

**Onderwerp**

Consultatieadvies onderdeel opsporing in een digitale omgeving modernisering Wetboek van Strafvordering

Minister van Justitie en Veiligheid
t.a.v. Directeur Wetgeving en Juridische Zaken,
mevr. [REDACTED]
Postbus 20301
2500 EH Den Haag

VERZONDEN - 6 NOV. 2018

Organisatieonderdeel
Staf Korpsleiding

Geachte heer Grapperhaus,

Behandeld door
Projectteam MWvSv

Bij brief van 10 oktober 2018, kenmerk [REDACTED] heeft u de politie gevraagd te adviseren over het conceptwetsvoorstel inzake de opsporing in een digitale omgeving. Dit conceptwetsvoorstel is onderdeel van de modernisering van het Wetboek van Strafvordering. Met belangstelling heb ik kennis genomen van het wetsvoorstel, en maak graag van de gelegenheid gebruik mijn reactie te geven.

Functie

Telefoon

Allereerst maak ik een tweetal algemene opmerkingen, waarna ik in de volgorde van het wetsvoorstel mijn reactie op de verschillende artikelen zal geven.

E-mail

Algemeen

Ons kenmerk
[REDACTED]

Uw kenmerk
[REDACTED]

In afschrift aan

Datum
6 november 2018

Bijlage(n)
0

Pagina
1

Het conceptwetsvoorstel betreft aanpassing van het eerder in consultatie gegeven voorstel voor Boek 2 van het gemoderniseerde wetboek. In mijn advies daarover¹ heb ik mij op verschillende punten kritisch uitgelaten over de wijze waarop de regeling van het opsporingsonderzoek in digitale omgevingen was vormgegeven. Het is daarom goed dat, door de instelling van de Commissie modernisering opsporingsonderzoek in het digitale tijdperk onder leiding van prof. E.J. Koops (hierna: commissie Koops), dit deel van het nieuwe wetboek nogmaals grondig is bezien. Het verheugt mij te constateren dat in het voorgelegde conceptwetsvoorstel een groot aantal van de aanbevelingen van deze commissie is overgenomen. Hierdoor zal het nieuwe wetboek beter aansluiten bij de ontwikkelingen op het gebied van de digitale opsporing. Daarmee is niet gezegd dat het nieuwe wetboek op termijn niet (wederom) aangepast moet worden aan nu nog onvoldoende voorzienbare ontwikkelingen, maar het gekozen begrippen- en normeringskader biedt mijns inziens voldoende flexibiliteit om dergelijke toekomstige wetswijzigingen goed in te passen in het nieuwe wettelijke systeem. In die zin draagt het wetsvoorstel, in ieder geval op systematisch niveau, bij aan een meer toekomstbestendig wetboek. Om te bevorderen dat toekomstige wetswijzigingen zo vroeg als mogelijk in voorbereiding kunnen worden genomen pleit de commissie Koops voor de instelling van een permanente technisch-juridische adviescommissie die de wetgever proactief en tijdig adviseert over maatregelen die nodig zijn in het licht van ontwikkelingen op de middellange termijn op het gebied van technologie, strafrechtelijke rechtshandhaving en privacybescherming.² Ik ondersteun deze aanbeveling van harte, en lever vanuit de politie graag een bijdrage aan een dergelijke adviescommissie.

De regeling van het opsporingsonderzoek in digitale omgevingen gaat over de gevallen waarin en de voorwaarden waaronder opsporingdiensten (digitale) gegevens kunnen vergaren bij de opsporing van strafbare feiten. De normering van het bewaren, hergebruiken, verstrekken en verwijderen van die gegevens vindt niet plaats in het Wetboek van Strafvordering, maar in de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens. Deze beide wetten zullen de komende jaren ook worden gemoderniseerd. Ik hecht er aan te benadrukken dat bij de modernisering van genoemde twee

¹ Brief van 27 juni 2017, kenmerk KNP13001161.

² Commissie modernisering opsporingsonderzoek in het digitale tijdperk, *Regulering van opsporingbevoegdheden in een digitale omgeving*, s.l. 2018, blz. 64-65.

Onderwerp

Consultatieadvies onderdeel opsporing in een digitale omgeving modernisering Wetboek van Strafvordering

Datum

6 november 2018

Pagina

2 van 11

wetten de samenhang met het Wetboek van Strafvordering aandacht behoeft. Wijzigingen in de normering van het gebruik van eenmaal vergaarde gegevens kan immers aanleiding geven tot een herwaardering van de normering van de bevoegdheden waarmee die gegevens worden vergaard. De regels over vergaring enerzijds en verwerken anderzijds moeten als geheel evenwichtig en werkbaar zijn. Ook de commissie Koops vraagt hier aandacht voor.³

Ik geef u voorts in overweging de modernisering van de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens op dezelfde wijze vorm te geven als de modernisering van het Wetboek van Strafvordering door vroegtijdige betrokkenheid van de ketenorganisaties mogelijk te maken en een parallel traject in te richten waarin de uitvoeringsconsequenties worden onderzocht.

Begrippen en definities

In het eerste onderdeel van het wetsvoorstel worden verschillende reeds bestaande begrippen gedefinieerd. Ten aanzien van de wijzigingen in de begrippen 'geautomatiseerd werk', 'digitale-gegevensdrager' en 'gegevens' onderschrijf ik de daarin aangebrachte wijzigingen.

