aangemerkt.

Het bestanddeel wederrechtelijk ('without right') laat de verdragsstaten ruimte om omstandigheden en voorwaarden aan te geven waaronder het onderscheppen van een gegevensoverdracht met een technisch hulpmiddel niet wederrechtelijk is. Dat is bijvoorbeeld het geval bij bevoegd afluisteren door handhavingsautoriteiten, of onder omstandigheden in een werkgever-werknemer-relatie. Voor het gebruik van cookies waarmee kennis kan worden genomen van het surfgedrag van een internet-

gebruiker op een bepaalde site, geldt *mutatis mutandis* hetzelfde als ter zake onder artikel 2 is opgemerkt.

Artikel 3 bevat evenals artikel 2 enkele aanvullende keuze-elementen; ook hier zal Nederland daarvan geen gebruik hoeven te maken.

Artikel 4: aantasting van gegevens

Het eerste lid van dit artikel stelt strafbaar het opzettelijk en wederrechtelijk aantasten van de integriteit van computergegevens. Als delictshandelingen zijn opgenomen het beschadigen, wissen, aantasten, wijzigen en onderdrukken. Het artikel bestrijkt niet alleen rechtstreekse aantasting van computergegevens maar ook de effecten van computervirussen, computerwormen, Trojaanse paarden en dergelijke. Anders dan in het huidige Nederlandse artikel 350a Sr is de invoer van gegevens en de toevoeging van gegevens aan reeds bestaande geen onderwerp van deze bepaling.
Het strafbaar stellen van het opzettelijk en wederrechtelijk invoeren of toevoegen van gegevens impliceert misbruik (*furtum usus*) van de gegevensverwerkende apparatuur. De verdragspartijen waren van mening dat het aan de individuele staten moest worden overgelaten of die gedragingen strafbaar zouden moeten zijn. Het toevoegen van gegevens zal naar zijn effect doorgaans niet te onderscheiden zijn van het veranderen van die gegevens.

Het staat de verdragspartijen vrij om – al dan niet in de vorm van een strafuitsluitingsgrond – te bepalen in welke gevallen de aantasting van de integriteit van computergegevens niet wederrechtelijk is, zoals bijvoorbeeld thans opgenomen in het vierde lid van artikel 350a Sr met betrekking tot het onschadelijk maken van computervirussen. Het omzetten van computergegevens in een versleutelde vorm is weliswaar een verandering in de zin van artikel 4 maar behoeft al naar gelang de omstandigheden niet als wederrechtelijk te gelden.

In de slotzin van paragraaf 62 van het *Explanatory Memorandum* wordt gerefereerd aan een handeling die op het internet bekend staat als «spoofing». Onder *spoofing* kan een complex van samenhangende handelingen worden verstaan met als doel het verbergen van de oorsprong van elektronische berichten. Bij regulier gebruik van e-mailprogramma's bevat het bericht het adres van de werkelijke afzender. Samen met de andere gegevens van de header is de uiteindelijke route en oorsprong van het bericht door de ontvanger na te gaan. Sommige e-mailprogramma's laten toe een ander adres te vermelden, voor het geval de gebruiker van het adres zich voor de verzending van e-mail van een ander computersysteem wil bedienen. Spoofers bedienen zich van een vals e-mailadres teneinde aansprakelijkheid voor hun handelingen te ontgaan, bijvoorbeeld in geval van verspreiding van virussen of ongevraagde commerciële e-mails (*spam*), of om de indruk te wekken dat een bericht van een bepaalde persoon of instelling afkomstig is.
Mail Transport Agents (MTA's) zijn computerprogramma's die het transport van e-mailberichten verzorgen. In het algemeen accepteren zij geen e-mailverkeer om door te sturen naar andere bepaalde computers (geen «open relay»), maar kunnen in speciale gevallen daartoe wel worden geconfigureerd. Computerkrakers (hackers) proberen dergelijke MTA's wel te kraken of eigen MTA's te installeren op slecht beveiligde systemen. MTA's kunnen ook controleren of het IP-adres van de verzendende computer hoort bij de domeinnaam van de afzender. Niet alle MTA's doen dit en daarvan kan de spoofer gebruik maken. Eenmaal op het internet ondervinden de berichten met vals afzenderadres geen hindernis meer.

Op deze wijze kan de afzender uit de headerinformatie niet meer de herkomst van het bericht vaststellen.
De verdragspartijen konden het niet eens worden over een zelfstandig strafrechtelijk verbod van de manipulatie van headergegevens van e-mail of van andere verkeersgegevens. Een eventuele specifieke strafbaarstelling wordt aan de verdragspartijen zelf overgelaten. Voor Nederland zal hiervan geen gebruik worden gemaakt omdat de algemene computerdelicten afdoende voorzien in deze materie.

Het tweede lid van artikel 4 stelt de verdragspartijen in de gelegenheid als voorwaarde voor strafbaarheid op te nemen dat de genoemde handelingen ernstige schade veroorzaken. Nederland zal van deze mogelijkheid geen gebruik maken.

Artikel 5: Storen van een computersysteem

Onderwerp van artikel 5 is het opzettelijk en wederrechtelijk belemmeren van de werking van een computersysteem. De verdragstekst omschrijft belemmeren als «ernstig hinderen».
Daaronder dient men niet alleen te verstaan het tot stilstand brengen of uitschakelen, maar ook het vertragen of verstoren van het gegevensverwerkend proces. Het *Explanatory Memorandum* geeft geen nadere criteria ter bepaling wanneer er sprake is van ernstig hinderen. Als voorbeeld wordt vermeld het ter verwerking aanbieden van gegevens aan een computersysteem in een zodanige hoeveelheid of omvang dat het computersysteem niet meer in staat is met andere systemen te communiceren, zoals bijvoorbeeld geschiedt bij een *Denial-of-Service (DOS) attack* of bij computervirussen die de verzending van grote hoeveelheden gelijkvormige e-mailberichten genereren. Door het grote aanbod van berichten wordt de werking van het ontvangende systeem aanzienlijk vertraagd met mogelijk uitval als resultaat.

Artikel 5 stelt als voorwaarde voor strafbaarheid dat het belemmeren van de werking van een computersysteem geschiedt door de invoer, de overdracht, het beschadigen, het wissen, het aantasten, het wijzigen of het onderdrukken van computergegevens. Voor fysieke aantasting van gegevensverwerkende apparatuur dienen de klassieke bepalingen met betrekking tot zaaksbeschadiging te worden toegepast.

Artikel 5 heeft op zichzelf niet ten doel het strafbaar stellen van de verzending van *spam*. Hoewel *spam* in de regel in grote hoeveelheden wordt verzonden en deze verzending de werking van in de communicatieketen betrokken computersystemen kan vertragen, is hier doorgaans geen sprake van belemmeren of ernstige hinder. Indien daarvan echter wel sprake is, kan artikel 5 toepassing vinden. De verdragspartijen zagen daarnaast geen aanleiding voor een zelfstandige strafbaarstelling tegen *spam*.

Artikel 6: Misbruik van technische hulpmiddelen

Met name in de internetomgeving worden vaak middelen ter beschikking gesteld waarvan men gebruik kan maken om een van de in artikelen 2 tot en met 5 omschreven delicten te begaan. Deze middelen zijn bijvoorbeeld zogenaamde kraakprogramma's, passwoorden en toegangscodes – waarmee onbevoegd toegang tot een computersysteem- of computernetwerk kan worden verkregen – maar ook schade veroorzakende programma's als virussen en *worms*. Deze middelen kunnen ook bestaan in de vorm van apparaten of toestellen. In de opvatting van de verdragspartijen zou het in strafrechtelijke zin ongemoeid laten van het aanbod van dergelijke middelen leiden tot een soort zwarte markt met ernstige risico's voor de vertrouwelijkheid, de integriteit en de beschikbaarheid van

geautomatiseerde gegevensverwerking en gegevens. Artikel 6 richt zich dan ook tegen de vervaardiging, de verspreiding en het anderszins beschikbaar stellen van dergelijke middelen. Onder dit laatste wordt mede begrepen het opnemen van een hyperlink naar de site van waaraf deze middelen kunnen worden gedownload. Als delictshandelingen worden genoemd het vervaardigen, verkopen, verkrijgen voor gebruik, invoeren, verspreiden of anderszinds beschikbaar stellen. Het enkele bezit van dergelijke middelen – daaronder mede te verstaan het ter beschikking hebben van deze middelen – is eveneens strafbaar. Dit is apart opgenomen onder letter b, enerzijds in verband met de in het derde lid voorziene mogelijkheid van een voorbehoud en anderzijds in verband met de daarbij voorziene mogelijkheid van een beperking in de strafbaarheid van het enkele bezit. Deze laatste mogelijkheid is opgenomen ten behoeve van de Verenigde Staten van Amerika, omdat de wetgeving van een aantal staten om reden van bewijsmotieven slechts het bezit van méér dan één passwoord strafbaar stelt.

Voorwerp van het strafrechtelijk verbod zijn die middelen die hoofdzakelijk voor het begaan van de genoemde delicten zijn ontworpen of aangepast. Uit de inrichting en de eigenschappen van het middel dient te blijken dat dit door de producent ook bedoeld is om een delict als omschreven in de artikelen 2 tot en met 5 te begaan. Het Verdrag gebruikt hier niet de term «uitsluitend» of «specifiek» omdat daardoor onoverkomelijke bewijsproblemen zouden ontstaan. De verdachte zou om in een dergelijk geval vrijuit te gaan slechts behoeven aan te tonen dat het middel ook voor enig ander gebruik geschikt is. De term «hoofdzakelijk» sluit niet uit dat ander al dan niet legitiem gebruik mogelijk is, maar impliceert dat zodanig gebruik als ondergeschikt moet worden beschouwd ten aanzien van de naar objectieve maatstaven vast te stellen gebruiksmogelijkheden, nl. als hulpmiddel tot het begaan van een der in de artikelen 2 tot en met 5 genoemde delicten.[1]

De gedraging dient opzettelijk en wederrechtelijk te zijn en dient te geschieden met het oogmerk dat een of meer van de in de artikelen 2 tot en met 5 gedefinieerde delicten wordt begaan. Het staat de verdragsstaten vrij om al dan niet in de vorm van een strafuitsluitingsgrond te bepalen wanneer de vervaardiging etc. van bovenstaande middelen niet wederrechtelijk is. Het tweede lid geeft hiervan een voorbeeld, namelijk in geval apparatuur of voorzieningen bedoeld voor het testen of het beveiligen van computersystemen. De vervaardiging en de verspreiding van dergelijke apparatuur is derhalve niet strafbaar.

Het derde lid geeft de verdragspartijen de mogelijkheid om een voorbehoud te maken. Zoals hierboven reeds aangegeven mag een verdragsstaat het enkele bezit van middelen in de zin van artikel 6 van strafbaarheid uitzonderen. Eveneens is een voorbehoud mogelijk ten aanzien van de onder het eerste lid onder a opgenomen delictshandelingen, met uitzondering van de verkoop, de verspreiding of het anderszins beschikbaar stellen van computerwachtwoorden, toegangscodes of soortgelijke gegevens waarmee toegang kan worden verkregen tot een computersysteem of een deel daarvan. Het voorbehoud kan derhalve wel worden gemaakt ten behoeve van «het vervaardigen», «het zich verwerven voor gebruik», of «de invoer». Nederland zal hiervan geen gebruik maken.

Artikelen 7 en 8: Computer-gerelateerde valsheid en computer-gerelateerde fraude

De artikelen 7 en 8 zijn zogenaamde assimilatiebepalingen. Deze geven de individuele verdragspartij opdracht te onderzoeken in hoeverre de bestaande bedrogs- en valsheidbepalingen in de nationale omgeving van

[1] Paragraaf 73 Explanatory Memorandum.

toepassing zijn op handelingen die of op elektronische wijze worden uitgevoerd dan wel gericht zijn op de wederrechtelijke verkrijging van elektronische waarden.

Artikel 7 richt zich op de invoering van een bepaling voor de elektronische omgeving, parallel aan de traditionele bepaling of bepalingen inzake valsheid in geschrift. In de verschillende nationale strafrechtstelsels stelt men in het algemeen aan geschrift de eis van visuele leesbaarheid en dient de inhoud een verklaring te bevatten, of – zoals naar Nederlands recht – een menselijke gedachte-uiting. Computergegevens zullen in een aantal gevallen niet aan die voorwaarden voldoen. Het manipuleren van computergegevens kan echter, indien men in het maatschappelijk verkeer op de juistheid daarvan vertrouwt, tot dezelfde schadelijke gevolgen leiden als het vervalsen van een geschrift. Artikel 7 beoogt in het bijzonder de integriteit van computerrecords en -bestanden te beschermen indien in het maatschappelijk verkeer op de juistheid daarvan wordt vertrouwd.

