PLATFORM BOD
BIJZONDERE OPSPORINGS DIENSTEN

> Postbus 19266 3501 DG UTRECHT

Telefoon
Telefax (088) 1550275
Doorkiesnummer

Datum
26 maart 2015
Uw kenmerk

Ons kenmerk

Betreft
Bijlage 1 bij brief met kenmerk

Reactie Platform Bijzondere Opsporingsdiensten inzake concept-Contourennota Modernisering Wetboek van Strafvordering, kenmerk MinVenJ

Op 3 februari 2015 heeft het platform BOD'en (hierna: het Platform) de contourennota met brief van de Minister van Veiligheid & Justitie in goede orde ontvangen.

Het Platform heeft met belangstelling kennis genomen van de inhoud van deze contourennota en maakt bij deze graag gebruik van de gelegenheid om op de inhoud van deze contourennota in te gaan. Hierbij volgt het Platform niet altijd de volgorde waarin de contourennota de verschillende onderwerpen beschrijft, maar verwijst wel steeds naar de betreffende paragrafen van de contourennota. Het Platform zal verder niet op alle punten in de contourennota ingaan, maar behoudt zich het recht voor om bij de consultaties van de onderscheiden conceptwetsvoorstellen alsnog opmerkingen te maken indien daartoe aanleiding bestaat.

Overzicht en consistentie van de voorstellen
In het algemeen zullen de komende periode een behoorlijk aantal wetsvoorstellen het licht gaan zien die gaan bijdragen aan de modernisering van het Wetboek van Strafvordering. Sommige van die voorstellen beogen slechts een systematische ordening, maar andere zullen meer inhoudelijke wijzigingen tot stand gaan brengen. Het is op dit moment lastig om te overzien hoe alle voorstellen en denkrichtingen zullen uitwerken en of en in hoeverre ze invloed op elkaar zullen uitoefenen.

Als voorbeeld kan genoemd worden, de in de paragrafen 1.3 en 2.2.2 van Deel II van de contourennota voorgestelde vereenvoudiging van de verdenkingscriteria naar de abstracte ernst van een strafbaar feit. Deze vereenvoudiging werkt onder andere door naar de gevallen waarin een bepaalde bevoegdheid kan worden toegepast. Een van de voorgestelde criteria is: "misdrijf waarop een gevangenisstraf van 4 jaar of meer is gesteld", dat zal worden gehanteerd bij een aantal bevoegdheden zoals het opnemen van vertrouwelijke communicatie en het opnemen van telecommunicatie. Voor enkele misdrijven zal dit ook voor de BOD'en in de toekomst betekenen dat de genoemde bevoegdheden niet meer kunnen worden ingezet.

In dit verband valt bijvoorbeeld te denken aan misdrijven als bedoeld in artikel 272 WvSr (schending van ambtsgeheimen; maximaal 1 jaar gevangenisstraf), artikel 321 WvSr (verduistering, bijvoorbeeld in het kader van beleggingsfraude; maximaal 3 jaar gevangenisstraf), artikel 323a WvSr (fraude met gemeenschapsgelden; maximaal 3 jaar gevangenisstraf) en artikel 420quater WvSr (schuldwitwassen; maximaal 2 jaar gevangenisstraf). Ook voor de opsporing van WED-delicten waarvoor maximaal 2 jaar gevangenisstraf kan worden opgelegd (art. 6 lid 1 onder 2e WED) zal de voorgenomen vereenvoudiging van de verdenkingscriteria op dit vlak gevolgen hebben.

Het Platform meent dat het ongewenst is wanneer de toepassing van bevoegdheden als het opnemen van vertrouwelijke communicatie en telecommunicatie bij de opsporing van dit soort misdrijven niet langer mogelijk zou zijn. Het Platform plaatst dan ook een kanttekening bij de opmerking in de contourennota op pagina 44 dat de gevolgen van een vereenvoudiging van de verdenkingscriteria wat betreft de opsporingsbevoegdheden 'niet groot zijn'.

In par. 4.2 van Deel I van de contourennota wordt aangegeven dat er een integrale concepttekst van het nieuwe Wetboek van Strafvordering zal worden bijgehouden. Het Platform zou het op prijs stellen als deze integrale concepttekst op de een of andere manier kan worden geraadpleegd of ter beschikking kan worden gesteld, zodat het Platform de effecten die de verschillende wijzigingen zullen hebben op de opsporingspraktijk en processen van de BOD'en, intern en tijdig kan toetsen. Indien nodig kan het Platform dan de daarbij geconstateerde inconsistenties of nieuwe knelpunten voor de opsporingspraktijk signaleren.

Specifieke wensen van het platform BOD'en

1. Gelijkstelling bijzondere en algemene opsporingsambtenaren

Het Platform is van mening dat er geen onderscheid moet worden gemaakt tussen algemene opsporingsambtenaren van de BOD'en en die van de Nationale Politie met betrekking tot het toekennen van opsporingsbevoegdheden, tenzij daarvoor een gerechtvaardigd belang is aan te wijzen. Voor een gelijkstelling van opsporingsambtenaren van de BOD'en (en die van de Koninklijke Marechaussee) met die van de politie is met name reden gezien de maatschappelijke ontwikkelingen in de afgelopen jaren. Deze ontwikkelingen hebben ertoe geleid dat het inzetten van specifieke (bijzondere) opsporingsbevoegdheden door de BOD'en steeds vaker noodzakelijk is. Immers, de criminaliteit die zich voordoet op de taakgebieden van de BOD'en is de afgelopen jaren steeds zwaarder en georganiseerder geworden en de fraudes complexer, waardoor meer traditionele opsporingsbevoegdheden als het opnemen van telecommunicatie (art. 126m/t WvSv) in veel gevallen niet meer toereikend zijn om het strafrechtelijke bewijs rond te krijgen.

