Regulering van opsporingsbevoegdheden in een digitale omgeving

Commissie modernisering opsporingsonderzoek in het digitale tijdperk

juni 2018

Aanbevolen citeerwijze: Commissie modernisering opsporingsonderzoek in het digitale tijdperk, *Regulering van opsporingsbevoegdheden in een digitale omgeving*, s.l. 2018.

Inhoudsopgave

Afkortingen

AI	Artificial Intelligence
AMvB	Algemene maatregel van bestuur
ANPR	*Automatic Number Plate Recognition*, automatische kentekenplaatherkenning
AVG	Algemene verordening gegevensbescherming
BOB	Bijzondere opsporingsbevoegdheid
CCIII	Wet(svoorstel) computercriminaliteit III
CVC	Card Verification Code
EHJ	Europese Hof van Justitie
EHRM	Europees Hof voor de Rechten van de Mens
EVRM	Het Europees Verdrag tot bescherming van de Rechten van de Mens en de Fundamentele Vrijheden
FIOD	Fiscale Inlichtingen- en Opsporingsdienst
Gw	Grondwet
IoT	*Internet of Things*, internet der dingen
IP	Internet Protocol
IMSI	International Mobile Subscriber Identity, uniek identificatienummer verbonden aan een gebruiker van een mobiele telefoon
J&V	Justitie & Veiligheid
NAW	Naam, adres, woonplaats
NFC	*Near Field Communication*, draadloze communicatiemethode die onder andere wordt gebruikt voor draadloze betalingen
NFI	Nederlands Forensisch Instituut
OM	Openbaar Ministerie
OSINT	Open-Source Intelligence
PW 2012	Politiewet 2012
r-c	rechter-commissaris
RFID	*Radio-frequency identification*, identificatie met radiogolven
Sr	Wetboek van Strafrecht
Sv	Wetboek van Strafvordering
Tw	Telecommunicatiewet
URL	*Uniform Resource Locator*, padverwijzing naar een bron op het internet.
Wbp	Wet bescherming persoonsgegevens
WED	Wet op de economische delicten
Wet RO	Wet op de rechterlijke organisatie
Wjsg	Wet justitiële en strafvorderlijke gegevens
Wpg	Wet politiegegevens
WRR	Wetenschappelijke Raad voor het Regeringsbeleid

1. Inleiding

1.1. Achtergrond

Het huidige Wetboek van Strafvordering kwam in 1926 tot stand, na een parlementaire voorgeschiedenis van 12 jaar. Hoewel veel van de beginselen die de memorie van toelichting van 1914 verwoordt onverminderd gelden, heeft het wetboek de daaropvolgende eeuw velerlei aanpassingen en reparaties ondergaan vanwege maatschappelijke en technische ontwikkelingen en politieke wensen.[1] De overzichtelijkheid is er daarbij niet altijd beter op geworden. De huidige wetgever acht het raadzaam om het wetboek integraal bij de tijd te brengen. Het gaat daarbij niet om een herziening, maar om een modernisering: het systeem en de terminologie worden geordend, de rechtsontwikkeling wordt gecodificeerd en gestreefd wordt naar een wetboek dat weer geruime tijd meekan.

Daarbij benoemt de memorie van toelichting veranderende technologie als een van de hoofdthema's van de moderniseringsoperatie.[2] Nieuwe technische mogelijkheden hebben geleid tot een reeks van strafvorderlijke bevoegdheden die onvoldoende systematische samenhang hebben met het systeem van bestaande bevoegdheden. De aanpassing van de wet loopt dan ook regelmatig achter bij de snelle technische ontwikkelingen, met name op het vlak van informatie- en communicatietechnologie. Het moderniseringsvoorstel probeert in dat licht een deel van de opgelopen achterstand in te halen.

De technische ontwikkelingen zijn van belang voor diverse onderdelen van het strafprocesrecht. Het meest duidelijk komt dat naar voren in de regeling van opsporingsbevoegdheden, aangezien de opsporingsinstanties steeds meer moeten opereren in een digitale context. Bij de modernisering van de regeling van opsporingsbevoegdheden, die zijn weerslag heeft gekregen in een conceptwetsvoorstel tot vaststelling van Boek 2 van het nieuwe Wetboek van Strafvordering (hierna: conceptwetsvoorstel), is het een substantiële uitdaging om niet alleen de opgelopen achterstand in te halen, maar ook vooruit te kijken en een regeling te treffen die in staat is de voorzienbare technologische ontwikkelingen in de komende tijd op te vangen.

In het voortraject dat heeft geleid tot de totstandkoming van het conceptwetsvoorstel is uitgebreid overleg gevoerd met partijen uit de praktijk, om te zorgen voor een actuele, houdbare en werkbare regeling. Desondanks heeft het uiteindelijke in februari 2017 voor consultatie gepubliceerde conceptwetsvoorstel van verschillende kanten kritiek gekregen. Dat betrof zowel kritiek op meer conceptuele aspecten ("beslag" op gegevens, de bevoegdheidstoedeling) als praktische bezwaren tegen bepaalde artikelen of het ontbreken daarvan. Kort na de publicatie van de consultatieversie, in april 2017, gaf de Hoge Raad bovendien in het langverwachte "smartphone-arrest"[3] een suggestie voor normering van het onderzoek in smartphones bij aanhouding, die over het algemeen (met name op het punt van de bevoegdheidstoedeling) gunstiger werd ontvangen dan de in het conceptwetsvoorstel opgenomen regeling daaromtrent.

Een en ander vormde aanleiding tot een meer fundamentele bezinning op de regeling van het opsporingsonderzoek in een digitale context, in de vorm van het instellen van een Commissie modernisering opsporingsonderzoek in het digitale tijdperk.

---

[1] Memorie van toelichting bij het conceptwetsvoorstel tot vaststelling van Boek 1 van het nieuwe Wetboek van Strafvordering (consultatieversie), p. 4.

[2] Memorie van toelichting bij het conceptwetsvoorstel Boek 1 (consultatieversie), p. 14.

[3] HR 4 april 2017, ECLI:NL:HR:2017:584. Het gaat overigens om drie op dezelfde dag gewezen arresten (eveneens ECLI:NL:HR:2017:588 en ECLI:NL:HR:2017:592), die echter alle dezelfde algemene overwegingen bevatten ten aanzien van het onderzoek in smartphones in het kader van inbeslagneming bij aanhouding. Om die reden wordt meestal alleen verwezen naar het eerste arrest en wordt, ook in dit rapport, gemakshalve gesproken van "het" smartphone-arrest.

1.2. Opdracht, samenstelling en proces van de commissie

1.2.1. Opdracht

De commissie is ingesteld op verzoek van de Directie Wetgeving en Juridische Zaken van het Ministerie van Justitie en Veiligheid (destijds nog het Ministerie van Veiligheid en Justitie). Bij Besluit van de toenmalige Minister van Veiligheid en Justitie is de commissie officieel ingesteld.[4] De commissie is in eerste instantie ingesteld voor de periode van 1 juni 2017 tot 1 januari 2018. Bij besluit van de Minister van Justitie en Veiligheid en de Minister voor Rechtsbescherming van 18 december 2017[5] is deze periode verlengd tot 1 mei 2018. Tevens zijn er in dit besluit enkele nieuwe leden benoemd.

De commissie heeft tot taak de minister te adviseren over de vraag of de wettelijke regeling van het opsporingsonderzoek, zoals neergelegd in het conceptwetsvoorstel Boek 2, voldoet, of bijstelling dan wel aanvulling behoeft in het licht van de volgende vragen:

1. In verband met de toenemende digitalisering van de criminaliteit en de uitdagingen waaraan de opsporing de komende decennia het hoofd moet bieden, heeft de opsporing behoefte aan een wettelijk kader dat snelle, wendbare opsporing mogelijk maakt, vooral in digitale omgevingen. Is het "pakket" van bevoegdheden in Boek 2, waaronder de nieuwe bevoegdheden uit het wetsvoorstel Computercriminaliteit III, voldoende toekomstbestendig met het oog op de technologische ontwikkelingen, die (ook) voor de opsporing van de (cyber)criminaliteit kunnen worden gebruikt? Deze vraag impliceert niet alleen een analyse van, en eventuele aanpassingsvoorstellen voor, het voorgestelde "pakket" van bevoegdheden vanuit het perspectief van digitale ontwikkelingen, maar ook een reflectie op de vraag of de klassieke manier van normeren in het strafprocesrecht flexibel genoeg is om nieuwe fenomenen in de (cyber)criminaliteit aan te pakken of nieuwe technologieën in te passen, en de vraag of nieuwe legislatieve instrumenten nodig zijn en zo ja, op welke wijze daarbij de eisen van een integere opsporing en conformiteit met de grond- en mensenrechten kunnen worden gewaarborgd.

2. Digitaal opgeslagen gegevens zijn een belangrijke bron voor de opsporing. Deze gegevens vallen onder de regeling van Hoofdstuk 7 (bevoegdheden betreffende voorwerpen en gegevens) van het nieuwe Boek 2. Nieuw is het voorstel om ook te spreken over de inbeslagneming van gegevens (zie de Titels 7.3, 7.4 en 7.5). De commissie heeft tot taak om te onderzoeken in hoeverre de voorgestelde definitie en regeling van beslag op gegevens werkbaar en toereikend zijn en zo neen welke alternatieven (beter) zijn.

3. Een van de nieuwe onderwerpen in Hoofdstuk 7 is de normering van het onderzoek aan elektronische gegevensdragers en geautomatiseerde werken. Voorgesteld wordt dit onderzoek (ter inbeslagneming van de gegevens of ter kennisneming van de gegevens) altijd met een bevel van de officier van justitie te laten plaatsvinden. Op 4 april heeft de Hoge Raad een arrest gewezen over deze problematiek (HR 4 april 2017, ECLI:NL:HR:2017:584, hierna: het smartphone-arrest). De Hoge Raad maakt een onderscheid tussen vormen van onderzoek aan elektronische gegevensdragers en geautomatiseerde werken naar gelang de mate van inbreuk op de privacy die het onderzoek maakt. In hoeverre geeft het arrest van de Hoge Raad aanleiding om het voorstel aan te passen?

1.2.2. Samenstelling

Voorzitter van de commissie is prof. E.J. (Bert-Jaap) Koops. Het Ministerie van Justitie en Veiligheid, het Openbaar Ministerie (hierna: OM), de zittende magistratuur, de Nederlandse Orde van Advocaten, de Politie, de Bijzondere opsporingsdiensten en de wetenschap zijn vertegenwoordigd in de commissie. De volledige samenstelling van de commissie is opgenomen in Bijlage I.

[4] Staatscourant 12 juli 2017, nr. 39081.
[5] Staatscourant 28 december 2017, nr. 73969.

1.2.3. Proces

In de periode 1 juli 2017 tot en met 1 mei 2018 is de commissie elf keer bij elkaar gekomen voor een reguliere vergadering van 2 tot 2,5 uur. Tijdens de eerste vergadering heeft de commissie gezamenlijke uitgangspunten vastgesteld. Ook heeft de commissie aan de hand van de opdracht een Landkaart probleemvelden opgesteld. In deze Landkaart werden de belangrijkste problemen en knelpunten binnen de opdracht van de commissie geïnventariseerd, geclusterd en geprioriteerd. Voor de geprioriteerde knelpunten hebben de leden van de commissie deelnotities opgesteld die gedurende de vergaderingen van de commissie zijn besproken.

Naast de reguliere vergaderingen heeft de commissie ook twee expertsessies georganiseerd. Op 12 oktober 2017 werd een sessie georganiseerd over de vraag in welke gevallen het onderzoek aan een digitale-gegevensdrager of geautomatiseerd werk een meer dan geringe dan wel zeer ingrijpende inbreuk op de persoonlijke levenssfeer van betrokkenen oplevert. Naast enkele leden van de commissie waren daar ook experts van de politie en het OM bij aanwezig. Op 24 november 2017 is een expertsessie "Opsporing en toekomstige technologie" gehouden. De kernvraag op deze middag luidde: "Hoe ziet de wereld er in 2027 en 2040 uit en wat betekent dat voor de regeling van de opsporing van strafbare feiten?" Ook bij deze expertsessie waren leden van de commissie aanwezig, evenals diverse experts vanuit de wetenschap en de opsporing. De inzichten uit de discussies tijdens beide expertsessie zijn gebruikt in het rapport.

Tot slot is de commissie op 1 en 2 maart 2018 bij elkaar gekomen in Rotterdam voor een tweedaagse bijeenkomst waarbij een eerste concept van dit rapport is besproken en resterende onderwerpen aan de orde zijn geweest.

1.3. Uitgangspunten en aard van het advies

De commissie heeft bij het begin van haar werk enkele uitgangspunten vastgesteld. Doel van deze uitgangspunten was om houvast te bieden bij het afbakenen van de opdracht en discussies richting te geven. De uitgangspunten zijn opgenomen in Bijlage II.

Voor een goed begrip van de aard van het advies is het zinvol hier enkele uitgangspunten nader toe te lichten. De eerste drie uitgangspunten zien op het treffen van een goede balans tussen abstractie en specificiteit. De regeling van opsporing in het gemoderniseerde Wetboek van Strafvordering moet zo simpel zijn als mogelijk, en zo complex als nodig. Technologie-onafhankelijkheid is geen doel op zich: de regeling van opsporing moet zo technologie-onafhankelijk zijn als mogelijk (in verband met duurzaamheid), maar moet ook zo technologie-specifiek zijn als nodig (in verband met rechtszekerheid). Dit betekent volgens de commissie dat de regeling van opsporing in hoge mate technologie-onafhankelijk moet zijn qua leidende concepten en systematiek, maar technologie-specifiek mag (en soms moet) zijn in de regeling van bepaalde concrete bevoegdheden.

In het verlengde hiervan heeft de commissie zich geconcentreerd op de systematiek van de regeling in de Hoofdstukken 7 en 8 van het conceptwetsvoorstel, qua structuur, concepten en manier van regelen, evenals op de invulling van relevante details die sterk samenhangen met deze systematiek. De adviezen bevatten dan ook soms concrete tekstvoorstellen (bijvoorbeeld ten aanzien van definities), maar geven veelal meer algemeen een benadering aan die nog uitwerking behoeft in concrete wetteksten of in de memorie van toelichting. Het is binnen het gegeven tijdpad onmogelijk voor de commissie om concreet, tekst-gericht wetgevingsadvies te geven; dat ziet de commissie ook niet als haar primaire taak. Belangrijker is dat het advies conceptuele helderheid biedt en handvatten bevat voor aanpassing van het wettelijk stelsel langs de lijnen die de commissie aanbeveelt; de uitwerking daarvan kan vervolgens door daartoe toegeruste gremia worden opgepakt.

Bij het streven naar toekomstbestendigheid van het wetboek heeft de commissie een horizon gehanteerd van tien tot vijftien jaar vanaf nu, oftewel rond 2030. Dat lijkt wellicht lang, maar is relatief kort ten opzichte van de wenselijke periode van houdbaarheid van het gemoder-

niseerde wetboek. Indien het gemoderniseerde wetboek, naar het zich laat aanzien, op zijn vroegst in 2023 of 2024 in werking zal treden, en aannemend dat de wenselijke houdbaarheid (in elk geval qua systematiek en gehanteerde concepten) bij inwerkingtreding toch zeker zo'n tien à vijftien jaar zal zijn, zou een horizon van 2040 eerder voor de hand liggen. Hoewel de commissie aanvankelijk ook een dergelijke horizon voor ogen had, heeft zij deze in de loop van haar discussies losgelaten. Gezien de dynamiek van technologische ontwikkelingen is nauwelijks te overzien hoe de wereld er over ruim twintig jaar uit zal zien, mede gezien het feit dat moeilijk is te voorspellen welke technische ontwikkelingen een brede maatschappelijke adoptie zullen krijgen en welke uitwerking dat heeft op de maatschappij. Met de kennis van nu kunnen we wel stellen dat een commissie die in 1995 een opdracht zou hebben gekregen een toekomstbestendige regeling voor digitale opsporing te ontwerpen, de nodige moeite zou hebben gehad om een wettelijke regeling voor te stellen die qua systematiek anno 2018 nog bij de tijd zou zijn. Een horizon van 2030 acht de commissie al ambitieus genoeg; voor deze periode kunnen wel enigszins onderbouwde uitspraken worden gedaan over de grote lijnen van voorzienbare ontwikkelingen – in elk geval welke tendensen zich naar verwachting voordoen en voortzetten (vgl. hfd. 2). Daarbij beseft de commissie dat ook binnen deze periode zich al uiteenlopende onvoorziene technische ontwikkelingen kunnen voordoen die op onderdelen tot meer of minder ingrijpende wijziging van de regeling van opsporingsbevoegdheden nopen.

Binnen deze horizon waren vragen 2 en 3 van de opdracht relatief goed beantwoordbaar. Vraag 1 over het totale pakket van bevoegdheden is echter aanzienlijk complexer. De wens dat de voorgestelde regeling langere tijd mee kan, in de zin dat de gehanteerde systematiek robuust genoeg is om toekomstige ontwikkelingen met relatief overzienbare actualiseringsslagen op te vangen, is voorstelbaar, maar ook erg ambitieus. Daarbij komt dat het antwoord op vragen 2 en 3 een weerslag heeft op vraag 1, in die zin dat de gekozen uitgangspunten voor normering van het overnemen van (opgeslagen) gegevens en het onderzoek aan geautomatiseerde werken en digitale-gegevensdragers verenigbaar moeten zijn, en liefst moeten samenvallen, met de uitgangspunten voor normering van andere bevoegdheden waarmee digitale gegevens kunnen worden vergaard en onderzocht. Juist dit laatste betreft een breed scala aan bevoegdheden, die op verschillende manier geraakt kunnen worden door toekomstige technologische ontwikkelingen. Dit betekent dat de opdracht van de commissie breed en complex is, en niet volledig te vervullen is binnen de relatief korte periode die zij tot haar beschikking heeft gehad. De commissie verwijst in dat verband ook nadrukkelijk op de beperkingen in het advies die hieronder (par. 1.4 en hfd. 0) worden toegelicht.

Verder heeft de commissie als uitgangspunt gehanteerd te streven naar consensus, maar niet te werken met compromissen die leiden tot vage voorstellen. Gezien de samenstelling van de commissie is consensus over alle onderwerpen niet mogelijk, behalve waar het wetstechnische of puur conceptuele vraagstukken betreft. De commissie bestaat immers uit vertegenwoordigers van verschillende organisaties, die deels tegenstrijdige belangen vertegenwoordigen en soms ook uiteenlopende visies op de opsporing hebben. Op het vlak van normering is consensus niet mogelijk, in de zin dat er geen voldoende heldere voorstellen te formuleren zijn waar alle commissieleden zich, mede met het oog op het draagvlak bij de eigen organisatie, onverkort achter kunnen scharen. Gekozen is daarom voor voorstellen die gebaseerd zijn op de discussies in de commissie en de daarbij uitgewisselde argumenten, waarbij de voorzitter ernaar gestreefd heeft een redelijke middenweg te bewandelen gelet op de uiteenlopende belangen en visies die in de discussies naar voren zijn gekomen. Op de belangrijkste punten waar binnen een deel van de commissie substantiële bezwaren of twijfels bestonden bij een voorstel, is dat in het rapport aangegeven, zodat de wetgever dit kan meewegen bij de verwerking van de voorstellen. De betrokken organisaties houden daarbij de mogelijkheid open om, mede naar aanleiding van uit te voeren effectonderzoek, in het verdere wetgevingstraject hun eigen visie op onderdelen voor het voetlicht te brengen.

