

Vergaderjaar 2001–2002

28 366

Gegevensvergaring in strafvordering

Nr. 1

BRIEF VAN DE MINISTER VAN JUSTITIE

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 1 mei 2002

Bij brief van 19 juni 2001 zond ik u het rapport Gegevensvergaring in strafvordering van de Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij (Just01-524) toe. Over het rapport zijn in de afgelopen maanden 12 adviezen ontvangen. Met deze adviezen is bij het opstellen van het kabinetsstandpunt rekening gehouden.

Bij de opsporing van misdrijven spelen gegevens die bij derden beschikbaar zijn een onmisbare rol. Deze rol neemt toe. Ten eerste omdat er als gevolg van de ontwikkelingen op het gebied van de informatie- en communicatietechnologie steeds meer gegevens beschikbaar zijn bij instellingen en bedrijven over de personen die van hen diensten of producten afnemen, of van wie zij om andere redenen gegevens verwerken. Wanneer deze gegevens kunnen bijdragen aan de opsporing van strafbare feiten is het voor de instanties die belast zijn met de opsporing van belang om over deze gegevens de beschikking te kunnen krijgen. De tweede reden waarom gegevens steeds belangrijker worden voor de opsporing is omdat informatie steeds vaker nog slechts in geautomatiseerde vorm beschikbaar is, zodat de inbeslagneming van bescheiden in betekenis voor de opsporing afneemt. Hierdoor ontstaat er in de opsporingspraktijk een steeds grotere behoefte aan om de beschikking te kunnen krijgen over geautomatiseerde gegevens. Tegelijkertijd heeft het privacyrecht zich verder ontwikkeld en is de bescherming van persoonsgegevens toegenomen. Het persoonsgegeven is gejuridiseerd. Verstrekking ten behoeve van de opsporing is niet zondermeer toegestaan. Gelet op deze ontwikkelingen behoeft de gegevensvergaring voor de opsporing van strafbare feiten een eigen zelfstandige regeling in het Wetboek van Strafvordering. Het rapport van de commissie biedt hiervoor het kader.

Hierbij zendt het kabinet zijn standpunt over het rapport en over de daarin opgenomen aanbevelingen.

De Minister van Justitie,
A. H. Korthals

Kabinetsstandpunt over het rapport Gegevensvergaring in strafvordering van de Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij

Inhoud:

| | |
|---|-----------|
| Inleiding | 3 |
| 1. Hoofdlijn van het rapport | 3 |
| 2. Algemene reactie op het rapport | 4 |
| 3. Uitgangspunten voor nieuwe wetgeving | 5 |
| 4. De voorgestelde bevoegdheden | 11 |
| 5. Aanvullende waarborgen | 22 |
| 6. Verhouding tot andere wetsvoorstellen | 27 |
| 7. Conclusie | 31 |
| Bijlage: beknopte samenvatting van de adviezen | 32 |

Inleiding

De Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij had tot taak¹ te komen tot uitgangspunten voor de wetgeving voor de strafvorderlijke gegevensvergaring in de informatiemaatschappij. Zij diende te bezien welke vormen van gegevensvergaring en -bewerking voor de strafvordering noodzakelijk zijn en regeling behoeven in het Wetboek van Strafvordering.

De achtergrond van deze opdracht aan de Commissie zijn de veranderingen die zich als gevolg van de ontwikkelingen op het gebied van de informatie- en communicatietechnologie voordoen in de wijze waarop gegevens worden verwerkt en de wijze waarop de instanties die belast zijn met de opsporing van strafbare feiten gegevens kunnen vergaren. Instellingen en bedrijven beschikken over steeds meer en steeds beter toegankelijke gegevens over de personen die van hen diensten of producten afnemen, of van wie zij om andere redenen gegevens verwerken. Wanneer gegevens over personen kunnen bijdragen aan de opsporing van strafbare feiten is het voor de instanties die belast zijn met de opsporing van strafbare feiten van belang om over deze gegevens de beschikking te kunnen krijgen.

De Commissie bracht op 14 mei 2001 haar rapport uit. Het kabinet heeft veel waardering voor de wijze waarop de Commissie haar taak heeft uitgevoerd. De Commissie heeft een veelomvattend rapport opgesteld.

1. Hoofdpijn van het rapport

De gegevens die derden over personen en hun handelingen bewaren, kunnen van grote betekenis zijn voor het strafvorderlijk onderzoek. In dit kabinetsstandpunt wordt gesproken van de houders van gegevens, waarmee bedoeld wordt op een ieder die toegang heeft tot gegevens. Sectoren die ten behoeve van de opsporing van strafbare feiten veelvuldig bevestigd worden zijn de communicatiesector, de sector transport en mobiliteit, de sector financiële dienstverlening en de overheid. Doel van de gegevensvergaring is bijvoorbeeld te komen tot vaststelling van de identiteit, geld- en goederenstromen, het vermogen of het relatienetwerk van een persoon.

In de praktijk doen zich daarbij de volgende knelpunten voor. In de eerste plaats is vaak niet duidelijk op basis van welke titel welke gegevens gevraagd en verstrekt kunnen en mogen worden. De regeling van bevoegdheden op dit terrein in het Wetboek van Strafvordering is fragmentarisch en niet toereikend. Dit heeft rechtsonzekerheid tot gevolg voor zowel de houders van gegevens als de tot opsporing bevoegde instanties. In de tweede plaats blijkt in de praktijk gegevensvergaring voor een belangrijk deel plaats te vinden op basis van vrijwillige medewerking. De houders van gegevens zijn in dat geval verantwoordelijk en aansprakelijk voor de verstrekking van de gegevens. Zij kennen echter niet alle feiten en omstandigheden die nodig zijn om af te kunnen wegen of de verstrekking van gegevens noodzakelijk is voor de opsporing. De tot opsporing bevoegde instanties kunnen en willen namelijk vaak geen vertrouwelijke opsporingsinformatie aan derden verstrekken.

Teneinde aan deze knelpunten tegemoet te komen concludeert de Commissie dat een nieuwe regeling in het Wetboek van Strafvordering nodig is. Als belangrijk uitgangspunt voor deze nieuwe regeling hanteert de Commissie dat de verantwoordelijkheid voor strafvorderlijke gegevensvergaring bij tot de opsporing bevoegde instantie dient te liggen: deze doet een vordering tot het verstrekken van gegevens en de houder van de gegevens is verplicht daaraan te voldoen. Een ander uitgangspunt is dat de regeling gebaseerd dient te zijn op een indeling in categorieën op basis van de aard van de gegevens, omdat de aard van de

¹ Artikel 2 van de Regeling Commissie strafvorderlijke gegevensvergaring in de informatiemaatschappij (Stcrt. 17 maart 2000, nr. 55).

gegevens bepalend is voor de vraag of en in welke mate sprake kan zijn van een inbreuk op de persoonlijke levenssfeer. Ook dient de regeling rekening te houden met de verschillende soorten handelingen die van een houder kunnen worden gevraagd. Naarmate een bevoegdheid dieper ingrijpt in de persoonlijke levenssfeer, dan wel meer inspanning vraagt van de houder van de gegevens, dient deze te berusten bij een hogere instantie en van zwaardere voorwaarden te zijn voorzien. De regeling dient daarbij te voldoen aan de eisen van artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM). Met inachtneming hiervan stelt de Commissie voor in het Wetboek van Strafvordering bevoegdheden op te nemen terzake van het vorderen van de houder van gegevens dat hij:

- identificerende gegevens verstrekt: naam, adres, woonplaats, geboortedatum, geslacht, en administratieve kenmerken zoals een klantnummer of rekeningnummer;
- ook andere dan identificerende gegevens verstrekt, met uitzondering van gevoelige gegevens;
- gegevens verstrekt die na het tijdstip van de vordering worden ontvangen en verwerkt (toekomstige gegevens);
- gevoelige gegevens verstrekt: persoonsgegevens betreffende onder andere iemands godsdienst of levensovertuiging, ras, politieke gezindheid of gezondheid;
- bepaalde gegevens bewerkt;
- bepaalde gegevens gedurende veertien dagen beschikbaar houdt.

De Commissie formuleert flankerende waarborgen betreffende onder andere de vergoeding van kosten die houders ter uitvoering van de vordering maken en het recht van belanghebbenden om beklag in te dienen tegen de vordering en tegen de kennisneming of het gebruik van gegevens die gevorderd zijn.

2. Algemene reactie op het rapport

Het rapport geeft een heldere beschrijving van de praktijk van de strafvorderlijke gegevensvergaring en een goede analyse van de knelpunten die zich daarin voordoen. Terecht wordt geconcludeerd dat nieuwe wetgeving nodig is. De Commissie formuleert hiervoor goede uitgangspunten. De voorstellen van de Commissie voor nieuwe bevoegdheden in het Wetboek van Strafvordering kunnen op hoofdlijnen worden overgenomen. Zoals in enkele adviezen naar voren is gekomen, is de reikwijdte van de voorgestelde bevoegdheden echter ruim, nu in beginsel geen gegevens daarvan zijn uitgesloten, behoudens gegevens die beschikbaar zijn bij beroepsverschoningsgerechtigden. Gelet op het belang van de opsporing van ernstige misdrijven acht het kabinet dit echter noodzakelijk. Hierna onder 3.2 wordt dit nader toegelicht. In het belang van de opsporing van ernstige misdrijven moet de officier van justitie in beginsel over elke soort gegevens de beschikking kunnen krijgen. Een voorwaarde hierbij is dat de bevoegdheden aan passende voorwaarden worden gebonden. De voorstellen van de commissie voorzien hierin. De voorstellen sluiten op dit punt aan bij de andere bevoegdheden in het Wetboek van Strafvordering. Dit neemt niet weg dat in het belang van de bescherming van de persoonlijke levenssfeer enkele beperkingen kunnen worden aangebracht in de door de Commissie voorgestelde bevoegdheden. Het kabinet meent dat de bevoegdheid tot het vorderen van identificerende gegevens en de bevoegdheid tot het vorderen van toekomstige gegevens beperkt moeten worden tot de houder van gegevens die anders dan ten behoeve van persoonlijk gebruik gegevens verwerkt. Ook dienen identificerende gegevens niet te kunnen worden gevorderd in het kader van een verkennend onderzoek. Met betrekking tot de bevoegdheid betreffende het bewerken van gegevens heeft het kabinet een ander wettelijk kader voor ogen dan

de commissie voorstelt. Dit zal nog afzonderlijk aan adviserende instanties worden voorgelegd.

Naast enkele beperkingen kunnen aanvullende waarborgen worden voorgesteld, teneinde een verantwoorde toepassing van de bevoegdheden en een zorgvuldige omgang met de aldus verkregen gegevens te bewaken. In dat verband wordt voorgesteld te bepalen dat de bevoegdheid tot het vorderen van identificerende gegevens alleen door daartoe aangewezen en geautoriseerde opsporingsambtenaren kan worden toegepast. Ook wordt de aanbeveling van het College Bescherming Persoonsgegevens gevolgd om op termijn in de Wet politieregisters een verplichting op te nemen tot het houden van een *audit* op de gegevensverwerking door de politie. Hiermee wordt uitvoering gegeven aan het project van zelf-evaluaties waarmee reeds een start is gemaakt. Daarnaast dienen politie en openbaar ministerie inzicht te geven in de aantallen malen dat de bevoegdheden worden toegepast.

In het navolgende wordt op al deze punten ingegaan. Een wetsvoorstel betreffende deze voorstellen zal worden voorbereid.

3. Uitgangspunten voor nieuwe wetgeving

3.1. Verantwoordelijkheid bij de tot opsporing bevoegde instantie

Zoals de meeste adviezen onderschrijft het kabinet het uitgangspunt dat de verantwoordelijkheid voor de gegevensvergaring bij de tot opsporing bevoegde instantie dient te liggen. In het Wetboek van Strafvordering dient daarom een stelsel van bevoegdheden tot het vorderen van gegevens te worden opgenomen, op grond waarvan houders van gegevens verplicht zijn gegevens te verstrekken. Een dergelijk stelsel komt het meest tegemoet aan de knelpunten in de praktijk en het voldoet het meest aan de eisen die op grond van artikel 10 van de Grondwet en artikel 8 van het EVRM gesteld moeten worden aan een regeling van bevoegdheden die een inbreuk op de persoonlijke levenssfeer kunnen inhouden. Als alternatief is in de literatuur¹ en in het advies van de Nederlandse Vereniging voor Rechtspraak² wel naar voren gekomen dat de vrijwilligheid bij gegevensverstrekking voorop dient te staan. Pas indien vrijwillige verstrekking geen resultaat oplevert, zou terug gevallen moeten kunnen worden op dwangmiddelen, dat wil zeggen op bevoegdheden van de tot opsporing bevoegde instanties tot het vorderen van gegevens. Dit alternatief biedt echter geen adequate oplossing voor de in de praktijk gesignaleerde knelpunten. De rechtsonzekerheid die het gevolg is van het ontbreken van een eenduidige regeling in het Wetboek van Strafvordering en de ongewenste verdeling van verantwoordelijkheden die aan de orde is bij de verstrekking van gegevens door medewerking op vrijwillige basis worden daarmee namelijk niet opgelost. Ook ziet dit alternatief eraan voorbij dat niet alleen de belangen van de houder van de gegevens en die van de opsporing in het geding zijn, maar dat tevens belangen van derden in het geding zijn. Het gaat hierbij om de personen op wie de gegevens betrekking hebben en van wie de persoonlijke levenssfeer in het geding kan zijn. Gelet op dit belang voorziet het alternatief van de vrijwilligheid niet in een regeling die voldoet aan de eisen van artikel 10 van de Grondwet en artikel 8 van het EVRM. Die eisen houden in dat bevoegdheden die een inbreuk op de persoonlijke levenssfeer kunnen inhouden bij wet moeten zijn voorzien, en dat die wettelijke regeling moet voldoen aan eisen van toegankelijkheid en voorzienbaarheid en waarborgen moet bevatten tegen willekeur. Indien vrijwilligheid voorop staat en de tot opsporing bevoegde instantie in overleg met de houder van de gegevens komt tot afspraken welke gegevens in een bepaald geval verstrekt zullen worden, is van een wettelijke regeling die aan deze eisen voldoet geen sprake. Door middel van een uitgewerkte regeling in het Wetboek van

¹ E.C. Mac Gillavry, Nederlands Juristenblad 31 augustus 2001, blz. 1411 ev. en E.C. Mac Gillavry, RM Themis 2002/1, blz. 27 ev., F. Kuitenbrouwer, NRC Handelsblad 6 februari 2002, G. Knigge, Delikt en Delinkwent, maart 2002, blz. 227 ev.

² Zie als bijlage de beknopte samenvatting van de adviezen.

Strafvordering zoals door de Commissie voorgesteld kan hieraan wel worden voldaan.

