Het Cyber-crimeverdrag, de Nederlandse strafwetgeving en de (computer)criminalisering van de maatschappij

Koops, E.J.

Published in:
Computerrecht

Publication date:
2003

Koops, B.J. (2003). Het Cyber-crimeverdrag, de Nederlandse strafwetgeving en de (computer)criminalisering van de maatschappij. Verschenen in *Computerrecht, 02*, 115-123

Het Cybercrime-verdrag, de Nederlandse strafwetgeving en de (computer)criminalisering van de maatschappij

Bert-Jaap Koops[1]

Op 23 november 2001 ondertekende Nederland in Boedapest het Cybercrime-verdrag van de Raad van Europa.[2] *Het verdrag is een unieke poging om mondiaal de wetgeving op het gebied van computercriminaliteit te "approximeren". Hoewel Nederland, met name op het vlak van formeel strafrecht, een internationale voortrekkersrol heeft gespeeld, biedt het verdrag ook voor Nederland nog diverse punten om de nationale wetgeving aan te passen. Bovendien is de Nederlandse wetgever uit zichzelf al druk doende met wijziging van de wetgeving rond computercriminaliteit. Alle reden dus voor een inventarisatie van de wetgeving die Nederland te wachten staat in het kader van de bestrijding van computercriminaliteit.*

In dit artikel geef ik een overzicht van aanhangige en te verwachten wetgeving, na kort de wetsgeschiedenis tot nu toe in het geheugen te hebben geroepen. Aan de hand van de bepalingen uit het Cybercrime-verdrag (hierna ook: CCV) loop ik de Nederlandse initiatieven na, eerst de materieelrechtelijke bepalingen, en dan de formeelrechtelijke. Op de derde pijler van het verdrag – rechtsmacht en rechtshulp – ga ik niet in. Ik behandel zowel de aanpassingen waartoe het Cybercrime-verdrag noopt, als wijzigingen die de Nederlandse wetgever uit zichzelf heeft voorgenomen.

1. De Nederlandse wetgeving tot nu toe

Om het geheugen op te frissen, zij vooraf nog even gewezen op de Nederlandse wetsgeschiedenis tot nu toe.[3] In 1985 stelde de minister van justitie de Commissie Computercriminaliteit in (de eerste Commissie-Franken). Het resulterende rapport *Informatietechniek en strafrecht* uit 1987 leidde na de nodige discussie in 1990 tot een wetsvoorstel, dat eind 1992 werd aangenomen. Op 1 maart 1993 trad de Wet

---

[1] Dr. Bert-Jaap Koops is universitair hoofddocent ICT-recht bij het Centrum voor Recht, Bestuur en Informatisering van de Universiteit van Tilburg.

[2] Verdrag inzake de bestrijding van strafbare feiten verbonden met eleketronische netwerken, Trb. 2002, 18. Op <http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm> vindt men de tekst van het verdrag, het toelichtend rapport en een ratificatieoverzicht. Een uitvoerige bespreking van het verdrag biedt Kaspersen 2002.

[3] Zie uitgebreid Van Dijk & Keltjens 1995.

computercriminaliteit in werking.[4] De meeste bepalingen uit die wet zijn sindsdien niet meer (of nog niet) aangepast.
De wetgever vond al snel dat vanwege de stormachtige technische ontwikkelingen een vervolg nodig was; daartoe werd in juli 1999 een wetsvoorstel Computercriminaliteit II bij de Tweede Kamer ingediend, dat naast herstel van schoonheidsfoutjes uit de eerste wet diverse nieuwe bepalingen voorstelde, waarvan ik de belangrijkste hieronder zal behandelen.[5] De behandeling van het wetsvoorstel heeft grote vertraging opgelopen; na intrekking van het gedeelte over aansprakelijkheid van tussenpersonen (waaronder Internetaanbieders), stelde de Tweede Kamer in september 2000 in het Verslag een berg vragen die nog altijd[6] op antwoord wachten. De verwachting is dat de regering het wetsvoorstel Computercriminaliteit II zal aangrijpen om de aanpassingen die het Cybercrime-verdrag eist door te voeren, hetgeen een substantiële aanvulling op het wetsvoorstel zou betekenen, dat vermoedelijk ook advies van de Raad van State behoeft. Het zal dus nog een tijd duren voor dit wetgevingstraject wordt afgerond.[7]
Wel is de wetgeving intussen door de wet BOB[8] uitgebreid met diverse opsporingsbevoegdheden die voor de bestrijding van computercriminaliteit van belang kunnen zijn, zoals direct afluisteren (art. 126l/s Sv) en infiltratie (art. 126h/p Sv). Ook heeft de wet Herziening gerechtelijk vooronderzoek[9] op ondergeschikte punten geleid tot aanpassing in verband met de doorzoeking.

2. Materieel strafrecht

2.1. BVD-delicten

De eerste groep delicten van het Cybercrime-verdrag betreft misdrijven tegen de beschikbaarheid, deugdelijkheid (integriteit en authenticiteit) of vertrouwelijkheid van computersystemen en gegevens (aan te duiden als "BVD-delicten"). Op één belangrijk punt na (zie par. 2.2), brengt dit voor Nederland weinig nieuws. De Nederlandse bepalingen over computervredebreuk (art. 138a Sr; de beveiligingseis van dit artikel is toegestaan volgens art. 2 CCV), onderscheppen van gegevens (art. 139a-c Sr), gegevensmanipulatie (art. 350a-b Sr) en computersabotage (art. 161sexies-septies en 351-351bis Sr) voldoen grotendeels aan de eisen van het verdrag.
Op één punt kan men voor aanpassing pleiten: onder art. 5 CCV (computersabotage) vallen blijkens de memorie van toelichting ook verstikkingsaanvallen (*denial-of-service attacks*), terwijl deze niet altijd strafbaar zijn naar huidig Nederlands recht. De

---

[4] Stb. 1993, 33.
[5] TK 1998-1999, 26 671, nrs. 1-3. Zie voor een bespreking Koops & Schellekens 1999.
[6] Althans bij afronding van dit artikel, op 20 januari 2003.
[7] Waar ik in 1999 nog vermocht te verwachten dat rond 2005 het wetsvoorstel Computercriminaliteit III zou worden ingediend (Koops & Schellekens 1999, p. 1770), durf ik nu slechts te hopen dat tegen die tijd de wet Computercriminaliteit II in werking zal zijn getreden.
[8] Stb. 1999, 245.
[9] Stb. 1999, 243.

computersabotagebepalingen zien immers slechts op gemeengevaarlijke delicten (art. 161sexies-septies Sr) of op computers voor het algemene nut (art. 351-35bis Sr); van computervredebreuk (art. 138a Sr) is bij een verstikkingsaanval niet per se sprake, aangezien niet noodzakelijk wordt binnengedrongen in een computer. Daarom is bijvoorbeeld een verstikkingsaanval op de webstek van een e-handelbedrijf naar huidig recht niet altijd strafbaar. Nu wordt in Computercriminaliteit II een nieuwe strafbepaling voorgesteld voor e-bommen (voorgesteld art. 138b Sr), maar dat betreft alleen het via telecommunicatie toesturen van gegevens aan iemand "om *diens* toegang tot dat netwerk of die dienst te belemmeren" (mijn cursivering). Verstikkingsaanvallen beogen echter niet zozeer om de toegang van het slachtoffer zelf tot het netwerk te verhinderen, maar om de toegang van potentiële klanten tot de dienst van het slachtoffer te belemmeren. Het valt dus te overwegen om het voorgestelde art. 138b Sr uit te breiden met verstikkingsaanvallen, bijvoorbeeld door "diens toegang tot dat netwerk of die dienst" te vervangen door "de toegang tot een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst".
Ook een ander instrument noopt tot het strafbaarstellen van verstikkingsaanvallen: artikel 4 van het ontwerp-Kaderbesluit over aanvallen op informatiesystemen[10] bepaalt dat het ernstig hinderen of onderbreken van de werking van een informatiesysteem strafbaar moet zijn. Ook zal de bepaling over computervredebreuk aangepast moeten worden indien dit Kaderbesluit wordt aangenomen, want artikel 3 daarvan stelt ook strafbaar het binnendringen in *onbeveiligde* systemen met het oogmerk iemand schade te berokkenen of met het oogmerk economisch voordeel te bewerkstelligen. Bovendien noemt het ontwerp-Kaderbesluit als strafverzwarende omstandigheid "indien door het strafbare feit aanzienlijke opbrengsten werden verkregen", waarop een maximumstraf van ten minste vier jaar gevangenis zou moeten staan. Dat zou dan eveneens moeten worden ingevoegd in de Nederlandse wet.

