PLATFORM BOD
BIJZONDERE OPSPORINGSDIENSTEN

Platform Bijzondere Opsporingsdiensten

Fiscale Inlichtingen- en Opsporingsdienst
Rijksgebouw De Knoop
Croeselaan 14
3521 CA Utrecht
Postbus 19266
3501 DG Utrecht

Platform BOD-en
[redacted]

Datum
2 november 2018

Bijlagen
1

Ministerie van Justitie en Veiligheid
T.a.v. de heer F.B.J. Grapperhaus
De minister van Justitie en Veiligheid
Postbus 20301
2500 EH Den Haag

Uw kenmerk
Ons kenmerk [redacted]
Betreft Consultatie onderdeel opsporing in een digitale omgeving modernisering Wetboek van Strafvordering

Zijne Excellentie,

Bij schrijven d.d. 10 oktober 2018, uw kenmerk [redacted], heeft u voor advies voorgelegd een nieuw onderdeel van het concept-Boek 2 (Het opsporingsonderzoek) van het nieuwe Wetboek van Strafvordering.

Namens de leden van het Platform Bijzondere Opsporingsdiensten maken wij van de gelegenheid gebruik een reactie te geven op het genoemde concept wetsvoorstel. Onze reactie treft u in de bij deze brief gevoegde bijlage aan.

Graag worden wij op de hoogte gehouden over de verdere voortgang.

Met vriendelijke groet,

De Voorzitter Platform Bijzondere Opsporingsdiensten

[redacted]
Directeur FIOD

PLATFORM BOD
BIJZONDERE OPSPORINGS DIENSTEN

Bijlage 1 bij brief Platform Bijzondere Opsporingsdiensten d.d. 2 november 2018 met kenmerk Platform/2018-041.

Reactie Platform Bijzondere Opsporingsdiensten inzake het conceptwetsvoorstel met betrekking tot de opsporing in een digitale omgeving (Boek 2), in het kader van de modernisering van het nieuwe Wetboek van Strafvordering.

Op 10 oktober 2018 heeft het platform Bijzondere Opsporingsdiensten (hierna: het Platform) het conceptwetsvoorstel met bijbehorende toelichting voor "bevoegdheden ter opsporing in een digitale omgeving (Boek 2)" van het toekomstige Wetboek van Strafvordering, met brief van de Minister van Veiligheid & Justitie, ontvangen.

Bij het ontwerpen van de onderhavige voorstellen heeft de wetgever gebruik gemaakt van de adviezen van de Commissie modernisering opsporingsonderzoek in het digitale tijdperk onder voorzitterschap van prof. E.J. Koops (hierna: commissie-Koops).[1] De commissie-Koops had tot taak de Minister van Justitie & Veiligheid te adviseren over de vraag of de wettelijke regeling van het opsporingsonderzoek, zoals voorgesteld in het in 2017 in consultatie gegeven concept-Boek 2 van het Wetboek van Strafvordering, bijstelling dan wel aanvulling behoeft.

Het Platform heeft met belangstelling kennis genomen van de inhoud van het conceptvoorstel met betrekking tot de opsporing in een digitale omgeving zoals dat is komen te luiden na advisering door de commissie-Koops en maakt bij deze graag gebruik van de gelegenheid om op de inhoud ervan in te gaan.

In het algemeen constateert het Platform met instemming dat een groot aantal adviezen die de commissie-Koops aan de minister heeft gegeven met betrekking tot de opsporing in een digitale omgeving, zijn overgenomen. Daardoor worden bepaalde, bestaande bevoegdheden weer bij de tijd gebracht en worden bovendien enkele nieuwe en nuttige bevoegdheden toegevoegd. Daarnaast lijkt het onderhavige voorstel voldoende flexibiliteit in de regeling in te bouwen om toekomstige ontwikkelingen op het gebied van de digitalisering in te passen in de wettelijke regeling, waarmee ook is voorzien in het streven naar een meer toekomstbestendig wetboek. Het Platform ondersteunt in dit verband de aanbeveling van de commissie-Koops om een permanente adviescommissie in te stellen die de wetgever proactief en tijdig op technisch-juridisch vlak adviseert over maatregelen die nodig zijn in het licht van toekomstige ontwikkelingen op het gebied van techniek, strafrechtelijke handhaving en privacybescherming,[2] zodat er een goede balans wordt getroffen tussen het algemene belang van een effectieve opsporing en het beschermen van de privacy van burgers.

In een aantal gevallen zou het in dit verband overigens een goede zaak zijn indien de invoering van de in dit wetsvoorstel beschreven bevoegdheden, of in ieder geval een deel daarvan, versneld zou kunnen worden. In de praktijk is er immers nu al behoefte aan deze nieuwe, hierna nog nader te bespreken, bevoegdheden.[3] Ten aanzien van bestaande bevoegdheden is inmiddels ook een bestendige lijn in de

---

[1] In deze commissie was ook het Platform Bijzondere Opsporingsdiensten vertegenwoordigd.

[2] Rapport Commissie Modernisering opsporingsonderzoek in het digitale tijdperk, *Regulering van opsporingsbevoegdheden in een digitale omgeving*, s.l. 2018, p. 64-65.

[3] Zie ook Rapport Commissie Modernisering opsporingsonderzoek in het digitale tijdperk, *Regulering van opsporingsbevoegdheden in een digitale omgeving*, s.l. 2018, p. 63.

jurisprudentie ontstaan, met name waar het onderzoek aan gegevens in een in beslag genomen gegevensdrager of geautomatiseerd werk betreft.[4] Eerdere invoering van deze in de jurisprudentie min of meer uitgekristalliseerde bevoegdheden ligt dan ook voor de hand. Bovendien kan daardoor ook al in een eerder stadium de nodige ervaring worden opgedaan met de uitoefening van deze bevoegdheden en de nodige (bestuurlijke) informatie worden verzameld ten behoeve van de evaluatie van de verschillende bevoegdheden en de effecten op de administratieve lasten, voordat het gemoderniseerde Wetboek van Strafvordering over enige jaren wordt ingevoerd.

In dit verband valt met name maar niet uitsluitend te denken aan de volgende bevoegdheden:

- Netwerkzoeking op afstand (art. 2.7.3.2.1, derde lid);
- Netwerkzoeking na inbeslagneming van de gegevensdrager of het geautomatiseerde werk (art. 2.7.3.2.3, derde lid);
- Onderzoek van gegevens die na inbeslagneming van de gegevensdrager of het geautomatiseerd werk binnenkomen (art. 2.7.3.2.6);
- Bevel analyse van gegevens jegens een derde (art. 2.7.3.3.6a);
- Stelselmatig overnemen van persoonsgegevens uit publiek toegankelijke bronnen (art. 2.8.2.4.1).

Derhalve geeft het Platform de wetgever in overweging om te bezien of invoering van de thans voorgestelde bevoegdheden gefaseerd kan plaatsvinden. In dat geval wordt de implementatie van het gemoderniseerde Wetboek van Strafvordering vergemakkelijkt omdat dan niet alle bevoegdheden op één moment worden ingevoerd. Daaruit vloeit tevens voort dat de opsporing al op kortere termijn efficiënter kan werken in het licht van de elkaar snel opvolgende technische ontwikkelingen in de digitale omgeving. Tot slot kan er dan al praktijkervaring worden opgedaan en kan worden onderzocht wat de voor- en nadelen ervan zijn in het kader van de evaluatie van de nieuwe bevoegdheden.

