



Ministerie van Defensie

> Retouradres Postbus 2509LP Den Haag
Ministerie van Justitie en Veiligheid
De minister van Justitie en Veiligheid
Postbus 20301
2500 EH Den Haag

Ministerie van Defensie

Staf Commandant Koninklijke
Marechaussee
Cluster Juridische Zaken
Plein-Kalvermarkt Complex
Kalvermarkt 32
Den Haag
2509LP Den Haag
www.marechaussee.nl

Onze referentie

*Bij beantwoording, datum,
onze referentie en onderwerp
vermelden.*

Datum 24 september 2019
Betreft Consultatieadvies KMar voorgestelde Innovatiewet Strafvordering

Excellentie,

Op 6 juni jl. hebt u de Koninklijke Marechaussee (KMar) het concept van het wetsvoorstel Innovatiewet Strafvordering ter advisering aangeboden. Dit wetsvoorstel strekt tot aanpassing van het Wetboek van Strafvordering (WvSv) met het oog op de bevordering van innovatie binnen het strafprocesrecht en daarmee de modernisering van het WvSv. Ik heb met belangstelling kennis genomen van het wetsvoorstel. In navolging van uw verzoek voor 5 oktober a.s. te reageren, verstrek ik graag hierbij het advies van de KMar.

Advies***Wetsteksten***

Het voorstel bewerkstelligt dat, indien het tot wet wordt verheven, vooruitlopend op de inwerkingtreding van het nieuwe, gemoderniseerde WvSv, al enkele voor de strafrechtspraktijk relevante onderwerpen toegepast kunnen worden. Vanwege het strafvorderlijke legaliteitsbeginsel (artikel 1 WvSv) en het daarmee samenhangende rechtszekerheidsbeginsel is een wijziging van het huidige WvSv nodig middels een formele wet, ergo deze Innovatiewet.

Omtrent die onderwerpen bestaat bij u het vaste voornemen ze op te nemen in het nieuwe wetboek, met daaraan gekoppeld een evaluatie- en horizonbepaling. Het is enerzijds de bedoeling dat aan de hand van pilotprojecten door de betrokken

ketenpartners ervaring kan worden opgedaan ter eventuele verbetering van de beoogde regelgeving alvorens deze rond 2025 in werking treedt. Anderzijds biedt het de mogelijkheid eventuele uitvoeringsconsequenties in kaart te brengen. Bovenal biedt het de kans aan de praktijk al eerder te beschikken over een aantal strafvorderlijke voorzieningen waaraan, zoals u terecht constateert, nu reeds behoefte bestaat. Vooral voor de KMar (en andere opsporingsdiensten) zijn de navolgende 3 onderwerpen relevant waartoe ik mijn advies dan ook wil toespitsen:

1. Het vastleggen en kennisnemen van gegevens door een netwerkzoeking ook ná inbeslagname mogelijk te maken (artt. 554 en 555) en de expliciete bevoegdheid van kennisneming en vastlegging van ná inbeslagneming binnengekomen gegevens (art. 556);
2. Opnamen van beeld en/of geluid als zelfstandig bewijsmiddel door deze op te nemen als wettig bewijsmiddel (art. 557);
3. Het ook kunnen toepassen van een aantal lichtere en vaak gebruikte bijzondere opsporingsbevoegdheden door de hulpofficier van justitie die in de huidige wet alleen zijn toegekend aan de officier van justitie (art. 558).

Ad 2 en 3

Ten aanzien van het tweede en derde onderwerp kan ik mij vinden in de voorgestelde wetsartikelen en bijbehorende toelichting, al acht ik het tweede lid van het voorgestelde artikel 557 onnodig. Mijns inziens zou volstaan kunnen worden met een passage in de memorie van toelichting waarin wordt gerefereerd aan de reeds in het recht geldende en bij hulpofficieren van justitie goed bekende beginselen van proportionaliteit en subsidiariteit. Het ligt in de rede nogmaals nadrukkelijk de aandacht te vestigen op deze beginselen in een aanvullende opleiding voor de hulpofficieren die participeren in de pilot.

Ad 1

Ten aanzien van het eerste onderwerp zie ik nog enkele mogelijkheden ter verbetering dan wel verduidelijking.