Dat vraagt om bewustwording en efficiency en vereist dat de opsporingsambtenaren van de BOD'en evenals die van de Nationale Politie en de Koninklijke Marechaussee in beginsel de beschikking krijgen over alle opsporingsbevoegdheden om de ondermijnende criminaliteit effectief op te sporen en een halt toe te roepen, alsmede om crimineel vermogen af te pakken. Dit is mede mogelijk omdat de professionalisering van de medewerkers van de BOD'en gelijke tred heeft gehouden met de ontwikkelingen in de georganiseerde criminaliteit. In een aantal recentere onderzoeken is gebleken dat het kunnen opnemen van vertrouwelijke communicatie (art. 126l/s WvSv) essentieel is geweest voor het succesvol verzamelen van bewijsmateriaal dat een bijdrage levert aan het succesvol afsluiten van strafrechtelijke onderzoeken. Ook het stelselmatig inwinnen van informatie (art. 126j/qa WvSv) draagt in onderzoeken steeds vaker bij aan essentiële onderdelen van de bewijsvoering. Daarnaast ervaart de maatschappij fraude steeds meer als ernstig en heeft fraude de laatste jaren meer en meer de aandacht van de politiek. Deze ontwikkelingen rechtvaardigen de inzet van specifieke en zwaardere opsporingsmiddelen in grote fraudezaken.

In het voorstel rondom de bijzondere opsporingsbevoegdheden wordt voor de stelselmatige informatie-inwinning en de infiltratie thans onderscheid gemaakt tussen opsporingsambtenaren van politie (art. 141 onder b WvSv) enerzijds en de algemene opsporingsambtenaren van de Koninklijke Marechaussee (art. 141 onder c WvSv) en de BOD'en (art. 141 onder d WvSv) anderzijds. Deze laatsten kunnen momenteel alleen in samenwerking met de politie deze bevoegdheden uitoefenen, mits zij voldoen aan bij amvb te stellen eisen van bekwaamheid (opleiding).

Een aantal medewerkers van de FIOD zijn opgeleid en qua kennis en vaardigheden op met name financieel-economisch gebied in staat om deze bevoegdheden uit te oefenen. Als gevolg van de regeling dat zij slechts in samenwerking met (en in ondergeschiktheid aan) de politie (DLOS) de genoemde bevoegdheden mogen uitoefenen, zijn de BOD'en hierbij echter afhankelijk van de prioriteitenstelling van de Nationale Politie. Deze prioriteitenstelling leidt er in bepaalde gevallen toe dat fraudeonderzoeken, waarin de inzet van de speciaal opgeleide medewerkers en hun specialistische kennis essentieel is, worden achtergesteld bij onderzoeken die door de politie worden uitgevoerd. Dit heeft tot gevolg dat een fraudeonderzoek moet worden gestopt, of voorlopig moet worden stilgelegd in afwachting van het vrijkomen van de benodigde capaciteit bij de Nationale Politie, terwijl die capaciteit bij de BOD'en al voorhanden is.

In het streven naar maximale efficiency en effectiviteit in strafrechtelijke onderzoeken naar ernstige fraude is het voor de BOD'en, mede gelet op het voorgaande, noodzakelijk om *zelfstandig* bevoegdheden en bijzondere opsporingsmiddelen in te kunnen zetten. Overigens moeten de kennis- en vaardigheidsvereisten als hiervoor bedoeld, onverkort gelden voor álle opsporingsambtenaren en opsporingsdiensten en zal op dit gebied de samenwerking met de Nationale Politie worden voortgezet. Het is dan aan de BOD'en om op enig moment te besluiten om dit soort heimelijke bevoegdheden in te gaan zetten en daartoe te investeren in de opleiding en inzet van medewerkers of middelen, dan wel daarin uitdrukkelijk de samenwerking te zoeken met de Nationale Politie.

2. *Professioneel verschoningsrecht*

In par. 2.1.5 van Deel II (p. 39) wordt terecht opgemerkt dat het hebben van een geheimhoudingsplicht niet zonder meer leidt tot een verschoningsrecht ex artikel 218 WvSv, maar dat daarvoor ook aanvullende eisen moeten zijn vervuld. Vervolgens wordt opgemerkt dat de geheimhoudingsplichten niet in het Wetboek van Strafvordering zijn geregeld, zodat dit onderwerp binnen het project modernisering WvSv niet verder zal worden meegenomen. Wel zal aan de hand van de jurisprudentie van de HR nader worden ingekaderd in welke gevallen een geheimhoudingsplicht tot een verschoningsrecht kan leiden. Dit voorstel treft naar onze mening slechts een deel van de problematiek van het professioneel verschoningsrecht in het strafproces.

Het professioneel verschoningsrecht is een zeer belangrijk item dat zich bij uitstek leent om in het Wetboek van Strafvordering geregeld te worden. Het Platform stelt daartoe een aantal oplossingsrichtingen voor, die ieder voor zich maar ook in onderlinge samenhang (een deel van) de problematiek kunnen oplossen:

1. *Reikwijdte strafvorderlijk verschoningsrecht*
   Geef justitiabelen meer duidelijkheid over de (oorspronkelijke) strekking en omvang van het strafvorderlijk verschoningsrecht, door in de wet of in de Memorie van Toelichting te omschrijven wat er in ieder geval wel en wat er in ieder geval niet onder het strafvorderlijk verschoningsrecht valt. Anders gezegd: de Memorie van Toelichting zou een nadere, niet limitatieve, toelichting kunnen geven over het wettelijke begrip "als zodanig toevertrouwd" in (het te concipiëren equivalent van) artikel 218 WvSv. Hierbij kan met name gedacht worden aan de uitwisseling van informatie tussen cliënt en de verschoningsgerechtigde in zijn hoedanigheid van advocaat of notaris, in het kader van de klassieke hulpverlening of bijstand in relatie tot rechtsgedingen die rechtens niet anders dan door een advocaat of notaris kan worden verleend. Het Platform meent dat in dit kader aan twee onderwerpen aandacht zou moeten worden besteed:

a. Een omschrijving van welke werkzaamheden wel door een verschoningsgerechtigde 'als zodanig' worden verricht en welke niet. Bij dit laatste moet onder andere gedacht worden aan werkzaamheden als fiscaal en bedrijfsadvies, bestuur van een vennootschap of trust, vastgoedadvies of forensisch onderzoek, of aan gevallen als het waarnemen als getuige van een strafbaar feit.
b. Het verschoningsrecht strekt zich niet uit over informatie in welke vorm dan ook, die dient te worden opgenomen in openbare registers of voor gebruik tegenover derden, zoals leveringsaktes voor registergoederen en volmachten.