De huidige wet kent geen definitie van het begrip 'communicatie'. Het wetsvoorstel geeft, in navolging van het advies van de commissie Koops, wel een definitie. Deze is aanzienlijk ruimer dan de huidige (in wetstoelichtingen opgenomen) definitie zoals die in het kader van bevoegdheden zoals het vorderen van communicatie, interceptie en het opnemen van vertrouwelijke communicatie gehanteerd wordt. De voorgestelde definitie is meer technisch van aard (alle gegevensuitwisseling, van welke aard ook) dan de huidige werkdefinitie waarin aspecten als de vertrouwelijkheid en de betrokkenheid van personen bepalen of sprake is van communicatie. Een concreet gevolg van de nieuwe definitie is dat ook gegevensuitwisseling tussen apparaten en "zelfcommunicatie" onder het communicatiebegrip gaan vallen. In de normering van verschillende opsporingsbevoegdheden wordt, via een verwijzing naar het telecommunicatiegeheim zoals bedoeld in de Grondwet, vervolgens bepaald dat bijvoorbeeld alleen een machtiging van de rechter-commissaris wordt vereist als sprake is van vormen van communicatie die door dat grondwettelijke telecommunicatiegeheim worden beschermd. Ik kan deze benadering vanuit conceptueel oogpunt onderschrijven. Tegelijkertijd stel ik vast dat het moeilijk te overzien is wat op de langere termijn, als het belang voor de opsporing van de gegevensuitwisseling tussen apparaten zal toenemen, de precieze gevolgen zullen zijn van de voorgestelde verruiming van het communicatiebegrip.

De introductie van de wettelijke definitie van 'communicatie' lijkt overigens niet geheel consequent te zijn doorgevoerd in het wetsvoorstel. Op meerdere plaatsen wordt in bepalingen nog gesproken over 'telecommunicatie' (zie bijvoorbeeld artikel 2.7.3.3.4, derde lid). Ook in hoofdstuk 8 van het wetsvoorstel Boek 2 komt het begrip 'telecommunicatie' nog voor, zonder dat het voorliggende conceptwetsvoorstel daarop wijzigingen aanbrengt.

Het conceptwetsvoorstel bevat in onderdeel C een aantal nieuwe begrippen ('onderzoek van gegevens', 'kennismaken van gegevens', 'overnemen van gegevens', 'stelselmatig onderzoek van gegevens', en 'ingrijpend stelselmatig onderzoek van gegevens'). Deze begrippen komen in de plaats van het begrip 'inbeslagneming van gegevens' zoals dat werd gebruikt in de consultatieversie van Boek 2. In mijn advies daarover raadde ik de introductie van het concept van beslag op gegevens af. Met instemming stel ik vast dat in het voorliggende wetsvoorstel dat concept niet terugkeert, maar is gekozen voor een ander begrippenkader.

³ Ibidem, blz. 24-25.

Onderwerp

Consultatieadvies onderdeel opsporing in een digitale omgeving modernisering Wetboek van Strafvordering

Datum

6 november 2018

Pagina

3 van 11

Van de genoemde begrippen worden in het conceptwetsvoorstel definities gegeven. Deze definities geven mij geen aanleiding tot opmerkingen. Taalkundig werkt het begrip 'onderzoek van gegevens' minder fraai uit in verschillende bepalingen doordat wordt gesproken over 'onderzoek van gegevens aan gegevens'. Als alternatieve formulering zou wellicht overwogen kunnen worden te spreken over 'gegevensonderzoek', alhoewel ook die term in zinsverband enigszins wringt.

In uw aanbiedingsbrief verzoekt u om advies over de vraag of de hier bedoelde definities in de wet zelf, of in de memorie van toelichting moeten worden opgenomen. Op zichzelf zie ik weinig meerwaarde in het opnemen van deze definities in de wet zelf. Om enige rechtsontwikkeling mogelijk te maken heeft opname in de memorie van toelichting de voorkeur.

Titel 7.3 Onderzoek van gegevens

Bewijs van overnemen van gegevens met mogelijkheid tot uitstel (art. 2.7.3.1.1)

In artikel 2.7.3.1.1 is het huidige artikel 125m in gewijzigde vorm overgenomen. Daarbij is een aantal inhoudelijke wijzigingen aangebracht.

Het huidige artikel 125m verplicht tot het informeren van betrokkenen over het overnemen van gegevens tijdens een doorzoeking. Het voorgestelde artikel kent die verplichting niet alleen bij een doorzoeking, maar ook bij een betreding (zonder dat sprake is van doorzoeken). Een en ander betekent dat indien na het betreden van een plaats bijvoorbeeld foto's van die plaats worden gemaakt waarmee direct zichtbare gegevens (zoals meterstanden of documenten) worden vastgelegd, er anders dan naar huidig recht een bewijs van overnemen van gegevens afgegeven of achtergelaten moet worden. Alhoewel ik de achtergrond van deze wijziging begrijp, wijs ik er wel op dat sprake is van een administratieve lastenverzwaring. De omvang daarvan is moeilijk vast te stellen nu, wegens het ontbreken van een wettelijke verplichting, in de huidige praktijk niet apart wordt geregistreerd dat tijdens een betreding bijvoorbeeld foto's zijn gemaakt waarmee gegevens zijn overgenomen. De lastenverzwaring zal overigens vermoedelijk beperkt zijn. Overwogen kan overigens ook worden om de verplichting tot het afgeven van een bewijs van overnemen te beperken tot gevallen waarin *digitale* gegevens worden overgenomen en gevallen waarin toepassing is gegeven aan de omzettingbepaling van artikel 2.7.3.2.2, derde lid.

