

AAN De Minister van Justitie

DATUM 12 mei 2004

ONS KENMERK z2004-0287*

CONTACTPERSOON

UW BRIEF VAN 20 februari 2004

UW KENMERK 5270150/04/6

ONDERWERP Advies conceptwetsvoorstel Aanpassing aan het
Cybercrime Verdrag

Bij brief van 20 februari 2004 heeft u het College bescherming persoonsgegevens (CBP) verzocht te adviseren over het conceptwetsvoorstel tot wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering met het oog op de goedkeuring van het Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken (Wetsvoorstel Aanpassing aan het Cybercrime Verdrag). Het conceptwetsvoorstel heeft tot doel de Nederlandse wetgeving aan te passen, zodat het Cybercrime Verdrag (CV) door Nederland kan worden geratificeerd. Het Cybercrime Verdrag strekt ertoe de samenleving te beschermen tegen strafbare feiten verbonden met elektronische netwerken. Het Cybercrime Verdrag bevat daartoe zowel bepalingen van materieel en formeel strafrechtelijke aard, als bepalingen inzake internationale samenwerking en tot slot inwerkingtredings- en overige bepalingen.

1. Inleiding

Het CBP onderkent dat dit wetsvoorstel in verband moet worden gezien met recent tot stand gebrachte, aanhangige en in voorbereiding zijnde voorstellen. De conceptmemorie van toelichting noemt in dit verband: de Wet Computercriminaliteit, het Wetsvoorstel Computercriminaliteit II, de Wet Bijzonder opsporingsbevoegdheden, de Wet Vorderen gegevens telecommunicatie, de Wet Vorderen gegevens financiële sector, het Wetsvoorstel Bevoegdheden vorderen gegevens en het Wetsvoorstel Uitvoeringswet EU-rechtshulpovereenkomst. Het CBP komt op dit bredere kader graag in verband met de implementatie van deze wetgeving nader terug.

Het CBP maakt van deze gelegenheid wel reeds gebruik om zijn zorgen te uiten over de onderlinge samenhang en consistentie van bestaande wettelijke bepalingen en lopende wetgevingstrajecten op het onderhavige terrein. Het is het CBP bovendien gebleken dat bij bedrijven en instellingen (met name in de telecommunicatiesector) meer en meer onduidelijkheid ontstaat over de vraag wat de verplichtingen zijn waaraan zij uiteindelijk zullen hebben te voldoen op grond van dit aanzienlijke regelcomplex.

Het CBP adviseert u mogelijke knelpunten in de samenhang en consistentie tussen de onderscheiden regelingen te inventariseren en daar in de memorie van toelichting uitdrukkelijk aandacht aan te besteden. Tevens adviseert het CBP u de sectoren die aan het conceptwetsvoorstel onderworpen zullen zijn, in het bijzonder de telecommunicatiesector, grondig voor te lichten over het geheel van de voor hen op dit gebied geldende verplichtingen bij inwerkingtreding van de verschillende wetten.

Het CBP beperkt zich in het onderhavige advies tot de (wijze van) implementatie van het Cybercrime Verdrag, waar het de verwerking van persoonsgegevens betreft. Het CBP stelt daarbij voorop dat het de bestrijding van strafbare feiten verbonden met elektronische netwerken een maatschappelijk relevant doel van wetgeving vindt. Gezien het veelal grensoverschrijdende karakter ervan steunt het CBP in algemene zin internationale samenwerking. Het CBP staat ten gronde dan ook positief ten opzichte van ratificatie van het Cybercrime Verdrag en de daartoe vereiste implementatiewetgeving. Het CBP verwijst in dit verband naar de brief van zijn voorganger, de Registratiekamer, van 13 maart 2000 (z2000-0223.01) aan de Vaste Commissie van justitie van de Tweede Kamer.

Het CBP ziet aanleiding omtrent de volgende aspecten van het conceptwetsvoorstel te adviseren:

- Strafrechtelijke bescherming van het communicatiegeheim
- Strafvorderlijke bevoegdheden en de bandbreedte van het Cybercrime verdrag
- Strafvorderlijke waarborging van het communicatiegeheim in private netwerken en vorderen gegevens telecommunicatie
- Tot wie de vordering zich richt
- Notificatie en geheimhoudingsplicht

2. Strafrechtelijke bescherming van het telecommunicatiegeheim

Het telecommunicatiegeheim is verankerd in artikel 13 van de Grondwet. Het Wetboek van Strafrecht (Sr) kent diverse bepalingen die beogen het telecommunicatiegeheim te beschermen, zoals artikel 138a, de artikelen 139a tot en met 139e, artikel 374bis en de artikelen 441 en 441a. Op 9 december 2002 (z2002-1348) heeft het CBP de Staatssecretaris van Economische Zaken geadviseerd over het concept Wetsvoorstel Wijziging van de Telecommunicatiewet en enkele andere wetten in verband met de implementatie van een nieuw Europees regelgevingskader voor elektronische communicatienetwerken en -diensten (wetsvoorstel 28 851). Het CBP drong daarbij aan op doordenking van de implicaties van introductie van de begrippen elektronische communicatie en openbare elektronische communicatienetwerken en -diensten, waar het voormelde strafbaarstelling betreft. Bij de behandeling van wetsvoorstel 28 851 in de Tweede Kamer heeft de Minister van Economische Zaken aangekondigd in overleg met het Ministerie van Justitie te onderzoeken in hoeverre de strafbaarstelling in de artikelen 139a tot en met 139e Sr aanpassing behoeft. Dit heeft nog niet tot aanpassing of voorstellen daartoe geleid.

