Ministerie van Defensie

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
[redacted]

Bij beantwoording, datum, onze referentie en onderwerp vermelden.

> Retouradres Postbus 2509LP Den Haag

Ministerie van Justitie en Veiligheid
Directie Wetgeving en Juridische Zaken
T.a.v. de directeur DWJZ
Turfmarkt 147
2511 DP Den Haag

Datum

Betreft Consultatieadvies KMar voor het onderdeel opsporing in een digitale omgeving inzake de modernisering Wetboek van Strafvordering

Op 4 oktober jl. hebt u de Koninklijke Marechaussee (KMar) een nieuw onderdeel van het concept-Boek 2 (Het opsporingsonderzoek) van het gemoderniseerde Wetboek van Strafvordering ter advisering aangeboden. Het betreft wijzigingen in hoofdstuk 7 en 8 van het concept-Boek 2 Sv, dat eerder in consultatie is gegeven. Naar aanleiding van het rapport van de Commissie modernisering opsporingsonderzoek in het digitale tijdperk, onder voorzitterschap van prof. E.J. Koops (hierna de Commissie Koops) is dit deel van het wetboek nogmaals bezien en grondig gewijzigd. De wijzigingen behelzen vooral een andere normering van het onderzoek van (digitale) gegevens op zich en onderzoek van gegevens in en aan digitale-gegevens dragers en geautomatiseerde werken.

Ik heb met belangstelling kennis genomen van het voorgestelde onderdeel van het concept-Boek 2. In navolging van uw verzoek verstrek ik graag hierbij het advies van de KMar.

Advies

Plaats definities

Alvorens op de inhoud van de voorgestelde wetsartikelen in te gaan, wil ik uw vraag beantwoorden of een voorkeur bestaat om een aantal nieuwe definities in de nieuwe titel 7.3 'Onderzoek van gegevens' op te nemen, of alleen in de Memorie van Toelichting (MvT). Op zich bieden beide plaatsen een logische vindplaats om te

kunnen achterhalen wat de wetgever bedoelt met bepaalde begrippen. Een opname in een of meer artikelen en niet louter in de MvT heeft de navolgende voordelen en daarom mijn voorkeur. De vindbaarheid is door opname in de wetstekst sneller en het geeft een duidelijker houvast op welke wijze bepaalde begrippen volgens de wetgever dienen te worden uitgelegd. In de MvT kan daarnaast een nadere toelichting worden gegeven al dan niet met praktijkvoorbeelden. Door de opname van de definities in een afdeling 'algemene bepalingen' (afdeling 7.3.1) is ook voor de artikelen erna helder wat steeds met die begrippen wordt bedoeld, zonder dat men hoeft te zoeken in de MvT.

Nieuwe bevoegdheden

Met de voorgestelde wijzigingen wordt in belangrijke mate een meer effectieve en toekomstbestendige opsporing bewerkstelligd en dat juich ik dan ook toe. Daarmee bedoel ik met name de volgende nieuwe of verruimde mogelijkheden (in chronologische volgorde):

- De verplichting tot geheimhouding voor die personen (bedrijven en instellingen) bij wie een onderzoek van gegevens heeft plaatsgevonden, of tot wie een bevel tot medewerking aan ontsleuteling of tot verstrekking van gegevens is gegeven (art. 2.7.3.1.2).
- De bevoegdheid bij een doorzoeking van een plaats onderzoek van gegevens (kennisnemen en overnemen/kopiëren) op afstand te kunnen verrichten (art. 2.7.3.2.1, derde lid);
- De verwerking van het arrest van de Hoge Raad van 4 april 2017 (ECLI:NL:HR:2017:592, NJ 2017/230) v.w.b. de gelaagde bevoegdheid in het bevel tot '(ingrijpend) stelselmatig onderzoek' (art. 2.7.3.2.2);
- De bevoegdheid tot het verrichten van een zogenoemde netwerkzoeking buiten de situatie van een doorzoeking, dus na inbeslagname van een digitale gegevensdrager of geautomatiseerd werk (art. 2.7.3.2.3, derde lid);
- De bevoegdheid tot het nemen van digitale bevriezingsmogelijkheden, gelijkelijk aan die ter voorkoming van het o.a. wegmaken van voorwerpen (art. 2.7.3.2.4);
- De bevoegdheid na inbeslagneming van een digitale gegevensdrager of geautomatiseerd werk gedurende drie dagen onderzoek van gegevens (w.o. binnenkomende berichten), of een netwerkzoeking te verrichten (art. 2.7.3.2.6);
- Het bevel (tot medewerking aan) ontsleuteling van een digitale gegevensdrager of een geautomatiseerd werk met de verduidelijking in de MvT dat er een "duldplicht" is voor verdachten in geval van biometrische beveiliging of versleuteling (art. 2.7.3.2.7);
- De bevoegdheid tot een generiek bevel tot verstrekken van gegevens, gelijktijdig dan wel opeenvolgend, t.a.v. een ieder van wie wordt vermoed dat diegene toegang heeft tot die gegevens (art. 2.7.3.3.3, vijfde lid);
- Het bevel tot (eerst) verwerking van gegevens en de daardoor verkregen gegevens verstrekt (analyse) (art. 2.7.3.3.6a);
- Het bevel tot locatiebepaling ter aanhouding van de verdachte of ter uitvoering van een bevel tot bepaalde heimelijke (bijzondere opsporings-) bevoegdheden (art. 2.8.2.10.1).