Een tweede wijziging ten opzichte van het huidige wetboek is de normering van het moment waarop het bewijs van overnemen afgegeven of achterlaten moet worden. Het huidige wetboek spreekt over 'zo spoedig mogelijk', terwijl het voorgestelde artikel de term 'direct' gebruikt. Op zichzelf zie ik geen bezwaar tegen deze wijziging, maar wil er wel op wijzen dat tijdens doorzoekingen soms grote hoeveelheden data worden overgenomen, waarbij niet al 'direct' aangegeven kan worden wat de aard van de overgenomen gegevens is. Het huidige artikel 125m maakt het mogelijk om het bewijs van overnemen enige tijd na afsluiting van de doorzoeking af te geven. In die tijd kunnen de overgenomen gegevens globaal bezien worden, waardoor in het bewijs van overnemen een (globale) omschrijving van die gegevens opgenomen kan worden. Als het bewijs van overnemen meteen bij het afsluiten van een doorzoeking afgegeven moet worden, zal een beschrijving van de 'aard van de overgenomen gegevens' noodzakelijkerwijs nog globaler zijn. Te denken is aan een omschrijving als 'alle gegevens op de D:-schijf met de volumenaam XYZ'. Ik verzoek u hieraan in de memorie van toelichting aandacht te besteden.

In het derde lid van het voorgestelde artikel 2.7.3.1.1 wordt de huidige mogelijkheid om het bewijs van overnemen in het belang van onderzoek uit te stellen gewijzigd. Nu is de

Onderwerp

Consultatieadvies onderdeel opsporing in een digitale omgeving modernisering Wetboek van Strafvordering

Datum

6 november 2018

Pagina

4 van 11

officier van justitie zelfstandig bevoegd tot dergelijk uitstel te besluiten. In het wetsvoorstel is opgenomen dat de officier van justitie die een dergelijk besluit heeft genomen, een machtiging van de rechter-commissaris moet vragen om het besluit tot uitstel te handhaven. Deze regeling is identiek aan de beoogde regeling bij de inbeslagneming van voorwerpen. Bij beslag op voorwerpen wordt, doordat het voorwerp aan de beschikkingsmacht van de beslagene wordt onttrokken, een stevige inbreuk op diens rechten gemaakt. De beslagene van die inbreuk (tijdelijk) in het ongewisse laten is dan ook een beslissing die rechterlijke betrokkenheid rechtvaardigt. Bij het overnemen van gegevens, waarbij per definitie de beschikkingsmacht van betrokkene *niet* wordt aangetast, is de zwaarte van de inbreuk mijns inziens niet zodanig dat het uitstellen van notificatie een voorafgaande rechterlijke toets noodzakelijk maakt. Ik dring er dan ook op aan de tweede en derde volzinnen van het derde lid te schrappen.

Een derde wijziging die ten opzichte van het huidige wetboek wordt voorgesteld is een vereenvoudiging van de definitie van 'betrokkene' als degene aan wie het bewijs van overnemen afgegeven moet worden. Deze vereenvoudiging leidt tot een overzichtelijker stelsel en is beter werkbaar.

Geheimhouding (art. 2.7.3.1.2)

Artikel 2.7.3.1.2 legt een geheimhoudingsplicht op aan al degene die betrokken zijn bij een betreding of doorzoeking waarbij onderzoek van gegevens is gedaan dan wel tot wie een bevel tot het verstrekken van gegevens is gericht. Het is goed vast te stellen dat, net als naar huidig recht, de wet zelf een geheimhoudingsplicht oplegt en dat daarvoor geen apart te geven bevel nodig is. Ook het feit dat deze wettelijke geheimhoudingsplicht niet beperkt blijft tot personen aan wie een bevel tot gegevensverstrekking is gericht, maar wordt uitgebreid naar doorzoekingen en betredingen is een goede stap.

In de conceptmemorie van toelichting wordt ingegaan op de beperking tot degene die 'anders dan voor persoonlijk gebruik gegevens verwerkt'. Daarbij wordt aangegeven dat deze beperking met zich meebrengt dat alleen gegevens die door 'bedrijven of instellingen' worden verwerkt wordt bedoeld. Dit kan de vraag oproepen of informele burgerinitiatieven, zoals onderzoeksgroepen of -collectieven, waar een doorzoeking plaatsvindt of waaraan een bevel tot gegevensverstrekking wordt gegeven, onder de voorgestelde wettelijke geheimhoudingsplicht vallen, hetgeen wenselijk zou zijn. Ik verzoek u hieraan in de memorie van toelichting aandacht te besteden.

Steunbevoegdheden voor onderzoek van gegevens met mogelijkheid tot doorzoeken op afstand (art. 2.7.3.2.1)

Het huidige artikel 125i betreft de doorzoeking ter vastlegging van gegevens. Dit artikel voldoet in de praktijk, en wordt daarom terecht inhoudelijk ongewijzigd in het nieuwe wetboek overgenomen. In het derde lid van het voorgestelde artikel 2.7.3.2.1 is een welkome aanvulling opgenomen waardoor het uitvoeren van een doorzoeking ter vastlegging van gegevens, met toestemming van degene bij wie de gegevens worden doorzocht, ook mogelijk wordt vanaf afstand. In de praktijk bestaat hieraan behoefte zowel bij de politie als bij sommige partijen bij wie een doorzoeking plaatsvindt. Voor zowel de politie als de 'doorzochte' partij kan het efficiënter en minder belastend zijn om een, soms meerdere dagen durende gegevenszoeking niet op de locatie van de doorzochte partij uit te voeren, maar via een netwerkverbinding vanaf een politielocatie. Het voorgestelde derde lid voorziet dus in een behoefte, en is helder geformuleerd. Alleen het gebruik van de woorden 'bij een persoon' roept de vraag op of hieronder zowel natuurlijke als rechtspersonen moeten worden verstaan. Ik adviseer dit in de memorie van toelichting te verduidelijken.

