OPENBAAR MINISTERIE

College van procureurs-generaal

Postbus 20305, 2500 EH Den Haag

Prins Clauslaan 16
2595 AJ Den Haag
[redacted]
www.om.nl

Ministerie van Justitie en Veiligheid
Directie Wetgeving
t.a.v mw. [redacted]
Postbus 20301
2500 EH DEN HAAG

Datum 01 november 2018
Onderdeel [redacted]
Ons kenmerk [redacted]
Uw kenmerk [redacted]
Onderwerp Advies onderdeel opsporing in een digitale omgeving modernisering Wetboek van Strafvordering

Bij beantwoording de datum en ons kenmerk vermelden.

Geachte mevrouw [redacted],

Bij brief van 10 oktober 2018 heeft u namens de minister van Justitie en Veiligheid het College van procureurs-generaal gevraagd te adviseren over een nieuw onderdeel van het concept-Boek 2 (Het opsporingsonderzoek) van het nieuwe Wetboek van Strafvordering. Dit onderdeel betreft de opsporing in een digitale omgeving.

In het oorspronkelijk aan de ketenpartners ter advisering voorgelegde conceptwetsvoorstel Boek 2, was een onderdeel opgenomen onder de titel "Inbeslagneming van gegevens". Deze versie stuitte op veel kritiek vanuit de praktijk. Als reactie op deze kritiek heeft de toenmalige minister van Veiligheid en Justitie de Commissie modernisering opsporingsonderzoek in het digitale tijdperk ingesteld, onder voorzitterschap van prof. E.J. Koops. In deze commissie waren vrijwel alle ketenpartners en de wetenschap vertegenwoordigd.

De commissie kreeg als opdracht de minister te adviseren over de vraag of de wettelijke regeling van het opsporingsonderzoek, zoals voorgesteld in het concept-Boek 2, voldoet, dan wel bijstelling of aanvulling behoeft. In het rapport Regulering van opsporingsbevoegdheden in een digitale omgeving[1] analyseert de

[1] Commissie modernisering opsporingsonderzoek in het digitale tijdperk, *Regulering van opsporingsbevoegdheden in een digitale omgeving*, s.l. 2018.

commissie de digitale ontwikkelingen die spelen in opsporingsonderzoeken. Het rapport bevat waardevolle adviezen die beogen de wetgever een handreiking te bieden zodat een wettelijk antwoord kan worden gevonden op de uitdagingen die de digitale samenleving met zich meebrengt voor de opsporing.

Het College heeft met waardering kennisgenomen van het rapport van de commissie-Koops. Tevens stelt het College vast dat een groot aantal aanbevelingen uit het rapport van de commissie zijn verwerkt in het nu voorliggende onderdeel ten behoeve van de opsporing in een digitale omgeving. Er is een goede balans getroffen tussen de rechtsbescherming van burgers en de mogelijkheden voor de opsporing. Hoewel nog niet op alle onderdelen even consequent doorgevoerd - later in het advies wordt hierop teruggekomen - meent het College dat het wetsvoorstel in ruime mate techniekonafhankelijk is opgesteld, zodat ook toekomstige technische ontwikkelingen in het door het commissierapport bestreken nieuwe Wetboek van Strafvordering kunnen worden ondergebracht.

Het College heeft derhalve met instemming van het conceptwetsvoorstel kennisgenomen en is gaarne bereid om daarover te adviseren. Ter wille van de overzichtelijkheid zal het College een advies opstellen, waarbij artikelsgewijs een aantal op- en aanmerkingen worden gemaakt.

Alvorens op de onderscheiden artikelen in te gaan wil het College gaarne de aandacht vestigen op het volgende. De commissie-Koops heeft er op pagina 24 van het rapport op gewezen dat de wisselwerking tussen de normering van de *vergaring* van gegevens en de normering van de *verwerking* van gegevens een belangrijk aandachtspunt is bij de regeling van opsporingsbevoegdheden. Het is noodzakelijk dat de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg), die beiden gaan over de verwerking van gegevens, goed aansluiten op hetgeen met betrekking tot de vergaring van gegevens wordt geregeld in het Wetboek van Strafvordering. Het College dringt erop aan dat tijdig beide eerstgenoemde wetten zullen worden bezien in het licht van de wijzigingen die worden voorgesteld in het kader van de opsporing in een digitale omgeving.

Artikel 2.1.1.1 Definities

In artikel 2.1.1.1 wordt in onderdeel d de definitie van 'communicatie' gewijzigd. Het College merkt op dat deze definitie nog niet in alle bepalingen consequent wordt doorgevoerd. In de laatste versie van het conceptwetsvoorstel tot vaststelling van Boek 2 waar het College over beschikt wordt nog verschillende

keren gesproken over 'telecommunicatie' waar 'communicatie' is bedoeld. Het College adviseert om het wetsvoorstel na te kijken op een consistent gebruik van het begrip 'communicatie'.