De kritiek¹ dat het door de Commissie voorgestelde stelsel van bevoegdheden niet zou passen binnen de systematiek van het Wetboek van Strafvordering wordt door het kabinet niet gedeeld. Deze kritiek stelt dat de voorgestelde bevoegdheden een inlichtingenplicht scheppen en dat in de voorstellen van de Commissie te weinig ruimte blijft bestaan voor de vrijwilligheid. Er wordt daarbij een vergelijking getrokken met de vrijheid van burgers tot het afleggen van een verklaring. Over het hoofd wordt evenwel gezien dat er een verschil is tussen het afleggen van een verklaring en het verstrekken van gegevens. Onder gegevens wordt verstaan: informatie die is vastgelegd of opgeslagen op een gegevensdrager, hetzij op schrift, hetzij in elektronische vorm. Ook de reeds in het Wetboek van Strafvordering opgenomen bevoegdheden tot het vorderen van gegevens uit een geautomatiseerd werk (125i) en het vorderen van de opgave van gegevens in het kader van het strafrechtelijk financieel onderzoek (126a) hanteren dit gegevensbegrip. Het verstrekken van gegevens houdt veelal in dat de gegevens voor een ander doel worden gebruikt dan waartoe ze door de houder van de gegevens zijn verwerkt. Om die reden dient een toetsing plaats te vinden met het oog op de afweging van enerzijds het belang dat zorgvuldig wordt omgegaan met persoonsgegevens en anderzijds het opsporingsbelang. Hiervoor biedt het Verdrag inzake gegevensbescherming van de Raad van Europa van 28 juni 1981 (verdrag tot bescherming van personen in verband met de geautomatiseerde verwerking van persoonsgegevens, Trb. 1988, 7) een kader. Artikel 9 van het verdrag bepaalt dat doelafwijkend gebruik mogelijk is, indien dit bij wet is voorzien en noodzakelijk is in een democratische samenleving in het belang van het bestrijden van strafbare feiten. Er dient dus voldaan te worden aan het noodzakelijkheids criterium. In de Nederlandse wetgeving is dit neergelegd in artikel 43 van de Wet bescherming persoonsgegevens. Het verstrekken van gegevens is – ook vanwege dit toetsingskader – niet hetzelfde als het afleggen van een verklaring, waarbij iemand uit eigen wetenschap feiten of omstandigheden meedeelt of vragen beantwoordt. Wel is enige nuancering mogelijk van het door de Commissie ingenomen standpunt² dat naast de in het Wetboek van Strafvordering op te nemen bevoegdheden geen ruimte meer zou bestaan voor het op vrijwillige basis vragen en verstrekken van gegevens. Gesteld zou namelijk kunnen worden dat het niet nodig is bevoegdheden uit het Wetboek van Strafvordering toe te passen indien de houder van gegevens bereid is op vrijwillige basis mee te werken aan het verstrekken van gegevens. In het bijzonder zou dit opgaan wanneer het gegevens betreft van de houder zelf, dan wel gegevens van derden die *geen* persoonsgegevens zijn. Vastgesteld kan echter worden dat deze gevallen zich in de praktijk nauwelijks voordoen. Bedacht moet bovendien worden dat ook indien het gaat om gegevens van derden die geen persoonsgegevens zijn, er nog altijd belangen van derden aan de orde kunnen zijn die verstrekking problematisch maken, bijvoorbeeld een contractuele geheimhoudingsplicht. Bij de gegevensvergaring ten behoeve van de opsporing gaat het in de praktijk meestal om persoonsgegevens van derden. Voor deze gegevens is de verstrekking op basis van vrijwilligheid geen goed alternatief. Hierbij is namelijk het belang van een derde in het geding, namelijk van degene op wie de gegevens betrekking hebben. Indien het gaat om het verstrekken van persoonsgegevens betreffende een derde, dient verstrekking – als gezegd – op vrijwillige basis daarom (indien verstrekking onvermijdbaar is met de doeleinden waarvoor de gegevens zijn verkregen, hetgeen meestal het geval is) plaats te vinden met inachtneming van de criteria van artikel 43 van de Wet bescherming persoonsgegevens. Dit artikel houdt in – zoals hiervoor al aan de orde kwam – dat de houder van de gegevens moet afwegen of de verstrekking van gegevens noodzakelijk is in het belang van de opsporing van strafbare feiten. De tot opsporing

¹ Zie noot 2.

² Paragraaf 9.9. van het rapport.

bevoegde instantie kan er niet zondermeer van uitgaan dat de houder van de gegevens zich bewust is van de afweging die hij dient te maken. De houder van de gegevens beschikt bovendien niet voor de daarvoor relevante informatie. Hier ligt nu juist een belangrijk knelpunt in de praktijk. Daarbij komt dat artikel 43 van de WBP maar ten dele een wettelijke regeling vormt die voldoet aan de hiervoor al genoemde eisen van toegankelijkheid en voorzienbaarheid en die waarborgen bevat tegen willekeur. Zeker indien het gaat om gegevens die diep ingrijpen in de persoonlijke levenssfeer wegen deze eisen van artikel 8 EVRM zwaar. Daarom is het ongewenst artikel 43 van de WBP te beschouwen als basis voor reguliere verstrekking van persoonsgegevens ten behoeve van de opsporing. Artikel 43 dient slechts betekenis te blijven behouden voor de gevallen, waarin het belang van de opsporing evident zwaarder weegt dan het belang van de bescherming van persoonsgegevens. Dan is ook voldaan aan het voorzienbaarheidsvereiste van artikel 8 van het EVRM.

Bespreking verdient nog of het mogelijk is in het Wetboek van Strafvordering een stelsel van bevoegdheden op te nemen als door de Commissie voorgesteld, maar dan zonder dat deze een verplichting tot verstrekking voor de houder van de gegevens zouden inhouden. Een dergelijke wettelijke regeling zou voldoen aan eisen van toegankelijkheid en voorzienbaarheid en zou waarborgen bevatten tegen willekeur. Wat echter niet opgelost zou worden is dat de houders van gegevens belast blijven met de afweging op grond van artikel 43 WBP en verantwoordelijk en aansprakelijk blijven voor de verstrekking. Zij blijven belast met een afweging die zij eigenlijk niet kunnen maken. (Contractuele) belangen van derden kunnen bovendien in de weg staan aan verstrekking op vrijwillige basis. De strafvorderlijke gegevensvergaring zou bovendien blijven berusten op de als uitzondering bedoelde bepaling van artikel 43, onderdeel b, WBP. Een verdeling van verantwoordelijkheden die inhoudt dat de tot opsporing bevoegde instantie beschikt over alle relevante informatie die nodig is om af te wegen of gegevens daadwerkelijk nodig zijn voor de opsporing, terwijl de onwetende houder van gegevens moet beslissen over het verstrekken van gegevens is, gelet op het voorgaande, in de ogen van het kabinet niet gewenst. Het kabinet hecht aan het uitgangspunt dat de verantwoordelijkheid voor de gegevensvergaring bij de tot opsporing bevoegde instanties dient te liggen. Het stelsel van bevoegdheden als door de Commissie voorgesteld vormt een consistent geheel, waarin de verantwoordelijkheden daar worden neergelegd waar zij thuishoren: zij worden gedragen door de met opsporing belaste overheidsinstanties en blijven niet berusten bij de particuliere houders van gegevens.

3.2. De eisen van artikel 10 Grondwet en artikel 8 EVRM

Hiervoor kwamen deze eisen al ter sprake. In deze paragraaf wordt hierop uitgebreider ingegaan en worden de voorstellen van de Commissie hieraan getoetst. Hierbij wordt er van uitgegaan dat de toepassing van de voorgestelde bevoegdheden tot het vorderen van gegevens een inbreuk op de persoonlijke levenssfeer kunnen inhouden. De mate waarin de persoonlijke levenssfeer van degene op wie de gegevens betrekking hebben in het geding kan zijn, verschilt evenwel per bevoegdheid. Zo kan de bevoegdheid tot het vorderen van identificerende gegevens in beperkte mate raken aan de persoonlijke levenssfeer, terwijl de bevoegdheid tot het vorderen van gevoelige gegevens in grote mate aan de persoonlijke levenssfeer kan raken. Ingevolge artikel 10 van de Grondwet dient een beperking van het recht op eerbiediging van de persoonlijke levenssfeer een basis te hebben in een wet in formele zin. Ingevolge artikel 8, tweede lid, van het EVRM is inmenging van enig openbaar gezag in de uitoefening van het recht op eerbiediging van de persoonlijke levenssfeer alleen toegestaan voor zover daarin bij de wet is voorzien en

dit in een democratische samenleving noodzakelijk is in het belang van enkele met name genoemde doelen, waaronder het voorkomen van strafbare feiten, hetgeen de opsporing daarvan omvat.

Bij de eis dat inmenging in het recht op bescherming van de persoonlijke levenssfeer noodzakelijk moet zijn in een democratische samenleving geldt een eigen beoordelingsruimte voor de nationale overheid. Deze eis van noodzakelijkheid heeft twee kanten. Ten eerste moet worden bezien of de bevoegdheid tot inmenging in de persoonlijke levenssfeer nodig is voor de strafrechtelijke handhaving, dat wil zeggen dat het individuele belang van de burger bij bescherming van de persoonlijke levenssfeer in bepaalde gevallen minder zwaar dient te wegen dan het algemene belang van de strafrechtelijke handhaving. Het dient, in het licht van de jurisprudentie van het Europese Hof voor de rechten van de mens, hierbij te gaan om een «*pressing social need*». Ten tweede dient bij de concrete toepassing van de bevoegdheid voldaan te zijn aan de eisen van proportionaliteit en subsidiariteit.

Met de Commissie is het kabinet van mening dat de voorgestelde bevoegdheden noodzakelijk zijn voor de strafrechtelijke handhaving. Daartoe bestaat een aantal redenen. De eerste reden is dat gegevens die bij derden beschikbaar zijn voor de opsporing van misdrijven onmisbaar zijn. In veel opsporingsonderzoeken spelen dergelijke gegevens een belangrijke rol. Het belang van gegevens voor de opsporing neemt bovendien sterk toe. Als gevolg van de ontwikkelingen op het gebied van de informatie- en communicatietechnologie zijn steeds meer gegevens beschikbaar bij instellingen en bedrijven over de personen die van hen diensten of producten afnemen, of van wie zij om andere redenen gegevens verwerken. Wanneer deze gegevens kunnen bijdragen aan de opsporing van strafbare feiten is het voor de instanties die belast zijn met de opsporing van belang om over deze gegevens de beschikking te kunnen krijgen. De tweede reden waarom de voorgestelde bevoegdheden nodig zijn is dat informatie steeds vaker nog slechts in geautomatiseerde vorm beschikbaar is, zodat de inbeslagneming van bescheiden in betekenis voor de opsporing afneemt. Ook hierdoor ontstaat er in de opsporingspraktijk een steeds grotere behoefte aan om de beschikking te kunnen krijgen over geautomatiseerde gegevens. De inbeslagneming van de fysieke dragers van geautomatiseerde gegevens zal daarbij vaak disproportioneel zijn, terwijl het motief om in beslag te nemen oneigenlijk is. Het gaat immers niet om de drager, maar om de gegevens. Door deze ontwikkelingen bestaat er in de opsporingspraktijk een toenemende behoefte aan het vorderen van geautomatiseerde gegevens, in ruimere mate dan thans op basis van artikel 125i Sv mogelijk is. De derde reden waarom de bevoegdheden nodig zijn, is dat het privacyrecht in de vorm van de bescherming van persoonsgegevens sterk ontwikkeld is. Het persoonsgegeven is gejuridiseerd, zodat verstrekking ten behoeve van de opsporing niet zondermeer is toegestaan. Normering hiervan is nodig. Gegevensvergaring ten behoeve van de opsporing is onmisbaar en behoeft, gelet op de voornoemde ontwikkelingen een eigen zelfstandige regeling. De wet dient een sluitend stelsel van bevoegdheden te bevatten voor de gegevensvergaring ten behoeve van opsporingsonderzoek. Aan de eis dat de bevoegdheden in een democratische samenleving noodzakelijk zijn in het belang van de opsporing is hiermee voldaan.

De eis dat inmenging in de wet is voorzien, houdt in dat in het nationale recht een regeling van een bevoegdheid tot inmenging in de persoonlijke levenssfeer is opgenomen en dat die regeling voor de burger voldoende toegankelijk en voorzienbaar is. Indien de regeling is opgenomen in de wet in formele zin, zoals hier het voornemen is, is voldaan aan de eisen dat de regeling in het nationale recht is opgenomen en dat die regeling voor de burger voldoende toegankelijk is.

De eis van voorzienbaarheid brengt met zich mee dat de regeling voldoende precies moet zijn geformuleerd, zodat de burger vooraf kan weten onder welke omstandigheden en voorwaarden de bevoegdheid mag worden toegepast. De regeling moet bovendien waarborgen bieden tegen willekeurige inmenging van de overheid in het persoonlijke leven van de burger en tegen misbruik van bevoegdheid (Kruslin en Huvig, EHRM 24 april 1990, NJ 1991, nr. 523). Deze eis weegt zwaarder naarmate een bevoegdheid meer ingrijpend is en heimelijk kan worden toegepast (P.G. en J.H. vs. Het VK, EHRM 25 september 2001). Voor de toetsing aan deze eisen is het volgende van belang. In de door de Commissie voorgestelde bevoegdheden is telkens de aard en de omvang van de bevoegdheid omschreven. Onderscheiden is in soorten gegevens en ook zijn de gevallen omschreven waarin de bevoegdheid kan worden toegepast en zijn de bevoegde autoriteiten aangewezen. Naarmate de bevoegdheid ingrijpender is, dient het te gaan om een verdenking van een ernstiger misdrijf en komt de bevoegdheid toe aan een hogere autoriteit. Hetzelfde geldt naarmate de bevoegdheid meer inspanning vraagt van de houder van de gegevens. Voor de gevallen waarin de bevoegdheden tot het vergaren van gegevens worden toegestaan, sluit de Commissie aan bij de gevallen die bekend zijn in het Wetboek van Strafvordering. Van belang is dat voor de meest ingrijpende bevoegdheden een machtiging van de rechter-commissaris is vereist. Bij de hierna afzonderlijk te bespreken bevoegdheden komt dit aan de orde. Met het voorgaande wordt bereikt dat de regeling voldoende precies is geformuleerd, zodat de burger vooraf kan weten onder welke omstandigheden en voorwaarden de bevoegdheid mag worden toegepast. Hiermee wordt voldaan aan de eis van voorzienbaarheid. Ook biedt de aanwijzing van de bevoegde autoriteiten een waarborg tegen willekeurige inmenging in de persoonlijke leven van de burger en tegen misbruik van bevoegdheid. Daarvoor zijn ook van belang de volgende door de Commissie voorgestelde waarborgen:

- Een vordering tot het verstrekken van gegevens dient altijd schriftelijk te zijn.
- De vordering dient een zo nauwkeurig mogelijke aanduiding te bevatten van de gegevens die worden gevorderd.
- Van de verstrekking van gegevens dient een proces-verbaal te worden opgemaakt waarin de feiten of omstandigheden waaruit blijkt dat is voldaan aan het vereiste van een verdenking van een strafbaar feit van een bepaalde ernst en de reden waarom de gegevens in het belang van het onderzoek worden gevorderd dienen te worden vermeld.
- Het proces-verbaal dient, voor zover het voor het onderzoek in de zaak van betekenis is, bij de processtukken te worden gevoegd.
- Aan de persoon over wie de gegevens zijn gevorderd, dient, zodra het belang van het onderzoek het toelaat, mededeling te worden gedaan over de toepassing van de bevoegdheid. Dit laatste geldt niet voor de bevoegdheid tot het vorderen van identificerende gegevens.