2. *Codificatie van het begrip 'zeer buitengewone omstandigheden'*
In de jurisprudentie is de doorbreking van het verschoningsrecht op grond van de aanwezigheid van zeer buitengewone omstandigheden mogelijk gemaakt, waarbij de toetsing plaatsvindt door de rechter-commissaris. Het Platform hecht zeer aan de codificatie van deze jurisprudentie. Het medisch verschoningsrecht bijvoorbeeld, leidt in de praktijk tot het blokkeren van efficiënte opsporingsonderzoeken in de gezondheidszorg. Dit kan worden ondervangen door de zeer buitengewone omstandigheden voor doorbreking van het verschoningsrecht in de wet op te nemen, waarbij in de Memorie van Toelichting als (niet limitatief) voorbeeld gevallen van zeer ernstige zorgfraude kunnen worden genoemd. Op deze wijze zal de Nederlandse wetgeving ook beter aansluiten op vergelijkbare wetgeving in andere landen die een wettelijke 'fraud exemption' kennen op het verschoningsrecht.
Daarnaast ontstaat hierdoor de mogelijkheid om de startinformatie jegens een verdachte verschoningsgerechtigde, na toetsing door de rechter-commissaris, aan het dossier toe te voegen zonder deze eerst te moeten voorleggen aan de verdachte verschoningsgerechtigde zelf, hetgeen om opsporingstechnische redenen niet wenselijk is.

3. *Waarborgeisen met betrekking tot digitale verschoningsgerechtigde informatie*
Zoals hierna onder punt 4 nog zal worden toegelicht, is het met name bij vastgelegde gegevens, maar ook bij de inbeslagneming van digitale gegevensdragers praktisch onmogelijk om potentieel verschoningsgerechtigde informatie vooraf uit te sluiten. Het huidige Wetboek van Strafvordering kent hiervoor ook geen uitzondering. De hypothetische mogelijkheid dat opsporingsambtenaren van dergelijke informatie kennis zouden kunnen nemen is dan ook vaak grond voor de verdediging tot het voeren van verweren op dit punt.
De jurisprudentie lijkt op dit punt wel ruimte te bieden: indien de procedures bij de inbeslagneming of vastlegging van gegevens(dragers) en het onderzoek in die gegevens voldoende waarborgen bieden waarmee het strafvorderlijk verschoningsrecht gewaarborgd wordt, is het vastleggen van potentieel verschoningsgerechtigde informatie of de inbeslagneming van gegevensdragers die dergelijke informatie bevatten niet bij voorbaat onrechtmatig. Het is wenselijk deze jurisprudentie te codificeren, zodat de huidige werkwijze niet langer (noodgedwongen) buitenwettelijk is.

4. *Efficiënte toetsingsprocedure verschoningsgerechtigde informatie*
De huidige jurisprudentie legt het oordeel of er sprake is van informatie die onder het strafvorderlijke verschoningsrecht valt, primair bij de verschoningsgerechtigde zelf. Dit oordeel moet worden gerespecteerd, tenzij daaraan redelijkerwijs kan worden getwijfeld, of wanneer het vragen van een dergelijk oordeel om praktische redenen niet mogelijk is. Dit laatste is bijvoorbeeld het geval wanneer tijdens een doorzoeking door de officier van justitie als bedoeld in art. 96c WvSv bedrijfsadministratie in beslag is genomen waarin zich potentieel[1] verschoningsgerechtigde informatie bevindt.

[1] Potentieel, omdat ten eerste nog niet kan worden ingeschat of informatie inderdaad onder een verschoningsrecht valt en ten tweede omdat bij de inbeslagneming of vastlegging niet altijd vooraf al bekend is dát en zo ja, waar dergelijke informatie zich in die administratie bevindt.

Het Platform is voorstander van een toetsingsprocedure waarin de rechter-commissaris primair de inhoud van informatie toetst om te beoordelen of die informatie onder het verschoningsrecht valt en zo ja, of er zeer buitengewone omstandigheden zijn die maken dat het verschoningsrecht moet wijken voor het belang van de waarheidsvinding. Op deze manier kan de betreffende informatie sneller beschikbaar komen voor het onderzoeksteam. Als tegenwicht kan de beklagprocedure van artikel 552a WvSv dienen, die per 1 maart 2015 overigens is aangevuld door de invoering van een aantal in het kader van die procedure in acht te nemen termijnen.

Het Platform meent dat hiertoe artikel 98 WvSv tot een algemene regeling kan worden omgevormd, zodat de rechter-commissaris in alle gevallen beslist over de kennisneming van informatie die mogelijk onder het verschoningsrecht valt, alsmede over de vraag of in voorkomende gevallen sprake is van zeer uitzonderlijke omstandigheden die maken dat het belang van de waarheidsvinding moet prevaleren boven het belang dat het verschoningsrecht beoogt te beschermen.