1.4. Beperkingen

De commissie is zich bewust van significante beperkingen in haar rapport. Voor een deel betreft dit fundamentele beperkingen in verband met de reikwijdte van de opdracht, die de aard van het advies beïnvloeden; deze worden zelfstandig behandeld in hoofdstuk 0 vanwege het belang van een goed begrip van deze beperkingen voor de besluitvorming over het verdere wetgevingstraject. Daarnaast zijn er onderwerpen die wel binnen de opdracht van de commissie vallen en die de commissie van belang acht om te adresseren in het wetgevingstraject, maar waar zij in de vergunde tijd niet aan toe is gekomen. Bepaalde onderwerpen uit de Landkaart bleken te complex om voldoende uit te werken binnen de looptijd van de commissie. Dit betreft bijvoorbeeld vraagstukken rond opsporing door burgers en rond grootschalig niet-persoonsgericht onderzoek, dat wil zeggen (veelal ongericht) onderzoek waarbij gegevens van veel mensen in enige mate worden verwerkt maar dat ten aanzien van elk individu geen of slechts een beperkte privacyinbreuk oplevert.[6] Ook een gedegen analyse van de mogelijke langeretermijngevolgen voor de opsporing van de ontwikkelingen in bijvoorbeeld neurotechnologie, robotica en autonome systemen bleek binnen het bestek van dit rapport niet mogelijk; op dergelijke ontwikkelingen wordt slechts incidenteel ingegaan. Naast de beperkingen in reikwijdte qua opdracht en behandelde onderwerpen, heeft de tijdsdruk waaronder dit rapport tot stand is gekomen ook tot gevolg dat enkele onderwerpen wel zijn behandeld, maar niet op detailniveau konden worden uitgewerkt, zodat de desbetreffende behandeling en aanbevelingen een relatief algemeen karakter houden.

[6] Aan dit onderwerp is wel aandacht besteed in de specifieke context van het overnemen van gegevens uit publiek toegankelijke bronnen, in het bijzonder in relatie tot crawlers (zie par. 6.4.3 onder “De inzet van crawlers”), maar niet in algemene zin.

2. Achtergrond: schets van het digitale landschap

In dit hoofdstuk wordt het digitale landschap geschetst, zowel voor wat betreft de huidige stand van zaken en met name de ontwikkelingen daarin die relevant zijn voor de opsporing (par. 2.1) als voor wat betreft de belangrijkste toekomstige ontwikkelingen, voor zover deze op dit moment te overzien zijn (par. 2.2). Het overzicht is allerminst volledig, schetst slechts grove contouren van het digitale landschap en is (zeker voor de technisch onderlegde lezer) in de beknoptheid wat kort door de bocht geformuleerd; de doelstelling van dit hoofdstuk is ook niet een wetenschappelijk onderbouwd overzicht van technologische ontwikkelingen te bieden, maar vooral de minder technisch georiënteerde lezer enig houvast te bieden voor de techno-sociale context waarin de juridische analyses en adviezen in de volgende hoofdstukken moeten worden geplaatst.

2.1. Het digitale landschap anno 2018

2.1.1. Inleiding

Technische ontwikkelingen beïnvloeden de samenleving, en daarmee ook de opsporing. Dit gebeurt bijvoorbeeld op de navolgende wijzen.

- De apparaten die gebruikt worden door burgers en bedrijven worden ook gebruikt door verdachten, en komen zo binnen als “digitaal beslag” of bieden nieuwe uitdagingen op het gebied van interceptie (opnemen communicatie).
- Nieuwe technieken zijn (in het begin) vaak niet goed beveiligd, daarnaast weten mensen nog niet goed hoe ermee om te gaan. Dit biedt mogelijkheden voor nieuwe business-modellen voor criminaliteit.
- Nieuwe technieken kunnen strafbare feiten en verdachten detecteren of gegevens vastleggen (die dan mogelijk te vorderen of anderszins te verkrijgen zijn).
- De opsporingsdiensten kunnen de nieuwe technieken zelf gebruiken (als detectiemiddel, maar ook als analysemethode). Daardoor kan bij toepassing van bestaande bevoegdheden ook de impact van deze toepassing veranderen.
- Nieuwe technieken kunnen ook gebruikt worden om opsporing te detecteren (sensoren, camera’s, detectieapps) of opzettelijk te belemmeren (versleuteling, verplaatsen naar een land zonder rechtshulprelatie).

In deze paragraaf benoemen we (zonder een uitputtend overzicht te geven) relevante technische ontwikkelingen die momenteel een belangrijke invloed hebben op (digitale) opsporing.

2.1.2. Digitalisering en beschikbaarheid van gegevens

Een eerste ontwikkeling betreft in algemene zin de digitalisering die het dagelijks leven doormaakt en de daarmee gepaard gaande toename in vastlegging en hergebruik van gegevens. In vroeger tijden werden de meeste fysieke gedragingen of gedachtenuitingen niet vastgelegd op een wijze die ze voor latere één-op-één reproductie of voor velerlei hergebruik geschikt maakte. Dat is met de komst van sensoren zoals camera’s en het geautomatiseerd monitoren van Internetgebruik (bijvoorbeeld via cookies) veranderd. Gedragingen van personen wordt in steeds toenemende mate digitaal vastgelegd en kunnen mede daardoor ook steeds gemakkelijker uitgewisseld of gereproduceerd worden. Sommige gedragingen spelen zich zelfs uitsluitend af in het digitale domein, en niet meer in het fysieke. Deze ontwikkeling wordt versterkt door de steeds grotere beschikbaarheid van persoonlijke apparatuur die op elk moment van de dag een grote diversiteit aan gegevens kan vastleggen of verwerken; foto’s, aantekeningen, communicatie met anderen, locatiegegevens, internetgegevens, aankopen, interesses, lichamelijke gegevens – de mogelijkheden zijn feitelijk onbegrensd.

De beschikbaarheid van deze gegevens heeft een grote invloed op de opsporing, omdat ieder gegeven potentieel relevant kan zijn voor de opsporing. In algemene zin richt de opsporing zich dus in toenemende mate op het ontsluiten van dergelijke relevante gegevens. Dit stuit op diverse problemen, waarvan verschillende aspecten hierna verder worden uitgewerkt.

2.1.3. Encryptie en beveiliging

In toenemende mate gebruiken consumentproducten standaard-encryptie. Wat vroeger alleen weggelegd was voor overheden en grote bedrijven, is nu een beveiliging die iedere burger gebruikt. In veel gevallen is de versleuteling of andere afscherming zelfs niet door de gebruiker uit te schakelen.

Een eerste voorbeeld is het toegenomen gebruik van dataversleuteling. Er zijn verschillende producten beschikbaar (al dan niet betaald) waarmee alle data op een laptop of desktop schijf volledig worden versleuteld. Gecombineerd met een goed, lang wachtwoord kan de schijf niet door een derde ontgrendeld worden. Dit levert bijvoorbeeld een probleem op in kinderporno- en computervredebreukonderzoeken.

Met de komst van de smartphone vindt communicatie steeds minder in spraak en steeds meer in tekst en beelden plaats. Deze tekst en foto's worden uitgewisseld via een veelheid aan platforms (WhatsApp, Facebook Messenger, Skype, Signal, Telegram, enz.). Vrijwel al deze platforms leveren tegenwoordig diensten waarbij de data in transit volledig versleuteld zijn. Gecombineerd met de moeite en kennis die het kost om uit een datastroom de oorspronkelijke communicatie te reconstrueren en de kennis die nodig is om te interpreteren wat dat dan betekent, heeft dit ertoe geleid dat het tappen van dit soort communicatie de afgelopen jaren steeds minder succesvol is geworden.[7] Ook al heeft een onderzoek de hoogste prioriteit, allerlei communicatie van en naar verdachten vindt plaats zonder dat de opsporingsdienst er kennis van kan nemen.

De smartphone heeft er ook voor gezorgd dat gegevens die mensen graag privé willen houden, beschikbaar zijn geworden op een apparaat dat ze overal meenemen. Dat gaf een eerste druk op de aanbieders van smartphones om toestellen beter te beveiligen, onder meer door de inhoud standaard te versleutelen. Elke nieuwe versie heeft betere beveiliging, omdat dit inmiddels onderdeel van het bedrijfsmodel is geworden. Het is daardoor steeds moeilijker om gegevens aanwezig in een smartphone inzichtelijk te maken voor de opsporing.

2.1.4. Verbindingen

Een tweede probleem als het gaat om interceptie is dat je met smartphones en andere functioneel vergelijkbare apparaten via allerlei verbindingen het internet op kan. Dat betekent dat een data-tap op een mobiele aansluiting niets onderschept als de gebruiker overstapt op wifi. Als dat het wifinetwerk van de woning van de verdachte is, kan daar ook een tap op aangevraagd worden, maar er zijn legio mogelijkheden voor gebruikers om een andere verbinding te kiezen. Denk aan restaurants, tankstations of wifi-hotspots van providers.

Als iemand zijn internetverkeer echt geheim wil houden kan hij een moeilijk te achterhalen fysieke verbinding kiezen, maar ook gebruik maken van een Virtual Private Network (VPN-verbinding). Al het verkeer wordt dan door een versleutelde tunnel geleid, waardoor het tappen van de verbinding bij de telecomaanbieder geen inhoud, maar ook geen metadata meer oplevert.

2.1.5. Publiek toegankelijke bronnen

De afgelopen jaren is het aantal internetgebruikers dat informatie op internet plaatst of over wie informatie op internet wordt geplaatst enorm toegenomen. Dit leidt tot een toename van de vindbaarheid van subjecten en informatie. Helemaal omdat het internet niet makkelijk vergeet zal de historie op het World Wide Web alleen maar verder uitdijen. Afhankelijk van de

[7] Odinot e.a. 2012.

doelstelling van het platform schermt de beheerder zijn platform in voorkomende gevallen echter steeds beter af. Met name jongeren denken steeds beter na over wie ze wel of niet toegang willen geven tot hun gegevens, waardoor er binnen die leeftijdsgroep relatief steeds minder onbewust openbaar wordt gezet.

Overigens leidt de toename van communicatie online mogelijk ook tot een afname van communicatie in de publieke ruimte. Dit maakt het werk van de wijkagent bijvoorbeeld lastiger. Om te weten wat er speelt moet hij (herkenbaar) toetreden tot een online gemeenschap waarin ook allerlei gesprekken plaatsvinden waar hij liever niet van zou weten. Dat leidt tot wrijving en is lastig met beleid op te lossen.

2.1.6. Dataverzameling door derden

Een aantal grote, vooral Amerikaanse, bedrijven is in staat gebleken een groot gedeelte van de wereldbevolking te binden aan haar producten. Die producten moeten goed afgestemd zijn op de behoeften van haar gebruikers om populair te blijven (bijvoorbeeld Apple, Samsung). Daarnaast moet vaak ook voorzien worden in de behoeften van adverteerders om advertentie-inkomsten te kunnen genereren (bijvoorbeeld Google, Facebook). Voor beide doelen is het belangrijk om heel veel data over apparaten en haar gebruikers te vergaren, te analyseren en eventueel te bewaren. Bijna alle partijen verzamelen informatie over de locatie van het gebruikte apparaat (en daarmee ook van de gebruiker), de instellingen (bijvoorbeeld de taal), het appgebruik, contactinformatie en informatie die helpt bij het samenstellen van belangstellingsprofielen.

De opsporing kan maar heel weinig gebruik maken van de informatie die voorhanden is bij deze bedrijven. Gegevens die door de bedrijven worden aangeduid als “niet-inhoudelijke” gegevens kunnen in sommige gevallen worden verkregen zonder rechtshulpverzoek. Onder “niet-inhoudelijk” valt bijvoorbeeld een creditcardnummer dat een Google-account houder heeft geregistreerd of de laatst gebruikte (Nederlandse) IP-adressen van een Facebook-gebruiker. Zo’n bevraging dient vaak ter identificatie van de beheerder van een account.

Alle overige gegevens worden door de bedrijven aangeduid als “inhoudelijk” en worden in het algemeen alleen verstrekt na een rechtshulpverzoek. De vraag of deze “content” communicatie bevat, is daarbij niet relevant. De inhoud van een biografie op Facebook, foto’s, locatiegegevens van een apparaat – het is allemaal inhoud. Gezien de doorlooptijd van rechtshulpverzoeken (regelmatig minimaal zes maanden, soms meer dan een jaar), de hoge eisen die regelmatig worden gesteld (je moet zo specifiek de vraag stellen dat je eigenlijk al zou moeten weten wat het antwoord is) en de geringe hoeveelheid, gefilterde, informatie die de bedrijven leveren, is dat voor de meeste onderzoeken de investering niet waard.

Daarnaast gelden voor communicatie en inhoud op de netwerken van grote internationale aanbieders de regels van die aanbieders, die kunnen afwijken van de Nederlandse wetgeving en ook niet altijd inzichtelijk zijn voor de Nederlandse overheid.

2.1.7. De “cloud”

De afgelopen jaren werden dataopslag en -transport goedkoper en kwam de technologie beschikbaar voor virtualisatie en gedistribueerde opslag. Daarmee werd “de cloud” een consumentenproduct. De instellingen van een toestel kunnen online worden opgeslagen, foto’s en video’s, e-mails, chats, agenda en eventueel een volledige reservekopie ook. De gebruiker van het apparaat weet niet (meer) wat op het apparaat staat en wat alleen in de cloud is opgeslagen. Zolang zijn internetverbinding werkt, is er voor de gebruiker eigenlijk geen verschil.

Voor de opsporing betekent deze ontwikkeling dat zelfs als de smartphone kan worden geopend, de informatie die echt van belang is steeds vaker niet op het toestel zelf staat, maar alleen beschikbaar is in de cloud-opslag. Het zelfstandig achterhalen van deze gegevens is, juridisch gezien, vaak niet mogelijk omdat de data zich misschien in een buitenlands deel van de cloud bevinden.

Een ander gevolg van deze ontwikkeling is dat het ontoegankelijk maken van bepaalde informatie door middel van beslag op een apparaat niet goed meer werkt. Zo kan een verdachte zijn strafbare gedragingen thans eenvoudig voortzetten door een nieuw toestel te verbinden met de cloud en de daarin aanwezige gegevens weer te gebruiken.

De opsporing moet er bij een doorzoeking ook rekening mee houden dat anderen dan de verdachte mogelijk toegang hebben tot diens gegevens die zijn opgeslagen in de cloud en deze snel zouden kunnen verwijderen voordat ze kunnen worden overgenomen.

2.1.8. Sensoren

Sensoren zijn elektronische detectoren, vaak te zien als een verlengstuk van de menselijke zintuigen. Ze worden steeds belangrijker omdat elektronica almaar kleiner, mobieler, beter en goedkoper wordt. Een belangrijke categorie sensoren zijn beveiligingscamera's, die een voorname bron van opsporingsinformatie en daadwerkelijk bewijs vormen. Er worden steeds meer camera's geïnstalleerd, met name door consumenten, ook in de vorm van bijvoorbeeld dashcams. Je zou zelfs de smartphonecamera's die burgers op straat gebruiken onder dit begrip kunnen vangen. Een relatief nieuw fenomeen op dat gebied is de bodycam: een camera die door de politie op straat gedragen wordt en opnames kan maken van de interacties die de agent heeft.

De data die de sensoren genereren kunnen worden vastgelegd. In combinatie met slimme software kunnen er conclusies worden getrokken over de waarneming van de sensor, wat voor de opsporing bruikbare informatie kan opleveren. Denk aan geluiddetectie of het waarnemen van verboden stoffen. Deze technologieën zijn nog in ontwikkeling.

2.1.9. Cryptovaluta

Dankzij de soms exorbitante koersstijgingen voelen meer mensen zich aangetrokken tot het "investeren in" cryptovaluta. Waar het voorheen eigenlijk alleen technisch onderlegde mensen waren, soms met een crimineel doel, kun je nu op nagenoeg elke consumenten-pc en smartphone een bitcoin-*wallet* aantreffen. In opsporingsonderzoeken zijn cryptovaluta met name van belang bij (cyber)afpersing, *dark market*-handel en witwasonderzoeken. Enerzijds bieden ze extra pseudonimiteit, anderzijds kan veel informatie worden achterhaald uit analyses omdat alle transacties openbaar zijn. In toenemende mate zijn partijen zich daarvan bewust en pogen zij die analyse te frustreren.

De commissie merkt in relatie tot cryptovaluta op dat zij aanvankelijk het onderwerp van beslag op elektronisch geld (zoals cryptovaluta) op de Landkaart probleemvelden had geagendeerd, maar dat bij discussie binnen de commissie op dit punt geen knelpunten leken te bestaan. Daarom wordt aan dit onderwerp in de rest van dit rapport geen bijzondere aandacht besteed in relatie tot de regulering van opsporingsbevoegdheden.

2.1.10. *Anti-forensics* en manipulatie

Zoals de politie steeds nieuwe opsporingsmethodes bedenkt en ontwikkelt, zo zijn ook misdadigers bezig met de bescherming van hun activiteiten, bijvoorbeeld door het beveiligen van hun omgeving. Op digitaal gebied kan daarbij gedacht worden aan beveiligingssystemen, signaalverstoring en encryptie, en het gebruik van camera's of afluistersystemen ter beveiliging van locaties of auto's. Maar ook een crimineel netwerk met een WhatsApp-groep kan heel snel een waarschuwing verspreiden dat er een inval gaande of aanstaande is. Om de toegang tot hun gegevens te beschermen kunnen ze gebruik maken van genoemde versleuteling en veilige verbindingen.

De politie moet een in beslag genomen geautomatiseerd werk onmiddellijk van verbindingen ontdoen, omdat verdachten een wiscommando kunnen toesturen. Ook moet de politie de camera en microfoon van het apparaat afplakken om te voorkomen dat er opnames van de digitaal rechercheur worden gemaakt. Met een toestel waarvan de gebruiker de beveiliging van het

besturingssysteem deels onklaar heeft gemaakt, kunnen allerlei trucjes zijn uitgehaald die de opsporing kunnen dwarsbomen.

Het is voor opsporingsfunctionarissen, net als voor het overige publiek, steeds lastiger geen sporen achter te laten waardoor werk en privé gelinkt kunnen worden of anoniem (zonder politie-sporen) gegevens op internet te benaderen. De grote aanbieders worden er steeds beter in gebruikers te identificeren, ook als ze niet of met een ander account zijn ingelogd. Dit levert risico's op voor het opsporingsonderzoek, de opsporingsfunctionaris persoonlijk of voor getuigen of slachtoffers die niet openbaar willen maken dat zij contact hebben met de politie.

Nieuwe technieken zijn online beschikbaar, waarmee (bewegend) beeld en audio kunnen worden gemanipuleerd op een manier die nauwelijks van echt te onderscheiden is. Dit kan bepaalde strafbare feiten faciliteren (denk aan CEO-fraude waarbij medewerkers een opdracht tot betaling denken te krijgen van hun baas of afpersing met nep-porno) maar het kan ook dienen om bewijs te construeren waarmee de opsporing wordt gemanipuleerd.

2.1.11. Geautomatiseerde dataverwerking en -analyse

De digitale opsporing heeft de afgelopen jaren een aanzienlijke groei doorgemaakt, in aandacht, prioriteit, aantal medewerkers, kennisniveau en voorzieningen. Een vanuit het oogpunt van professionalisering belangrijke toekomstige ontwikkeling zit in het centraliseren van de opslag van digitaal onderzoeksmateriaal. Dit zal zorgen voor een hoog niveau van beschikbaarheid, integriteit en beveiliging. Toegang tot data zal dan niet meer afhankelijk zijn van medewerking van de digitaal specialist bij de politie maar wordt geregeld in een centraal autorisatiesysteem.

Het door het NFI ontwikkelde platform Hansken wordt steeds meer gebruikt om inbeslaggenomen gegevensdragers en de daarop aanwezige gegevens (verder te noemen: het digitaal beslag) te beheren en inzichtelijk te maken.[8]

Met de centrale opslag en verwerking van digitaal beslag, wordt het eenvoudiger om expert-kennis te delen en beschikbaar te maken voor de rechercheurs. Dit kan gaan om het labelen van domeinnamen in internethistorie (financiële pagina, nieuwswebsite, kinderpornoforum) maar ook om het herkennen van objecten op foto's (IS-vlaggen, wapens, enz.).