Artikel 7 heeft als onderwerp het vervalsen van computergegevens. Op welke wijze die gegevens worden vervalst is irrelevant. De handelingen dienen te resulteren in wat in de bepaling wordt omschreven als niet-oorspronkelijke gegevens. Artikel 7 stelt niet de eis dat de gegevens direct leesbaar en begrijpelijk zijn.

Artikel 7 sluit niet de handeling in die ten onzent wel als intellectuele valsheid wordt aangemerkt. Hiermee wordt niet gedoeld op het vervalsen van een bestaand geschrift, maar het opmaken van een geschrift waarvan de inhoud als vals en daarom als misleidend moet worden beschouwd. Niet alle verdragsstaten kennen een dergelijk concept. Artikel 7 staat het strafbaarstellen van het valselijk opmaken van een elektronisch document niet in de weg.

Ten behoeve van *common-law*-landen staat de mogelijkheid open als voorwaarde voor strafbaarheid op te nemen dat de dader handelt met de opzet tot bedrog of soortgelijke oneerlijke bedoeling.

Nederland behoeft wegens artikel 7 geen wetgevende maatregelen te treffen. Gelet op de in de jurisprudentie van de Hoge Raad neergelegde functioneel-equivalente interpretatie, kunnen ook computerbestanden en computerrecords, mits bestemd om tot bewijs te dienen, onder artikel 225 Sr worden gevat. Aan computervarianten van de specifieke valsheid-delicten is naast het bestaande artikel 232 Sr geen behoefte. Voor een recente wijziging van dit laatste artikel in verband met het bepaalde in het Europese Kaderbesluit inzake fraude in verband met niet-contante betaal-middelen zij verwezen naar de Wet Fraude niet-chartaal geldverkeer.[1] Artikel 8 verplicht de verdragspartijen tot het nemen van wettelijke maat-regelen indien de bestaande bedrogbepalingen niet tevens van toepas-sing zijn op bedrog in verband met computersystemen en -netwerken. Bedrog in strafrechtelijke zin houdt onder meer in dat de dader een weder-rechtelijke vermogensverschuiving tot stand brengt door een bedrieglijke voorstelling van zaken. Een vergelijkbare handeling is ook in verband met computersystemen en -netwerken denkbaar. Veel vermogens-componenten, op welker verkrijging de opzet van de dader is gericht, kunnen zich immers in een elektronische vorm voordoen (bijvoorbeeld computerprogrammatuur, bestanden met een economische waarde, elek-tronisch geld, maar ook elektronische diensten). Om die vermogens-componenten te verkrijgen manipuleert de dader het onderliggende gege-vensverwerkende proces. Artikel 8 formuleert de wederrechtelijke vermogensverschuiving als het opzettelijk en wederrechtelijk bij een ander veroorzaken van het verlies van een vermogensbestanddeel door een handeling die geschiedt met de bedriegelijke of anderszins oneerlijke

[1] Wet van 21 april 2004, Stb. 2004, 180.

bedoeling om voor zichzelf of een ander wederrechtelijk een economisch voordeel te verkrijgen. De feitelijke handeling bestaat uit het invoeren, wijzigen, wissen of onderdrukken van computergegevens (letter a) dan wel het verstoren van de werking van een computersysteem (letter b).

Nederland hoeft geen aanvullende wettelijke maatregelen te treffen, gelet op de artikelen 326 en volgende van het Wetboek van Strafrecht, in het bijzonder artikel 326c.

Artikel 9: Delicten in verband met kinderpornografie

De ratio van artikel 9 is tweevoudig. Zoals is uiteengezet in paragraaf 102 van het *Explanatory Memorandum* strekt de strafbaarstelling van de verschillende gedragingen in de eerste plaats tot directe bescherming van minderjarigen tegen misbruik. Daarnaast beoogt de bepaling gedragingen tegen te gaan die kinderpornografie als maatschappelijk aanvaard of gewenst beogen voor te stellen en minderjarigen zouden kunnen bewegen zich aan dergelijke handelingen deel te nemen.
Het gezamenlijke onderwerp van die gedragingen is pornografisch materiaal met als onderwerp minderjarige kinderen. De indeling van het artikel in verschillende leden is er niet alleen ter verhoging van de duidelijkheid maar heeft vooral een relatie met de wens van bepaalde verdragspartijen zich het recht voor te behouden zich niet te binden aan de inhoud van de gehele bepaling. Het vierde lid geeft aan naar welke onderdelen van de voorgaande leden een voorbehoud mag verwijzen. Gezien de inrichting van artikel 240b Sr zoals dit artikel na de inwerkingtreding van de Wet Herziening Zedelijkheidswetgeving (Stb. 2000, 388) luidt, heeft Nederland op dit punt geen behoefte aan voorbehouden.

Artikel 10: Delicten met betrekking tot inbreuken op auteursrecht en naburige rechten

De ratio van deze bepaling is vooral gelegen in de wens van de verdragspartijen dat voor de bestrijding van schendingen van het auteursrecht (eerste lid) en van de naburige rechten (tweede lid) een beroep kan worden gedaan op het strafrechtelijk sanctiestelsel, indien daarbij gebruik is gemaakt van een computersysteem of computernetwerk. Aangezien toepassing van strafrecht op het gebied van de intellectuele eigendom in de wetgeving van de verdragspartijen niet in een zelfde omvang toepassing vindt, was er voldoende aanleiding voor de opname van een bepaling als artikel 10. Anders dan het betreffende onderdeel in de Aanbeveling van 1989 dat zich alleen richtte op computerprogrammatuur, is artikel 10 van toepassing op elk werk of prestatie in elektronische vorm die onder die wetten bescherming ondervindt. Tevens strekt de bescherming zich uit tot de naburige rechten.

Morele rechten zijn uitgezonderd van de bepaling. Op de verdragspartijen rust geen verplichting om alle schendingen van het auteursrecht en naburige rechten met een strafsanctie te bedreigen.

Het derde lid van artikel 10 bevat de mogelijkheid tot het maken van een voorbehoud: sommige verdragspartijen zien geen mogelijkheden voor toepassing van het strafrecht indien schendingen van het auteursrecht worden begaan door publieke organisaties, bijvoorbeeld op het gebied van omroep.

De strafbepalingen in de Nederlandse Auteurswet en de Wet op de naburige rechten voldoen aan de door het Verdrag gestelde eisen, aangezien deze bepalingen anders dan in artikel 10 Verdrag geen ondergrens voor strafbaarheid kennen. Bij het vragen van rechtshulp met betrekking tot de

opsporing en vervolging van genoemde delicten moet er rekening mee worden gehouden dat bij bepaalde gedragingen dubbele strafbaarheid kan ontbreken, of omdat de gedraging in de termen van het Verdrag als onvoldoende ernstig moet worden aangemerkt, of omdat door de aangezochte verdragspartij een voorbehoud op basis van het derde lid van artikel 10 is gemaakt. Voor de rechtshulpverlening zal dit naar verwachting niet leiden tot onoverkomelijke problemen.

Artikel 11: Poging, medeplichtigheid, uitlokking

Dit artikel verplicht de verdragspartijen met betrekking tot de feiten, genoemd in de artikelen 2 tot en met 10 van het Verdrag, te voorzien in strafbaarheid van opzettelijke medeplichtigheid aan of uitlokking tot het plegen van het feit. Wat betreft de feiten, genoemd in de artikelen 3 tot en met 5, 7, 8 en 9, eerste lid, letter a en c, worden de verdragspartijen verplicht ook de opzettelijke poging strafbaar te stellen, tenzij daarvoor op grond van het derde lid een voorbehoud wordt gemaakt. In het Nederlandse strafrecht zijn de poging en de genoemde deelnemingsvormen in beginsel van toepassing op alle delicten; een voorbehoud als bedoeld in het derde lid hoeft niet gemaakt te worden.

Artikel 12: Aansprakelijkheid van rechtspersonen

Hoewel de tekst van de bepaling zich beperkt tot de strafbare feiten gedefinieerd in het Cybercrime Verdrag, wordt met de opneming beoogd een algemene aansprakelijkheid van rechtspersonen in het leven te roepen. De bepaling laat de mogelijkheid open deze aansprakelijkheid strafrechtelijk dan wel civielrechtelijk of administratiefrechtelijk vorm te geven. De Nederlandse wetgever heeft sinds lang voorzien in strafrechtelijke aansprakelijkheid van rechtspersonen en hun leidinggevenden, zoals vastgelegd in artikel 51 Sr, naast civielrechtelijke aansprakelijkheid op grond van de artikelen 6:162 BW en verder. Artikel 12 voegt aan de omvang en voorwaarden van de huidige strafrechtelijke en civielrechtelijke aansprakelijkheid naar Nederlands recht niets toe en kan daarom buiten verdere beschouwing blijven.

Artikel 13: Sancties en maatregelen

Het Verdrag geeft geen voorschriften met betrekking tot de hoogte van de straffen die de verdragspartijen aan het begaan van de strafbare feiten zoals gedefinieerd in de artikelen 2 tot en met 10 in hun nationale wetgeving dienen te verbinden. Gezien de divergentie van de nationale sanctiestelsels moet dit aan de individuele verdragspartij worden overgelaten. Artikel 13 volstaat met de opdracht aan de verdragspartijen om doeltreffende, proportionele en afschrikwekkende sancties, waaronder vrijheidsstraffen, te stellen. Wat betreft de rechtspersonen wordt uitdrukkelijk bepaald dat de sancties van strafrechtelijke of niet-strafrechtelijke aard kunnen zijn, maar in ieder geval wel financiële sancties dienen te omvatten.

Artikel 14: Reikwijdte van procesrechtelijke maatregelen

Artikel 14 van het Verdrag bepaalt dat de in Afdeling 2 geregelde bevoegdheden en procedures van toepassing dienen te zijn ten aanzien van:

a. De strafbare feiten, bedoeld in de artikelen 2 tot en met 11 van het Verdrag;
b. Andere strafbare feiten, begaan met behulp van een computersysteem, waartoe delicten behoren die weliswaar van eenzelfde type zijn als de onder a) genoemde maar die buiten het geharmoniseerde

kader van het Verdrag vallen. In algemene zin kan men hier noemen de uitings- en verspreidingsdelicten, gepleegd met behulp van elektronische middelen, of bijvoorbeeld het spioneren in of het wederrechtelijk overnemen van informatie uit computersystemen dat als zodanig in het Verdrag onder a) niet wordt genoemd, of het wederrechtelijk vervaardigen van elektronische kopieën van onder de Auteurswet 1912 beschermde werken als computerprogrammatuur, voor zover niet begrepen onder artikel 10 van het Verdrag.

c) Elk ander strafbaar feit, waarvan het bewijs zich in elektronische vorm bevindt. Bewijs dient hier te worden gelezen als «potentieel bewijs» en sluit sporen of aanwijzingen voor verder onderzoek in. Deze laatste groep delicten betreft elk al dan niet met behulp van computertechnologie gepleegd delict, voor de opsporing waarvan bewijs kan worden gevonden in een computersysteem of op een elektronische gegevensdrager die daarvan al dan niet onderdeel uitmaakt. Een voorbeeld van deze groep is een overtreding van de Opiumwet voor de opsporing waarvan een elektronische communicatie met de verdachte wordt afgetapt en opgenomen, of een btw-fraude waarvoor onderzoek van de in een computersysteem opgeslagen administratie van een onderneming nodig is.

De tekst van het artikel impliceert dat digitaal of elektronisch bewijsmateriaal in een strafprocedure onder het nationale recht toelaatbaar is. Voor verdragsstaten met een vrij bewijsstelsel zal dat in beginsel het geval zijn; voor verdragstaten met een geheel of gedeeltelijk formeel bewijsstelsel kan daartoe wetswijziging nodig zijn. Het Nederlandse strafrechtelijke bewijsrecht zoals beschreven in de artikelen 339 Sv en verder, verzet zich niet tegen het gebruik van digitaal of elektronisch bewijs mits vervat in de vorm van een der voorgeschreven bewijsmiddelen. Het daarvoor meest gerede bewijsmiddel is dat van de schriftelijke bescheiden (artikel 344, sub 5, Sv). Onder verwijzing naar HR 21 januari 1991 (NJ 1993, 693) kan worden gesteld dat digitaal of elektronisch vastgelegde gegevens als zodanig kunnen worden aangemerkt. Digitale of elektronische gegevens die een afbeelding of geluidsfragment representeren zijn, evenmin als dat het geval is bij traditionele afbeeldingen of geluidsopnamen, niet als bewijsmiddel toelaatbaar, maar de inhoud ervan kan wel als stuk van overtuiging ter kennis van de rechter worden gebracht.