Een andere wijziging die mij wenselijk lijkt is evenmin ingegeven door het Cybercrime-verdrag, maar door een inconsistentie in de Nederlandse wet zelf. Op diverse punten loopt de strafbaarstelling van het onderscheppen van directe communicatie of gegevensoverdracht (art. 139a-b Sr) uit de pas met de bevoegdheid tot direct afluisteren (art. 126l/s Sv), terwijl dit eigenlijk grotendeels spiegelbepalingen zouden moeten zijn. Discrepanties zijn onder andere niet-vertrouwelijke gesprekken of gegevensoverdracht en niet-communicatieve gegevensoverdracht: het afluisteren daarvan is wel strafbaar, maar valt niet onder de bevoegdheid van direct afluisteren. Het ligt voor de hand het eerste te schrappen uit de strafbaarstelling (niet-vertrouwelijke communicatie afluisteren is immers geen privacyinbreuk), maar het andere zou onder de bevoegdheid van direct afluisteren moeten worden gebracht. Nu kan justitie bijvoorbeeld met richtmicrofoons de beeldschermstraling van een schoot-pc aftappen op basis van de veel lichtere

[10] Voorstel voor een Kaderbesluit van de Raad over aanvallen op informatiesystemen, COM/2002/173def, *Pb* 27 augustus 2002, C203E/109, beschikbaar via <http://recht.nl/7687>.

bevoegdheid tot observatie (mits zij kan verwachten dat de schoot-pc geen communicatie zal verwerken, hetgeen vaak het geval zal zijn). Dit lijkt mij een even ingrijpende inbreuk als het aftappen van communicatie (en het wordt in art. 139a-b Sr dan ook daarmee op één lijn gesteld), en daarom zou dit onder art. 126l/s Sv moeten worden gebracht.[11] Een ander punt is het opnemen van communicatie door een communicatiedeelnemer; dat is niet strafbaar, maar valt wel onder de bevoegdheid tot direct afluisteren, omdat de wetgever het inmiddels wel als privacyinbreuk beschouwt (in tegenstelling tot 1971, toen art. 139a-b werd ingevoerd). Het gewijzigde privacyinzicht zou moeten leiden tot het schrappen van de uitsluiting voor communicatiedeelnemers in art. 139a-b Sr.

2.2. 'Misbruik van hulpmiddelen'

Veel ingrijpender dan het voorgaande is evenwel art. 6 CCV, dat misbruik van hulpmiddelen strafbaar stelt (de term uit het verdrag, 'devices', omvat zowel apparatuur als programmatuur; ik gebruik daarom de term 'hulpmiddel' in plaats van de gebruikelijker vertaling 'apparaat'). Volgens het verdrag moeten tal van, kort gezegd, voorbereidingshandelingen strafbaar worden gesteld die worden gepleegd met het doel om een van de voorgaande delicten te plegen. Het gaat om bijvoorbeeld het ontwikkelen, verspreiden of voorhanden hebben van apparatuur of programmatuur voor hacken, virusverspreiding of gegevensonderschepping. Ook het voorhanden hebben van wachtwoorden of toegangscodes waarmee toegang tot een computer(systeem) kan worden verkregen, is strafbaar als men van plan is om daarmee bijvoorbeeld computervredebreuk te plegen.[12] Bij voorhanden hebben mag de strafbaarstelling zich beperken tot het bezit van meerdere exemplaren. Een lidstaat heeft de mogelijkheid om een voorbehoud te maken bij dit artikel, maar zij moet in elk geval wel de verkoop, verspreiding en het beschikbaarstellen van 'te misbruiken hulpmiddelen' strafbaar stellen. Dit is bepaald een vérgaande strafbaarstelling, ondanks de inkleding met opzet- en wederrechtelijkheidseisen en de toevoeging dat het bevoegd testen of beschermen van een computersysteem is toegestaan. Voor Nederland betekent het een ingrijpende uitbreiding van het materiële strafrecht, zelfs als Nederland een voorbehoud zou maken bij de ratificatie. Tot nu toe heeft Nederland het strafbare 'misbruik van hulpmiddelen'

---

[11] De redenering dat het afluisteren van een (niet-communicatieve) schoot-pc zo ingrijpend is dat de wetgever het niet heeft willen toestaan, noch bij direct afluisteren noch bij observatie, valt niet te lezen in de BOB-wetsgeschiedenis. De wetgever heeft bij de observatiebevoegdheid alleen communicatie uitgesloten, maar niet non-communicatieve gegevensoverdracht, zodat mijns inziens het afluisteren van een (stand-alone) schoot-pc op basis van art. 126g/o Sv is toegestaan.

[12] De volledige tekst luidt: 'a. the production, sale, procurement for use, import, distribution or otherwise making available of: i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Article 2 – 5; ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with intent that it be used for the purpose of committing any of the offences established in Articles 2 - 5; and b. the possession of an item referred to in paragraphs (a)(1) or (2) above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 – 5.'

beperkt tot apparatuur voor het kraken van telecomdiensten (waarmee iemand zonder te betalen gebruik kan maken van bijvoorbeeld betaal-tv of telefonie) (art. 326c lid 2 Sr), middelen voor het omzeilen van technische beveiliging van computerprogrammatuur (art. 32a Auteurswet) en het reclame maken voor afluisterapparatuur (art. 441a Sr). Het Cybercrime-verdrag dwingt Nederland om een veel algemener strafbepaling op te nemen over allerlei handelingen met hulpmiddelen indien iemand beoogt daarmee een computerdelict te plegen.

Art. 6 CCV weerspiegelt een tendens die mij zorgen baart. De EG-richtlijn Auteursrecht in de informatiemaatschappij[13] bevat een soortgelijke bepaling (ook art. 6) over omzeiling van technische bescherming van auteursrechtelijk beschermde werken. De Nederlandse wetgever kiest voor implementatie hiervan in het civiele recht en – vooralsnog – niet in het strafrecht, maar gaat wel bekijken hoe dit zich verhoudt tot de strafrechtelijke normering in het kader van art. 6 Cybercrime-verdrag.[14] De (internationale) tendens is duidelijk. Naast het bestrijden van onrechtmatige handelingen zelf, richten de pijlen zich steeds meer ook op voorbereidingshandelingen. Hier kunnen legitieme redenen van handhaafbaarheid en symboolwerking aan ten grondslag liggen, maar de wetgever begeeft zich hiermee wel op een hellend vlak. Waar art. 32a Auteurswet zich nog beperkt tot hulpmiddelen die *uitsluitend* bestemd zijn voor de te bestrijden onrechtmatigheden, richten de genoemde artikelen 6 zich op hulpmiddelen die *hoofdzakelijk* gebruikt (kunnen) worden voor onrechtmatigheden. Zo maakt het voorgestelde art. 29a Auteurswet omzeilingsmaatregelen en -handelingen onrechtmatig die 'slechts een commercieel *beperkt* doel of nut hebben anders dan het omzeilen' of die '*vooral* ontworpen, vervaardigd of aangepast worden met het doel het omzeilen' (mijn cursivering).[15] Daarmee vervaagt de grens tussen rechtmatigheid en onrechtmatigheid, want het is best mogelijk dat iemand een hulpmiddel wil gebruiken voor rechtmatige toepassingen – het feit dat cd-branders in de praktijk hoofdzakelijk worden gebruikt voor het illegaal copiëren van auteursrechtelijk beschermde liedjes wil nog niet zeggen dat een cd-brander zelf een onrechtmatigheidsstempel moet krijgen.

Veel zal afhangen van de uitwerking die de opzeteis in de praktijk zal krijgen: hoe bewijs je dat iemand iets met een hulpmiddel doet met het oogmerk om een computerdelict te plegen? Hopelijk zullen OM en rechterlijke macht hier grote terughoudendheid betrachten. En zolang de gevolgen van uitgebreide criminalisering van technische voorbereidingshandelingen onvoldoende bekend en overdacht zijn, acht ik het wenselijk dat Nederland in elk geval een voorbehoud maakt voor het ontwikkelen en voorhanden hebben van hulpmiddelen.