3. Gegevensvergaring: nationale en grensoverschrijdende aspecten

Toestemming tot kennisneming van inhoud gegevensdragers

In paragraaf 3.8 van de discussienota over gegevensvergaring[2] wordt voorgesteld het onderzoek aan of in (in beslag genomen) digitale gegevensdragers, waaronder smartphones en computers, afhankelijk te maken van voorafgaande toestemming van een officier van justitie. In paragraaf 2.2.6 van Deel II van de contourennota wordt in dit kader onder andere opgemerkt dat het niet goed valt te rechtvaardigen dat het onderzoek in een computer en het vastleggen van daarop opgeslagen gegevens tijdens een doorzoeking wel met specifieke waarborgen is omgeven, terwijl dat niet het geval is wanneer diezelfde computer tijdens de doorzoeking in beslag wordt genomen en vervolgens wordt onderzocht.

De minister wil daarom – en kennelijk in alle gevallen waarin sprake is van de inbeslagneming van digitale gegevensdragers – de waarborgen die gelden voor het tijdens een doorzoeking vastleggen van gegevens (zie art. 125i WvSv e.v.) van overeenkomstige toepassing laten zijn. In dit verband valt echter niet goed te rijmen dat die waarborgen per se een toestemmingsvereiste van de officier van justitie of een machtiging van een RC zouden moeten bevatten. In de huidige regeling zoals neergelegd in artikel 125i WvSv en verder is immers ook niet vereist dat toestemming gegeven wordt om de vastgelegde gegevens inhoudelijk te onderzoeken. Andere bevoegdheden die bijdragen aan de waarheidsvinding, zoals de opsporingsfouillering, vereisen in het nieuwe wetboek bovendien kennelijk juist geen bevel van de officier van justitie of een machtiging van de rechter-commissaris meer, waar dat momenteel wel is voorgeschreven (zie hiervoor bijvoorbeeld par. 3.5 van Deel II).

Ten tweede is in geval van een doorzoeking al vooraf besloten dat voor het onderzoek relevante gegevens die tijdens de doorzoeking kunnen worden aangetroffen, zullen worden vastgelegd. Deze vastlegging van gegevens heeft, net als de inbeslagneming van de digitale gegevensdragers of andere voorwerpen, als primaire doel om de waarheid aan de dag te brengen. Uit deze vatbaarheidsgrond en uit staande jurisprudentie van de HR is zonder meer af te leiden dat dit impliceert dat de vastgelegde gegevens en de in beslag genomen gegevensdragers worden onderzocht op informatie die kan bijdragen aan de waarheidsvinding. Zo beschouwd is het onderzoek van in beslag genomen gegevensdragers en vastgelegde gegevens een *implied power* oftewel onlosmakelijk verbonden aan de bevoegdheden tot inbeslagneming respectievelijk de vastlegging van gegevens. Hierbij past dan niet dat er een extra schakel wordt tussengevoegd in de vorm van een toestemmingsvereiste voor het onderzoeken van de opgeslagen gegevens. Die toestemming zal in de praktijk overigens naar alle waarschijnlijkheid ook vrijwel altijd worden verleend, aangezien zonder kennisneming van de inhoud van de opgeslagen gegevens geen toets op relevantie van die gegevens mogelijk is.

---

[2] Zie http://www.rijksoverheid.nl/onderwerpen/wetgeving-en-rechtsgebieden/documenten-en-publicaties/publicaties/2014/06/06/onderzoek-ter-plaatse-inbeslagneming-en-doorzoeking-en-onderzoek-van-gegevensdragers-en-in-geautomatiseerde-werken-discussiestuk.html; laatstelijk geraadpleegd op 18 februari 2015.

Bovendien is de mate van privacygevoeligheid van digitale en analoge gegevens niet zonder meer verschillend en kan dan ook niet dienen als onderscheidend criterium voor het al dan niet vereisen van toestemming tot kennisneming van die gegevens. Tijdens een klassieke doorzoeking in een woning zullen vaak zelfs meer privacygevoelige gegevens worden ingezien (ter beoordeling op relevantie voor de waarheidsvinding en inbeslagneming of vastlegging ervan) dan er gegevens worden vastgelegd, omdat bij de klassieke doorzoeking alle ruimten en voorwerpen in de woning systematisch en grondig worden bekeken. De vraag is dus gerechtvaardigd of een klassieke doorzoeking uiteindelijk niet meer inbreuk maakt op de privacy van de bewoners dan de vastlegging van digitale gegevens.

Daar komt bij dat het vaak niet mogelijk is om digitale gegevens te scheiden in voor het onderzoek wel of niet relevante gegevens. Verder is het vaak noodzakelijk om een complete image te maken in verband met onderzoek naar verborgen en gewiste bestanden. Om die reden moet doorgaans de complete gegevensdrager in beslag worden genomen of geïmaged (ex art. 125i WvSv e.v.).[3] Tijdens doorzoekingen worden er zodoende noodzakelijkerwijs vaak grote hoeveelheden digitale gegevens (variërend van enkele MB's tot ettelijke TB's) vastgelegd. Deze gegevens kunnen echter vervolgens alleen efficiënt en doelgericht worden onderzocht met behulp van forensische tools en voor het onderzoek relevante trefwoorden. Hetzelfde geldt overigens voor het onderzoek aan in beslag genomen gegevensdragers en computers. Bijgevolg zullen in beide gevallen vele bestanden nooit daadwerkelijk worden ingezien, hoewel die mogelijkheid in theorie aanwezig is.

Bovendien moet onderscheid gemaakt worden in de mate van privacygevoeligheid van gegevens en in de soort en opslagcapaciteit van gegevensdragers. Denk hierbij bijvoorbeeld aan allerlei apparatuur die steeds vaker met microchips worden uitgerust. De vraag is dan steeds aan de orde of en in hoeverre door kennisneming van die gegevens een min of meer compleet beeld van iemands privéleven kan worden verkregen. Digitale bedrijfsadministratie zal mede om die reden dan ook niet even privacygevoelig zijn als gegevens die op een smartphone zijn opgeslagen. Wat dit laatste betreft moet ook aandacht gegeven worden aan het feit dat de burger deze gegevens ook zelf en bewust op andere manieren vastlegt: voorheen plakte hij de gemaakte foto's in een fotoalbum, tegenwoordig staan diezelfde foto's steeds vaker of nog uitsluitend in de cloud of op een gegevensdrager.