In een afzonderlijk kader zijn de voor de Titels 7.3, 7.4, 7.5 en 7.6 relevante definities geformuleerd. Vooralsnog is het de bedoeling dat deze definities niet in de wet, maar in de memorie van toelichting worden opgenomen. Het College kan zich in deze werkwijze vinden, omdat dit meer mogelijkheden biedt voor de rechtsontwikkeling.

Een paar definities in het kader behoeven echter nog enige aanpassing. De onderdelen d en e definiëren het 'stelselmatig onderzoek van gegevens' respectievelijk het 'ingrijpend stelselmatig onderzoek van gegevens'. Onder 'stelselmatig onderzoek van gegevens' wordt verstaan: een onderzoek waarbij op voorhand redelijkerwijs voorzienbaar een min of meer volledig beeld van bepaalde aspecten van iemands privéleven kan ontstaan. Onder 'ingrijpend stelselmatig onderzoek van gegevens' wordt verstaan: een onderzoek waarbij op voorhand redelijkerwijs voorzienbaar een ingrijpend beeld van iemands privéleven kan ontstaan.
In de toelichting op artikel 2.7.3.2.2 wordt een uitvoerige beschouwing gewijd aan het richtinggevende arrest van de Hoge Raad over het onderzoek aan een inbeslaggenomen smartphone.[2] Dit arrest uit april 2017 bevatte een nieuwe koers met betrekking tot het onderzoek aan elektronische gegevensdragers en geautomatiseerde werken. Er wordt een driedeling aangebracht. Als eerste stelt de Hoge Raad dat de algemene bevoegdheid van opsporingsambtenaren, neergelegd in artikel 94 Sv, in verbinding met de artikelen 95 en 96 Sv, voldoende legitimatie biedt voor een onderzoek aan de smartphone indien de met het onderzoek samenhangende inbreuk op de persoonlijke levenssfeer als beperkt kan worden beschouwd. De memorie van toelichting geeft een aantal voorbeelden over de vraag wat als beperkt onderzoek moet worden beschouwd.
Voorts oordeelt de Hoge Raad dat indien dat onderzoek zo verstrekkend is dat een min of meer compleet beeld is verkregen van bepaalde aspecten van het persoonlijk leven van de gebruiker van de gegevensdrager of het geautomatiseerde werk, dat onderzoek jegens hem onrechtmatig kan zijn. Dit tweede onderdeel van de driedeling wordt vertaald naar onderdeel d, het stelselmatig onderzoek van gegevens.
Ten slotte stelt de Hoge Raad in rechtsoverweging 2.8 dat in het licht van artikel 8 EVRM moet worden gewezen op de mogelijkheid dat aan een onderzoek door de rechter-commissaris in het bijzonder valt te denken in gevallen waarin 'op

[2] ECLI:NL:HR:2017:584

voorhand is te voorzien' dat de inbreuk op de persoonlijke levenssfeer zeer ingrijpend zal zijn.
Het College merkt op dat er een belangrijk verschil is ontstaan tussen het arrest van de Hoge Raad en de formulering in het wetsvoorstel. De Hoge Raad zegt heel concreet, dat 'als het onderzoek zo verstrekkend is dat', het onderzoek jegens hem onrechtmatig kan zijn. En in de laatste zin van rechtsoverweging 2.8 heeft de Hoge Raad het over gevallen waarin 'op voorhand is te voorzien' dat de inbreuk op de privacy ingrijpend zal zijn. Het concrete 'zo verstrekkend is' en 'op voorhand is te voorzien' van de Hoge Raad wordt in de definitie omgezet in 'op voorhand *redelijkerwijs* voorzienbaar'. Maar door de toevoeging van het woord 'redelijkerwijs' ontstaat een voor de praktijk wel heel vage formulering. Wanneer is er geen sprake van 'op voorhand redelijkerwijs voorzienbaar'? Het College vreest dat dit in de praktijk voortdurende discussies gaat opleveren omdat hier nooit een afdoende antwoord op is te geven. Het College dringt erop aan dat de formulering van de Hoge Raad in rechtsoverweging 2.8 met betrekking tot het kunnen voorzien van de mate van inbreuk op de persoonlijke levenssfeer wordt overgenomen en adviseert om in de definitie van het stelselmatig onderzoek van gegevens het woord 'redelijkerwijs' te schrappen. Het stelselmatig onderzoek van gegevens wordt alsdan gedefinieerd als een onderzoek waarbij het op voorhand is te voorzien dat een min of meer volledig beeld van bepaalde aspecten van iemands privéleven kan ontstaan.
Hetzelfde geldt voor de definitie van een ingrijpend stelselmatig onderzoek van gegevens. Mede gelet op rechtsoverweging 2.8, waar de Hoge Raad met name de situatie bedoelt waarbij de inbreuk op de persoonlijke levenssfeer zo ingrijpend is dat de rechter-commissaris erbij zou moeten worden betrokken, pleit het College ervoor dat ook in onderdeel e het woord 'redelijkerwijs' wordt geschrapt en het ingrijpend stelselmatig onderzoek van gegevens wordt gedefinieerd als een onderzoek waarbij op voorhand is te voorzien dat een ingrijpend beeld van iemands privéleven kan ontstaan.