---

[13] Richtlijn 2001/29/EG van 22 mei 2001, *PbEG* 22 juni 2001, L 167/10.
[14] TK 2001-2002, 28 482, nr. 3, p. 27.
[15] TK 2001-2002, 28 482, nrs. 1-2, p. 8.

2.3. Valsheid, fraude en uitingsdelicten

De titel over valsheid (art. 7 CCV) en fraude (art. 8 CCV) heeft geen gevolgen voor het Nederlandse strafrecht; de bestaande, traditionele bepalingen voldoen ook in een netwerkomgeving. Op het gebied van uitingsdelicten heeft het verdrag echter wel iets nieuws voor Nederland gebracht: de bepaling over kinderpornografie. Het verdrag omvat namelijk ook virtuele kinderpornografie: realistische afbeeldingen die een minderjarige weergeven in pornografische handelingen. Voorheen hanteerde Nederland het argument dat kinderpornografie alleen strafwaardig is als daarbij daadwerkelijk kinderen zijn misbruikt; in het buitenland acht men echter vaak ook fictieve (maar realistische) kinderporno strafwaardig, bijvoorbeeld omdat het zou kunnen aanzetten tot misbruik van kinderen. Hoewel Nederland een voorbehoud had kunnen maken op dit punt, heeft de wetgever ervoor gekozen om ook virtuele kinderpornografie strafbaar te stellen. In de wet partiële wijziging zedelijkheidswetgeving is art. 240b Sr daartoe aangepast. Nederland heeft daarbij ook de ondergrens van 16 jaar verhoogd naar 18 jaar, de norm die het verdrag hanteert.[16] In dit geval stelt een verdragsbepaling voor online situaties dus ook de norm voor offline situaties, want nu zijn ook fysieke pornografische foto's van 17-jarigen in Nederland strafbaar.
Inmiddels is een aanvullend protocol bij het verdrag gereed dat het uitingsdelict van racisme en xenofobie met behulp van computernetwerken strafbaar stelt.[17] Nederland zal dit protocol ongetwijfeld ondertekenen.

2.4. Overige materieelrechtelijke onderwerpen

Art. 10 CCV draagt de lidstaten op om inbreuken op het auteursrecht en de naburige rechten (volgens de Berner Conventie, het Verdrag van Rome, het TRIPs-verdrag en de WIPO-verdragen uit 1996) strafbaar te stellen voorzover de inbreuken moedwillig ('wilfully', een beperktere term dan opzettelijk of 'intentionally'), op commerciële schaal en met behulp van een computer(systeem) plaatsvinden. Een lidstaat kan echter ook voor een grotendeels niet-strafrechtelijke handhaving kiezen, mits deze maar effectief is en is toegestaan onder de genoemde verdragen. Nederland implementeert de vereiste vernieuwingen in het wetsvoorstel Uitvoering richtlijn auteursrecht en naburige rechten in de informatiemaatschappij (de richtlijn die de WIPO-verdragen vertaalt naar EG-recht).[18]
Artikelen 11-12 van het verdrag bieden vervolgens nog enkele bepalingen over poging, strafbare deelnemingsvormen en aansprakelijkheid van rechtspersonen, die in Nederland reeds geldend recht zijn. Art. 13 geeft een ruime keuzemogelijkheid voor de bepaling van sancties voor de computerdelicten uit het verdrag.

---

[16] Stb. 2002, 388.
[17] Zie <http://www.coe.int/T/E/Communication_and_Research/Press/Theme_Files/Cybercrime/Index.asp>.
[18] TK 2001-2002, 28 482, nrs. 1-3.

Hoewel het verdrag een hoop regelt, zijn er ook diverse onderwerpen die niet in het verdrag worden behandeld, bijvoorbeeld omdat er geen overeenstemming over bestond of omdat gedragingen onvoldoende strafwaardig werden geacht. Te denken valt aan het aanbieden van illegale goederen of diensten op het Internet, (het gebruik van) anonimiseringsdiensten en ongevraagde commerciële berichten (spam). Evenmin is de aansprakelijkheid van Internetaanbieders geregeld.[19] Voor de laatste twee onderwerpen zal Nederland de wetgeving wel dienen aan te passen vanwege EG-richtlijnen: voor spam moet een opt-inregime komen, aldus de Richtlijn Privacy en elektronische communicatie,[20] en Internetaanbieders moeten volgens de Richtlijn Elektronische handel[21] onder voorwaarden uitsluiting van aansprakelijkheid krijgen. Dit laatste geldt ook voor de strafrechtelijke aansprakelijkheid: de wetgever heeft voorgesteld om na art. 53-54 Sr (de drukpersdelicten) een nieuw art. 54a op te nemen met een vervolgingsuitsluitingsgrond voor een aanbieder van telecomdiensten voor de doorgifte of opslag van gegevens, mits deze op bevel van de officier van justitie de gewraakte gegevens ontoegankelijk maakt. De officier heeft voor een dergelijk bevel machtiging van de r-c nodig.[22]

Voor de volledigheid zij nog gewezen op de overige voorstellen uit het wetsvoorstel Computercriminaliteit II. Naast de reeds genoemde strafbaarstelling van e-bommen (voorgesteld art. 138b Sr), wordt een strafbaarstelling voorgesteld van kennisneming door telecomaanbieders van netpost- of stempostberichten die niet voor hen zijn bestemd (voorgesteld art. 273d Sr, art. 374bis-oud). De bepaling over vervalste betaalpassen (art. 232 Sr) wordt uitgebreid met het vervalsen van andere voor het publiek beschikbare kaarten bestemd voor betalingen of voor andere elektronische dienstverlening.[23]

3. Formeel strafrecht

Het tweede gedeelte van het verdrag bevat bepalingen over formeel strafrecht, die zien op het onderzoek van computers en computergegevens, en het onderzoek van telecommunicatie. De reikwijdte daarvan is niet beperkt tot de computerdelicten: art. 14 CCV geeft aan dat de bevoegdheden ook toepasbaar moeten zijn bij andere delicten gepleegd met behulp van een computer en bij delicten waarbij elektronisch bewijs van belang kan zijn. Dat is geen verrassing voor de Nederlandse wetgever, aangezien die dezelfde benadering hanteert.

---

[19] Zie Kaspersen 2002, p. 18-21, voor de redenen waarom deze onderwerpen niet zijn opgenomen.
[20] Art. 13 Richtlijn 2002/58/EG, *PubEG* 31 juli 2002, L 201/37.
[21] Richtlijn 2000/31/EG van 8 juni 2000*, PubEG* 17 juli 2000, L 178.
[22] TK 2001-2001, 28 197, nrs. 1-3. (Het eerdere voorstel voor aansprakelijkheid van tussenpersonen in het wetsvoorstel Computercriminaliteit II is ingetrokken, TK 1999-2000, 26 671, nr. 5.)
[23] Zie hierover Koops & Schellekens 1999, p. 1767-1769.

3.1. Bevriezing van gegevens

Het verdrag opent het formele gedeelte met een voor Nederland nieuw fenomeen. Om te voorkomen dat de opsporing hinder ondervindt van de vluchtigheid van elektronische gegevens, hetgeen met name in een internationale context nogal eens kan voorkomen, wordt een steunmaatregel ingevoerd om de veiligstelling of 'bevriezing' ('preservation') van gegevens te bevelen (art. 16 CCV). Als er aanwijzingen zijn dat gegevens bijzonder kwetsbaar zijn voor verlies of wijziging, kan justitie bevelen dat deze voor een (verlengbare) periode van maximaal 90 dagen worden bewaard in de oorspronkelijke vorm. Aansluitend kan justitie dan maatregelen nemen om de gegevens op de gewenste manier te verkrijgen, bijvoorbeeld nadat een officieel rechtshulpverzoek tot 'uitlevering' van de gegevens is binnengekomen. Voor verkeersgegevens gelden daarbij nog aanvullende eisen: de veiliggestelde verkeersgegevens moeten beschikbaar zijn onafhankelijk van het aantal dienstaanbieders die de communicatie hebben vervoerd, en bovendien moeten onverwijld aan justitie voldoende verkeersgegvens doorgegeven kunnen worden opdat die het gevolgde of te volgen pad van de communicatie verder kan traceren (art. 17 CCV). De bedoeling is dat deze maatregelen laagdrempelig kunnen worden getroffen, zonder veel voorwaarden; het gaat immers nog niet om de kennisneming van de gegevens door justitie, maar alleen om het verzekeren van de mogelijkheid dat justitie – op basis van een andere bevoegdheid – er later kennis van kan nemen.