Artikel 15: Voorwaarden en waarborgen

De strafvorderlijke bevoegdheden en maatregelen dienen door de verdragspartij in het nationale strafrecht te worden omgezet. De doelstelling van het Verdrag is niet – en kan dit ook niet zijn – de harmonisatie van strafvorderlijke bevoegdheden in algemene zin, maar de harmonisatie van de als ondergrens noodzakelijk geachte strafvorderlijke bevoegdheden in verband met de vergaring van elektronisch bewijs zoals omschreven in artikel 14 van het Verdrag. De vergaring van elektronisch bewijs is in het algemeen geen zelfstandig onderdeel van de bestaande, traditionele wetten. Onder omstandigheden kan elektronisch bewijs eveneens worden vergaard met gebruikmaking van traditionele dwangmiddelen en bevoegdheden. Het Verdrag eist niet dat de verdragspartijen een zelfstandig stelsel tot vergaring van elektronisch bewijs in het leven roepen. Waar bestaande dwangmiddelen en bevoegdheden mede strekken ter vergaring van dergelijk bewijs kan met de bestaande wetgeving worden volstaan. Waar deze niet voldoet aan de bepalingen van het Verdrag, dient in een aanvulling of uitbreiding te worden voorzien. De bestaande bevoegdheden in nationale wetstelsels zijn ingebed in een systeem van voorwaarden en waarborgen dat vorm geeft aan de aan het strafrecht ten grondslag gelegde beginselen als bijvoorbeeld die van een eerlijk proces en beginselen van subsidiariteit en proportionaliteit. Het ligt dan ook voor

de hand om bij aanvulling of uitbreiding van de bestaande wettelijke bevoegdheden in verband met de vergaring van elektronisch bewijs aan te sluiten bij het bestaande stelsel van voorwaarden en waarborgen en bij nieuwe bevoegdheden die voorwaarden en waarborgen te kiezen die van toepassing zijn op vergelijkbare traditionele bevoegdheden ter vergaring van strafrechtelijk bewijs. Het gaat daarbij vooral om proportionaliteit, subsidiariteit en een adequate rechtsbescherming.

Het Verdrag gaat uit van de realiteit dat er een grote diversiteit bestaat tussen de verschillende nationale stelsels met betrekking tot deze voorwaarden en waarborgen en laat het daarom aan de verdragspartijen op welke wijze zij daaraan vorm geven. Als minimum verwijst artikel 15 verwijst naar het EVRM dat in deze voor de lidstaten van de Raad van Europa in het bijzonder relevant is, en naar andere internationale instrumenten die op overeenkomstige wijze van betekenis zijn voor niet-lidstaten. Bij de toelating van nieuwe verdragspartijen zal mede bepalend zijn op welke wijze zij vorm geven aan de bescherming van fundamentele rechten zoals besloten in het EVRM.

Het tweede lid geeft een niet-limitatieve algemene opsomming van de voorwaarden en waarborgen die in algemene zin in het strafprocesrecht worden toegepast, zoals rechterlijk of ander onafhankelijk toezicht, gronden voor de toepassing, beperking tot bepaalde doelen en beperking in de tijd. Deze voorwaarden en waarborgen behoeven niet in de strafwet te zijn opgenomen maar kunnen ook worden ontleend aan bijvoorbeeld de Grondwet of aan de rechtspraak. Toepassing van deze voorwaarden en waarborgen kan leiden tot bepaalde toepassingsmodaliteiten. Het is de verdragspartijen niet toegestaan zodanige voorwaarden aan de toepassing van de door het Verdrag gegeven bevoegdheden te stellen, dat toepassing ervan in belangrijke mate zou worden verhinderd. De verdragspartijen wordt aangeraden om bij implementatie rekening te houden met de mate van indringendheid van de maatregelen en dat bepalend te laten zijn voor de formulering van de voorwaarden en waarborgen terzake van de specifieke bevoegdheid. Aanvullend worden in paragraaf 147 van het *Explanatory Memorandum* als mogelijke voorwaarden en waarborgen nog genoemd het verbod tot zelfincriminatie, wettelijke privileges (bijvoorbeeld het verschoningsrecht van wettelijke geheimhouders) en het voorschrift om personen en plaatsen die voorwerp van de strafrechtelijke maatregel zijn, specifiek aan te duiden.

Het derde lid leidt niet zozeer tot concrete verplichtingen voor de verdragspartijen maar is meer de formulering van een beginsel. Voor de Nederlandse rechtsorde kan worden verwezen naar de ongeschreven beginselen van subsidiariteit en proportionaliteit. Aan de uitwerking van het beginsel van het derde lid kan door de verdragspartijen op verschillende wijze vorm worden gegeven.

Teneinde het belang aan te geven van het in artikel 14 en 15 bepaalde wordt in de individuele bepalingen van artikel 16 tot en met 21 steeds naar deze bepalingen terugverwezen.

Artikel 16: Spoedbewaring van opgeslagen computergegevens

De bevoegdheid van artikel 16 dient om er toe om de beschikbaarheid te verzekeren van zogenaamde vluchtige computergegevens, dat wil zeggen gegevens die op enig moment als resultaat van een geautomatiseerde gegevensverwerking zijn ontstaan maar waarvan de bewaring door de houder – of beter door zijn geautomatiseerde gegevensverwerkend systeem – niet waarschijnlijk is of niet kan worden aangenomen. De verdragstekst duidt dergelijke gegevens aan als «bijzonder vatbaar voor

verlies of wijziging». Dergelijke gegevens worden met name gevonden in computerregistraties die naar hun aard als tijdelijk zijn aan te merken, bijvoorbeeld de registratie van gebruiksgegevens door specifieke apparatuur als onderdeel in een computer- of telecommunicatienetwerk. In het artikel zelf worden met name de verkeersgegevens genoemd. De verdere bewaring van deze gegevens is niet geboden wegens het bestaan van een wettelijke verplichting of een belang van de houder, bijvoorbeeld de specificatie van nota's of het verhelpen van storingen. Niettemin kan de beschikbaarheid van die gegevens van belang zijn voor het strafrechtelijk onderzoek.

Bij de Tweede Kamer is inmiddels in behandeling het wetsvoorstel «Bevoegdheden vorderen gegevens» (Kamerstukken II 2003/04, 29 441). Dat wetsvoorstel beperkt zich niet tot gegevens die in een elektronische vorm zijn opgeslagen maar sluit tevens andere vastleggingen van gegevens in, waarvan papier de belangrijkste is. Het wetsvoorstel schept hiermee bevoegdheden met een ruimere strekking dan die in de verdragsverplichtingen van artikel 16 (en ook artikel 18) besloten ligt. Voor de toelichting op het door dat wetsvoorstel bepleite wettelijke stelsel zij verwezen naar de memorie van toelichting bij dat wetsvoorstel (idem, nr. 3). Hier kan daarom worden volstaan met een korte bespreking van enkele belangrijke elementen van artikel 16 van het Verdrag.

Toepassing van de bevoegdheid, voorzien in artikel 16 van het Verdrag, strekt alleen tot de bewaring van dergelijke gegevens. Het daadwerkelijk ter beschikking brengen van de betreffende gegevens geschiedt door de toepassing van de bevoegdheid, voorzien in artikel 18 van het Verdrag. Het is de bedoeling dat toepassing van artikel 16 wordt belast met zo weinig mogelijk formaliteiten ten einde onmiddellijke en flexibele toepassing mogelijk te maken. Van de houder van de desbetreffende gegevens wordt niet meer verlangd dan dat hij deze behoedt voor verlies of wijziging. Een bevel op de voet van artikel 16 van het Verdrag staat verder gebruik van (een kopie) van de betreffende gegevens niet in de weg.

Het eerste lid van artikel 16 betreft de mogelijkheid om «de spoedbewaring te bevelen of op soortgelijke wijze de spoedbewaring te bewerkstelligen van gespecificeerde computergegevens (...) die zijn opgeslagen door middel van een computersysteem». Het artikel strekt daarmee niet tot een algemene registratieplicht van gegevens waarvan de onmiddellijke bewaring kan worden bevolen.

Het tweede lid van artikel 16 geeft aan dat het bevel van het eerste lid alleen gericht kan worden tot de persoon die de specifieke gegevens in zijn bezit heeft of tot welker toegang hij gerechtigd is. Dat laatste houdt in dat een persoon feitelijk en bevoegd toegang tot deze gegevens heeft. Een bevel tot bewaring houdt mede in dat de bevolene zorg draagt voor de bewaring van de integriteit van de gegevens, dat wil zeggen dat zij in de dezelfde vorm of toestand worden bewaard als waarin zij zich op het moment van de uitvoering van het bevel bevonden. De maximale duur van de bewaring bedraagt 90 dagen met de mogelijkheid van verlenging. Dit laatste is vooral van belang in verband met de verlening van rechtshulp. Met het verkrijgen van een uitleveringsbevel kan, althans in andere jurisdicties dan de Nederlandse, soms veel tijd gemoeid zijn. Hoe de bewaring van de veiliggestelde gegevens voor het overige plaats dient te vinden en onder welke (aanvullende) voorwaarden is ter bepaling aan de verdragspartijen.

Het derde lid van artikel 16 geeft de mogelijkheid tot het opleggen van geheimhouding aan de bevolene of aan degene aan wie de bewaring van de gegevens is opgedragen.

Artikel 17: Spoedbewaring en gedeeltelijke verstrekking van verkeersgegevens

Artikel 17 richt zich specifiek op de spoedbewaring van verkeersgegevens, zoals gedefinieerd in artikel 1, onder d, van het Verdrag. De bevoegdheid dient tot het veiligstellen van de verkeersgegevens met betrekking tot een specifieke communicatie door middel van computersystemen. Het uiteindelijke doel hiervan is het vinden van de bron van de communicatie. Daarvoor zal dikwijls niet voldoende zijn om de gegevens bij de laatste serviceprovider in de communicatieketen veilig te stellen; ook de gegevens van serviceproviders die een functie in het geheel van de communicatieketen vervullen, kunnen daartoe nodig zijn. Artikel 17 bevat in het eerste lid, onder letter a, de verplichting van de verdragspartij om te verzekeren dat een spoedbewaring van gegevens mogelijk is «ongeacht of een of meer serviceproviders bij de overdracht van die gegevens betrokken waren». Hiermee is beoogd aan te geven dat geen tijd wordt verloren met het doorlopen van procedures tot uitoefening van de bevoegdheid van artikel 16- en dat voor iedere communicatiedienstverlener afzonderlijk – maar dat het bevel aanstonds werking kan hebben voor alle betrokken serviceproviders. Het is aan de verdragspartijen om hieraan uitwerking te geven. Dit kan in de vorm van een centraal bevel dat van toepassing is voor alle daarin genoemde dienstverleners, maar volgens het *Explanatory Memorandum* (paragraaf 168) is ook denkbaar het bevel werking te geven ten opzichte van ten tijde van de uitgifte van het bevel nog niet geïdentificeerde serviceproviders. Een andere mogelijkheid is het scheppen van een wettelijke verplichting a) ten aanzien van een aldus bevolen serviceprovider om na te gaan of andere serviceproviders in de communicatieketen zijn betrokken, deze het bestaan en de inhoud van het bevel kenbaar te maken, en b) het scheppen van een wettelijke verplichting voor deze laatste serviceprovider tot nakoming van het bevel en de daarbij behorende waarschuwingsplicht. Het door het Verdrag beoogde effect kan ook worden bereikt door een bevel tot spoedbewaring te omringen met minimale formaliteiten, zoals het openen van de mogelijkheid het bevel mondeling te geven en de bevoegdheid ertoe te leggen op een zo laag mogelijk niveau in de opsporingsorganisatie. Dit staat er niet aan in de weg om van het bevel een schriftelijk bevestiging te verlangen of goedkeuring door een verantwoordelijke autoriteit.