Helaas wordt ten aanzien van het onderzoek van gegevens toch één niet langer houdbare beperking in stand gehouden, namelijk het territorialiteitsbeginsel ten aanzien van gegevens die zich in de cloud bevinden. In de toelichting op het onderhavige wetsvoorstel wordt bij artikel 2.7.3.2.3 immers opgemerkt dat "uit de wetsgeschiedenis blijkt dat degene die een netwerkzoeking uitvoert zich ervan dient te vergewissen dat het elders aanwezige geautomatiseerde werk binnen zijn bevoegdheid valt. Gaat het om een computersysteem dat zich kennelijk in het buitenland bevindt, dan zal hij zich, behoudens een uitdrukkelijke verdragsrechtelijke grondslag, van onderzoek daarin moeten onthouden."[5]

In het consultatieadvies voor de Boeken 1 en 2 d.d. 26 juni 2017 heeft het Platform deze onhoudbaarheid al geadresseerd: "Deze behoudende instelling werkt – in de toekomst maar ook nu al – belemmerend voor de effectiviteit van de bestrijding van zware, georganiseerde criminaliteit, zeker ook op fiscaal en financieel-economisch gebied, en leidt ertoe dat het nieuwe Wetboek van Strafvordering op dit punt niet als gemoderniseerd en toekomstbestendig zal kunnen worden aangemerkt."

Zoals het Platform in het consulatieadvies ook al heeft opgemerkt, is de huidige

---

[4] Zie onder andere HR 4 april 2017, ECLI:NL:HR:2017:584.

[5] In de toelichting wordt in dit verband verder verwezen naar *Kamerstukken II* 1989/90, 21 551, nr. 3, p. 11-12 en *Kamerstukken II* 2015/16, 34 372, nr. 3, p. 42-50.

situatie immers dat allerlei clouddiensten grote hoeveelheden gegevens opslaan voor zeer vele gebruikers wereldwijd. De opslaglocaties zijn eveneens verspreid over de hele wereld, gegevens kunnen zonder veel moeite worden verplaatst van de ene naar de andere opslaglocatie en worden bovendien vaak op meerdere locaties opgeslagen om gegevensverlies te voorkomen. Dit maakt dat ook de eindgebruikers niet meer weten op hoeveel of welke gegevensdrager(s) de gegevens staan, of waar ter wereld die gegevensdragers zich bevinden. Ook de aanbieders van clouddiensten kunnen nu al vaak niet meer aangeven waar bepaalde gegevens zich bevinden. De in de cloud opgeslagen gegevens kunnen op elk moment en vanaf elke plaats via het internet worden benaderd en bewerkt. De kans is daardoor zeer groot dat gegevens die in de cloud worden opgeslagen, per saldo terecht komen op een gegevensdrager die zich fysiek buiten Nederland bevindt, maar waarvan de exacte locatie niet of slechts met zeer veel moeite is te bepalen. Bovendien is het uitermate onzeker dat die locatie een dag later nog dezelfde is.[6]

Indien en voor zover dus al op een bepaald moment kan worden bepaald in welk land gegevens zijn opgeslagen, zal met behulp van een rechtshulpverzoek aan het betreffende land moeten worden getracht de benodigde gegevens te verkrijgen. Dit leidt tot vaak lange doorlooptijden omdat de uitvoering van rechtshulpverzoeken doorgaans veel tijd vergt, of omdat getracht zal moeten worden om de gegevens op een andere wijze te verkrijgen in het geval met het betreffende land geen rechtshulpverdrag is gesloten.

De techniek van cloudopslag enerzijds en het onverkort vasthouden aan het territorialiteitsbeginsel anderzijds zorgen in de praktijk dan ook voor beperkingen die in de huidige tijd niet meer zijn te rechtvaardigen. Anders gezegd: het territorialiteitsbeginsel is niet meer hanteerbaar voor in de cloud opgeslagen gegevens. Een herbezinning op de onderliggende ratio voor bevoegdheden die in de virtuele wereld van gegevens en gegevensopslag moeten worden uitgeoefend ligt daarom in de rede.[7]

Intussen blijken de opsporingsdiensten van veel staten zich in de praktijk al toegang te verschaffen tot gegevens die buiten hun eigen landsgrenzen zijn opgeslagen, hetgeen meestal voortvloeit uit het feit dat de opsporende staat niet zeker weet op welk grondgebied de gegevens zich bevinden.[8] In ieder geval is er toenemende behoefte aan versterking van opsporingsbevoegdheden met betrekking tot de grensoverschrijdende toegang tot gegevens ten behoeve van bewijsgaring, als gevolg van de technologische ontwikkelingen, de toenemende complexiteit en het internationale karakter van computercriminaliteit.[9]

---

[6] Zie ook B.J. Koops, C. Conings en F. Verbruggen, *Zoeken in computers naar Nederlands en Belgisch recht*, Oisterwijk: Wolf Legal Publishers 2016, p. 155-158.

[7] Te meer nu bij de totstandkoming van het Cybercrimeverdrag (in de jaren 1990) partijen kennelijk nog niet tot overeenstemming konden komen over voorwaarden waaronder in dit soort situaties grensoverschrijdende toegang tot gegevens mogelijk is en de mate waarin het in de praktijk voor de opsporing tot problemen zou leiden niet werd voorzien (zie ook Kamerstukken II 2015/16, 34 372, nr. 3, p. 44). Daarnaast geeft artikel 32 van het Cybercrimeverdrag enerzijds geen fiat voor verdergaande bevoegdheden, maar sluit ze anderzijds ook niet uit; zie B.J. Koops, C. Conings en F. Verbruggen, *Zoeken in computers naar Nederlands en Belgisch recht*, Oisterwijk: Wolf Legal Publishers 2016, p. 159.

[8] Zie ook *Kamerstukken II* 2015/16, 34 372, nr. 3, p. 45.

[9] Zie *Kamerstukken II* 2015/16, 34 372, nr. 3, p. 42-50. Zie voor de recentere ontwikkelingen in de EU het bericht *"Europees onderzoeksbevel moet in werking treden"*, *NJB* 2017, afl. 22, nr. 1225: "Justitiële autoriteiten zouden ook toegang moeten hebben tot bewijsmateriaal in de cloud dat in een andere lidstaat of elders in de

In het onlangs verschenen kronieknummer van het Nederlands Juristenblad wordt in dit verband bovendien het volgende opgemerkt: "Rechtshandhaving is nog steeds grotendeels een nationale aangelegenheid, gebonden aan territoriale grenzen, terwijl data in de cloud zijn opgeslagen, verspreid over verschillende servers in verschillende landen. Niet zelden is de locatie van de data het enige internationale element in een strafzaak. Dan zijn de procedures van wederzijdse rechtshulp, zelfs als zij zijn gebaseerd op nieuwe instrumenten als het Europees onderzoeksbevel, erg omslachtig." [10]

De Europese Commissie heeft in dit licht op 17 april 2018 twee voorstellen gepresenteerd op het gebied van elektronische bewijsgaring, namelijk het voorstel voor een Verordening betreffende het Europees bevel tot verstrekking en het Europees bevel tot bewaring van elektronisch bewijsmateriaal in strafzaken,[11] en het daarmee samenhangende voorstel voor een Richtlijn tot vaststelling van geharmoniseerde regels inzake de aanwijzing van wettelijke vertegenwoordigers ten behoeve van de bewijsgaring in strafprocedures.[12] Deze voorstellen strekken tot de invoering van een Europees verstrekkingsbevel en een Europees bewaringsbevel. Beide bevelen worden door een justitiële autoriteit van een lidstaat uitgevaardigd of bekrachtigd met het oog op de verstrekking of bewaring van gegevens die zijn opgeslagen door een dienstverlener *in een andere jurisdictie*. De bevelen kunnen worden gericht tot alle dienstverleners die diensten verlenen in de EU, ook al bevinden de data zich elders en vaak buiten de EU.[13]

Zeker nu de invoering van het gemoderniseerde Wetboek van Strafvordering nog enige jaren op zich zal laten wachten, is er voor de wetgever naar de mening van het Platform geen belemmering om – minst genomen – nu al te bezien hoe de voorstellen van de Europese Commissie in dit verband zouden kunnen worden meegenomen in de verschillende bevoegdheden ten aanzien van het overnemen en het onderzoek van gegevens, met name die gegevens die zich naar alle waarschijnlijkheid buiten Nederland bevinden.