Nederland kent tot nu toe een dergelijk bevriezingsbevel niet en zal dat dus moeten invoeren. Een aanzet daartoe is reeds gegeven door de Commissie-Mevis, die voorstellen heeft gedaan voor strafvorderlijke gegevensvergaring in de informatiemaatschappij.[24] Het voorgestelde art. 126nh biedt de hulpofficier van justitie de bevoegdheid te vorderen dat gegevens gedurende twee weken toegankelijk blijven. Het voorstel bevat wel een belangrijke inperking voor de categorie misdrijven: bevriezing zou alleen mogen worden bevolen bij voorlopigehechtenismisdrijven (grofweg: misdrijven met een maximum van ten minste vier jaren gevangenisstraf) die een ernstige inbreuk op de rechtsorde opleveren; bovendien moet het onderzoek het bevel dringend vorderen. De Commissie heeft kennis van de langere termijn uit het (toen nog concept-)Cybercrime-verdrag, maar vindt twee weken voldoende in de Nederlandse context.[25] Het kabinet, dat het overigens eens is met het voorstel, acht zich echter gebonden aan de termijn van 90 dagen uit het verdrag.[26] Volgens mij kan men de bepaling uit het verdrag ook anders lezen: de termijn van 90 dagen is een maximumtermijn, maar indien een kortere termijn volstaat in het licht van de snelheid van de nationale procedures ("a period of time as long as necessary") is dat ook toegestaan. Ik zou daarom liever een kortere bevriezingsperiode zien, desnoods met een verlengingsmogelijkheid tot een totaal van 90 dagen.

---

[24] Commissie-Mevis 2001.
[25] Commissie-Mevis 2001, p. 71.
[26] TK 2001-2001, 28 366, nr. 1, p. 22.

De eis van dringendheid is ingegeven door de doelafwijkende verwerking van de te bevriezen gegevens waar het bevel toe noodzaakt; de eis van ernstige inbreuk op de rechtsorde wordt niet gemotiveerd door de Commissie, maar het kabinet geeft aan dat terughoudendheid gewenst is door de lasten voor het bedrijfsleven en de bijzondere inspanning die veelal zal worden gevraagd. Het kabinet wil de bevoegdheid doen toekomen aan de officier van justitie en niet aan de hulpofficier (mede vanwege de langere bevriezingstermijn). Door al deze eisen lijkt de voorgestelde bevoegdheid beperkter te zijn dan de bedoeling is van het Cybercrime-verdrag; een bevriezingsbevel zal onder deze voorwaarden immers niet in alle gevallen kunnen worden gegeven waarin behoefte bestaat aan bepaalde gegevens. Toch is de terughoudendheid van de Commissie-Mevis en het kabinet op dit punt op haar plaats. Het gaat immers om een instrumentalisering van maatschappelijke processen ten behoeve van de strafvordering: gegevens die normaliter zouden worden vernietigd moeten voor justitie bewaard worden, hetgeen ook lasten met zich meebrengt voor de geadresseerde. Daarom zijn de eisen van ernstige misdrijven en dringendheid passend, ook al gaat het wellicht in tegen de geest van het Cybercrime-verdrag.

Het bevriezingsbevel moet overigens worden onderscheiden van het ontoegankelijkmakingsbevel uit het wetsvoorstel Computercriminaliteit II (voorgesteld art. 125o Sv, zie par. 3.3).

3.2. Opvragen van gegevens

Art. 18 CCV bevat de bevoegdheid tot een ‘uitleveringsbevel’ voor computergegevens, alsmede voor de bevoegdheid om gebruikersgegevens bij telecomaanbieders op te vragen. Nederland kent sinds de wet Computercriminaliteit art. 125i Sv, dat de mogelijkheid biedt aan de rechter-commissaris om tijdens een gerechtelijk vooronderzoek (gvo) toegangsverschaffing tot gegevens te bevelen. In theorie is dit voldoende om aan het Cybercrime-verdrag te voldoen, maar de eisen zijn dermate zwaar (zeker nu sinds de wet Herziening gvo uit 2000 in veel minder gevallen een gvo wordt geopend) dat de bevoegdheid in de huidige context te beperkt is. Art. 125i Sv wordt weinig toegepast, en voor het opvragen van gebruikersgegevens moet justitie meestal toevlucht nemen tot een verzoek op basis van art. 8 onder e j^{o} art. 43 Wet bescherming persoonsgegevens (Wbp), waarbij de geadresseerde zelf een afweging moet maken of het belang van de strafvordering opweegt tegen het belang van persoonsgegevensbescherming van de betrokkene. Dat is geen handige constructie als het gaat om strafvordering. Nederland is dus toe aan actualisering van het ‘uitleveringsbevel’ voor gegevens, en de wetgever heeft daartoe twee sporen uitgezet.
Het eerste spoor is het instellen van de reeds genoemde Commissie-Mevis, die in mei 2001 voorstellen heeft gedaan voor onder andere het uitleveringsbevel. De voorstellen van de commissie zijn uitgebreid, en ik kan in dit bestek slechts ingaan op de belangrijkste voorstellen. Onder afschaffing van het huidige art. 125i Sv, zouden volgens

de commissie bevoegdheden moeten worden ingevoerd om, in volgorde van oplopende zwaarte, identificerende, 'andere' en gevoelige gegevens te kunnen opvragen (respectievelijk voorgesteld art. 126nc, 126nd en 126nf Sv). 'Andere' gegevens zijn gegevens die niet identificerend of gevoelig zijn; gevoelige gegevens zijn de gegevens genoemd in art. 16 Wbp en de inhoud van netpost of stempost bij een telecomaanbieder. Ook zouden toekomstige 'andere' gegevens moeten kunnen worden opgevraagd, hetgeen wil zeggen dat iemand na het bevel binnenkomende gegevens moet doorsluizen aan justitie (voorgesteld art. 126ne Sv).
De belangrijkste voorgestelde bevoegdheid is het opvragen van 'andere' gegevens. Deze bevoegdheid zou toekomen aan de officier van justitie bij voorlopigehechtenismisdrijven;[27] bij lichtere strafbare feiten is de vordering ook mogelijk, maar dan heeft de officier voorafgaande machtiging van de rechter-commissaris nodig. Toekomstige gegevens kunnen worden opgevraagd onder dezelfde voorwaarden, voor een (verlengbare) periode van vier weken; in dringende gevallen kan, met toestemming van de r-c, worden gevorderd dat binnenkomende gegevens 'direct na verwerking' (zeg maar *real-time*) of binnen een bepaalde periode worden verstrekt. Voor opvragen van gevoelige gegevens is altijd machtiging van de r-c nodig, en dit kan alleen bij voorlopigehechtenismisdrijven die een ernstige inbreuk op de rechtsorde vormen en indien het onderzoek dit dringend vordert. Identificerende gegevens zouden daarentegen bij elk strafbaar feit door elke opsporingsambtenaar kunnen worden gevorderd. Naast het opvragen van bestaande gegevens, kan ook worden gevraagd om gegegens te bewerken (door datadelven of registervergelijking), bij zware misdrijven, in dringende gevallen en met machtiging van de r-c. Al deze bevoegdheden worden, naast de traditionele opsporing van gepleegde strafbare feiten, ook steeds voorgesteld in het kader van beraamde georganiseerde misdaad (titel V van het Eerste Boek Sv).
Al deze vorderingen kunnen, naar analogie met bestaande medewerkingsplichten, niet worden gericht aan de verdachte, en verschoningsrechten zijn steeds van toepassing. Een belangrijk uitgangspunt, dat bekritiseerd is door diverse instanties,[28] is dat alle bevoegdheden ook kunnen worden toegepast bij niet-verdachten, al zou het proportionaliteitsbeginsel tot meer terughoudendheid moeten nopen wanneer gegevens van niet-verdachten worden opgevraagd. Hiermee verkrijgen de bevoegdheden een potentieel zeer grote reikwijdte.
Het kabinet is het grotendeels eens met de voorstellen.[29] Wel legt het kabinet een beperking aan bij het bevel tot verstrekking van identificerende gegevens: dit bevel kan alleen worden gegeven in de beroepsmatige sfeer (aan rechtspersonen en aan natuurlijke personen in de uitoefening van een beroep of bedrijf); dit geldt ook voor het bevel voor toekomstige gegevens. Bovendien wordt de bevoegdheid bij identificerende gegevens