De opsporingsautoriteit die een bevel krachtens artikel 16 van het Verdrag richt tot een serviceprovider tot spoedbewaring van bepaalde verkeersgegevens, is niet noodzakelijk op de hoogte van het feit dat mogelijk meerdere dienstverleners bij de communicatie betrokken waren. Hij komt hiervan eerst op de hoogte indien de desbetreffende gegevens krachtens een bevel ex artikel 18 Verdrag aan hem verstrekt zijn. Aangezien er tussen de toepassing van beide bevoegdheden enige tijd kan zijn verlopen, bestaat het risico dat de belangrijke verkeersgegevens inmiddels bij de andere serviceproviders niet meer (volledig) beschikbaar zijn en dat een spoedbewaring zinloos is geworden. De serviceproviders dienen daarom wettelijk verplicht te worden om in geval van een spoedbewaring aan de hand van veiliggestelde verkeersgegevens na te gaan of meer serviceproviders in de communicatieketen waren betrokken en zo ja, een zodanig deel van de verkeersgegevens aan de opsporingsautoriteiten te verstrekken dat deze serviceprovider kan worden geïdentificeerd. Dit gegeven zal veelal niet meer betreffen dan het code- of IP-nummer van de betreffende serviceprovider. Vanzelfsprekend is niemand gehouden tot het onmogelijke. Indien een serviceprovider niet weet wie de tussenliggende schakel is of wie de desbetreffende gegevens heeft – denk aan internetverkeer waarbij berichten als het ware worden opgeknipt in diverse pakketjes die allemaal een eigen route kunnen volgen – kan hij die informatie dus ook niet verstrekken.

Artikel 18: Verstrekkingsbevel

Het eerste lid van artikel 18 verplicht de verdragsstaten tot het in het leven roepen van een bevoegdheid om te bevelen dat gespecificeerde computergegevens worden overgelegd. Gezien de plaats en samenhang van de bepaling gaat het hier om gegevens die zijn opgeslagen op een gegevensdrager die al dan niet deel uitmaakt van een computersysteem ofnetwerk. De bevolene is degene die deze gegevens in zijn bezit heeft of, zoals de verdragstekst aangeeft, tot welker toegang hij gerechtigd is. Van het eerste geval is sprake indien hij eigenaar of houder is van de desbetreffende gegevensdrager, van het tweede geval is sprake indien hij bevoegd is zich door middel van de systeemfuncties of applicatieprogrammatuur toegang tot deze gegevens te verschaffen en daar bepaalde handelingen – zoals downloaden of kopiëren – mee te verrichten. Het bestaan van een dergelijke bevoegdheid kan volgen uit de wet of uit overeenkomst. De toelichting in paragraaf 173 van het *Explanatory Memorandum* laat de mogelijkheid open dat de bevolen persoon bevoegd is met betrekking tot gegevens die niet op het grondgebied van de eigen staat zijn opgeslagen. Dit staat de verplichting tot nakoming van het bevel niet in de weg.

De verdragstekst spreekt over gespecificeerde computergegevens. Dit betekent dat het bevel dient te omschrijven welke gegevens worden verlangd. De verdragstekst geeft geen aanwijzingen voor de mate van specificiteit. Deze dient voldoende bepaald te zijn gezien het beginsel van proportionaliteit. Artikel 15 stelt de verdragsstaat overigens in de gelegenheid tot het stellen van toepassingsvoorwaarden die bijvoorbeeld worden ontleend aan de nationale wet en rechtspraak met betrekking tot overeenkomstige bevoegdheden.

Tevens wordt het onder verwijzing naar artikel 15 aan de verdragsstaten overgelaten welke opsporingsautoriteit zij met de bevoegdheid van artikel 18 bekleden. Ook hier kan worden aangesloten bij de wetgevingstraditie van de betrokken verdragsstaat.

De tekst van artikel 18 geeft niet aan in welke vorm of op welke wijze de gegevens door de bevolene moeten worden verstrekt. Het *Explanatory Memorandum* gaat ervan uit dat dit door de individuele verdragsstaat nader wordt bepaald, net zoals de termijn waarbinnen aan het bevel gehoor moet zijn gegeven. Ook wordt voorzien dat de bevolene geheimhouding kan worden opgelegd ten aanzien van het feit en de inhoud van de maatregel. Daarnaast kan de verdragsstaat bepalen dat bepaalde personen zich van de nakoming van het bevel kunnen verschonen, naar gelang hun relatie tot het onderzochte strafbare feit of tot de persoon van de verdachte, hun maatschappelijke functie of de aard van de gegevens.

Artikel 18 geeft aan dat het bevel wordt gericht tot personen of instellingen die over de benodigde computergegevens beschikken. Alleen in die gevallen is nakoming van het bevel mogelijk. Serviceproviders die onderwerp van de voorlopige maatregelen van artikel 16 en 17 waren, zullen een opvolgend bevel zoals voorzien in artikel 18 in ieder geval kunnen nakomen.

Het derde lid van artikel 18 richt zich op de verkrijging van specifieke gegevens van specifieke houders. Het gaat om serviceproviders in de zin van artikel 1, onder c, van het Verdrag en om de gegevens van hun abonnees. Aangezien deze informatie bij de serviceprovider niet altijd in elektronische vorm beschikbaar hoeft te zijn, wordt ter verduidelijking de term «abonnee-informatie» gebruikt, waarmee ook papieren of anderszins vastgelegde administraties bedoeld worden. In het algemeen betreft dit

gegevens over de woon- of verblijfplaats van de relatie, het technisch adres of nummer, de aard en eventuele locatie van de gebruikte communicatieapparatuur en de aard van de verleende communicatiedienst. Deze gegevens betreffen niet alleen de communicatiedienst maar bijvoorbeeld ook de periode van de communicatieovereenkomst. Deze abonneegegevens zijn nodig ter voorbereiding van de maatregelen zoals voorzien in de artikelen 20 en 21 (het in real-time vergaren van verkeersgegevens en het in real-time onderscheppen van inhoudelijke gegevens), maar ook ter identificatie van personen wier communicatiegegevens daarbij zijn aangetroffen. De verdragstekst strekt niet tot het opleggen van een administratieverplichting en het verifiëren van de juistheid van deze gegevens. Het *Explanatory Memorandum* benadrukt dat de bevoegdheid niet kan worden aangewend ter verkrijging van (grote delen van) de abonneeadministratie ten behoeve van analyse of datamining. Toepassing van de bevoegdheid is niet beperkt tot de gegevens betreffende de verdachte.

Artikel 19: Doorzoeking en inbeslagneming van opgeslagen computergegevens

Artikel 19 heeft ten doel het creëren van een strafvorderlijke bevoegdheid ten behoeve van het vergaren van elektronisch bewijsmateriaal. Het artikel richt zich op het onderzoek naar opgeslagen gegevens die zich op een gegevensdrager bevinden, die al dan niet onderdeel uitmaakt van een computersysteem of -netwerk. Het wordt aan de verdragsstaat overgelaten op welke wijze dit resultaat wordt bereikt, dat wil zeggen langs de weg van de traditionele bevoegdheden tot doorzoeking en inbeslagneming of door middel van deze specifieke bevoegdheid. In sommige gevallen kan worden volstaan met de inbeslagneming van gegevensdragers of van zelfstandige, eenvoudig verplaatsbare computersystemen (PC, lap top, palm computer). In andere gevallen is inbeslagneming van de apparatuur niet aangewezen, gezien de feitelijke onmogelijkheid om de gegevensdrager van de betreffende apparatuur af te zonderen of gezien het feit dat de belangen van andere gebruikers aan het buiten werking stellen van het geheel of een deel van het systeem in de weg staan. In dat laatste geval verschaft artikel 19 een zelfstandige bevoegdheid tot het onderzoeken van de inhoud van een computersysteem of – netwerk. Artikel 19 is derhalve geformuleerd als een aanvullende bevoegdheid op de klassieke zoek- en inbeslagnemingbevoegdheid. Om dit tot uitdrukking te brengen treft men in artikel 19 als centrale handelingsbegrippen aan: «doorzoeken of zich op vergelijkbare wijze toegang verschaffen tot» («to search or simarly access») onderscheidenlijk «in beslag nemen of op vergelijkbare wijze zekerstellen» («to seize or similarly secure»). Het gebruik van deze termen moet de verdragspartijen inspireren tot het aanbrengen van voorwaarden en waarborgen op een zelfde wijze als dit ten aanzien van de klassieke bevoegdheden van doorzoeking en inbeslagneming is geregeld (zie artikel 15 van het Verdrag).

Het eerste lid van artikel 19 regelt dat opsporingsautoriteiten bevoegd zijn tot het doorzoeken van een computersysteem of onderdeel daarvan en de daarin opgeslagen computergegevens en tot het doorzoeken van een opslagmedium voor computergegevens. Het betreft onderzoek van gegevens in een op een bepaalde plaats aangetroffen geautomatiseerd werk of gegevensdrager ten einde vast te kunnen stellen of deze gegevens te behoeve van de strafvordering dienen te worden veiliggesteld. Het artikel regelt niet op welke wijze de opsporingsautoriteiten zich toegang kunnen verschaffen tot een bepaalde plaats of de beschikking over een bepaalde gegevensdrager kunnen verwerven. Men mag aannemen dat de nationale wetten daartoe toereikende bevoegdheden bevatten. Met de toevoeging «op haar grondgebied» wordt tot uitdrukking gebracht dat de bevoegdheid van het eerste lid zonder toestemming van de betrokkene slechts kan

worden uitgeoefend voor zover het computersysteem, computernetwerk of gegevensdrager zich op het territorium van de opsporende staat bevindt.

Teneinde het onderzoek in geautomatiseerde werken mogelijk te maken bevat artikel 19 een aantal steunbevoegdheden. Tijdens een doorzoeking van een computersysteem is de opsporingsautoriteit bevoegd het onderzoek vanaf de plaats van onderzoek uit te breiden tot gegevens in een verbonden computersysteem indien er redenen bestaan om aan te nemen dat voor de strafvordering benodigde gegevens zich in dat systeem bevinden. Voorwaarde is dat het betrokken computersysteem of de gegevensdrager zich binnen het territorium van de onderzoekende verdragspartij bevindt («op haar grondgebied») en dat vanuit het onderzochte systeem rechtmatig toegang kan worden verkregen tot het verbonden systeem. De rechtmatigheid dient beoordeeld te worden vanuit het perspectief van de reguliere gebruiker van het oorspronkelijke systeem. Wanneer deze rechtmatig toegang heeft tot het verbonden computersysteem, is de opsporingsautoriteit bevoegd tot het doen van onderzoek in dit systeem eventueel met gebruikmaking van de toegangsmiddelen van de gebruiker. Het nationale recht bepaalt de uitvoeringsmodaliteiten en de wijze van uitvoering van een netwerkzoeking, zoals procedure, bevoegde autoriteit en de criteria die aanleiding geven tot het instellen van een netwerkdoorzoeking.[1]
Het derde lid specificeert de handelingen die met betrekking tot de aangetroffen gegevens mogen worden uitgevoerd: inbeslagneming of vergelijkbare wijze van zekerstelling. Het onderzochte computersysteem zelf mag derhalve worden gebruikt om een geheugendump of een reservekopie van de aangetroffen gegevens op een gegevensdrager te maken. Deze drager zal in de regel toebehoren aan de opsporingsorganen. Indien het een aan derden toebehorende drager betreft is deze na uploaden vatbaar voor (klassieke) inbeslagneming. De opsporingsautoriteiten zijn bevoegd tot het treffen van maatregelen ter handhaving van de integriteit van de veiliggestelde gegevens. Strafbare of inbreukmakende gegevens die in de onderzochte systemen worden aangetroffen mogen worden verwijderd of ontoegankelijk worden gemaakt (bijvoorbeeld door versleuteling). Dit laatste maakt het mogelijk de situatie later te herstellen.

De verdragstekst verzet zich niet tegen onderzoek van gegevens die pas gedurende het onderzoek in het systeem worden opgeslagen (bijvoorbeeld inkomend e-mail-verkeer). Het nationale recht regelt de toelaatbaarheid van deze zogenoemde bijvangst.

Het vierde lid voorziet in een bevoegdheid te bevelen dat personen die kennis hebben van de werking van het te onderzoeken systeem of van de aangebrachte beveiligingen tegen onbevoegde toegang tot het systeem of daarin aanwezige gegevens, de benodigde informatie verstrekken. Deze bevoegdheid kan alleen worden toegepast «voor zover in redelijkheid mogelijk», wat beperkingen kan inhouden zowel ten aanzien van de kring der personen als ten aanzien van de aard van de inspanning en de relatie met de persoon ten wiens laste het onderzoek geschiedt.[2]

De steunbevoegdheden van artikel 19 zijn thans ondergebracht in de zevende afdeling van titel IV van het tweede boek van het Wetboek van Strafvordering.