Hiermee sluit de Commissie aan bij de systematiek van andere in het Wetboek van Strafvordering opgenomen opsporingsbevoegdheden. Hiermee is voorzien in waarborgen tegen willekeurige inmenging van de overheid in het persoonlijke leven van de burger en tegen misbruik van bevoegdheid. Deze waarborgen bevorderen dat verantwoording moet en kan worden afgelegd over de toepassing van de bevoegdheden. Gelet op het voorgaande kan gesteld worden dat de voorgestelde regeling voldoet aan de eisen van artikel 10 van de Grondwet en artikel 8 van het EVRM.

3.3. Over welke personen mogen gegevens gevorderd worden?

Een belangrijk punt bij de voorgestelde bevoegdheden is de vraag over welke personen gegevens mogen worden vergaard. De Commissie stelt voor dat ook omtrent anderen dan de verdachte gegevens mogen worden

vergaard, omdat ook gegevens betreffende andere personen nodig kunnen zijn in het belang van het strafvorderlijk onderzoek. Het kan bijvoorbeeld gaan om gegevens van het slachtoffer of gegevens van derden waarmee de (potentiële) verdachte contacten heeft onderhouden en die kunnen bijdragen aan een goede afronding van het strafvorderlijk onderzoek. Het kabinet stemt op dit punt in met de voorstellen van de Commissie. Hiermee wordt aangesloten bij de bevoegdheden tot observatie, opnemen van vertrouwelijke communicatie en onderzoek aan telecommunicatie. Ook de bestaande bevoegdheden tot inbeslagneming en doorzoeking zijn niet beperkt tot de persoon van de verdachte of tot voorwerpen die van de verdachte zijn. De kring van personen van wie gegevens gevorderd kunnen worden, wordt afgegrensd door het belang van het opsporingsonderzoek. Alleen indien gegevens van personen redelijkerwijs kunnen bijdragen aan een goede afronding van het opsporingsonderzoek, kunnen deze gegevens worden vergaard. Bij gegevens van niet-verdachte personen zal hiervan doorgaans minder snel sprake zijn dan bij gegevens van de verdachte. Het beginsel van proportionaliteit brengt bovendien met zich mee dat aan de motivering voor het vorderen van gegevens over personen die niet verdachte zijn hogere eisen worden gesteld dan aan de motivering voor het vorderen van gegevens over de verdachte. Het beginsel van proportionaliteit houdt namelijk in dat de eventuele beperking van de persoonlijke levenssfeer van de persoon over wie gegevens vergaard worden in verhouding moeten staan tot het belang voor het opsporingsonderzoek. Een beperking van de persoonlijke levenssfeer van de verdachte is eerder gerechtvaardigd dan een beperking van de persoonlijke levenssfeer van een niet verdachte persoon. Het voorgaande brengt met zich mee dat de voorgestelde bevoegdheden weliswaar in beginsel kunnen worden toegepast ter verkrijging van gegevens betreffende niet verdachte personen, maar dat hierbij grotere terughoudendheid geboden is. In het proces-verbaal dient hierover verantwoording te worden afgelegd.

3.4. Van welke houders van gegevens mogen gegevens worden gevorderd?

In haar voorstellen brengt de Commissie een beperking aan in de kring van houders jegens wie de voorgestelde bevoegdheden kunnen worden toegepast. Identificerende gegevens mogen uitsluitend worden gevorderd van degene van wie, vanwege de activiteiten die hij verricht, kan worden aangenomen dat hij over identificerende gegevens zou kunnen beschikken. Wanneer er veel derden zijn die over de gezochte gegevens zouden kunnen beschikken dient een beperking van het aantal te bevragen derden te worden aangebracht. Indien bijvoorbeeld gezocht wordt naar het bedrijf waarbij een auto is gehuurd, zullen er veelal aanwezig zijn op grond waarvan een selectie kan worden gemaakt, bijvoorbeeld alleen de bedrijven in de omgeving waar de desbetreffende persoon woont. De bevoegdheid mag dus niet ongericht jegens derden worden toegepast, maar er hoeft geen redelijk vermoeden te bestaan dat de gegevens aanwezig zullen zijn. Bij de formulering van de bevoegdheid wordt dit aangeduid met de woorden: degene die daarvoor redelijkerwijs in aanmerking komt. De bevoegdheid tot het vorderen van andere dan identificerende gegevens kan alleen worden toegepast jegens de derde van wie op grond van feiten of omstandigheden vermoed kan worden dat hij tot de gewenste gegevens toegang heeft. Dit is een zwaardere beperking. Dergelijke beperkingen voorkomen zogenaamde *fishing expeditions*: zouden ze ontbreken dan zouden de tot opsporing bevoegde autoriteiten, op zoek naar gegevens over een bepaalde persoon, hun netten overall kunnen uitgooien. Ten eerste rijst hierbij de vraag of een dergelijke wijze van zoeken gerechtvaardigd zou kunnen zijn in het belang van het onderzoek. Ten tweede zou een dergelijke ruime werking van de bevoegdheden

ingrijpend zijn voor de personen op wie de gegevens betrekking hebben: zij kunnen niet onopgemerkt blijven. Ten derde zou het ook ingrijpend zijn voor de houders van gegevens: zij zouden verplicht zijn na te gaan of zij over de gevraagde gegevens beschikken, terwijl er geen aanwijzingen daartoe zijn. Dit zou tot een grote belasting leiden.

Hierna wordt bij de afzonderlijke bevoegdheden aangegeven welke betekenis deze beperkingen hebben voor de nieuwe regeling. Bij enkele bevoegdheden zal worden voorgesteld deze te beperken tot houders die anders dan ten behoeve van persoonlijk gebruik gegevens verwerken. De bevoegdheden moeten niet (zonder meer) kunnen worden toegepast indien de houder verdachte is of een zogenaamde verschoningsgerechtigde. Op dit punt wordt aangesloten bij de bestaande regelingen in het Wetboek van Strafvordering. In paragraaf 5 wordt hier nader op ingegaan.

Met de Commissie is het kabinet van oordeel dat de bevoegdheden in het Wetboek van Strafvordering in beginsel ook kunnen worden toegepast jegens overheidsdiensten. De bevoegdheden in het Wetboek van Strafvordering hebben voorrang boven de regelgeving betreffende verwerking van gegevens door overheidsdiensten en andere met publieke taken belaste instanties. Dit geldt ook daar waar in bijzondere wetten aan bepaalde personen een geheimhoudingsplicht wordt opgelegd. Ook gegevens bij toezichthoudende instanties, die zijn vergaard door de uitoefening van toezichthoudende bevoegdheden, kunnen door toepassing van de bevoegdheden in het Wetboek van Strafvordering ten behoeve van de opsporing worden verkregen. De verdenking van een strafbaar feit is een voldoende rechtvaardiging om, met het doel te komen tot opheldering van het strafbare feit, gericht gegevens te vergaren bij overheidsdiensten dan wel organisaties met een publieke toezichtstaak.

Het voorgaande is niet van toepassing indien in bijzondere wetten bijzondere regels zijn opgenomen voor de verstrekking van gegevens ten behoeve van strafvorderlijk onderzoek. Het kan hierbij gaan om regels voor gegevens die in beginsel altijd ten behoeve van strafvorderlijk onderzoek beschikbaar moeten kunnen zijn. Zo is voor bepaalde categorieën gegevens in de gemeentelijke basisadministratie bepaald dat politieambtenaren daartoe, ten behoeve van de goede vervulling van hun taak, toegang hebben. Voor de vergaring van deze gegevens is toepassing van strafvorderlijke bevoegdheden niet nodig. Het kan hierbij ook gaan om regels voor gegevens die niet zonder meer ten behoeve van strafvorderlijk onderzoek beschikbaar moeten kunnen zijn. Een voorbeeld hiervan zijn de gegevens van de Algemene Inlichtingen- en Veiligheidsdienst. Hierop zijn de strafvorderlijke bevoegdheden niet van toepassing.

4. De voorgestelde bevoegdheden

4.1. De bevoegdheid tot het vorderen van identificerende gegevens

De Commissie stelt voor in het Wetboek van Strafvordering een bevoegdheid op te nemen tot het vorderen van identificerende gegevens van een bepaalde persoon. Daaronder worden verstaan: naam, adres, woonplaats, geboortedatum, geslacht en administratieve kenmerken. Administratieve kenmerken betreffen de relatie tussen de persoon die onderwerp is van onderzoek en de houder van de gegevens. Het kan bijvoorbeeld gaan om een klantnummer, een nummer van een polis, een bankrekeningnummer, of een lidmaatschapsnummer. De bevoegdheid strekt ertoe dat de opsporingsambtenaar kan vaststellen wat de identiteit is van de persoon waarop het onderzoek is gericht. Ook dient de bevoegdheid ertoe dat gegevens vergaard kunnen worden die de opsporingsambtenaar in staat stellen vast te stellen of er een relatie bestaat tussen de persoon waarop het onderzoek is gericht en de houder van de gegevens. De Commissie stelt voor dat de bevoegdheid kan worden toegepast door de opsporingsambtenaar

in geval van verdenking van een strafbaar feit, dan wel in geval van verdenking dat in georganiseerd verband misdrijven worden beraamd of gepleegd die een ernstige inbreuk op de rechtsorde opleveren. Daarnaast zou de bevoegdheid toekomen aan de officier van justitie, indien dit noodzakelijk is voor de uitvoering van een verkennend onderzoek. De gegevens kunnen gevorderd worden van degene die daarvoor redelijkerwijs in aanmerking komt, dat wil zeggen elke houder die in verband met de activiteiten die hij verricht over de gevorderde gegevens zou kunnen beschikken. De bevoegdheid omvat de bevoegdheid te vorderen dat antwoord gegeven wordt op de zogenaamde ja/nee-vraag: de vraag of identificerende gegevens over een persoon beschikbaar zijn.

In enkele adviezen is kritiek geuit op dit voorstel. De Nederlandse Orde van Advocaten (NOvA) meent dat de bevoegdheid in feite een informatieplicht inhoudt en dat deze aan te weinig beperkingen is gebonden. De NOvA stelt als beperkingen voor dat de bevoegdheid alleen betrekking zou mogen hebben op gegevens van de verdachte, alleen gericht zou mogen worden tot de houder van wie redelijkerwijs vermoed wordt dat hij toegang heeft tot de gegevens en alleen in geval van verdenking van misdrijven als bedoeld in artikel 67 Sv. Dit laatste is ook door de Nederlandse Vereniging van Banken (NVvB) naar voren gebracht, die bovendien meent dat de tussenkomst van de officier van justitie nodig is. Het Verbond van Verzekeraars (VvV) bepleit zwaardere eisen aan de motivering waarom aan de houder gegevens worden gevorderd. Veel adviezen zijn negatief over het voorstel de bevoegdheid tot het vorderen van identificerende gegevens toe te staan in een verkennend onderzoek.

In reactie op deze bezwaren uit de adviezen kan het volgende worden opgemerkt over de door de Commissie voorgestelde bevoegdheid tot het vorderen van identificerende gegevens. Op de vraag of de bevoegdheid moet worden beperkt tot gegevens betreffende de verdachte is hiervoor al in gegaan onder 3.3.

Van welke houders van gegevens mogen identificerende gegevens worden gevorderd?

Hiervoor onder 3.4 is ingegaan op de vraag van welke houders gegevens gevorderd mogen worden. Onder 3.1. is bovendien betoogd dat er geen sprake is van een inlichtingenplicht. De opsporingsambtenaar kan de burger niet zomaar benaderen en hem open vragen stellen. De opsporingsambtenaar kan uitsluitend diegene benaderen waarvan aannemelijk is, vanwege de activiteiten die hij verricht, dat hij identificerende gegevens van een bepaalde persoon verwerkt. Aan deze houder van gegevens kunnen alleen limitatief omschreven identificerende gegevens worden gevorderd. Degene tot wie de vordering zich richt dient uitsluitend na te gaan of hij deze gegevens verwerkt en hij dient deze – indien dit het geval is – te verstrekken. De vordering dient schriftelijk te worden gedaan. Dat de opsporingsambtenaar zich uitsluitend kan richten tot degene die vanwege de activiteiten die hij verricht daarvoor in aanmerking komt, betekent dat het dient te gaan om een houder van gegevens die een bepaalde functie vervult in het maatschappelijk verkeer. Het kabinet meent dat het wenselijk is dit concreter tot uitdrukking te brengen in de bevoegdheid. Uitgesloten moet worden dat van iemand die uitsluitend persoonlijke contacten onderhoudt met de persoon op wie het onderzoek zich richt, gevorderd kan worden gegevens te verstrekken. Juist het vorderen van gegevens in de sfeer van persoonlijke contacten kan de indruk wekken dat het bij deze bevoegdheid om een soort informatieplicht zou gaan en kan als ingrijpend voor de persoonlijke levenssfeer worden ervaren. Daarnaast kan worden opgemerkt dat in de praktijk de verzoeken om identificerende gegevens, zoals ook uit het rapport van de Commissie

naar voren komt, vooral worden gericht tot bedrijven en andere instellingen, en dat deze geen betrekking hebben op uitsluitend persoonlijke contacten. Het belang voor de opsporingspraktijk bij identificerende gegevens ligt vooral bij de gegevens bij bedrijven en instellingen. Indien het belang van de bescherming van de persoonlijke levenssfeer enerzijds en het belang van de opsporing anderzijds tegen elkaar worden afgewogen is het gewenst de toepassing van deze bevoegdheid te beperken tot degene die anders dan ten behoeve van persoonlijk gebruik gegevens verwerkt. Dit betekent dat de bevoegdheid alleen kan worden aangewend jegens rechtspersonen en jegens natuurlijke personen in de uitoefening van een beroep of bedrijf. Het gaat daarbij om overheidsdiensten, verenigingen, professionele dienstverleners en instellingen die diensten verlenen op het terrein van cultuur, sport, hobby enzovoort, al dan niet op commerciële basis. Personen die als cliënt, afnemer van diensten of anderszins betrokken zijn bij deze instellingen weten of kunnen weten dat hun gegevens in verband daarmee verwerkt worden. Dergelijke gegevens liggen buiten de strikt persoonlijke sfeer. Gegevens die worden vastgelegd voor persoonlijk gebruik, als bedoeld in artikel 2, tweede lid, onder a, WBP vallen hiermee buiten de bevoegdheid. Identificerende gegevens die worden verwerkt ten behoeve van persoonlijk gebruik kunnen dan nog uitsluitend door de officier van justitie worden gevorderd, zoals hierna aan de orde zal komen.