Gelet op het vorenstaande is het Platform van mening dat het onderzoek van tijdens een doorzoeking vastgelegde gegevens of in tijdens een doorzoeking in beslag genomen gegevensdragers impliciet al is gegeven op het moment dat een officier van justitie of een rechter-commissaris heeft besloten dat er een doorzoeking zal plaatsvinden. Dit besluit zal mede of grotendeels zijn gebaseerd op het vermoeden dat tijdens de doorzoeking voorwerpen of gegevens zullen worden gevonden die kunnen bijdragen aan de waarheidsvinding. De doorzoeking is immers een steunbevoegdheid voor de inbeslagneming of de vastlegging en in die bevoegdheden ligt, zoals hiervoor al aangegeven, een *implied power* besloten om de in beslag genomen gegevensdragers en vastgelegde gegevens te onderzoeken.

Daarnaast zal de vatbaarheidsgrond 'waarheidsvinding' er in alle gevallen toe leiden dat een eventuele toestemming tot onderzoek van gegevens gegeven zal worden, waarmee deze toestemming wordt gereduceerd tot een formele letter en haar doel, te weten privacybescherming, voorbij zal schieten. Daarentegen zal de lastendruk bij de officieren van justitie of RC's toenemen als de wet zal bepalen dat zij eerst toestemming moeten verlenen voordat in beslag genomen gegevensdragers of vastgelegde gegevens daadwerkelijk mogen worden onderzocht. En elke gegeven toestemming zal tevens moeten worden vastgelegd hetgeen ook voor de opsporingsinstanties een onnodige lastenverzwaring inhoudt.

---

[3] Zie in dit verband ook EHRM 14 maart 2013, nr. 24117/08 (Bernh Larsen Holding vs. Noorwegen). In deze zaak vorderde de Noorse belastingdienst op grond van de Noorse fiscale wetgeving de verstrekking van gegevens van een bedrijf, die waren opgeslagen op een server die mede door andere bedrijven werd gebruikt en waarop ook privébestanden van werknemers en derden waren opgeslagen. Het EHRM oordeelde dat art. 8 EVRM niet was geschonden, omdat de procedure van vastlegging van de gegevens met voldoende waarborgen was omgeven. Die waarborgen hielden overigens niet in dat er een (rechterlijke) toestemming zou moeten worden gegeven voor de kennisneming van de aldus vastgelegde gegevens.

Netwerkzoeking en vastlegging van gegevens in de cloud
In verband met het vorige onderwerp vragen wij ook aandacht voor de beperking die de wetsgeschiedenis aan de praktijk heeft opgelegd met betrekking tot de netwerkzoeking en het vastleggen van gegevens die zich buiten Nederland bevinden. Vastlegging van gegevens is niet toegestaan en netwerkzoekingen moeten worden gestaakt indien en zodra blijkt dat gegevens zich buiten Nederland bevinden. Een rechtshulpverzoek is dan vereist om die gegevens alsnog te verkrijgen.

In de huidige tijd, waarin steeds meer gegevens in de cloud worden opgeslagen, is deze beperking niet langer houdbaar en zou moeten worden opgeheven. Daarnaast is een rechtshulpverzoek geen adequate methode om gegevens die zich buiten Nederland bevinden, te verkrijgen. De cloud is immers een ongrijpbaar begrip en de opslag van gegevens in die cloud beperkt zich niet tot één bepaalde, vaste plaats. Gegevens in de cloud kunnen zich tegelijkertijd op verschillende plekken bevinden, of over meerdere plekken zijn verdeeld. Gegevens in de cloud zijn immers zeer vluchtig; het ene moment staan zij bijvoorbeeld op een server in Delfzijl, het volgende moment op een server in Tuvalu. Daarnaast kan de provider die clouddiensten aanbiedt, evenmin aangeven waar gegevens zich op een bepaald moment bevinden.[4]

Gelet op het voorgaande stellen wij voor, overeenkomstig de Belgische wetgeving terzake,[5] een regeling in het wetboek op te nemen waardoor de gegevens die zich buiten Nederland bevinden, in ieder geval kunnen worden veiliggesteld voor het strafrechtelijk onderzoek, eventueel in afwachting van de formele of stilzwijgende toestemming van het betreffende land waar de gegevens waren opgeslagen en voor zover dat land kan worden geïdentificeerd.

Vorderen gegevens
In het kader van de bevoegdheden tot het vorderen van gegevens doet de contourennota in paragraaf 2.2.6 van Deel II drie voorstellen:

a. Beperking van de reikwijdte van de vorderingsbevoegdheden tot gegevens die voor zakelijke doeleinden worden verwerkt;
b. Het laten vervallen van het onderscheid tussen identificerende, gevoelige en andere gegevens;
c. Heroverweging van het uitgangspunt dat opsporingsambtenaren in beginsel niet mogen verzoeken om vrijwillige verstrekking van gegevens.