- Termijnen

Het voorgestelde artikel over de netwerkzoeking geeft de mogelijkheid voor de officier van justitie (ovj) een bevel te geven voor 3 dagen waarin de netwerkzoeking kan plaatsvinden. Dat bevel dient binnen een maand na de inbeslagneming van het geautomatiseerde werk te worden gegeven. Evenwel kan die periode van een maand telkens worden verlengd met een maand. De pilots zullen moeten uitwijzen of de periode van 3 dagen, die eenmaal kan worden verlengd tot in totaal 6 dagen, voldoende is om gedegen onderzoek te verrichten. Onduidelijk is waar de termijn van 3 dagen uit voort komt en lijkt ook wat krap, gezien de sterk toenemende digitalisering. De verlengingen met een maand om het bevel tot een netwerkzoeking te geven, geeft in ieder geval ruimte om in de opsporingsonderzoeken waarin veel apparaten in beslag worden genomen, te kunnen inventariseren in welke geautomatiseerde werken verder onderzoek wenselijk is. Terecht wordt de noodzaak daartoe beargumenteerd in de memorie van toelichting op p. 32.

De termijn in het volgende artikel, artikel 556, staat echter met die verlengingsmogelijkheid op gespannen voet door de uitleg die er in de memorie van toelichting (p. 34) aan wordt gegeven. Het artikel 555 laat de termijn open

waarbinnen de ovj *het bevel* kan geven, inhoudende dat gedurende de 3 dagen (te verlengen tot maximaal een maand) *na de datum van inbeslagneming* de dan nog binnengekomen gegevens worden bekeken en vastgelegd. De toelichting vermeldt echter *'Het voorgaande betekent dat de opsporing, indien het onderzoek van binnekomende berichten na inbeslagneming gewenst is, snel na de inbeslagneming moet beschikken over een bevel van de officier van justitie. Dergelijk onderzoek is immers slechts mogelijk gedurende drie dagen na het moment van inbeslagneming. Niet het moment van het geven van het bevel is voor deze termijn dus doorslaggevend, wel het moment van inbeslagneming van het geautomatiseerde werk.'* Het zou echter meer in de rede liggen dat als na 1 of enkele maanden wordt besloten tot een netwerkzoeking o.g.v. artikel 555, dan tevens de mogelijkheid bestaat voor de ovj *alsnog* te bevelen dat de gegevens, die in de 3 dagen *na inbeslagneming* zijn binnengekomen, kunnen worden bekeken en vastgelegd. Daarmee wordt de termijn van drie dagen niet opgerekt, omdat de startdatum van binnengekomen berichten nog steeds is gekoppeld aan de datum van inbeslagneming. Mijn advies is daarom de memorie van toelichting overeenkomstig aan te passen.

Overigens wil ik daarbij opmerken dat het niet altijd eenvoudig zal zijn vast te stellen wanneer bepaalde gegevens zijn binnengekomen. Ook kunnen bepaalde gegevens in een cloud na inbeslagneming van het geautomatiseerde werk nog worden gewijzigd in geval anderen daartoe toegang hebben. Bijvoorbeeld door mede-accounthouders via hun eigen geautomatiseerde werk. Een strakke termijn van 3 dagen, die slechts eenmaal en na verkregen machtiging van de rechter-commissaris kan worden verlengd tot een maand, kan de beoogde effectiviteit (zie p. 30-31) van deze netwerkzoeking juist verminderen. Ik geef u daarom in overweging de verlengingsmogelijkheid overeen te brengen met die in artikel 555, derde lid.

- Digitale bevroeringsmogelijkheden

In het wetsvoorstel worden niet al digitale bevroeringsmaatregelen mogelijk gemaakt, terwijl dat voornemen wel in de modernisering WvSV bestaat (zie art. 2.7.41 in de 'ambtelijke eindversie' van mei dit jaar en art. 2.7.3.2.4 van de consultatieversie van oktober 2018 inzake de wijzigingen aangebracht in het conceptwetsvoorstel tot vaststelling van Boek 2 van het nieuwe Wetboek van Strafvordering n.a.v. het rapport van de Commissie Koops¹ d.d. juni 2018). Dit is opmerkelijk, omdat de Commissie Koops heeft geadviseerd tot deze bevroeringsmogelijkheden mede ten behoeve van de netwerkzoeking. Zie p. 198 van het rapport:

'Ten eerste betreft dat bevroeringsmaatregelen, die nodig kunnen zijn omdat digitale gegevens dynamisch zijn en snel gewijzigd of verwijderd kunnen worden. De formulering van de bevroeringsmaatregelen in de artikelen 2.7.1.1.5 en 2.7.2.2.4 lijkt ruim genoeg, maar de bevoegdheden zijn pas beschikbaar vanaf het moment van doorzoeking of binnentreden. Dat sluit voorafgaande bevroeringsmaatregelen uit, zoals het fysiek onderbreken van netwerkverbindingen of gebruik van stoorzenders. Daarbij ontbreken bevoegdheden ter bevroering van gegevens op inbeslaggenomen gegevensdragers; de noodzaak voor dergelijke bevroering neemt echter sterk toe, omdat ook gegevens op inbeslaggenomen gegevensdragers op

¹ Commissie Koops: Commissie modernisering opsporingsonderzoek in het digitale tijdperk

allerlei manieren gewijzigd of ontoegankelijk gemaakt kunnen worden (zie par. 5.5.1). Volgens de commissie is daarom een meer algemene, techniek-onafhankelijke regeling wenselijk voor bevrozingsmaatregelen in het kader van doorzoekingen of inbeslagneming van gegevensdragers; de memorie van toelichting moet daarbij een (niet-limitatieve) opsomming van dergelijke maatregelen geven (zie Aanbeveling 26).'

In de toelichting bij artikel 2.7.41 van de 'ambtelijke eindversie' is te lezen (p. 407): *'De meest vergaande bevrozingsmaatregel ter voorkoming van wijziging of verlies van gegevens is het maken van een volledige kopie ("image") van de inhoud van de digitale-gegevensdrager of het geautomatiseerd werk door de opsporingsambtenaar. In de toelichting op artikel 2.7.39 is besproken dat het maken van een image van een digitale-gegevensdrager of een geautomatiseerd werk in beginsel een vorm van stelselmatig onderzoek van gegevens is waarvoor dus een bevel van de officier van justitie is vereist. Wanneer een image wordt gemaakt door de opsporingsambtenaar als bevrozingsmaatregel, moet het dus gaan om de situatie waarin het bevel van de officier van justitie niet kan worden afgewacht, terwijl er tegelijkertijd zonder het maken van de image een grote kans is op wijziging of verlies van de gegevens. Door het maken van de image stelt de opsporingsambtenaar de gegevens als het ware veilig. Een stelselmatig onderzoek aan de gegevens is niet mogelijk. Daarvoor is een bevel van de officier van justitie nodig.'*

Mede gezien de mogelijkheid van verlenging van de netwerkzoeking na inbeslagneming, is het veiligstellen van gegevens van belang, zowel voor een effectieve opsporing als ook voor latere controle. Daarom adviseer ik u de voorgenomen digitale beveiligingsmaatregelen eveneens alvast in de Innovatiewet op te nemen.

- **Rechtshulpverzoeken**

Artikel 554 stelt duidelijk dat de uitbreiding van de netwerkzoeking die artikel 555 biedt, een afwijking betreft van het huidige artikel 125j WvSv. Volgens de memorie van toelichting bij artikel 555 (p. 31) is een belangrijk verschil met artikel 125j door het woord 'gebruiker' in artikel 555 i.p.v. 'de personen die plegen te werken of te verblijven op de plaats van de doorzoeking', zoals in artikel 125j. De gebruiker kan volgens de memorie van toelichting een rechtmatige, vaste gebruiker van het apparaat zijn, maar ook een kortstondige of zelfs onrechtmatige gebruiker (bijvoorbeeld een dief van een smartphone) zijn. De netwerkzoeking o.g.v. artikel 555 ziet daarmee louter op de verbindingen tussen gebruiker en het elders aanwezige apparaat, zolang de toegang rechtmatig is (geen hacken). Mede hierdoor wordt een 'uitbreiding van de reikwijdte van de bevoegdheid tot netwerkzoeking' bewerkstelligd met het doel de netwerkzoeking 'voldoende tot zijn recht' te laten komen (p. 30). De noodzaak daartoe is, zo staat ook vermeld in de toelichting, dat meer en meer gegevens worden gegenereerd en *online* worden bewaard en dus *elders* worden opgeslagen. Elders in Nederland, maar veelal in een of meerdere landen buiten Nederland. Dat is ook de reden dat ik n.a.v. de verwerking van de aanbevelingen van de Commissie Koops in het concept van het gemoderniseerde Boek 2, heb geadviseerd het territorialiteitsbeginsel los te laten en dit te verduidelijken in de memorie van toelichting. Zie de brief van 5-11-2019 met kenmerk KMar2018013427:

'het territorialiteitsbeginsel niet meer van toepassing kan worden geacht op cloudopslag wegens het internationale karakter ervan en de voortschrijdende ontwikkelingen ten aanzien van wereldwijde opslag van gegevens. Zolang de gebruiker rechtmatig toegang heeft tot de gegevens en de Nederlandse Staat rechtsmacht heeft ten aanzien van de gebruiker, is in geval van cloudopslag een subject-georiënteerde benadering goed verdedigbaar. Het verdient zeker de voorkeur boven een object-georiënteerde benadering, die uitgaat van de plaats waar de gegevens zijn opgeslagen waarvan zowel de gebruiker als het land van opslag doorgaans geen weet hebben en die een effectieve en toekomstbestendige opsporing in de weg staat.'