Onderwerp

Consultatieadvies onderdeel opsporing in een digitale omgeving modernisering Wetboek van Strafvordering

Datum

6 november 2018

Pagina

5 van 11

Onderzoek van gegevens en schakelbepaling voor omzetten analoge gegevens (art. 2.7.3.2.2)

In het voorgestelde artikel 2.7.3.2.2 wordt het onderzoek aan digitale-gegevensdragers en geautomatiseerde werken genormeerd. In de consultatieversie van het wetsvoorstel Boek 2 (februari 2017) was een voorstel opgenomen waarbij voor iedere vorm van onderzoek aan iedere digitale-gegevensdrager of geautomatiseerd werk voorafgaande toestemming van de officier van justitie werd vereist. In mijn consultatieadvies op dat voorstel⁴ heb ik aangegeven dat die benadering tot forse overnormering zou leiden, nu daarmee ook vormen van onderzoek die geen of weinig privacyinbreuk maken aan een toestemmingseis werden onderworpen. Ik wees er daarnaast op dat sommige apparaten zo weinig, of zo weinig privacygevoelige gegevens bevatten dat zelfs een uitputtende vorm van onderzoek in die gegevens geen of slechts een lichte privacyinbreuk maken. Ik pleitte in mijn advies voor codificatie van de jurisprudentie van de Hoge Raad, zoals die vanaf april 2017 tot ontwikkeling is gekomen. De commissie Koops komt tot dezelfde aanbeveling.

Ik stel met instemming vast dat in het voorliggende wetsvoorstel aan deze adviezen gehoor is gegeven: niet iedere vorm van onderzoek vergt een bevel van de officier van justitie of machtiging van de rechter-commissaris, maar alleen die vormen van onderzoek die (voorzienbaar) tot een 'min of meer volledig of ingrijpend beeld van bepaalde aspecten van iemands privéleven' kunnen leiden. Het kernbegrip is daarbij de stelselmatigheid van het onderzoek. De conceptmemorie van toelichting gaat op heldere wijze in op de vraag welke vormen van onderzoek stelselmatig kunnen zijn, en welke niet. Met name over de vraag welke vormen van onderzoek geen of slechts een beperkte inbreuk op de persoonlijke levenssfeer maken zijn sinds de arresten van de Hoge Raad in april 2017 in lagere rechtspraak verschillende uitspraken gedaan. Ongetwijfeld zullen nog meer uitspraken volgen, waarmee een steeds duidelijker beeld zal ontstaan over de invulling van het begrip stelselmatigheid in de context van het onderzoek aan digitale-gegevensdragers en geautomatiseerde werken. Het verdient aanbeveling in de uiteindelijke memorie van toelichting ter verdere verduidelijking aandacht te besteden aan deze jurisprudentie.

In de formulering van het voorgestelde eerste lid van artikel 2.7.3.2.2 wordt niet alleen het onderzoek in een digitale-gegevensdrager of geautomatiseerd werk zelf genormeerd, maar ook het onderzoek aan gegevens die daaruit zijn overgenomen. Zodra gegevens worden overgenomen en vastgelegd in een politiesysteem, is op die gegevens de Wet politiegegevens van toepassing. Gewaakt moet worden voor dubbele normering of onduidelijkheid als gevolg van de toepasselijkheid van meerdere wettelijke kaders. Dit is wat mij betreft een uitdrukkelijk punt van aandacht bij de komende modernisering van de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens.

Ten aanzien van het derde lid, waarin de omzetting van analoge in digitale gegevens wordt genormeerd, lijkt de formulering niet goed aan te sluiten op de beoogde situatie. De bepaling kan zo gelezen worden alsof voor iedere omzetting van analoge naar digitale gegevens een bevel van de officier van justitie wordt vereist. Zoals ook uit de conceptmemorie van toelichting blijkt is dit niet bedoeld: alleen als die omzetting bedoeld is om stelselmatig of ingrijpend stelselmatig onderzoek mogelijk te maken is een bevel vereist. Wellicht kan de bepaling verduidelijkt worden door niet te spreken over 'indien vervolgens onderzoek van gegevens aan die digitale gegevens wordt verricht', maar 'indien vervolgens *stelselmatig of ingrijpend stelselmatig* onderzoek van gegevens aan die digitale gegevens wordt verricht.'

⁴ Zie mijn brief van 27 juni 2017, kenmerk KNP13001161, bijlage 2, blz. 58.

Onderwerp

Consultatieadvies onderdeel opsporing in een digitale omgeving modernisering Wetboek van Strafvordering

Datum

6 november 2018

Pagina

6 van 11

Netwerkzoeking (art. 2.7.3.2.3)

Het huidige wetboek maakt het mogelijk om tijdens een doorzoeking via een op de plaats van de zoeking aanwezige computer verbinding te maken met een computer op een andere locatie. Deze netwerkzoeking keert in het nieuwe wetboek terug, waarbij ook de mogelijkheid wordt geopend tot netwerkzoeking na inbeslagneming van een computer. Deze mogelijkheid was ook al opgenomen in de eerdere consultatieversie van Boek 2 (februari 2017), maar is het voorliggende wetsvoorstel naar aanleiding van de aanbevelingen van de commissie Koops verder uitgewerkt en genormeerd. Ook in deze aangepaste vorm is de nieuwe regeling van de netwerkzoeking een welkome uitbreiding voor de praktijk, zeker in combinatie met het voorgestelde artikel over ontsluiting (artikel 2.7.3.2.7).