Ad a. Beperking reikwijdte vorderingsbevoegdheden tot zakelijk verwerkte gegevens

De minister overweegt de reikwijdte van de vordering tot verstrekking van gegevens in het nieuwe wetboek te beperken tot gegevens die voor zakelijke doeleinden, dat wil zeggen anders dan voor persoonlijk of huishoudelijk gebruik worden verwerkt. Het huidige artikel 126nd WvSv bevat deze beperking echter niet: op grond van deze bevoegdheid kunnen andere dan identificerende of gevoelige gegevens worden gevorderd 'van degene van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot bepaalde opgeslagen of vastgelegde gegevens'. Hierbij wordt dus aangeknoopt bij de mogelijkheid van toegang tot bepaalde gegevens en niet bij de hoedanigheid van de persoon die daar toegang toe heeft. De enige restrictie die de wetsgeschiedenis aan de toepassing van deze bevoegdheid heeft gesteld is, dat van degene van wie de gegevens gevorderd worden, geen onevenredige inspanning mag worden gevergd, gelet op de beginselen van proportionaliteit en subsidiariteit. Bovendien hoeft het in deze gevallen ook niet alleen te gaan om persoonsgegevens als bedoeld in de Wet bescherming persoonsgegevens (Wbp). In de formulering van het huidige artikel 126nd WvSv is dan ook niet aangesloten bij de Wbp-begrippen 'verantwoordelijke' of 'bewerker'.[6]

---

[4] In de toelichting op het conceptwetsvoorstel Computercriminaliteit III worden deze aspecten op pagina 9 ook onderkend. Zie www.internetconsultatie.nl/computercriminaliteit, laatstelijk geraadpleegd op 17 februari 2015.

[5] Zie C. Conings & J.J. Oerlemans, 'Van een netwerkzoeking naar online doorzoeking: grenzeloos of grensverleggend?', Computerrecht 2013/5.

[6] Zie *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 23-24.

Voor zover als argument voor de voorgenomen beperking wordt aangevoerd dat van particulieren al niet gevorderd mag worden voor zover zij als verdachte kunnen worden aangemerkt, merkt het Platform op dat een verbod op het vorderen van gegevens bij een verdachte ook nu al in de wet is opgenomen (art. 126nd lid 2 WvSv). In zoverre zal een beperking tot gegevens die voor zakelijk gebruik worden verwerkt, geen invloed hebben op de omstandigheid dat jegens verdachten ook nu al geen vordering tot het verstrekken van gegevens mag worden gedaan.

Aan de andere kant beschikken particulieren, ook wanneer zij geen verdachte zijn, mogelijk over voor een strafrechtelijk onderzoek relevante gegevens. Indien de bevoegdheid tot het vorderen van gegevens zou worden beperkt tot degenen die deze gegevens voor zakelijke doeleinden verwerkt, kan de opsporingsambtenaar dan alleen nog maar gegevens van een particulier verkrijgen voor zover deze vrijwillig daaraan meewerkt. De afweging om gegevens al dan niet aan de opsporing beschikbaar te stellen kan echter niet of niet goed gemaakt worden door die particulier zelf, omdat deze onvoldoende – en nog minder dan verantwoordelijken of bewerkers in de zin van de Wbp – kennis draagt van alle achtergronden van het verzoek. Het is juist dit argument geweest dat ten grondslag heeft gelegen aan de invoering van artikel 126nd WvSv, bezien vanuit de verstrekking van persoonsgegevens op grond van artikel 43 Wbp.[7]

Het niet langer kunnen vorderen van particulieren van de verstrekking van gegevens zal er tevens toe leiden dat bij die particulieren dan de betreffende gegevensdragers in beslag moeten worden genomen, of de nodige gegevens zullen moeten worden vastgelegd via de bevoegdheden als bedoeld in artikel 125i WvSv en verder. Dit zal immers het gevolg zijn wanneer het nieuwe wetboek niet langer de minder ingrijpende mogelijkheid van het vorderen van gegevens bij die particulier mogelijk maakt. Op deze wijze zullen ook veel meer gegevens worden verkregen dan noodzakelijk.[8] Dit lijkt voor het Platform een onwenselijke situatie vanuit het oogpunt van de niet verdachte burger, die niet meer dan strikt noodzakelijk betrokken zou moeten worden bij een strafrechtelijk onderzoek.

Ad b. Onderscheid tussen categorieën van gegevens vervalt

Het Platform ondersteunt dit voorstel, mede gelet op de huidige uitvoeringsproblemen en de onnodige administratieve lasten die door dit onderscheid, alsmede door het onderscheid in bevoegde functionarissen, worden veroorzaakt.
Ter illustratie: indien opsporingsambtenaren een pasfoto van verdachte willen hebben, bijvoorbeeld in verband met de ondersteuning van een observatieteam of het samenstellen van een fotoconfrontatiemap, kunnen zij wel een pasfoto uit het reisdocumentatieregister vragen op grond van artikel 73 Paspoortuitvoeringsregeling, maar moeten zij voor diezelfde pasfoto bij anderen een vordering ex artikel 126nf WvSv doen, gelet op het feit dat de HR in het Translinkarrest (HR 23 maart 2010, *NJ* 2010, 355) heeft bepaald dat een pasfoto in beginsel gevoelige gegevens bevat, zoals etnische afkomst. Dit schijnbaar willekeurige onderscheid in zwaarte van bevoegdheden (een eenvoudige vordering bij het reisdocumentenregister versus een vordering tot uitlevering met machtiging van de RC) is in de praktijk moeilijk uit te leggen en leidt tot onnodige lastenverzwaring.

In dit verband pleit het Platform er tevens voor om, indachtig het uitgangspunt van het project modernisering WvSv, de bevoegdheden tot het vorderen van gegevens toe te kennen aan de opsporingsambtenaren eventueel na een bevel daartoe door de officier van justitie. De opsporingsambtenaren zijn immers degenen die deze bevoegdheden in de praktijk uitvoeren, terwijl deze praktijk ook in het nieuwe stelsel niet anders zal zijn.

---

[7] Zie *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 2.

[8] Zie ook *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 3 en p. 12.

Ad c. Vrijwillige verstrekking van gegevens

De oorspronkelijke ratio achter het beginselverbod op desgevraagde verstrekking van gegevens ten behoeve van de opsporing en de daaruit voortvloeiende verplichting voor een opsporingsambtenaar om die gegevens te verkrijgen door middel van een vordering daartoe is, dat de houder van de gevraagde gegevens vaak niet of onvoldoende in staat zou zijn om de afweging te maken of er een dwingende en gewichtige reden is die verstrekking van gegevens op grond van artikel 43 Wbp noodzakelijk maakt.[9] Aldus werd echter vrijwel iedere vorm van het *desgevraagd* vrijwillig verstrekken van gegevens onmogelijk gemaakt, hetgeen de nodige extra administratieve lasten met zich meebrengt. Er moeten nu immers vorderingen ex artikel 126nd WvSv worden opgemaakt.