Door dergelijke grootschalige digitale opslag en geautomatiseerde doorzoekingsmogelijk-heden worden nieuwe vragen opgeworpen. Waar in het verleden de diepgang en omvang van het onderzoek naar de data van een in beslag genomen smartphone impliciet werd gereguleerd door de schaarse kennis en het vele handwerk die ervoor nodig waren, wordt een onderzoek naar eenvoudig te interpreteren data steeds vaker "een druk op de knop". Dat noopt tot expliciet maken van proportionaliteitseisen in concrete richtlijnen voor digitaal onderzoek.

Daarnaast zorgt centralisatie ervoor dat er in de onderzoeksdata van een heel onderzoek of meerdere onderzoeken tegelijk kan worden gezocht. Het biedt ook de mogelijkheid om het ver-werken van digitaal beslag centraal te reguleren volgens de Wet politiegegevens (hierna: Wpg).

2.2. Voorzienbare grote ontwikkelingen in het toekomstige digitale landschap

2.2.1. Inleiding

De verwachting is dat de komende jaren digitale technologieën zich onverminderd snel zullen blijven ontwikkelen. Dalende kosten van rekenkracht, opslagcapaciteit en connectiviteit, miniaturisering en nieuwe innovaties drijven deze ontwikkeling.

Hoewel een breed scala aan digitale technologieën en toepassingen de opsporing gaat beïn-vloeden, ziet de commissie met name de in deze paragraaf beschreven digitale technologieën als van wezenlijke invloed. Voor een groot deel van deze technologieën geldt dat zij reeds nu een effect hebben op onze maatschappij en dat de invloed ervan in de komende jaren alleen

[8] Zie https://www.forensischinstituut.nl/forensisch-onderzoek/hansken (laatst geraadpleegd 1 juni 2018).

maar toeneemt (denk bijvoorbeeld aan grootschalige gegevensverwerking, kunstmatige intelligentie en *cloud computing*), voor een aantal geldt dat zij zich nog in het experimentele of zelfs conceptuele stadium bevinden en de invloed op onze maatschappij vermoedelijk pas over (enkele) jaren voelbaar en duidelijk wordt (quantumcomputers, mens-machine interfaces, *mixed reality*).

Bij het bespreken van deze technologieën is het van belang om in het oog te houden dat het geen op zichzelf staande technologieën zijn, maar dat zij elkaar beïnvloeden, versterken en doorgaans in samenhang gebruikt worden. Naast de kruisbestuiving tussen digitale technologieën is er ook interactie met andere technologieën. Bijvoorbeeld nanotechnologie, biotechnologie, informatietechnologie en de cognitieve wetenschappen (samen afgekort als NBIC) beïnvloeden elkaar. Tegen deze achtergrond moeten de hieronder beschreven technologieën en ontwikkelingen worden gezien.

2.2.2. Digitale technologieën en toepassingen relevant voor de opsporing

Grootschalige gegevensverwerking

Grootschalige gegevensverwerking, ook wel aangeduid met termen als *data mining* en *big data* is nu reeds van wezenlijk belang voor de opsporing. Er is steeds meer ruwe data beschikbaar (zowel inhoudelijke data als metadata) die gebruikt kan worden om de waarheid aan het licht te brengen. De uitdaging is om deze data, waarvan de omvang te groot is geworden om op traditionele wijze te verwerken, op een zinvolle manier te analyseren en op te werken tot bruikbare informatie en kennis voor de opsporing. Door ontwikkelingen op het gebied van data-analysetechnologie en kunstmatige intelligentie is de politie steeds beter in staat om deze uitdaging het hoofd te bieden. In dit kader wordt ook wel gesproken over de informatiegestuurde opsporing.[9]

Cloud computing

Cloud computing en aanverwante toepassingen zoals *software as a service* blijven in de toekomst naar verwachting onverminderd relevant. Vanuit het perspectief van de opsporing is het met name relevant dat interacties tussen gebruikers in toenemende mate gemedieerd en gefaciliteerd worden door derde partijen en de locatie waar gegevens zich bevinden niet altijd eenduidig is vast te stellen.

Het "Internet van Alles"

Het Internet is ontstaan als een netwerk van netwerken dat primair computers met elkaar verbond. Inmiddels zijn het niet enkel computers meer die met elkaar verbonden zijn, maar allerlei apparaten variërend van auto's tot koelkasten. Naast het "Internet der Dingen" (*Internet of Things*) ontstaat er door draagbare apparaten (*wearables*) en implantaten langzamerhand ook een "Internet der Mensen" (*Internet of People*). De volgende stap is dat al deze apparaten en mensen naadloos op elkaar aansluiten en met elkaar samenwerken waardoor en er een "Internet van Alles" (*Internet of Everything*) ontstaat. Naast interconnectiviteit spelen ook sensoren en mens-machine-interfaces een belangrijke rol in deze ontwikkeling. Voor de opsporing is met name relevant dat al deze verbonden apparaten en sensoren data genereren en daarmee sporen bevatten die voor de opsporing potentieel relevant zijn.

Kunstmatige intelligentie

Hoewel "sterke" kunstmatige intelligentie (ook wel *general artificial intelligence* genoemd) nog ver in de toekomst lijkt te liggen, worden op het gebied van kunstmatige intelligentie (ook

[9] Voor een overzicht zie De Vries 2017.

vaak aangeduid als *artificial intelligence*, AI) momenteel grote stappen gezet; denk bijvoorbeeld aan *machine learning*. Diverse toepassingen van kunstmatige intelligentie zijn voor de opsporing in de komende jaren relevant. Hierbij kunnen we grofweg een onderscheid maken tussen kunstmatige intelligentie als het voorwerp van een onderzoek en kunstmatige intelligentie als middel binnen de opsporing.

Kunstmatige intelligentie kan in het private domein voor allerlei toepassingen gebruikt worden. De gegevensverwerking die daarbij plaatsvindt, kan relevant zijn voor de opsporing wanneer er een strafbaar feit is gepleegd waarbij de inzet van kunstmatige intelligentie (mogelijk) een rol heeft gespeeld, bijvoorbeeld bij koersmanipulatie of een verkeersdelict met een zelfrijdende auto. Dan is er sprake van kunstmatige intelligentie als *voorwerp van onderzoek*. Het gaat dan met name over de vraag hoe beslissingen tot stand zijn gekomen. Ook de gegevens die door AI-systemen worden verwerkt kunnen relevant zijn voor de opsporing.

Kunstmatige intelligentie kan op allerlei manieren *als middel* binnen een strafrechtelijk onderzoek gebruikt worden. Allereerst kan gedacht worden aan de toepassing van kunstmatige intelligentie voor het zoeken en verzamelen van gegevens. Een voorbeeld hiervan is de inzet van zelflerende crawlers om het internet af te zoeken. Ten tweede kan gedacht worden aan het geautomatiseerd analyseren van grote hoeveelheden gegevens om tot nieuwe inzichten te komen (bijvoorbeeld via *machine learning*). Binnen deze categorie kunnen wij ook algoritmische besluitvorming vatten: het geautomatiseerd nemen van besluiten betreffende de opsporing.

Verder in de toekomst kan kunstmatige intelligentie waarschijnlijk ook (volledig) autonoom worden ingezet binnen de opsporing. Een rudimentaire vorm hiervan is al zichtbaar bij de (private) inzet van *Sweetie*, de chatbot die wordt ingezet om geautomatiseerd mensen op te sporen die zoeken naar seksuele contacten met minderjarigen via de webcam.[10]

Robotisering

Richting de toekomst valt een steeds verdergaande robotisering van de samenleving te voorzien. Deze ontwikkeling wordt momenteel primair beschouwd vanuit economisch perspectief (denk aan arbeidsmarktvraagstukken en aansprakelijkheid), maar ook voor de opsporing zijn robots relevant. Vanuit strafrechtelijk en strafvorderlijk perspectief zijn robots primair relevant daar waar zij door personen of organisaties worden ingezet voor criminele doeleinden. Vanuit strafvorderlijk perspectief zijn robots op verschillende manieren relevant. Allereerst kunnen de gegevens die een robot verwerkt relevant zijn voor de waarheidsvinding. Voorts is de vraag wie voor het handelen van een robot verantwoordelijk is van belang.

Distributed ledger-technologie (Blockchain)

Distributed ledger-technologie is een databanktechnologie waarbij meerdere kopieën van dezelfde databank verspreid worden over verschillende knooppunten in een netwerk. Door middel van een consensus-algoritme worden wijzigingen in de databanken geverifieerd. Hierdoor ontstaat er één versie van de waarheid die vastgelegd is op verschillende plekken. Het grote voordeel is dat er geen centrale autoriteit nodig is die de databank beheert en daarmee ook de volledige controle over de inhoud heeft. *Blockchain*-technologie is het bekendste voorbeeld van een *distributed ledger*.

Vanuit strafrechtelijk en strafvorderlijk perspectief is *distributed ledger*-technologie nu nog met name relevant omdat het heeft geleid tot de ontwikkeling van cryptovaluta zoals Bitcoin en Ethereum. In de toekomst zal *distributed ledger*-technologie mogelijk op een breder gebied relevant zijn. Een aldus veranderend ecosysteem voor betalingen en andere transacties is ook

[10] Zie https://www.terredeshommes.nl/programmas/sweetie-20-webcamseks-met-kinderen-de-wereld-uit (laatst geraadpleegd 1 juni 2018).

relevant voor de opsporing, omdat daardoor het belang van traditionele centrale spelers zoals banken afneemt en transacties anoniemer worden.

Het verdwijnen van vertrouwde en aanspreekbare partijen betekent ook dat enige behoedzaamheid raadzaam is ten aanzien van data afkomstig uit dergelijke *ledgers*. Niet alleen kunnen in de toekomst zwakheden in de onderliggende technologie worden gevonden die maken dat de informatie gemanipuleerd zou kunnen worden; ook heeft het consensusmodel als nadeel dat een partij met een (al dan niet geheime) meerderheid de daarin vervatte informatie kan wijzigen.[11]

Virtual, augmented en mixed reality

Virtual reality, *augmented reality* en *mixed reality* zijn benamingen voor toepassingen waarmee met behulp van informatietechnologie de perceptie van gebruikers (visueel, maar ook auditief en zelfs qua reuk) wordt aangepast. In de meeste gevallen wordt hiervoor momenteel een bril (al dan niet met geïntegreerde koptelefoon) gebruikt die het gezichtsveld van de gebruiker aanpast. In de toekomst zijn ook andere technieken mogelijk om een virtueel beeld over het reële gezichtsveld te projecteren.

In het bijzonder zijn *augmented reality* en *mixed reality* relevant vanuit strafvorderlijk perspectief omdat zij het beeld van de werkelijkheid voor de gebruiker, en daarmee de perceptie van de werkelijkheid die de basis vormt voor het handelen van een individu, veranderen. In dit kader wordt al gesproken over de "dood van de realiteit".[12] Vanuit strafvorderlijk perspectief is het dan met name de vraag of en zo ja hoe in het onderzoek het "beeld" dat een verdachte, slachtoffer of getuige had van een misdrijfsituatie gereconstrueerd kan worden en hoe die verschillende beelden zich tot elkaar, en "de" werkelijkheid, verhouden.

Mens-machine-interfaces en menselijke "augmentatie"

In de toekomst zullen digitale technologieën steeds verder integreren met het menselijk lichaam. Bekende voorbeelden van technologieën in het menselijk lichaam die al (grootschalig) worden toegepast zijn cochleair implantaten (geïmplanteerde gehoorapparaten), *pacemakers* en diepe hersenstimulatoren. Ook RFID-chips kunnen al lange tijd worden geïmplanteerd. Bij technologieën die aan het menselijk lichaam verbonden zijn valt te denken aan prothesen zoals kunstarmen en -benen. De meeste van deze apparaten hebben één specifieke functie die niet direct wordt aangestuurd door de hersenen zelf. De volgende stap in de ontwikkeling zijn mens-machine-interfaces waarmee wij met behulp van onze hersenen direct implantaten en prothesen kunnen aansturen. Hierbij kan bijvoorbeeld gedacht worden aan armen of benen die met behulp van onze hersensignalen worden bestuurd.[13] Dit opent ook de weg voor menselijke "augmentatie": het vrijwillig vervangen van bijvoorbeeld ledematen door sterkere kunstmatige varianten, of zintuigen als zicht, gehoor, geur en smaak door kunstmatige zintuigen. Deze implantaten en prothesen kunnen waardevolle informatie voor de opsporing bevatten. Denk bijvoorbeeld aan een cochleair implantaat met een opslagfunctie: het kan zeer interessant zijn voor de opsporing om toegang te krijgen tot de opgeslagen audio-gegevens. Daadwerkelijke mens-machine-interfaces waarbij sprake is van een directe uitwisseling van informatie tussen het apparaat en onze hersenen bieden de opsporing nog meer mogelijkheden, maar roepen ook fundamentele vragen op over de grenzen van de opsporing.

[11] https://medium.com/@homakov/how-to-destroy-bitcoin-with-51-pocked-guide-for-governments-83d9bdf2ef6b (laatst geraadpleegd 1 juni 2018).
[12] Zie B. Crecente (2017), Magic Leap: Founder of Secretive Start-Up Unveils Mixed-Reality Goggles, https://www.rollingstone.com/glixel/features/lightwear-introducing-magic-leaps-mixed-reality-goggles-w514479 (laatst geraadpleegd 1 juni 2018).
[13] Hotson e.a. 2016.

DNA en synthetische biologie

DNA is een informatiedrager. Informatie uit het menselijk DNA kan wel worden afgelezen maar van oudsher niet of nauwelijks worden beschreven; met de ontwikkeling van Clustered Regularly Interspaced Short Palindromic Repeats (CRISPR) is het wel mogelijk geworden om specifieke aanpassingen in (menselijk of dierlijk) DNA te doen.[14] Dat zal belangrijke gevolgen hebben voor (onder andere) het materiële strafrecht; de consequenties voor de opsporing zijn op dit moment nog moeilijk te bepalen.

Wel voorzienbaar relevant voor de opsporing is synthetische biologie, waarbij synthetisch DNA of andere soortgelijke moleculen kunnen worden gebruikt om informatie in op te slaan en vervolgens weer uit te lezen. Hoewel praktische toepassingen nog ver weg lijken, kan de toekomstige opslag van grote hoeveelheden gegevens in synthetisch DNA vanuit de opsporing wel praktische vragen opwerpen (bijvoorbeeld hoe dergelijk materiaal te vinden als het zich bevindt in reageerbuisjes of mogelijk ook is ingebracht in het menselijk lichaam), alsook juridische vragen (hoe een dergelijke informatiedrager moet worden gekwalificeerd en onder welke voorwaarden gegevens eruit mogen worden onderzocht).

Biometrie

Naar verwachting zal de toepassing van biometrie steeds relevanter worden voor de opsporing. Hierbij kan gedacht worden aan toepassingen van gezichtsherkenning, maar ook het herkennen van bijvoorbeeld unieke looppatronen (*gait recognition*) of zelfs lichaamsgeur (*scent biometrics*).

Quantumcomputers

De huidige generatie computers is gebaseerd op binaire gegevensverwerking. Bij quantumcomputers wordt gebruikt gemaakt van de specifieke eigenschappen van de quantummechanica om berekeningen uit te voeren. Dit maakt de parallelle berekening van alle mogelijke oplossingen voor een probleem mogelijk. Voor specifieke taken betekent dit dat taken bijna oneindig veel sneller kunnen worden uitgevoerd dan met de huidige generatie computers. De consequenties hiervan voor de maatschappij in het algemeen en het strafrecht in het bijzonder zijn nog niet goed te overzien.

Een vraagstuk dat in de context van quantumcomputatie al wel zichtbaar is, is het effect van quantumcomputatie op encryptie. Zo wordt het met behulp van quantumcomputers mogelijk om de huidige generatie encryptieprotocollen, die nu verondersteld worden "onkraakbaar" te zijn, eenvoudig te breken. Afhankelijk van de schaal en snelheid van deze ontwikkeling, heeft dit gevolgen zowel voor de criminaliteit (toename in bijvoorbeeld fraude en andere vormen van computercriminaliteit) als voor de opsporing (mogelijk meer toegang tot versleutelde gegevens).

Daarnaast betekent de ontwikkeling van quantumcryptografie dat door het zogenaamde "waarnemerseffect" het traditionele afluisteren onmogelijk wordt.[15] Het waarnemerseffect is een fenomeen in de quantummechanica waarbij het enkele observeren van iets, de staat ervan verandert. Dit betekent dat partijen altijd weten wanneer er meegekeken of geluisterd wordt, hetgeen vanuit het perspectief van de toepassing van heimelijke bevoegdheden natuurlijk onwenselijk is.

[14] Zie https://nl.wikipedia.org/wiki/CRISPR (laatst geraadpleegd 1 juni 2018).
[15] Zie Seshu 2008.

2.2.3. Belangrijke techno-sociale tendensen relevant voor de opsporing[16]

Technologische turbulentie

De Commissie Grondrechten in het Digitale Tijdperk (Commissie-Franken) constateerde reeds in 2000 dat door de snelle ontwikkeling van digitale technologieën er een permanente situatie van "technologische turbulentie" bestaat.[17] Het tempo waarmee technologieën en toepassingen elkaar opvolgen maakt het voor de wetgever lastig om deze ontwikkelingen te reguleren en ze te vatten in heldere wettelijke kaders. Sinds het werk van de Commissie-Franken is de turbulentie alleen maar toegenomen. Dit maakt niet alleen het voorspellen van de maatschappelijke effecten van nieuwe technologieën en toepassingen moeilijk, maar ook eventuele beschouwingen op de toekomstbestendigheid van het strafvorderlijk kader.

Veranderende actoren en rolverdelingen

Digitale technologie zorgt ervoor dat nieuwe maatschappelijke actoren ontstaan en dat de rollen van bestaande actoren veranderen. Veel van ons handelen in de digitale wereld wordt mogelijk gemaakt door platformen en diensten van derden (denk aan sociale media). Niet alleen is een groot deel van de digitale infrastructuur in handen van (buitenlandse) private actoren, ook liggen de meeste data en de kennis over technologieën en toepassingen bij hen. Hierdoor spelen zij in de opsporing een relevante rol. Niet alleen als lijdend voorwerp waar bijvoorbeeld gegevens kunnen worden gevorderd, maar ook als partijen die actief bij kunnen dragen aan (proactieve) opsporing. Een ander voorbeeld van veranderende rolverdelingen is het feit dat burgers een steeds actievere rol krijgen bij politiewerk. Burgers weten door ingebouwde beveiliging waar hun gestolen smartphone is, vinden zelf hun gestolen inboedel op een online marktplaats of identificeren een oplichter via sociale media. Soms gaat het zelfs zo ver dat een burger zich een dekmantel aanmeet of een mogelijke verdachte met geweld bedreigt. Door WhatsApp-groepen, camerasystemen en andere sensoren organiseren buurten hun eigen surveillance. Dit leidt tot allerlei juridische maar ook politieke vraagstukken.

Decentralisatie

Hoewel het huidige model van internetgebruik primair gekenschetst kan worden als een gecentraliseerd client-server-model, zijn er ook sterke tendensen tot decentralisatie zichtbaar (denk onder andere aan *peer-to-peer* netwerken, persoonlijke datakluizen en *distributed ledger*-technologie). Wanneer gegevensopslag en -verwerking gedecentraliseerd zijn, is er geen centraal aanspreekpunt meer voor de opsporing als het gaat om bijvoorbeeld het vorderen van gegevens. Dit bemoeilijkt het effectief uitoefenen van opsporingsbevoegdheden.

Internationalisering

Internationalisering speelt al heel lang een rol in de opsporing. Ontwikkelingen als *cloud computing* en het "Internet van Alles" dragen eraan bij dat deze tendens in de toekomst wordt voortgezet. Voor strafvorderlijk onderzoek betekent dit dat jurisdictievraagstukken, tot vrij recente tijden grotendeels beperkt tot onderzoek naar bepaalde typen criminaliteit, nu in vrijwel ieder onderzoek van enige omvang prominent worden.