De MvT en het rapport van de Commissie Koops, waarnaar in de MvT meermaals verwezen wordt, geven n.m.m. voldoende onderbouwing van het nut en de noodzaak van deze nieuwe of verruimde bevoegdheden, plichten en bevelsmogelijkheden. Ook komt een aantal daarvan tegemoet aan de eerder gegeven consultatiereactie van de KMar inzake de concept-Boeken 1 en 2 (referentienummer KMar2017006819), zoals met betrekking tot een ontsleutelingsbevel (punt 42), een generiek bevel (punt 46), een getrapte bevoegdheidsverdeling voor het onderzoek van gegevens (punt 48), de reikwijdte van de netwerkzoeking gekoppeld aan de plaats van betreding of doorzoeking en niet meer aan de plaats van onderzoek (punt 49) en een bevoegdheid van de opsporingsambtenaar tot het nemen van digitale bevriezingsmaatregelen (punt 50). Tevens passen de geformuleerde definities beter bij de digitale ontwikkelingen, zoals de geïntroduceerde definitie van communicatie. Deze beslaat niet alleen de communicatie tussen personen, maar ook de gegevensuitwisseling tussen apparaten en de communicatie van iemand met zichzelf. Ondanks dat het moeilijk is alle mogelijke ontwikkelingen te voorzien, komen de gekozen begrippen mij voldoende toekomstbestendig voor.

Aandachtspunten

Ondanks dat ik overwegend positief ben gestemd over de voorgestelde wetsteksten, vraag ik uw aandacht voor het volgende (wederom in chronologische volgorde).

- Uitstel bewijs van overnemen gegevens

Gelijk aan de voorgenomen regeling bij inbeslagname van voorwerpen, is in artikel 2.7.3.1.1, derde lid, de mogelijkheid tot uitstel opgenomen van het afgeven of achterlaten van het bewijs dat gegevens zijn overgenomen (notificatie). Dat uitstel kan alleen worden gehandhaafd als een rechter-commissaris daartoe een machtiging verleent. Daar waar een machtiging voor een dergelijk uitstel van een hogere autoriteit bij beslag op voorwerpen nog begrijpelijk is wegens de inbreuk op het eigendomsrecht, is dat bij het overnemen van gegevens niet. Volgens de voorgestelde definitie van overnemen van gegevens worden de gegevens immers alleen gekopieerd en is er juist geen inbreuk op het eigendomsrecht of de beschikkingsmacht. In sommige gevallen zal het overnemen een inbreuk kunnen maken op het recht op bescherming van de persoonlijke levenssfeer (privacy), maar het voert mijns inziens te ver om in dergelijke gevallen voor uitstel van een notificatie een machtiging van een rechter-commissaris te eisen. Mijn advies is daarom de laatste twee zinnen in het derde lid te schrappen.

- Stelselmatig

Het begrip stelselmatig is in geval van stelselmatige observatie (het huidige art. 126g Sv) door jarenlange rechtspraak juridisch ingevuld en bij opsporingsambtenaren goed bekend. Het voorgestelde artikel 2.7.3.2.2 introduceert stelselmatig en ingrijpend stelselmatig onderzoek van gegevens. Definities ervan zijn eveneens voorgesteld en de MvT geeft een op zich goed en uitgebreid kader dat helpt bij de bepaling of een bepaald onderzoek van gegevens een beperkte, een meer dan geringe, of ingrijpende inbreuk maakt op de privacy van een persoon. Doordat voor het bepalen van stelselmatigheid bij onderzoek in een digitale omgeving andere factoren van belang kunnen zijn dan voor het bepalen van stelselmatigheid bij observatie in de fysieke wereld (bijvoorbeeld de

hoeveelheid gegevens en mate van automatisering van het onderzoek), is een dergelijke uitgebreide toelichting zeker geen luxe. Daarom adviseer ik u voor de bevoegdheden tot stelselmatig overnemen van gegevens uit publiek toegankelijke bronnen (art. 2.8.2.4.1) en stelselmatige locatiebepaling ter aanhouding (art. 2.8.2.10.1) eveneens in de MvT een duidelijke toelichting te bieden ter bepaling van de stelselmatigheid.