Implementatie van het Cybercrime Verdrag leidt tot invoering van bevoegdheden met betrekking tot private netwerken. Het CBP nodigt daarom ook u uit tot heroverweging van (de reikwijdte van) voormelde strafbaarstelling, met name in artikel 374bis Sr dat is gericht op openbare telecommunicatiediensten. Daarnaast leidt ook de toenemende omvang van communicatie in niet openbare netwerken naar het oordeel van het CBP tot de noodzaak (de reikwijdte van) voormelde strafbaarstelling aan te passen. Veelal zijn inbreuken op communicatie middels niet openbare netwerken niet strafbaar, indien deze worden gepleegd door de rechthebbende op het netwerk. De vraag rijst of niet ook aan de toegang van de rechthebbende tot communicatie over zijn eigen netwerk nadere voorwaarden dienen te worden gesteld ter bescherming van het telecommunicatiegeheim van de gebruikers van dat netwerk. Zeker voor omvangrijke private

netwerken waarin vele duizenden personen plegen te communiceren in verschillende posities en onderlinge verhoudingen en met uiteenlopende redelijke verwachtingen ten aanzien van de bescherming van de vertrouwelijkheid van de communicatie acht het CBP dergelijke nadere voorwaarden nodig.

3. Strafvorderlijke bevoegdheden en de bandbreedte van het Cybercrime Verdrag

In algemene zin is het CBP van oordeel dat in het concept wetsvoorstel ten onrechte is nagelaten aan te geven hoe de wetgever de relatie ziet tussen het Cybercrime Verdrag en het Nederlandse stelsel van bestaande en komende bevoegdheden tot het vorderen van computergegevens, met inbegrip van verkeersgegevens en de interceptie van communicatie. Het CBP heeft daarbij zowel het oog op de ruimte die het Cybercrime Verdrag zelf laat voor implementatie in relatie tot het Wetboek van Strafvordering, als op reeds bestaande dan wel voorgestelde strafvorderlijke bevoegdheden die buiten het bestek van het Cybercrime Verdrag vallen.

Bevoegdheden buiten het Cybercrime Verdrag opschonen

Om met dat laatste te beginnen, is het voor het CBP de vraag in hoeverre de Nederlandse wetgever het stelsel van bevoegdheden zoals neergelegd in het Cybercrime Verdrag op zichzelf beschouwt als toereikend om de betreffende criminele gedragingen te kunnen opsporen dan wel om elektronisch bewijs te kunnen vergaren.

Het komt het CBP voor dat het Cybercrime Verdrag tamelijk omvattend is. Naar de opvatting van het CBP moet het Cybercrime Verdrag dan ook worden beschouwd als een maatgevend voorstel waar het gaat om het opsporen van criminele gedragingen waarbij computernetwerken (met inbegrip van private en openbare telecommunicatienetwerken) worden gebruikt alsmede het vergaren van elektronisch bewijsmateriaal. Het Cybercrime Verdrag beoogt de regelgeving van de verdragsstaten zodanig te harmoniseren dat zowel nationaal als grensoverschrijdend adequaat kan worden opgetreden tegen criminele activiteiten.

Als de Nederlandse regering met het CBP van oordeel is dat het Cybercrime Verdrag geen belangrijke omissies kent, is zij naar het oordeel van het CBP gehouden af te wegen wat de noodzaak is daarnaast nog aanvullende bevoegdheden in stand te laten dan wel voorstellen daartoe te handhaven. In plaats daarvan lijkt het voorgelegde implementatievoorstel als het ware te voorzien in een harmonisatie op minimaal niveau, met de verdragsverplichtingen als ondergrens. De conceptmemorie van toelichting neemt tot uitgangspunt dat Nederland nu al voor een zeer groot deel voldoet aan waartoe het Cybercrime Verdrag verplicht, zonder er bij stil te staan dat veel bestaande bevoegdheden soms al verder gaan dan datgene dat in het verdrag noodzakelijk is geacht of dat ze zelfs afwijken van het Verdrag. Het conceptwetsvoorstel voorziet vervolgens met name in toevoeging van een aantal nieuwe bepalingen in het Wetboek van Strafvordering.

Artikel 39, lid 3 CV bepaalt weliswaar dat het Cybercrime Verdrag niet aan de mogelijkheden van een verdragsstaat in de weg staat om andere bevoegdheden in het leven te roepen, wat in overweging 131 van het Explanatory Report (ER) wordt toegelicht. In artikel 15 CV is niettemin

neergelegd dat iedere lidstaat ervoor dient in te staan (“ensure”) dat de strafvorderlijke bevoegdheden en procedures als bedoeld in sectie 2 CV zodanig worden geïmplementeerd, dat deze in evenwicht zijn met een adequate bescherming van de mensenrechten als bedoeld in het EVRM. Specifieke bevoegdheden dienen volgens datzelfde artikel te worden omgeven met adequate waarborgen, terwijl ook de impact van de implementatievoorstellen op de rechten, verantwoordelijkheden en legitieme belangen van derden door de verdragstaat in overweging dient te worden genomen.