Het voornemen bestaat deze bepaling op te nemen in de Experimenteerwet Sv, waardoor vooruitlopend op de inwerkingtreding van het nieuwe Wetboek van Strafvordering in de praktijk ervaring opgedaan kan worden. Zo kan worden beoordeeld of de opgenomen termijnen (termijn waarbinnen na inbeslagneming gestart moet worden met een netwerkzoeking en maximale duur van een netwerkzoeking) voldoende werkbaar zijn.

Digitale bevroezingsmogelijkheden (art. 2.7.3.2.4)

De commissie Koops heeft geadviseerd een algemene bevroezingsbevoegdheid in digitale omgevingen in de wet op te nemen, nu de bestaande bevroezings- en ordebevoegdheden alleen van toepassing zijn bij zoekings- en betredingssituaties. Ook daarbuiten (of daaraan voorafgaand) kan het in verband met de vluchtigheid van digitale gegevens van belang zijn om maatregelen te kunnen treffen ter voorkoming van verlies of wijziging van gegevens. Het voorgestelde artikel 2.7.3.2.4 voorziet hierin, en zal buiten twijfel stellen dat opsporingsambtenaren (binnen de grenzen van proportionaliteit en subsidiariteit) bevoegd zijn maatregelen tegen gegevensverlies te nemen. Het voorgestelde artikel is daarmee een goede aanvulling op de reeds bestaande bevroezings- en ordemaatregelen.

Geautomatiseerd werk van een aanbieder (art. 2.7.3.2.5)

Het voorgestelde artikel 2.7.3.2.5 vervangt het huidige artikel 125la, waarin is geregeld dat tijdens een doorzoeking ter vastlegging bij een communicatieaanbieder alleen bij dringende noodzaak en met machtiging van de rechter-commissaris – kortgezegd – inhoudelijke communicatie (e-mail etc.) mag worden onderzocht. De reikwijdte van het huidige artikel is beperkt tot de situatie van een doorzoeking op de locatie van een communicatieaanbieder. Het voorgestelde artikel breidt deze reikwijdte uit tot situaties waarin een apparaat of gegevensdrager bij een communicatieaanbieder in beslag is genomen en later op het politiebureau wordt onderzocht. Hiermee wordt, zoals in de conceptmemorie van toelichting terecht wordt aangegeven, een onevenwichtigheid die in het huidige wetboek bestaat weggenomen. Deze uitbreiding zal enig werklasteffect hebben in de keten.

Binnenkomende berichten na inbeslagneming (art. 2.7.3.2.6)

Veel apparaten hebben een verbinding met het internet. Na inbeslagneming van een apparaat kunnen daarom, via die internetverbinding, door externe systemen nog wijzigingen worden aangebracht op het apparaat. Er kunnen nog berichten binnenkomen, apps worden bijgewerkt etc. etc. Het voorgestelde artikel 2.7.3.2.6 regelt dat, als een onderzoeksbevel is afgegeven, ook kennis mag worden genomen van gegevens die in de eerste drie dagen na de inbeslagneming op het apparaat zijn 'binnengekomen'. In deze eerste periode geldt het algemene leerstuk van de 'bijvangst'⁵, en mag, mits reeds

⁵ Zie Commissie modernisering opsporingsonderzoek in het digitale tijdperk, *Regulering van opsporingsbevoegdheden in een digitale omgeving*, s.l. 2018, blz. 92-93.

Onderwerp

Consultatieadvies onderdeel opsporing in een digitale omgeving modernisering Wetboek van Strafvordering

Datum

6 november 2018

Pagina

7 van 11

een onderzoeksbevel is afgegeven, kennis worden genomen van deze berichten. De officier van justitie kan deze periode met machtiging van de rechter-commissaris verlenen voor ten hoogste een maand.

Op zichzelf is de voorgestelde bepaling van waarde voor de opsporingspraktijk. Momenteel is onduidelijk of kennis genomen mag worden van 'nagekomen berichten'. In die zin ondersteun ik de invoering van een uitdrukkelijk bevoegdheid op dit punt. Niettemin heb ik enige twijfel bij de voorgestelde vormgeving van deze bevoegdheid. Met name de genoemde termijnen komen mij als te beperkt voor, zeker in situaties waarin het veel tijd kost om toegang tot het apparaat te verkrijgen. Ook in gevallen waarin in een onderzoek vele apparaten in beslag genomen worden kunnen de gestelde termijnen knellen, eenvoudigweg omdat niet altijd voldoende capaciteit beschikbaar is om alle inbeslaggenomen apparaten snel aan een onderzoek te onderwerpen. In deze situaties kan het voorkomen dat pas na het verstrijken van de maximale termijn van een maand kennis kan worden genomen van de inhoud van een inbeslaggenomen apparaat. Het is te voorzien dat in de toekomst steeds vaker het uitschakelen van de internetverbinding niet mogelijk is, niet gegarandeerd kan worden, of dat de aanwezigheid van een actieve internetverbinding niet vastgesteld kan worden. Daardoor kan niet altijd voorkomen worden dat tussen het moment van inbeslagneming en het moment waarop toegang wordt verkregen tot het apparaat nieuwe gegevens binnenkomen. Ook is het om technische redenen niet altijd mogelijk achteraf te bepalen wanneer welke gegevens op het apparaat zijn binnengekomen, waardoor ook niet bepaald kan worden welke gegevens binnen de eerste maand zijn ontvangen en welke daarna. Nu ook voor deze bepaling het voornemen bestaat een experiment mogelijk te maken, stel ik voor de evaluatie van het experiment af te wachten en op basis daarvan te bezien of deze bepaling aanpassing behoeft.