Titel 7.3 Onderzoek van gegevens

Artikel 2.7.3.1.1 Notificatie in geval van doorzoeking of betreding

In dit artikel wordt voorgeschreven dat indien tijdens een doorzoeking of betreding gegevens worden overgenomen, in beginsel direct een bewijs van uitoefening van deze bevoegdheid wordt afgegeven of achtergelaten. Deze bepaling komt grotendeels overeen met het voorgestelde artikel 2.7.2.1.4 waarin is bepaald dat bij inbeslagneming van een voorwerp een soortgelijk bewijs wordt afgegeven of achtergelaten. Daarover heeft het College bij gelegenheid van de

consultatie over enkele onderdelen van de modernisering van het Wetboek van Strafvordering bij brief van 24 juli jl. geadviseerd (kenmerk WBOM/17851).

Hoewel het voor de praktijk wat meer werk betekent, kan het College zich vinden in het voorstel dat de verplichting tot het afgeven of achterlaten van een bewijs wordt uitgebreid naar de situatie waarin gegevens worden overgenomen tijdens een betreding. De handeling is immers dezelfde, er worden gegevens gekopieerd, alleen de omstandigheid waaronder dit gebeurt, is anders. Vanuit het perspectief van de rechtsbescherming is het opheffen van deze ongelijkheid alleszins te billijken. De uitbreiding betekent wel dat in meer gevallen dan thans het geval is, een bewijs van uitoefening van deze bevoegdheid zal moeten worden uitgereikt of achtergelaten. Het is immers bepaald niet ondenkbaar dat tijdens een betreding voor de hand liggende gegevens worden overgenomen, bijvoorbeeld door het maken van een foto van een pagina in een opengeslagen ordner.

In het artikel wordt voorgeschreven dat het bewijs 'direct' wordt afgegeven of achtergelaten en dat het bewijs 'de aard' van de overgenomen gegevens bevat. Het College merkt op dat het lang niet altijd mogelijk is om onmiddellijk na het overnemen van de gegevens de aard van de gegevens te omschrijven, omdat de gegevens dan nog niet zijn bekeken, bijvoorbeeld omdat de tijd daarvoor ontbreekt of omdat de gegevens zijn versleuteld. Het College gaat ervan uit dat aan het voorschrift ook wordt voldaan als er in het bewijs van het overnemen van gegevens staat dat gegevens zijn overgenomen die op een bepaalde locatie staan. Het verdient aanbeveling om deze notie in enkele zinnen in de memorie van toelichting op te nemen.

In het derde lid wordt een regeling getroffen voor het uitstellen van het afgeven of het achterlaten van het bewijs dat gegevens zijn overgenomen. De officier van justitie kan, indien het belang van het onderzoek dit dringend vereist, bevelen dat het afgeven of achterlaten van het bewijs wordt uitgesteld. Dit bevel tot uitstel kan alleen worden gehandhaafd na een machtiging van de rechter-commissaris. Deze regeling komt overeen met de regeling voor het uitstel van het bewijs van inbeslagneming van voorwerpen in het voorgestelde artikel 2.7.2.1.3. De bezwaren die het College in zijn hierboven genoemde consultatiebrief naar voren heeft gebracht, zijn onverminderd van kracht op de thans voorliggende conceptregeling. Thans is het zo dat de officier van justitie op de voet van artikel 125m, tweede lid, Sv bij de uitoefening van zijn bevoegdheid tot doorzoeking, zelfstandig bevoegd is te beslissen tot het uitstel van de mededeling dat dat gegevens zijn vastgelegd. Als de doorzoeking door de rechter-commissaris plaatsvindt, is de rechter-commissaris daartoe bevoegd. In de huidige regeling is de beslissing tot uitstel van de notificatie dus voorbehouden aan degene die de