Het is daarnaast voor de eigenaar van de gegevens al zonder meer mogelijk de gegevens te benaderen, dus zonder dat deze zich hoeft te bekommeren over de vraag, of het land waar zijn eigen gegevens zijn opgeslagen wel weet heeft dat de gegevens zich daar bevinden, laat staan voor de toegang tot die gegevens al dan niet uitdrukkelijk toestemming geeft.[14] Een subject-georiënteerde benadering, waarbij de focus ligt op de gewoonlijke verblijfplaats van het subject,[15] of eerder nog

---

wereld is opgeslagen. De Commissie werkt momenteel aan oplossingen om justitiële autoriteiten te voorzien van moderne opsporingsmethoden waarmee zij gemakkelijker toegang kunnen krijgen tot elektronisch bewijsmateriaal. De Commissie zal op de JBZ-Raad van 8 juni oplossingen voorstellen om de toegang tot elektronisch bewijsmateriaal in het buitenland te vereenvoudigen."

[10] Zie J.S. Nan, "Kroniek van het straf(proces)recht", *NJB* 2018, afl. 35, p. 2693.

[11] COM(2018) 225.

[12] COM(2018) 226.

[13] Zie in dit verband ook *Kamerstukken II* 2018/19, 32 317, nr. 526, waarin de Minister van Justitie & Veiligheid in een brief aan de Kamer bericht over de Amerikaanse CLOUD act, een reactie op juridische kwesties die voortkomen uit de ontwikkeling van de internationale dataopslag in de digitale wereld.

[14] De eigenaar van de gegevens kan overigens ook bewust gebruik maken van de technische aspecten van opslag in de cloud en zo de strafvordering frustreren: zie B.J. Koops, C. Conings en F. Verbruggen, *Zoeken in computers naar Nederlands en Belgisch recht*, Oisterwijk: Wolf Legal Publishers 2016, p. 166-167.

[15] Met 'subject' wordt in dit verband in ieder geval bedoeld: de strafrechtelijk onderzochte persoon.

een benadering die zich oriënteert op de vraag of Nederland voor een bepaald delict rechtsmacht heeft, verdient daarom de voorkeur boven de object-georiënteerde benadering die uitgaat van de opslaglocatie van de gegevens en in de praktijk dus vaak grote uitvoeringsproblemen met zich brengt. [16]

Deze nieuwe benadering maakt het voor de praktijk mogelijk dat gegevens in ieder geval kunnen worden overgenomen, waardoor het veilig stellen van dit soort bewijsmateriaal niet langer afhankelijk is van onzekere factoren als de opslaglocatie van de gegevens, de medewerking of het medeweten van het land waar de opslaglocatie zich bevindt en of er met dat land wederzijdse rechtshulp is overeengekomen. Daarnaast worden hiermee ook enkele van de doelen van de modernisering van het Wetboek van Strafvordering nog beter gediend, namelijk die van een techniekonafhankelijk(er) en die van een toekomstbestendig(er) wetboek.

Gelet op het voorgaande wordt nogmaals voorgesteld om bij de verschillende nieuwe bevoegdheden, zoals die in de thans voorgestelde artikelen 2.7.3.2.3 en 2.7.3.2.6, niet langer uit te gaan van de vraag op welke plaats de gegevens zich fysiek bevinden, maar van de vraag waar het subject gewoonlijk verblijft, dan wel of Nederland voor een bepaald delict rechtsmacht heeft.

Op deze plaats merkt het Platform alvast op dat bij artikel 2.7.3.2.6 nader zal worden ingegaan op het begrip 'opslag' als bedoeld in de artikelen 2.7.3.2.3 en 2.7.3.2.6, alsmede over de (on)bepaalbaarheid van het tijdstip waarop een gegeven is gegenereerd of opgeslagen als waar het is opgeslagen.

In het vervolg van deze reactie wordt de volgorde in het conceptvoorstel aangehouden en gaat het Platform specifiek in op een aantal van de voorgestelde bepalingen.

Onderdeel A: Definities (art. 2.1.1.1)

In het in een eerder stadium al voorgestelde artikel 2.1.1.1 worden met name de definities van de begrippen gegevensdrager, geautomatiseerd werk en gegevens nader omschreven en enigszins gewijzigd, in overeenstemming met de betreffende adviezen van de commissie-Koops.

Met deze vooral vanuit techniek ingegeven wijzigingen kan worden ingestemd.

Onderdelen B en C: Onderzoek van gegevens

In de onderdelen B en C van dit conceptvoorstel wordt de bevoegdheid tot het onderzoeken van gegevens in den brede opnieuw geregeld, mede naar aanleiding van recente jurisprudentie op dit gebied. Verder is met instemming te constateren dat het begrip 'beslag op gegevens' niet meer terugkomt, maar is gekozen voor de beter op de praktijk aangesloten en inmiddels volledig ingeburgerde term 'overnemen van gegevens' zoals die in onderdeel C wordt voorgesteld.

---

[16] Bovendien lijkt het uitgangspunt dat de doorzoeking naar gegevens wordt gelokaliseerd daar waar die gegevens staan opgeslagen, niet bepaald een overtuigde keuze van de Raad van Europa; zie B.J. Koops, C. Conings en F. Verbruggen, *Zoeken in computers naar Nederlands en Belgisch recht*, Oisterwijk: Wolf Legal Publishers 2016, p. 159.

Samengevat kan het Platform instemmen met de voorstellen inzake het onderzoek van gegevens zoals opgenomen in de nieuwe Titel 7.3. Ten aanzien van een aantal onderwerpen maakt het Platform nog de volgende opmerkingen.

Definities van enkele gebruikte begrippen
Voorafgaand aan de voorgestelde bepalingen voor Afdeling 7.3.1 (onderdeel C) worden enkele begrippen nader gedefinieerd, zoals onderzoek van gegevens. In artikel 2.7.3.2.1 wordt vervolgens voor het eerst gesproken van 'onderzoek van gegevens aan gegevens'. Volgens de toelichting is het begrip 'onderzoek van gegevens' een koepelterm, waaronder dan het geheel aan handelingen moet worden verstaan dat ten aanzien van gegevens kan worden uitgevoerd. Het betreft hier zowel handelingen die worden uitgevoerd aan apparaten waarop gegevens zijn opgeslagen, als handelingen aan gegevens. Vandaar dat soms wordt gesproken over 'onderzoek van gegevens aan gegevens', aldus de concepttoelichting bij onderdeel B en C.