In het licht daarvan kan niet slechts worden volstaan met toevoeging van vanwege het Cybercrime Verdrag vereiste bevoegdheden. Het nieuw te creëren stelsel van bevoegdheden dient naar de opvatting van het CBP tevens een opschoning van het bestaande areaal aan opsporingsmiddelen met zich te brengen. Reeds eerder heeft het CBP een dergelijke benadering bepleit, onder meer naar aanleiding van de voorstellen van de Commissie Mevis (CBP advies van 18 oktober 2001, Z2001-0735). Het CBP acht een samenloop van bestaande en nieuwe bevoegdheden ongewenst. De verschillende vorderingsmogelijkheden, elk met zijn eigen voorwaarden en waarborgen, dienen zorgvuldig ten opzichte van elkaar te worden afgegrensd. Het naast elkaar laten bestaan van verschillende bevoegdhedenstelsels acht het CBP ontoelaatbaar.

Instandhouding van de bestaande en onderweg zijnde bevoegdheden met slechts toevoeging van de nieuwe bevoegdheden voortvloeiende uit het Cybercrime Verdrag zal naar de stellige verwachting van het CBP leiden tot situaties waarin de opsporingsinstanties zullen kunnen kiezen uit diverse, naast elkaar bestaande dan wel elkaar overlappende bevoegdheden.

Een voorbeeld daarvan biedt de concept memorie van toelichting op pagina 13 waar het de bevoegdheid betreft tot het opnemen van communicatie. De toelichting noemt een aantal bevoegdheden die daarbij “in beeld komen”, namelijk de artikelen 126l, 126m en 126t Sv. De mogelijke toepassing van andere bevoegdheden zoals onder meer het onderzoek in een geautomatiseerd werk (125i Sv), de uitlevering tot inbeslagneming (96a Sv) of zelfs de vrijwillige verstrekking van gegevens (artikel 11.13 Telecommunicatiewet, artikel 9 juncto artikel 43 Wet bescherming persoonsgegevens) wordt daarbij ten onrechte niet belicht.

Aldus draagt deze wijze van implementeren van het Cybercrime Verdrag bij aan een onoverzienbaar stelsel van inbreukmakende bevoegdheden. Bij het CBP bestaat dan ook gereede twijfel of na implementatie nog wel wordt voldaan aan de vereisten van bepaaldheid en voorzienbaarheid, die artikel 15 CV en artikel 8 EVRM in samenhang bezien stellen aan te maken inbreuken op de persoonlijke levenssfeer. Bestaande voorwaarden en waarborgen bij specifieke bevoegdheden kunnen met gebruikmaking van andere bevoegdheden eenvoudig worden omzeild. Voor de bevoegde autoriteiten ligt de weg van de minste weerstand aldus open. De rechtszekerheid is daarmee allerminst gediend, terwijl ook de legitieme belangen van niet-verdachte personen en van derden daarmee steeds verder uit zicht raken.

Implementatieruimte Cybercrime Verdrag in relatie tot het Wetboek van Strafvordering

Het Cybercrime Verdrag verplicht tot het treffen van wettelijke maatregelen. Hierbij is veelal een bepaald minimum vereist. Bij de invulling daarvan heeft Nederland weinig keus, behoudens waar het betreft de vorm en compenserende waarborgen. Ter motivering hiervan is het Verdrag voldoende. Het Verdrag laat de lidstaten op andere onderdelen een zekere ruimte tot invulling daarvan. De wetgeving die valt binnen die ruimte wordt rechtstreeks door het Verdrag gerechtvaardigd, zij het dat een separate motivering vereist is voor de mate waarin Nederland van de geboden ruimte gebruik maakt. Voor maatregelen die daarentegen niet op het Verdrag berusten is een zelfstandige verantwoording noodzakelijk ter onderbouwing van de voorstellen.

In het in te dienen wetsvoorstel dient naar het oordeel van het CBP alsnog nauwkeurig te worden aangegeven welke maatregelen als verplicht moeten worden beschouwd, welke berusten op nadere invulling door de Nederlandse wetgever van het Verdrag en welke maatregelen als zodanig niet op het Verdrag berusten. Zonder deze explicitering laat het conceptwetsvoorstel zich in die zin ook niet goed beoordelen.

Een voorbeeld kan dit illustreren. Het Verdrag verplicht ertoe de opsporingsbevoegdheden van sectie 2 van het Verdrag toe te laten ter opsporing van de feiten die ingevolge sectie 1 van het Verdrag strafbaar dienen te worden gesteld (MvT p. 20). In het conceptwetsvoorstel is voorgesteld de betreffende bevoegdheden toe te laten ter opsporing van feiten genoemd in artikel 67, eerste lid Sv. Bovendien worden in artikel 67, eerste lid, Sv in het conceptwetsvoorstel een aantal strafbare feiten uit sectie 1 van het Verdrag, te weten de artikelen 138a, 138b, 139d tweede lid, 350 a en 350b opgenomen.

Aldus worden de vorderingsbevoegdheden van het Verdrag toepasbaar ter opsporing van andere delicten dan bedoeld in het Verdrag, terwijl voor bepaalde delicten uit het Verdrag ook andere bevoegdheden dan die van het Verdrag toepasselijk kunnen zijn. Naar de opvatting van het CBP is dit een bovenmatige vorm van meeliften met het Cybercrime Verdrag die ten minste afzonderlijk in de toelichting dient te worden verantwoord. Het verdient aanbeveling het conceptwetsvoorstel alsnog kritisch op dit punt door te lichten.