Dataficering

Een fenomeen dat zich momenteel voltrekt is de "dataficering" van onze samenleving. Bij het gebruik van de bovengenoemde technologieën worden enorme hoeveelheden (persoons)ge-

[16] Zie ook Koops 2016 voor een overzicht van grootschalige tendensen.
[17] Franken e.a. 2000, p. 5.

gevens gegenereerd en verwerkt. Deze gegevens worden gebruikt voor het maken van analyses en beslissingen over mensen en organisaties. Dit zorgt voor verbeteringen in processen, maar bergt ook het risico in zich dat mensen gereduceerd worden tot de gegevens die over hen beschikbaar zijn (hun "dataschaduw").[18] Naarmate meer gegevens beschikbaar komen en de technologie om deze gegevens te verwerken verbetert (denk aan kunstmatige intelligentie) zal de dataficering zich steeds sneller voltrekken.

"Onlife"

Met het internet als alles doorsnijdende en omvattende infrastructuur voor menselijke communicatie en interactie vervaagt het traditionele onderscheid tussen "online" en "offline" steeds verder. Digitale technologie medieert in toenemende mate onze omgang met de fysieke wereld (denk bijvoorbeeld *augmented* en *mixed reality*). Hierdoor ontstaat er een gemengde werkelijkheid: een "interrealiteit" of een "onlife" wereld.[19] Traditionele uitgangspunten voor regulering die geënt zijn op een onderscheid tussen de fysieke en de digitale wereld komen daarmee onder druk te staan.

[18] Zie bijvoorbeeld Van den Hoven e.a. 2016.
[19] Floridi 2014.

3. Fundamentele aandachtspunten die de commissieopdracht overstijgen

3.1. Jurisdictie

Een van de belangrijkste vraagstukken met betrekking tot opsporingsbevoegdheden in het digitale domein betreft niet zozeer het stelsel van bevoegdheden in de nationale wetgeving als wel de reikwijdte ervan in de internationale context. Steeds vaker blijken gegevens in het buitenland opgeslagen; vaak ook is niet bekend of gegevens die vanuit Nederland benaderbaar zijn, binnen of buiten de landsgrenzen zijn opgeslagen (*loss of knowledge of location*-problematiek). Wanneer gegevens zich buiten de landsgrenzen bevinden, bestaan knelpunten vanwege rechtsmacht. De bestaande procedures van rechtshulp zijn in de praktijk vaak omslachtig en traag, waardoor voor opsporingsonderzoeken relevante gegevens buiten het bereik van de Nederlandse overheid blijven. Deze knelpunten kunnen niet unilateraal worden opgelost, en behoren dan ook niet tot de opdracht van de commissie, en kunnen evenmin binnen het project Modernisering Strafvordering worden opgelost. Voor een adequate regeling van het opsporingsonderzoek in digitale omgevingen is het wel van groot belang dat dit vraagstuk met urgentie op Europees en internationaal niveau wordt geadresseerd.[20] Dit betekent dat Nederland de huidige inzet om op internationaal niveau, waaronder de Raad van Europa en de Europese Unie, tot een adequate regeling te komen, moet voortzetten en verder kracht moet bijzetten.

3.2. Het opsporingsbegrip en doeleinden van (cyber)criminaliteitsbestrijding

Al enkele decennia is een ontwikkeling zichtbaar waarin de opsporingsdiensten niet meer uitsluitend reactief optreden (in de zin dat pas activiteiten worden ontplooid nadat van een strafbaar feit is gebleken). In toenemende mate wordt proactief gehandeld, door reeds beschikbare informatie uit eerdere opsporingsonderzoeken en andere (al dan niet publiek toegankelijke) bronnen te analyseren. Deze aanpak heeft primair tot doel betere keuzes te kunnen maken in de allocatie van schaarse capaciteit voor toezicht en opsporing. Zo kan een geografische analyse van eerder gemelde woninginbraken inzicht geven in patronen in locaties en tijdstippen, die gebruikt kunnen worden voor het intensiveren van toezicht op bepaalde plaatsen en momenten. Dergelijke analyses kunnen zich ook richten op personen. Dan kan worden gesproken van *profiling*, waarbij op basis van statistische analyse de kans wordt berekend dat iemand een strafbaar feit heeft gepleegd of zal plegen. De inzet van geautomatiseerde data-analyse vergt in dit verband aandacht (zie daarover nader par. 3.4). Voor zover dergelijke proactieve analyses echter niet (primair) gericht zijn op opsporing en vervolging van personen, maar (ook) op andere doelen zoals het beëindigen van strafbare feiten, rijst de vraag in hoeverre dit onder het opsporingsbegrip valt en of en in hoeverre opsporingsbevoegdheden daartoe kunnen worden ingezet.

Het primaire doel van het Wetboek van Strafvordering is “te bevorderen dat de strafwet wordt toegepast op de werkelijk schuldige, en te voorkomen dat de onschuldige veroordeeld of zo mogelijk zelfs vervolgd wordt.”[21] Hieruit spreekt een duidelijke gerichtheid op een individuele verdachte. Aan de opsporingsdiensten worden daartoe opsporingsbevoegdheden toegekend, die bedoeld zijn om de waarheid boven tafel te krijgen.

Sommige vormen van digitale criminaliteit, zoals internetoplichting, ransomware en *Distributed Denial of Service*-aanvallen, kenmerken zich door enerzijds een veelal internationaal karakter (in de zin dat de daders zich in andere landen bevinden) en anderzijds door het soms

[20] Voor een analyse en beleidsaanbevelingen, zie Koops & Goodwin 2014.
[21] Memorie van toelichting conceptwetsvoorstel Boek 1, p. 6.

grote aantal slachtoffers. Het internationale aspect brengt met zich dat, in combinatie met de toenemende mogelijkheden voor daders om hun identiteit en sporen te verhullen, vaak op voorhand kan worden ingeschat dat de kans op identificatie en succesvolle vervolging van een verdachte zeer klein is. Het grote aantal slachtoffers brengt met zich dat het snel beëindigen van het strafbare feit een belangrijk doel van de opsporingsinstanties is. Als dat niet mogelijk is, wordt gestreefd naar de identificatie van slachtoffers (om deze te kunnen waarschuwen en helpen) of het vergaren van informatie over de werkwijze (om te gebruiken in andere onderzoeken of om preventieadviezen te kunnen geven aan potentiële slachtoffers). In de bestrijding van cybercriminaliteit staat daarmee de opsporing en vervolging van daders niet altijd meer voorop. In plaats daarvan komt meer nadruk te liggen op het beëindigen van het strafbare feit door in te grijpen op de infrastructuur die daarbij wordt gebruikt. Dat ingrijpen kan vereisen dat opsporingsbevoegdheden worden ingezet, waarbij de vraag speelt of, als de opsporing en vervolging van daders niet meer het primaire doel is, de inzet van opsporingsbevoegdheden is toegelaten.

In het conceptwetsvoorstel Boek 1 wordt een nieuwe definitie van het opsporingsbegrip voorgesteld:

> **Artikel 1.1.2.2 [artikel 132a]**
>
> Onder de opsporing van strafbare feiten waarmee opsporingsambtenaren zijn belast, wordt verstaan het verrichten van onderzoek met betrekking tot strafbare feiten met een strafvorderlijk doel.

Uit deze definitie volgt dat, naast specifieke voorwaarden die aan de toepassing van opsporingsbevoegdheden zijn verbonden, met opsporing een strafvorderlijk doel nagestreefd moet worden. De toepassing van opsporingsbevoegdheden zonder dat daarmee een strafvorderlijk doel wordt beoogd is hiermee niet in overeenstemming. Onder "strafvorderlijk doel" wordt, blijkens de memorie van toelichting (p. 6-7), verstaan "het bevorderen dat de overheidsreactie op een vermoedelijk gepleegd strafbaar feit in alle opzichten adequaat is". De gerichtheid op strafvorderlijke beslissingen, die in de huidige definitie van het opsporingsbegrip besloten ligt (artikel 132a Sv[22]) komt daarmee te vervallen. Het komt de commissie voor dat de nieuwe definitie van opsporing meer ruimte biedt voor opsporingsonderzoek dat niet gericht is op het identificeren van een verdachte, maar op het beëindigen van het strafbare feit. De commissie beveelt aan hierover in de memorie van toelichting bij artikel 1.1.2.2 een nadere beschouwing op te nemen.

Aanbeveling 1: maak in de memorie van toelichting bij artikel 1.1.2.2 duidelijk dat onder opsporing ook wordt verstaan het onderzoek naar aanleiding van een strafbaar feit waarbij de identificatie en vervolging van de dader niet voorop staat, maar waarbij ook andere doelen worden nagestreefd zoals beëindiging van het strafbare feit of het anderszins beschermen van de belangen van slachtoffers. → *p. 193*[23]

Een andere vraag is of onderzoekshandelingen die uitgevoerd worden zonder primair oogmerk op het identificeren van een verdachte en het verzamelen van bewijsmateriaal ten behoeve van vervolging, anders genormeerd moeten worden dan in het voorgestelde wetboek is voorzien.

[22] Artikel 132a (huidig) Sv luidt: "Onder opsporing wordt verstaan het onderzoek in verband met strafbare feiten onder gezag van de officier van justitie met als doel het nemen van strafvorderlijke beslissingen."

[23] De verwijzing aan het eind van elke aanbeveling verwijst naar de pagina in hoofdstuk 8 (Samenvatting, conclusies en aanbevelingen) waarop naar deze aanbeveling wordt verwezen. In hoofdstuk 8 zijn aanklikbare verwijzingen aangebracht, zodat de lezer (in de digitale versie van dit rapport) eenvoudig vandaaruit naar de desbetreffende aanbevelingen in de hoofdstukken kan navigeren voor het naslaan van de bijbehorende analyse en context. Via de aanklikbare verwijzingen in de aanbevelingen in de hoofdstukken kan de lezer (terug)navigeren naar de samenvatting.

De normering van onderzoekshandelingen wordt (hoofdzakelijk) gebaseerd op de mate van inbreuk op grondrechten die daarbij (normaliter) wordt gemaakt. De mate van inbreuk hangt daarbij niet in overwegende mate af van de vraag of de inzet van een bevoegdheid gericht is op het identificeren en vervolgen van een verdachte of op het beëindigen van een strafbaar feit, al zal het doel wel mede bepalend zijn voor de beantwoording van proportionaliteits- en subsidiariteitsvragen.

De vraag kan daarbij gesteld worden of het stelsel van waarborgen binnen het Wetboek van Strafvordering past bij overheidsingrijpen gericht op het beëindigen van strafbare feiten zonder (mede)oogmerk van vervolging. Het stelsel is van oudsher ingericht met een bepaalde balans tussen toezicht vooraf (bij toestemming voor inzet van bevoegdheden) en toezicht achteraf, waarbij het laatste met name is geconcentreerd rond het onderzoek ter zitting. Bij verstoring ontbreekt het laatste element, zodat een nieuwe balans nodig lijkt om een adequaat stelsel van waarborgen te bereiken voor de inzet van bevoegdheden die niet gericht is op het vervolgen van een verdachte. Anderzijds kan worden gesteld dat deze redenering dan ook zou moeten gelden voor die gevallen waarin wel sprake is van een klassieke gerichtheid op vervolging maar waarin geen daadwerkelijke vervolging en berechting plaatsvindt (vgl. par. 4.3.2). Dit zou aanleiding geven tot een fundamentele stelselwijzing. Het valt buiten de opdracht van de commissie om te adviseren over wat een adequaat stelsel zou kunnen zijn. De commissie acht het mogelijk dat op langere termijn, als de inzet van opsporingsbevoegdheden met het uitsluitende doel het beëindigen van strafbare feiten of het beschermen van de belangen van slachtoffers meer regel dan uitzondering wordt, een nadere regeling (binnen of buiten Sv) aan de orde zou kunnen zijn.

3.3. Wisselwerking Sv-Wpg

Een belangrijk aandachtspunt bij de regeling van opsporingsbevoegdheden is de wisselwerking tussen normering van de *vergaring* van gegevens en de normering van de *verwerking* van gegevens. De vergaring van gegevens wordt genormeerd in het nieuwe Boek 2, waarin vooral eisen staan voor de uiteenlopende manieren waarop gegevens kunnen worden verkregen. Voor een deel normeert Boek 2 ook de verwerking, waaronder opslag en gebruik, van de aldus vergaarde gegevens. Dit kan worden verklaard door het feit dat gebruik van een bepaalde opsporingsbevoegdheid impliciet met zich brengt dat, in elk geval tot op zekere hoogte, gegevens die met de bevoegdheid zijn verkregen, ook kunnen worden geanalyseerd en gebruikt. Doelbinding speelt daarbij een belangrijke rol: de geïmpliceerde analyse- en gebruiksmogelijkheden bij een bevoegdheid zijn normaliter beperkt tot de context van het geval waarvoor de bevoegdheid wordt ingezet. Verder of ander gebruik is mogelijk, voor zover dat expliciet is geregeld (doelafwijkend gebruik kan immers niet worden ingelezen als impliciet toegestaan door de regeling van een bepaalde opsporingsbevoegdheid).

De regeling van verder gebruik van vergaarde gegevens vindt momenteel grotendeels plaats in de Wpg en Wet justitiële en strafvorderlijke gegevens (hierna: Wjsg). De opdracht van de commissie beperkt zich tot Boek 2 van het voorgestelde nieuwe Wetboek van Strafvordering, wat betekent dat het voor de commissie niet mogelijk was een geïntegreerde visie te ontwikkelen op de regeling van opsporingsbevoegdheden op basis waarvan een samenhangend advies zou kunnen worden gegeven over de normering van bevoegdheden in Boek 2 alsmede over de implementatie van Richtlijn 2016/680/EU in de te herziene Wpg en de aangekondigde integratie en modernisering van de Wpg en Wjsg[24].

De normering van de initiële gegevensvergaring en de normering van het gegevensgebruik hangen sterk met elkaar samen. Deze normeringen moeten in verband met elkaar worden beschouwd omdat beide (zowel vergaring als daarop volgend bewaren en gebruiken) een inbreuk

[24] Zie *Kamerstukken II* 2013/14, 33 842, nr. 2.

op privacyrechten maken. Naarmate het gebruik van gegevens na vergaring ruimer en indringender mogelijk is, wordt de normering van de vergaring zelf belangrijker (er moet immers rekening worden gehouden met meer of ingrijpender gevolgen bij ruimer gebruik). Ook het omgekeerd geldt: een strikte normering van het gebruik van gegevens kan een ruimere vergaringsbevoegdheid rechtvaardigen. Nu de opdracht van de commissie beperkt is tot het wettelijk kader van de gegevensvergaring, is het bestaande wettelijke kader van de Wpg en Wjsg als referentiekader gehanteerd.

Bij de aangekondigde modernisering van laatstgenoemde wetten zal ook beoordeeld moeten worden op welke wijze de beoogde wijzigingen doorwerken in de hiervoor beschreven samenhang tussen normering van de vergaring en de normering van het gebruik van gegevens. Omgekeerd moet de normering in het gemoderniseerde Wetboek van Strafvordering ook beoordeeld worden in samenhang met de modernisering van de Wpg en Wjsg. De commissie benadrukt daarom het belang van een samenhangende visie op de normering van zowel gegevensvergaring als gebruik: Sv en Wpg/Wjsg moeten in samenhang het opsporingsonderzoek reguleren op een manier die een goede balans biedt tussen enerzijds de effectiviteit van de rechtshandhaving en anderzijds rechtsbescherming in de vorm van afdoende waarborgen die inbreuken op grondrechten kunnen legitimeren als noodzakelijk in een democratische samenleving.

Aanbeveling 2: bij het moderniseringstraject is het van belang een integrale visie te hanteren op de normering van zowel gegevensvergaring als -gebruik: Sv en Wpg moeten in samenhang het opsporingsonderzoek reguleren op een manier die een goede balans biedt tussen effectiviteit en rechtsbescherming. → *p. 193*

3.4. Geautomatiseerde data-analyse

3.4.1. Algemeen

Tegen de achtergrond van de bovenstaande discussie rondom de wisselwerking tussen het Wetboek van Strafvordering en de Wpg en de Wjsg speelt de discussie rondom geautomatiseerde data-analyse. Nieuwe technologieën stellen de politie in staat om grote hoeveelheden gegevens te ontsluiten, verrijken, analyseren en visualiseren. Door gegevens uit verschillende bronnen te combineren kunnen de opsporingsdiensten tot nieuwe inzichten en verbanden komen die relevant zijn voor de uitvoering van de algemene politietaak (informatiegestuurd politiewerk) en voor specifieke opsporingsonderzoeken (informatiegestuurde opsporing).[25] Verder richting de toekomst is de verwachting dat ook voorspellende opsporing (*predictive policing*) breder toegepast wordt. De opsporing is dan "data-gedreven" (*data-driven*) en op voorhand ongericht. Complexe algoritmische berekeningen liggen daarbij ten grondslag aan de te nemen strafvorderlijke beslissingen. Het gaat hierbij ook niet zozeer meer om het enkele oplossen van misdrijven als wel om het voorkomen van misdrijven op basis van patroonherkenning en profilering. Schematisch kan het volgende onderscheid worden gehanteerd:

Geautomatiseerde data-analyse binnen de politie		
Informatie-gestuurd politiewerk	Geautomatiseerde data-analyse voor ongerichte en/of proactieve opsporing	Geautomatiseerde data-analyse voor gerichte, reactieve opsporing

Omdat de verzameling en het verdere gebruik van persoonsgegevens door de opsporingsdiensten een inbreuk op de persoonlijke levenssfeer vormt, moet dit bij wet zijn voorzien, met een expliciete wettelijke basis bij een meer dan geringe inbreuk. Geautomatiseerde data-analyse

[25] De Vries 2017.

ten behoeve van de opsporing wordt deels gereguleerd in het Wetboek van Strafvordering en deels in de Wpg. Voor wat betreft de normering van het *verzamelen* van gegevens moeten we primair kijken naar het Wetboek van Strafvordering. Voor het verdere *gebruik* vormt de Wpg het belangrijkste toetsingskader. Beide wetten kennen andere uitgangspunten: in Sv staat de bescherming van burgers tegen inbreuken door de overheid voorop, terwijl in de Wpg de nadruk ligt op een effectief en efficiënt gebruik van gegevens.[26] Ook kennen beide wetten een andere vorm van toezicht als het gaat om de bescherming van gegevens: in het Wetboek van Strafvordering is het de officier van justitie en in voorkomende gevallen de rechter-commissaris die het vergaren van de gegevens gelast en toetst, in de Wpg is het de bevoegd functionaris die het (her)gebruik van vergaarde gegevens toetst met op afstand toezicht door de functionaris gegevensbescherming en de Autoriteit Persoonsgegevens.