De vraag die hierbij opkomt is, of de term 'onderzoek van gegevens aan gegevens' wel zo noodzakelijk is voor een goed begrip van wat de verschillende bevoegdheden van Titel 7.3 behelzen. Het is een moeilijk leesbare term, terwijl voor iedereen duidelijk is dat het bij deze bevoegdheden gaat om het onderzoek van gegevens, ongeacht of die zijn opgeslagen op of benaderbaar zijn door middel van een al dan niet in beslag genomen gegevensdrager of geautomatiseerd werk, of die zijn overgenomen uit een gegevensdrager of geautomatiseerd werk. Het onderzoek van die gegevens staat derhalve centraal. Bovendien wordt uiteindelijk maar een keer gesproken van 'onderzoek van gegevens aan gegevens' (artikel 2.7.3.2.3, eerste lid), terwijl 'onderzoek van gegevens' elders wordt gebruikt (bijvoorbeeld in artikel 2.7.3.2.3, tweede lid), soms in combinatie met 'onderzoek aan gegevens' (bijvoorbeeld in artikel 2.7.3.2.2, eerste lid). Tenslotte is het praktische verschil tussen het onderzoek *van* gegevens en het onderzoek *aan* gegevens dusdanig klein dat beter gekozen kan worden voor de eenduidige term 'onderzoek van gegevens'.

Derhalve wordt voorgesteld om niet te spreken van 'onderzoek van gegevens aan gegevens' zoals met name in artikel 2.7.3.2.3, eerste lid, maar van 'onderzoek van gegevens' waaronder dan eveneens is te verstaan het onderzoek aan gegevens.

Los hiervan heeft de wetgever gevraagd of definities van de begrippen onderzoek, kennisnemen en overnemen van gegevens, alsmede al dan niet ingrijpend stelselmatig onderzoek van gegevens in de wet moeten worden opgenomen, of dat deze in de toelichting beter op hun plaats zouden zijn.

Hoewel er zeker iets voor is te zeggen om deze begrippen in de wet zelf op te nemen omdat zij daar ook meerdere keren worden gebruikt en opneming in de wet kan bijdragen aan een eenduidige uitleg van die begrippen, lijkt het daarvoor al voldoende als deze begrippen in de toelichting worden uitgelegd. Opneming van deze begrippen in de wet is dan ook niet noodzakelijk.

Dit geldt zeker ten aanzien van de toch enigszins open geformuleerde begrippen 'stelselmatig' en 'ingrijpend stelselmatig' onderzoek van gegevens. De concepttoelichting geeft ten aanzien van beide begrippen immers een goed en uitgebreid kader weer en noemt daarbij de relevante kaders die dienen bij de beantwoording van de vraag of een bepaald voorgenomen onderzoek van gegevens een beperkte inbreuk op de privacy vormt – in welk geval de opsporingsambtenaar zelfstandig bevoegd is tot dat onderzoek – of dat een dergelijk onderzoek een meer

dan geringe inbreuk zal maken op de privacy van een persoon en derhalve een bevel van de officier van justitie nodig is, eventueel aan te vullen met een machtiging van de rechter-commissaris.

Mogelijk dat in de toelichting nog nader kan worden verduidelijkt wanneer er sprake is van het overnemen van gegevens, in relatie tot het afgeven of achterlaten van een bewijs van uitoefening als bedoeld in artikel 2.7.3.1.1. Door de wijze waarop dit begrip thans is geformuleerd ("het kopiëren van gegevens uit een externe bron, ongeacht de vraag of de gegevens in de externe bron beschikbaar blijven") vallen hier strikt genomen ook de gevallen onder waarin bijvoorbeeld foto's gemaakt worden van gegevens, zoals kentekenplaten op voertuigen of meterstanden, zonder dat de gegevensdragers[17] op zichzelf in beslag (kunnen) worden genomen. De vraag is dus of dit bijkomend effect door de wetgever beoogd is. De mogelijk hieruit voortvloeiende verzwaring van de administratieve lasten is op voorhand moeilijk in te schatten maar lijkt overigens gering.

Bewijs van uitoefening van de bevoegdheid tot het overnemen van gegevens
In artikel 2.7.3.1.1, eerste lid, wordt bepaald dat wanneer tijdens een doorzoeking of betreding van een plaats gegevens worden overgenomen, van de uitoefening van deze bevoegdheid direct een bewijs moet worden afgegeven of achtergelaten. Het is echter praktisch niet altijd mogelijk een dergelijk bewijs direct af te geven of achter te laten, met name in de gevallen dat grote hoeveelheden gegevens zijn overgenomen waarvan de aard – die immers op grond van het eerste lid in het bewijs moet worden vermeld – zich niet altijd eenvoudig en snel laat bepalen.

Daarom wordt voorgesteld het woord 'direct' in deze bepaling te vervangen door 'zo spoedig mogelijk'. Dit geeft meer tijd om de aard van de overgenomen gegevens te bepalen, terwijl in de huidige praktijk vaak al een kopie van de overgenomen gegevens wordt achtergelaten waaruit betrokkene zelf ook al de aard van de overgenomen gegevens kan afleiden.

Geheimhoudingsplicht jegens derden
In artikel 2.7.3.1.2 wordt bepaald dat degene die anders dan voor persoonlijk gebruik gegevens verwerkt en jegens wie, kort gezegd, een bevoegdheid uit titel 7.3 wordt uitgeoefend, in het belang van het onderzoek geheimhouding moet betrachten over datgene wat hem met betrekking tot die bevoegdheid bekend is.

Het Platform is verheugd te constateren dat deze mogelijkheid van het opleggen van geheimhouding jegens derden bij wie op enigerlei wijze gegevens zijn overgenomen, thans expliciet in de wet wordt geregeld.

Overnemen van gegevens in relatie tot het doorzoeken of betreden van plaatsen
In artikel 2.7.3.2.1 is ten eerste het huidige artikel 125i opgenomen, dat de vastlegging van gegevens regelt in het kader van de betreding en de doorzoeking van plaatsen. Nieuw is het derde lid, dat de mogelijkheid biedt om met toestemming van een bepaalde categorie van betrokkenen een doorzoeking van een plaats voor het verrichten van het onderzoek van gegevens op afstand uit te voeren. Volgens de toelichting kan het onderzoek van gegevens immers een tijdrovende bezigheid zijn,

---

[17] In de gegeven voorbeelden: het voertuig waarop het kenteken is aangebracht respectievelijk de elektriciteits- of gasmeter. In dit soort gevallen zou dan beter gesproken kunnen worden van het registreren van gegevens: zie Rapport Commissie Modernisering opsporingsonderzoek in het digitale tijdperk, *Regulering van opsporingsbevoegdheden in een digitale omgeving*, s.l. 2018, p. 157.

zodat de doorzoeking op afstand in bepaalde gevallen inderdaad een goed alternatief kan zijn ten opzichte van het voor langere tijd stilleggen van een kantoor of bedrijf.

Onderzoek van gegevens in gegevensdragers en geautomatiseerde werken
In artikel 2.7.3.2.2 is de neerslag te vinden van het hiervoor reeds aangehaalde smartphone-arrest van de Hoge Raad van 4 april 2017. Deze bepaling voorziet in feite in een drietrapsbevoegdheid, waardoor, zeker gelet op de goede en uitgebreide toelichting bij dit artikel, in de praktijk voldoende tegemoet wordt gekomen aan de mogelijke inbreuken op de privacy en de consequenties daarvan als gevolg van het onderzoek van gegevens die zijn opgeslagen op of toegankelijk zijn via een gegevensdrager of geautomatiseerd werk en die ten behoeve van een opsporingsonderzoek zijn overgenomen, dan wel worden onderzocht nadat die gegevensdrager of dat werk in beslag is genomen.