4. Strafvorderlijke waarborging van het communicatiegeheim in private netwerken en vorderen gegevens telecommunicatie.

Met het oog op het voorgaande vraagt het CBP meer in het bijzonder uw aandacht voor de bescherming van het communicatiegeheim in private netwerken door een effectief stelsel van waarborgen in de regeling van strafforderlijke bevoegdheden alsmede voor het stelsel van bevoegdheden ter zake van het vorderen van verkeersgegevens.

Bescherming van het communicatiegeheim in private netwerken

In de huidige artikelen 125i en 126m Sv is verschil gemaakt tussen het vorderen van gegevens in geautomatiseerde werken en het doen opnemen van telecommunicatie. Onder geautomatiseerd werk verstaat artikel 80sexies Sr een inrichting die bestemd is om langs elektronische weg gegevens op te slaan en te verwerken. Opslag van gegevens staat daarin dus centraal en niet zozeer communicatie. Onder telecommunicatie verstaat artikel 126m Sv niet voor het publiek bestemde communicatie via een openbaar telecommunicatienetwerk, dan wel met gebruikmaking van openbare telecommunicatiediensten.

Het Nederlands stelsel van strafvorderlijke bevoegdheden maakt thans een onderscheid tussen opsporingsbevoegdheden tot onderzoek aan geautomatiseerde werken in Boek I, Titel IV, afdeling 7 enerzijds en bijzondere opsporingsbevoegdheden tot onderzoek aan telecommunicatie in Boek I, Titel IVA, afdeling 7, (inmiddels gewijzigd bij de Wet vorderen gegevens telecommunicatie) anderzijds. Daaraan zijn inmiddels toegevoegd de bijzondere opsporingsbevoegdheden tot het vorderen van gegevens van de financiële sector in Boek I, Titel IVA, afdeling 8. Voorts is aanhangig het Wetsvoorstel bevoegdheden vorderen gegevens dat nieuwe opsporingsbevoegdheden en bijzondere opsporingsbevoegdheden bevat, die -onder meer- in de plaats zullen treden van Boek I, Titel IVA, afdeling 8. In deze regelingen worden onderscheidingen aangebracht tussen verschillende categorieën van gegevens, zoals identificerende gegevens, verkeersgegevens, andere dan identificerende gegevens en bijzondere gegevens.

Anders dan het huidige Nederlandse stelsel behandelt het Cybercrime Verdrag telecommunicatie als een vorm van overdracht van computergegevens. Het Verdrag maakt bij bevoegdheden ten aanzien van computergegevens onderscheid tussen bevoegdheden met betrekking tot opgeslagen computergegevens in artikel 19 CV en het real time onderscheppen van de inhoud van communicatie tijdens de overdracht ervan in artikel 21 CV. Blijkens het Explanatory Report zien de bevoegdheden in het Cybercrime Verdrag in het algemeen op alle vormen van gegevens, waaronder drie specifieke vormen van computergegevens: verkeersgegevens, inhoudgegevens en abonneegegegevens. Deze computergegevens kunnen in twee vormen bestaan: opgeslagen of in het proces van communicatie. De bevoegdheden van artikel 21 CV zien op de inhoud van bepaalde communicatie die wordt verzonden middels een computersysteem. Onder een computersysteem zijn in het Cybercrime Verdrag ook telecommunicatiesystemen begrepen, ongeacht of deze openbaar dan wel besloten zijn (publicly or privately owned, overweging 207 ER). Het begrip 'content data' (inhoudgegevens) is niet in het Cybercrime Verdrag zelf gedefinieerd, maar blijkens overwegingen 209 en 229 ER is bedoeld de inhoud van de overgebrachte berichten.

In dit verband vraagt het CBP uw aandacht voor de toepassing van de bevoegdheden tot onderzoek van telecommunicatie in niet-openbare netwerken. Het CBP constateert dat overweging 120 ER enerzijds wijst op de bijzondere beschermenswaardigheid van de inhoud van de communicatie, maar dat het Cybercrime Verdrag anderzijds deze categorie van gegevens in opgeslagen vorm op dezelfde voet behandelt als andere gegevens. Het CBP acht dit een belangrijke inconsistentie van het Cybercrime Verdrag. Immers, niet valt in te zien waarom kennisneming door politie en justitie van een e-mailbericht in opgeslagen vorm met andere waarborgen zou dienen te zijn omgeven dan wanneer datzelfde bericht zou worden onderschept in de fase van overbrenging.

Waar het Cybercrime Verdrag onderscheid maakt tussen het real time aftappen van communicatie enerzijds en het vorderen van opgeslagen computergegevens anderzijds, dient de wetgever zich, naar het oordeel van het CBP, tenminste uit te spreken over de vraag welk regime toepasselijk moet worden geacht voor het vorderen van de inhoud van in geautomatiseerde werken opgeslagen berichten. Bij de totstandkoming van het Cybercrime Verdrag kwam blijkens

overweging 190 ER, eveneens de vraag naar voren of een ongeopend e-mailbericht in de postbus bij een internet service provider nu een opgeslagen computergegeven dan wel telecommunicatie is ('stored computerdata' of 'data in transfer'). Het antwoord op die vraag zou moeten worden gegeven door iedere verdragstaat afzonderlijk die zijn nationale wet daarop zou moeten nazien. Het CBP dringt er dan ook op aan dat ook de Nederlandse wetgever zich daarover ook in het conceptwetsvoorstel uitsprekt. In het wetsvoorstel Bevoegdheden vorderen gegevens (Kamerstukken II, 29 441, nr. 3, p.14) is aan de inhoud van een e-mail die is opgeslagen bij een internetaanbieder dezelfde bescherming gegeven als aan de brief die is toevertrouwd aan de instelling van vervoer. Deze gegevens mogen alleen worden gevorderd voor zover deze gegevens klaarblijkelijk van de verdachte afkomstig zijn, voor hem bestemd zijn of op hem betrekking hebben, of indien zij klaarblijkelijk tot het begaan van het strafbare feit hebben gediend, of klaarblijkelijk met betrekking tot die gegevens het strafbare feit is gepleegd.