[27] Preciezer: bij misdrijven als omschreven in art. 67 lid 1 Sv; ik hanteer gemakshalve de term 'voorlopigehechtenismisdrijven'.
[28] Zie TK 2001-2001, 28 366, nr. 1, p. 12.
[29] Zie het kabinetsstandpunt van 1 mei 2002, TK 2001-2001, 28 366, nr. 1.

beperkt tot misdrijven (waar de commissie ook van overtredingen uitging). De bevoegdheid tot bewerken heeft de instemming van het kabinet, zij het dat volgens hem de bewerking niet door de houder maar door opsporingsambtenaren moet worden uitgevoerd; deze bevoegdheid wordt in een apart wetsvoorstel ondergebracht.[30]

Het tweede spoor voor 'uitlevering' van gegevens betreft de telecommunicatie. De regering heeft naast het instellen van de Commissie-Mevis (en de daarop te baseren wetsvoorstellen) namelijk een wetsvoorstel ingediend over het vorderen van gegevens betreffende telecommunicatie.[31] Het gaat daarbij om twee soorten gegevens: verkeersgegevens (zie par. 3.4) en gebruikersgegevens. Deze laatste categorie is hier relevant: het zijn de gegevens die in art. 18 lid 1 onder b CCV apart worden genoemd. Hier wordt het ingewikkeld. De uitwerking van de regeling van telecomgebruikersgegevens is bepaald onduidelijk. De regering spreidt de gebruikersgegevens namelijk uit over twee bevoegdheden: de identificerende gebruikersgegevens (NAW-gegevens, nummer en soort dienst) worden ondergebracht in een nieuw art. 126na/ua Sv[32] (onder dezelfde voorwaarden als het kabinet voorstelt voor identificerende gegevens in het Mevis-traject)[33], maar tegelijk worden alle gebruikersgegevens (zowel de identificerende gegevens als gegevens over bijvoorbeeld betaling) samengenomen met de verkeersgegevens in een herzien art. 126n/u Sv. Identificerende gebruikersgegevens kunnen dus op basis van twee verschillende bevoegdheden worden opgevraagd, en in de toekomst wellicht nog op basis van een derde bevoegdheid (de identificerende gegevens van het komende wetsvoorstel strafvorderlijke gegevensvergaring). Tegelijk zorgen het wetsvoorstel en de toelichting voor begripsmatige verwarring, omdat zij gebruikersgegevens aanduiden *als verkeersgegens* (de memorie van toelichting meldt: 'verkeersgegevens, in de wettekst omschreven als "gegevens over een gebruiker en het telecommunicatieverkeer met betrekking tot die gebruiker"'),[34] terwijl tegelijkertijd ook een onderscheid wordt gemaakt tussen verkeersgegevens en gebruikersgegevens[35]. Het begrip 'verkeersgegevens' krijgt daardoor twee betekenissen: een enge betekenis (de gebruikelijke en bestaande betekenis: gegevens over telecommunicatieverkeer) en een

[30] TK 2001-2001, 28 366, nr. 1, p. 20.
[31] TK 2001-2002, 28 059, nrs. 1-3.
[32] De bestaande artikelen 126na/ua Sv (het inzetten van IMSI-vangers om nummergegevens te kunnen achterhalen) worden hernummerd tot 126nb/ub Sv.
[33] De categorie strafbare feiten is voor de identificerende telecomgebruikersgegevens bij nota van wijziging opgetrokken van alle strafbare feiten naar misdrijven. TK 2001-2002, 28 059, nr. 6.
[34] TK 2001-2002, 28 059, nr. 3, p. 7.
[35] De memorie van toelichting hanteert kopjes als 'Verkeersgegevens, artikelen 126n en 126u' en 'Gebruikersgegevens, artikelen 126na en 126ua'. Verder suggereren zinnen als 'Bij verkeersgegevens (…) gaat het om de uiterlijke kenmerken van telecommunicatie en niet om de inhoud van hetgeen via het telecommunicatieverkeer wordt uitgewisseld' (nr. 3, p. 7) dat het begrip 'verkeersgegevens' ook in de traditionele betekenis wordt gebruikt – gebruikersgegevens (bijvoorbeeld over betaling) gaan immers evenmin over 'de uiterlijke kenmerken van telecommunicatie' als over de inhoud van telecommunicatie.

ruime betekenis (gegevens over telecomgebruikers en telecommunicatieverkeer). Het komt de inzichtelijkheid en kenbaarheid van de wet niet ten goede.
Veel kwalijker vind ik echter dat de wetgever de telecomgegevens loskoppelt van de algemene gegevens. De Commissie-Mevis en het kabinet hebben er bewust voor gekozen om voor verkeersgegevens een zelfstandig traject te bewandelen, waardoor de voorstellen voor 'strafvorderlijke gegevensvergaring in de informatiemaatschappij' alle mogelijke gegevens betreffen behalve telecomgegevens. Commissie en kabinet benadrukken dat verkeersgegevens een bijzondere categorie vormen, vanwege de historische ontwikkeling die heeft geleid tot een reeds bestaand wettelijk kader, waarbij onder andere een praktijk is ontstaan dat verkeersgegevens direct (moeten kunnen) worden doorgeleid.[36] Ik vind het echter een zwaktebod om op basis daarvan telecomgegevens af te zonderen: juist wanneer men een integrale visie ontwikkelt op gegevensvergaring in de huidige maatschappij, moet men geïntegreerd kijken naar alle mogelijke soorten gegevens.
Om die reden vind ik ook het indienen en snel behandelen van een wetsvoorstel tot vorderen van gegevens in de financiële sector[37] ongelukkig. Dat wetsvoorstel is ingegeven door een protocol bij het EU-rechtshulpverdrag dat in het kader van terrorismebestrijding volgens de EU versneld moet worden geïmplementeerd. De bepalingen komen overeen met het kabinetsstandpunt over de voorstellen van de Commissie-Mevis (namelijk bevoegdheden voor het opvragen van identificerende, 'andere', toekomstige en gevoelige gegevens).
Hoewel de voorstellen in deze drie verschillende wetgevingstrajecten inhoudelijk wel op elkaar worden afgestemd, schuilt er een groot gevaar in de splitsing. Het onderwerp van strafvorderlijke gegevensvergaring is fundamenteel van groot belang en heeft ingrijpende gevolgen voor de maatschappij en voor de rol van het strafrecht daarbinnen. Daarom moet er een fundamenteel debat worden gevoerd in het parlement over de achtergrond en visie die ten grondslag liggen aan de keuzes die de wetgever maakt. Er bestaat nu echter een levensgroot risico dat bij de behandeling van het wetsvoorstel vorderen gegevens financiële sector het fundamentele debat vooruit wordt geschoven naar de behandeling van het komende wetsvoorstel strafvorderlijke gegevensvergaring, aangezien dat immers gaat over de algemene uitgangspunten en visies. Wanneer dat wetsvoorstel dan uiteindelijk ter sprake zal komen, zal kunnen worden terugverwezen naar de financiëlesectorwet en mogelijk ook de telecomgegevenswet; dat zijn dan immers precedenten met een wellicht al 'bestendige praktijk' waar men toch moeilijk meer op terug kan komen.
Een aanwijzing hiervoor is reeds te vinden in de nota naar aanleiding van het verslag bij de financiëlesectorwet. De regering geeft daar aan dat de financiëlesectorwetgeving zal worden vervangen door de algemene gegevensvergaringswetgeving. 'Het vervangen van de in het wetsvoorstel opgenomen regeling voor de financiële sector door een algemene