Het is vooral goed om te constateren dat in de toelichting expliciet wordt geconcludeerd dat, gelet op het geobjectiveerde criterium "*op voorhand redelijkerwijs voorzienbaar* zijn dat een min of meer volledig beeld van bepaalde aspecten van het persoonlijk leven van betrokkene kan worden verkregen", het onderzoek niet met terugwerkende kracht onrechtmatig is wanneer na het verrichten van het onderzoek van gegevens (alsnog) blijkt dat het onderzoek uiteindelijk toch een meer dan geringe inbreuk op de privacy heeft gemaakt. En alleen wanneer er dus *op voorhand* sprake lijkt te zijn van een meer dan geringe inbreuk op de privacy van betrokkenen, dient het bevel tot onderzoek van gegevens te worden gegeven door de officier van justitie, zodat het onderzoek van gegevens waarvan op voorhand juist geen of slechts een geringe inbreuk op de privacy is te verwachten, zelfstandig door de opsporingsambtenaar kan worden verricht.

Deze bepaling komt in zijn huidige vorm voldoende tegemoet aan de bezwaren die het Platform op dit punt in haar advies in de formele consultatie van Boek 2 in 2017 heeft geuit. Met name daar waar het gaat om bedrijfsgegevens die naar hun aard veelal niet of slechts in geringe mate privacygevoelig zijn, constateert het Platform met tevredenheid dat de opsporingsambtenaar voldoende ruimte heeft en behoudt om zelfstandig onderzoek in dergelijke gegevens te verrichten.

Netwerkzoeking
In artikel 2.7.3.2.3, eerste lid, is het huidige artikel 125j opgenomen, dat het onderzoek regelt van gegevens die elders zijn opgeslagen maar die vanaf de plaats waar het onderzoek plaatsvindt, rechtmatig kunnen worden benaderd (de netwerkzoeking). Nieuw is het derde lid, waarin wordt voorgesteld om onderzoek van gegevens mogelijk te maken die elders zijn opgeslagen maar rechtmatig kunnen worden benaderd vanuit een gegevensdrager of geautomatiseerd nadat die gegevensdrager of dat geautomatiseerd werk in beslag is genomen (de netwerkzoeking vanuit een in beslag genomen gegevensdrager of geautomatiseerd werk). Uiteraard gaat deze bevoegdheid niet zo ver, dat vanuit de gegevensdrager of het geautomatiseerd werk toegang wordt verkregen tot gegevens waar de rechthebbende van de gegevensdrager of het werk zelf niet rechtmatig toegang toe heeft, vrij vertaald het hacken in elders aanwezige gegevensdragers of geautomatiseerde werken met behulp van op een bepaalde plaats aanwezige of in beslag genomen gegevensdragers of geautomatiseerde werken (artikel 2.7.3.2.3, tweede en derde lid).

Met name de mogelijkheid om een netwerkzoeking te verrichten met of via een in beslag genomen gegevensdrager of geautomatiseerd werk voorziet in de huidige

praktijk in een behoefte en is daarmee een goede aanvulling op de bevoegdheid van de netwerkzoeking 'ter plaatse'. Zoals hiervoor reeds opgemerkt, zou het daarom een goede zaak zijn als deze nieuwe bevoegdheid al eerder zou kunnen worden ingevoerd.

Bovendien houdt artikel 2.7.3.2.3, vijfde lid, voldoende rekening met de mogelijkheid dat de toegang tot een in beslag genomen gegevensdrager of geautomatiseerd werk niet altijd direct na de inbeslagneming kan worden verkregen. In dergelijke gevallen heeft de officier van justitie namelijk maximaal een maand de tijd om te bezien of die toegang verkregen kan worden, waarna de netwerkzoeking als bedoeld in het derde lid kan worden uitgevoerd. Deze periode kan telkens met een maand worden verlengd. Deze mogelijkheid van verlenging zal met name nuttig zijn in de gevallen dat ook binnen de periode dat het bevel tot onderzoek van gegevens als hier bedoeld moet worden gegeven, nog geen toegang tot de in beslag genomen gegevensdrager of het in beslag genomen geautomatiseerde werk kan worden verkregen.

Het Platform geeft ten aanzien van de bevoegdheid tot netwerkzoeking na inbeslagneming dan ook in overweging deze vooruitlopend op de invoering van het gemoderniseerde Wetboek van Strafvordering te implementeren.

Echter, het Platform verwijst hierbij nogmaals uitdrukkelijk naar hetgeen hiervoor is gezegd over de niet langer houdbare notie van territorialiteit die onnodig beperkend is in de huidige praktijk ten aanzien van gegevens die in de cloud zijn opgeslagen.

Bevriezen van gegevens
In artikel 2.7.3.2.4 wordt de mogelijkheid geopend dat opsporingsambtenaren de nodige maatregelen kunnen nemen ter voorkoming van wegmaking, onbruikbaarmaking, wijziging of verlies van gegevens. Onder dergelijke maatregelen valt blijkens de toelichting op dit artikel ook het open houden van een geautomatiseerd werk, het onderbreken van netwerkverbindingen, het gebruik van stoorzenders om communicatie te verbreken, alsmede het maken van een image van de inhoud van een gegevensdrager of geautomatiseerd werk.

Deze nieuwe bevoegdheid is – ook voor de huidige praktijk – een goede uitbreiding van de mogelijkheden om onderzoek van gegevens mogelijk te maken en het voorstel tot invoering van deze bevoegdheid wordt daarom door het Platform zeker ondersteund.

Onderzoek van gegevens na inbeslagneming
In artikel 2.7.3.2.6 wordt bepaald dat het bevel tot onderzoek van gegevens als bedoeld in de artikelen 2.7.3.2.2, eerste lid, en 2.7.3.2.3, eerste lid, zich tevens uitstrekt over gegevens die eerst na de inbeslagneming van de gegevensdrager of het geautomatiseerde werk en wel gedurende drie dagen na die inbeslagneming worden opgeslagen. Onder omstandigheden kan dit bevel voor ten hoogste een maand worden verlengd.

Enerzijds is het goed om te constateren dat met deze nieuwe bepaling tegemoet wordt gekomen aan een in de huidige praktijk spelend probleem. Er worden immers reeds nu al smartphones en dergelijke in beslag genomen, waarop na die inbeslagneming nog allerlei gegevens worden ontvangen. Dit hangt ook samen met hetgeen hiervoor is opgemerkt ten aanzien van het bevriezen van gegevens en specifiek de maatregel van het open houden van een gegevensdrager of een geautomatiseerd werk. Door dit open houden is de kans immers reëel dat er ook na

de inbeslagneming nog steeds gegevens worden ontvangen.

De huidige formulering van deze bepaling leidt echter ook tot enkele, vooral vanuit technisch oogpunt ingegeven moeilijkheden. Zo is het niet altijd mogelijk om te bepalen op welk tijdstip een gegeven is gegenereerd, of op welk tijdstip een gegeven exact is ontvangen. Verder worden gegevens tegenwoordig lang niet altijd op de gegevensdrager of in het geautomatiseerd werk zelf opgeslagen, maar kan daarentegen via die apparaten toegang worden verkregen tot die gegevens die zich dan ergens 'in de cloud' bevinden. Door nu te bepalen dat gegevens mogen worden onderzocht mits zij tot maximaal *drie dagen* na de inbeslagneming van de gegevensdrager of het geautomatiseerde werk daarop zijn *opgeslagen*, kan discussie ontstaan[18] over de vraag wanneer die gegevens daadwerkelijk zijn gegenereerd en of die gegevens daadwerkelijk op de in beslag genomen gegevensdrager of het geautomatiseerde werk zijn opgeslagen. Dit is een onwenselijke situatie.

Gelet op het voorgaande stelt het Platform voor om deze bepaling zodanig aan te passen dat gegevens die pas worden *gegenereerd* nadat een gegevensdrager of geautomatiseerd werk in beslag is genomen, eveneens kunnen worden onderzocht na een daartoe strekkend bevel als bedoeld in de artikelen 2.7.3.2.2, eerste lid en 2.7.3.2.3, eerste lid. Op deze manier is het niet meer relevant of die gegevens ook daadwerkelijk op de te onderzoeken gegevensdrager of het geautomatiseerde werk zijn opgeslagen.