Bevel ontsleuteling (art. 2.7.3.2.7)

De vergrendeling van digitale apparaten en de versleuteling van daarop opgeslagen gegevens vormt in toenemende mate een beperking voor de opsporing van strafbare feiten. Het is daarom goed dat in het voorgestelde artikel 2.7.3.2.7 de huidige bevoegdheid tot het geven van een ontsleutelingsbevel wordt overgenomen. De voorgestelde uitbreiding tot inbeslaggenomen apparaten is gerechtvaardigd: er is immers geen reden waarom een dergelijk bevel alleen gegeven zou moeten kunnen worden tijdens een doorzoeking, zoals onder de huidige wet in artikel 125k is opgenomen.

Het voorgestelde tweede lid beslecht de discussie over de vraag of een verdachte moet dulden dat zijn vinger op de vingerafdrukscanner van zijn telefoon mag worden gelegd. De commissie Koops heeft, mijns inziens op overtuigende wijze, onderbouwd dat een dergelijke duldplicht niet in strijd is met het nemo tenetur-beginsel. In afwijking echter van het advies van de commissie Koops⁶ is de voorgestelde bepaling beperkt tot vingerafdrukken, irisvergelijking en gezichtsvergelijking. In de conceptmemorie van toelichting wordt gesteld dat op dit moment niet te voorzien is van welke andere biometrische beveiligingsmethoden apparaten in de toekomst voorzien zullen zijn. Daarmee zou een meer technologie-onafhankelijke formulering van het tweede lid mogelijk teveel ruimte geven aan inbreuken waarvan de zwaarte op dit moment niet te overzien is. Alhoewel ik begrip heb voor deze benadering, acht ik de kans groot dat deze bepaling in de (al dan niet nabije) toekomst gewijzigd zal moeten worden om nieuwe vormen van biometrische beveiliging te kunnen omvatten.⁷ Het verdient daarom sterk aanbeveling om op dit punt een meer technologie-onafhankelijke formulering in de wet te hanteren, en in een algemene maatregel van bestuur de toegestane biometrische kenmerken te benoemen. In

⁶ Ibidem, blz. 107.

⁷ De commissie Koops noemt geur, bloedvaten in de retina, DNA, bloedsomloop, afdrukken van bijvoorbeeld oor of handpalm en gedragskenmerken zoals stemherkenning, stapherkenning en toetsaanslagritme. Zie ibidem, blz. 104.

Onderwerp

Consultatieadvies onderdeel opsporing in een digitale omgeving modernisering Wetboek van Strafvordering

Datum

6 november 2018

Pagina

8 van 11

een dergelijke algemene maatregelen kunnen dan voor bepaalde biometrische kenmerken ook eventuele aanvullende voorschriften worden gegeven. Op deze wijze kan sneller worden ingespeeld op nieuwe technologische ontwikkelingen.

De commissie Koops heeft ook aandacht besteed aan de mogelijkheid om buiten medewerking of bij verzet of vermissing van een persoon biometrische kenmerken te vergaren ten bate van de ontgrendeling van apparaten. De commissie ziet hierin een parallel met de reeds bestaande wettelijke mogelijkheden om bijvoorbeeld vingerafdrukken te vergaren voor vergelijkend onderzoek (zie het voorgestelde artikel 2.6.5.4.2, derde lid). Op grond hiervan komt de commissie tot de aanbeveling een bevoegdheid in te voeren op basis waarvan de officier van justitie kan bevelen dat in het belang van het onderzoek biometrische gegevens van de verdachte die buiten zijn medeweten zijn verkregen, kunnen worden gebruikt ten behoeve van de ontsluiting van een digitale-gegevensdrager of een geautomatiseerd werk.⁸ In het nu voorliggende conceptwetsvoorstel is een dergelijke bepaling niet opgenomen. Ik dring er op aan in het nieuwe wetboek alsnog in deze mogelijkheid te voorzien.

Afdeling 7.3.3 Verstrekking van gegevens

In onderdeel D van het conceptwetsvoorstel wordt een aantal wijzigingen voorgesteld op de consultatieversie Boek 2 (februari 2017). In het navolgende zal ik ingaan op de verschillende artikelen zoals die zullen luiden na de nu voorgestelde wijzigingen.

Inhoud bevel (art. 2.7.3.3.1)

Het voorgestelde artikel 2.7.3.3.1 bepaalt dat, net als in het huidige wetboek, dat bevelen tot het verstrekken van gegevens schriftelijk dienen te zijn. Ook de vereiste inhoud van een dergelijk bevel komt overeen met de huidige wettelijke bepalingen. De voorgestelde bepaling geeft mij geen aanleiding tot opmerkingen.

Bevel bevrozing gegevens (art. 2.7.3.3.2)

Het huidige artikel 126ni is vrijwel ongewijzigd overgenomen in het voorgestelde artikel 2.7.3.3.2. Over dit artikel heb ik geen opmerkingen.

Bevel verstrekken gegevens (art. 2.7.3.3.3)

Zoals ik reeds in mijn advies op het conceptwetsvoorstel Boek 2 heb aangegeven, wint de wettelijke regeling rondom het vorderen van gegevens aan overzichtelijkheid en werkbaarheid doordat de huidige complexe en over meerdere artikelen verspreide regeling is vereenvoudigd in het voorgestelde artikel 2.7.3.3.3.