[1] Paragraaf 194 Explanatory Memorandum.
[2] Paragraaf 200 Explanatory Memorandum.

Artikelen 20 en 21: «Real-time» vergaring van verkeersgegevens en Onderschepping van inhoudelijke gegevens

De tekst van de artikelen 20 en 21 vertoont qua structuur en strekking in hoge mate overeenkomst. Zij kunnen daarom gezamenlijk worden behandeld.

De artikelen 20 en 21 verplichten tot de invoering van een bevoegdheid tot het vergaren van verkeersgegevens respectievelijk tot het onderscheppen en vastleggen van (de inhoud van) een elektronische communicatie, hetzij door de opsporingsautoriteiten zelf, hetzij door medewerking van de betrokken serviceprovider. De bedoeling van de verdragstekst is dat de opsporingsautoriteiten onder alle omstandigheden in staat zijn om toegang te verkrijgen tot de verkeersgegevens over, respectievelijk de inhoud van een specifieke elektronische communicatie. Geschiedt dit in de desbetreffende verdragsstaat door het opleggen van een medewerkingsverplichting aan serviceproviders, dan kan deze weg worden gevolgd. Indien daartoe bijvoorbeeld geen toereikend wettelijk kader aanwezig is, dan dient de opsporingsautoriteit over de bevoegdheden te beschikken om zelf toegang tot deze verkeersgegevens respectievelijk de inhoud van de specifieke elektronische communicatie te verwerven. Het wordt aan de verdragsstaten overgelaten om de verhouding tussen en de toepassingsvoorwaarden van deze beide bevoegdheden te regelen, mits een en ander maar tot een sluitend systeem leidt. Het verdrag dwingt hierbij niet tot de keuze voor een van beide bevoegdheden. Dit wordt mede tot uitdrukking gebracht door de zinsnede in beide bepalingen, dat een serviceprovider slechts gehouden is tot uitvoering van een bevel voor zover dat ligt «binnen zijn bestaande technische mogelijkheden». Dit staat er overigens niet aan in de weg dat de nationale wetgever zodanige wettelijke verplichtingen aan de serviceproviders oplegt dat voldoende technische waarborgen worden verkregen voor een effectieve uitvoering van de bevelen.

Artikel 20 betreft het in *real-time vergaren van zogenaamde verkeersgegevens. Artikel 1 sub d van het Verdrag bevat de definitie van verkeersgegevens. Het Verdrag gaat, zoals hierboven aan het slot van paragraaf 2.5 werd uiteengezet, niet uit van een stelsel waarin voor communicatiedienstverleners een wettelijke verplichting bestaat tot opslag van alle verkeersgegevens voor een bepaalde tijd. Was dat wel het geval, dan zouden de verkeersgegevens steeds ex post* van de communicatiedienstverlener kunnen worden verkregen. Het Verdrag gaat ervan uit dat beide mogelijkheden zich kunnen voordoen, nl. dat verkeersgegevens wel of niet (voor kortere of langere tijd) door de service provider worden bewaard. In het eerste geval kunnen de autoriteiten de verkeersgegevens verkrijgen door middel van een uitleveringsbevel op de voet van artikel 18 van het Verdrag, zonodig voorafgegaan door een bevriezingsbevel op de voet van artikel 16 van het Verdrag. In het tweede geval kunnen de autoriteiten de verkeersgegevens verkrijgen door een bevel aan de serviceprovider om de gegevens in *real-time* te vergaren, of door de gegevens zelf te vergaren, een en ander zoals beschreven in artikel 20 van het Verdrag.

Artikel 21 betreft het in *real-time* onderscheppen en vastleggen van de inhoud van specifieke communicatie.

De artikelen 20 en 21 bevatten niet het element «publieke dienstverlening» of «publiek netwerk». De bevoegdheden dienen dan ook tevens toepassing te vinden in besloten of private communicatienetwerken. De nationale wetgever zal de aftapbaarheid van verkeersgegevens en communicatie-inhoud daardoor niet alleen kunnen verzekeren door het opleggen van technische verplichtingen en medewerkingsverplichtingen

aan communicatiedienstverleners alleen. Door middel van welke bevoegdheid in een concreet geval verkeersgegevens worden vergaard en op welke wijze van de communicatieinhoud wordt kennisgenomen, is ter bepaling aan de verdragspartijen. Indien in een staat de grondwet niet toelaat dat beide vergaar-/onderschepmodaliteiten worden ingevoerd, kan deze staat op grond van het tweede lid een zeer beperkt voorbehoud maken.

Het derde lid voorziet in de mogelijkheid van het opleggen van een geheimhoudingsplicht aan (personeel van) de serviceprovider die de maatregel van artikel 20 of 21 heeft uitgevoerd of bij de uitvoering heeft geassisteerd.

De verdragstekst laat toe dat bij implementatie in de nationale wetgeving aan de artikelen 20 en 21 een verschillend toepassingsbereik wordt gegeven. De aanhef van artikel 21 geeft de mogelijkheid toepassing van de bevoegdheid te beperken tot de opsporing van ernstige misdrijven. Het nationale recht bepaalt vervolgens wat als een ernstig delict moet worden beschouwd, bijvoorbeeld aan de hand van een minimumstrafmaat. Artikel 20 bevat een dergelijke beperking niet. Omdat de verdragsstaten vanuit het bestaande nationale recht – waarvan de toepassing met een beroep op artikel 15 immers is toegestaan – zouden kunnen besluiten tot toepassingsbeperkingen ten aanzien van de bevoegdheid van artikel 20, geeft artikel 14 de regel dat aan de toepassing van de op grond van artikel 20 ingestelde bevoegdheden geen verdergaande beperkingen mogen worden gesteld dan aan de toepassing van bevoegdheden die op artikel 21 zijn gegrond.

Het vierde lid van de artikelen 20 en 21 verwijst steeds niet alleen naar artikel 14 maar ook naar artikel 15 en wel in verband met de bevoegdheid van de verdragsstaat nadere uitvoeringsmodaliteiten te regelen. In het Explanatory Memorandum wordt een aantal voorbeelden van zulke voorwaarden en rechtswaarborgen genoemd, mede onder verwijzing naar de belangrijkste relevante beslissingen van het EHRM.[1]
Het wettelijk stelsel in het Nederlandse Wetboek van Strafvordering en de Telecommunicatiewet gaat uit van een wettelijk afdwingbare medewerking van aanbieders van *openbare* elektronische communicatiediensten en -netwerken. De bestaande voorwaarden en waarborgen ten aanzien van dit stelsel behoeven in verband met de verdragstekst geen aanpassing. Wel dient te worden voorzien in een zelfstandige bevoegdheid van opsporingsautoriteiten tot het door mdidel van technische middelen vergaren van verkeersgegevens met betrekking tot specifieke elektronische communicaties, respectievelijk de kennisname en vastlegging van de inhoud die communicaties voor de gevallen waarin het huidige stelsel van bevoegd tappen niet voorziet, respectievelijk waarin een toekomstig stelsel van verplichte opslag van verkeersgegevens niet voorziet.

Artikel 22: Rechtsmacht

Artikel 22 betreft de rechtsmacht die de verdragspartijen dienen te vestigen ten behoeve van de delicten, bedoeld in de artikelen 2 tot en met 11 van het Verdrag. Voor zover de in het eerste lid van dat artikel uitgewerkte beginselen in het Nederlandse strafrecht (artikelen 2 tot en met 8 Sr) worden toegepast, behoeven deze hier geen nadere bespreking. Dat geldt op overeenkomstige wijze voor het derde lid in verband met de regels van de Uitleveringswet.

Nadere beschouwing verdient echter het eerste lid, onderdeel d. Daarin is neergelegd dat een Verdragspartij rechtsmacht dient te vestigen over feiten, door een van haar onderdanen begaan, indien het feit strafbaar is

[1] Paragraaf 214 Explanatory Memorandum.

onder de strafwet van de staat waar het feit is begaan of indien het feit is begaan buiten de territoriale rechtsmacht van enige staat.

De rechtsmacht van staten strekt zich krachtens het internationale recht niet uit tot plaatsen of ruimten die wij met de vrije zee of de vrije ruimte kunnen aanduiden. Het Verdrag houdt er evenwel rekening mee dat de plegers van genoemde delicten zich aan de rechtsmacht van staten kunnen onttrekken door zich al dan niet vergezeld van de geautomatiseerde middelen waarmee de delicten worden begaan, op deze vrije zee of in deze vrije ruimte op te houden.

Artikel 5 Sr geeft voor Nederland een beperkte toepassing aan de in onderdeel d geregelde rechtsmacht, namelijk (1e) indien het gaat om feiten die een «loyale Nederlander» niet behoort te begaan, (2e) indien het feit tevens strafbaar is volgens het recht van de staat op welk territorium de Nederlander het feit begaat of (3e) indien het gaat om kinderporno en ernstige zedendelicten jegens een minderjarige. Met betrekking tot artikel 240b Sr voldoet de Nederlandse strafwet op dit punt dus aan beide delen van onderdeel d van artikel 22 van het Verdrag. Wat betreft de andere in het Verdrag gedefinieerde computerdelicten voorziet onze strafwet nog niet in rechtsmacht. Gelet op de doelstelling van het Verdrag is het niettemin wenselijk dat zoveel mogelijk wordt aangesloten bij het in het Verdrag gekozen stelsel van toedeling van nationale rechtsmacht. Daarbij is van belang dat deze aansluiting kan worden bereikt met een geringe aanpassing van artikel 5 Sr, daar deze strikt kan worden beperkt tot de feiten zoals benoemd in het Cybercrime Verdrag. De noodzakelijke aanvulling van artikel 5 Sr zal worden opgenomen in het Wetsvoorstel computercriminaliteit-II (26 671), door middel van een nota van wijziging.

Tenslotte verdient het vijfde lid van artikel 22 nog toelichting. Dit artikellid is opgenomen in de verwachting dat toepassing van de leer van de locus delicti door verdragspartijen op strafbare gedragingen die worden begaan in of met behulp van een internationaal communicatienetwerk zoals het internet, kan leiden tot rechtsmachtcumulatie. Het vijfde lid nodigt de verdragspartijen uit in die gevallen door middel van een consultatieprocedure te komen tot bepaling van het meest gerede forum. Partijen worden geacht in die procedure hun belangen en daarmee samenhangende argumenten uit te wisselen teneinde tot een gezamenlijk besluit te komen. Deze consultatie kan er bijvoorbeeld ook toe leiden dat verdragspartijen besluiten om bepaalde verdachten in de ene verdragsstaat en andere verdachten in de andere verdragsstaat te vervolgen. Verwezen zij ook naar paragraaf 239 van de *Explanatory Memorandum*.

Artikel 23: Algemene beginselen met betrekking tot internationale samenwerking

Artikel 23 geeft het algemene kader voor de wijze waarop rechtshulp moet worden verleend. De samenwerking – op basis van de bepalingen van dit Verdrag, op basis van andere internationale instrumenten en vooral op basis van nationale wetten – dient zo breed mogelijk te geschieden voor het doel van die samenwerking, dat wil zeggen ten behoeve van procedures en opsporingsonderzoeken inzake de misdrijven met betrekking tot computersystemen en computergegevens – wat zowel de misdrijven van de artikelen 2 tot en met 11 omvat als de misdrijven waarbij ICT gebruikt wordt als hulpmiddel – en inzake de misdrijven voor de opsporing waarvan bewijs in elektronische vorm nodig is. Uiteraard stemt de opsomming van artikel 23 overeen met die van artikel 14. Artikel 23 noopt niet tot aanpassing van de Nederlandse wet.