De Wetenschappelijke Raad voor het Regeringsbeleid (hierna: WRR) stelt in zijn rapport *Big Data in een vrije en veilige samenleving* dat de waarborgen voor betrokkenen primair in de verzamelfase zitten, maar in veel mindere mate in de fase van de analyse en het gebruik.[27] Het verzamelen van gegevens kent door het strafvorderlijk kader in Sv veel juridische waarborgen (bijvoorbeeld een bevel van de officier van justitie en de machtiging van de rechter-commissaris in een aantal gevallen). Dit geldt in veel mindere mate voor de verdere verwerking van persoonsgegevens in het kader van de analyse en het gebruik zoals gereguleerd door de Wpg. In deze fase is er primair een interne toets door de "bevoegd functionaris" en de functionaris gegevensbescherming en extern systeemtoezicht in de vorm van de Autoriteit Persoons-gegevens. Dit kan worden gezien als een potentieel risico voor de privacy (en andere rechten) van betrokkenen alsmede voor de integriteit van onderzoeken.[28]

De commissie onderschrijft de aanbeveling van de WRR dat de fase van analyse en gebruik aandacht behoeft in het licht van het stelsel van rechtsbescherming bij grootschalige data-analyse in de toekomst. De vraag is of de mogelijke inbreuken op grondrechten van betrokkenen en risico's voor de integriteit van de opsporing bij (substantiële vormen van) geautomatiseerde data-analyse enkel binnen de Wpg kunnen worden genormeerd. Deze vraag overstijgt de opdracht van de commissie en kan niet binnen dit rapport worden behandeld. De commissie merkt op dat in dit kader naast de Algemene Verordening Gegevensbescherming[29] (AVG) de Richtlijn politie- en justitiegegevens (2016/680),[30] die thans nog geïmplementeerd moet worden, van groot belang is. Daarin worden eisen en beperkingen gesteld aan omvang en (beschrijving van) doelen van gegevensverzameling, het hergebruik van gegevensverzamelingen reeds in bezit van de opsporing en, in het bijzonder, geautomatiseerde data-analyse van persoonsgegevens die strafvorderlijke consequenties voor betrokkene met zich kan brengen. Een verdergaande behandeling van deze vraagstuk overstijgt de opdracht van de commissie en kan daarom niet binnen dit rapport worden uitgevoerd.

Wel lichten wij één aspect van deze vraag nader uit, dat de commissie van bijzonder belang acht voor het moderniseringstraject in het algemeen, namelijk de uitlegbaarheid van algoritmische analyse en besluitvorming.

3.4.2. Uitlegbaarheid

Complexe algoritmische besluitvorming kan bijzondere risico's voor grondrechten van burgers en de integriteit van de opsporing met zich brengen; te denken valt aan de mogelijke gevolgen van vals-positieven en ongegronde aannames gebaseerd op ondoorzichtige algoritmische analyses. De nieuwe Richtlijn politie- en justitiegegevens (artikel 11) en het Nederlandse

[26] Zie de memorie van toelichting bij de Wet politiegegevens, *Kamerstukken II* 2005/06, 30 327, nr. 3, p. 3.
[27] WRR 2016, p. 27.
[28] Zie in dit kader Schermer 2017.
[29] Verordening 2016/679 van 27 april 2016, *Publicatieblad van de Europese Unie* L119/1.
[30] Richtlijn 2016/680 van 27 april 2016, *Publicatieblad van de Europese Unie* L119/89.

wetsvoorstel ter implementatie hiervan onderkennen met de volgende bepaling dit risico (artikel 7a, eerste lid, implementatievoorstel):

> Een besluit dat uitsluitend op geautomatiseerde verwerking is gebaseerd, met inbegrip van profilering, dat voor de betrokkene nadelige rechtsgevolgen heeft of hem in aanmerkelijke mate treft, is verboden, tenzij wordt voorzien in voorafgaande menselijke tussenkomst door of namens de verwerkingsverantwoordelijke en in specifieke voorlichting aan de betrokkene.[31]

De vraag is evenwel in hoeverre menselijke tussenkomst nog mogelijk of relevant is wanneer de besluitvorming door een geautomatiseerd werk ondoorzichtig of zelfs ondoorgrondelijk is. De eis van menselijke tussenkomst bij op grond van geautomatiseerde data-analyse genomen beslissingen biedt voor de langere termijn geen voldoende garantie voor de uitlegbaarheid, en daarmee voor de aanvechtbaarheid, van de genomen beslissing: naarmate algoritmes slimmer worden, kunnen mensen wel betrokken worden bij besluitvorming, maar zullen zij toch leunen op de algoritmische uitkomst, omdat ze steeds moeilijker zelfstandig een oordeel kunnen vormen over het te nemen besluit. Juist daarom is een ander onderdeel van de in de Richtlijn voorziene waarborgen, "om uitleg over het na een dergelijke beoordeling genomen besluit te krijgen", des te belangrijker. Voorkomen moet worden dat beslissingen worden genomen zonder dat de gronden voor de beslissing in voldoende mate inzichtelijk kunnen worden gemaakt.

Zowel de AVG als de Richtlijn politie- en justitiegegevens bevatten een verbod op volledig geautomatiseerde beslissingen, maar staan geautomatiseerde beslissingen wel toe als voldoende waarborgen bestaan. De AVG (die niet van toepassing is in de context van opsporing, waarvoor de Richtlijn geldt) is op het punt van uitlegbaarheid iets uitgebreider en omvat naast het vereiste van menselijke tussenkomst ook de mogelijkheid "nuttige informatie over de onderliggende logica" te verstrekken (artikelen 13 en 15 AVG). De Richtlijn bepaalt dat "geautomatiseerde individuele besluitvorming" enige vorm van menselijke tussenkomst moet hebben, maar heeft geen vergelijkbare bepaling over informatievoorziening over de onderliggende logica. Overweging 38 van de Richtlijn spreekt wel over de waarborg "om uitleg over het na een dergelijke beoordeling genomen besluit te krijgen", maar deze waarborg keert niet terug in artikel 11 van de Richtlijn. In het implementatiewetsvoorstel is dit echter wel opgenomen: de betrokkene heeft recht op informatie over "het bestaan van geautomatiseerde besluitvorming, met inbegrip van de in artikel 7a, eerste lid, bedoelde profilering, en nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene" (voorgesteld artikel 24b, tweede lid, onderdeel e, Wpg)[32]. Een vergelijkbare bepaling wordt voorgesteld in het kader van het implementatievoorstel voor de Wjsg (voorgesteld artikel 17b Wjsg).

De vraag is of deze bepalingen voldoende zijn om uitlegbaarheid van (mede) op geautomatiseerde data-analyse gebaseerde beslissingen in het kader van de strafvordering te waarborgen. Dergelijke beslissingen zullen, naarmate geautomatiseerde data-analyse zich verder ontwikkelt en steeds betere uitkomsten zal laten zien, vaker voorkomen, zowel beslissingen in de opsporings- en vervolgingsfase als beslissingen in het kader van het onderzoek ter zitting. Vergelijkbaar met de "chain of custody" van forensisch bewijs, zou ook de "chain of arguments" die ten grondslag ligt aan de inzet van opsporingsbevoegdheden en de bewijsvoering verdedigbaar moeten zijn. Dat vergt inzicht in de beslissingen die worden genomen bij het opsporingsonderzoek, bijvoorbeeld over de inzet van bepaalde bevoegdheden of in de uitvoering daarvan.

Verder is relevant dat opsporingsdiensten en het OM toegang hebben tot grote datasets en tot de technologie om deze te analyseren. Geautomatiseerde data-analyse toegepast op grote

[31] *Kamerstukken II* 2017/18, 34 889, nr. 2.
[32] *Kamerstukken II* 2017/18, 34 889, nr. 2.

datasets kan leiden tot een selectieve presentatie van data aan een rechter, die zou kunnen bijdragen aan een (mogelijk onterechte) rechterlijke overtuiging. Denk bijvoorbeeld aan een situatie waarin een geautomatiseerde data-analyse uit 50.000 regels chat-gegevens resulteert in een selectie van acht regels die een bepaald beeld van de verdachte oproepen, terwijl uit dezelfde dataset ook acht regels te vinden zijn die het tegengestelde beeld zouden oproepen. Het beginsel van "equality of arms" impliceert dat de verdediging de mogelijkheid moet hebben om het bewijsmateriaal te betwisten; uitlegbaarheid vergt in dit verband daarom ook verantwoording over de totstandkoming van de op geautomatiseerde data-analyse gebaseerde selectie van bewijsmateriaal uit datasets waarin ook potentieel ontlastend bewijs te vinden is.

Op zich is dit geen nieuwe problematiek: strafvorderlijke beslissingen en beslissingen ter zitting moeten altijd uitlegbaar, in de zin van gemotiveerd, zijn (waardoor zij ook aanvechtbaar worden omdat een procesdeelnemer argumenten kan aandragen tegen deze motivering). In die zin is geen expliciete eis van uitlegbaarheid nodig in het strafproces: die eis is, hoewel impliciet, stevig verankerd in het stelsel. Toch kan de vraag worden opgeworpen of, met de doorontwikkeling van geautomatiseerde data-analyse, een explicitering van de eis van uitlegbaarheid – zoals ook in de AVG en Richtlijn opgenomen – voor de toekomst wenselijk zou zijn. Naarmate bij beslissingen in het strafproces meer gewicht toegekend zou worden aan uitkomsten van geautomatiseerde data-analyse, bestaat het risico dat de klassieke uitlegbaarheid in de zin van motiveringseisen wordt gereduceerd tot het verwijzen naar het feit dat dit de uitkomst is van geautomatiseerde data-analyse en dat de desbetreffende vorm van geautomatiseerde data-analyse kennelijk betrouwbaar wordt geacht ("system says no" of in dit geval eerder "system says so"). Daarbij zou wellicht te snel over het hoofd worden gezien dat de betrouwbaarheid van een geautomatiseerde data-analyse niet alleen afhangt van de werking van een algoritme en van een bepaald succespercentage van het algoritme, maar ook afhangt van de manier waarop een zelflerend systeem tot regels is gekomen (aan de hand van de gebruikte datasets voor training en analyse), van de data die in casu als input zijn gebruikt voor de geautomatiseerde data-analyse, en van de presentatie van de uitkomsten. Op de korte termijn, waarin geautomatiseerde beslissingen nog geen gemeengoed zijn en als zodanig ook veelal kritisch bevraagd zullen worden, is het risico op een "system says so"-tunnelvisie klein, maar voor de langere termijn, naarmate de samenleving meer zal gaan leunen op geautomatiseerde beslissingen in veel contexten, neemt het risico toe op niet specifiek gemotiveerde, en daarmee moeilijk weerlegbare, beslissingen. Om die reden lijkt het belangrijk een expliciete uitlegbaarheidseis op te nemen in het Wetboek van Strafvordering voor (mede) op geautomatiseerde data-analyse gebaseerde beslissingen in het strafproces. Daarvoor volstaan de (voorgestelde) bepalingen in Wpg en Wjsg als zodanig niet, omdat de reikwijdte van beslissingen verder reikt dan de verwerking van politie- en justitiële gegevens: de problematiek speelt, als aangegeven, ook bij beslissingen over inzet van opsporingsbevoegdheden en de bewijsbeslissingen bij het onderzoek ter zitting (niet alleen ten aanzien van bewijs maar ook voor straftoemeting), alsook bij bijvoorbeeld beslissingen in het kader van TBS en voorwaardelijke invrijheidsstelling. Aangezien deze problematiek de opdracht van de commissie overstijgt, adviseert de commissie de wetgever aandacht te besteden aan geautomatiseerde data-analyse en het belang van uitlegbaarheid daarbij, niet alleen in het kader van Boek 2 maar binnen het gehele moderniseringstraject.

Aanbeveling 3: de wetgever dient aandacht te besteden aan geautomatiseerde data-analyse in het moderniseringstraject in brede zin, en daarbij de mogelijkheid te overwegen in het Wetboek van Strafvordering de momenteel impliciete eis van uitlegbaarheid van strafvorderlijke beslissingen te expliciteren indien deze beslissingen (mede) op geautomatiseerde data-analyse worden gebaseerd. → *p. 193*

3.5. Het systeem van normering en het stelsel van toezicht

Naast het hierboven behandelde onderscheid in normering van vergaring dan wel gebruik van gegevens, zijn er andere relevante aspecten van normering die de opdracht van de commissie overstijgen. Een van de uitgangspunten in het huidige en ook het gemoderniseerde Wetboek van Strafvordering is dat naarmate een bevoegdheid ingrijpender is, voorafgaande toestemming van een hogere autoriteit is vereist.[33] Achteraf dient verantwoording te worden afgelegd over de toepassing van de bevoegdheid en kan controle plaatsvinden door de zittingsrechter, over de band van artikel 359a Sv. Ook het gemoderniseerde wetboek kent een regeling met betrekking tot processuele sancties op onrechtmatig handelen.[34]

De commissie tekent daarbij aan dat de huidige – alsook de door de commissie in paragraaf 4.2 voorgestelde – systematiek van normering vooraf, met als centrale pijler de bevoegde autoriteit, in toenemende mate knelpunten kan gaan opleveren. Dit komt omdat de technisch-sociale ontwikkelingen van de afgelopen en komende decennia betekenen dat het steeds eenvoudiger is geworden, en nog verder zal worden, om iemands privéleven in beeld te brengen. Er zijn meer data, op meer plaatsen aanwezig, die op meer manieren kunnen worden vergaard en gemakkelijker in onderlinge samenhang kunnen worden verwerkt.[35] Dit betekent dat bij een gemiddeld opsporingsonderzoek bij de toepassing van opsporingsbevoegdheden met een digitale component – oftewel vrijwel elk onderzoek – snel de drempel van (in termen van het door de commissie voorgestelde algemene normeringscriterium, zie par. 4.2) stelselmatigheid zal worden bereikt, en dat (in elk geval op termijn) in toenemende mate ook sneller dan voorheen sprake zal zijn van (de in par. 4.2 eveneens voorgestelde drempel van) ingrijpende stelselmatigheid, zelfs bij traditioneel minder ingrijpende bevoegdheden.

De consequentie van deze constatering is een duivels dilemma. Wanneer we enerzijds vasthouden aan eenzelfde niveau van rechtsbescherming, zal bij een gemiddeld onderzoek steeds vaker betrokkenheid van de rechter-commissaris nodig zijn (omdat bij de uitoefening van een opsporingsbevoegdheid een wezenlijk of aanzienlijk deel van het privéleven in beeld komt). Dit betekent niet alleen dat aanzienlijke uitbreiding van het aantal rechters-commissarissen nodig zijn, maar ook herbezinning op de rol van de rechter-commissaris in de opsporing, die zich dan "terug" zou kunnen ontwikkelen van rechter in het vooronderzoek tot onderzoeksrechter. Wanneer we anderzijds vasthouden aan de huidige organisatie van opsporing qua bevoegdheidsverdeling tussen opsporingsambtenaar, officier van justitie en rechter-commissaris (waarbij de laatste alleen in de meest ingrijpende gevallen betrokken is), betekent dit dat de drempel van (ingrijpende) stelselmatigheid steeds opgeschoven zal moeten worden (het beeld van iemands privéleven zal steeds scherper moeten zijn voordat de rechter-commissaris erbij betrokken moet worden), wat resulteert in een *de facto* erosie van rechts-bescherming. Simplistisch gezegd: handhaving van de systematiek in toetsing vooraf, komt op termijn neer ofwel op rechterlijke betrokkenheid bij een groot deel van de opsporings-onderzoeken ofwel op een geleidelijke erosie van privacy. Beide opties zijn volgens de commissie onwenselijk. De commissie concludeert daarom dat voor de kortere termijn, waar nodig met uitbreiding van de capaciteit van het OM en de kabinetten r-c, wel met de huidige systematiek valt te werken voor zover het gaat om de rechtsbescherming bij inbreuken op de privacy van verdachten, maar dat op (middel)lange termijn de rechtsbescherming mogelijk anders zal moeten worden ingericht.

[33] *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 51 en 99 en *Kamerstukken II* 2015/16, 29 279, nr. 278, p. 51 (Contourennota).

[34] In het gemoderniseerde wetboek wordt voorgesteld om de processuele sancties niet langer in één voorschrift onder te brengen, maar verspreid over drie losse artikelen te regelen. Het verlies van het recht om de verdachte te vervolgen van het Openbaar Ministerie wordt geregeld in Boek 3 (artikel 3.1.8), bewijsuitsluiting wordt geregeld in Boek 4 (artikel 4.3.2.6) en strafvermindering in het Wetboek van Strafrecht (artikel 44b).

[35] Zie Koops 2006b voor onderbouwing van deze tendens.

Aanbeveling 4: de wetgever dient zich rekenschap te geven van het inzicht dat, in het licht van de hier geschetste ontwikkeling, het systeem van toezicht vooraf op kortere termijn, waar nodig met capaciteitsuitbreiding, werkbaar is, maar op (middel)lange termijn moet worden herzien. Gezien de centrale rol van toetsing vooraf in de normeringssystematiek, dient tijdig nagedacht te worden over eventuele op (middel)lange termijn benodigde aanpassingen in deze systematiek. → *p. 193*

Eventuele onvolkomenheden in het toezicht vooraf kunnen (niet volledig maar wel tot op zekere hoogte) worden gecompenseerd door toezicht achteraf. De commissie constateert dat in veel gevallen de inzet van middelen niet achteraf door een rechter zal worden gecontroleerd. Enerzijds omdat lang niet ieder opsporingsonderzoek leidt tot het aanhangig maken van een strafzaak bij de rechter, anderzijds omdat het vooral voor niet-verdachten lastig kan zijn om tijdens het strafvorderlijk vooronderzoek een rechterlijk oordeel te verkrijgen over de vergaring of andere verwerking van "hun" gegevens (vgl. ook par. 4.3.2 onder "Beklag tegen kennisneming en gebruik"). Dit in de praktijk bestaande beperkte rechterlijk toezicht creëert vanuit de optiek van rechtsbescherming een lacune. De commissie merkt daarbij op dat de beperkte toetsing achteraf op de vergaring en verwerking van gegevens naast persoonlijke risico's voor burgers ook maatschappelijke risico's creëert, met name in termen van verlies van vertrouwen in het functioneren van de desbetreffende overheidsorganen.

Daarbij moet worden opgemerkt dat het systeem van normering nog verder wordt gecompliceerd doordat er bij digitale opsporing ook veelal gegevens van niet-verdachte derden in beeld kunnen komen. Het is evident dat de zich ontwikkelende inzet van digitale opsporingsmiddelen en -methodieken een steeds grotere impact zal kunnen hebben op de privacy van niet alleen verdachten, maar ook van andere burgers. Er is ook een tendens zichtbaar om steeds meer informatie uit systemen aan elkaar te koppelen dan wel met elkaar te vergelijken. Dit alles onderstreept het belang van een zorgvuldige omgang binnen de opsporingsinstanties met gegevens, de gegevens van niet als verdachte aangemerkte derden daaronder nadrukkelijk begrepen, en het belang van adequaat toezicht hierop.

De commissie wijst erop dat in het wetsvoorstel Computercriminaliteit III (hierna: wetsvoorstel CCIII) het toezicht achteraf in het Wetboek van Strafvordering wordt uitgebreid door de introductie van een vorm van systeemtoezicht door de Inspectie Justitie en Veiligheid.[36] Het gaat daarbij specifiek om het houden van toezicht op – kort gezegd – de uitoefening van de bevoegdheid tot binnendringen in een geautomatiseerd werk en het verrichten van onderzoek. De in het wetsvoorstel aangewezen Inspectie ressorteert thans onder het Ministerie van Justitie en Veiligheid. De vraag kan worden gesteld, zowel om inhoudelijke redenen als om redenen van beeldvorming, of deze Inspectie de aangewezen instantie is om genoemd toezicht vorm te geven. Er is reeds nu een groot belang gemoeid met de inrichting van een niet alleen goed en gericht, maar ook in brede kring als onafhankelijk beschouwd, extern toezichtsorgaan, dat toezicht houdt op de wijze waarop de opsporingsinstanties omgaan met in het kader van strafrechtelijke onderzoeken verkregen gegevens. Dit belang zal de komende jaren bovendien alleen nog toenemen. In dit licht zou het de voorkeur verdienen om bedoeld extern systeemtoezicht te beleggen bij een instantie die zowel qua personele samenstelling als organisatorische inbedding verder af staat van het Ministerie van Justitie en Veiligheid dan de huidige Inspectie.

In dit kader merkt de commissie op dat in het kader van het wetsvoorstel CC III al is voorgesteld het externe toezicht inzake de daar aan de orde zijnde bevoegdheden tot digitale gegevensvergaring onder te brengen bij een externe Commissie van Toezicht, vergelijkbaar met de Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten.[37] Een

[36] *Kamerstukken I* 2016/2017, 34372, A (artikel 126nba lid 7 Sv). Zie ook *Kamerstukken I* 2016/17, 34372, D, p. 30-34.