- Netwerkzoeking van gegevens in het buitenland

Het artikel 2.7.3.2.3 regelt de zogenoemde netwerkzoeking. Daarbij is geregeld dat in het geval de netwerkzoeking tijdens een *betreding of doorzoeking* of *na inbeslagname* plaatsvindt, het onderzoek niet verder mag gaan dan – kort gezegd – de persoon die op de plaats van betreding of doorzoeking, of de gebruiker van de inbeslaggenomen digitale-gegevensdrager of het geautomatiseerd werk, "legaal" toegang heeft tot die elders aanwezige gegevensdrager of het werk. Anders gezegd, met een bevel van de OvJ verkrijgt de opsporingsambtenaar dezelfde toegang als bovenbedoelde persoon of gebruiker. Dit geeft blijk van een subject-georiënteerde benadering die op mijn instemming kan rekenen. Terecht wordt immers in de MvT benoemd dat tegenwoordig rekening moet worden gehouden met de opslag van gegevens in een "cloud" en er al meerdere cloudopslagdiensten bestaan. Naar mijn mening moet er zelfs eerder rekening mee worden gehouden dat deze vorm van opslag gemeengoed wordt en zal leiden tot de toekomstige situatie dat bijna geen digitale gegevens meer zullen worden opgeslagen en dus voor de opsporing zijn te vinden, op de digitale-gegevensdrager of het geautomatiseerd werk dat een verdachte bij zich draagt of thuis heeft liggen. Deze opsporingsbevoegdheid zoals geformuleerd, voldoet in een, waarschijnlijk toenemende, behoefte.

De MvT meldt echter verder dat uit de wetsgeschiedenis blijkt dat degene die de netwerkzoeking uitvoert, zich dient te vergewissen dat het elders aanwezige geautomatiseerde werk binnen zijn bevoegdheid valt. Als het computersysteem zich in het buitenland bevindt dan zal onderzoek daarin niet zijn toegestaan, tenzij daarvoor een uitdrukkelijke verdragsrechtelijke grondslag is. Ter onderbouwing van dat uitgangspunt wordt verwezen naar de MvT bij de Wet Computercriminaliteit III (Kamerstukken 34 372, nr. 3, p. 42-50). Mij lijkt dat dit uitgangspunt niet overeenkomt met de wens tot een modern en toekomstbestendig en daarmee effectief wetboek te komen. Althans, geen houdbaar uitgangspunt meer in geval van opslag van gegevens in een cloud en wel om de volgende redenen.

Het merendeel van eerder bedoelde cloudopslagdiensten bevindt zich nu niet in Nederland en het ligt niet in de lijn der verwachting dat die situatie anders wordt. Bijvoorbeeld de servers van Dropbox bevinden zich op verschillende plaatsen in de Verenigde Staten (zie www.dropbox.com) en Apple heeft meerdere *datacenters* verspreid over de wereld en maakt daarnaast gebruik van opslagdiensten van Google en Amazon (zie www.iculture.nl). Het voorgestelde artikel is zoals uit de MvT blijkt, bedoeld om de netwerkzoeking voldoende tot zijn recht te laten komen. Wanneer voor iedere netwerkzoeking een rechtshulpverzoek moet worden gedaan, als al te herleiden is (na de nodige tijd en moeite) waar de gezochte gegevens zich bevinden en ook een verdragsgrondslag voor een rechtshulpverzoek bestaat, zal daarentegen geen sprake kunnen zijn van een effectieve opsporingsbevoegdheid.