In dat advies pleitte ik voor de introductie van een mogelijkheid om in bepaalde gevallen te kunnen werken met een generiek bevel. Met instemming stel ik vast dat daarvoor in het nu voorgestelde vijfde lid een voorzienig is opgenomen, die mij nuttig en werkbaar voorkomt. Het voorstel komt er op neer dat een bevel tot het verstrekken van soortgelijke gegevens gedurende twee weken gericht kan worden tot meerdere partijen. Daarmee wordt het opmaken van een bevel per partij overbodig, hetgeen tot vermindering van administratieve handelingen leidt. Momenteel onderzoek ik de mate waarin de voorgestelde bepaling tot verlaging van administratieve lasten zal leiden. Vooruitlopend op de uitkomsten daarvan vraag ik mij af of de termijn van twee weken niet zodanig kort is dat dit generieke bevel in de praktijk slechts van beperkte meerwaarde zal blijken te zijn. Met name in situaties waarin het resultaat van de eerste toepassing van het bevel afgewacht moet worden alvorens te kunnen bepalen of een tweede toepassing aan het generieke bevel gegeven moet worden, bijvoorbeeld richting een andere, soortgelijke partij.

⁸ Commissie modernisering opsporingsonderzoek in het digitale tijdperk, *Regulering van opsporingsbevoegdheden in een digitale omgeving*, s.l. 2018, blz. 108.

Onderwerp

Consultatieadvies onderdeel opsporing in een digitale omgeving modernisering Wetboek van Strafvordering

Datum

6 november 2018

Pagina

9 van 11

In het derde lid, onder e is de bevoegdheid van opsporingsambtenaren opgenomen om camerabeelden van bewakingscamera's op te vragen (het recent in werking getreden artikel 126nda). In de voorgestelde formulering wordt de term "beeldmateriaal" gebruikt. In toenemende mate maken bewakingscamera's ook geluidsopnamen, en worden bewakingsystemen ook uitgerust met sensoren die trillingen of temperatuur meten. Camerasystemen worden ook steeds intelligenter, bijvoorbeeld doordat gezichtsherkenning wordt toegepast. Dat betekent dat camerasystemen ook kunnen registreren dat een bepaalde persoon op meerdere momenten 'in beeld' is geweest. Met andere woorden: bewakingscamera's leggen meer vast dan alleen beelden. Ik zie op voorhand geen reden om deze andere gegevens uit te sluiten van de onderhavige bevoegdheid, en pleit er dan ook voor de term 'beeldmateriaal' te vervangen door het neutralere 'materiaal' of 'gegevens'.

Bevel verstrekken gegevens aanbieder (art. 2.7.3.3.4)

In dit conceptartikel is de regeling van de artikelen 126n en 126na overgenomen. In het huidige artikel 126na is bepaald dat opsporingsambtenaren in geval van verdenking van een misdrijf bevoegd zijn NAW-gegevens, nummer en soort dienst van een gebruiker van een communicatiedienst op te vragen bij de communicatieaanbieder. In de voorgestelde bepaling wordt deze 'verdenkingsvoorwaarde' niet meer expliciet verwoord, maar wordt verwezen naar de voorwaarde die geldt in artikel 2.7.3.3.3, eerste lid. Daarin is de verdenkingsvoorwaarde gesteld op 'een misdrijf waarop naar de wettelijke omschrijving gevangenisstraf van een jaar of meer is gesteld'. Dit leidt dus tot een verhoging van de verdenkingsvoorwaarde voor het vorderen van gebruikersgegevens. Ik acht deze verhoging ongewenst en onnodig, en dring er daarom op aan het huidige criterium 'verdenking van een misdrijf' in het wetsvoorstel te verwerken.

Bevel verstrekken gegevens telecomaandbieder (art. 2.7.3.3.5)

Het voorgestelde artikel 2.7.3.3.5 vervangt het huidige artikel 126ng, tweede en vierde lid. Er worden geen inhoudelijke wijzigingen voorgesteld. Het wetsvoorstel geeft mij op dit onderdeel dan ook geen aanleiding tot opmerkingen.

Bevel toekomstige gegevens (art. 2.7.3.3.6)

In deze bepaling zijn onderdelen van de huidige artikelen 126n en 126ne inhoudelijk ongewijzigd overgenomen. Het conceptwetsvoorstel geeft mij geen aanleiding tot opmerkingen.

Data-analyse door private partijen (art. 2.7.3.3.6a)

In deze nieuwe bepaling wordt geregeld dat de officier van justitie een partij kan bevelen een bewerking uit te voeren op de gegevens van die partij en de daardoor verkregen (nieuwe) gegevens te verstrekken. Een soortgelijk voorstel werd in 2001 door de commissie Mevis gedaan.⁹ Ook de commissie Koops beveelt de introductie van deze bevoegdheid aan, mede omdat het een meer proportionele en minder inbreukmakende wijze van gegevensvergaring kan zijn. Ik ben bijzonder verheugd dat deze bevoegdheid in het conceptwetsvoorstel is opgenomen. De formulering van het wetsartikel en de daarop gegeven toelichting acht ik duidelijk en werkbaar.

Notificatie (art. 2.7.3.3.7)

In het voorgestelde artikel 2.7.3.3.7 wordt de huidige regeling van de notificatieplicht uit artikel 126bb overgenomen. In het voorliggende wetsvoorstel wordt hierop een kleine wijziging aangebracht (C, onderdeel 15). In mijn consultatieadvies op Boek 2 merkte ik op dat uit artikel 2.7.3.3.7 (wellicht onbedoeld) een uitbreiding van de notificatieplicht voortvloeide, en verzocht de bepaling daarop aan te passen. Nu ik in onderhavig conceptwetsvoorstel op dit punt geen aanpassing zie, vraag ik nogmaals aandacht voor dit

⁹ Zie Rapport van de Commissie Strafvorderlijke gegevensvergaring in de Informatiemaatschappij, 2001, blz. 67-68.

Onderwerp

Consultatieadvies onderdeel opsporing in een digitale omgeving modernisering Wetboek van Strafvordering

Datum

6 november 2018

Pagina

10 van 11

punt. Ik verwijs naar mijn brief van 27 juni 2017, kenmerk KNP13001161, bijlage 2, blz. 56.