Hierbij kan ook aansluiting gezocht worden bij artikel 2.7.3.3.6, waarin de bevoegdheid is geregeld om van een derde, onder bepaalde voorwaarden, gegevens te vorderen die eerst na het tijdstip van het bevel worden verwerkt. En voor zover het gegevens betreft die zijn te beschouwen als communicatie die wordt beschermd door het telecommunicatiegeheim als bedoeld in artikel 13 van de Grondwet, kan daaraan de aanvullende eis van een machtiging van de rechter-commissaris worden verbonden.

Ten aanzien van de in deze bepaling opgenomen termijnen van drie dagen en een maand merkt het Platform op, dat deze termijnen om verschillende redenen kunnen gaan knellen. Ten eerste is er niet altijd voldoende capaciteit beschikbaar om in beslag genomen gegevensdragers en geautomatiseerde werken binnen een maand, laat staan binnen drie dagen, te onderzoeken op voor het opsporingsonderzoek relevante gegevens. Ten tweede kan soms pas na verloop van meer dan een maand toegang worden verschaft tot de gegevens omdat de beveiliging van een in beslag genomen gegevensdrager of geautomatiseerd werk slechts na verloop van tijd kan worden doorbroken. In beide gevallen is het zonder meer mogelijk dat gegevens worden gegenereerd die op dergelijke apparaten worden opgeslagen of via die apparaten zijn te benaderen.

Een hieraan gerelateerde kwestie is dat gedurende de gehele periode dat geprobeerd wordt om toegang te krijgen tot een in beslag genomen gegevensdrager of geautomatiseerd werk, nieuwe gegevens gegenereerd kunnen worden. Aangezien vaak niet is te bepalen wanneer deze gegevens exact zijn gegenereerd, bestaat de mogelijkheid dat ook gegevens die pas na drie dagen na het moment van inbeslagneming van een gegevensdrager of geautomatiseerd werk kunnen worden benaderd. Hieruit volgt dat de termijn van drie dagen als genoemd in artikel

[18] Zeker wanneer pas na langere tijd dan drie dagen na de inbeslagneming toegang tot de in beslag genomen gegevensdrager of het in beslag genomen geautomatiseerde werk kan worden verkregen.

2.7.3.2.6, eerste lid, in de praktijk waarschijnlijk niet werkbaar is omdat de scheidslijn tussen gegevens die binnen deze drie dagen zijn gegenereerd en gegevens die meer dan drie dagen na de inbeslagneming zijn gegenereerd niet of nauwelijks is te trekken.

Hoewel het Platform het op zichzelf zonder meer positief vindt dat de wetgever deze praktische kwestie probeert op te lossen, adviseert het om de thans voorgestelde termijnen nog eens kritisch te bezien. Daar dit echter mogelijk pas na enige tijd goed kan worden beoordeeld stelt het Platform voor om ook met deze bepaling op korte termijn te gaan experimenteren, zodat ervaring kan worden opgedaan met deze nieuwe bevoegdheid en aan de hand daarvan kan worden bekeken of en op welke wijze deze bepaling aanpassing behoeft.

Een bevel als bedoeld in artikel 2.7.3.2.6, eerste lid, moet worden gegeven door de officier van justitie, waaruit volgt dat een opsporingsambtenaar niet zelfstandig kennis zou mogen nemen van gegevens die kort na de inbeslagneming van een gegevensdrager of geautomatiseerd werk gegenereerd en benaderbaar worden. In bepaalde gevallen is het echter wel gewenst dat een opsporingsambtenaar wel zelfstandig kennis kan nemen van gegevens na inbeslagneming.

Een praktisch voorbeeld kan deze wens verduidelijken:
Een (buitengewoon opsporings)ambtenaar van de Belastingdienst/Douane houdt op Schiphol een persoon staande en bij controle van diens bagage treft de ambtenaar een hoeveelheid verdovende middelen aan. De persoon wordt daarop aangehouden en zijn smartphone wordt in beslag genomen ten behoeve van de waarheidsvinding. Uit onderzoek van de contactgegevens kan immers mogelijk worden vastgesteld aan wie de verdachte de verdovende middelen had moeten afleveren. Kort na de inbeslagneming van de smartphone komt er een kort berichtje binnen van een onbekende persoon, waaruit blijkt dat en waar hij de verdachte wil ontmoeten om de verdovende middelen over te nemen en hoe de verdachte hem kan herkennen. Het is derhalve van belang dat de identiteit van die tweede persoon direct wordt vastgesteld en eveneens kan worden aangehouden.

In dit voorbeeld zou de opsporingsambtenaar, gelet op artikel 2.7.3.2.6, niet zelfstandig van dat bericht kennis mogen nemen, omdat daarvoor een bevel van de officier van justitie nodig is. Het is echter in dit soort gevallen noodzakelijk dat direct actie kan worden ondernomen zodat een bevel van de officier van justitie niet kan worden afgewacht. Bovendien is het vaak niet te vermijden dat de opsporingsambtenaar al kennis neemt van een dergelijk gegeven, bijvoorbeeld als hij op dat moment de maatregelen van artikel 2.7.3.2.4 neemt om te voorkomen dat de smartphone in de beveiligde stand komt (oftewel het open houden van het geautomatiseerde werk).

Het Platform stelt daarom voor om in artikel 2.7.3.2.6 de aanvullende mogelijkheid op te nemen dat bij dringende noodzakelijkheid en indien een bevel van de officier van justitie niet kan worden afgewacht, de opsporingsambtenaar zelfstandig kennis kan nemen van gegevens die na de inbeslagneming van een gegevensdrager of geautomatiseerd werk gegenereerd worden in die zin, dat het onderzoek door de opsporingsambtenaar zodanig beperkt moet blijven dat er geen sprake is van (indringend) stelselmatig onderzoek als bedoeld in Titel 7.3.

Opheffing beveiliging en ontsleuteling
In artikel 2.7.3.2.7 wordt de bestaande bevoegdheid van de officier van justitie om

degene van wie redelijkerwijs kan worden vermoed dat hij de beveiliging van een gegevensdrager of geautomatiseerd werk of de versleuteling van gegevens ongedaan kan maken, overgenomen vanuit het huidige artikel 125k en daarbij tevens uitgebreid tot andere dan de in laatstgenoemd artikel genoemde situaties. Vooral die uitbreiding wordt door het Platform met instemming ontvangen.

In het tweede lid van artikel 2.7.3.2.7 wordt verder de mogelijkheid geopend voor de opsporingsambtenaar om zelfs tegen de wil van degene van wie redelijkerwijs kan worden vermoed dat hij deze beveiliging of versleuteling ongedaan kan maken, de maatregelen te treffen die daartoe redelijkerwijs noodzakelijk zijn. In de bijbehorende toelichting wordt hieraan toegevoegd dat in deze bevoegdheid ligt besloten dat de uitvoering van dit bevel gepaard kan gaan met het toepassen van (gepaste) lichamelijke dwang en er aldus sprake is van een duldplicht voor personen, onder wie ook verdachten, voor het meewerken aan de ongedaanmaking van een biometrische beveiliging of versleuteling. Terecht wordt hier gesproken van een duldplicht en geconstateerd dat de formulering zoals hier voorgesteld niet raakt aan of strijdt met het nemo-teneturbeginsel.

Het Platform is verheugd te zien dat deze mogelijkheid wordt geopend en voegt hieraan toe dat deze bepaling ook in de huidige praktijk zal voorzien in een toenemende behoefte om beveiligingen van apparaten en versleutelingen van gegevens ongedaan te maken.