bevoegdheid tot doorzoeking heeft toegepast. Dat zou ook in de nieuwe regeling zo moeten zijn. Naar het oordeel van het College is de beslissing tot het handhaven van het uitstel van het bewijs van het overnemen van gegevens, niet goed los te zien van de beslissing tot het overnemen van de gegevens zelf. De rechter-commissaris zal in de beoordeling over de vraag of het uitstellen van het afgeven van het bewijs van het overnemen van gegevens dient te worden gehandhaafd vrijwel onvermijdelijk treden in de vraag of deze gegevens wel overgenomen hadden mogen worden, of er een voldoende verdenking bestond om deze bevoegdheid uit te oefenen en of het bevel tot uitstel wel gegeven had mogen worden. De rechter-commissaris treedt daarmee in de bevoegdheid van de officier van justitie. Vanuit systematisch oogpunt is de voorgestelde keuze daarom ongelukkig te noemen. Bovendien merkt het College op dat het in de voorgestelde regeling gaat om het overnemen van gegevens, waarbij de gegevens zelf nog steeds ook in de beschikkingsmacht van de rechthebbende blijven. Van een inbreuk op het eigendomsrecht, die de tussenkomst van de rechter-commissaris nog zou kunnen rechtvaardigen, is hier geen sprake. Het College adviseert dan ook om het derde lid van artikel 2.7.3.1.1 aan te passen, in die zin dat daarin tot uitdrukking wordt gebracht dat de officier van justitie het afgeven of achterlaten van het bewijs van ontvangst in het belang van het onderzoek kan uitstellen en dat de rechter-commissaris dezelfde bevoegdheid toekomt indien hij degene is die de bevoegdheid tot doorzoeking heeft toegepast.

Artikel 2.7.3.1.2 Geheimhouding

Op grond van dit artikel zijn bepaalde personen verplicht geheimhouding in acht te nemen over onderdelen van het onderzoek van gegevens. Aan de ene kant wordt de geheimhouding voor medewerkers van bijvoorbeeld een datacenter terecht uitgebreid naar situaties waarbij het onderzoek ter plaatse wordt gedaan. Aan de andere kant wordt de geheimhouding nu beperkt in die zin dat deze niet geldt in de privésfeer. Het College meent dat op deze wijze goed rekening is gehouden met de diverse belangen en heeft met instemming kennisgenomen van deze nieuwe bepaling.

Artikel 2.7.3.2.1 Steunbevoegdheden en doorzoeking op afstand

Dit artikel bepaalt allereerst welke steunbevoegdheden kunnen worden uitgeoefend voor het verrichten van onderzoek van gegevens. Het gaat om bevoegdheden tot het betreden en doorzoeken van plaatsen. Het derde lid betreft een geavanceerde variant van de gebruikelijke doorzoeking, namelijk de doorzoeking op afstand.

Het College heeft met instemming kennisgenomen van de voorgestelde regeling waarbij het mogelijk wordt om ten behoeve van het verrichten van onderzoek van gegevens bij een persoon, met diens toestemming te doorzoeken op afstand. Deze regeling biedt zowel voor de politie als voor de onderzochte persoon voordelen. Zo kan worden voorkomen dat de onderzochte persoon in zijn werk wordt gehinderd doordat het onderzoek niet op de werkvloer, maar vanaf een politielocatie wordt verricht.
Wel vraagt het College zich af of onder een 'persoon' ook een rechtspersoon kan worden begrepen.

Ten slotte een redactionele opmerking. Artikel 2.7.3.2.1 is het eerste artikel waar wordt gesproken over het onderzoek 'van gegevens aan gegevens'. Op pagina 13 van de memorie van toelichting wordt uitgelegd dat voor deze titel van belang is dat 'het onderzoek van gegevens' als een koepelterm moet worden gezien. Daaronder wordt verstaan het geheel aan handelingen dat ten aanzien van gegevens wordt uitgevoerd. Het betreft zowel handelingen aan apparaten waarop gegevens zijn opgeslagen als handelingen aan gegevens. Vandaar, zo vervolgt de memorie van toelichting, dat soms wordt gesproken over het onderzoek *van* gegevens *aan* gegevens.
Het College is niet blij met deze cascade van voorzetsels. (Soms lijkt de formulering te suggereren dat het om twee verschillende soorten of verzamelingen van gegevens gaat: zoiets als onderzoek *van* het hart dat plaatsvindt *aan* de pols.) De meest simpele oplossing van het probleem lijkt een volledige vervanging van het begrip 'onderzoek van gegevens' door de term 'gegevensonderzoek'.