Anders gezegd, de inbreuk op het soevereiniteitsbeginsel is beperkt dan wel nihil te achten, doordat;

- dezelfde digitale weg wordt bewandeld als de gebruiker, feitelijk wordt in zijn of haar plaats getreden,
- door de netwerkzoeking niet van meer of andere gegevens wordt kennisgenomen dan waar de gebruiker al rechtmatig toegang toe had, evenmin worden de gegevens gewijzigd of weggenomen, en
- het land van opslag doorgaans geen weet heeft dat de gegevens (ook) in zijn land (kortdurend) zijn opgeslagen en deze hem ook niet expliciet zijn verstrekt om vrij te gebruiken.

Ik acht het daarom niet meer van deze tijd dat te allen tijde eerst een rechtshulp verzoek dient te worden gedaan als blijkt dat de gegevens in een ander land zijn opgeslagen. Voor mijn stelling vind ik tevens steun in de recente Aanwijzing OM van maart 2019; genaamd 'Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex artikel 126nba Sv'. Deze aanwijzing geeft weliswaar regels voor de toepassing van de bevoegdheid tot het op afstand heimelijk *binnendringen* van een geautomatiseerd werk met het oog op het verrichten van bepaalde onderzoekshandelingen (art. 126nba, eerste lid, art. 126uba, eerste lid, en art. 126zpa, eerste lid Sv), maar het handelen in de internationale context is vergelijkbaar. Daarvoor worden afwegingscriteria gegeven voor die gevallen dat een rechtshulpverzoek niet mogelijk is, of redelijkerwijs niet kan worden afgewacht. Opvallend daarbij is dat 'de opslag in de cloud' wordt genoemd als een omstandigheid die het redelijkerwijs onmogelijk kan maken de exacte locatie van de gegevens vast te stellen. Alsdan mag volgens de aanwijzing ervan worden uitgegaan dat de gegevens in Nederland staan en worden de Nederlandse rechtsregels toegepast.

Ik heb enig begrip voor de terughoudendheid die uw departement betracht, daar u in de 'ambtelijke eindversie' stelt dat beleidsvorming op dit terrein enorm in beweging is, ook op internationaal gebied, en een internationale aanpak de voorkeur heeft. Desondanks acht ik de ontwikkelingen dusdanig snel gaan ('on line' opslag neemt toe) en de inbreuk op het soevereiniteitsbeginsel dusdanig verwaarloosbaar (vluchtigheid van gegevens, onbekendheid van locatie óók voor het land zelf) dat ik persisteer in mijn eerdere advies. Al zijn er ook geluiden² een *andere invulling* te geven aan het territorialiteitsbeginsel, door de bevoegdheid tot extraterritoriale inzet van opsporingsbevoegdheden vanuit het eigen grondgebied

² Zie de bijdrage van M.F.H. Hirsch Ballin in *Ars Aequi* 2018 (6) 462-476, hoogleraar aan de Vrije Universiteit Amsterdam.

te verbinden aan de bevoegdheid strafrechtelijke rechtsmacht uit te oefenen. Op die manier staat het territorialiteitsbeginsel de inzet van digitale opsporingsbevoegdheden *vanuit het eigen grondgebied* niet meer in de weg en kan zelfs de opsporing efficiënter worden gemaakt en de bescherming van slachtoffers van allerlei vormen van cybercrime worden versterkt.