[36] Commissie-Mevis 2001, p. 90-92; TK 2001-2001, 28 366, nr. 1, p. 29-30.
[37] TK 2001-2002, 28 353, nrs. 1-3, wetsvoorstel van 26 april 2002; gewijzigd voorstel van wet, EK 2002-2003, 28 353, nr. 83, van 28 november 2002.

regeling behoeft voor de instellingen in de financiële sector geen gevolgen te hebben, omdat de bevoegdheden *hetzelfde zullen kunnen blijven*. De bevoegdheden die in het wetsvoorstel worden voorgesteld voor de financiële sector komen namelijk geheel overeen met de betreffende bevoegdheden zoals deze zijn voorgesteld door de Commissie Mevis' (mijn cursivering).[38] Met andere woorden: de regering houdt er geen rekening mee dat het parlement bij het latere, algemene wetsvoorstel wel eens andere keuzes zou kunnen maken dan bij het eerdere financiëlesectorwetsvoorstel. Dit suggereert dat het benodigde fundamentele debat evenmin gevoerd zal gaan worden bij het algemene, integrale wetsvoorstel. Dat een dergelijk scenario allerminst fictie is, heeft de wetgeving over de kostenverdeling bij aftapbaarheid aangetoond: bij de specifieke wet (over GSM) werd vooruitverwezen[39] naar het algemene beleid (het Beleidsvoornemen bevoegd aftappen) dat later terugverwees[40] naar de specifieke wet – een inhoudelijk debat schitterde door afwezigheid; hetzelfde geldt voor het invoeren van de telecommunicatietap bij beraamde georganiseerde misdaad[41].

Het opvragen van gegevens uit art. 18 CCV wordt in Nederland aldus ingrijpend herzien. Aan de voorstellen van de Commissie-Mevis en van het kabinet ligt een duidelijke visie ten grondslag, die primair uitgaat van het opsporingsbelang. Zaken als de persoonlijke levenssfeer, lasten voor maatschappelijke actoren en het onderscheid tussen verdachten en niet-verdachten worden wel meegewogen, maar dan gaat het naar mijn gevoel vooral om afrondingsverschillen. De prijs die de maatschappij betaalt wordt met name ingegeven door de behoefte van de opsporing en door de technische mogelijkheden[42]. Op die visie is kritiek mogelijk, zoals diverse instanties en personen hebben aangetoond,[43] en het parlement moet daarom een fundamenteel en uitgebreid debat voeren over de voorgestelde bevoegdheden.

---

38 TK 2002-2003, 28 353, nr. 6, p. 1-2.
39 TK 1994-1995, 24 108, nr. 3, p. 2.
40 TK 1995-1996, 24 679, nr. 1, p. 9-11.
41 Zie Koops 2002, p. 150-151.
42 Stuitend vind ik het slaafs volgen van de technische mogelijkheden waar het kabinet blijk van geeft: 'De ontwikkelingen in de informatietechnologie bieden echter mogelijkheden waaraan de opsporing niet voorbij kan gaan. Met de Commissie verwacht het kabinet dat de behoefte aan bewerkingen ten behoeve van de opsporing in de toekomst zal toenemen. De toepassing van informatieen communicatietechniek maakt het mogelijk dat grote gegevensbestanden aanwezig zijn en dat hieraan door een bewerking belangrijke informatie voor strafvorderlijk onderzoek is te ontlenen. In het kader van strafvorderlijk onderzoek zal daarop steeds vaker een beroep worden gedaan. Het is gewenst in het Wetboek van Strafvordering hiertoe een bevoegdheid op te nemen, om deze ontwikkeling in goede banen te leiden.' TK 2001-2002, 28 366, nr. 1, p. 20. Met andere woorden: omdat de technische mogelijkheden een opsporingsbehoefte kweken, moet de wetgever aan die behoefte voldoen.
43 Zie bijvoorbeeld de bronnen vermeld in TK 2001-2002, 28 366, nr. 1, p. 5n en Dommerings column in *Netkwesties*, <http://www.netkwesties.nl/editie24/column1.html>.

3.3. Doorzoeking en 'inbeslagneming'

Artikel 19 CCV regelt de doorzoeking van computer(systemen) en de 'inbeslagneming' van gegevens. Onderdelen van dit artikel lijken geïnspireerd door de Nederlandse wetgeving: de netwerkzoeking van art. 125j Sv en het medewerkingsbevel om beveiliging ongedaan te maken van art. 125k Sv vinden we in dezelfde vorm terug in het verdrag. Voor de doorzoeking zelf, het inbeslagnemen van gegevensdragers en het copiëren van gegevens zijn in Nederland geen afzonderlijke bevoegdheden nodig, aangezien deze passen binnen de bestaande kaders van doorzoeking en inbeslagneming. Op één punt noodzaakt het verdrag echter wel tot aanpassing: in Nederland kunnen gegevens niet inbeslaggenomen worden, aangezien het geen goederen zijn. Dat betekent dat justitie gegevens wel kan copiëren ten behoeve van de waarheidsvinding, maar daarbij blijven de gegevens beschikbaar voor de betrokkene. Soms kan het echter ook wenselijk zijn om de gegevens aan diens beschikkingsmacht te onttrekken, bijvoorbeeld bij digitale kinderporno of kraakprogramma's (zoals men goederen ook in beslag kan nemen ter onttrekking aan het verkeer). Volgens het verdrag moet daartoe ook een bevoegdheid bestaan. Hierin wordt voorzien in het wetsvoorstel Computercriminaliteit II (voorgesteld art. 125o Sv). Mocht achteraf blijken dat de ontoegankelijk gemaakte gegegens bijvoorbeeld geen kinderporno betroffen, dan kan de ontoegankelijkmaking weer ongedaan worden gemaakt; anders zal de rechter bij zijn eindoordeel of bij afzonderlijke beschikking meestal tot vernietiging van de gegevens beslissen (voorgesteld art. 354 en 552fa Sv).

Los van het verdrag zijn er nog twee onvolkomenheden in de Nederlandse wetgeving op dit vlak. De eerste betreft het feit dat er alleen een doorzoeking ter inbeslagneming kan plaatsvinden, maar niet ter onderzoek van gegevens. Aangezien gegevens niet inbeslaggenomen kunnen worden, kan er theoretisch geen doorzoeking worden aangevraagd als justitie alleen beoogt om een computer te doorzoeken en gegevens te copiëren. In de praktijk kan natuurlijk altijd een doorzoeking ter inbeslagneming van een gegevens*drager* plaatsvinden, maar dat verdient geen schoonheidsprijs. De Commissie-Mevis en het kabinet beogen dit theoretische probleem op te lossen door een zelfstandige bevoegdheid in te voeren tot doorzoeking 'ter vastlegging van gegevens' (voorgesteld nieuw art. 125i Sv).[44] Dit is een nuttig voorstel dat de systematiek van de wet versterkt. Een andere onvolkomenheid heeft tot nu toe echter te weinig aandacht gekregen. De wetgever heeft voorzien in de mogelijkheid iemand te bevelen om een beveiliging ongedaan te maken (art. 125k Sv), maar deze mogelijkheid is beperkt tot de situatie van een doorzoeking. Justitie kan echter ook buiten een doorzoeking in bezit komen van beveiligde computers of beveiligde gegevens (bijvoorbeeld wanneer de r-c tijdens een gerechtelijk vooronderzoek een schoot-pc in beslag neemt, art. 104 Sv). Is het niet wenselijk om ook in dergelijke gevallen een ongedaanmakingsbevel te kunnen geven? Zoals het algemeen geredigeerde art. 125l Sv (over verschoningsgerechtigden) spreekt over 'onderzoek in een geautomatiseerd werk', zo zou ook art. 125k kunnen worden

[44] Commissie-Mevis 2001, p. 88-90 en 100; TK 2001-2001, 28 366, nr. 1, p. 28.

uitgebreid tot elk computeronderzoek. Hetzelfde geldt voor art. 125n, de bepaling over vernietiging en bewaring van gegevens, dat ook niet alle mogelijke gevallen van computeronderzoek beslaat. Gelukkig heeft de Tweede Kamer inmiddels dit punt voorgelegd aan de minister.[45]