Ten aanzien van de in artikel 2.7.3.2.7, tweede lid, genoemde biometrische kenmerken wordt nog wel opgemerkt dat het noemen van specifieke biometrische kenmerken mogelijk te beperkend zal zijn voor de (nabije) toekomst, als ook andere kenmerken dan vingerafdrukken of opnamen van iris of gezicht kunnen worden gebruikt als vormen van beveiliging.

Het Platform adviseert dan ook om in de wet alleen het begrip biometrische kenmerken te gebruiken en de nadere benoeming van die kenmerken in een algemene maatregel van bestuur op te nemen, zodat sneller kan worden ingespeeld op toekomstige ontwikkelingen op dit vlak. Verder zouden in deze algemene maatregel van bestuur aanvullende voorschriften kunnen worden opgenomen met betrekking tot de uitvoering van deze bevoegdheid.

Onderdeel D: Verstrekking van gegevens

In dit onderdeel worden bepalingen voorgesteld die in grote lijnen overeenkomen met de huidige bepalingen in de artikelen 126n tot en met 126ni, 126u tot en met 126ui, 126zh, 126zj en 126zja en enkele andere hiermee verband houdende artikelen zoals artikel 126bb Sv.

Het Platform constateert met instemming dat in het algemeen is afgestapt van het gebruik van de term 'inbeslagneming van gegevens' en weer wordt teruggegrepen op het ingeburgerde 'verstrekken van gegevens'. Verder is er door het onderhavige voorstel meer eenvoud gebracht in de verschillende bepalingen die de verstrekking van verschillende soorten gegevens regelen.

Specifiek ten aanzien van artikel 2.7.3.3.3, vijfde lid, merkt het Platform op dat het invoeren van de mogelijkheid om een generiek bevel tot verstrekking van gegevens te geven, in de praktijk zeer waarschijnlijk zal leiden tot een verlichting van administratieve lasten. Door middel van een generiek bevel kunnen immers

meerdere personen worden bevolen om bepaalde gegevens te verstrekken en dat gedurende twee weken, waar in de huidige praktijk voor iedere persoon en voor elke verstrekking in beginsel een apart bevel moet worden opgemaakt.

Bevel tot het analyseren van gegevens
In artikel 2.7.3.3.6a, eerste lid, wordt de nieuwe bevoegdheid neergelegd om degene die anders dan ten behoeve van persoonlijk gebruik gegevens verwerkt en waarvan kan worden vermoed dat hij toegang heeft tot bepaalde gegevens, bevelen dat hij deze gegevens bewerkt en de daardoor verkregen gegevens verstrekt. In het tweede lid is bepaald dat een opsporingsambtenaar de betreffende persoon aanwijzingen kan geven ten behoeve van de wijze waarop de analyse van gegevens wordt uitgevoerd.

Het Platform constateert met instemming dat met deze bevoegdheid wordt voorzien in een groeiende behoefte in de praktijk. Het komt immers steeds vaker voor dat niet alleen reeds vastgelegde gegevens nodig zijn voor het opsporingsonderzoek, maar dat het ook gewenst kan zijn dat deze reeds vastgelegde gegevens zodanig worden bewerkt dat daardoor nieuwe, evenzeer relevante gegevens worden gegenereerd, waarmee in de opsporing ook de nodige tijd en capaciteit kan worden bespaard. Een tweede voordeel van deze nieuwe bevoegdheid is, zoals ook in de toelichting ter plaatse wordt opgemerkt, dat hierdoor kan worden voorkomen dat gegevens die niet relevant zijn voor het onderzoek toch (onbedoeld) worden verstrekt, bijvoorbeeld doordat het technisch niet mogelijk is de relevante gegevens te scheiden van de niet relevante gegevens zoals in het geval van een grote hoeveelheid boekhoudkundige gegevens die op een zinvolle wijze moeten worden geordend door middel van een softwarepakket.

Vooral de mogelijkheid van het geven van aanwijzingen door een opsporingsambtenaar, indien de officier van justitie dat in zijn bevel bepaalt, kan verder bijdragen aan het nut van deze bevoegdheid. Zoals uit de toelichting kan worden afgeleid, kunnen de aanwijzingen van de opsporingsambtenaar meer of minder vergaand zijn: afhankelijk van de omvang van het bedrijf tegen wie het hier bedoelde bevel is gericht, kan de rol van de opsporing groter of kleiner zijn. Onder het geven van aanwijzingen wordt blijkens de toelichting mede verstaan, het leveren van hardware en software ter uitvoering van de analyse. Op deze wijze biedt het tweede lid de ruimte om de aanwijzingen aan te passen aan de specifieke casus.

In artikel 2.7.3.3.6a, derde lid, wordt verder de mogelijkheid gecreëerd om degene die de analyse mogelijk moet gaan uitvoeren, eerst te bevelen de nodige inlichtingen te verschaffen over de gegevens waartoe hij toegang heeft en over de handelingen die nodig zijn om de bewerkingen als bedoeld in het eerste lid uit te voeren.

Het Platform is dan ook verheugd te constateren dat tegemoet wordt gekomen aan een behoefte in de praktijk door middel van deze nieuwe bepalingen.

Vrijwillige verstrekking van gegevens
In artikel 2.7.3.3.10 is bepaald dat in de gevallen waarin een bevel tot verstrekking van gegevens kan worden gegeven als bedoeld in Afdeling 7.3.3, het niet is toegestaan te vragen om vrijwillige verstrekking van gegevens, tenzij het verzoek zodanig is gemotiveerd dat het de verantwoordelijke in staat stelt te beoordelen of aan de voorwaarden voor verstrekking op grond van artikel 41 van de Algemene Verordening Gegevensbescherming is voldaan.

Het Platform leidt hieruit af dat het min of meer absolute verbod op het verzoeken

om vrijwillige verstrekking van gegevens in de meer eenvoudige gevallen wordt opgeheven.

Met deze bepaling wordt immers, naar het lijkt, de verstrekking van gegevens door met name overheidsorganen ten behoeve van de opsporing ook zonder daartoe strekkende vordering mogelijk gemaakt. Immers, overheidsorganen zijn doorgaans veel beter dan particulieren (zowel burgers als zakelijke gegevensverwerkers) in staat om de juiste afweging als bedoeld in artikel 41 van de Algemene Verordening Gegevensbescherming te maken, terwijl verzoeken tot verstrekking van gegevens aan dergelijke organen ook vaak meer met redenen kunnen worden omkleed. In de samenwerking tussen de verschillende opsporingsinstanties en toezichthoudende diensten is het overigens van belang dat informatie kan worden verkregen zonder dat dit steeds op een wettelijk bevel moet worden gebaseerd. Zo heeft de FIOD momenteel toegang tot informatie van toezichthouders als de Belastingdienst zonder dat daarvoor steeds een wettelijke vordering moet worden gedaan. Het is van belang dat deze mogelijkheid behouden blijft. Mede als gevolg van de mogelijkheid om desgevraagd en mits voldoende gemotiveerd, dus ook zonder een expliciet bevel tot uitlevering, gegevens te verkrijgen zullen de administratieve lasten die het aanvragen en afgeven van dergelijke bevelen met zich meebrengen, afnemen ten opzichte van de huidige praktijk.