Met deze beperking van de bevoegdheid wordt tegemoet gekomen aan de bezwaren in een aantal adviezen en publicaties en wordt de bevoegdheid meer toegespitst op de in de opsporingspraktijk bestaande behoefte.

Wie is bevoegd en in geval van welke strafbare feiten?

Enkele adviezen bepleiten de bevoegdheid niet toe te staan in geval van verdenking van een strafbaar feit, maar in geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid. Ook wordt in één advies bepleit dat niet de opsporingsambtenaar, maar de officier van justitie bevoegd zou moeten zijn.

Voor de vraag in welke gevallen de bevoegdheid tot het vorderen van identificerende gegevens moet zijn toegestaan is het van belang dat de categorie identificerende gegevens een beperkte categorie gegevens betreft die op zichzelf slechts in beperkte mate kan raken aan de persoonlijke levenssfeer en waarvan de vordering niet zeer belastend is voor de houder van de gegevens. Om die reden kan zij in meer gevallen zijn toegestaan dan de bevoegdheid tot het vorderen van andere dan identificerende gegevens. Daarnaast is van belang dat de zogenaamde identificerende gegevens de basis vormen van het opsporingsonderzoek, met name bij de start daarvan. Cruciaal is immers vast te kunnen stellen met welke personen men van doen heeft in het opsporingsonderzoek en verbanden te kunnen leggen tussen situaties en personen. Identificerende gegevens zijn ook nodig alvorens andere bevoegdheden kunnen worden toegepast. Het belang dat de tot opsporing bevoegde instanties bij deze categorie gegevens hebben is daarom groot. Om die reden dient de bevoegdheid beschikbaar te zijn voor een ruimere categorie strafbare feiten dan die is omschreven in artikel 67, eerste lid, Sv. De beschikbaarheid voor elk strafbaar feit lijkt echter – gelet op het beginsel van proportionaliteit – te ruim. Beperking van deze bevoegdheid tot de opsporing van misdrijven sluit beter aan bij de andere bevoegdheden in het Wetboek van Strafvordering. Om die reden meen ik dat het wenselijk is deze bevoegdheid te beperken tot de gevallen waarin sprake is van verdenking van een misdrijf. Omdat de categorie identificerende gegevens een beperkte categorie gegevens betreft, en gelet op de toedeling van andere bevoegdheden in het Wetboek van Strafvordering, is het niet nodig en niet gewenst de bevoegdheid tot het vorderen van identificerende gegevens bij een hogere autoriteit neer te leggen. Iedere opsporingsambtenaar

moet bevoegd zijn tot de toepassing van deze bevoegdheid, zeker nu toepassing van deze bevoegdheid is beperkt tot degene die gegevens verwerkt anders dan ten behoeve van persoonlijk gebruik. Het is wel gewenst de toepassing van de bevoegdheid in de praktijk te beperken tot daartoe geautoriseerde opsporingsambtenaren. Dit kan bevorderen dat bedrijven en instellingen waarvan gegevens worden gevorderd op een eenduidige wijze worden benaderd en dat desgewenst tot sectorale afspraken kan worden gekomen.

De «ja / nee vraag»

In afwijking van het voorstel van de Commissie, behoeft in de bevoegdheid niet te worden opgenomen dat antwoord gegeven moet worden op de zogenaamde ja/nee-vraag, de vraag of identificerende gegevens over een persoon beschikbaar zijn. Gesteld kan immers worden dat de bevoegdheid deze vraag te stellen en de plicht hierop te antwoorden inherent zijn aan de bevoegdheid de identificerende gegevens zelf te vorderen, met de daaraan verbonden plicht deze – indien beschikbaar – te verstrekken. Het opnemen van de ja/ nee vraag suggereert bovendien dat identificerende gegevens gevorderd kunnen worden ook indien geen enkele aanwijzing bestaat dat de houder over de gezochte gegevens zou kunnen beschikken. Weliswaar wordt met de Commissie ingestemd dat de bevoegdheid er mede toe strekt dat vastgesteld kan worden of er een relatie bestaat tussen de persoon waarop het onderzoek is gericht en de houder van de gegevens. De betekenis hiervan is echter dat hieromtrent zekerheid kan worden verkregen, daar waar eerst slechts van aanwijzingen sprake was.

Het verkennend onderzoek

Veel adviezen zijn negatief over het voorstel de bevoegdheid tot het vorderen van identificerende gegevens toe te staan in een verkennend onderzoek.

Met de Commissie kan worden ingestemd dat de categorie identificerende gegevens basaal zijn bij een strafrechtelijk onderzoek, ook bij een verkennend onderzoek. Het verkennend onderzoek richt zich op aanwijzingen dat binnen verzamelingen van personen misdrijven worden beraamd of gepleegd die een ernstige inbreuk op de rechtsorde opleveren. Op deze wijze kan worden vastgesteld op welke wijze sectoren in de samenleving onder invloed staan van de zware of georganiseerde criminaliteit en kan opsporing worden voorbereid. Daartoe kunnen op grote schaal persoonsgegevens worden vastgelegd die afkomstig zijn, hetzij uit open bronnen, hetzij op basis van vrijwillige medewerking, van particulieren. Het verkennend onderzoek is bij uitstek onderzoek naar gegevens uit bestaande persoonsregistraties. Alleen wanneer er ruimte is dergelijke gegevens te verkrijgen kan het tot goede resultaten leiden. Het vergaren van identificerende gegevens is daarbij van groot belang. De indruk bestaat dat binnen het verkennend onderzoek te weinig mogelijkheden bestaan tot het bijeenbrengen van gegevens die een goed verkennend onderzoek mogelijk maken. Nu de Commissie ook zelf echter aangeeft dat gekomen moet worden tot een scherpere afbakening van het verkennend onderzoek, dient hier eerst meer inzicht in te worden verkregen, alvorens tot een toekenning van bevoegdheden kan worden overgegaan. Om die reden dient op dit moment te worden afgezien van het toekennen van de bevoegdheid tot het vorderen van identificerende gegevens in een verkennend onderzoek. Wel dienen de ervaringen in de huidige praktijk met het verkennend onderzoek, alsmede met onderzoeksvormen die daaraan verwant zijn, verder in kaart te worden gebracht. Een gelegenheid hiervoor is de evaluatie van de wet bijzondere opsporingsbevoegdheden, die in 2003 zal worden afgerond.

4.2. Bevoegdheid tot het vorderen van ook andere dan identificerende gegevens

De Commissie stelt voor in het Wetboek van Strafvordering een bevoegdheid op te nemen tot het vorderen van ook andere dan identificerende gegevens, met uitzondering van gevoelige gegevens. De bevoegdheid kan worden toegepast door de officier van justitie in geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, Sv, dan wel in geval van verdenking dat in georganiseerd verband van misdrijven worden beraamd of gepleegd die een ernstige inbreuk op de rechtsorde opleveren. De gegevens kunnen gevorderd worden van degene van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot de gegevens.

De Nederlandse Orde van Advocaten (NOvA) meent dat deze bevoegdheid beperkt moet worden tot gegevens van de verdachte. Ook meent de NOvA dat de beperking dat de gegevens alleen kunnen worden gevorderd van degene van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot de gegevens, in feite geen beperking inhoudt, nu de bevoegdheid tot het vorderen van identificerende gegevens jegens een ruimere kring van houders kan worden toegepast.

In reactie hierop kan het volgende worden opgemerkt. Op de vraag of de bevoegdheid moet worden beperkt tot gegevens betreffende de verdachte is hiervoor al ingegaan onder 3.3.

De NOvA constateert terecht dat de drempel voor de toepassing van de bevoegdheid tot het vorderen van identificerende gegevens lager ligt dan de drempel bij de bevoegdheid tot het vorderen van ook andere dan identificerende gegevens. Indien er geen redelijk vermoeden bestaat, maar er zijn wel aanwijzingen dat de houder van de gegevens toegang heeft tot gegevens betreffende een bepaalde persoon, kan door toepassing van de bevoegdheid tot het vorderen van identificerende gegevens daaromtrent zekerheid verkregen worden. Dit is ook een functie van de bevoegdheid tot het vorderen van identificerende gegevens. De vordering identificerende gegevens is minder belastend voor de persoonlijke levenssfeer van degene op wie de gegevens betrekking hebben dan de vordering van andere dan identificerende gegevens. Om die reden kan een lagere drempel gelden, temeer nu voorgesteld wordt deze bevoegdheid te beperken tot de houder van gegevens die gegevens verwerkt anders dan ten behoeve van persoonlijk gebruik.

De voorgestelde bevoegdheid tot het vorderen van ook andere dan identificerende gegevens is de basisbevoegdheid in de voorstellen van de Commissie. De officier van justitie is in beginsel bevoegd tot het vorderen van alle denkbare gegevens, met uitzondering van de gevoelige gegevens, in geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, Sv. Voor de zeer beperkte categorie van de identificerende gegevens is daarnaast de opsporingsambtenaar zelfstandig bevoegd. De bevoegdheid houdt in dat de officier van justitie uitsluitend vooraf bepaalde gegevens kan vorderen: hij dient vooraf de gegevens zo nauwkeurig mogelijk te beschrijven. De bevoegdheid dient gericht te worden toegepast, op basis van een op feiten of omstandigheden gegrond vermoeden dat deze bepaalde gegevens bij de houder beschikbaar zijn. De bevoegdheid staat toe dat gegevens worden gevorderd omtrent een groep van personen. Wanneer bijvoorbeeld in de bagage van een vlucht op 10 april van Amsterdam naar Panama een pakket cocaïne is gevonden, kan de vordering van de passagierslijst van die vlucht eraan bijdragen dat de persoon die de bagage meebracht, kan worden achterhaald. Een vordering, niet gericht op een op voorhand bepaalde persoon, is in dit geval gerechtvaardigd omdat er een aanknopingspunt is voor een opsporingsonderzoek: er is cocaïne gevonden en dus een vermoeden van een

strafbaar feit. In een dergelijk geval worden terecht gegevens vergaard. Wanneer de vordering niet begrensd is door een op voorhand bepaalde persoon, dient er een andere begrenzing te zijn. Deze vloeit logisch voort uit het belang van het onderzoek. Blijvend bij het voorbeeld is het niet in het belang van het onderzoek alle passagierslijsten van 10 april te vorderen, maar dient te worden volstaan met de passagierslijsten naar Panama, of alleen de lijsten van de vluchten die vertrokken tussen bijvoorbeeld 10.00 en 12.00 uur. Nu de bevoegdheid betrekking kan hebben op een onbepaalde groep van personen, waaronder onverdachte personen, is het van belang dat voorzien is in een goede regeling voor het verdere gebruik en de vernietiging van de aldus verkregen gegevens. De Wet politieregisters bevat zo'n regeling. De gegevens die de officier van justitie verkrijgt door de toepassing van de bevoegdheid worden door de politie verwerkt en vallen onder het regime van de Wet politieregisters. Hierna in paragraaf 5 wordt daarop ingegaan.

4.3. Bevoegdheid tot het vorderen van toekomstige gegevens

De Commissie stelt voor in het Wetboek van Strafvordering op te nemen een bevoegdheid tot het vorderen van zogenaamde toekomstige gegevens: gegevens die op het moment van de vordering nog niet bestaan en pas na het tijdstip van de vordering zullen ontstaan en voor het eerst worden verwerkt. De hiervoor besproken bevoegdheden hadden allemaal betrekking op zogenaamde historische gegevens. De Commissie heeft dat in de formulering van de bevoegdheden tot uitdrukking gebracht met de woorden «opgeslagen of vastgelegde gegevens». Bij de bevoegdheid tot het vorderen van toekomstige gegevens gaat het in beginsel om dezelfde gegevens als bij historische gegevens. Het verschil is het moment van eerste verwerking in relatie tot het moment van de vordering. De voorwaarden die de commissie aan deze bevoegdheid verbindt zijn dezelfde als de voorwaarden die worden verbonden aan de bevoegdheid tot het vorderen van historische gegevens, die hiervoor onder 4.2 zijn besproken. Het doel van de bevoegdheid is dat deze kan voorkomen dat een vordering tot het verstrekken van gegevens door de officier van justitie telkens moet worden herhaald, bijvoorbeeld indien de officier van justitie elke week gegevens wil vorderen over de afgelopen week. Een dergelijke herhaling zou zowel voor de officier van justitie als voor de houder van de gegevens meer lasten met zich meebrengen. Ook heeft de bevoegdheid tot doel dat gevorderd kan worden dat gegevens direct na eerste verwerking worden verstrekt. Dit laatste kan in de voorstellen van de Commissie echter alleen onder de voorwaarde dat het onderzoek dit dringend vordert en nadat hiertoe een machtiging van de rechter-commissaris is verleend. Dezelfde voorwaarden gelden voor de vordering dat de gegevens telkens binnen een bepaalde periode na verwerking worden verstrekt.

Het College Bescherming Persoonsgegevens (CBP) meent dat de bevoegdheid tot het vorderen van toekomstige gegevens gericht moet worden ingezet en beperkt moet worden tot gegevens betreffende de verdachte. De Nederlandse Vereniging van Banken (NVvB) meent dat het direct doorgeleiden van toekomstige gegevens (monitoren) teveel inspanningen zal vergen van de banken.

In reactie hierop wordt het volgende opgemerkt. Er dient onderscheiden te worden in het vorderen van toekomstige gegevens zonder dat direct verstrekt moet worden en het vorderen terwijl wel direct verstrekt moet worden, het zogenaamde monitoren. Indien bijvoorbeeld fraude met een pasje wordt onderzocht, kan het zeer aan de opheldering van het strafbare feit bijdragen wanneer van de

houder van gegevens kan worden gevorderd direct melding te doen, wanneer, waar en op welke wijze het pasje wordt gebruikt.

Een directe doorgeleiding zal echter in beginsel extra belastend zijn voor de houder, omdat hij dan zelf moet opletten wanneer de gegevens ontstaan en voor het eerst verwerkt worden, waarna zij direct verstrekt moeten worden. Ook zal een dergelijke verwerking van gegevens door de houder veelal verder afstaan van het doel waartoe hij de gegevens in het kader van zijn normale activiteiten verwerkt. Dergelijke inspanningen dienen beperkt te worden tot de dringend noodzakelijke gevallen. Om deze redenen zijn hieraan zwaardere voorwaarden verbonden. Een uitgangspunt dat hiervoor al aan de orde kwam, is namelijk dat naarmate de toepassing van een bevoegdheid meer inspanning vraagt van de houder van de gegevens, deze dient te berusten bij een hogere autoriteit en van zwaardere voorwaarden dient te zijn voorzien. Daarin is bij deze bevoegdheid dan ook voorzien: de bevoegdheid kan alleen worden toegepast indien het onderzoek het dringend vordert en na machtiging van de rechter-commissaris. De rechter-commissaris zal bij de afweging of hij tot machtiging zal overgaan, dienen te toetsen of sprake is van een dringend onderzoeksbelang.