Het Platform ondersteunt dan ook het voornemen van de minister om het beginselverbod op vrijwillige verstrekking van gegevens te heroverwegen. In dit verband geeft het Platform nog mee, dat hierbij ook gedacht zou kunnen worden aan een regeling, waardoor in ieder geval de verstrekking van gegevens door overheidsorganen ten behoeve van de opsporing in beginsel zonder daartoe strekkende vordering kan geschieden. Immers, overheidsorganen zijn doorgaans veel beter dan particulieren (zowel burgers als zakelijke gegevensverwerkers) in staat om de juiste afweging als bedoeld in artikel 43 Wbp te maken. Overigens maakt het verbod van vrijwillige verstrekking van gegevens dat BOD'en soms een vordering ex artikel 126nd WvSv moeten doen bij hun 'eigen' inspectie, hetgeen onder meer hogere administratieve lasten met zich meebrengt en in de praktijk leidt tot onbegrip.

4. De getuige en het verhoor bij de politie

In paragraaf 2.1.5 en par. 3.4 van Deel II wordt gesproken over het opnemen van rechten en plichten van een getuige bij een verhoor door opsporingsambtenaren. De vraag is echter of alle rechten en plichten van een getuige, zoals die nu her en der in het wetboek voorkomen, één op één van toepassing kunnen zijn op het getuigenverhoor door een opsporingsambtenaar. Bij eerdere gelegenheden, laatstelijk nog tijdens de expertmeeting getuigen op 15 januari 2015, is voorgesteld om te bezien of niet alle, maar bepaalde rechten en plichten die een getuige heeft bij een verhoor door de RC, niet ook van overeenkomstige toepassing zouden kunnen worden verklaard voor een verhoor door een opsporingsambtenaar. Er wordt dan met name gedoeld op de mogelijkheid van aanwezigheid bij het getuigenverhoor van een raadsman of vertrouwenspersoon ten behoeve van de getuige en van de raadsman van de verdachte. Daarnaast wordt voorgesteld de wijze van vastlegging van het getuigenverhoor en de audiovisuele registratie van getuigenverhoren te codificeren.

Het Platform merkt hierbij op dat daar waar de bestaande praktijken worden gecodificeerd en de beslissing tot het al dan niet toelaten van bepaalde personen tot het getuigenverhoor als discretionaire bevoegdheid bij de officier van justitie komt te liggen, er voor de praktijk geen al te grote impact is te verwachten. Zodra echter die aanwezigheden als een recht in de wet worden vastgelegd dan wel dat auditieve of audiovisuele registratie van getuigen (en dan niet alleen van minderjarigen) een verplichting wordt, zal dat wel degelijk een grote impact hebben op het opsporingsproces. Te denken valt aan de situatie dat in een strafrechtelijk onderzoek meerdere verdachten zijn. Dit betekent dat even zovele raadslieden moeten worden uitgenodigd om bij een getuigenverhoor aanwezig te zijn, hetgeen bijvoorbeeld alleen al agendatechnisch tot problematische situaties zal leiden. Daarnaast zal de aanwezigheid van de raadsman van de verdachte de verklaringsbereidheid van de getuige mogelijk negatief beïnvloeden.

---

[9] *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 2.

Gedelegeerd RC-verhoor
In de praktijk komen opsporingsambtenaren van de BOD'en regelmatig getuigen tegen die intrinsiek verklaringsbereid zijn (bijvoorbeeld accountants of medewerkers van banken) maar vanwege hun civiele aansprakelijkheidsrisico liever door middel van een wettelijke plicht 'gedwongen' willen worden om een getuigenverklaring af te leggen. Momenteel is die wettelijke verplichting mogelijk in de vorm van een RC-verhoor. Daarbij zijn dan de nodige rechten en plichten opgenomen, zoals een verschijningsplicht en een spreekplicht en heeft de verdediging ook het recht om eventueel bij dergelijke verhoren aanwezig te zijn. De praktijk leert echter ook dat de RC vaak niet op korte termijn dergelijke getuigen zelf kan horen en dan gebruik maakt van de mogelijkheid om de uitvoering van dat verhoor te delegeren aan opsporingsambtenaren (ex art. 177 WvSv). Andere redenen van delegatie zijn gelegen in de dossierkennis en vakinhoudelijke kennis die de RC ontbeert of zich pas na enige tijd eigen kan maken. Nadeel van deze delegatiemogelijkheid is momenteel echter, dat gelet op het arrest HR 22 november 1983 (*NJ* 1984, 805) de rechten en plichten bij het RC-verhoor niet meegaan met de delegatie. Het Platform stelt daarom voor, om in het nieuwe wetboek een regeling op te nemen voor het gedelegeerde RC-verhoor, waarin de RC kan beschikken dat een RC-verhoor aan opsporingsambtenaren gedelegeerd kan worden en onder welke voorwaarden dat verhoor kan plaatsvinden.

Gelet op eerdere voorstellen en besprekingen in dit verband, zoals laatstelijk in de expertmeeting getuigen op 15 januari 2015, is er draagvlak voor dit punt. Het Platform verzoekt dan ook aandacht te blijven houden voor een goede regeling van het gedelegeerd RC-verhoor.

5. Nieuwe heimelijke bevoegdheden

Nieuwe bevoegdheden
In paragraaf 2.2.7 van Deel II wordt onder andere voorgesteld enkele nieuwe bevoegdheden op te nemen, waaronder de 'stille sms' met behulp van een IMSI-catcher en het vergaren van persoonsgegevens op het internet. Het Platform ondersteunt dit initiatief van harte, omdat dit geheel aansluit bij de huidige stand van de technologie en deze bevoegdheden inmiddels algemeen aanvaard zijn als reguliere opsporingsmiddelen.