Daarbij kan de vraag worden gesteld of bij een onderzoek van gegevens een meer dan geringe inbreuk wordt gemaakt op het soevereiniteitsbeginsel van een ander land en onverkort zou moeten worden vastgehouden aan de territorialiteit bij gegevens die zijn opgeslagen in een cloud. Opsporingsambtenaren treden immers niet fysiek op in het andere land en de gegevens worden niet weggenomen of raken uit de beschikkingsmacht van de gebruiker. Het onderzoek aan gegevens wordt immers gedefinieerd in het voorstel als - kort gezegd - kennisnemen en kopiëren. Dat gebeurt via de al bestaande rechtmatige toegangsmogelijkheid van de gebruiker. De hulp van een ander land of zelfs van de clouddienst, is daarbij niet nodig.
Dergelijke clouddiensten zijn ook juist bedoeld om informatie van niet-ingezetenen daarin op te slaan. De opslagservice wordt aan een ieder op deze wereld aangeboden met een opslagcapaciteit en snelheid die almaar toeneemt om aan de vraag te kunnen blijven voldoen. Doorgaans weet de gebruiker niet in welk land of landen de gegevens worden opgeslagen. Het doet voor de gebruiker ook niet ter zake, zolang hij of zij snel en op elke locatie ter wereld toegang heeft en de gegevens veilig zijn. Nieuwe fenomenen als blockchain-systemen tonen aan dat de veiligheid en toegankelijkheid van gegevens bij de gebruikers van dergelijke systemen voorop staat en het kunnen identificeren van de locatie(s) waar de gegevens zijn opgeslagen, (volstrekt) irrelevant is.
De kans is groot dat ook de gebruiker van een cloudopslag, waarschijnlijk ook de clouddienst zelf, niet weet waar bepaalde gegevens zich op een concreet moment bevinden. Gegevens zijn immers razendsnel te benaderen, te bewerken en te verplaatsen. Clouddiensten verdelen de gegevens over meerdere opslaglocaties omwille van de veiligheid of slaan ze op meerde locaties op.
De aangehaalde passage in de MvT bij de Wet Computercriminaliteit III onderkent deze ontwikkelingen en de gevolgen voor de opsporing:
'Voor de opsporing van grensoverschrijdende ernstige strafbare feiten, waarbij gebruik wordt gemaakt van geautomatiseerde werken voor de verwerking en de opslag van gegevens, is het van essentieel belang dat gebruik kan worden gemaakt van onderzoeksbevoegdheden, ook wanneer dat betekent dat daarmee toegang wordt verkregen tot geautomatiseerde werken die zich buiten Nederland bevinden.
(...)
In internationaal verband is vastgesteld dat het territorialiteitsbeginsel in «cyberspace» onder druk staat en dat het beginsel niet kan worden toegepast als de exacte locatie van gegevens onduidelijk is. In het kader van het overleg in de Raad van Europa worden de mogelijkheden onderzocht voor het verbeteren van het vergaren van digitaal bewijs in de Cloud en voor het versterken van de procedures voor rechtshulp bij digitale onderzoeken.
In cyberspace is de feitelijke locatie van gegevens echter niet altijd te achterhalen. In afwachting van de verdere ontwikkeling van het internationaalrechtelijke kader voor de uitoefening van rechtsmacht bij de bestrijding van computercriminaliteit zal zelfstandig opgetreden moeten kunnen worden, om te voorkomen dat internet een vrijplaats wordt voor criminaliteit. Dit kan met zich meebrengen dat opsporingshandelingen worden verricht met betrekking tot gegevens die niet in Nederland zijn opgeslagen. Er zullen toetsingscriteria worden opgesteld voor dit optreden, deze criteria zullen worden vastgelegd in een OM-Aanwijzing of bij algemene maatregel van bestuur.'

Ik adviseer u dan ook dringend om in de MvT te verduidelijken dat 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.