3.4. Onderzoek van telecommunicatie

Bevoegdheden tot onderzoek van telecommunicatie worden – terecht – gevoelig gevonden, zo blijkt uit de speciale positie die art. 20 CCV (verkeersgegevens) en art. 21 CCV (aftappen) innemen in art. 14 CCV: lidstaten kunnen meer beperkingen aanleggen in de reikwijdte van deze bevoegdheden dan bij de andere bevoegdheden. Voor Nederland brengt het verdrag geen veranderingen met zich mee – onderzoek van telecommunicatie is al ruimschoots mogelijk op basis van art. 126n/u (verkeersgegevens) en art. 126m/t Sv (aftappen). (Aanpassing van de tapbepalingen is wel nodig op grond van het rechtshulpverdrag tussen EU-lidstaten, dat onder andere grensoverschrijdend aftappen regelt; hiertoe worden art. 126m/t Sv aangepast en nieuwe artikelen 552ob-oc en 552qe ingevoegd; dit valt buiten het bestek van dit artikel.[46])
Op tapgebied is er verder geen wetgevingsactiviteit, maar bepaalde jurisprudentie geeft aanleiding om eens grondig te kijken naar de praktijk van het tappen: zijn er wel voldoende waarborgen voor een rechtmatige uitoefening van de aftapwetgeving? Het in strijd met de wet structureel bewaren van gesprekken met geheimhouders[47] en geluiden dat met tapverslagen mogelijk gemanipuleerd is[48] kunnen incidenten of verdedigingsvondsten betreffen, maar het kunnen ook indicaties zijn dat er onvoldoende toezicht bestaat op de aftappraktijk. Een gedegen onderzoek hiernaar zou welkom zijn. Vooral het terrein van verkeersgegevens is echter volop in beweging.[49] In de eerste plaats ligt er het reeds genoemde wetsvoorstel vorderen gegevens telecommunicatie, dat naast op het opvragen van gebruikersgegevens ook een herziening van de regeling van verkeersgegevens inhoudt. De belangrijkste wijzigingen betreffen het uitbreiden van art. 126n/u Sv met gebruikersgegevens (bijvoorbeeld ook over de betaling van telecomdiensten), het onderscheiden tussen bestaande en toekomstige gegevens, het

---

45 TK 2000-2001, 26 671, nr. 6, p. 11 en 24.

46 Overeenkomst betreffende de wederzijdse rechtshulp in strafzaken tussen de lidstaten van de Europese Unie, 29 mei 2000, Trb. 2000, 96. Zie Kaspersen 2002, p. 38-41, voor een korte bespreking. Op 26 april 2002 is een wetsvoorstel ter implementatie ingediend: TK 2001-2002, 28 351, nrs. 1-2.

47 Rb. Almelo 9 augustus 2001, *Nieuwsbrief Strafrecht* 2001/10, nr. 234. In deze zaak deelde het OM mee dat 'in een negental tapkamers van de politie sedert 1994 geen enkel gesprek meer gewist is, omdat dit technisch niet mogelijk zou zijn. Bovendien hebben de onderzoeksteams nog steeds de beschikking over de originele disks', *Nieuwsbrief Strafrecht* 2001/10, p. 357-358. Zie ook Pres.Rb. 's-Gravenhage 19 december 2001, *Nieuwsbrief Strafrecht* 2002/1, nr. 26.

48 Hof Den Bosch 30 juli 2002, Rechtspraak.nl, LJN-nummer AE5920, <http://www.recht-spraak.nl/uitspraak/frameset.asp?ui_id=37100>.

49 Zie voor een overzicht van technische en juridische ontwikkelingen rond verkeersgegevens Hes, Ekker & Koops 2003, dat vele problemen aansnijdt die de wetgever zou moeten oplossen.

uitsluiten van de bevoegdheid bij heterdaad en bij simpele computervredebreuk, en het afschaffen van de eis van vermoedelijke deelname van de verdachte.
Vooral dat laatste levert een forse uitbreiding op van de reikwijdte van de bevoegdheid: justitie zou over iedereen verkeers- en gebruikersgegevens kunnen opvragen. De argumenten daarvoor zijn ontleend aan de voorstellen van de Commissie-Moons en het daarop gebaseerde wetsvoorstel herziening gerechtelijk vooronderzoek, naar aanleiding waarvan in de wet BOB de eis van deelname van de verdachte bij de telecommunicatietap is geschrapt. Nu die eis bij de zwaardere bevoegdheid (de tap) is vervallen, ligt het voor de hand de eis ook te schrappen bij de lichtere bevoegdheid (verkeersgegevens), zo luidt de redenering.[50] Die klopt echter maar ten dele: de georganiseerdemisdaadtap (art. 126t Sv) kan alleen worden uitgeoefend op 'betrokkenen' bij (vermoedelijke) georganiseerdemisdaadverbanden; er hoeft geen sprake te zijn van een verdachte, maar justitie moet wel het vermoeden hebben dat iemand ernstige georganiseerde misdaad beraamt of pleegt. Bij de georganiseerdemisdaadbevoegdheid voor verkeersgegevens wordt echter geen beperking tot 'betrokkenen' voorgesteld.[51] Een belangrijk verschil lijkt mij ook dat bij de telecomtap de subsidiariteit en proportionaliteit de r-c er in hoge mate van zullen weerhouden om niet-verdachten af te laten tappen, terwijl dat bij verkeersgegevens niet zo hoeft te zijn. Verkeersgegevens zijn bij uitstek interessant in beginstadia van opsporingsonderzoeken, om verbanden in kaart te brengen en om uit te vinden wie nader onderzoek zou kunnen behoeven. Het ligt daarom voor de hand dat ruimschoots gebruik zal worden gemaakt van de mogelijkheid verkeersgegevens van niet-verdachten op te vragen.
Daar komt nog bij dat het object van de bevoegdheid wordt uitgebreid met tal van nieuwe soorten gegevens: ook adressen van weblocaties en van individuele pagina's binnen een weblocatie vallen eronder, alsmede locatiegegevens (voorzover deze samenhangen met een belhandeling) en gegevens over bijvoorbeeld het gebruik van doorschakelfuncties.[52] Al met al ontstaat een bevoegdheid waarmee veel meer dan vroeger een indringend beeld van (een deel van) iemands persoonlijke levenssfeer kan worden verkregen, ook van niet-verdachten. Dat rechtvaardigt de vraag of het handhaven van de bestaande voorwaarden wel een juiste keuze is. Nu is de beperking in strafbare feiten – de bevoegdheid mag slechts worden toegepast bij voorlopigehechtenismisdrijven – redelijk zwaar, maar de bevoegde autoriteit – de officier van justitie – lijkt mij in bepaalde opzichten aan de lichte kant.[53] Het lijkt mij wenselijk dat er meer gedifferentieerd wordt tussen de 'traditionele' verkeersgegevens (wie heeft wanneer hoe lang met wie gebeld) en nieuwe soorten verkeersgegevens die aanzienlijk privacygevoeliger zijn. Voor bijvoorbeeld gegevens

[50] TK 2001-2002, 28 059, nr. 3, p. 9.
[51] Hetgeen overigens niet bijzonder veel uitmaakt, aangezien het begrip 'betrokkene' bijzonder ruim kan worden uitgelegd, zie Koops 2002, p. 191.
[52] TK 2001-2002, 28 059, nr. 3, p. 7-8.
[53] Mijns inziens bestaat er een onoplosbaar spanningsveld tussen het vertrouwen van de wetgever in de magistratelijkheid van de officier van justitie (iemand die de belangen van verdachte, derden en opsporing afweegt) en de rol als spil van het opsporingsonderzoek die hij sinds de wet herziening gvo heeft gekregen.

over Internetbezoek en locatiegegevens (welke plaatsen heeft iemand bezocht, zowel online als offline), die qua privacygevoeligheid aanleunen tegen de inhoud van communicatie, zou een aanvullende voorwaarde van machtiging van de r-c op zijn plaats zijn, en misschien ook een beperking als 'indien het onderzoek dit dringend vordert'.