Artikel 24: Uitlevering

Uitlevering is onderdeel van de internationale rechtshulp. Artikel 24 regelt in het eerste lid de uitlevering van verdachten van strafbare feiten, zoals in hoofdstuk II van het Verdrag gedefinieerd. De minimumeis is een strafbedreiging van ten minste 1 jaar. Indien de verdragspartijen in een tussen hen van kracht zijnd ander uitleveringsverdrag een andere strafmaat hanteren, geldt deze in plaats van de in het Cybercrime Verdrag genoemde strafmaat. Binnen de Europese Unie is vooral het kaderbesluit van de Raad van de Europese Unie betreffende het Europees aanhoudingsbevel en de procedures van overleveringg tussen de lidstaten van de Europese Unie van 13 juni 2002 (2002/584/JBZ) (Pb EG L 190) bepalend, waarbij is voorzien in een categorie *cybercrimes.*
Het tweede lid van artikel 24 bevat een soort internationaal kettingbeding: de verdragspartijen zijn verplicht om de misdrijven van het Cybercrime Verdrag als uitleverbare delicten op te nemen in elke andere uitleveringsovereenkomst die zij met een van de verdragspartijen zullen sluiten.

Het derde lid biedt de mogelijkheid om het Cybercrime Verdrag als basis voor uitlevering te gebruiken, indien geen ander instrument tussen partijen van kracht is of indien de bestaande verdragen de misdrijven van het Verdrag (nog) niet omvatten.

Indien partijen geen verdrag behoeven om uit te leveren, verplicht het vierde lid ertoe de delicten van hoofdstuk II van het Verdrag als uitleverbare delicten aan te merken.

Het vijfde lid verwijst naar bepalingen van het nationale recht, in het bijzonder in verband met toepasselijke weigeringsgronden.

Het zesde lid werkt het beginsel «dedere aut judicare» uit indien de nationale wetgeving van een verdragspartij de uitlevering van eigen onderdanen uitlevert: als gij niet uitlevert, zult gij zelf berechten, en omgekeerd.

Artikel 24 noopt niet tot aanpassing van de Nederlandse wet.

Artikel 25: Algemene beginselen met betrekking tot wederzijdse bijstand

Artikel 25 vormt de inleiding op de overige bepalingen van rechtshulp en noopt als zodanig niet tot aanpassing van de Nederlandse wet. In de tekst van het artikel wordt nogmaals de intentie tot uitdrukking gebracht dat het verdrag beoogt dat de verdragspartijen elkaar op ruimhartige wijze van rechtshulp voorzien. De maatregelen van de artikelen 27 tot en met 35 die partijen in hun nationale wetgeving dienen om te zetten, scheppen daartoe mede de mogelijkheid. De ruimhartige samenwerking hoeft zich echter niet tot deze maatregelen te beperken.

Het derde lid maakt het mogelijk dat de verdragspartijen moderne communicatietechnieken gebruiken om elkaar rechtshulpverzoeken te doen. De gebruikelijke praktijk is dat rechtshulpverzoeken schriftelijk worden gedaan en ter uitvoering ook schriftelijk aan de betrokken opsporingsautoriteiten worden doorgegeven. Het Verdrag geeft in voorkomende gevallen prioriteit aan snelheid, door gebruik van al dan niet beveiligde fax en e-mail toe te staan, indien gewenst eventueel gevolgd door een schriftelijke bevestiging. Per e-mail ontvangen rechtshulpverzoeken mogen niet worden geweigerd vanwege het gebruikte communicatiemiddel. De beantwoording van een via deze communicatiemiddelen gedaan verzoek dient in beginsel met dezelfde middelen te geschieden.

Zoals in de aanhef aangegeven, worden rechtshulpverzoeken in beginsel uitgevoerd op basis van het nationale recht van de aangezochte Partij. Dat nationale recht kan beperkingen inhouden met betrekking tot de wijze waarop een verzoek kan worden uitgevoerd of moet worden geweigerd. Het vierde lid sluit ten aanzien van de delicten van het Verdrag in ieder geval toepassing van de zogenoemde *fiscal offence-exceptie uit.*

Het vijfde lid geeft aan dat de aanwezigheid van dubbele strafbaarheid niet moet worden beoordeeld op basis van de formele delictsomschrijving of categorisering van het delict, maar uitsluitend op basis van de eventuele strafbaarheid van het onderliggende gedrag naar de nationale wet.

Artikel 26: Informatieverstrekking op eigen initiatief

Artikel 26 is ontleend aan artikel 10 van het Verdrag inzake het witwassen, de opsporing en de confiscatie van opbrengsten van misdrijven (Trb. 1990, 172). Een dergelijke bepaling komt eveneens voor in artikel 28 van het Verdrag inzake de strafrechtelijke bestrijding van corruptie (Trb. 2000, 130). Door plaatsing van een soortgelijke bepaling in het Cybercrime Verdrag alsmede door opname in het Tweede Additionele Protocol bij het Europees Verdrag aangaande de wederzijdse rechtshulp in strafzaken (Trb. 2002, 30) worden de toepassingsmogelijkheden van deze bevoegdheid verder verbreed. Verdragspartijen zijn bevoegd elkaar uit eigen beweging informatie te verstrekken die verkregen is in het kader van een strafrechtelijk onderzoek, waarvan zij vinden dat de autorititeiten van een ander land daarvan op de hoogte dienen te zijn. Dit kan leiden tot het starten van een opsporingsonderzoek in de andere staat of tot het doen van een rechtshulpverzoek, maar het kan ook juist tot het tegendeel leiden, namelijk dat de geïnformeerde staat afziet van (verdere) stappen in de wetenschap dat de informerende staat reeds actie onderneemt of heeft ondernomen. Uiteraard mag de informatieverstrekking afhankelijk worden gemaakt van een geheimhoudingsplicht of specifieke gebruiksvoorwaarden. De ontvangende staat is hieraan gebonden. Indien wetgeving of andere factoren aan de zijde van de ontvangende partij naleving van die verplichtingen zouden verhinderen, dient dit te worden gemeld. De verstrekkende partij heeft dan de mogelijkheid de voorwaarden aan te passen of, na afweging van de nadelige gevolgen van het niet verstrekken tegen de nadelen van het niet nakomen van de beperkingen, alsnog te verstrekken.

Artikel 26 noopt niet tot aanpassing van de Nederlandse wet.

Artikelen 27 en 28

De artikelen 27 en 28 van het Verdrag zijn bedoeld voor situaties waarin twee individuele verdragspartijen voor het verlenen van rechtshulp geen beroep kunnen doen op een ander instrument dat tussen hen van kracht is dan het Cybercrime Verdrag zelf. Deze situatie zal zich niet snel voordoen maar is niet geheel denkbeeldig. Niet alle lidstaten van de Raad van Europa hebben het op 20 april 1959 te Straatsburg totstandgekomen Europees Verdrag aangaande de wederzijdse rechtshulp in strafzaken (Trb. 1965, 10) geratificeerd, terwijl dit aan ondertekening en ratificatie van het Cybercrime Verdrag niet in de weg staat. Evenmin zijn alle lidstaten van de Raad van Europa voorzien van bilaterale rechtshulpverdragen met de verdragspartijen die geen lid van de Raad van Europa zijn. Een vergelijkbare situatie kan zich voordoen bij toekomstige toetreding van een verdragspartij die geen lid is van de Raad van Europa. Het kan niet worden uitgesloten dat rechtshulpverlening door of aan Nederland op de bepalingen van titel 4 wordt gegrond, reden waarom een korte bespreking is aangewezen.

De artikelen 27 en 28 vinden op de voet van de eerste volzin van het eerste lid toepassing indien er tussen betrokken partijen geen toepasselijke regeling is. Maar de tweede volzin van het eerste lid van beide artikelen maakt duidelijk dat de artikelen in onderling overleg ook toegepast kunnen worden als er wel een toepasselijke regeling is. Daartoe kan bijvoorbeeld aanleiding bestaan indien deze artikelen meer en betere mogelijkheden voor internationale samenwerking bieden dan het bestaande rechtshulpverdrag.

Artikel 27

Artikel 27, eerste lid, noemt als basis voor rechtshulpverlening het bestaan van een verdrag inzake wederzijdse bijstand of een regeling op basis van zogenaamde uniforme of wederkerige wetgeving. Deze laatste figuur komt met name voor tussen de Scandinavische landen. Nederland bedient zich op dit gebied van verdragen.
Artikel 27, tweede lid, voorziet in de aanwijzing van een centrale autoriteit voor de afhandeling van rechtshulpverzoeken. Uiterlijk bij de ratificatie van het Verdrag dienen de verdragspartijen aan de Secretaris-generaal van de Raad van Europa op te geven welke instantie in het kader van artikel 27 als centrale autoriteit is aangewezen. De Secretaris-generaal houdt van de opgaven van de verschillende verdragspartijen een centraal register bij. De verdragsstaat ziet erop toe dat de gegevens in het register met de actualiteit blijven overeenstemmen (tweede lid, onderdeel d). Voor Nederland zal als centrale autoriteit in het kader van artikel 27 optreden het daarvoor in aanmerking komende dienstonderdeel van het Ministerie van Justitie.
Het derde lid van artikel 27 brengt tot uitdrukking dat een rechtshulpverzoek volgens de door de verzoekende staat aangegeven procedures wordt uitgevoerd, tenzij de nationale wetgeving – op basis waarvan het rechtshulpverzoek immers, gelet op artikel 25, vierde lid, eerste volzin, van het Verdrag, wordt uitgevoerd – zich daarmee niet zou verdragen. De centrale autoriteit stelt de verzoekende staat van een afwijkende uitvoering van het rechtshulpverzoek op de hoogte; zie ook het zevende lid van artikel 27.
Artikel 25, vierde lid, van het Verdrag verwijst naar mogelijke gronden voor weigering van een rechtshulpverzoek. Het vierde lid van artikel 27 voorziet daarnaast in de mogelijkheid om een verzoek om rechtshulp nog op een aantal andere gronden te weigeren. De reden hiervoor is dat aan partijen die niet over een rechtshulpverdrag beschikken, minder vergaande verplichtingen tot samenwerking kunnen worden opgelegd dan aan partijen die hun betrekkingen in dit opzicht wel hebben geregeld. Als aanvullende weigeringsgronden worden aangemerkt het feit dat de rechtshulp wordt gevraagd met betrekking tot een zogenaamd politiek misdrijf (letter a) en de in de internationale rechtspraktijk als standaardformulering bekende aantasting van soevereiniteit, (nationale) veiligheid, openbare orde of andere wezenlijke belangen (letter b).
Het vijfde lid van artikel 27 geeft aan dat de uitvoering van een rechtshulpverzoek kan worden opgeschort indien de uitvoering ervan schade zou toebrengen aan een eigen strafrechtelijk onderzoek of vervolging. Het zesde lid verplicht de aangezochte staat in die situatie met de verzoekende staat te overleggen of, in welke mate of onder welke voorwaarden alsnog aan het verzoek kan worden voldaan.
Het zevende lid van artikel 27 regelt de informatieverplichting van de aangezochte staat met betrekking tot de uitvoering van het rechtshulpverzoek. In alle gevallen dient de verzoekende staat onverwijld te worden geïnformeerd over het resultaat van de uitvoering van het verzoek. Dat geldt evenzeer indien de aangezochte staat zich op een weigeringsgrond beroept (bijvoorbeeld op grond van het vierde lid) of de uitvoering van het verzoek opschort of uitstelt (bijvoorbeeld op grond van het zesde lid) dan

wel het verzoek niet heeft kunnen uitvoeren (bijvoorbeeld op de voet van het derde lid, maar ook vanwege andere, feitelijke redenen) of indien uitvoering van het verzoek naar verwachting aanzienlijke vertraging zal ondervinden. De toelichting moet met redenen worden omkleed.

Het achtste lid opent de mogelijkheid dat de verzoekende staat de aangezochte staat verzoekt om geheimhouding van het feit dat een rechtshulpverzoek is gedaan en van het onderwerp dat het betreft. Een dergelijke geheimhouding kan gewenst zijn ter bescherming van andere of verbonden strafrechtelijke opsporingsonderzoeken in de verzoekende staat. Indien geheimhouding niet mogelijk is, dient de aangezochte staat dat onverwijld ter kennis te brengen van de verzoekende staat, waarna deze kan besluiten het rechtshulpverzoek in te trekken of alsnog te laten uitvoeren.