Deelname pilots

Door de toenemende digitalisering en de steeds sneller op elkaar volgende technische ontwikkelingen zijn nieuwe bevoegdheden voor in het digitale domein hard nodig om de opsporing effectief te laten blijven. De modernisering van het Wetboek van Strafvordering komt daaraan tegemoet, zij het pas over enkele jaren. Daarom ben ik verheugd met de in de concepttoelichting beschreven pilots (p. 17-21), die al een paar bevoegdheden in de meer nabije toekomst bereikbaar maken. Met deze pilots kunnen de betrokken ketenorganisaties alvast ervaring opdoen ter verbetering van de voorgenomen regelgeving. Daarnaast kunnen met de pilots eventuele uitvoeringsconsequenties in kaart worden gebracht en worden bezien of flankerend beleid noodzakelijk is (zie p. 12). Tevens bieden volgens de concepttoelichting de pilots een uitgelezen mogelijkheid de financiële consequenties nauwkeurig in kaart te brengen en te bezien wat een efficiënte en praktische werkwijze met betrekking tot die bevoegdheden kan zijn (p. 18). De KMar zou daarom graag deelnemen aan de pilots die relevant zijn voor de opsporing, te weten de pilots met de onderwerpen die in deze nota op p. 3 onder 1, 2 en 3 zijn genoemd.

Ten aanzien van de pilot aangaande de hulpofficier van justitie (nr. 3) acht ik echter een deelname meteen vanaf de datum dat de voorgestelde Innovatiewet in werking treedt (voorzien op 1-01-2021) niet opportuun. De KMar zit op dat moment in de laatste fase van een reorganisatietraject, die mede van invloed is op het aantal en de positionering van de hulpofficieren binnen de organisatie. Tevens is een traject ingezet om de kwaliteit van de hulpofficieren te versterken en vindt de komende jaren weer een intensivering plaats op de militaire politiezorg. Een gelijktijdig lopende pilot kan deze trajecten verstoren. Anderzijds kunnen deze trajecten de uitkomsten van de pilot, waarin immers zal worden beproefd of de hulpofficier bepaalde officiersbevoegdheden op gelijkwaardig niveau kan uitoefenen, vertroebelen. Deelname op een later moment heeft daarom mijn voorkeur en blijf ik graag op de hoogte van de ontwikkelingen in deze.

Voor beide andere pilots (nrs. 1 en 2) zie ik mogelijkheden voor een zinvolle deelname door de KMar in samenwerking met de relevante ketenpartners. De organisaties zijn, zo is ook te lezen in de toelichting (p. 19-20), uitgenodigd om voorstellen hieromtrent te doen in het kader van deze consultatie. Binnen het relatief korte tijdsbestek van deze consultatie en deels gedurende de vakantieperiode, is het niet mogelijk gebleken al *vastomlijnde* voorstellen te doen. Met uw departement en andere betrokken ketenorganisaties is het overleg ook nog gaande over onder andere de omvang en reikwijdte van de pilots, welke organisatie(s) ze het beste kan of kunnen uitvoeren, de wijze van opslag en overdracht van de gegevens binnen de keten en de borging van de authenticiteit van de gegevens. Doordat deze zaken nog niet helder zijn en het tevens om nieuwe

bevoegdheden gaat, is een *concrete* inschatting van de initiële kosten en impact van de pilots op dit moment nog niet te maken. Daarnaast zijn de pilots juist mede bedoeld om te beproeven en zo gaandeweg meer en meer inzichtelijk te krijgen wat de (financiële) effecten zijn van de voorgestelde wetsteksten op de werkprocessen, bedrijfsvoering en IV-infrastructuur.

Gezien de aanhoudende druk op de taakuitoefening van de KMar, de mede daaruit voortvloeiende capaciteitsproblemen en de benodigde investeringen in onder andere IV en opleidingen om deze pilots van nut te laten zijn, is evenwel een budget neutrale uitvoering van de pilots onwaarschijnlijk. Door de op onderdelen tevens noodzakelijke samenwerking tussen bepaalde ketenorganisaties, zoals bij de gewenste digitale uitwisseling van audiovisuele beelden, zou ook het creëren van een aparte voorziening vanuit uw departement in de rede liggen. Indien mogelijk heeft een enigszins flexibele voorziening de voorkeur vanwege de op voorhand moeilijk in te schatten totale initiële kosten.

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd.

De Commandant Koninklijke Marechaussee



Luitenant-generaal

A handwritten signature in blue ink, consisting of a large, stylized 'C' shape.

Ministerie van Defensie
MPC 58B
Postbus 20701
2500 ES Den Haag



20190926.140.14.17.0005

Gezien scankamer
JenV

26 SEP. 2019

FMHaaglanden

26 SEP. 2019

Ontvangen

Ministerie van Justitie & Veiligheid
De Minister van Justitie & Veiligheid
Postbus 20301
2500 ED Den Haag



Ministerie van Defensie