In de tweede plaats zijn verkeersgegevens onderwerp van discussie in breder, Europees, verband, waar sterk wordt nagedacht over een bewaarplicht voor verkeersgegevens.[54] Nederland kent reeds een beperkte bewaarplicht van drie maanden voor enkele soorten verkeersgegevens bij mobiele telecommunicatie,[55] maar dat is allerminst een algemene bewaarplicht. Binnen de EU wordt, vooral op aandrang van enkele lidstaten en met een krachtige wind in de rug sinds de aanslagen van 11 september 2001, een kaderbesluit overwogen dat lidstaten zou verplichten bewaring te eisen van verkeersgegevens gedurende één tot twee jaar.[56] De nieuwe richtlijn Privacy en elektronische communicatie[57] en het Cybercrime-verdrag moedigen een bewaarplicht niet aan, maar staan deze wel toe.
In dit bestek kan ik niet uitgebreid ingaan op de voor- en nadelen van een bewaarplicht. Veel zal afhangen van de precieze invulling: welke gegevens moeten worden bewaard, bij welke soorten telecommunicatie, en hoe wordt dit technisch en organisatorisch uitgevoerd? Maar los van dergelijke concrete punten moet vooral het *uitgangspunt* van een bewaarplicht ter discussie worden gesteld. Tot nu toe heeft justitie altijd genoegen genomen met het opvragen van gegevens die op het moment van de vordering aanwezig waren; als de telecomaanbieder gegevens had gewist, viste justitie achter het net. Daar hoorde je nooit klachten over (althans niet op wetgevingsniveau). Natuurlijk heeft justitie behoefte aan meer en meer gegevens en natuurlijk zijn bepaalde opsporingsonderzoeken minder succesvol omdat waardevolle gegevens worden gewist, maar dat is niets nieuws. Ik heb weinig concrete argumenten gehoord om nu plotseling over te gaan tot een bewaarplicht voor verkeersgegevens – de post-11-september-*terrorisme*bestrijdingsrage kan in elk geval geen reden zijn een bewaarplicht in te voeren ten behoeve van de opsporing van alle mogelijke misdrijven. Door het gebrek aan een deugdelijke,

---

[54] Zie over de bewaarplicht Koops 2002, p. 131-139. Zie voor een overzicht van internationale officiële uitspraken over de (on)wenselijkheid van een bewaarplicht voor verkeersgegevens *IR Traffic Data Retention*, <http://is.lse.ac.uk/staff/hosein/collaborative/ir_retention.html>, bijgewerkt 23 mei 2001, en de discussiestukken op het Cybercrime-discussieplatform <http://cybercrime-forum.jrc.it> onder 'data retention'.
[55] Art. 13.4 lid 2 Telecommunicatiewet. De te bewaren gegevens zijn tijdstip, nummer en basisstation, aldus art. 7 Besluit bijzondere vergaring nummergegevens telecommunicatie, Stb. 2002, 31, van kracht sinds 1 maart 2002.
[56] Zie het Belgische voorstel *Draft Framework Decision on the retention of traffic data and on access tot this data in connection with criminal investigations and prosecutions*, beschikbaar op <http://www.statewatch.org/news/2002/aug/05datafd.htm>, met analyse in <http://www.statewatch.org/news/2002/aug/analy11.pdf>.
[57] Richtlijn 2002/58/EG van 12 juli 2002, *PbEG* 31 juli 2002, L201/37.

uitgewerkte motivering faalt de (Europese) wetgever in het aantonen waarom een bewaarplicht noodzakelijk zou zijn in een democratische samenleving.

4. Conclusie

Het Cybercrime-verdrag is een belangrijke stap in de internationale strijd tegen computercriminaliteit. De approximatie van wetgeving is toe te juichen, aangezien alleen door adequate wetgeving in zo veel mogelijk landen de cybermisdaad, die zich van nature weinig van grenzen aantrekt, effectief te bestrijden valt. De Nederlandse wetgeving is al goed toegerust op de eisen van het verdrag, maar op enkele punten moet Nederland de wetgeving aanpassen. De belangrijkste vernieuwingen zijn de strafbaarstelling van 'misbruik van hulpmiddelen', de strafbaarstelling van virtuele kinderpornografie (die reeds is geïmplementeerd), het bevriezingsbevel en de 'inbeslagneming' (ontoegankelijkmaking) van gegevens.

Ook los van de eisen van het Cybercrime-verdrag valt er het nodige te verbeteren aan de Nederlandse wetgeving, waartoe onder andere het wetsvoorstel Computercriminaliteit II aanzetten geeft. Belangrijker nog zijn de ontwikkelingen in het formele strafrecht: er staan ingrijpende wijzigingen op stapel voor het opvragen van gegevens, zowel algemene als telecomgegevens, en een mogelijke bewaarplicht voor verkeersgegevens zal nog van zich laten horen.

Veel van deze ontwikkelingen vind ik positief. Het is belangrijk om een adequate strafbaarstelling te hebben van de diverse vormen van computercriminaliteit, en het is even belangrijk dat justitie voldoende middelen heeft om computercriminaliteit effectief op te sporen. Diverse voorgestelde wetswijzigingen dragen daartoe bij.

Maar ik zie ook een duidelijke keerzijde in de voorstellen. De ingrijpendste wijzigingen die ons te wachten staan dragen ook bij tot (computer)criminalisering van de maatschappij. De strafbaarstelling van technische voorbereidingshandelingen en de onrechtmatigverklaring van omzeiling van auteursrechtbeveiligingen gaan niet uit van het bestrijden van strafwaardige handelingen zelf, maar van het criminaliseren van handelingen waar op zich niets mis mee hoeft te zijn. Dit zou uiteindelijk kunnen leiden tot een risicoaansprakelijkheid voor het ontwikkelen of bezitten van technologie die wellicht óók gebruikt kan worden voor onoorbare doeleinden – een schrikbeeld dat niet alleen technologische innovatie maar ook de rechtsstaat onder druk zet.

Ook de strafvorderlijke ontwikkelingen tonen een toenemende greep van de strafvordering op de maatschappij. De Nederlandse voorstellen voor het vorderen van gegevens (zowel algemene als telecom- en financiële gegevens) gaan primair uit van de behoefte van strafvorderlijke instanties, waarbij tegenwichten als privacy en maatschappelijke lasten meer in de marge dan in de kern worden meegewogen. Nog verdergaand is de Europese dreiging van een bewaarplicht voor verkeersgegevens, die een aanzienlijke instrumentalisering van een maatschappelijk proces ten behoeve van de strafvordering zou betekenen. De maatschappij wordt zodanig ingericht dat, mocht er ooit een strafbaar feit worden gepleegd, justitie makkelijker in staat zal zijn dat op te lossen.

Dat hoeft niet per definitie afgewezen te worden, maar in schaal en mate van doelafwijking gaat een bewaarplicht voor verkeersgegevens wel erg ver in de verstrafrechtelijking van de maatschappij.
De wetgever moet uiterst voorzichtig zijn met een dergelijke instrumentalisering en criminalisering van maatschappelijke processen. Strafvordering is er tenslotte voor de maatschappij, en niet omgekeerd.

Literatuur

Commissie-Mevis 2001
Commissie-Mevis, *Gegevensvergaring in strafvordering. Nieuwe bevoegdheden tot het vorderen van gegevens ten behoeve van strafvorderlijk onderzoek*, 2001.

Van Dijk & Keltjens 1995
Chr.H. van Dijk & J.M.J. Keltjens, *Computercriminaliteit*, Zwolle: Tjeenk Willink 1995.

Hes, Ekker & Koops 2003
R. Hes, A.H. Ekker & B.J. Koops, *Verkeersgegevens. Een juridische en technische inventarisatie*, Amsterdam: Otto Cramwinckel 2003.

Kaspersen 2002
Rik Kaspersen, 'Het Cybercrime-verdrag van de Raad van Europa', in: J.E.J. Prins e.a. (red.), *Recht & Informatietechnologie* (losdelig), Den Haag: Sdu, augustus 2002.

Koops & Schellekens 1999
B.J. Koops & M.H.M. Schellekens, 'Computercriminaliteit II: de boeven zijn er – nu de wet weer', *Nederlands Juristenblad* 1999, p. 1764-1772.

Koops 2002
B.J. Koops, *Strafvorderlijk onderzoek van (tele)communicatie 1838-2002. Het grensvlak tussen opsporing en privacy*, Deventer: Kluwer 2002.