De wetgever heeft zich tot dusver steeds op het standpunt gesteld dat in aanvulling op de voorgestelde bijzondere bevoegdheden tot het onderzoek van telecommunicatie ook nog de algemene bevoegdheden ten aanzien van geautomatiseerde werken kunnen worden aangewend, zoals het verrichten van computerdoorzoekingen bij internetproviders op grond van artikel 125i Sv. Het CBP vraagt zich af of hiermee kan worden volstaan. Het CBP adviseert u dringend het stelsel van bevoegdheden bij gelegenheid van implementatie van het Cybercrime Verdrag zo in te richten dat de bevoegdheden ten aanzien van geautomatiseerde werken niet meer toepasbaar zijn op telecommunicatie, zowel voor wat betreft de inhoud als de verkeersgegevens, ongeacht waar deze gegevens aangetroffen kunnen worden.

Door Kaspersen (zie H.W.K. Kaspersen, ICT en strafrecht; reeks Elektronisch communicatierecht, deel 9; Broadcast Press, Hilversum, 2003, p. 59) is ten aanzien van de onderhavige implementatiewet reeds opgemerkt dat men zich kan voorstellen dat voor toepassing van de bevoegdheden tot aftappen (en overigens ook die tot het vorderen van verkeersgegevens) op niet-openbare telecommunicatiediensten zwaardere eisen worden gesteld dan bij openbare diensten. Het CBP steunt die benadering. Anders dan bij het aftappen van openbare telecommunicatienetwerken en diensten, kan met dergelijke bevoegdheden de medewerking worden gevorderd van private partijen die zelf direct belang hebben bij geheimhouding van de inhoud van het berichtenverkeer dat over zo'n besloten netwerk wordt gevoerd. Dat belang kan bijvoorbeeld zijn gelegen in de bescherming van bedrijfsgeheimen, in het kunnen uitwisselen van gedachten en ideeën zonder dat de buitenwereld daar (nog) kennis van neemt of in het in stand houden van een bijzondere vertrouwensrelatie (denk bijvoorbeeld aan computernetwerken waarover mede interne accountants, advocaten of consultants communiceren). Ook de belangen van werknemers die van dergelijke netwerken gebruik maken verdienen nadere afweging.

Tenslotte maakt het CBP bezwaar tegen het slordige gebruik van terminologie in het conceptwetsvoorstel, met name waar het de interceptie van communicatie betreft. Volgens het conceptwetsvoorstel wordt artikel 21 CV "bestreken" door artikel 126l Sv, voor zover het betreft het door een opsporingsambtenaar opnemen dan wel aftappen van gegevens die aangemerkt kunnen worden als vertrouwelijke communicatie. De conceptmemorie van toelichting voegt daar op pagina 13 aan toe dat de artikelen 126m en 126t en enkele andere artikelen "in beeld komen".

Wat het strafvorderlijk deel betreft wordt eenvoudig verwezen naar een groot aantal bestaande en komende bevoegdheden die “van belang” dan wel “relevant” zouden zijn, ofwel de in het Cybercrime Verdrag voorgestelde bevoegdheden zouden “bestrijken”. De toetsing van de voorgestelde inbreuken aan het proportionaliteitsvereiste van artikel 8 EVRM waartoe de wetgever zich gehouden moet achten komt er zo wel zeer bekaaid af.

Bescherming van verkeersgegevens in relatie tot andere categorieën van gegevens

Het Cybercrime Verdrag deelt computergegevens in drie categorieën in (zie ER overweging 136), namelijk abonneegegevens, verkeersgegevens en inhoudsgegevens (subscriber, traffic en content data), die elk in twee vormen voorkomen namelijk “stored or in process of communication”. Tot de abonneegegevens behoren blijkens artikel 18, derde lid CV onder meer gegevens, niet zijnde verkeers- of inhoudsgegevens betreffende het type en bijbehorende technische voorzieningen van de gebruikte communicatiedienst, de identiteit van de abonnee, telefoon- en toegangsnummer, rekeninginformatie en informatie over de locatie van de communicatieapparatuur. Volgens overweging 170 ER ziet de bevoegdheid van artikel 18 CV alleen op opgeslagen, reeds bestaande gegevens.

In de Wet Vorderen gegevens telecommunicatie (Staatsblad 2004, 15) wordt onderscheid gemaakt tussen gegevens over een gebruiker en gegevens over het telecommunicatieverkeer met betrekking tot die gebruiker. De bevoegdheid van artikel 126n Sv omvat beide categorieën van gegevens en komt toe aan de Officier van Justitie. De minder vergaande bevoegdheid in artikel 126na voor opsporingsambtenaren ziet alleen op het vorderen van gegevens van een gebruiker.