Het negende lid van artikel 27 kan worden toegepast bij dringende aangelegenheden. Wat een dringende aangelegenheid is, is in het *Explanatory Memorandum* niet nader toegelicht. Uit de verdere tekst van het artikellid kan men in ieder geval afleiden dat een dringende aangelegenheid aan de orde is indien met het volgen van de gebruikelijke procedure via de centrale autoriteiten zodanig veel tijd gemoeid zou zijn dat uitvoering van het rechtshulpverzoek weinig tot geen resultaat oplevert of dat de gewenste resultaten niet tijdig beschikbaar zijn om voortzetting van de opsporing door de verzoekende staat mogelijk te maken. In zodanige gevallen, ter bepaling door de verzoekende staat, kunnen rechtshulpverzoeken rechtstreeks in handen worden gesteld van de voor uitvoering verantwoordelijke juridische autoriteiten, onder verzending van een afschrift van het verzoek aan de betrokken centrale autoriteit (letter a). Onder het Nederlandse internationale strafrecht is de officier van justitie de verantwoordelijke juridische autoriteit. Mocht de ontvangende autoriteit niet bevoegd zijn tot uitvoering van het rechtshulpverzoek – zowel in geval van absolute als van relatieve incompetentie – is hij verplicht het rechtshulpverzoek door te zenden aan de wel bevoegde instantie onder berichtgeving daarvan aan de verzoekende staat (letter c). In Nederland komt dit alleen voor bij verrichtingen die tot de bevoegdheid van de rechter-commissaris behoren (zie de artikelen 552n e.v. Sv). Tevens is voorzien dat verzoeken om rechtshulp of andere communicaties verlopen door middel van Interpol (letter b). Wanneer het rechtshulpverzoek niet de uitvoering van dwangmiddelen impliceert kan het verzoek of de communicatie rechtstreeks geschieden tussen de betrokken autoriteiten – lees: politiediensten – van de verdragspartijen (letter d). In afwijking van het bovenstaande is iedere verdragspartij bevoegd om bij ondertekening, of ten laatste bij ratificatie, aan te geven dat zij alle rechtshulpverzoeken uitsluitend tot haar centrale autoriteit kunnen worden gericht. Dit kan volgens de verdragstekst worden gedaan «om redenen van doelmatigheid», wat betekent dat het inschakelen van de centrale autoriteit in de betreffende staat inderdaad de meest efficiënte manier is om de uitvoering ervan te bewerkstelligen. Nederland zal van deze mogelijkheid geen gebruik maken.

Artikel 28

Artikel 28 van het Verdrag richt zich, gelet op de formulering in het eerste lid, op dezelfde situaties die in het eerste lid van artikel 27 worden genoemd. Het artikel geeft de aangezochte staat de mogelijkheid een zekere controle uit te oefenen over het elektronische bewijsmateriaal dat aan de verzoekende staat wordt verstrekt. In een dergelijke mogelijkheid is niet voorzien in de artikelen 23 tot en met 26 van het Verdrag. Eventuele waarborgen ten aanzien van de betrokken personen dienen te worden ontleend aan de van kracht zijnde algemene rechtshulpinstrumenten

tussen de betrokken verdragspartijen. Bij toepassing van artikel 27 is er in beginsel geen instrument van kracht waaraan dergelijke waarborgen kunnen worden ontleend, zodat een zelfstandige regeling nodig is. De tekst van artikel 28 van het Verdrag is overigens ontleend aan artikel 25 van het Tweede Additionele Protocol bij het Europees Verdrag aangaande de wederzijdse rechtshulp in strafzaken (Trb. 2002, 30), zodat de regeling ook langs die weg toepassing kan vinden.

Het tweede lid van artikel 28 staat de aangezochte staat toe voorwaarden te verbinden aan het verstrekken van informatie en materiaal ter uitvoering van een rechtshulpverzoek. Onder informatie en materiaal worden de informatie en de informatiedragers verstaan, papier en elektronische informatiedragers daaronder begrepen. In verband met de inhoud en de strekking van het Cybercrime Verdrag dient hier vooral te worden gedacht aan elektronisch bewijsmateriaal dat in veel gevallen zal bestaan uit gegevens die als persoonsgegevens kunnen worden aangemerkt. De aangezochte staat kan ter bescherming van dergelijke persoonsgegevens twee typen voorwaarden stellen.
– Verlangd kan worden dat de informatie of het materiaal door de ontvangende autoriteiten vertrouwelijk wordt behandeld, maar dan alleen als het onderliggende rechtshulpverzoek zonder deze voorwaarde niet zou kunnen worden uitgevoerd (letter a). Dat kan bijvoorbeeld het geval zijn indien het materiaal informatie zou verschaffen over de identiteit van een informant. De verplichting tot vertrouwelijkheid moet hier niet in absolute zin worden gelezen. Het voornaamste doel is het bereiken van een zorgvuldige omgang en het tegengaan van een ruime verspreiding. De gestelde voorwaarde is niet bedoeld om de verzoekende te verhinderen het materiaal (uiteindelijk) als bewijs aan de rechter voor te leggen.
– Als tweede voorwaarde kan worden bepaald dat de informatie of het materiaal alleen mag worden gebruikt voor het doel – lees de strafzaak – waarvoor de rechtshulp is gevraagd. Zonder dat deze voorwaarde is gesteld is de verzoekende verdragspartij vrij in het gebruik van de informatie of het materiaal. Gebruik van de informatie of het materiaal in een andere strafzaak is dan alleen mogelijk indien de aangezochte verdragspartij daartoe toestemming verleent. Ook deze gebruiksbeperking dient niet te absoluut te worden uitgelegd. Wanneer het materiaal door de verzoekende staat eenmaal in een strafdossier is opgenomen, komt deze informatie mede ter beschikking van anderen en daarmee in het publieke domein.

Het derde lid van artikel 28 verplicht de verzoekende staat die aan deze voorwaarden niet kan voldoen om dit onverwijld ter kennis van de aangezochte staat te brengen, waarna deze kan besluiten de informatie of het materiaal al dan niet te verstrekken.
Het vierde lid geeft de verstrekkende verdragspartij, die verstrekking aan een of meer voorwaarden heeft verbonden, de bevoegdheid in het licht van de gestelde voorwaarden naar het gebruik van de informatie of het materiaal door de ontvangende staat te informeren, terwijl de ontvangende staat verplicht is tot het geven van een toelichting. De aangezochte verdragsstaat wordt niet geacht van de verzoekende partij de invoering van een protocolplicht met betrekking tot het gebruik van het materiaal te verlangen.

Artikelen 29 tot en met 34

De artikelen 29 tot en met 34 van het Verdrag vormen de internationale equivalent van de daarmee overeenkomende bepalingen in titel 2 van afdeling 2 van hoofdstuk II van het Verdrag. Titel 1 van deze afdeling richt zich op de zogenaamde voorlopige maatregelen, titel 2 op het onderzoek

van computersystemen en titel 3 op de inrichting van het zogenaamde 24/7 contactpunt.

- De artikelen 29 en 30 betreffen de voorlopige maatregelen en vormen daarmee het equivalent van de artikelen 16 en 17.
- Artikel 31 betreft het doorzoeken en in beslag nemen van gegevens en vormt daarmee het equivalent van artikel 19.
- Artikel 32 betreft de grensoverschrijdende toegang tot opgeslagen computergegevens met toestemming of indien deze publiekelijk toegankelijk zijn; zie de toelichting hieronder.
- De artikelen 33 en 34 betreffen het real-time vergaren van verkeersgegevens en het onderschappen van inhoudelijke gegevens en vormen daarmee het equivalent van de artikelen 20 en 21.

Artikelen 29 en 30

Artikel 29 verwijst naar de bevoegdheid van artikel 16 onder toevoeging van toepassingsvoorwaarden en procedurele voorschriften. Het eerste lid stelt nog eens duidelijk dat een spoedbewaring van specifieke gegevens alleen zinvol is, indien de verzoekende partij voornemens is een rechtshulpverzoek ter toepassing van artikel 18 of 19 te doen. Met deze laatste verzoeken kan ter afhandeling van formaliteiten een zodanige hoeveelheid tijd gemoeid zijn dat de gevraagde gegevens niet meer beschikbaar zijn. Een verzoek om toepassing van een laagdrempelig bevriezingsbevel kan de nodige tijdsruimte scheppen ter voorbereiding van een rechtshulpverzoek ter uitvoering van artikel 18 of 19. De bewaring van de bevroren gegevens (zie het zevende lid) dient door de nationale wet te worden gegarandeerd voor een periode van minimaal 60 dagen, te verlengen met zoveel dagen als nodig is voor de afhandeling van een opvolgend rechtshulpverzoek ter toepassing van artikel 18 of 19. Is de verzoekende partij niet in staat om een opvolgend rechtshulpverzoek binnen de gegeven termijn in te dienen, dan komt de bewaringsplicht van de houder te vervallen, zoals te regelen bij implementatie van artikel 16. De in dat artikel genoemde termijnen worden geacht voldoende te zijn om tevens de afhandeling van rechtshulpverzoeken mogelijk te maken.
Het tweede lid somt de informatie op die door de verzoekende Staat moet worden verschaft. Deze informatie is niet alleen van belang voor de communicatie maar kan voor de aangezochte Staat van belang zijn voor een effectieve uitvoering van het verzoek. De verzoekende Staat dient tevens aan te geven welke maatregel hij overweegt teneinde daadwerkelijk de beschikking over de bevroren gegevens te verkrijgen.
Uitvoering van een bevriezingsbevel kan slechts worden geweigerd in de gevallen voorzien in de leden 3 tot en met 6. Gezien de aard en de bedoeling van de maatregel bepaalt het derde lid dat de aangezochte Staat in beginsel niet de voorwaarde van dubbele strafbaarheid mag stellen. De reden hiervoor is dat zo weinig mogelijk tijd verloren mag gaan tussen het doen van een verzoek en de uitvoering daarvan. Ook met het onderzoek naar het bestaan van dubbele strafbaarheid kan tijd verloren gaan, niet in de laatste plaats indien het bestaan ervan voor de aangezochte staat niet aanstonds uit de inhoud van het verzoek zou blijken. Deze voorwaarde van dubbele strafbaarheid kan daarentegen wel aan de orde komen bij een verzoek om toepassing van artikel 18 of 19. Indien de aangezochte Staat van mening is dat wegens het ontbreken van dubbele strafbaarheid een komend rechtshulpverzoek om toepassing van artikel 18 of 19 moet worden geweigerd, kan het nu reeds weigeren om het bevriezingsbevel uit te voeren, tenzij het gaat om een van de delicten als omschreven in de artikelen 2 tot en met 11 van het Verdrag. Het vijfde lid laat weigering van uitvoering van een bevel daarbuiten slechts toe in geval van een zogenaamd politiek delict of bij mogelijke aantasting van soevereiniteit, (nationale) veiligheid, openbare orde of andere wezenlijke belangen.

De verzoekende Staat doet geen zelfstandig verzoek voor toepassing van artikel 17. De tekst van artikel 29 strekt tevens tot uitvoering van de in artikel 17 voorziene procedure met betrekking tot een specifieke elektronische communicatie die door middel van de computersystemen op het grondgebied van de aangezochte Staat heeft plaatsgevonden.

Artikel 30 legt aan de aangezochte Staat nog de verplichting op om de verzoekende Staat mededeling te doen van de identiteit van de buitenlandse provider die in de communicatieketen was betrokken, zodat eventueel een derde Staat voor rechtshulp kan worden benaderd. Verstrekking van die informatie kan alleen worden geweigerd met een beroep op de gronden genoemd in het tweede lid, die gelijkluidend zijn aan die van artikel 29, vijfde lid.

Artikel 31

Artikel 31 betreft de wederzijdse bijstand met betrekking tot de toegang tot opgeslagen computergegevens en verwijst daarmee inhoudelijk naar artikel 19. Het tweede lid scherpt nog eens in dat het verzoek om rechtshulp moet worden uitgevoerd in de geest van artikel 23 van het Verdrag en met inachtneming van eventueel andere instrumenten. Het derde lid bepaalt dat aan een verzoek ten spoedigste moet worden voldaan indien aan de daar bedoelde voorwaarden wordt voldaan.

Artikel 32

Artikel 32, dat ook gelezen moet worden in samenhang met de specifieke onderzoeksbevoegdheden van het Verdrag, geeft aan voor welke beperkte gevallen grensoverschrijdende zelfhulp is toegestaan zonder dat de betrokken verdragspartij zich daartegen kan verzetten (zie ook paragraaf 292 van het Explanatory Memorandum).

Onderdeel a spreekt van toegang tot zogenaamde open bron («open source») gegevens. Indien bepaalde elektronische informatie door middel van een computersysteem dat zich op het grondgebied van een andere verdragspartij bevindt, aan het publiek wordt aangeboden (bijvoorbeeld gegevens op een bepaalde web-site), dan zijn de opsporingsautoriteiten van andere verdragspartijen bevoegd om zich toegang tot die gegevens te verschaffen en een kopie daarvan te *downloaden* zonder dat daarvoor toestemming wordt verkregen van de verdragspartij op wiens grondgebied het computersysteem zich bevindt.