Artikel 2.7.3.2.2 Codificatie van het smartphone-arrest

In dit nieuwe artikel wordt zowel het onderzoek aan digitale gegevensdragers en geautomatiseerde werken als het onderzoek aan digitale gegevens die zijn overgenomen uit een digitale gegevensdrager of een geautomatiseerd werk genormeerd. Met dit artikel wordt de normering met betrekking tot het onderzoek aan inbeslaggenomen elektronische gegevensdragers en geautomatiseerde werken - zoals de Hoge Raad die heeft neergelegd in het eerdergenoemde richtinggevende arrest van april 2017 – gecodificeerd.
Het College heeft met instemming kennisgenomen van de wijze waarop het zogenaamde smartphone-arrest van de Hoge Raad is gecodificeerd. De uiteenzetting in de memorie van toelichting is helder en geeft de praktijk voldoende handvatten waardoor de regeling goed werkbaar zal zijn in de praktijk.
Wel dient naar het oordeel van het College, zoals hiervoor uiteengezet, de definitie van het (ingrijpend) stelselmatig onderzoek van gegevens te worden

ontdaan van het ín deze context onduidelijke 'redelijkerwijs'. Dat is voor de praktijk niet goed werkbaar.

Het derde lid verklaart de normering met betrekking tot het stelselmatig onderzoek van gegevens en ingrijpend stelselmatig onderzoek van gegevens van overeenkomstige toepassing in de gevallen dat analoog vastgelegde gegevens worden omgezet in digitale gegevens en ook indien aan die omgezette digitale gegevens onderzoek wordt verricht. De commissie-Koops heeft deze schakelbepaling aanbevolen.

Het College merkt op dat de commissie-Koops in aanbeveling 24 schrijft dat er een schakelbepaling moet worden ingevoerd die bepaalt dat, waar analoog vastgelegde gegevens waarover een opsporingsinstantie beschikt worden omgezet in digitale gegevens, dezelfde normering geldt voor dit digitaal overnemen van de analoge gegevens als van toepassing is op het overnemen van digitale gegevens. En dat op het verdere onderzoek van aldus gedigitaliseerde gegevens dezelfde normering van toepassing is als op het onderzoek vanuit een geautomatiseerd werk of digitale gegevensdrager overgenomen digitale gegevens.
Echter, de wijze waarop de voorgestelde bepaling is geformuleerd kan mogelijk zodanig worden gelezen dat voor iedere omzetting van ieder analoog vastgelegd gegeven het eerste en tweede lid van toepassing is. Dat zou tot gevolg hebben dat bijvoorbeeld ook in het geval de opsporingsambtenaar slechts een enkele foto maakt van een document (digitalisering) en deze foto vervolgens op het bureau bekijkt (onderzoek aan het digitale gegeven) een bevel van de officier van justitie, eventueel na een daartoe verleende machtiging van de rechter-commissaris, noodzakelijk is. Dat is blijkens pagina 94 van het rapport van de commissie-Koops uitdrukkelijk niet de bedoeling.
Het College dringt erop aan dat het artikel iets anders wordt geformuleerd, zodat duidelijk is dat de bepaling ziet op de situatie dat op voorhand voorzienbaar is dat de omzetting van analoge gegevens naar digitale gegevens een meer dan geringe inbreuk op de persoonlijke levenssfeer oplevert en dat dan het eerste en tweede lid van overeenkomstige toepassing zijn.

Artikel 2.7.3.2.3 Netwerkzoeking

De huidige netwerkzoeking, die is geregeld in artikel 125j Sv, wordt uitgebreid. Artikel 2.7.3.2.3 maakt het mogelijk dat de officier van justitie kan bevelen dat een opsporingsambtenaar gegevens onderzoekt die in een elders aanwezige digitale gegevensdrager of een elders aanwezig geautomatiseerd werk zijn opgeslagen. De netwerkzoeking is dan niet meer beperkt tot de gegevens in een bedrijfsnetwerk, maar betreffen ook gegevens die zijn opgeslagen in de cloud en

via een internetverbinding eenvoudig te benaderen zijn. Met de uitbreiding van de bestaande bevoegdheid komt de wetgever tegemoet aan een in de praktijk sterk levende behoefte. Het College verwelkomt dit artikel dan ook met grote instemming.
De vernieuwde netwerkzoeking zal worden opgenomen in een experiment. Alsdan zal blijken of het artikel in de praktijk voldoet. Het College geeft er de voorkeur aan om de resultaten van het experiment af te wachten alvorens voorstellen tot verbetering te doen.