In de Aanwijzing opsporingsbevoegdheden[19] van het College van PG's zijn echter nog enkele andere categorieën genoemd[20] waarbij het niet nodig is om de verstrekking van gegevens te vorderen, c.q. om vrijwillige verstrekking als hier bedoeld, te verzoeken:

- Vrijwillige medewerking door een burger (waaronder wordt verstaan: op eigen initiatief of desverzocht door de opsporingsambtenaar);
- Verstrekking van gegevens door een bedrijf of instelling wanneer die gepaard gaat met het doen van een aangifte van een strafbaar feit;
- Vrij opvraagbare gegevens (bijvoorbeeld uit openbare registers of het internet);
- Verkrijging van gegevens op grond van bijzondere wetgeving;
- Vrijwillige verstrekking van gegevens door een bedrijf of instelling, uit eigen beweging en wanneer die gegevens niet vallen onder de bescherming van de AVG.

Het Platform stelt daarom voor om artikel 2.7.3.3.10 met deze andere categorieën uit te breiden, dan wel de formulering van dit artikel zodanig aan te passen dat ook deze andere categorieën onder de werking ervan worden gebracht. In de toelichting op dit artikel kan dan nader worden omschreven wat de reikwijdte van deze bepaling is.

Onderdeel E: Ontoegankelijk maken van gegevens

In Titel 7.4 worden een aantal bepalingen neergelegd die het ontoegankelijk maken en het vernietigen van gegevens regelen. Het betreft hier dan met name gegevens met een illegale inhoud, waarvan het niet wenselijk is dat deze gegevens ongecontroleerd in het maatschappelijke verkeer blijven of daarin terugkeren. Hieronder kunnen ook gegevens worden verstaan met betrekking tot welke of met behulp waarvan het strafbare feit is begaan. De achterliggende gedachte van het ontoegankelijk maken of vernietigen van dit soort gegevens is dat het disproportioneel kan zijn om het beslag op een gegevensdrager

[19] Zoals deze geldt vanaf 1 september 2014, gepubliceerd in *Stcrt.* 2014, 24442.

[20] Zie Aanwijzing opsporingsbevoegdheden par. 2.10 (p. 21).

of geautomatiseerd werk te handhaven omdat er illegale gegevens op zijn aangetroffen, terwijl er daarnaast ook legale gegevens op een apparaat zijn opgeslagen.

Het Platform begrijpt deze achterliggende gedachte op zich heel goed, maar vreest dat deze regeling in de praktijk niet altijd of in voldoende mate uitvoerbaar is. Het is in de praktijk dan ook eerder gebruikelijk dat een beslagene bij de opsporingsinstantie aangeeft welke legale gegevens hij nodig heeft en dat die legale gegevens dan in kopie worden teruggegeven. Het is namelijk niet gegarandeerd dat wanneer illegale gegevens ontoegankelijk gemaakt zijn, die gegevens na teruggave van de gegevensdrager of het geautomatiseerde werk door de beslagene niet weer toegankelijk gemaakt kunnen worden. Verder is het de vraag hoe ontoegankelijk gemaakte gegeven op een later tijdstip en bij een afzonderlijke rechterlijke beslissing kunnen worden vernietigd als bedoeld in artikel 2.7.4.3, wanneer de gegevensdrager of het geautomatiseerde werk in de tussentijd weer is teruggegeven aan beslagene. Vernietiging van de betreffende gegevens zal in dergelijke gevallen dan niet of nauwelijks meer kunnen plaatsvinden.

Het Platform stelt daarom voor in de regeling van Titel 7.4 op te nemen dat een beslagene in voorkomende gevallen bij de opsporing kan verzoeken om een kopie van door hem nader aan te duiden, legale gegevens en eventueel tegen een weigering aan een dergelijk verzoek te voldoen, de mogelijkheid van beklag te openen.

Onderdeel G: Stelselmatig overnemen van gegevens uit publiek toegankelijke bronnen

In artikel 2.8.2.4.1 wordt bepaald dat onder voorwaarden gegevens kunnen worden overgenomen uit publiek toegankelijke bronnen. Hiermee wordt niet alleen het advies van de Commissie-Koops overgenomen, maar komt de wetgever tevens tegemoet aan een wens die verschillende ketenpartners, waaronder het Platform, op dit punt hebben geuit in hun eerdere consultatieadviezen op de conceptvoorstellen inzake Boek 2.

Het platform wijst aanvullend op het grote belang van de fraudebestrijding om ook in de fase vóór de verdenking uit publiek toegankelijke bronnen gegevens te kunnen verzamelen; hierbij valt te denken aan de Panama papers en de Paradise papers. Er kan dan bijvoorbeeld onderzoek worden gedaan op websites van rechtspersonen en socialemediapagina's van rechtspersonen, of op webpagina's van nieuwsmedia, openbare blogs en vlogs die duidelijk bedoeld zijn om gegevens wereldkundig te maken. In eerste instantie zal deze vorm van gegevensvergaring dan ook niet kunnen worden aangemerkt als het stelselmatig overnemen van gegevens uit publiek toegankelijke bronnen zodat een onderzoek als hier bedoeld kan plaatsvinden op basis van de algemene taakstellende artikelen.[21]

Het Platform dringt er daarom op aan om in de toelichting duidelijk te maken dat het verzamelen van gegevens voordat sprake is van een verdenking niet als stelselmatig is aan te merken en derhalve geen bevel van de officier van justitie behoeft.

Het Platform kijkt verder uit naar de in de memorie van toelichting op te nemen factoren die een rol spelen bij het bepalen van de stelselmatigheid van deze bevoegdheid en naar de handvatten die de wetgever beoogt te bieden voor de factoren die voorafgaand aan de inzet van deze bevoegdheid kunnen bepalen of er inderdaad sprake is van stelselmatigheid.

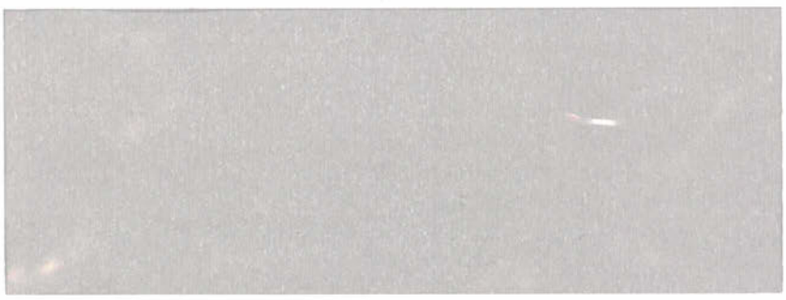
---

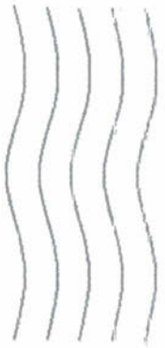
[21] Zie Rapport Commissie Modernisering opsporingsonderzoek in het digitale tijdperk, *Regulering van opsporingsbevoegdheden in een digitale omgeving*, s.l. 2018, p. 157-158.

Onderdeel H: Locatiebepaling ter aanhouding van een persoon
In artikel 2.8.2.10.1 wordt de mogelijkheid gecreëerd om met behulp van een technisch hulpmiddel stelselmatig de locatie van een persoon vast te stellen, ten einde die persoon te kunnen aanhouden of ter uitvoering van een bevoegdheid als bedoeld in de afdelingen 8.2.1 tot en met 8.2.8. Het bevel wordt gegeven voor een periode van maximaal een maand en kan telkens met ten hoogste een maand worden verlengd.

Het Platform onderschrijft de behoefte aan regeling en inzet van deze bevoegdheid en constateert met tevredenheid dat ook deze bepaling voorziet in een behoefte die het Platform in haar consultatieadvies d.d. 26 juni 2017 heeft geuit.

PLATFORM
B.O.D.
BIJZONDERE
OPSPORINGS
DIENSTEN





Gezien scankar-
Jenv

06 NOV. 2018

FMHaaglanden

06 NOV. 2018

Ontvangen