De NVvB meent dat het direct doorgeleiden van toekomstige gegevens (monitoren) teveel inspanningen zal vergen van de banken. De concrete omstandigheden van het geval en de aard van de gegevens die gevorderd worden, zullen bepalend zijn voor de vraag welke inspanningen nodig zijn. De officier van justitie en de rechter-commissaris zullen bij hun beoordeling van de toepassing van deze bevoegdheid deze inspanningen moeten meewegen. Van de houder van gegevens mogen geen onevenredige inspanningen worden gevraagd; de gevraagde handelingen dienen binnen het bereik van de normale activiteiten te vallen. De kosten die gemoeid zijn met het verstrekken van toekomstige gegevens dienen voor rekening van de strafvorderlijke overheid te komen.

Het College Bescherming Persoonsgegevens (CBP) stelt voor dat toekomstige gegevens alleen zouden mogen worden gevorderd voor zover zij de verdachte betreffen. Inderdaad ligt het in de rede te veronderstellen dat er in het belang van de opsporing geen belang bestaat bij toekomstige gegevens van niet-verdachte personen. Immers de opsporing is niet gericht op het in beeld brengen van niet-verdachten, maar op het in beeld brengen van verdachten. Het kan evenwel toch nodig zijn voor dat laatste doel, ook toekomstige gegevens over niet-verdachten te vergaren. Indien de verdachte bijvoorbeeld – door gebruik van diens codes dan wel pasjes – de bankrekening van een ander gebruikt, dan wel een ander handelingen laat verrichten, dan kan het in het belang van het onderzoek zijn gegevens betreffende die ander te vergaren. Dezelfde redenen als die hiervoor in paragraaf 3.3 zijn gegeven, spelen ook hier een rol. Om die reden lijkt deze door het CBP voorgestelde beperking minder gewenst.

Er is geen sprake van dat deze bevoegdheid zou kunnen inhouden dat van de houder van gegevens zou kunnen worden gevorderd dat hij gegevens verwerkt die hij normaliter niet verwerkt, dan wel dat hij verplicht zou kunnen zijn tot het verwerken of vergaren van gegevens. In enkele publicaties¹ werd de suggestie gedaan dat burgers verplicht zouden kunnen worden tot het bijhouden van een dagboek. Nog daargelaten dat in het geval van een dagboek moeilijk sprake kan zijn van een redelijk vermoeden bij de officier van justitie dat de houder van gegevens toegang heeft tot bepaalde gegevens – hoe zou hij kunnen vermoeden dat er een dagboek is, laat staan wat daarin geschreven wordt – is dit niet de aard van de bevoegdheid. De bevoegdheid strekt slechts tot het vorderen van vooraf bepaalde gegevens die op een later tijdstip toch al zouden worden verwerkt, en niet tot het vorderen dat bepaalde gegevens worden verwerkt of vergaard die normaliter niet zouden worden verwerkt. In de

¹ Zie noot 2, Mac Gillavry en Kuitenbrouwer.

formulering van de bevoegdheid is hieraan mede uitdrukking gegeven doordat in de bevoegdheid tot het vorderen van toekomstige gegevens wordt terugverwezen naar de bevoegdheid tot het vorderen van reeds opgeslagen of vastgelegde gegevens.

De aard van de bevoegdheid tot het vorderen van toekomstige gegevens brengt met zich mee dat zij vooral van betekenis is indien een houder gegevens vanwege zijn reguliere activiteiten verwerkt. Alleen indien vanwege dergelijke activiteiten gegevens worden verwerkt, kan immers vermoed worden dat gegevens op een later tijdstip verwerkt zullen gaan worden. Het kabinet stelt daarom voor de bevoegdheid tot het vorderen van toekomstige te beperken tot de houders die anders dan ten behoeve van persoonlijk gebruik gegevens verwerken.

4.4. Bevoegdheid tot het vorderen van gevoelige gegevens

De Commissie stelt voor in het Wetboek van Strafvordering een bevoegdheid op te nemen tot het vorderen van gevoelige gegevens. De bevoegdheid kan worden toegepast door de officier van justitie indien het belang van het onderzoek dit dringend vordert, na machtiging door de rechter-commissaris, in geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, Sv dat gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert, dan wel in geval van verdenking dat in georganiseerd verband van misdrijven worden beraamd of gepleegd die een ernstige inbreuk op de rechtsorde opleveren. De gegevens kunnen gevorderd worden van degene van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot de gegevens.

Onder gevoelige gegevens worden verstaan: gegevens die vanwege hun aard een indringende inbreuk kunnen maken op de persoonlijke levenssfeer. Het gaat om de gegevens, bedoeld in artikel 16 van de Wet bescherming persoonsgegevens: gegevens over bijvoorbeeld iemands godsdienst, ras, politieke gezindheid, gezondheid of diens seksuele leven. Daarnaast gaat het om gegevens betreffende de inhoud van een e-mail die is opgeslagen bij een internetaanbieder.

Het College Bescherming Persoonsgegevens (CBP) brengt in zijn advies naar voren dat ook bij het vragen van identificerende gegevens sprake kan zijn van gevoelige gegevens, bijvoorbeeld indien adresgegevens worden gevraagd aan een kerkgenootschap. In de reactie van de Nederlandse Vereniging van Banken (NVvB) is de vraag gesteld welke bevoegdheid gehanteerd moet worden indien de gegevens die de officier van justitie vordert op grond van de hiervoor besproken bevoegdheid, gevoelige gegevens blijken te zijn.

In reactie zij opgemerkt dat de gevoelige gegevens zijn uitgezonderd van de bevoegdheid tot het vorderen van identificerende gegevens en de bevoegdheid tot het vorderen van andere dan identificerende gegevens, juist omdat – zoals het CBP terecht opmerkt – ook bij die bevoegdheden sprake kan zijn van gevoelige gegevens.

In deze bevoegdheden wordt bepaald dat de te vorderen gegevens geen betrekking mogen hebben op onder andere iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven of lidmaatschap van een vakvereniging. Dit betekent bijvoorbeeld dat van een kerkgenootschap, een vakvereniging of een vereniging van personen die een bepaalde aandoening hebben niet op basis van de bevoegdheid tot het vorderen van identificerende gegevens, gegevens gevorderd kunnen worden. Bij deze instellingen is vooraf duidelijk dat het om gevoelige gegevens gaat. Bij ander instellingen ligt dat anders. Indien de officier van justitie bijvoorbeeld gegevens vordert betreffende de financiële transacties van een persoon in een bepaalde periode, dan dient hij de alge-

mene bevoegdheid toe te passen. Immers gegevens over financiële transacties zijn geen gevoelige gegevens. Indien tussen deze gegevens, gegevens zitten over giften aan een levensbeschouwelijke organisatie, kunnen deze gegevens op zichzelf wel beschouwd worden als gevoelige gegevens, maar deze kunnen dan toch verstrekt worden op grond van de algemene bevoegdheid: pas achteraf kan worden vastgesteld dat tussen de gevraagde gegevens, gevoelige gegevens zaten. Bij de toepassing van deze opsporingsbevoegdheid is, net als bij verschillende andere opsporingsbevoegdheden, vooraf niet geheel te voorzien wat het resultaat zal zijn. Dit maakt de toepassing van de bevoegdheid niet achteraf onrechtmatig. Het resultaat kan, indien het relevant is voor het betreffende opsporingsonderzoek, ook verder worden verwerkt.

Tot de gevoelige gegevens behoren ook de inhoud van een e-mail die is opgeslagen bij aanbieder van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst. Gegevens daarover mogen alleen worden gevorderd voor zover «de 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.» Hierbij wordt het wetsvoorstel computercriminaliteit gevolgd (Kamerstukken II 1998/99, 26 671, nr. 2) omvat naast voorstellen tot wijziging). Een zelfde soort beperking geldt nu reeds ingevolge artikel 125i, tweede lid. De Nederlandse Orde van Advocaten (NOvA) vraagt zich af wie beoordeelt of e-mail betrekking heeft op de verdachte. Deze beoordeling ligt bij de officier van justitie. De door de NOvA genoemde beperking houdt in dat de officier van justitie alleen gegevens uit een e-mail afkomstig van of geadresseerd aan de verdachte kan vorderen, tenzij hij aanwijzingen heeft dat ook andere e-mail klaarblijkelijk op de verdachte betrekking heeft.

4.5. Bevoegdheid tot het bewerken van gegevens

De Commissie stelt voor in het Wetboek van Strafvordering een bevoegdheid op te nemen tot het vorderen van een bewerking van gegevens. De Commissie stelt voor dat de bevoegdheid kan worden toegepast door de officier van justitie indien het belang van het onderzoek dit dringend vordert, na machtiging door de rechter-commissaris, in geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, Sv dat gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert, dan wel in geval van verdenking dat in georganiseerd verband misdrijven worden beraamd of gepleegd die een ernstige inbreuk op de rechtsorde opleveren. De bewerking kan gevorderd worden van degene van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot de gegevens. Onder het bewerken van gegevens wordt verstaan het verkrijgen van nieuwe gegevens door een analyse, een vergelijking of een combinatie van verschillende gegevens of verschillende verzamelingen van gegevens. De nieuwe gegevens ontstaan eerst door de bewerking en zijn zonder deze bewerking niet beschikbaar.

Het College Bescherming Persoonsgegevens (CBP), de Nederlandse Orde van Advocaten (NOvA) en het Overlegorgaan Post en Telecommunicatie, Deelorgaan aftappen (OPT/DAF) zijn negatief over het voorstel te komen tot een bevoegdheid tot het vorderen van een bewerking van gegevens. Zij menen dat houders van gegevens te zeer worden betrokken bij het verrichten van opsporingshandelingen en dat sprake is van een te vergaande inbreuk op de persoonlijke levenssfeer. Het openbaar ministerie is positief over deze bevoegdheid en meent dat geen machtiging van de rechter-commissaris zou moeten zijn vereist.

Het kabinet is van mening dat de voorgestelde bevoegdheid – zoals in de adviezen naar voren komt – ingrijpend kan zijn. Zoals de Commissie ook aangeeft, levert het bewerken van gegevens meestal een grotere spanning op met de normen voor een zorgvuldige omgang met persoonsgegevens, dan het enkele verstrekken van gegevens. Door een bewerking van gegevens kunnen nieuwe gegevens zichtbaar worden die zonder bewerking niet zichtbaar zijn. Onverwachte informatie over personen kan zo beschikbaar komen. Ook zal een bewerking veelal een grotere inspanning vergen van de houder dan het enkele verstrekken van gegevens zonder voorafgaande bewerking.

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 informatie- en communicatietechniek maakt het mogelijk dat grote gegevensbestanden aanwezig zijn en dat hieraan door een bewerking belangrijke informatie voor strafvorderlijk onderzoek is te onttelen. 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. Het kabinet stelt echter een van de voorstellen van de Commissie afwijkend kader voor. Dit houdt in dat indien het onderzoek naar een ernstig misdrijf zeer gebaat zou zijn bij een bewerking van gegevens die beschikbaar zijn bij derden, omdat door deze bewerking kan worden achterhaald wie de verdachte is van het misdrijf, terwijl een vergelijkbaar resultaat niet langs andere weg verkregen kan worden, de officier van justitie de bevoegdheid heeft, na machtiging van de rechter-commissaris, bevel te geven tot een bewerking van gegevens door opsporingsambtenaren en tot het daartoe gebruiken van gegevens die bij derden beschikbaar zijn. De bewerking kan inhouden dat een vergelijking plaatsvindt met gegevens bij de politie, dan wel met gegevens bij andere derden. De bewerking dient plaats te vinden op een zodanige wijze, toe te passen na advies van het CBP, dat over zo min mogelijk personen gegevens beschikbaar komen. Dit kan plaatsvinden door de bewerking geheel langs geautomatiseerde weg plaats te laten vinden waarbij niet van de ingevoerde gegevens, maar uitsluitend van de resultaten van de bewerking kennis kan worden genomen (black box). De kosten daarvan komen voor rekening van de overheid. Na afronding van de bewerking dienen alle niet relevante gegevens vernietigd te worden. De bewerking wordt beschreven, zodat deze achteraf controleerbaar is.

Dit kader wijkt af van het voorstel van de Commissie, omdat het uitgangspunt niet meer is dat de bewerking wordt uitgevoerd door de houder van de gegevens, maar dat deze wordt uitgevoerd door opsporingsambtenaren. Hiermee wordt tegemoet gekomen aan de bezwaren dat houders van gegevens te zeer worden betrokken bij het verrichten van opsporingshandelingen. Daarnaast is het voorstel in de wet op te nemen dat de bewerking dient plaats te vinden op een zodanige wijze dat over zo min mogelijk personen gegevens beschikbaar komen. Het CBP dient hierover om advies te worden gevraagd. Gelet op dit van de voorstellen van de commissie afwijkende kader acht het kabinet het gewenst dit onderdeel van de voorstellen in een apart wetsvoorstel onder te brengen en afzonderlijk in consultatie te geven aan de adviserende organen.

4.6. Bevoegdheid tot het vorderen dat gegevens beschikbaar worden gehouden

De Commissie stelt voor in het Wetboek van Strafvordering een bevoegdheid op te nemen tot het vorderen dat geautomatiseerde gegevens gedurende een periode van veertien dagen beschikbaar blijven. De bevoegdheid kan worden toegepast door de hulp-officier van justitie indien het

belang van het onderzoek dit dringend vordert, in geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, Sv dat gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert, dan wel in geval van verdenking dat in georganiseerd verband van misdrijven worden beraamd of gepleegd die een ernstige inbreuk op de rechtsorde opleveren. De vordering kan worden gericht tot degene van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot de gegevens. In de vordering dienen de gegevens die beschikbaar gehouden moeten worden te worden vermeld.

Het College Bescherming Persoonsgegevens (CBP) meent dat er aanleiding is te komen tot een bevoegdheid tot het vorderen dat gegevens beschikbaar blijven (bevriezen). Het Overlegorgaan Post en Telecommunicatie, Deelorgaan aftappen (OPT/DAF) meent dat voor deze bevoegdheid zwaardere waarborgen nodig zijn. Ook de Nederlandse Vereniging van Banken (NVvB) pleit daarvoor. De Nederlandse Orde van Advocaten (NOvA) vindt dat deze bevoegdheid een te actieve opstelling van de houder van de gegevens vraagt en meent dat de verschoningsplicht van de advocaat zich er niet mee verhoudt.

In reactie hierop wordt het volgende opgemerkt.