- Biometrische beveiliging

In artikel 2.7.3.2.7, tweede lid wordt in geval van biometrische beveiliging of vergrendeling de mogelijkheid tot het geven van een bevel ontsleuteling aan de opsporingsambtenaar beperkt tot drie beveiligings- c.q. vergrendelingsmogelijkheden; de vingerafdruk, of de opname van iris of gezicht. Het rapport van de Commissie Koops adviseert niet tot een dergelijke beperking. De MvT bij dit artikel geeft als onderbouwing:
'*Ondanks de voorspelling van de commissie Koops dat er meer vormen van biometrische beveiliging mogelijk worden in de toekomst is er niet voor gekozen om een techniek onafhankelijke bepaling voor te stellen. Het is thans niet te voorzien welke mate van inbreuk op de persoonlijke levenssfeer van betrokkene dit zou kunnen opleveren en tevens zou dit, bijvoorbeeld bij de afname van DNA, aanvullende regelgeving vergen.*' Ik acht deze onderbouwing niet overtuigend. Een van de doelen van de modernisering van het wetboek is nu juist een toekomstbestendig wetboek. Het artikel sluit eerder aan bij de mogelijkheden van nu. Terwijl in het rapport van de Commissie Koops ook voorbeelden van biometrische beveiliging en vergrendeling worden genoemd, die eveneens slechts een lichte inbreuk op de persoonlijke levenssfeer opleveren als de verdachte het afnemen of meten ervan zou moeten dulden. Te denken valt aan bloedsomloop en geur. Ik zie geen reden deze mogelijkheden bij voorbaat uit te sluiten, zeker als de MvT een uitgebreide toelichting op de (internationaal) gestelde grenzen biedt. Het advies is daarom de zinssnede '*in de vorm van een vingerafdruk of een opname van de iris of gezicht*' ofwel te verwijderen ofwel het woord 'waaronder' daaraan voorafgaand op te nemen, zodat de bepaling techniek onafhankelijker wordt. Tevens adviseer ik in het artikel de mogelijkheid op te nemen biometrische gegevens, die buiten medeweten van de verdachte (en dus ook in geval van zijn of haar vermissing) zijn of worden vergaard, kunnen worden gebruikt voor ontsleuteling, gelijkelijk aan artikel 2.6.5.4.2, derde lid van het concept-Boek 2. Minder systematisch, maar desalniettemin zou een verduidelijking in de MvT een alternatief kunnen zijn, dat onder '*kan de officier van justitie bevelen dat de opsporingsambtenaar deze beveiliging of versleuteling ongedaan maakt*', tevens valt het buiten medeweten van de verdachte vergaren en gebruiken van biometrische gegevens ten behoeve van de ontsleuteling. Ook de Commissie Koops heeft in haar rapport hiertoe geadviseerd (zie aanbeveling 29).

- Beeldmateriaal

Het komt mij consistenter voor als in artikel 2.7.3.3.3, derde lid onder e het woord 'beeldmateriaal' wordt vervangen door 'opname van beeld of geluid', zoals ook in

artikel 4.3.2.2, eerste lid onder e. Al is een nog meer techniek-onafhankelijke formulering te prefereren, doordat nu maar zeker in de toekomst ook andere bewakingsgegevens op te vragen zijn, zoals tijdsstip en aantal malen dat een geluids-, trillings- of warmte alarm is afgegaan of een patroondoorbreking automatisch is vastgesteld. Dergelijke gegevens zijn niet gevoeliger van aard dan de andere soort gegevens opgenomen in het derde lid waardoor zij niet ook door een opsporingsambtenaar bevolen zouden mogen worden.

- Persoon

O.a. de artikelen 2.7.3.1.2, 2.7.3.2.1 en 2.7.3.3.6a beperken de daarin gegeven bevoegdheid of plicht tot 'diegene die anders dan ten behoeve van persoonlijk gebruik gegevens verwerkt'. De MvT meldt over deze artikelen dat daarmee 'bedrijven en instellingen' worden bedoeld. Ook de artikelen 2.7.3.1.1, 2.7.4.1, 2.7.3.2.1 en 2.8.2.10.1 kunnen feitelijk worden uitgeoefend jegens een rechtspersoon, terwijl alleen 'persoon' in de formulering is opgenomen. Aangezien op andere plaatsen in de concepten van Boek 1 tot en met 6 wel expliciet wordt vermeld dat onder een persoon, slachtoffer of betrokkene ook een *rechtspersoon* wordt verstaan (zie bijvoorbeeld art. 1.7,1.1, aanhef onder a, ten eerste en art. 2.1.1.1, aanhef onder e, art. 3.2.2,), is het advies met het oog op consistentie deze verduidelijking in het desbetreffende artikel op te nemen. Een andere mogelijkheid is een algemene bepaling in ofwel Boek 1 ofwel 2, die vergelijkbaar met artikel 51 Wetboek van Strafrecht, dat bepaalt dat strafbare feiten kunnen worden begaan door natuurlijke personen en rechtspersonen, bepaalt dat bevoegdheden kunnen worden uitgeoefend jegens natuurlijke en rechtspersonen.

Tot slot wil ik nogmaals mijn waardering te kennen geven voor de wijze waarop u vorm geeft aan dit veelomvattende wetgevingsproces. Doordat gekozen is voor het formeel en informeel continu (her)betrekken van de ketenorganisaties bij de vormgeving van de wetsvoorstellen, ben ik ervan overtuigt dat een effectiever, modern en toekomstbestendig wetboek tot stand komt.

De Commandant Koninklijke Marechaussee

[redacted]

Luitenant-generaal

[redacted]