Onderdeel b komt er kort gezegd op neer dat geen toestemming van de andere verdragspartij nodig is indien computergegevens naar het territoir van een andere verdragspartij worden overgehaald met toestemming van de persoon die met betrekking tot die gegevens handelingsbevoegd is. De plaats waar deze persoon zich hierbij bevindt is irrelevant: hij kan zich op het grondgebied van een van beide verdragspartijen bevinden of zelfs in een derde staat, zolang hij maar bevoegd is tot verstrekking. Deze bevoegdheid kan hij ontlenen aan de wet, aan een overeenkomst of aan zijn relatie met de gegevens. In alle andere situaties zal de opsporende Staat zijn toevlucht moeten nemen tot het vragen van rechtshulp.

Artikelen 33 en 34

De artikelen 33 en 34 verwijzen naar de bevoegdheden van de artikelen 20 en 21. Het Verdrag stelt hier geen nadere eisen of voorwaarden aan de verzoeken om rechtshulp en aan de uitvoering ervan door de aangezochte Staat. Vanwege de gevoeligheid van deze maatregelen laat het Verdrag dit aan de nationale wetgever over. Het tweede lid van artikel 33 stelt dat de

maatregel van het in real-time vergaren van verkeersgegevens tenminste ter opsporing van dezelfde delicten moet openstaan als ten behoeve van het binnenlands gebruik. Deze voorwaarde wordt niet gesteld ten aanzien van het onderschappen en vastleggen van (de inhoud van) elektronische communicatie, zoals geregeld in artikel 21 waarnaar artikel 34 inhoudelijk verwijst.

Artikel 35

Artikel 35 betreft het zogenaamde 24/7 netwerk. Iedere Verdragspartij dient ervoor te zorgen dat er op alle zeven dagen van de week gedurende de volle 24 uur een contactpunt beschikbaar is dat in staat is de onmiddellijke bijstand te (doen) verzekeren die nodig kan zijn voor onderzoek of vervolging van strafbare feiten. Dit contactpunt dient ten behoeve van de opsporingsorganen van de andere verdragspartijen permanent bereikbaar te zijn. Het artikel omschrijft de taken die aan dit contactpunt zijn toebedacht. Het contactpunt is bedoeld ter vergemakkelijking van eventuele rechtshulp. Een verdragsstaat die overweegt om een verzoek om rechtshulp te doen kan bij het contactpunt inwinnen over de wijze waarop dit het beste en het snelste kan geschieden en of een dergelijk verzoek onder de wetgeving van de aan te zoeken staat kan worden aangewend. Het contactpunt is verder bedoeld om in contact te treden met andere nationale autoriteiten teneinde de prompte afhandeling van inkomende rechtshulpverzoeken te bevorderen en daarbij coördinerend op te treden. Om deze taken naar behoren te kunnen uitvoeren is het contactpunt voorzien van moderne communicatiemiddelen. Het contactpunt is niet bedoeld als substituut voor de centrale autoriteit. In Nederland zal een 24/7 contactpunt naar verwachting worden ondergebracht bij het Korps landelijke politiediensten, onder gezag van het openbaar ministerie. Aangezien het 24/7-contactpunt zelf geen opsporingshandelingen verricht behoeft de instelling ervan geen wettelijke regeling.

Artikel 36

Het eerste lid bepaalt dat ondertekening van het Verdrag openstaat voor de leden van de Raad van Europa. Dit sluit zowel de tegenwoordige als toekomstige leden in. Tot ondertekening van het Verdrag zijn tevens bevoegd de niet-lidstaten die aan de onderhandelingen deelnamen. Dit zijn Canada, Japan, de Verenigde Staten van Amerika en Zuid-Afrika, welke landen het Verdrag op 23 november 2001 te Boedapest hebben ondertekend. Andere Staten die tot het Verdrag wensen toe te treden zullen de weg van artikel 37 dienen te volgen.
Het derde lid bepaalt dat het Verdrag in werking treedt op de eerste dag van de maand die volgt na het verstrijken van een periode van drie maanden na het tijdstip waarop vijf Partijen het Verdrag hebben geratificeerd, aanvaard of goedgekeurd volgens de procedure van het tweede lid. Van deze vijf Partijen dienen tenminste drie lid van de Raad van Europa te zijn. Inmiddels is aan deze voorwaarde voldaan; het Verdrag is met ingang van 1 juli 2004 in werking getreden.

Artikel 37

Artikel 37 regelt in het eerste lid de toetreding van nieuwe Verdragspartijen na de inwerkintreding van het Verdrag. Het comité van Ministers is bevoegd tot het uitnodigen van Partijen om toe te treden. Hiermee wordt gedoeld op niet-lidstaten van de Raad van Europa. Voor toetreding is een meerderheidsbesluit nodig van het Comité van Ministers zoals beschreven in het Statuut van de Raad van Europa, én een unaniem besluit van de vertegenwoordigers van de Verdragspartijen die in het Comité van Ministers vertegenwoordigd zijn. Gebruik is in dergelijke

situaties om de vertegenwoordigers van niet-lidstaten voor die gelegenheid uit te nodigen zitting te nemen in het Comité van Ministers.

Artikel 40

In de verdragstekst is op diverse plaatsen de mogelijkheid geopend tot het afleggen van verklaringen. Een verklaring kan nodig zijn om een verdragspartij in staat te stellen een bepaling in het nationale recht te implementeren, rekening houdende met in het nationale recht geïncorporeerde beginselen of begrippen. Een verklaring kan leiden tot modaliteiten in de werking van de betreffende bepaling en dient daarom door neerlegging ter kennis van de overige verdragspartijen te worden gebracht. De tekst van artikel 40 verwijst naar de bepalingen van het Verdrag waarin de mogelijkheid van een verklaring is voorzien. Nederland maakt van deze mogelijkheid geen gebruik.

Artikel 41

Dit artikel bevat een in algemene termen gestelde voorziening die in de context van dit Verdrag nodig was voor de Verenigde Staten van Amerika. Onder de Amerikaanse constitutie is een individuele lidstaat bij uitsluiting bevoegd tot het vaststellen van eigen wetgeving behoudens op de terreinen die aan de federale wetgever zijn voorbehouden, zoals die inzake het interstatelijk economisch verkeer of het verkeer met het buitenland. Dit betekent dat aan de Amerikaanse constitutie geen juridische bevoegdheden kunnen worden ontleend om de individuele Amerikaanse (deel)staten te verplichten tot het aannemen van wetgeving ter implementatie van het bepaalde in hoofdstuk II van het verdrag. Artikel 41 opent de mogelijkheid om voorbehouden te maken doch beperkt deze tegelijkertijd in belangrijke mate. Het eerste lid van artikel 41 stelt dat eventuele voorbehouden geen invloed mogen hebben op het verlenen van rechtshulp zoals geregeld in hoofdstuk III van het verdrag. Het tweede lid beoogt de omvang van eventuele voorbehouden te beperken. Aan het maken van voorbehouden is tevens de inspanningsverplichting gekoppeld (zie het derde lid van artikel 41) om de desbetreffende lidstaten tot een verdragsconforme opstelling te bewegen.

Aangezien computercriminaliteit in de zin van het Verdrag vrijwel in alle gevallen een interstatelijk of internationaal karakter heeft, mag worden aangenomen dat de effecten ervan voor de internationale samenwerking op strafrechtelijk gebied verwaarloosbaar zijn. Vrijwel alle Amerikaanse Staten beschikken sinds lange tijd over uitgebreide wetgeving op het gebied van computercriminaliteit. De Verenigde Staten dienen bij ratificatie van het Verdrag te specificeren in welke mate deze lokale wetgeving niet aan hoofdstuk II van het Verdrag voldoet.

Artikel 42

In de tekst van een aantal bepalingen is voorzien in de mogelijkheid dat een verdragspartij een voorbehoud maakt ten aanzien van bepaalde verplichtingen. In totaal is dit op negen plaatsen mogelijk. Dit relatieve hoge aantal was nodig om tegemoet te komen aan de verdragspartijen voor wie de materie van het Verdrag als betrekkelijk nieuw moest worden aangemerkt. Andere verdragspartijen achten zich niet in staat tot implementatie van delen van het Verdrag wegens uit het nationale recht voortvloeiende bezwaren van fundamentele aard. Artikel 42 specificeert op welke plaatsen van het Verdrag de mogelijkheid van een voorbehoud is voorzien. Het Koninkrijk maakt, zoals in de toelichting op het desbetreffende artikel is uiteengezet, een voorbehoud ten aanzien van artikel 22, tweede lid. Andere voorbehouden zijn voor het Koninkrijk niet nodig.

Artikel 44

Tijdens de onderhandelingen is voorzien dat nieuwe ontwikkelingen van de informatie- en communicatietechnologie dringende aanleiding kunnen vormen tot aanvulling of wijziging van de verdragstekst. Daarom is voorzien in een flexibele, laagdrempelige procedure met de mogelijkheid van initiatief bij de individuele verdragspartijen. Iedere verdragspartij is op grond van artikel 44, eerste lid, bevoegd tot het doen van wijzigingsvoorstellen. De CDPC van de Raad van Europa adviseert het Comité van Ministers over het wijzigingsvoorstel. Het Comité van Ministers consulteert de betrokken ministers van de verdragspartijen die geen lid zijn van de Raad van Europa, en besluit tot al dan niet aanname van het wijzigingsvoorstel. Indien het voorstel wordt aangenomen wordt het aan de betrokken partijen toegezonden die de Secretaris-generaal vervolgens dienen te berichten dat zij het voorstel aanvaarden. Deze procedure stelt Partijen in de gelegenheid het voorstel ter goedkeuring voor te leggen aan het nationale parlement. Het wijzigingsvoorstel wordt van kracht dertig dagen nadat alle partijen hun instemming aan de Secretaris-generaal hebben kenbaar gemaakt.

Artikel 44 sluit niet uit dat de CDPC of het Comité van Ministers ter voorbereiding van de besluitvorming een of meer deskundigencommissies benoemen. De procedure van artikel 44 is bedoeld voor ondergeschikte wijzigingen of aanpassingen van de verdragstekst. In geval van substantiële wijziging of aanvulling is de weg van een Aanvullend Protocol voorzien. Zie het Eerste Additionele Protocol bij het Cybercrime Verdrag inzake racistische en xenophobe uitingen (Trb. 2003, 60).

Artikel 45

Artikel 45, eerste lid, bepaalt dat de CDPC door betrokken Partijen geïnformeerd dient te worden over de uitleg en toepassing van de verdragstekst. Daartoe kan aanleiding bestaan indien tussen Partijen discussie ontstaat over de betekenis van de verdragstekst. De CDPC dient ervan op de hoogte te zijn, hoe de verdragstekst in de praktijk wordt toegepast. Het tweede lid ziet op de situatie dat Partijen niet tot een gezamenlijke uitleg van de verdragstekst kunnen geraken. Het Verdrag voorziet niet in de oprichting van een onafhankelijk orgaan dat Partijen geschillen over de uitleg van de verdragstekst beslecht. Partijen worden uitgenodigd om een mogelijk geschil in goed overleg te regelen. Partijen zijn bevoegd hun geschil voor te leggen aan de CDPC, onverminderd hun bevoegdheid tot het aangaan van internationale arbitrage of inschakeling van het Internationale Gerechtshof te Den Haag.

Artikel 46

Artikel 46 nodigt de verdragspartijen uit, periodiek te beraadslagen over de inhoud van het verdrag, de wijze waarop de bepalingen van het Verdrag in nationale wetgeving zijn omgezet, de toepassing en de betekenis van het Verdrag in de praktijk, met als doel de inventarisatie van eventuele problemen en mogelijk daaruit voortvloeiende behoefte tot aanpassing of aanvulling van de verdragstekst. De CDPC heeft hierbij krachtens het derde lid een beperkte, namelijk een faciliterende en ondersteunende rol. Wel rust op de CDPC de verplichting om in samenwerking met de verdragspartijen de gehele verdragstekst te onderwerpen aan een evaluatie, drie jaar na de inwerkintreding van het Verdrag. Dat moment zal zich op zijn vroegst voordoen in de loop van 2007. De CDPC is bevoegd tot

het doen van wijzigingsvoorstellen. Ook individuele Partijen zijn daartoe bevoegd op grond van artikel 44.

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

De Minister van Buitenlandse Zaken,
B. R. Bot