[37] Zie het advies en het nader rapport van de Raad van State, *Kamerstukken II* 2015/16, 34372, nr. 4, p. 6-10.

dergelijke commissie zou dan achteraf toezicht uit kunnen oefenen op de rechtmatigheid van de uitvoering van de strafrechtelijke bevoegdheden inzake gegevensvergaring en -verwerking, de wijze van opslag, verdere verwerking en vernietiging daaronder begrepen. Voorafgaand aan de eventuele instelling van een dergelijke commissie zou een gedegen reflectie moeten plaatsvinden op het volledige samenstel van toezicht.[38] Dan zou ook opnieuw naar de rol van de rechter(-commissaris) in de normering van de opsporingsbevoegdheden en de processuele sancties moeten worden gekeken. Ook zou helderheid moeten worden verkregen over de manier waarop de verschillende vormen van toezicht (vooraf en achteraf, intern en extern) zich tot elkaar verhouden.

Al met al concludeert de commissie dat op de langere termijn een reflectie op het stelsel van toezicht op de opsporing nodig is. Een dergelijke reflectie gaat de opdracht van de commissie te buiten, maar is wel van wezenlijk belang voor een toekomstbestendig Wetboek van Strafvordering.

Aanbeveling 5: de commissie beveelt aan om in de context van het verdere wetgevingstraject specifiek aandacht te besteden aan de houdbaarheid van het systeem van toezicht op de langere termijn, alsmede aan de inrichting van extern toezicht op de gegevensvergaring en -verwerking door opsporingsdiensten, en daarbij mede de reeds eerder gedane suggesties te betrekken. → *p. 193*

3.6. Tussenconclusie

De commissie heeft in dit hoofdstuk diverse aandachtspunten gesignaleerd die suggereren dat meer reflectie nodig is dan het enkele verbeteren – waar nodig – van de regeling in Hoofdstukken 7 en 8 van Boek 2 van het conceptwetsvoorstel. Sommige onderwerpen die de commissieopdracht overstijgen, zoals jurisdictie en de ontwikkelingen in geautomatiseerde data-analyse, vergen zelfstandig en dringend aandacht van het kabinet in samenspraak met overige beleidsmakers. Andere aandachtspunten, zoals de wisselwerking tussen Sv en Wpg en het systeem van normering en het stelsel van toezicht, hebben implicaties voor de houdbaarheid van een gemoderniseerd wetboek op de (middel)lange termijn. Binnen het moderniseringstraject is in dat licht reflectie wenselijk op de vraag waar de nadruk moet komen te liggen: het voor dit moment vasthouden aan bestaande kaders (zoals het in zelfstandige trajecten behandelen van Sv en Wpg, of het huidige toezichtskader) waarbinnen momenteel goed kan worden gewerkt maar die op (middel)lange termijn steeds meer kunnen gaan knellen; of een meer fundamentele herziening waarbij ook bestaande kaders ter discussie kunnen staan.

Dit geconstateerd hebbend, heeft de commissie vervolgens geprobeerd om binnen de bestaande kaders voorstellen te doen die de werkbaarheid en toekomstbestendigheid van de regeling van bevoegdheden in de Hoofdstukken 7 en 8 van Boek 2 bevorderen. Deze worden in de volgende hoofdstukken weergegeven.

[38] Zie voor een overzicht Devroe e.a. 2017. Zie ook de Memorie van Antwoord bij het wetsvoorstel computercriminaliteit III, waarin een korte schets wordt gegeven van alle toezichtvormen die er nu al bestaan, *Kamerstukken I* 2016/17, 34 372, D. Zie ook voetnoot 92 en bijbehorende tekst over toezicht door de procureur-generaal bij de Hoge Raad.

4. Algemene benadering

4.1. Inleiding: toekomstbestendigheid, rechtszekerheid, dataficering en volatilisering

Vraag 1 uit de opdracht van de commissie betreft een visie op de toekomstbestendigheid van het pakket van bevoegdheden. Hierbij wordt verwezen naar de uitdagingen voor de opsporing in "de komende decennia". De commissie leidt hieruit af dat de wens bestaat dat de regeling van bevoegdheden in het nieuwe wetboek dermate robuust is dat deze, in elk geval qua gehanteerde concepten en systematiek, langere tijd mee kan. Die wens is logisch, gezien de majeure operatie die een complete modernisering van een wetboek inhoudt; dat doet men niet met het oog op de korte termijn, maar juist met oog voor de langere termijn. De wens is echter ook problematisch, in het licht van digitale ontwikkelingen.

Hoewel de technologie zich niet altijd zo snel en onvoorspelbaar ontwikkelt als soms wel wordt gesteld – grootschalige ontwikkelingen als het web, mobiele telefonie en de cloud komen niet uit de lucht vallen maar zijn jaren in ontwikkeling – is het moeilijk te overzien hoe het digitale landschap er in pakweg 2040 zal uitzien. De periode van "de komende decennia" is simpelweg te lang om de ontwikkeling, adoptie en implicaties van grootschalige ontwikkelingen die nu gaande zijn of in de kinderschoenen staan – zoals quantumcomputers, *machine learning*, breinlezen of het Internet of People – goed te kunnen duiden. Het is zelfs niet goed mogelijk om deze ontwikkelingen goed in te schatten voor de komende tien tot vijftien jaar.

Het is in dat licht van wezenlijk belang om de wens tot toekomstbestendigheid in perspectief te plaatsen. Evenals bij het streven naar techniek-onafhankelijke wetgeving, past een kanttekening bij toekomstbestendige wetgeving: wetgeving die in hoge mate techniek-onafhankelijk is, en daarmee vermoedelijk ook toekomstbestendig, zal dermate abstract zijn dat niet meer duidelijk is wat de wetgeving precies regelt. Het spanningsveld tussen techniek-onafhankelijkheid en rechtszekerheid bestaat ook bij toekomstbestendige wetgeving: er moet een goede balans worden gevonden tussen wetgeving die voldoende duurzaam is en tegelijk ook voldoende rechtszekerheid biedt.[39]

Binnen dit spanningsveld moet de wetgever rekening houden met een wereld waarin de digitalisering tot in de haarvaten doorgedrongen zal zijn. Alles is herleidbaar, en wordt ook steeds meer herleid, tot data – een tendens die wordt aangeduid met "dataficering" (*datafication*).[40] Deze data worden deels bewust gegenereerd en verspreid, maar deels ook onbewust afgegeven – opgevangen door sensoren die gedrag omzetten in data – en afgeleid uit andere data. De hoeveelheid digitale sporen die mensen onbewust genereren met hun gedrag (de digitale schaduw) is al enkele jaren groter dan de hoeveelheid bewust gegenereerde data (de digitale voetafdruk).[41] Verder laat de wereld van de komende decennia zich ook karakteriseren door het vervagen van traditionele grenzen en onderscheiden (in par. 4.2 geven we enkele voorbeelden). In dit opzicht zet de tendens die de WRR al in 1997 aanduidde zich onverminderd voort, namelijk "volatilisering".[42] De term duidt op het kenmerk dat maatschappelijke

[39] Zie over dit spanningsveld Koops 2006a.
[40] https://en.wikipedia.org/wiki/Datafication (laatst geraadpleegd 1 juni 2018).
[41] Koops 2011, verwijzend naar IDC (2010), *The Digital Universe Decade – Are You Ready?*, https://www.emc.com/collateral/analyst-reports/idc-digital-universe-are-you-ready.pdf (laatst geraadpleegd 1 juni 2018). Zie ook IDC 2012, p. 2: "The amount of information individuals create themselves — writing documents, taking pictures, downloading music, etc. — is far less than the amount of information being created *about them* in the digital universe."
[42] Gelok & De Jong 1997.

processen door ICT veelal in een stroomversnelling komen, waarbij tijd en ruimte andere dimensies lijken te krijgen en fysieke en virtuele grensvervaging optreedt.[43]

Dataficering en volatilisering leiden tot een wereld waarin steeds meer data worden gegenereerd, opgeslagen en verwerkt, terwijl er steeds minder ankerpunten zijn om deze data te kunnen "plaatsen", in letterlijke alsook in overdrachtelijke zin. Voor wetgeving en wetgevingssystematiek heeft dit ingrijpende consequenties: in het spanningsveld tussen toekomstbestendigheid en rechtszekerheid, valt door dataficering en volatilisering steeds minder terug te vallen op vaste concepten die een duidelijk ankerpunt bieden of scherpe conceptuele grenzen kunnen bieden. Als alles vloeibaar wordt, valt weinig vast te pakken. Niettemin kan de wetgeving niet zonder handvatten die enige greep houden op dataontwikkelingen in de komende decennia: op de een of andere manier zullen concepten en onderscheiden moeten worden gehanteerd in het gemoderniseerde wetboek, die richting kunnen geven aan de uitoefening van bevoegdheden en die burgers voldoende inzicht geeft in wat zij in dat opzicht kunnen verwachten wanneer de bevoegdheden gepaard gaan met inbreuken op hun grondrechten.

Tegen deze achtergrond heeft de commissie, gezien de noodzaak van een voldoende mate van toekomstbestendigheid, gekozen voor nadruk op een heldere systematiek en duurzame concepten. Dit leidt, bij gebrek aan concrete ankerpunten waarop kan worden teruggevallen in een wereld van dataficering en volatilisering, tot tamelijk abstracte regelingen. Qua wetgevingssystematiek is dit de enige benadering die een redelijke kans maakt om enkele decennia mee te gaan. Een benadering die meer nadruk legt op rechtszekerheid en duidelijkheid voor de kortere termijn, in de vorm van concrete regeling en concepten die toegesneden zijn op de problematiek van de jaren '10, loopt een te groot risico om over tien jaar weer aan fundamentele herziening toe te zijn. De keuze voor tamelijk abstracte regelingen betekent dat de memorie van toelichting van fundamenteel belang is om het nadeel van abstractie – het gebrek aan rechtszekerheid – op te vangen. De commissie adviseert dan ook om een uitgebreide memorie van toelichting te schrijven, met voldoende voorbeelden die duidelijk maken hoe de concepten en regelingen in verschillende omstandigheden uitwerken, zowel voor de korte termijn (met voorbeelden voor de huidige praktijk en stand van de techniek) als voor de langere termijn, voor zover deze enigszins valt te overzien.

4.2. Algemeen normeringscriterium

4.2.1. Achtergrond: huidige normatieve kaders zijn niet goed bruikbaar

Het mensenrechtelijk kader

Normering van opsporing hangt samen met de ernst van de inbreuk op de persoonlijke levenssfeer (privacy).[44] Zwaardere inbreuken op de privacy vergen zwaardere waarborgen. Een van de belangrijkste waarborgen is de bevoegde autoriteit die toestemming moet geven voor de uitoefening van een bevoegdheid. Het Nederlandse systeem kent in dat opzicht hoofdzakelijk een driedeling: sommige bevoegdheden mogen door opsporingsambtenaren zelfstandig worden uitgeoefend (veelal bij geen of een geringe inbreuk, en in enkele gevallen ook bij een meer dan

[43] Gelok & De Jong 1997, Ten Geleide en p. 7.

[44] Normering hangt ook samen met inbreuk op andere grondrechten, alsmede met risico's voor de integriteit van de opsporing. Waar relevant vormen risico's voor de integriteit van de opsporing en inbreuken op andere grondrechten een zelfstandige basis voor een bepaald niveau van normering. Dit rapport richt zich vooral op de inbreuk op de privacy, omdat dit grondrecht bij de meeste opsporingsbevoegdheden het sterkst in het geding is. Waar relevant worden incidenteel ook andere grondrechten (zoals vrijheid van meningsuiting) betrokken in de overwegingen. Zie nader par. 4.2.5 over de verhouding tussen de normeringscriteria.

geringe inbreuk[45]), sommige bevoegdheden vergen een bevel van, of uitoefening door, de officier van justitie (veelal bij een meer dan geringe inbreuk), en sommige zijn onderworpen aan een machtiging van, of uitoefening door, de rechter-commissaris (veelal bij een zeer ingrijpende inbreuk). Het smartphone-arrest van de Hoge Raad van 4 april 2017 wijst ook op deze driedeling.

In het huidige wetboek is de toedeling van bevoegdheden veelal gebaseerd op de ernst van de inbreuk op grondrechten die de specifieke bevoegdheid (normaliter of gemiddeld) maakt. Deze ernst van de inbreuk wordt vooral ingeschat op basis van de samenhang met grondwettelijke bescherming (waaronder de vereisten van de artikelen 10 tot en met 13 Gw) en de beschikbare technologie en methoden voor uitoefening van de bevoegdheden, in combinatie met een contextuele inschatting van wat de burger in voor de desbetreffende bevoegdheid typische omstandigheden naar redelijkheid kan verwachten in termen van onderzoek door opsporingsinstanties. Voor de meeste bevoegdheden is de ernst wel tamelijk duidelijk, bijvoorbeeld samenhangend met een ideaaltypische of klassieke vorm van uitoefening van de bevoegdheid: doorzoeking van een voertuig is een relatief lichte bevoegdheid (denk aan de klassieke vorm van zoeken naar drugs of wapens, waarbij soms ook wat papieren of persoonlijke spullen in de auto kunnen worden aangetroffen); doorzoeking van een woning is een relatief zware bevoegdheid (denk aan de klassieke vorm van doorzoeking van de meest persoonlijke spullen en papieren die thuis worden bewaard). Sommige bevoegdheden kennen een breed spectrum aan mogelijke inbreuken, en differentiëren dan bijvoorbeeld naar de aard van gegevens (zoals bij vorderen van gegevens, waarbij identificerende gegevens een lichter regime kennen dan "gewone" gegevens, en "gevoelige" gegevens een zwaarder regime).

Bij het bepalen van de ernst van de inbreuk op grondrechten van specifieke bevoegdheden, speelt de jurisprudentie van het Europees Hof voor de Rechten van de Mens (hierna: EHRM) een belangrijke rol. Het Europees Verdrag voor de Rechten van de Mens (hierna: EVRM) is immers het belangrijkste normatieve kader voor de regulering van opsporingsbevoegdheden (belangrijker nog dan de Grondwet vanwege het grondwettelijk toetsingsverbod). Daarbij is van belang dat het EHRM expliciet kijkt naar de daadwerkelijke materiele inbreuk en de daar tegenoverstaande rechtsbescherming. De kwalificering van de zwaarte van de inbreuk in nationale wetgeving is daarbij, ondanks een marge van vrije oordeelsruimte, niet van doorslaggevend belang.[46]

Hoewel de commissie zeker EHRM-rechtspraak in haar overwegingen heeft betrokken, signaleert zij twee samenhangende factoren die de relevantie van het EVRM als belangrijkste normatieve kader verkleinen waar het gaat om adviezen voor de toekomstige regeling van opsporingsbevoegdheden, met name voor wetgeving die pas in de loop van de jaren '20 beslag moet krijgen.

De eerste factor is dat EHRM-zaken casuïstisch zijn: het Hof kijkt bij de toetsing aan artikel 8 EVRM naar alle factoren die in de onderhavige zaak relevant zijn, met nadruk op de concrete toepassing van een bevoegdheid (zoals de duur, intensiteit, plaats) en de daarbij gebruikte technologie, en met inachtneming van de nationale context en het hele stelsel van waarborgen in de nationale wetgeving. Dit maakt het op zich al niet eenvoudig om algemene conclusies te verbinden voor de concrete normering van specifieke opsporingsbevoegdheden. Dergelijke conclusies zijn nog veel moeilijker te trekken door de samenhang met de tweede factor: vanwege de doorlooptijd (van nationale rechtsmiddelen en vervolgens de procedure in

[45] Sommige bevoegdheden die een meer dan geringe inbreuk kunnen maken zijn toebedeeld aan opsporingsambtenaren en niet aan de officier van justitie, bijvoorbeeld in urgente of anderszins specifiek omlijnde situaties, zoals maatregelen ter identificatie of het onderzoek van speeksel bij verdenking van middelengebruik bij een geweldsdelict.

[46] Zie bijvoorbeeld EHRM 9 oktober 1979, Airey t. Ierland, Series A No. 41, § 26; EHRM 8 juni 1976, Engel en andere t. Nederland, Series A No. 22, § 81.

Straatsburg) betreffen EHRM-zaken veelal opsporingsactiviteiten die een jaar of vijf voor de uitspraak plaatsvonden. In die zin zien EHRM-uitspraken vooral op de (uitvoering van) wetgeving in het verleden en de doorwerking daarvan in het heden, en niet op de wetgeving in de (wat verdere) toekomst.

Voor een advies over de toekomstige regeling van technologie-gerelateerde opsporingsbevoegdheden impliceert dit dat weinig houvast kan worden gevonden in EHRM-rechtspraak, anders dan de duidelijke vaststelling dat een bepaald, hoewel niet altijd even duidelijk omlijnd, niveau van rechtsbescherming moet worden gehaald. Uitspraken over de uitoefening van opsporingsbevoegdheden in de techno-sociale context van 2013 en eerder geven weinig richting aan de wenselijke normering van opsporingsbevoegdheden in de techno-sociale context van 2024 en verder: niet alleen zal de technologie in de jaren '20 zich steeds verder doorontwikkeld hebben; ook de context waarin deze technologie zal worden toegepast kan aanzienlijk verschillen, zowel in maatschappelijk als in juridisch opzicht. Om één voorbeeld te geven: voor het gebruik van locatiebepaling door middel van GPS-trackers is *Uzun* de leidende uitspraak, een zaak uit 2010 die gaat over het gebruik van een peilbaken in 1995-1996.[47] Bij deze uitspraak heeft het Hof zich mede gebaseerd op de mogelijkheden van de gebruikte GPS-techniek in de jaren '90 en de daarmee samenhangende privacyinbreuk. Die techno-sociale context valt niet te vergelijken met die (voor zover te voorzien) van de jaren '20, en daarom kunnen uit *Uzun* nauwelijks specifieke conclusies worden getrokken over de wenselijke normering van locatiebepaling in het gemoderniseerde Wetboek van Strafvordering.

Dit betekent dat uit EHRM-rechtspraak alleen de algemene lijnen bruikbaar zijn voor de doeleinden van dit rapport: artikel 8, eerste lid, kent een brede (en dynamische) invulling van het begrip privéleven, en artikel 8, tweede lid, vergt dat inbreuken voorzienbaar zijn bij wet, wat een voldoende duidelijke wettelijke basis vergt, waarbij naarmate de inbreuk ernstiger is hogere kwaliteitseisen worden gesteld aan de wetgeving en zwaardere waarborgen nodig zijn. Onafhankelijk toezicht is in het stelsel van waarborgen van groot belang, bij voorkeur door een rechter, maar onder omstandigheden zijn ook andere vormen van onafhankelijk toezicht mogelijk. Deze lijnen hebben een leidraad gevormd in de discussies in de commissie, maar konden, in hun algemeenheid, niet als zodanig veel richting geven aan de concrete normering die voor specifieke opsporingsbevoegdheden in de (wat verdere) toekomst nodig is. Waar relevant wordt bij specifieke onderdelen (zoals bij de bespreking van het beslag op gegevens in par. 5.2) echter wel meer gedetailleerd op de verhouding met het EVRM ingegaan.