Nieuwe informatietechnieken brengen met zich mee dat bij bepaalde processen zogenaamde vluchtige gegevens ontstaan. Dit zijn gegevens die slechts gedurende een (zeer) korte periode door de houder worden bewaard. In bepaalde gevallen is er in het belang van de opsporing van misdrijven een grote behoefte aan de mogelijkheid te bewerkstelligen dat vluchtige gegevens beschikbaar blijven. Het gaat hierbij niet om toekomstige gegevens, maar om historische gegevens: gegevens die op het moment van de vordering reeds bestaan. Een vordering vluchtige gegevens beschikbaar te houden kan alleen worden gedaan, indien het bij de tot opsporing bevoegde instanties bekend is dat vluchtige gegevens aanwezig zijn, die nodig kunnen zijn voor het onderzoek. Een voorbeeld waarin dit het geval kan zijn betreft de situatie waarin kinderpornografie op internet wordt gesignaleerd. Vluchtige gegevens zijn in dit geval gegevens die zich slechts een korte tijd in de systemen van de internetaanbieder bevinden. Deze gegevens kunnen een spoor vormen naar diegenen die betrokken zijn bij het plaatsen van de kinderpornografie op internet. Het zal daarbij meestal gaan om gegevens die de houder van de gegevens slechts heel kort voor eigen bedrijfsdoeleinden bewaart. Een ander voorbeeld is de situatie waarin bij een schietincident met slachtoffers veel mogelijke betrokkenen op de plaats van het incident aanwezig waren en gegevens over deze betrokkenen wellicht beschikbaar zijn, omdat zij in de buurt van het incident elektronische handelingen hebben verricht of gebruik van mobiele telecommunicatie hebben gemaakt. Denkbaar is dat de tot opsporing bevoegde autoriteit van de bedrijven die beschikken over deze gegevens vordert gedurende een bepaalde periode de gegevens beschikbaar te houden, zodat kan worden onderzocht of het bijdraagt aan de opheldering van het delict om bepaalde van deze gegevens te vorderen. Hiermee kan de bevoegdheid tot het vorderen dat gegevens beschikbaar blijven voorkomen dat de officier van justitie – op verzoek van de hulpofficier van justitie of andere opsporingsambtenaren – ter veiligstelling van de gegevens direct de vordering doet tot het verstrekken van gegevens. In die zin kan de bevoegdheid bijdragen aan een proportionele inzet van bevoegdheden.

In verband met het belang van vluchtige gegevens voor de opsporing van misdrijven bevat ook het Verdrag Crime in Cyberspace (Trb 2002, 18) een bepaling betreffende een bevel tot het vastleggen van gegevens. In dit verdrag is bepaald dat de houder van gegevens verplicht kan worden

gedurende een termijn van 90 dagen gegevens vast te leggen. De reden hiervoor is dat rekening is gehouden met de lange periode die in een aantal landen gemoeid is met de uitvoering van een rechtshulpverzoek. Nederland is bij de implementatie van het verdrag gehouden deze termijn in de nationale wetgeving te garanderen. Om die reden wordt voorgesteld de door de Commissie voorgestelde bevoegdheid hieraan aan te passen.

Inderdaad dienen – zoals de adviezen benadrukken – bij deze bevoegdheid voldoende zware waarborgen van toepassing te zijn, mede in verband met de lasten die voor het bedrijfsleven aan de orde kunnen zijn. Het langer dan nodig voor de uitvoering van de eigen activiteiten beschikbaar houden van gegevens door de houder ten behoeve van strafvorderlijk onderzoek, levert namelijk een doelafwijkende verwerking van gegevens op en vergt veelal een bijzondere inspanning van de houder. Om die reden is terughoudendheid gewenst en dient een dergelijke vordering alleen gedaan te kunnen worden indien het belang van het onderzoek het dringend vordert en indien het gaat om de opsporing van een misdrijf als omschreven in artikel 67, eerste lid, Sv dat gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert, dan wel in geval van verdenking dat in georganiseerd verband van misdrijven worden beraamd of gepleegd die een ernstige inbreuk op de rechtsorde opleveren.

De vordering kan alleen worden gedaan met betrekking tot gegevens waarover de houder beschikkingsmacht heeft, dat wil zeggen met betrekking waartoe de houder beschikt over technische mogelijkheden om deze beschikbaar te houden. Indien de houder daarover niet beschikt kan hij aan de vordering geen gevolg geven. Daarbij geldt, ingevolge de beginselen van proportionaliteit en subsidiariteit, dat van de houder geen onevenredige inspanning mag worden verlangd. Van belang is dat inzicht bestaat in de gevolgen van een vordering tot het beschikbaar houden van de gegevens. Het ligt in de rede dat overleg plaatsvindt tussen de strafvorderlijke autoriteit en de houder over de inspanning die nodig is om vernietiging van de gegevens tegen te gaan. Het ligt evenzeer in de rede dat met sectoren waar deze bevoegdheid met enige regelmaat aan de orde kan zijn, afspraken worden gemaakt over de toepassing daarvan, ook met het oog op de kosten, die door de overheid gedragen worden.

Teneinde een afweging tussen enerzijds opsporingsbelang en anderzijds het belang van de houder van de gegevens zo goed mogelijk te waarborgen wordt voorgesteld de bevoegdheid bij een hogere autoriteit dan de hulp officier van justitie neer te leggen, namelijk bij de officier van justitie. Hier is temeer reden voor nu de maximale termijn wordt verhoogd naar 90 dagen, hetgeen tot een grotere belasting van de houder van de gegevens kan leiden. De officier van justitie is, gelet op zijn rol in het opsporingsonderzoek, beter in staat de vereiste afweging te maken. De bevoegdheid strekt slechts tot het beschikbaar houden van gegevens. Zij impliceert niet dat de gegevens verstrekt worden aan de bevoegde autoriteit. Om die reden is er geen voorziening nodig voor verschoningsgerechtigden. De vraag of gegevens onder het verschoningsrecht vallen, komt pas aan de orde indien een bevoegdheid verstrekking van de gegevens te vorderen wordt toegepast.

5. Aanvullende waarborgen

De Commissie stelt verschillende flankerende voorzieningen voor bij de door haar voorgestelde bevoegdheden tot het vorderen van gegevens. Het kabinet kan zich daarin veelal vinden. De voorstellen betreffende het beklagrecht verdienen aanvulling. Op enkele van deze voorstellen wordt hier ingegaan.

5.1. De vergoeding van kosten die houders ter uitvoering van een vordering maken

De Commissie stelt voor dat de kosten die aan de nakoming van een vordering kunnen worden toegerekend in de vorm van extra personeelskosten en extra administratiekosten voor vergoeding in aanmerking dienen te komen, voor zover deze kosten inzichtelijk gemaakt worden aan de overheid.

De adviezen ondersteunen dit en stellen dat de vergoeding kostendekkend dient te zijn.

In reactie hierop kan worden vermeld dat het kabinet met het voorstel van de Commissie instemt. De Commissie sluit aan bij de regeling van artikel 592 van het Wetboek van Strafvordering. Dit artikel regelt de vergoeding van kosten voor de uitlevering of overbrenging van voorwerpen en van het vastleggen of overbrengen van geautomatiseerde gegevens. Het gaat daarbij om kosten die verbonden zijn aan een individuele vordering of een individueel bevel. Het gaat niet om kosten die in het kader van de reguliere activiteiten toch al worden gemaakt. In geval van bijvoorbeeld een ingewikkelde zoekvraag kunnen de kosten van een individuele vordering hoog zijn. In beginsel dient de vergoeding – zoals de adviezen bepleiten – inderdaad kostendekkend te zijn. Dat deze kosten inzichtelijk worden gemaakt kan ook een dam opwerpen tegen vorderingen die veel inspanningen vragen van de houder van gegevens. Met de Commissie wordt ook ingestemd dat het gewenst kan zijn met houders van gegevens in bepaalde sectoren in het bedrijfsleven van wie veelvuldig gegevens worden gevorderd, afspraken te maken over standaardvergoedingen voor de inspanningen die zij moeten verrichten.

5.2. Beklagrecht

De Commissie stelt voor dat aan de belanghebbende recht op beklag toekomt tegen de vordering zelf en tegen de kennisneming of het gebruik van gegevens die gevorderd zijn op grond van de voorgestelde bevoegdheden. Zij sluit aan bij artikel 552a Sv waarin het beklag over onder andere inbeslagneming en kennisneming van geautomatiseerde gegevens is geregeld. Daarnaast stelt de Commissie voor dat de belanghebbende kan vorderen dat de verstrekte gegevens worden vernietigd. Zowel de houder van de gegevens tot wie de vordering is gericht als degene op wie de gegevens betrekking hebben, kunnen als belanghebbende worden aangemerkt. De Commissie meent dat dit recht op beklag geen opschortende werking dient te hebben, omdat een zorgvuldige toepassing van bevoegdheden reeds impliceert dat de opsporingsautoriteit bezwaren van de houder tegen het verstrekken van gegevens in zijn overwegingen betreft en omdat de voorwaarden die aan de bevoegdheden zijn verbonden, aangevuld met de mogelijkheid van beroep op een rechterlijke toets achteraf, voldoende waarborgen tegen een onredelijke of onrechtmatige toepassing van de gegevensvordering bevatten.

Het College Bescherming Persoonsgegevens bepleit in zijn advies een opschortend beklagrecht voor de verstrekker. Ook De Nederlandsche Bank en de Nederlandse Vereniging van Banken (NVvB) bepleiten dit. Als redenen worden genoemd dat een eenmaal verstrekt gegeven niet meer kan worden teruggegeven, zoals dat bij een in beslag genomen voorwerp wel kan. Ook wordt genoemd dat houders van gegevens geconfronteerd kunnen worden met een verlies van vertrouwen indien achteraf blijkt dat op onjuiste gronden gegevens zijn verstrekt, ook al ligt de verantwoordelijkheid daarvoor bij justitie. Tot slot wordt aangegeven dat een vooraf-

gaande toetsing door de rechter kan bijdragen aan de normering van de toepassing van de bevoegdheden.

Als reactie hierop kan het volgende worden opgemerkt. Zoals in enkele adviezen naar voren is gekomen, is de reikwijdte van de voorgestelde bevoegdheden tot het vorderen van gegevens ruim. Daarnaast kan worden vastgesteld dat de bevoegdheden weinig «natuurlijke grenzen» kennen: zij zijn eenvoudig, zonder al te veel praktische belemmeringen toe te passen. Gegevens kunnen makkelijk worden gekopieerd, de houder ondervindt veelal geen nadeel van het verstrekken van gegevens, hij verliest het bezit daarvan niet. Gegevens zijn bovendien eenvoudig te verwerken. Daarnaast kan – zoals in de adviezen naar voren kwam – inderdaad een rol spelen dat houders van gegevens te maken krijgen met een verlies van vertrouwen indien achteraf blijkt dat gegevens ten onrechte zijn verstrekt, ook al ligt de verantwoordelijkheid daarvoor bij justitie.

Met de adviezen wordt ingestemd dat een beklagrecht een waarborg kan bieden die bijdraagt aan een verantwoorde toepassing van de bevoegdheden en een zorgvuldige omgang met de verkregen gegevens. Dit geldt echter ook indien het beklagrecht geen opschortende werking heeft. Behandeling van beklag achteraf is ook normerend. Een gegeven kan inderdaad niet worden teruggegeven – zoals de adviezen stellen – maar het kan wel worden vernietigd. Daarmee kan het effect van de verstrekking ongedaan worden gemaakt. De beklagregeling moet dan ook mede inhouden – zoals de commissie heeft voorgesteld – dat van politie en openbaar ministerie gevorderd kan worden dat de verstrekte gegevens worden vernietigd, in de registers en de dossiers waarin het is opgenomen, en dat hiervan proces-verbaal wordt opgemaakt.

Met inachtneming hiervan kan worden ingestemd met het voorstel van de Commissie aan te sluiten bij artikel 552a Sv. Met de Commissie is de verwachting dat bij een zorgvuldige toepassing van bevoegdheden reeds rekening wordt gehouden met eventuele bezwaren van de houder tegen het verstrekken van gegevens. Dat neemt niet weg dat de houder van de gegevens ernstige bezwaren kan blijven behouden. De reden van het beklag kan zijn dat de houder meent dat er geen rechtsgrondslag voor de vordering is. Ook is denkbaar dat hij de gegevens niet wil verstrekken omdat het vertrouwelijke bedrijfsgegevens betreft. Tot slot kan hij menen dat van hem een onevenredige inspanning wordt gevraagd. Komt het tot beklag, dan toetst de rechter de rechtmatigheid van de toepassing van de bevoegdheid. Hij toetst – afhankelijk van de aard van het beklag – of de vordering aan de wettelijk vereisten en aan de eisen van proportionaliteit en subsidiariteit voldoet. Indien de klacht de vertrouwelijkheid van de gegevens betreft, weegt de rechter het belang van de opsporing af tegen het belang van de belanghebbende. De rechter die op het beklag beslist, dient aan te geven wat het gevolg is van het gegrond verklaren van het beklag.

De belanghebbende kan er belang bij hebben dat het beklag snel wordt behandeld en dat de gegevens – indien de rechter oordeelt dat het beklag gegrond is – zo spoedig mogelijk wordt vernietigd. Met het oog daarop wordt voorgesteld in de wet te bepalen dat de officier van justitie in overleg met de raadkamer die het beklag behandelt de datum voor de behandeling van het beklag vaststelt. Langs deze weg bestaat de mogelijkheid in geval van spoedeisend belang te komen tot een snelle behandeling van het beklag.

5.3. Het aanvullen van de notificatieplicht van artikel 126bb Sv.

De Commissie stelt voor dat een plicht voor de tot opsporing bevoegde instantie moet gelden om – zodra het belang van het onderzoek het

toelaat – de persoon op wie de gegevens betrekking hebben van de toepassing van de bevoegdheid tot het vorderen van gegevens op de hoogte te stellen. Deze notificatieplicht moet gelden voor alle bevoegdheden – behoudens de bevoegdheid tot het vorderen van identificerende gegevens.

Het College Bescherming Persoonsgegevens meent dat ook voor de bevoegdheid tot het vorderen van identificerende gegevens een notificatieplicht zou moeten gelden, zij het dat voor sectoren waar de bevoegdheid vaak zal worden toegepast zou kunnen worden volstaan met een regeling die inhoudt dat inzicht wordt gegeven in het verwijderen van niet voor de opsporing relevante gegevens.

In reactie hierop wordt het volgende vermeld. De achtergrond van de notificatieplicht is dat deze de betrokkene in de gelegenheid stelt een rechtsmiddel aan te wenden tegen een mogelijke inbreuk op zijn grondrecht op bescherming van de persoonlijke levenssfeer. Dit geeft invulling aan artikel 13 EVRM. Met de Commissie wordt betwijfeld of de notificatie ook de bevoegdheid tot het vorderen van «identificerende gegevens» zou moeten betreffen. De identificerende gegevens vormen een beperkte categorie gegevens. De bevoegdheid tot het vorderen van deze gegevens is niet ingrijpend te noemen, temeer niet nu toepassing van deze bevoegdheid is uitgesloten indien de enkele verstrekking van die gegevens reeds een gevoelig gegeven oplevert, dat wil zeggen een gegeven betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, of lidmaatschap van een vakvereniging. Ook de beperking van de bevoegdheid tot het vorderen van identificerende gegevens tot de houders die gegevens verwerken anders dan ten behoeve van persoonlijk gebruik, brengt met zich mee dat een notificatieplicht voor deze bevoegdheid minder aangewezen is. Een notificatieplicht zou een onevenredig zware belasting opleveren voor de bevoegde autoriteiten die moeten bewaken op welk moment notificatie dient plaats te vinden.