Artikel 2.7.3.2.5 Onderzoek van gegevens en netwerkzoeking bij aanbieder

In artikel 2.7.3.2.5 staat dat dat indien het bevel dat wordt gegeven bij een stelselmatig onderzoek van gegevens in een digitale gegevensdrager (2.7.3.2.2) dan wel in geval van een onderzoek van gegevens die in een elders aanwezig geautomatiseerd werk zijn opgeslagen (2.7.3.2.3) betrekking heeft op gegevens die in gebruik zijn bij een aanbieder van een communicatiedienst en die klaarblijkelijk betrekking hebben op communicatie die wordt beschermd door het telecommunicatiegeheim, dit bevel door de officier van justitie slechts kan worden gegeven indien het onderzoek dit dringend vereist en na een daartoe verleende machtiging van de rechter-commissaris.
Eenzelfde constructie wordt gebruikt voor artikel 2.7.3.3.5, waar het gaat over de verstrekking van gegevens. De officier van justitie kan, na een daartoe verleende machtiging door de rechter-commissaris, de aanbieder van een communicatie bevelen gegevens te verstrekken die betrekking hebben op communicatie die wordt beschermd door het telecommunicatiegeheim.

Het College vraagt zich af of de impliciete verwijzing naar artikel 13 van de Grondwet (Gw), door het noemen van het telecommunicatiegeheim, een gelukkige keuze is geweest. Helemaal uitgeschreven zou er, overeenkomstig de bedoeling, immers moeten komen te staan "...die wordt beschermd door het telecommunicatiegeheim, als bedoeld in artikel 13 van de Grondwet". Het voorgestelde artikel 2.7.3.2.5 betreft kort samengevat gegevens die zijn opgeslagen bij een aanbieder van een communicatiedienst en die worden beschermd door het telecommunicatiegeheim. Dat veronderstelt dat er ook gegevens zijn die weliswaar zijn opgeslagen op een digitale gegevensdrager bij een aanbieder van een communicatiedienst, maar die niet vallen onder het telecommunicatiegeheim. De vraag is welke gegevens wel en welke gegevens niet worden beschermd door het telecommunicatiegeheim.
Het College merkt op dat er meer grondrechten zijn die, volgens de Grondwet, bij wet kunnen worden beperkt. Zoals bijvoorbeeld de vrijheid van meningsuiting in artikel 7 Gw of het recht op het recht tot vergadering en betoging in artikel 9 Gw.

Maar bij beperkingen op deze grondrechten wordt in andere wetten niet eerst gerefereerd aan het grondrecht zelf. Het recht op de vrijheid van meningsuiting wordt bijvoorbeeld beperkt door de diverse uitingsdelicten in het Wetboek van Strafrecht. De Gemeentewet geeft het bestuur bevoegdheden om het recht tot betoging te beperken. Maar in deze gevallen wordt in de lagere regelgeving niet gerefereerd aan het grondrecht zelf. De beperking op het grondrecht zal zich in de praktijk moeten uitkristalliseren.

Het College adviseert om in de memorie van toelichting expliciet uit te leggen waarom deze bijzondere wijze van formuleren als onvermijdelijk wordt beschouwd.

Artikel 2.7.3.2.6 Nagekomen berichten op een inbeslaggenomen gegevensdrager

Artikel 2.7.3.2.6 betreft de mogelijkheid dat na inbeslagneming nieuwe inhoudelijke gegevens beschikbaar komen op (of via) een digitale gegevensdrager of een geautomatiseerd werk. Artikel 2.7.2.2.6 biedt de mogelijkheid dat een bevel, gegeven op grond van de artikelen 2.7.3.2.2, eerste lid, en 2.7.3.2.3, eerste lid, gedurende een periode van drie dagen na de inbeslagneming tevens strekt tot deze nieuwe, nagekomen gegevens. Deze termijn kan, na verkregen machtiging van de rechter-commissaris, op bevel van de officier van justitie met een maand worden verlengd.

Ook deze bepaling zal worden toegepast in een experiment. Het is binnen de voorgestelde termijnen niet altijd mogelijk om toegang te verkrijgen tot een versleutelde of met een wachtwoord beveiligde gegevensdrager. Bovendien is niet in alle gevallen vast te stellen wanneer de berichten zijn nagekomen, zodat niet kan worden vastgesteld of de berichten na afloop van de geldende termijn zijn binnengekomen of daarvoor. Het College adviseert dat in het experiment goed wordt gekeken of de nu voorgestelde termijnen werkbaar zijn.

Artikel 2.7.3.2.7 Ontsleuteling

Het bevel tot ontsleuteling is bedoeld om toegang te krijgen tot een vergrendeld apparaat of tot versleutelde gegevens die op een digitale gegevensdrager of op een geautomatiseerd werk zijn opgeslagen. Het College heeft met instemming kennis genomen van het feit dat het ontsleutelingsbevel tevens kan worden gegeven om onderzoek mogelijk te maken in een inbeslaggenomen digitale gegevensdrager of geautomatiseerd werk.