Bovendien kan uit de jurisprudentie ten aanzien van bijvoorbeeld de inzet van een IMSI-catcher worden afgeleid dat er gevallen kunnen zijn waarin die inzet, achteraf bezien, niet gebaseerd kan worden op de algemeen taakstellende artikelen als artikel 3 Wet BOD'en. Een expliciete wettelijke basis van dit soort 'nieuwe' bevoegdheden kan het risico uitsluiten dat een rechter in een concreet geval oordeelt dat de toepassing van zo'n bevoegdheid in de gegeven omstandigheden een meer dan geringe inbreuk op grondrechten heeft gemaakt en de resultaten van die toepassing derhalve als onrechtmatig verkregen van het bewijs worden uitgesloten.

6. Flexibiliteit in modaliteiten van vervolging

In paragraaf 2.6.4 van Deel II wordt onder andere voorgesteld de mogelijkheden tot het aangaan van een schikking te verruimen in die zin, dat het wetboek de mogelijkheid gaat geven om ook een schikking toe te laten na een rechterlijke beslissing in de ontnemingsprocedure. Hiermee wordt een kostbaar executietraject voorkomen. Voor zover in het kader van de ontneming van wederrechtelijk verkregen voordeel een strafrechtelijk financieel onderzoek is gestart, kan dit onderzoek nog maximaal twee jaar na de uitspraak in eerste aanleg voortduren. Een schikkingsmogelijkheid na die uitspraak in eerste aanleg kan ertoe leiden dat dit vaak langdurige onderzoek eerder kan worden gestaakt en de capaciteit die daardoor vrijkomt op andere zaken kan worden ingezet. Het Platform ondersteunt dit initiatief dan ook van harte.

In dit verband denkt het Platform tevens aan andere schikkingsvoorwaarden, zoals het meewerken door een rechtspersoon aan het doen aftreden van bestuurders die als verdachte zijn aangemerkt, of door het doen aanstellen van een integriteitsfunctionaris die met behulp van adequate bevoegdheden binnen de rechtspersoon kan waken voor toekomstig strafbaar handelen en daarop proactief kan reageren. Met het opleggen van dit soort proactieve schikkingsvoorwaarden kan niet alleen de door het strafbare feit ontstane schade worden hersteld, maar ook een op de toekomst gerichte (versterking van de) compliance van de rechtspersoon en haar medewerkers worden bereikt.

7. Internationale samenwerking in strafzaken

In paragraaf 2.7 van Deel II geeft de minister weer welke richting hij wil geven aan de regeling rondom de internationale samenwerking in strafzaken. Het Platform onderschrijft het voorstel om te komen tot één apart boek 7 ten behoeve van alle internationale strafrechtelijke samenwerking, zowel binnenkomend als uitgaand. Hierdoor wordt de complete rechtsmaterie beter toegankelijk gemaakt voor de opsporingspraktijk. Momenteel ontbreekt namelijk een duidelijk overzicht van de regelingen die gelden voor rechtshulpverzoeken aan het buitenland. Daarnaast kan beter ingespeeld worden op de komende ontwikkelingen binnen de EU zoals de Richtlijn inzake het Europees onderzoeksbevel (implementatie verwacht in 2017), waarbij de strafrechtelijke samenwerking tussen de lidstaten onderling sterk zal worden bevorderd. Als gevolg van deze ontwikkelingen zal er een tweedeling gaan ontstaan in het rechtshulpverkeer tussen enerzijds de EU-lidstaten en anderzijds derde landen. Afwijkende rechtshulpprocedures zullen duidelijker zichtbaar gaan worden indien het geheel in één boek te vinden is.

Verder onderschrijft het Platform ten volle de behoefte aan een eenvoudigere regeling van de kleine rechtshulpverlening in Nederland. Ruimere samenwerkingsmogelijkheden, het gelijkschakelen van opsporingsbevoegdheden en het voorkomen van vertragingen bij overdracht van resultaten zijn zaken die de BOD'en vanuit de praktijk graag snel gerealiseerd zou willen zien. Veel zaken zijn door onze nationale regelgeving momenteel namelijk behoorlijk gecompliceerd vormgegeven, waardoor vertraging in de uitvoering en afhandeling optreedt.

De voorgestelde wijziging van de raadkamerprocedures zoals thans neergelegd in de artikelen 552a en 552p WvSv zijn gunstig voor het terugdringen van de termijnen die nodig zijn om bewijsmateriaal aan een verzoekende buitenlandse staat over te dragen. Afschaffing van de verlofprocedure ex artikel 552p WvSv en de opneming van standaard behandeltermijnen in de nieuwe regelgeving zullen hieraan een goede bijdrage leveren en de doorlooptijden van rechtshulpverzoeken in Nederland aanzienlijk verkorten. Bovendien zal de nieuwe mogelijkheid van voorlopige terbeschikkingstelling van bewijsmateriaal aan het buitenland een substantiële verbetering van de internationale opsporingssamenwerking betekenen.

Met betrekking tot de eventuele veranderingen in de mate van rechtsbescherming als gevolg van de modernisering van het wetboek merkt het Platform op dat de rechtsbescherming in feite gelijkgeschakeld wordt aan de nationale bepalingen bij nationale strafrechtelijke onderzoeken. Artikel 552a WvSv voorziet nu en in de toekomst in een beklagmogelijkheid bij inbeslagneming. Dit is ook een gevolg van het volledig doorvoeren van het principe van wederzijdse erkenning bij de justitiële samenwerking in de EU. Beknotting of verkleining van rechtsbescherming door het wegvallen van achterhaalde langdurige procedures ter controle van rechtshulp verzoekende landen lijkt daarom niet het geval.