Wel is het gewenst te komen tot wat wel genoemd wordt statistische transparantie, deels in plaats van, deels in aanvulling op de notificatieplicht. Dat wil zeggen dat de politie en het openbaar ministerie inzicht geven in de aantallen malen waarin gegevens worden gevorderd, alsmede in de verdere verwerking van de verkregen gegevens, waarbij het toezicht daarop een belangrijke rol speelt. Op dat laatste wordt hierna onder 5.4. nader ingegaan. Nu een vordering schriftelijk dient te worden gedaan en zowel de politie als het openbaar ministerie hiervoor modellen zullen ontwikkelen die langs geautomatiseerde weg zullen worden verwerkt, is het mogelijk langs geautomatiseerde weg inzicht te verschaffen in de aantallen vorderingen. Ook het voorstel de toepassing van de bevoegdheid tot het vorderen van identificerende gegevens in de praktijk te beperken tot daartoe geautoriseerde opsporingsambtenaren kan hieraan bijdragen.

Bij de evaluatie van de Wet bijzondere opsporingsbevoegdheden wordt de notificatieplicht geëvalueerd. Met de resultaten daarvan zal rekening gehouden worden.

5.4. De regeling voor verwerken van gegevens in de Wet politieregisters

De Commissie sluit wat betreft het bewaren en vernietigen van gegevens aan bij de regeling in de Wet politieregisters. Zij meent dat de Wet politieregisters voldoende waarborgen biedt voor het verdere gebruik van gegevens die in een politieregister zijn opgenomen. Zij ziet daarom af van nadere voorstellen op dit punt.

Het College Bescherming Persoonsgegevens (CBP) meent dat meer controle op de naleving van de Wet politieregisters is vereist. Het CBP dringt aan op de introductie van de verplichting voor de opsporingsinstanties om zelf periodiek een *audit* te laten verrichten op de gegevensverwerking.

Zoals in het voorgaande al enkele malen aan de orde kwam is het van belang dat voorzien is in een goede regeling voor het verdere gebruik en de vernietiging van de gegevens die verkregen zijn met behulp van de voorgestelde bevoegdheden. De Wet politieregisters bepaalt dat gegevens die in het kader van een strafvorderlijk onderzoek worden vergaard, in beginsel moeten worden opgeslagen in een zogenaamd tijdelijk register. Een tijdelijk register is een bijzonder register in de zin van de Wet politieregisters. Opneming van persoonsgegevens in een tijdelijk register vindt slechts plaats met het oog op het doel waarvoor het register is aangelegd. Dat betekent dat uitsluitend die gegevens worden bewaard die relevant zijn voor het desbetreffende strafvorderlijk onderzoek.

Wanneer de gegevens zijn verkregen, kan blijken dat zij niet van belang zijn voor het onderzoek. Indien zij dan reeds zijn opgeslagen, dienen zij te worden gewist. De Wet politieregisters voorziet erin dat gegevens die – al dan niet na afronding van het strafvorderlijke onderzoek – niet (meer) van belang zijn voor een goede uitvoering van de politietaak vernietigd dienen te worden. Van de vernietiging van de gegevens wordt proces-verbaal opgemaakt dat gedurende twee jaar wordt bewaard.

Met het CBP kan worden ingestemd dat een goede controle op de naleving van de Wet politieregisters nodig is. Nu opsporingsbevoegdheden mede kunnen worden toegepast ter verkrijging van gegevens over andere personen dan de verdachte, terwijl in bepaalde gevallen ook gegevens over een op voorhand onbepaalde groep van personen kunnen worden verkregen, zoals hiervoor onder 3.3. en 4.2. aan de orde kwam, moet er vertrouwen gesteld kunnen worden in de goede naleving van de Wet politieregisters. Ook gelet op denkbare alternatieven voor de notificatieplicht, bestaande uit het bieden van inzicht in de aantallen malen waarin gegevens worden gevorderd alsmede in de verdere verwerking van de verkregen gegevens, zoals hiervoor onder 5.3 al werden genoemd, is dit van belang. De regeling van opsporingsbevoegdheden in het Wetboek van Strafvordering en het omgeven van deze bevoegdheden met waarborgen, dient er mede toe de controleerbaarheid achteraf te bevorderen, vergelijk de hiervoor onder 3.2 besproken eisen van artikel 8 van het EVRM. Zeker voor die opsporingsonderzoeken die niet uitmonden in een strafzaak is het van belang dat door middel van toezicht op de naleving van de Wet politieregisters hieraan inhoud wordt gegeven.

Om voornoemde redenen neemt het kabinet het voorstel van het CBP over om te komen tot een verplichting voor opsporingsinstanties om periodiek een *audit* te laten verrichten op de gegevensverwerking. Het kabinet hecht veel belang aan het project van zelfevaluaties en *audits* dat in 2001 van start is gegaan. De ervaringen in dit project kunnen bijdragen aan de totstandkoming van een goede regeling in de Wet politieregisters. Op termijn zal in de Wet politieregisters een plicht tot een periodieke *audit* worden opgenomen. Daarbij zullen kwaliteitseisen aan de *audit* worden gesteld en wordt overwogen het CBP te belasten met het toezicht op deze *audits*. Het kabinet hecht veel belang aan de zelfevaluaties en onafhankelijke reviews die vanaf januari 2002 worden uitgeoefend ten aanzien van de bijzondere politieregisters die worden gevoerd bij de regionale politiekorpsen, het Korps landelijke politiediensten, de rijksrecherche en de Koninklijke marechaussee. De ervaring die hiermee worden opgedaan, zullen worden betrokken bij de totstandkoming van een goede regeling in de Wet politieregisters.

5.5. De regeling voor verschoningsgerechtigden

De Commissie sluit voor de zogenaamde beroepsmatige geheimhouders, zoals de advocaat, de notaris en de arts, aan bij de regeling van artikel 96a Sv: de beroepsmatige geheimhouder hoeft niet te voldoen aan een vordering tot het verstrekken van gegevens voor zover de verstrekking van gegevens strijdig zou zijn met zijn verschoningsrecht.

Het College Bescherming Persoonsgegevens (CBP) en de Nederlandse Orde van Advocaten (NOvA) bevelen – in aanvulling hierop – aan, te komen tot een regeling voor het vorderen van gegevens in de omgeving van de beroepsgeheimhouders. De Koninklijke Notariële Broederorganisatie (KNB) bepleit dat de voorzitter van de plaatselijke ring bij de zaak wordt betrokken indien in het kader van strafvorderlijke activiteiten het beroepsgeheim van een notaris in het geding komt.

Het kabinet meent met de Commissie dat voor de regeling voor de beroepsmatige geheimhouders aangesloten kan worden bij artikel 96a, derde lid, onder b, van het Wetboek van Strafvordering, dat betrekking heeft op de bevoegdheid tot het ter inbeslagneming vorderen van voorwerpen. Ook de bevoegdheden tot het vorderen van gegevens kunnen betrekking hebben op informatie die valt onder het verschoningsrecht, zodat een beperking van de werking van de bevoegdheden jegens beroepsmatige geheimhouders nodig is. Hiermee wordt erkend dat gegevens die onder het verschoningsrecht vallen geen onderwerp kunnen zijn van de toepassing van de voorgestelde bevoegdheden. Dit betekent tevens dat de bevoegdheden niet zodanig mogen worden aangewend dat deze gegevens langs andere weg verkregen worden. In de rechtspraak wordt dit ook aangenomen. Verwezen zij naar Hoge Raad 1 november 1988, NJ 1989, 349 en Hoge Raad 29 maart 1994, NJ 1994, 552. De ratio van een bepaling als artikel 96a, derde lid, onder b, verzet zich tegen de mogelijkheid dat de waarborg van deze bepaling zou worden omzeild door dezelfde gegevens bij een andere houder te vragen. Met de Commissie is het kabinet daarom van oordeel dat het niet nodig is hiervoor in de wet een regeling te treffen.

Indien een beroepsmatige geheimhouder zelf verdachte is in een zaak, kan dit een rechtvaardiging zijn gegevens te vergaren die in beginsel onder het verschoningsrecht vallen. Voor de vraag in hoeverre het toegestaan kan zijn dat over een geheimhouder zelf gegevens worden vergaard, is, zoals de Commissie aangeeft, het arrest van de Hoge Raad van 29 juni 1993 (NJ 692) van betekenis. Daarin wordt door de Hoge Raad uitgesproken dat als de geheimhouder zelf verdachte is in een onderzoek, zijn telefoonaansluiting mag worden afgeluisterd. Analooq hieraan kan worden gesteld dat indien de geheimhouder verdachte is over de geheimhouder zelf bij een derde gegevens kunnen worden gevorderd. Daarbij dient aangesloten te worden bij de in de huidige praktijk gevolgde gedragslijn dat indien het beroepsgeheim van de advocaat in het geding kan komen, het oordeel wordt ingewonnen van de deken van de plaatselijke orde van advocaten. Zo kan ook, zoals de KNB bepleit, indien het gaat om een notaris, de voorzitter van de plaatselijke ring bij de zaak worden betrokken.

6. Inpassing in het Wetboek van Strafvordering

De Commissie doet enkele aanbevelingen over de verhouding tussen de door haar voorgestelde bevoegdheden en andere bepalingen in het Wetboek van Strafvordering. Deze worden onderschreven. Op enkele van deze aanbevelingen wordt hier ingegaan.

6.1. De verhouding tot de bevoegdheden tot inbeslagneming

Gegevens kunnen ook verkregen worden door het in beslag nemen van de drager van de gegevens: papier, boeken, ordners, computers, floppies enzovoort. Het hoeft geen betoog dat het in beslag nemen van een gegevensdrager met het enkele oogmerk een daarop vastgelegd gegeven te verkrijgen, in veel gevallen disproportioneel zal zijn, zeker indien de gegevensdrager veel andere gegevens bevat, dan wel indien daardoor de houder van de gegevensdrager ernstig wordt benadeeld. Het kabinet is met de Commissie van oordeel dat de voorgestelde bevoegdheden tot het vorderen van gegevens inhouden dat de bevoegdheden tot inbeslagneming niet toegepast mogen worden met het doel gegevens te verkrijgen: er dient van de door de Commissie voorgestelde bevoegdheden gebruik te worden gemaakt. Alleen indien er omstandigheden zijn die ertoe nopen dat de gehele gegevensdrager wordt verkregen, kunnen de bevoegdheden tot inbeslagneming worden toegepast. Dit kan zich bijvoorbeeld voordoen indien langdurig onderzoek in dossiers nodig is voordat de gegevens die voor het strafvorderlijk onderzoek van belang zijn, kunnen worden geselecteerd. Indien langdurig onderzoek nodig is in geautomatiseerde werken, zal het vaak mogelijk zijn de relevante bestanden te kopiëren. Indien dit het geval is, dient van inbeslagneming van de geautomatiseerde werken te worden afgezien. Indien het doel is dat de gegevensdrager, bijvoorbeeld het originele document, wordt veilig gesteld, blijven vanzelfsprekend de bevoegdheden tot inbeslagneming van toepassing.

De Commissie stelt voor in het Wetboek van Strafvordering een bevoegdheid tot doorzoeking ter vastlegging van gegevens op te nemen, analoog aan de bevoegdheden tot doorzoeking ter inbeslagneming. Met het expliciteren dat doorzoeking mogelijk is, uitsluitend ter vastlegging van gegevens, wordt volgens de Commissie tot uitdrukking gebracht wat in de wet tot nu toe impliciet is gebleven, namelijk dat doorzoeking (uitsluitend) ter vastlegging van gegevens is toegestaan en dat daarbij onderzoek kan worden gedaan naar, inzage kan worden verkregen in en kopie kan worden gemaakt van gegevens die, hetzij op papier, hetzij op enige andere gegevensdrager, daaronder begrepen een geautomatiseerd werk, zijn opgeslagen.

6.2. Het wetsvoorstel computercriminaliteit II en Crime in Cyberspace

Het wetsvoorstel computercriminaliteit II (Kamerstukken II 1998/99, 26 671, nr. 2) omvat naast voorstellen tot wijziging van het Wetboek van Strafrecht, ook voorstellen tot wijziging van het Wetboek van Strafvordering. Daaronder is ook een terminologische aanpassing van artikel 125i begrepen. Dit artikel betreft de bevoegdheid van de rechter-commissaris te bevelen dat gegevens uit een geautomatiseerd werk worden verstrekt. Het artikel betreft uitsluitend gegevens die een direct verband hebben met het handelen van de verdachte. De hiervoor besproken voorstellen voor bevoegdheden tot het vorderen van gegevens omvatten mede de in artikel 125i Sv neergelegde bevoegdheid. Artikel 125i kan daarom vervallen. De terminologie zoals deze is gebruikt in het wetsvoorstel computercriminaliteit II is in de voorstellen van de Commissie overgenomen. Omdat de aanpassing van artikel 125i in het wetsvoorstel computercriminaliteit II een beperkt karakter heeft, bestaat er geen bezwaar tegen die aanpassing toch nog door te voeren, voor de beperkte periode waarin de wetgeving betreffende de hier besproken bevoegdheden tot het vorderen van gegevens nog niet tot stand is gekomen. Het wetsvoorstel computercriminaliteit II brengt ook wijzigingen aan in de artikelen 125j ev. Sv. Deze zijn mede van betekenis voor – en daarmee is dan ook rekening gehouden bij – het hiervoor onder 6.2. besproken voor-

stel betreffende de regeling van de bevoegdheid tot doorzoeking ter vastlegging van gegevens.

Bij de behandeling van het wetsvoorstel computercriminaliteit II kan het voorgaande zo nodig nog nader aan de orde komen.

In het voorjaar van 2002 zal een wetsvoorstel in consultatie gaan ter implementatie van het Verdrag Crime in Cyberspace (Trb 2002, 18). Op één onderdeel heeft de implementatie van het verdrag betrekking op de hiervoor besproken voorstellen. Het betreft artikel 16 van het verdrag dat betrekking heeft op het beschikbaar houden van gegevens. De hiervoor onder 4.6 voorgestelde bevoegdheid tot het beschikbaar houden van gegevens kan dienen ter implementatie van dit onderdeel van het verdrag.

6.3. Het wetsvoorstel vorderen gegevens telecommunicatie

Het Wetboek van Strafvordering kent, in combinatie met bepalingen in de Telecommunicatiewet, reeds bevoegdheden betreffende het vorderen van gegevens van aanbieders van openbare telecommunicatienetwerken en -diensten. Het betreft de bevoegdheden tot het opnemen van telecommunicatie, tot het vorderen van verkeersgegevens en tot het vorderen van gegevens betreffende naam, adres, woonplaats, nummer en soort dienst.¹ De twee laatstgenoemde bevoegdheden worden aangepast in het wetsvoorstel vorderen gegevens telecommunicatie (Kamerstukken II 2001/2002, 28 059, nrs. 1–2).

De Commissie meent dat de bevoegdheden die thans reeds gelden voor de telecommunicatie sector in de naaste toekomst gehandhaafd moeten blijven. Zij meent dat wel voorzien moet worden in een regeling die betrekking heeft op de gegevens die niet begrepen zijn onder de specifieke telecommunicatiebevoegdheden.