Het tweede lid bevat de bevoegdheid voor de officier van justitie om aan de opsporingsambtenaar te bevelen dat hij biometrische beveiliging of versleuteling in de vorm van een vingerafdruk of een opname van de iris of het gezicht, ongedaan maakt. Hiertoe kan de opsporingsambtenaar de redelijkerwijs noodzakelijke maatregelen treffen, ook tegen de wil van de degene die de beveiliging of versleuteling ongedaan kan maken.
De commissie-Koops heeft geconstateerd dat biometrische beveiliging op digitale gegevensdragers en geautomatiseerde werken van verdachten in toenemende mate problemen oplevert. De commissie-Koops voorspelt dat in de toekomst zich allerlei vormen van biometrische beveiliging zullen voordoen. Ondanks de voorspelling van de commissie-Koops dat er in de toerkomst meer vormen van biometrische beveiliging mogelijk worden is er niet voor gekozen om een techniekonafhankelijke bepaling voor te stellen. Volgens de memorie van toelichting omdat niet is te voorzien welke mate van inbreuk op de persoonlijke levenssfeer van de betrokkene dit zou kunnen opleveren en omdat dit aanvullende regelgeving zal vergen.
Het College volgt deze redenering niet en acht het onwenselijk dat niet wordt gekozen voor een techniekonafhankelijke bepaling. Op een gebied waar de ontwikkelingen zo snel gaan, raakt de wetgever per definitie snel op achterstand. De wetgever kan de nieuwe ontwikkelingen enigszins bijhouden door te kiezen voor een techniekonafhankelijke bepaling in de wet en de uitvoering in een relatief sneller te wijzigen AMvB op te nemen. Daarmee is niet gezegd dat daardoor minder rechtsbescherming ontstaat en dat daardoor eerder een inbreuk op de persoonlijke levenssfeer ontstaat. Immers, ook over een AMvB kan het parlement meebeslissen.
Het College adviseert derhalve dringend om de voorgestelde regeling techniekonafhankelijk op te stellen en de uitvoering later in AMvB's op te nemen.

Artikel 2.7.3.3.3 Bevel verstrekken gegevens

Artikel 2.7.3.3.3, derde lid, geeft de opsporingsambtenaar de bevoegdheid een bevel te geven tot de verstrekking van een aantal met name genoemde categorieën van gegevens. In onderdeel e wordt genoemd "beeldmateriaal gemaakt voor de beveiliging van goederen, gebouwen of personen.".
Tegenwoordig wordt echter in toenemende mate niet meer wordt volstaan met het vastleggen van beeldmateriaal als het gaat om de beveiliging, ook wordt gebruik gemaakt van andere technieken, zoals geluid en bewegings- en temperatuursensors. Het College geeft in overweging om, teneinde de technische ontwikkeling bij te kunnen houden, het woord "beeldmateriaal" te vervangen door "vervaardigde gegevens". De zin zou alsdan kunnen luiden: "voor de beveiliging van goederen, gebouwen of personen vervaardigde gegevens."

Artikel 2.7.4.1 Ontoegankelijk making en vernietiging van gegevens

In dit artikel is de bevoegdheid voor de officier van justitie opgenomen om gegevens die bij een onderzoek van gegevens zijn aangetroffen in een digitale gegevensdrager of in een geautomatiseerd werk en met betrekking tot welke of met behulp waarvan het strafbare feit is begaan, ontoegankelijk te maken, voor zover die ontoegankelijkmaking noodzakelijk is ter beëindiging van het strafbare feit of ter voorkoming van nieuwe strafbare feiten. De ontoegankelijkmaking van gegevens na inbeslagneming betreft een verruiming van de huidige regeling.

Het College merkt op dat de toelichting op dit artikel te weinig aandacht besteedt aan het feit dat het in de praktijk in veel gevallen onwenselijk is om gegevensdragers met ontoegankelijk gemaakte gegevens te retourneren aan de eigenaar. Het komt regelmatig voor dat de gegevensdrager versleutelde gegevens bevat, die vermoedelijk strafbaar zijn, maar waar de politie niet bij kan. Ook komt het voor dat strafbare gegevens op een zodanige wijze technisch (steganografisch) zijn verstopt in niet strafbare gegevens (zoals de foto's van dierbaren) dat deze voor de opsporing nauwelijks of niet vindbaar zijn. Het teruggeven van de gegevensdrager, ook als deze ontoegankelijk gemaakte gegevens bevat, is daarom in veel gevallen niet wenselijk.
In dit verband wijst het College ook naar pagina 53 van de conceptmemorie van toelichting bij Boek 6, waar helder uiteen wordt gezet waarom gegevensdragers, waar bijvoorbeeld kinderporno of lijsten met creditcardnummers zijn aangetroffen, niet worden teruggegeven aan de eigenaar. In de memorie van toelichting op Boek 6 staat: "Theoretisch is het denkbaar dat een digitaal compleet geschoonde gegevensdrager wordt teruggegeven (na het maken van een forensische kopie; *image*), maar dan gaan de inbeslaggenomen gegevens dus niet retour. Het retourneren van een deels geschoonde gegevensdrager – dus alle gegevensbestanden buiten bijvoorbeeld de geconstateerde kinderporno of creditcardgegevens – is risicovol en zou veel vergen van de opsporingsdiensten. Dan zou immers per bestand moeten worden bezien of het veilig is om terug te geven terwijl bekend is dat bestanden in andere – bijvoorbeeld fotobestanden – kunnen zijn verborgen. Vanwege de professionele versleuteling van dergelijke verborgen bestanden is technisch gezien niet uit te sluiten dat in de geretourneerde gegevensbestanden nog meer strafbaar materiaal aanwezig is, wat volstrekt onwenselijk is."
Dezelfde problemen die zich voordoen bij het retourneren van geschoonde gegevensdragers doen zich voor bij het eventueel retourneren van een gegevensdrager die gegevens bevat die ontoegankelijk zijn gemaakt. De memorie van toelichting op de ontoegankelijkmaking van gegevens mag niet onbedoeld de