Het CBP constateert dat de in het Cybercrime Verdrag beschreven abonneegegevens ook bepaalde verkeersgegevens omvatten als bedoeld in de Wet vorderen gegevens telecommunicatie. Het conceptwetsvoorstel gaat aan deze inconsistentie voorbij.

In het Wetsvoorstel Bevoegdheden vorderen gegevens (29441) wordt weer een ander onderscheid gehanteerd namelijk tussen identificerende gegevens, andere dan identificerende gegevens en gevoelige gegevens. Het Cybercrime Verdrag kent die laatste categorie weer niet. Anderzijds omvat de categorie abonneegegevens in het Cybercrime Verdrag zowel identificerende gegevens als andere dan identificerende gegevens als bedoeld in wetsvoorstel 29 441. In het laatstgenoemde wetsvoorstel stelt de wetgever zich op het standpunt dat waar de bevoegdheden de Wet Vorderen gegevens telecommunicatie ophouden, de bevoegdheden van wetsvoorstel 29 441 kunnen worden toegepast (MvT, nr. 3, p. 14: zie aldaar overigens ook het beoogde beschermingsregime voor opgeslagen e-mailberichten). Voor bepaalde gegevens ontstaan daarmee verschillende regimes, elk voorzien van eigen voorwaarden en waarborgen. Het CBP dringt in het licht van het voorgaande aan op een nadere afgrenzing van bevoegdheden. De implementatie van het Cybercrime Verdrag is de aangewezen gelegenheid om mogelijkheden om op andere bevoegdheden terug te vallen uit te sluiten. Dat kan alleen door diverse bepalingen nogmaals in samenhang te bezien, waarbij het Cybercrime Verdrag richtinggevend dient te zijn.

In het Cybercrime Verdrag worden bepaalde verkeersgegevens net zo gevoelig geacht als de inhoud van het verkeer. Het ER nodigt uit tot reflectie op dat onderwerp. In het conceptwetsvoorstel is daaraan ten onrechte nog geen gehoor gegeven. Overigens acht het CBP de gevoeligheidsbenadering slechts in zoverre adequaat dat het communicatiegeheim niet ziet op de mate waarin de inhoud van de communicatie informatie bevat die iets zegt over de persoon van een deelnemer aan de communicatie, als wel op het vertrouwelijke karakter van het communiceren als zodanig. Daarnaast blijft het CBP, anders dan de wetgever, van oordeel dat het uitgangspunt dat aan verkeersgegevens de bijzondere grondrechtelijke bescherming van het communicatiegeheim geheel moet worden ontzegd onjuist is. Het CBP verwijst naar het standpunt van 6 maart 2001 van zijn voorganger, de Registratiekamer, ten aanzien van het kabinetsstandpunt op het advies van de Commissie "Grondrechten in het digitale tijdperk" voor zover dit artikel 13 van de Grondwet betrof (z2000-1221.01).

5. Tot wie de vordering zich richt

De vorderingen als omschreven in het concept wetsvoorstel in artikel 126n, achtste lid, Sv, artikel 126nh, eerste lid, Sv, artikel 126u, achtste lid, Sv en artikel 126ui, eerste lid, Sv worden gedaan aan de aanbieder van een openbaar telecommunicatienetwerk of -dienst, dan wel -naar het CBP aanneemt: indien het een niet openbaar telecommunicatienetwerk -of dienst, dan wel geautomatiseerd werk betreft- degene van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot de gegevens waarop de vordering betrekking heeft. Het Cybercrime Verdrag schrijft niet voor aan wie dergelijke vorderingen gericht moeten kunnen worden. Het betreft hier derhalve een eigen keuze van de Nederlandse wetgever.

Het CBP heeft bezwaren tegen de keuze vorderingen in de sfeer van besloten netwerken te koppelen aan de -feitelijke- toegang tot de te verkrijgen gegevens. Het CBP adviseert u in plaats daarvan te bepalen dat vorderingen gericht dienen te zijn tot verantwoordelijken voor de verwerking van de te verkrijgen gegevens, een en ander in de zin van de Wet bescherming persoonsgegevens (WBP). Het verdient overweging de positie van bewerkers in de zin van de WBP daarbij nader te bezien.

Het CBP heeft in deze zin reeds geadviseerd op 18 oktober 2001 (z2001-0735) met betrekking tot bevoegdheden tot het vorderingen van gegevens (wetsvoorstel 29 441). Naar dat advies verwijst het CBP hier dan ook. Aangehaald zij hier het volgende: het CBP is er niet van overtuigd dat bij de uitoefening van de vorderingsbevoegdheden andere gegevens dan persoonsgegevens in het geding kunnen zijn, ten aanzien waarvan geen verantwoordelijke in de zin van de WBP kan bestaan. Ware dit al een reëel bezwaar dan zou ten aanzien van andere gegevens dan persoonsgegevens bovendien eenvoudig een ander adressaat van de vordering gekozen kunnen worden. Voorts brengt het hebben van toegang tot gegevens niet automatisch mee dat ook de feitelijke en juridische mogelijkheden bestaan om de gegevens ook daadwerkelijk te verstrekken teneinde aan een vordering te voldoen.