Het advies van het Overlegorgaan Post en Telecommunicatie, Deelorgaan aftappen spreekt van een onwenselijke uitbreiding van opsporingsbevoegdheden in relatie tot de regeling van de huidige bevoegdheden voor de sector van de telecommunicatieaanbieders. Betreurd wordt dat de duidelijkheid die het wetsvoorstel vorderen gegevens telecommunicatie schept nu weer tenietgedaan wordt. Men bepleit een meer op de sector toegesneden regeling van de algemene bevoegdheid.

Naar aanleiding hiervan kan worden opgemerkt dat inderdaad voorkomen moet worden dat de duidelijkheid die het wetsvoorstel vorderen gegevens telecommunicatie schept nu weer tenietgedaan wordt. Het kabinet ziet redenen de bevoegdheden die thans reeds voor de telecommunicatiesector gelden, te handhaven. Het betreft bijzondere bevoegdheden. De bevoegdheid tot het opnemen van telecommunicatie betreft gegevens die vallen onder de bescherming van artikel 13 van de Grondwet (telefoongeheim). De bevoegdheid tot het vorderen van verkeersgegevens betreft gegevens die vallen onder de EG-richtlijn betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de telecommunicatiesector.² Bijzonder is ook dat de aanbieders van openbare telecommunicatie verplicht zijn tot bepaalde investeringen teneinde toekomstige gegevens op een bepaalde wijze en *real time* te kunnen verstrekken. Bovendien geldt voor deze sector dat als gevolg van veel wetgeving zich een bepaalde praktijk heeft ontwikkeld.

Wel moet worden gezien hoe de door de Commissie voorgestelde algemene bevoegdheden tot gegevensvergaring zich verhouden tot hetgeen in de wetgeving betreffende gegevensvergaring in de telecommunicatiesector reeds tot stand is gekomen.

¹ Zie de artikelen 126m, 126n, 126t en 126u Sv en de artikelen 13.2 en 13.4, eerste lid, van de Telecommunicatiewet.

² Richtlijn 97/66/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de telecommunicatiesector, PbEG 1998, L 24.

Zoals de Commissie ook vaststelt, zijn de bevoegdheden voor de telecommunicatiesector gericht op bepaalde, nauw omschreven categorieën gegevens. Ten eerste gaat het om het direct doorgeleiden (*real time* aftappen) van de inhoud van telecommunicatie: telefoongesprekken en (ander) berichtenverkeer via internet. Dit valt geheel buiten de voorstellen van de commissie. Ten tweede gaat het om verkeersgegevens. Dat zijn gegevens betreffende de wijze van totstandkoming en afwikkeling van het telecommunicatieverkeer, zoals de betrokken nummers, de gebruikte apparatuur en het tijdstip van de aanvang en de duur van het verkeer. Deze categorie valt binnen de hiervoor besproken voorstellen. Ten derde gaat het om zogenaamde gebruikersgegevens, een categorie die sterk overeenkomt met de door de Commissie omschreven identificerende gegevens: gegevens betreffende naam, adres, woonplaats, nummer en soort dienst. In het wetsvoorstel vorderen gegevens telecommunicatie worden de categorie verkeersgegevens en de categorie gebruikersgegevens limitatief omschreven. Het is moeilijk te verdedigen dat van de aanbieders van openbare telecommunicatie beperkte categorieën gegevens gevorderd kunnen worden, terwijl van andere houders van gegevens met de voorgestelde bevoegdheden in beginsel alle gegevens gevorderd zouden kunnen worden. Om die reden en in verband met het vervallen van het huidige artikel 125i Sv (zie hiervoor onder 6.2), meent het kabinet dat het voorstel van de Commissie moet worden overgenomen dat voorzien moet worden in een regeling die betrekking heeft op de gegevens die niet begrepen zijn onder de specifieke telecommunicatiebevoegdheden. Bij de normering daarvan zal rekening gehouden worden met de reeds voor de sector geldende en in voorbereiding zijnde wetgeving. In aanvulling op het wetsvoorstel vorderen gegevens telecommunicatie dient daarom bij de uitwerking van de voorstellen van de Commissie gekomen te worden tot een bevoegdheid die betrekking heeft op de gegevens die niet reeds begrepen zijn onder de specifieke telecommunicatiebevoegdheden. Ook dienen de bevoegdheden betreffende het bewerken en het beschikbaar houden van gegevens voor deze sector van toepassing te zijn. Naar verwachting zullen de nieuwe bevoegdheden niet tot extra investeringen behoeven te leiden voor de aanbieders van openbare telecommunicatienetwerken en -diensten. Bij gelegenheid van het wetsvoorstel zal dit nader aan de orde komen. Met de sector zal overleg plaatsvinden over de wijze van toepassing van deze bevoegdheden.

6.4. Wetsvoorstel vorderen gegevens financiële sector

Ter uitvoering van het protocol bij het EU-rechtshulpverdrag (Trb 2000, 96) is als onderdeel van het Actieplan Terrorismebestrijding en veiligheid (Kamerstukken II 2001/2002, 27 925, nr. 10, blz. 14) het wetsvoorstel vorderen gegevens financiële sector opgesteld. Het wetsvoorstel is ter advisering voorgelegd aan de Raad van State. Het wetsvoorstel betreft de regeling in het Wetboek van Strafvordering van bevoegdheden tot het vorderen van gegevens van instellingen in de financiële sector. Het betreft bevoegdheden die geheel overeenkomen met de hiervoor onder 4.1–4.4. besproken bevoegdheden. In verband met de gebeurtenissen die op 11 september 2001 hebben plaatsgevonden in de Verenigde Staten van Amerika is binnen de Europese Unie besloten tot een versnelde totstandkoming van het protocol en zijn de lidstaten gehouden tot ratificatie van het protocol voor het einde van het jaar 2002. Om die reden dient het wetsvoorstel vooruit te lopen op de wetgeving ter uitvoering van de hiervoor besproken voorstellen. Indien de wetgeving ter uitvoering van de hiervoor besproken voorstellen echter tot stand komt en in werking treedt wordt daarmee de wetgeving voor de instellingen in de financiële sector overbodig en kan deze vervallen. Voor de instellingen in de financiële sector heeft dit geen gevolgen, nu de bevoegdheden hetzelfde blijven.

7. Conclusie

Het kabinet herkent de weergave van de huidige praktijk zoals deze door de Commissie Strafvorderlijke gegevensvergaring in de informatie-maatschappij is beschreven en de knelpunten die zich daarin voordoen. Het onderschrijft de uitgangspunten voor nieuwe wetgeving die door de Commissie zijn opgesteld. Op hoofdlijnen neemt het kabinet de voorstellen van de Commissie voor nieuwe bevoegdheden in het Wetboek van Strafvordering, als hiervoor besproken, over. Op de enkele onderdelen wijkt het kabinet van de voorstellen af.

Een belangrijke aanpassing is dat de bevoegdheid tot het vorderen van identificerende gegevens en de bevoegdheid tot het vorderen van toekomstige gegevens alleen kunnen worden toegepast jegens de houder van gegevens die anders dan ten behoeve van persoonlijk gebruik gegevens verwerkt. Identificerende gegevens kunnen niet worden gevorderd in het kader van een verkennend onderzoek. Ook wordt de bevoegdheid tot het vorderen dat geautomatiseerde gegevens gedurende een bepaalde periode beschikbaar blijven, neergelegd bij de officier van justitie. De periode kan evenwel – gelet op het Verdrag Crime in Cyberspace – 90 dagen bedragen. Met betrekking tot de bevoegdheid betreffende het bewerken van gegevens heeft het kabinet een ander wettelijk kader voor ogen dan de commissie voorstelt. Dit zal nog afzonderlijk aan adviserende instanties worden voorgelegd.

Daarnaast stelt het kabinet in aanvulling op de voorstellen van de Commissie het volgende voor. Voorgesteld wordt te bepalen dat de bevoegdheid tot het vorderen van identificerende gegevens alleen door daartoe aangewezen en geautoriseerde opsporingsambtenaren kan worden toegepast. Tevens wordt voorgesteld dat politie en het openbaar ministerie inzicht moeten geven in de aantallen malen dat de bevoegdheden worden toegepast, alsmede in de verdere verwerking van de daarmee verkregen gegevens. Op termijn komt er een verplichting voor de politie om periodiek een *audit* te laten verrichten op de gegevensverwerking. Hiermee wordt uitvoering gegeven aan het project van zelf-evaluaties waarmee reeds een start is gemaakt. Op termijn zal op basis daarvan de Wet politieregisters worden aangepast. Daarbij zullen kwaliteitseisen aan de *audit* worden gesteld. Overwogen wordt het CBP te belasten met het toezicht op deze *audits*.

Een wetsvoorstel betreffende deze voorstellen zal worden voorbereid. Daarbij wordt het concept-wetsvoorstel zoals dit in het rapport van de Commissie is opgenomen als uitgangspunt genomen en met inachtneming van het hiervoor gaande uitgewerkt.

Advies is uitgebracht door de Nederlandse Vereniging van Banken (NVvB), het College Bescherming Persoonsgegevens (CBP), de Koninklijke Marechaussee (Kmar), het Overlegorgaan Post en Telecommunicatie, Deelorgaan aftappen (OPT/DAF), De Nederlandsche Bank (DNB), het Korpsbeheerdersberaad en de Raad van Hoofdcommissarissen (KBB/RHC), de Koninklijke Notariële Broederorganisatie (KNB), het openbaar ministerie (OM), het Verbond van Verzekeraars (VvV), de Nederlandse Orde van Advocaten (NOvA), de Nederlandse Vereniging voor Rechtspraak (NVvR) en het Platform Bijzondere Opsporingsdiensten (PBOD). De meeste adviezen delen de conclusie van het rapport dat het gewenst is te komen tot een stelsel van bevoegdheden in het Wetboek van Strafvordering. De meeste adviezen bevestigen dat de voorstellen tegemoet komen aan knelpunten in de praktijk. CBP en NOvA menen dat de voorstellen onevenwichtig zijn: de balans slaat teveel door in het voordeel van de opsporing. Zij menen dat meer aandacht nodig is voor de belangen van degene op wie de gegevens betrekking hebben. Nu in beginsel elk gegeven relevant kan zijn voor de opsporing is de reikwijdte van de bevoegdheden zeer ruim. Zij zien een risico in de informatiehonger van de politie. Ook in de adviezen van de NVvB en het OPT wordt hierop gewezen. Het OM, de Kmar en PBOD bepleiten ruimte te houden voor vrijwilligheid. Het CBP daarentegen meent dat daarvoor geen ruimte meer mag bestaan: het Wetboek van Strafvordering dient een uitputtende regeling te bevatten. De NVvR heeft een voorkeur voor vergaring op basis van vrijwilligheid. Zij vindt het niet wenselijk en niet proportioneel direct een verplichting tot verstrekken in te zetten, terwijl op basis van vrijwilligheid waarschijnlijk hetzelfde resultaat kan worden bereikt. Waar het gaat om gegevens van derden geeft de NVvR in overweging een artikel in de WBP op te nemen, waarin de bevoegdheid tot verstrekking ten behoeve van strafvorderlijk optreden wordt opgenomen en waarbij de afweging van belangen bij de tot opsporing bevoegde instanties wordt gelaten. Indien niet op basis van vrijwilligheid wordt verstrekt zou de officier van justitie met machtiging van de rechter-commissaris kunnen bevelen dat de derde de gegevens verstrekt.

De NOvA meent dat de bevoegdheid tot het vorderen van identificerende gegevens in feite een informatieplicht inhoudt en dat deze aan te weinig beperkingen is gebonden. De NOvA stelt als beperkingen voor dat de bevoegdheid alleen betrekking zou mogen hebben op gegevens van de verdachte, alleen gericht zou mogen worden tot de houder van wie redelijkerwijs vermoed wordt dat hij toegang heeft tot de gegevens en alleen in geval van verdenking van misdrijven als bedoeld in artikel 67 Sv. Dit laatste is ook door de NVvB naar voren gebracht, die bovendien meent dat de tussenkomst van de officier van justitie nodig is. Het VvV bepleit zwaardere eisen aan de motivering waarom aan de houder gegevens worden gevorderd. De NOvA meent dat ook de bevoegdheden tot het vorderen van andere dan identificerende gegevens en tot het vorderen van gevoelige gegevens beperkt moeten worden tot gegevens van de verdachte.

Veel adviezen zijn negatief over het voorstel de bevoegdheid tot het vorderen van identificerende gegevens toe te staan in een verkennend onderzoek.

Het CBP meent dat de bevoegdheid tot het vorderen van toekomstige gegevens gericht moet worden ingezet en beperkt moet worden tot gegevens betreffende de verdachte. De NVvB meent dat het direct doorgeleiden van toekomstige gegevens (monitoren) teveel inspanningen zal vergen van de banken.

Het CBP meent dat er aanleiding is te komen tot een bevoegdheid tot het vorderen dat gegevens beschikbaar blijven (bevriezen). Het OPT meent dat voor deze bevoegdheid zwaardere waarborgen nodig zijn. Ook de

NVvB pleit daarvoor. De NOvA vindt dat deze bevoegdheid een te actieve opstelling van de houder van de gegevens vraagt en meent dat de verschoningsplicht van de advocaat zich er niet mee verhoudt. Het CBP, de NOvA en het OPT/DAF zijn negatief over het voorstel te komen tot een bevoegdheid tot het vorderen van een bewerking van gegevens. Zij menen dat houders van gegevens te zeer worden betrokken bij het verrichten van opsporingshandelingen en dat sprake is van een te vergaande inbreuk op de persoonlijke levenssfeer. Het OM is positief over deze bevoegdheid en meent dat geen machtiging van de rechter-commissaris zou moeten zijn vereist.

Het CBP en de NOvA bevelen aan, te komen tot een regeling voor het vorderen van gegevens in de omgeving van de beroepsgeheimhouders. De KNB bepleit dat de voorzitter van de plaatselijke ring bij de zaak wordt betrokken indien in het kader van strafvorderlijke activiteiten het beroepsgeheim van een notaris in het geding komt.

Het CBP bepleit een opschortend beklagrecht voor de verstrekker en meer aandacht voor de notificatie (mededeling achteraf aan de betrokkene). Ook DNB en de NVvB bepleiten dit.

Het CBP meent dat meer controle op de naleving van de Wet politie-registers is vereist. De adviezen ondersteunen dat de kosten die verbonden zijn aan het voldoen aan een vordering tot het verstrekken van gegevens, vergoed dienen te worden. Ook dient de verstrekker van de gegevens niet aansprakelijk te zijn indien de verstrekking van gegevens tot schade voor betrokkenen leidt.

Het advies van het OPT/DAF spreekt van een onwenselijke uitbreiding van opsporingsbevoegdheden in relatie tot de regeling van de huidige bevoegdheden voor de sector van de telecommunicatieaanbieders. Betreurd wordt dat de duidelijkheid die het wetsvoorstel vorderen gegevens telecommunicatie¹ schept nu weer tenietgedaan wordt. Men bepleit een meer op de sector toegesneden regeling van de algemene bevoegdheid.

¹ Kamerstukken II 2001/2002, 28 059, nrs. 1–3.