indruk wekken dat gegevensdragers met ontoegankelijk gemaakte gegevens in veel gevallen wel kunnen worden geretourneerd. Daarom adviseert het College om in de memorie van toelichting ook bij de ontoegankelijkmaking van gegevens deze problemen expliciet te benoemen.
Het College verwijst in dit verband voorts naar pagina 32 van zijn advies over Boek 6,[3] waar voorstellen worden gedaan voor een voor de praktijk werkbare procedure.

Afdeling 8.2.4 Stelselmatig overnemen van persoonsgegevens uit publiek toegankelijk bronnen

Bij de heimelijke bevoegdheid in Afdeling 8.2.4 en het verkennend onderzoek (artikel 2.9.1) is een aantal wijzigingen doorgevoerd naar aanleiding van het rapport van de commissie-Koops. Voorgesteld wordt een aantal begrippen rond het stelselmatig aan te passen. De nieuwe formulering luidt: 'stelselmatig, al dan niet op geautomatiseerde wijze, persoonsgegevens uit publiek toegankelijke bronnen overnemen', in plaats van 'stelmatig met een technisch hulpmiddel gegevens betreffende een persoon uit open bronnen vast te leggen'.
De nieuwe formulering is een verbetering en daarnaast is de keuze voor 'publiek toegankelijke bronnen' voorzien van een goede toelichting. Het gaat hier om bronnen waartoe toegang wordt verkregen zonder een beveiliging te doorbreken of omzeilen en zonder het aanwenden van technische ingrepen, valse signalen of valse sleutels, of het aannemen van een valse hoedanigheid. Het College heeft nog wel een opmerking over het begrip 'valse hoedanigheid'. Ook bij het onderzoeken van publiek toegankelijke bronnen en het overnemen van (persoons)gegevens in het kader van een verkennend onderzoek zal de opsporingsinstantie wel met een afgeschermd ip-adres moeten kunnen werken. In de memorie van toelichting moet worden opgenomen dat dit uitdrukkelijk niet onder een 'valse hoedanigheid' kan worden begrepen.

Ten slotte vraagt het College aandacht voor het bij AMvB kunnen stellen van eisen aan de geautomatiseerde wijze van 'overnemen' van de gegevens, met het oog op de integriteit en de authenticiteit van de overgenomen 'resultaten' In het derde lid van artikel 2.8.2.4.1, is opgenomen dat bij of krachtens AMvB regels worden gesteld over de geautomatiseerde wijze van overnemen van gegevens.
In de memorie van toelichting wordt hierover gezegd dat de factoren die een rol spelen bij het bepalen van 'stelselmatigheid' in de digitale omgeving op een rij zullen worden gezet. Zo worden explicieter handvatten geboden voor de factoren die voorafgaand aan de inzet van de bevoegdheid kunnen bepalen of wel of geen

[3] Advies College van procureurs-generaal, 11 juli 2018, kenmerk WBOM/17862

sprake is van stelselmatige inzet *(voor zover het uiteraard om persoonsgegevens gaat).*
Een punt van zorg hierbij is dat die handvatten of factoren *(bij of krachtens de AMvB)* enerzijds wel voldoende houvast moeten geven bij de beoordeling, maar niet te beperkend moeten zijn. Verder is het de vraag of hier het begrip stelselmatig een andere betekenis/invulling kan krijgen dan bijv. bij stelselmatige observatie, waar niet bij of krachtens AMvB nadere invulling aan dat begrip wordt gegeven.

Hoogachtend,

[redacted]

Procureur-generaal