Het CBP voegt daar in dit verband het volgende aan toe. Ten aanzien van openbare telecommunicatienetwerken - en diensten worden vorderingen gericht aan aanbieders, terwijl

ook daar denkbaar zou zijn dat van eenieder die toegang heeft tot de gegevens gevorderd zou kunnen worden tot verstrekking van die gegevens. Het CBP ziet voor dit onderscheid geen rechtvaardiging, temeer daar in de toelichting in plaats van het hebben van toegang tot gegevens herhaaldelijk wordt gesproken over de 'houder van de gegevens', welke terminologie overeenkomt met de aanduiding in Wet persoonsregistraties van degene die thans in de WBP verantwoordelijke is. Daarenboven spreekt de conceptmemorie van toelichting, waar het de bevrozing van gegevens betreft, op pagina 22 over de houder die 'beschikkingsmacht' over de gegevens heeft. Beschikkingsmacht wordt daarbij verstaan als het beschikken over de technische mogelijkheden. Naar de mening van het CBP wordt reeds daarmee onderkend dat het hebben van toegang niet op één lijn te stellen is met het (kunnen) voldoen aan een vordering. Dit geldt niet alleen voor de bevoegdheid tot bevrozing van gegevens, maar ook andere bevoegdheden, zoals het verstrekken van gegevens.

Als het naar de opvatting van de wetgever al niet past bij de vorderingsbevoegdheden het begrippenkader van de WBP te volgen, zal de wetgever op zijn minst zo nauwkeurig mogelijk in de wet hebben te formuleren wat in zijn bedoeling ligt. Voor de bevrozingsbevoegdheid houdt dit derhalve in dat deze bevoegdheid slechts zou kunnen worden uitgeoefend jegens de houder van gegevens of degene die beschikkingsmacht heeft over de gegevens, in plaats van degene die toegang heeft tot gegevens.

In dit kader adviseert het CBP u tevens tot bezinning op de mogelijke implicaties van een ruime kring van personen en instanties tot wie vorderingen zich kunnen richten. Een dergelijke complicatie kan zich bijvoorbeeld voordoen in het geval dat een verantwoordelijke tevens verdachte dan wel verschoningsgerechtigde is. Kunnen de gegevens dan niettemin worden gevorderd van de persoon die toegang tot de gegevens heeft? En geldt dat ook als die persoon niet onder zijn gezag staat?

In het verlengde daarvan ligt de vraag wat onder rechtmatige toegang verstaan dient te worden. Dit is niet alleen een kwestie van pieteit met degene van wie gegevens gevorderd worden, door deze niet met al te veel (feitelijke) inspanningen te belasten. Het is een principiële rechtsvraag die afweging door de wetgever behoeft: mag binnen de rechtmatige toegang tot bepaalde gegevensbestanden op het moment van de vordering iedere feitelijke vergaring geveerd worden? Dat leidt ertoe dat in de praktijk vorderingen tot de vraag zullen leiden hoever de rechtmatige toegang strekt, terwijl dergelijke vragen lang niet altijd tevoren tussen toegangsgerechtigde en verantwoordelijke zullen zijn besproken. Integendeel, toegang is veelal gekoppeld aan beperkte doeleinden. Het meewerken aan opsporingsonderzoeken zal daar vrijwel nooit onderdeel van uitmaken. Verplicht nu een vordering gegevens te bevrozen of te verstrekken tot een 'digitale huiszoeking' door de toegangsgerechtigde bij de verantwoordelijke, mits de toegangsgerechtigde daarbij de grenzen van zijn toegangsrecht maar niet overschrijdt?

Het CBP adviseert u, nu dergelijke vraagstukken pas meer uitgekristalliseerd kunnen worden benaderd in het concept wetsvoorstel, de kring van personen en instanties tot wie de vorderingen zich kunnen richten te beperken tot verantwoordelijken. Indien daar knelpunten in de praktijk uit

voortvloeien dienen de daarmee gepaard gaande implicaties nader gewogen te worden alvorens tot bepaalde uitbreiding alsnog kan worden besloten. Bij dit alles moet worden beseft dat naast de persoonlijke levenssfeer van burgers ook de rechtmatigheid van bewijsverkrijging met tussenkomst van particulieren onder de directe verantwoordelijkheid van met opsporing en vervolging van strafbare feiten belaste overheidsdienaren in het geding is.

6. Notificatie en geheimhoudingsplicht

De notificatieplicht van artikel 126bb Sv is ingevoerd bij de wet Bijzondere opsporingsbevoegdheden. Bij de eerste fase van de evaluatie van die wet is geconcludeerd dat zich gebreken voordoen in de naleving van die verplichting. Onduidelijk is in de praktijk wie genotificeerd moeten worden, wat de inhoud van de notificatieplicht is en op welk moment notificatie plaats moet vinden. In het verlengde van het voorgaande is het CBP er voorstander van ook op dit onderdeel zoveel mogelijk conform de WBP te normeren. Waar gegevens over personen worden verwerkt zonder dat die personen daarvan op de hoogte zijn, dient in adequate mogelijkheden tot bescherming van de persoonlijke levenssfeer te worden voorzien. Dat impliceert dat niet degene tot wie de vordering zich richt wordt genotificeerd, maar degene wie de gevorderde en verkregen gegevens betreffen, ongeacht of deze (achteraf) voor het onderzoek relevant zijn (gebleken).