Bevel ontsluiteling (van verstrekte gegevens) (art. 2.7.3.3.8)

In het voorgestelde artikel 2.7.3.3.8 worden wijzingen voorgesteld ter verduidelijking. Ik onderschrijf de voorgestelde wijzigingen.

Vrijwillige verstrekking (art. 2.7.3.3.10)

In deze reeds in de consultatieversie Boek 2 opgenomen nieuwe bepaling wordt het 'gesloten systeem' van het vorderen van gegevens genuanceerd. In het voorliggende wetsvoorstel wordt de bepaling inhoudelijk niet gewijzigd, maar slechts een verouderde verwijzing naar de Wet bescherming persoonsgegevens vervangen door een verwijzing naar de Uitvoeringswet Algemene Verordening gegevensbescherming. In mijn consultatiereactie op Boek 2¹⁰ vroeg ik aandacht voor situaties waarin weliswaar sprake is van persoonsgegevens, maar niettemin de privacywetgeving niet van toepassing is omdat de gegevens voor persoonlijk of huishoudelijke doeleinden worden verwerkt. Nu in het voorliggende wetsvoorstel op dit punt geen wijzigingen worden voorgesteld, ga ik ervan uit dat hieraan in de uiteindelijke memorie van toelichting aandacht zal worden besteed.

Ontoegankelijkmaking en vernietiging van gegevens (Titel 7.4)

De huidige regeling van het ontoegankelijk maken van gegevens wordt op een aantal punten gewijzigd. Eén van de wijzigingen is de uitbreiding van de regeling naar inbeslaggenomen apparaten. De gedachte hierachter is dat het disproportioneel kan zijn om het beslag op een apparaat te handhaven omdat er illegale gegevens op zijn aangetroffen. Handhaving van het beslag, uitmondend in verbeurdverklaring of onttrekking aan het verkeer en vernietiging, kan wringen als naast illegale gegevens ook volstrekt legale gegevens op het apparaat zijn opgeslagen. Door mogelijk te maken dat ook kan worden bevolen dat bepaalde gegevens op een inbeslaggenomen apparaat ontoegankelijk worden gemaakt en daarna worden vernietigd, zo is de gedachte, kan het apparaat vervolgens worden teruggegeven aan de beslagene.

Alhoewel ik deze gedachtegang goed kan volgen, is de voorgestelde regeling mijns inziens technisch en capacitair niet uitvoerbaar. In mijn consultatiereactie op Boek 2 vroeg ik aandacht voor de risico's die het teruggeven van 'geschoonde' gegevensdragers oplevert. Niet is te garanderen dat a. alle illegale gegevens ontoegankelijk zijn gemaakt (het komt bijvoorbeeld voor dat kinderpornografische afbeeldingen versleuteld zijn opgeslagen in andere, onschuldige foto's) en b. dat de ontoegankelijkmaking door de beslagene niet ongedaan kan worden gemaakt nadat hij het inbeslaggenomen apparaat weer heeft teruggekregen.

Alles overziend ontraad ik de uitbreiding van de regeling van ontoegankelijkmaking en vernietiging van gegevens naar inbeslaggenomen apparaten. Ik zie meer in een regeling waarlangs betrokkenen legale gegevens kunnen terugvragen. In mijn reactie op het conceptwetsvoorstel Boek 6 schetste ik op hoofdlijnen hoe een dergelijke regeling er uit zou kunnen zien.¹¹ Een dergelijke regeling zou mijns inziens, ondanks daarvan te verwachten uitvoeringslasten, op beter uitvoerbare wijze bijdragen aan de proportionaliteit van het beslag op gegevensdragers dan de voorgestelde regeling van ontoegankelijkmaking en vernietiging.

Openbronnenonderzoek

De voorgestelde wijziging van artikel 2.8.2.4.1 vloeit voort uit het advies van de commissie Koops. Niet langer wordt in de omschrijving van de bevoegdheid tot onderzoek in open bronnen de eis gesteld dat gebruik wordt gemaakt van een technisch hulpmiddel.

¹⁰ Zie mijn brief van 27 juni 2017, kenmerk KNP13001161, bijlage 2, blz. 57.

¹¹ Zie mijn consultatiereactie op Boek 6, brief van 31 juli 2018, kenmerk KNP13001161, blz. 56-57.

www.politie.nl

Onderwerp

Consultatieadvies onderdeel opsporing in een digitale omgeving modernisering Wetboek van Strafvordering

Datum

6 november 2018

Pagina

11 van 11

Daarnaast wordt de term 'open bronnen' vervangen door 'publiek toegankelijke bronnen'. Beide wijzigingen zijn wat mij betreft verbeteringen.

Stelselmatige locatiebepaling

In artikel 2.8.2.10.1 wordt voorgesteld de bevoegdheid tot stelselmatige locatiebepaling mede te kunnen inzetten ter aanhouding van een verdachte. Ook deze wijziging vloeit voort uit het advies van de commissie Koops. Alhoewel het gebruik van locatiebepalende technieken ter aanhouding vaak zodanig kortstondig zal zijn dat geen sprake is van stelselmatigheid, is niet geheel uit te sluiten dat in sommige gevallen langduriger gebruik moet worden gemaakt van deze techniek om een verdachte te lokaliseren. Het is daarom goed dat het mogelijk wordt gemaakt dat in die gevallen, met toestemming van de officier van justitie, gebruik kan worden gemaakt van deze bevoegdheid.

Ik vertrouw erop u hiernaar voldoende te hebben geïnformeerd.