Afnemende bruikbaarheid van bestaande afbakeningscriteria

Een algemeen probleem dat ten grondslag ligt aan de problematiek van onderzoek in een digitale omgeving in de 21e eeuw, is dat het steeds moeilijker wordt om op voorhand en in abstracto te kunnen bepalen welke mate van inbreuk een bepaalde bevoegdheid maakt. De belangrijkste huidige aanknopingspunten voor normering die zijn gecondenseerd in de Grondwet en het EVRM, zoals de woning en (de inhoud van) communicatie, worden geleidelijk maar onmiskenbaar steeds minder bruikbaar om lichtere van zwaardere privacyinbreuken te onderscheiden. Enerzijds is er steeds minder logische samenhang tussen een bepaald deel van het privéleven en een bepaalde bevoegdheid die dat deel van het privéleven blootlegt: huiselijk leven kan niet alleen in beeld komen door binnentreden en doorzoeking in de woning, maar ook door het vorderen van gegevens van een slimme energiemeter; foto's, dagboeken en administratie zijn niet alleen vindbaar door een woning te doorzoeken, maar ook door inbeslagneming van een smartphone bij aanhouding; inhoud van communicatie kan niet alleen worden verkregen door aftappen of direct afluisteren, maar ook door het vorderen van opgeslagen gegevens of het onderzoek aan een smartphone; gedrag kan niet alleen worden gevolgd door

[47] EHRM 2 september 2010, Uzun t. Duitsland, App.nr. 5623/05.

stelselmatige observatie, maar ook door het monitoren van sociale media. Anderzijds wordt ook de bandbreedte groter van de mogelijke ernst van privacyinbreuken: een telecomtap vangt niet alleen de van oudsher privacygevoelige gesprekken op, maar ook triviale berichten die apparaten aan elkaar zenden ("ik ben beschikbaar"); het overnemen van informatie uit publiek toegankelijke bronnen kan zich beperken tot een lichte privacyinbreuk, maar ook dusdanige vormen aannemen dat iemands halve privéleven naar voren kan komen. Daarbij vervagen klassieke scheidslijnen die in de 20e eeuw hanteerbare aanknopingspunten boden om het privéleven af te bakenen: het huis is niet langer de plaats bij uitstek waarbinnen het privéleven zich afspeelt, het lichaam raakt verbonden met de omgeving door technologie, en wat over een communicatie-infrastructuur gaat is niet beperkt tot gesprekken of berichten die mensen uitwisselen maar omvat allerlei vormen van gegevensverkeer.[48] En daarbovenop betekent de ontwikkeling van data mining en Big Data Analytics dat nieuwe informatie kan worden afgeleid uit bestaande data, wat onder andere betekent dat gevoelige gegevens (zoals iemands politieke voorkeur of medische conditie) kunnen worden afgeleid uit alledaagse gegevens en metadata (zoals iemands zoek- of aankoopgedrag of "vind ik leuk"-klikgedrag).[49]

Bij elkaar betekenen deze ontwikkelingen dat het moeilijker wordt om bij de vormgeving van opsporingsbevoegdheden op voorhand, dus in de wet, een vast beschermingsniveau te koppelen aan een bepaalde bevoegdheid. Het zal veelal van de context afhangen of bij de uitoefening van een bevoegdheid op voorhand redelijkerwijs voorzienbaar is dat een geringe, een meer dan geringe of een zeer ingrijpende inbreuk op de privacy zal worden gemaakt. Uit deze constatering heeft de commissie twee samenhangende conclusies getrokken. De eerste is dat de normering in het gemoderniseerde wetboek zal moeten werken met (tamelijk) abstracte criteria, die van geval tot geval geïnterpreteerd moeten en kunnen worden. De tweede is dat het wenselijk is om deze tamelijk abstracte normering meer systematisch door te voeren in het stelsel van bevoegdheden, nu het minder dan voorheen mogelijk is om op voorhand een zekere rangorde aan te brengen in bevoegdheden in termen van intrinsieke mate van ingrijpendheid. Het hanteren van hetzelfde of een vergelijkbaar criterium bij verschillende bevoegdheden kan helpen om de rechtszekerheid te vergroten en onderlinge consistentie van de interpretatie in de rechtspraktijk te bevorderen.

4.2.2. Het voorgestelde criterium van stelselmatigheid en ingrijpende stelselmatigheid

De uitdaging is een criterium te vinden voor onderzoek in een digitale omgeving dat onderscheid maakt tussen geringe, meer dan geringe en zeer ingrijpende inbreuken, waarbij dat onderscheid zowel zingevend (in de zin dat het een materieel criterium op abstract niveau biedt, dat verklaart waarom er verschil is in inbreuk en dat een interpretatiekader geeft bij onvoorziene gevallen) als werkbaar is (in de zin dat het operationaliseerbaar is en voldoende houvast geeft aan de praktijk in concrete zaken). Deze twee vereisten kennen een zeker spanningsveld: een zingevend criterium neigt meer naar abstractie, waarmee conceptuele helderheid kan worden bereikt, terwijl een werkbaar criterium meer neigt naar concreetheid, waarbij duidelijk is welke specifieke factoren het criterium handen en voeten geven. In dit spanningsveld adviseert de commissie om in elk geval het eerste aspect – conceptuele helderheid – zwaar te laten wegen. De reden hiervoor is dat het de bedoeling is dat het systeem van het gemoderniseerde wetboek relatief duurzaam is en bij voorkeur gedurende enkele decennia relevant blijft. Het is volstrekt niet te overzien hoe de technische maar ook sociale ontwikkelingen Nederland in de komende 25 jaar zullen veranderen; dat maakt het riskant, om niet te zeggen onmogelijk, om op dit moment concrete criteria en factoren te formuleren die ook over tien of twintig jaar nog relevant zijn om de ernst van privacyinbreuken van bevoegdheden te duiden. Een duurzamer benadering is om een materieel criterium te formuleren dat voldoende abstract is om toekomstvast te

[48] Voor een nadere probleemanalyse, zie Koops 2014. Vgl. ook Koops 2017.
[49] Kosinski e.a. 2013.

kunnen zijn, dat conceptueel hout snijdt, en daarmee een goed aanknopingspunt biedt voor een dynamische maar consistente interpretatie in de toekomst. Dit betekent dat de commissie ervoor kiest om in de wet een abstract criterium te hanteren, en in de toelichting duiding te geven aan dit criterium aan de hand van factoren en voorbeelden die voor de komende jaren relevant zijn, waarbij het aan de rechtspraktijk en rechtsontwikkeling wordt overgelaten om het abstracte criterium nader in te vullen en deze invulling te laten mee-ontwikkelen met verdere toekomstige ontwikkelingen in technologie en maatschappij.

In **stelselmatigheid** heeft de commissie een bruikbaar aanknopingspunt gevonden voor het gezochte criterium. Dit criterium wordt reeds gehanteerd bij enkele bijzondere opsporingsbevoegdheden (BOB). Het algemeen aanvaarde idee is dat een specifieke wettelijke bepaling nodig is wanneer sprake is van een "meer dan geringe inbreuk op de persoonlijke levenssfeer" (of bij inbreuken op andere grondrechten, of wanneer de inzet een bijzonder risico oplevert voor de integriteit van de opsporing; zie daarover par. 4.2.5). Dit wordt ingevuld met de bekende formule van een "min of meer compleet beeld van een of meer aspecten van het persoonlijk leven". Hierbij loopt de "meer dan geringe inbreuk" feitelijk gelijk op aan het begrip "stelselmatig". Zie bijvoorbeeld de passage in paragraaf 10.4.1 van de concept-memorie van toelichting (p. 60) bij Boek 2: "De inbreuk op de persoonlijke levenssfeer is bij niet-stelselmatige vastlegging beperkt. Dit wordt anders indien het onderzoek in open bronnen zo intensief en diepgaand is dat een min of meer volledig beeld van bepaalde aspecten van het persoonlijk leven ontstaat. In dat geval is een uitdrukkelijke wettelijke grondslag vereist." Ook bij stelselmatige observatie en stelselmatige inwinning van informatie is de term "stelselmatig" het kerncriterium waarmee de "geringe inbreuk" wordt onderscheiden van de "meer dan geringe" inbreuk.

Hieruit blijkt dat de term "stelselmatig" voor de toepassing van deze bevoegdheden sterk samenhangt met de notie van een "meer dan geringe inbreuk". Wanneer er sprake is van een meer dan geringe inbreuk is er dan dus (voor wat betreft het grondrecht op bescherming van de persoonlijke levenssfeer[50]) bij de genoemde bevoegdheden min of meer per definitie sprake van stelselmatigheid. De term moet dan ook in dit licht bezien worden, en niet vanuit het normale spraakgebruik.[51] "Stelselmatig" omvat handelingen die in het normale spraakgebruik niet als stelselmatig gezien zouden worden, maar in juridische zin wel tot gevolg hebben dat een "meer dan geringe inbreuk" wordt gepleegd. Een duidelijk voorbeeld is het bevragen van publiek toegankelijke bronnen: met een eenmalige zoekactie kan een flink beeld worden verkregen van het persoonlijk leven van de verdachte. Ook een kortdurende observatie met een technisch hulpmiddel in een bordeel is naar juridische maatstaven stelselmatig.[52] Hoewel in het normale spraakgebruik deze acties vermoedelijk door veel mensen niet als stelselmatig zouden worden gekenschetst, gelden ze juridisch wel als stelselmatig, omdat ze een meer dan geringe privacyinbreuk opleveren; dat wordt verwoord met het materiële criterium dat er een min of meer volledig beeld van bepaalde aspecten van iemands privéleven kan ontstaan. Deze juridische invulling moet in gedachten worden gehouden bij het bepalen van het verdere gebruik van deze term.

[50] Van een meer dan geringe inbreuk kan ook sprake zijn bij andere grondrechten, zoals de vrijheid van meningsuiting; daarvoor is het criterium van stelselmatigheid, in de betekenis van een min of meer volledig beeld van bepaalde aspecten van het persoonlijk leven, als zodanig niet geschikt. In die zin is stelselmatigheid een voldoende maar niet een noodzakelijke voorwaarde om te spreken van een "meer dan geringe inbreuk", zie par. 4.2.5.

[51] Van Dale (www.vandale.nl, laatst geraadpleegd 1 juni 2018) geeft als betekenis van *stelselmatig*: "1. systematisch; 2. voortdurend en opzettelijk."

[52] *Kamerstukken II* 1997/98, 25 403, nr. 7, p. 47.

Niet alleen bij enkele huidige BOB-bevoegdheden komt stelselmatigheid als criterium voor. Het is ook (impliciet[53]) gebruikt door de Hoge Raad in het smartphone-arrest om de ernst van de privacyinbreuk te duiden. Het criterium heeft daarmee de potentie getoond om breed toepasbaar te zijn, niet alleen bij bijzondere (of heimelijke) bevoegdheden, maar ook bij digitale doorzoekings- en beslagbevoegdheden. Daarbij heeft het ook de potentie om de onderlinge systematiek en consistentie binnen het wetboek te bevorderen. Het is een abstract, materieel criterium: de uitoefening van een bevoegdheid is stelselmatig als daarbij op voorhand redelijkerwijs voorzienbaar een min of meer volledig beeld van bepaalde aspecten van iemands privéleven kan ontstaan.

Met "op voorhand redelijkerwijs voorzienbaar" wordt hierbij aangeduid dat de vraag of uitoefening van een bevoegdheid stelselmatig is, wordt gesteld en beantwoord voorafgaand aan de inzet, gebaseerd op de voorgenomen acties tot vergaring en verwerking van gegevens en alle overige omstandigheden van het geval, waaronder de reeds uit het dossier bekende informatie over de verdachte (en over eventuele derden van wie redelijkerwijs voorzienbaar gegevens in beeld zouden komen). "Redelijkerwijs voorzienbaar" is daarbij een geobjectiveerd criterium: het gaat om wat een opsporingsfunctionaris in casu redelijkerwijs zou moeten voorzien, aan de hand van algemene en context-specifieke ervaringsregels en van een redelijke inschatting van de omstandigheden van het geval. Indien de uitoefening van een bevoegdheid leidt tot een min of meer volledig beeld van bepaalde aspecten van iemands privéleven, terwijl dat niet op voorhand redelijkerwijs voorzienbaar was, maakt dat die uitoefening niet met terugwerkende kracht stelselmatig, en is het dus ook niet met terugwerkende kracht onrechtmatig als niet was voldaan aan de desbetreffende vereisten bij stelselmatigheid. Onvoorzienbaar aangetroffen gegevens gelden als bijvangst en kunnen onder de bestaande regels voor de omgang met bijvangst worden gebruikt voor het bewijs.[54] Onvoorziene informatie die (al dan niet ingrijpende, zie onder) stelselmatigheid oplevert, maar niet relevant is voor het opsporingsonderzoek, moet buiten het opsporingsdossier blijven. Dit leidt er niet als zodanig toe dat een hogere autoriteit bij het vervolgen van het onderzoek zou moeten worden betrokken. Wel moet het feit dat onvoorzienbare gegevens zijn aangetroffen worden meegewogen bij de inschatting van de (al dan niet ingrijpende) stelselmatigheid van het vervolgonderzoek: gaat het echt om een incidentele vondst, dan zal het vervolgonderzoek niet meer of minder (ingrijpend) stelselmatig zijn dan voorheen. Gaat het echter – met de kennis van nu – om een indicatie dat er meer of gevoeliger gegevens aanwezig zijn dan eerder was ingeschat, in zodanige mate dat er een reële kans bestaat dat bij vervolgonderzoek nogmaals dergelijke gegevens in beeld kunnen komen, dan zal er wel sprake zijn van (al dan niet ingrijpende) stelselmatigheid en een hogere autoriteit moeten worden ingeschakeld.

Belangrijk is verder te benadrukken dat het gaat om *bepaalde aspecten* van iemands privéleven; het is voor stelselmatigheid niet relevant of een groot deel van iemands privéleven in beeld komt, het gaat erom dat een bepaald deel (vaak samenhangend met een bepaalde rol die iemand heeft in het sociale leven, zoals vader, leraar, golfer, gebedshuisganger, kroegbezoeker) min of meer volledig naar voren komt (door bijvoorbeeld een beeld te vormen van alle contacten binnen die sociale hoedanigheid).

Stelselmatigheid is een criterium dat het omslagpunt tussen geringe en meer dan geringe inbreuken definieert. Daarmee is het geschikt om de eerste twee delen van de driedeling in de bevoegde autoriteit die toestemming moet geven voor de uitoefening van een bevoegdheid (zie par. 4.2.1, begin), van elkaar te onderscheiden: het kan (ook bij andere dan de huidige of in het

[53] In HR 4 juni 2017 ECLI:NL:HR:2017:584 wordt de term "stelselmatig" zelf niet gebruikt, maar wel de geaccepteerde uitleg van dit criterium: "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."

[54] Zie ook par. 6.4.3 onder "Gaat het om de verwachting vooraf of het resultaat achteraf?"

wetsvoorstel voorgestelde nieuwe bevoegdheden waarin het begrip "stelselmatig" voorkomt) gebruikt worden als algemeen criterium om te bepalen of – in de regel – een bevoegdheid zelfstandig door een opsporingsambtenaar of op bevel van een officier van justitie kan worden uitgeoefend.[55] Voor het omslagpunt tussen het tweede en derde deel – oftewel de vraag wanneer een inbreuk op de persoonlijke levenssfeer zeer ingrijpend zal zijn en dus een machtiging van de rechter-commissaris is aangewezen bovenop een bevel van de officier van justitie – is een aanvullend criterium nodig. Hiervoor stelt de commissie het criterium voor van **ingrijpende stelselmatigheid**, dat op dezelfde manier wordt ingevuld als het criterium van stelselmatigheid, maar dan met een extra voorwaarde die aanduidt dat het om een zeer ingrijpende privacyinbreuk gaat. Uitoefening van een bevoegdheid is ingrijpend stelselmatig als daarbij op voorhand redelijkerwijs voorzienbaar een ingrijpend beeld van iemands privéleven kan ontstaan. Deze ingrijpendheid kan op twee alternatieve[56] manieren naar voren komen.

Ten eerste kan een ingrijpend beeld van iemands privéleven ontstaan als een min of meer volledig beeld ontstaat van een wezenlijk deel van iemands privéleven; de ingrijpendheid bestaat hier uit een *diepe* kijk in iemands privéleven, waarbij een wezenlijk deel naar voren komt. Het deelcriterium "wezenlijk" is geïnspireerd op de nadruk op identiteit in het Nederlandse privacybegrip: het gaat om "onbevangen *jezelf* kunnen zijn". Wezenlijke onderdelen van iemands privéleven zijn juist die delen die nauw samenhangen met iemands zelfbegrip ("wie ben ik?"). Zo zal de uitoefening van een bevoegdheid waarbij op voorhand redelijkerwijs voorzienbaar is dat "gevoelige" persoonsgegevens worden overgenomen, onder bepaalde omstandigheden kunnen raken aan een wezenlijk deel van iemands privéleven (namelijk diens medische, seksuele, religieuze, politieke of etnische identiteit). (Er is echter geen intrinsieke koppeling tussen wezenlijke ingrijpendheid en gevoelige persoonsgegevens, zie par. 4.2.3 op p. 42.) Het begrip "wezenlijk" sluit ook aan bij criteria die andere rechtsstelsels hanteren voor de meest ingrijpende inbreuk: Canada onderscheidt een "biografische *kern*",[57] Duitsland hanteert een "*kern*bereik" van de persoonlijke levenssfeer en een verbod op een "compleet *persoonlijkheids*profiel" als criterium: termen waarmee wordt aangeduid dat de kern – het *wezen* – van iemands leven wordt geraakt.[58]

Ten tweede kan een ingrijpend beeld van iemands privéleven ontstaan als een min of meer volledig beeld tot stand komt van een aanzienlijk deel van iemands privéleven; de ingrijpendheid bestaat hier uit een *brede* kijk in iemands privéleven, waarbij meerdere delen min of meer volledig naar voren komen, samenhangend met verschillende rollen in het sociale leven, zoals iemands gezinsleven, werk, sport, verenigingsleven, uitgaansleven, vriendenkringen, consumentengedrag en relatie met dienstverleners. Wanneer één deel van iemands privéleven min of meer volledig in beeld komt, is er sprake van stelselmatigheid; gaat het om een significant aantal aspecten dat bij elkaar een aanzienlijk deel van iemands leven blootlegt, dan is er sprake van ingrijpende stelselmatigheid. Wat een significant aantal inhoudt, is niet precies te zeggen; dat

[55] In de regel, aangezien weliswaar de officier van justitie veelal de aangewezen autoriteit is bij een meer dan geringe inbreuk (die hier samenvalt met het criterium van stelselmatigheid), maar in bepaalde, specifieke gevallen de wetgever ook een opsporingsambtenaar kan aanwijzen als bevoegde autoriteit bij een meer dan geringe inbreuk.

[56] Dat wil zeggen: niet-cumulatieve. Een ingrijpend beeld kan diep zijn, of breed, of (maar niet noodzakelijk) diep én breed.

[57] Zie bijvoorbeeld R. v. Plant [1993] 3 S.C.R. 281, p. 293: "it is fitting that s. 8 of the Charter should seek to protect *a biographical core* of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual" (cursivering toegevoegd).

[58] Zie bijvoorbeeld art. 100a lid 4 StPO (verwijzend naar een "Kernbereichs privater Lebensgestaltung") en Lindemann & Van Toor 2018 over dit Duitse begrip; en BVerfG 12 april 2005, Az. 2 BvR 581/01, Rn. 59 ("dass eine von Verfassungs wegen stets unzulässige 'Rundumüberwachung' (…), mit der ein umfassendes *Persönlichkeits*profil eines Beteiligten erstellt werden könnte, durch allgemeine verfahrensrechtliche Sicherungen auch ohne spezifische gesetzliche Regelung grundsätzlich ausgeschlossen sein werde", cursivering toegevoegd).

hangt af van de persoon, maar ook van de volledigheid van het beeld: een zeer volledig beeld van twee aspecten van iemands privéleven zal al ingrijpend kunnen zijn, een minder volledig beeld van drie aspecten hoeft dat niet te zijn. Waar het vooral om gaat is dat informatie uit verschillende contexten van iemands leven bij elkaar wordt gelegd op een manier dat het beeld als geheel ingrijpend wordt, zonder dat de informatie uit elk van die contexten op zichzelf ingrijpend is; zoals Nissenbaum aangeeft, ontstaan privacyinbreuken met name wanneer informatie uit een bepaalde context met een andere context vermengd raakt,[59] en het vermengen van substantiële informatie (het min of meer volledige beeld) uit meerdere contexten (een significant aantal delen van iemands leven) vormt daarom een zeer ingrijpende inbreuk op iemands privacy.