Waar in het conceptwetsvoorstel ook telecommunicatie middels private netwerken onder het bereik van strafvorderlijke vorderingsbevoegdheden wordt gebracht, verdient ter voorkoming van grotere onduidelijkheden de invulling van het begrip betrokkene, waar het telecommunicatie betreft, onder artikel 126bb, tweede lid, onder b, Sv uitbreiding dan wel herziening. Uiteindelijk is, in lijn van het voorgaande, van belang dat genotificeerd wordt degene wiens persoonlijke levenssfeer bij uitoefening van de bijzondere opsporingsbevoegdheid in het geding is. In het geval van het vorderen van gegevens of het inbreken op communicatiegeheimen zal dat eerder de personen betreffen die communiceren, dan degenen tot wie de vordering zich richt of de verdachte in onderzoek.

Het conceptwetsvoorstel koppelt aan de notificatieplicht een verplichting tot geheimhouding omtrent al datgene wat omtrent de vordering bekend wordt in het belang van het onderzoek. Met de laatste woorden wordt de relativiteit van de geheimhoudingsplicht ten opzichte van het onderzoeksbelang tot uitdrukking gebracht. De conceptmemorie van toelichting ziet voor de afweging van het onderzoeksbelang ten opzichte van de belangen van betrokkenen –in de zin van de WBP- om kennis te krijgen van de verwerking van hen betreffende persoonsgegevens een hoofdrol voor de officier van justitie weggelegd. Het bevreemdt dan ook dat de uiteindelijke verantwoordelijkheid voor die afweging desalniettemin bij degene tot wie de vordering zich richt wordt gelegd. Het verdient –niet alleen systematisch, maar ook principieel- de voorkeur de officier van justitie de gehele verantwoordelijkheid te laten dragen voor de verwerking van gegevens, waartoe de officier van justitie door het doen van een vordering verplicht, inclusief de afscherming van de verwerking zelf door geheimhouding. Het CBP adviseert de mogelijkheid te creëren bij het doen van de vordering te bepalen dat geheimhouding betracht dient te worden en de verplichting die geheimhoudingsplicht op te heffen, zodra die niet langer noodzakelijk is. Dit

leidt ertoe dat voor de betrokkene niet kenbare gegevensverwerkingen uitzondering blijven in plaats van uitgangspunt worden. Transparantie is een van de beginselen van gegevensbescherming die ook aan de WBP ten grondslag ligt. Uitsluitend indien het onderzoeksbelang, dan wel gewichtige belangen van derden daartoe noodzaken kan op het uitgangspunt van transparantie jegens de betrokkene een uitzondering gemaakt worden, hetgeen in beginsel een afweging van geval tot geval vergt.

7. Conclusie

Concluderend is het CBP van mening dat het Cybercrime Verdrag maatgevend dient te zijn voor het Nederlandse stelsel van strafbepalingen en strafvorderlijke bevoegdheden ter bestrijding van criminaliteit in verband met elektronische netwerken en het vergaren van elektronisch bewijs.

Het CBP adviseert u:

- Zowel bestaande als in voorbereiding zijnde bevoegdheden aan het Cybercrime Verdrag te toetsen.
- Afwijkingen van het Nederlands stelsel in verhouding tot het verplichte minimum aan regelgeving van het Cybercrime verdrag, zowel waar het bestaand recht als komend recht betreft, uitdrukkelijk te motiveren, in het bijzonder in het licht van het Cybercrime verdrag en artikel 8 EVRM.
- De waarborging van het telecommunicatiegeheim te verzekeren enerzijds een sluitend stelsel van strafbaarstellingen van ongerechtvaardigde inbreuken daarop en anderzijds een effectief systeem van waarborgen in de regeling van strafvorderlijke bevoegdheden. De volgende onderdelen dragen daaraan bij.
- Overlap van bevoegdheden zoveel mogelijk te voorkomen.
- Het aantal onderscheidingen in categorieën van gegevens te minimaliseren.
- Uitdrukkelijk uitspraak te doen onder welke categorie van gegevens een opgeslagen e-mail bericht bij een internet service provider valt
- Verkeersgegevens op gelijke wijze te beschermen als de inhoud van communicatie.
- Ongerechtvaardigde inbreuken op het recht vertrouwelijk te communiceren in besloten netwerken op gelijke wijze strafbaar te stellen als ongerechtvaardigde inbreuken op het recht vertrouwelijk te communiceren middels openbare netwerken met inachtneming van de eigen aard van interne netwerken, waarbij aan de positie van de rechthebbende nadere beperkingen dienen te worden gesteld.
- Inbreuken op het recht vertrouwelijk te communiceren middels interne netwerken met strengere waarborgen te omkleden, ter bescherming van de belangen van degene die middels een besloten netwerk plegen te communiceren en de aard die dergelijke communicatie kan hebben: zakelijke belangen, zoals bedrijfsgeheimen, bijzondere vertrouwensrelaties en dergelijke.
- Te bepalen dat vorderingen gericht dienen te worden tot verantwoordelijken in de zin van de Wet bescherming persoonsgegevens.
- Geheimhouding uitzondering in plaats van uitgangspunt te laten zijn.

- Duidelijker te specificeren ten opzichte van wie notificatie en de verplichting tot geheimhouding gelden, waarover deze zich uitstrekken en welke termijnen daarbij in acht genomen dienen te worden.

Tot slot dringt het CBP aan op grondige voorlichting van de verschillende maatschappelijke sectoren die naar verwachting regelmatig met vorderingen vanwege politie en justitie tot interceptie van (tele)communicatie geconfronteerd zullen worden.

Het CBP houdt zich gaarne bereid zijn advies nader toe te lichten.

Hoogachtend,

mr. U. van de Pol
waarnemend voorzitter