Het gekozen criterium van (ingrijpende) stelselmatigheid sluit goed aan bij de beeldspraak van de mozaïektheorie – één van de nieuwe raamwerken voor de conceptualisering van privacy die is voorgesteld om te vangen wat privacy inhoudt in een 21e eeuw waarin oude conceptualiseringen, zoals het onderscheid binnenshuis/publieke ruimte of inhoud/metadata, sterk aan betekenis inboeten.[60] De mozaïektheorie komt er kort gezegd op neer dat, voor de beoordeling van de mate van een privacyinbreuk, niet moet worden gekeken naar losse steentjes, maar naar het beeld dat ontstaat als je de nodige steentjes bij elkaar legt. De theorie is ontwikkeld en toegepast in Amerikaanse zaken over GPS-tracking, waarin gesteld is dat de privacyinbreuk van het traceren van de bewegingen van een auto gedurende een bepaalde periode niet moet worden beoordeeld op basis van het argument dat de auto op elk willekeurig moment in de publieke ruimte rondrijdt en iedereen die auto op dat moment ergens zou kunnen zien (en dat er daarom geen redelijke privacyverwachting zou bestaan in de locatiegegevens van de auto), maar op basis van het totale beeld dat ontstaat uit het traceren van de bewegingen over de hele periode; bij dat totaalplaatje bestaat wel een redelijke verwachting van privacy:

> unlike one's movements during a single journey, the whole of one's movements over the course of a month is not *actually* exposed to the public because the likelihood anyone will observe all those movements is effectively nil. Second, the whole of one's movements is not exposed *constructively* even though each individual movement is exposed, because that whole reveals more—sometimes a great deal more—than does the sum of its parts.[61]

In feite is het criterium van stelselmatigheid een vroege voorloper van de mozaïektheorie: het legt immers de nadruk op de volledigheid van het beeld dat ontstaat bij de uitoefening van een heimelijke bevoegdheid. Het in dit advies voorgestelde criterium bouwt hier naadloos op voort: bij een niet-stelselmatige uitoefening van een bevoegdheid worden slechts losse steentjes verzameld en bekeken; bij een stelselmatige uitoefening van een bevoegdheid ontstaat, door steentjes samen te leggen, een bepaald beeld ("mozaïek") van een persoon; bij een ingrijpend stelselmatige uitoefening van een bevoegdheid ontstaat een ingrijpend beeld van een persoon, dat zicht geeft op diens wezen (diep) of op een aanzienlijk deel van diens privéleven (breed). In mozaïekbeeldspraak: de nodige steentjes tezamen vormen een portret van iemand, en dat portret kan ingrijpend zijn als je – zoals bij een Rembrandt-portret – door iemands ogen naar binnen kunt kijken (diep), of als het een portret ten voeten uit betreft (breed).

[59] Nissenbaum 2010.

[60] Zie Koops, Newell & Škorvánek 2019 voor een analyse van oude en nieuwe raamwerken voor de beoordeling van privacyinbreuken in de context van stelselmatige locatiebepaling.

[61] United States v. Maynard, 615 F.3d 544, 558 (D.C.Cir. 2010). In cassatie werd de mozaïekredenering niet overgenomen door de meerderheid van het Supreme Court, die de privacyinbreuk niet baseerde op de redelijke privacyverwachting maar op de inbreuk op het eigendomsrecht van de auto, maar werd deze wel gehanteerd in de twee *concurring opinions*: United States v. Jones, 565 U.S. 400 (2012), 417-18 (Sotomayor, *concurrence*), 428-31 (Alito, *concurrence*).

Samenvattend stelt de commissie een algemeen normeringscriterium voor van (ingrijpende) stelselmatigheid:

1. *niet-stelselmatige* uitoefening van een bevoegdheid is mogelijk door een opsporingsambtenaar;
2. voor *stelselmatige* uitoefening van een bevoegdheid is in de regel[62] een bevel van de officier van justitie nodig; stelselmatig betekent dat bij de uitoefening van een bevoegdheid op voorhand redelijkerwijs voorzienbaar een min of meer volledig beeld van bepaalde aspecten van iemands privéleven kan ontstaan;
3. voor *ingrijpend stelselmatige* uitoefening van een bevoegdheid is een machtiging van de rechter-commissaris nodig; ingrijpend stelselmatig betekent dat bij de uitoefening van een bevoegdheid op voorhand redelijkerwijs voorzienbaar een ingrijpend beeld van iemands privéleven kan ontstaan.

Aanbeveling 6: de wetgever dient in de normeringssystematiek ten aanzien van bevoegdheden in een digitale omgeving (Hoofdstukken 7 en 8 van Boek 2) een algemeen normeringscriterium te hanteren van (ingrijpende) stelselmatigheid, dat in brede zin kan worden gebruikt om onderscheid te maken tussen geringe, meer dan geringe en zeer ingrijpende inbreuken en het daarmee (in de regel) samenhangende onderscheid tussen opsporingsambtenaar, officier van justitie en rechter-commissaris als bevoegde autoriteit. → *p. 194*

4.2.3. Toepassingsbereik en uitwerking

Zoals in par. 4.2.1. toegelicht, is het wenselijk om het voorgestelde criterium breder te hanteren dan alleen bij het onderzoek in/aan geautomatiseerde werken en digitale-gegevensdragers. De systematiek en onderlinge consistentie in het wetboek kunnen worden versterkt door het criterium bij meerdere bevoegdheden te hanteren, bijvoorbeeld ook bij de bestaande heimelijke bevoegdheden die reeds stelselmatigheid hanteren, waardoor de rechtsontwikkeling sneller op gang kan komen, kruisbestuiving kan ontstaan bij de interpretatie van de privacyinbreuk bij verschillende bevoegdheden, maar ook maatwerk kan worden geleverd door bevoegdheidsspecifieke interpretatie van het abstracte criterium.

Om te beginnen kan voor de interpretatie van "stelselmatig" deels worden aangesloten bij de bestaande interpretatie in wetgeving en jurisprudentie, die vooral ontwikkeld is in de rechtspraak betreffende stelselmatige observatie: het gaat om een samenstel van factoren als gebruik van een technisch hulpmiddel, plaats, frequentie, intensiteit en duur. De bestaande jurisprudentie, die met name ontwikkeld is in het kader van stelselmatige observatie, is echter maar van beperkte relevantie voor andere bevoegdheden dan stelselmatige observatie, met name waar het digitale vormen van onderzoek betreft. Plaats is weinig relevant bij mobiele apparaten, en duur zegt niets als in luttele seconden grote hoeveelheden data kunnen worden overgenomen en geautomatiseerde zoekopdrachten binnen fracties van seconden informatie opleveren. Voor de interpretatie van stelselmatigheid in andere contexten dan stelselmatige observatie moet daarom een nieuw factorenkader worden ontwikkeld dat is aangepast aan de context van digitaal onderzoek. Te denken valt bijvoorbeeld aan een samenstel van factoren als de hoeveelheid, aard en geautomatiseerde onderzoekbaarheid van de gegevens, type drager, wijze van opslag, en automatisering van het onderzoek. In de paragraaf over onderzoek van publiek toegankelijke bronnen wordt nader uitgewerkt welke factoren specifiek voor dat type onderzoek een rol kunnen spelen.

[62] Zie noten 45 en 55 over mogelijke uitzonderingen op de regel.

Verder stelt de commissie voor dat het onderzoeken van gegevens altijd als ingrijpend stelselmatig moet worden gekwalificeerd als daarbij redelijkerwijs voorzienbaar gegevens worden onderzocht[63] die onder het beroepsmatig verschoningsrecht vallen; dergelijk onderzoek is dus alleen mogelijk met machtiging van de rechter-commissaris (naast de aanvullende voorwaarden die samenhangen met de geheimhoudersbescherming), conform de regeling in Afdeling 7.6.2 van het conceptwetsvoorstel.[64] Het betreft immers gegevens die bij uitstek bestemd zijn om uitsluitend binnen de context van de relatie met de dienstverlener te worden gebruikt, waardoor het buiten de context halen van deze gegevens per definitie een zeer ingrijpende inbreuk is. Daarnaast betreft het vaak met een zekere waarschijnlijkheid (afhankelijk van de aard van de geheimhouder) gevoelige gegevens betreffende gezondheid, religieuze overtuiging of strafrechtelijke persoonsgegevens.

Buiten gegevens die onder het beroepsmatig verschoningsrecht vallen, is het niet mogelijk om eenduidige factoren te formuleren die één-op-één samenhangen met stelselmatigheid of ingrijpende stelselmatigheid. De commissie heeft hierover uitvoerig gediscussieerd, maar heeft geen concrete factoren kunnen vaststellen die in alle gevallen wijzen op ingrijpende stelselmatigheid. Voorbeelden komen vaak neer op een samenhang met gevoelige persoonsgegevens, maar gevoelige persoonsgegevens leveren lang niet altijd een ingrijpend beeld van iemands privéleven op. In een bepaalde context kan een foto een gevoelig persoonsgegeven betreffen dat een wezenlijk deel van iemands privéleven blootlegt, zoals een foto van een voetballer die seks heeft met een man, terwijl hij voor de buitenwereld en een deel van zijn omgeving en collega's als hetero door het leven gaat; in die context levert een dergelijke foto zeer privacygevoelige informatie op. Maar een foto van twee zoenende mannen die breed bekend staan als homoseksueel, is niet privacygevoelig voor zover het de seksuele voorkeur betreft; dat levert dus geen ingrijpend beeld van de personen op, omdat deze informatie al in de publieke sfeer is. Dat ligt echter weer anders als de foto een bekende heteroseksuele christelijke politicus betreft die bekend staat om zijn pleidooien voor monogamie, terwijl de vrouw op de foto niet zijn echtgenote is; in dat geval levert de foto wel een ingrijpend beeld van het privéleven op, omdat het een wezenlijk deel van zijn privéleven – zijn buitenechtelijke seksuele leven – blootlegt dat nog niet bekend was.

Maar bij al deze voorbeelden moet worden aangetekend dat de ingrijpende stelselmatigheid wordt bepaald aan de hand van wat op voorhand redelijkerwijs voorzienbaar is gelet op de voorgenomen acties tot vergaring en verwerking van gegevens; het valt bij de christelijke politicus niet te voorzien dat foto's naar boven zouden komen van seksuele contacten met andere vrouwen dan zijn echtgenote (men verwacht immers dat hij zelf ook monogaam is); het

[63] Hierbij wordt gedoeld op onderzoek waarbij door een opsporingsambtenaar van de inhoud van een bericht van of aan een verschoningsgerechtigde kennisgenomen wordt. Het enkele feit dat iemand mogelijk een bericht van een verschoningsgerechtigde op zijn telefoon heeft staan, maakt niet dat het kopiëren en onderzoeken van die telefoon daarmee altijd met machtiging van de rechter-commissaris dient plaats te vinden. Als de verwachting is dat het onderzoek niet leidt tot kennisname van de inhoud, dan is het onderzoek niet als zodanig ingrijpend stelselmatig.

[64] Onder onderzoek wordt in dit verband verstaan een handeling die gepaard gaat met het kennisnemen van de inhoud van de gegevens. Het is dit kennisnemen dat inbreuk maakt op de geheimhoudersbescherming. Het vastleggen van een verzameling gegevens waaronder zich redelijkerwijs voorzienbaar ook geheimhoudergegevens kunnen bevinden, zoals het maken van een image van een geautomatiseerd werk waarop een bedrijfsadministratie staat (en waarop dus vaak ook stukken van een notaris of advocaat zullen staan), is niet als zodanig ingrijpend stelselmatig voor zover het vastleggen niet gepaard gaat met kennisneming van de inhoud. Het voorstel van de commissie sluit voor wat betreft de kwalificatie van geheimhoudergegevens als ingrijpend stelselmatig dus aan op de voorgestelde regeling in afdeling 7.6.2 van het conceptwetsvoorstel. Zie bijvoorbeeld artikel 2.7.6.2.3.1, dat bepaalt dat in het geval gegevens of gegevensdragers bij niet-professioneel verschoningsgerechtigden in beslag worden genomen (of, in termen van dit advies, gegevens worden vastgelegd) de opsporingsambtenaar zich onthoudt van kennisneming vanaf het moment dat het redelijke vermoeden ontstaat dat het professioneel verschoningsrecht zich over een voorwerp of gegeven uitstrekt.

vinden van een dergelijke foto op de smartphone maakt het onderzoek daarom niet met terugwerkende kracht ingrijpend stelselmatig, en maakt het onderzoek dus ook niet met terugwerkende kracht onrechtmatig als er geen rechterlijke machtiging was – de foto is bijvangst en kan als zodanig worden gebruikt voor het bewijs, onder de bestaande regels voor de omgang met bijvangst.

Daarbij komt dat gegevensdragers als smartphones regelmatig enkele, en vaak een aanzienlijk aantal, gevoelige gegevens zullen bevatten: foto's kunnen blijk geven van iemands seksuele leven; opgeslagen (bijvoorbeeld koosjere of halal) recepten of boodschappenlijstjes kunnen religie reflecteren; app-berichten en opgeslagen favorieten kunnen politieke voorkeur of medische gegevens weergeven; opgeslagen gegevens uit *self-tracking*-applicaties (bijvoorbeeld hartslag tijdens joggen) geven inzicht in iemands gezondheidstoestand. Daarbij is niet alleen van belang dat, als hiervoor aangegeven, niet alle gegevens die in de dataprotectiewetgeving als "bijzonder" (oftewel gevoelig) worden aangemerkt, ook daadwerkelijk in de desbetreffende context van het opsporingsonderzoek bijzonder privacygevoelig zullen zijn – van de verdachte zal immers veelal de etnische afkomst, religieuze overtuiging en seksuele gerichtheid al wel bekend zijn bij de opsporingsdienst, en het redelijkerwijs voorzienbaar kunnen aantreffen van dergelijke gegevens legt daarom geen nieuw wezenskenmerk bloot. Daarbij is vooral van belang in welke mate redelijkerwijs verwacht kan worden dat de zoekactiviteiten eventuele gevoelige gegevens zullen opleveren die relevant zijn voor het onderzoek en in het onderzoeks- en procesdossier terecht zouden komen. De opname van nieuw of aanvullend aangetroffen gevoelige gegevens in het procesdossier verhoogt de kans dat deze een rol zullen spelen in het verdere onderzoek. Met name bij opname in het procesdossier zullen de gegevens een rol kunnen spelen in de bewijsvoering, en bijvoorbeeld ter zitting worden bediscussieerd, waardoor ze ook ter kennis kunnen komen van personen uit de omgeving van de verdachte, die niet altijd op de hoogte zijn van het desbetreffende wezenskenmerk (bijvoorbeeld van een bekeerde moslim), of van de manier waarop dit kenmerk tot uitdrukking komt in de privéactiviteiten van de verdachte (bijvoorbeeld het deelnemen aan een christelijke jongerenpraatgroep). Het is juist de mogelijke weerslag op het sociale leven van de verdachte die de zogenoemde gevoelige gegevens in dergelijke situaties ook daadwerkelijk *gevoelig* maken. Dit betekent ook dat wanneer het wezenskenmerk – bijvoorbeeld de religieuze overtuiging, de politieke voorkeur, het seksuele leven, of de gezondheidstoestand – algemeen of breed bekend is, de redelijke verwachting gevoelige gegevens te zullen aantreffen die relevant zijn voor het onderzoek en die in het dossier terecht kunnen komen, het onderzoek niet ingrijpend stelselmatig maakt. De (naar verwachting) nieuw aan te treffen gevoelige gegevens bevestigen in dergelijke gevallen slechts het bestaande beeld, en doen geen ingrijpend beeld van het privéleven *ontstaan*.

Verder is van belang dat de vele gevoelige gegevens die op een smartphone kunnen staan, lang niet altijd redelijkerwijs voorzienbaar ook daadwerkelijk naar boven komen bij het onderzoek aan de smartphone-gegevens. Het zal dan ook afhangen van het type zoekvragen, de typen bestanden waarin voorzienbaar gezocht zal worden en de intensiteit en omvang van het voorgenomen onderzoek, of redelijkerwijs voorzienbaar is dat gegevens naar voren komen die (afzonderlijk of in samenhang) een wezenlijk deel van iemands privéleven blootleggen. Daarbij zal vooral de *gerichtheid* van het voorgenomen onderzoek, en dus de specificiteit van de zoekvragen, een belangrijke rol spelen. Gerichte zoekvragen in bepaalde mappen of apps van de smartphone die samenhangen met drugshandel zullen niet redelijkerwijs voorzienbaar koosjere recepten, GroenLinks-likes of fitbit-data in beeld brengen. Naarmate het onderzoek echter ongerichter wordt – dus naarmate gewerkt wordt met algemenere zoektermen en daarbij veel of alle onderdelen van de smartphone bevraagd worden – neemt de kans aanmerkelijk toe dat gevoelige gegevens in beeld komen. Dat maakt het onderzoek nog niet per definitie ingrijpend stelselmatig (omdat als gezegd het enkele redelijkerwijs voorzienbaar aantreffen van gevoelige persoonsgegevens niet per se een wezenlijk deel van iemands privéleven blootlegt),

maar een onderzoek dat zich uitstrekt over alle of de meeste gegevens op de smartphone levert wel een grotere kans op dat gegevens in beeld komen die een wezenlijk deel van iemands privéleven blootleggen dat nog niet algemeen of breed bekend is. De (on)gerichtheid van het onderzoek is daarom een relevante factor bij het beantwoorden van de vraag of er sprake is van ingrijpende stelselmatigheid.

Verder kan ingrijpende stelselmatigheid niet worden vereenzelvigd met gevoelige persoonsgegevens omdat soms ook sprake kan zijn van ingrijpendheid zonder dat gevoelige persoonsgegevens worden overgenomen. Zo kan een jongen die deel uitmaakt van een *street gang* een bepaald imago willen ophouden om deel uit te maken van deze groep, maar in de beslotenheid van zijn slaapkamer en iPhone luisteren naar Jan Smit en streekromans lezen – muziek en boeken waarbij hij zichzelf kan zijn omdat hij zich van binnen een romanticus voelt, maar waarvan hij niet wil dat deze informatie bij zijn vrienden bekend raakt. De identiteit die samenhangt met het onbevangen jezelf kunnen zijn hoeft dus niet altijd gevoelige persoonsgegevens te betreffen. Tegelijkertijd zal de aanwezigheid van dergelijke informatie op iemands smartphone in verreweg de meeste gevallen niet betekenen dat er sprake is van ingrijpende stelselmatigheid – het is immers nauwelijks redelijkerwijs voorzienbaar dat a) iemand gegevens op de smartphone heeft die zijn innerlijke leven weerspiegelen maar die in strijd zijn met het imago dat hij ophoudt voor zijn omgeving, en b) dat deze gegevens met de voorgenomen zoekacties in beeld komen. Alleen in zeldzame uitzonderingsgevallen zal dit het geval zijn, bijvoorbeeld als uit contextinformatie – zoals een getuigenverklaring of eerdere observaties – bekend is dat de verdachte een bepaald wezenlijk deel van zijn leven geheim houdt voor zijn omgeving en wanneer redelijkerwijs voorzienbaar is dat de te zoeken, voor het onderzoek relevante, informatie op de smartphone samenhangt met dat geheime deel van het leven van de verdachte.

Kortom, de enkele verwachting dat gevoelige gegevens zullen worden overgenomen of bij onderzoek naar boven kunnen komen, zal nooit een voldoende reden zijn om van ingrijpende stelselmatigheid te spreken. Het zal altijd afhangen van de context, de omstandigheden van het geval en de voorgenomen wijze en omvang van zoeken welke mate van privacyinbreuk redelijkerwijs voorzienbaar is. Bovenstaande uitleg geeft ook aan dat er slechts in uitzonderingsgevallen sprake zal zijn van ingrijpende stelselmatigheid. Er moet worden gekeken naar de informatie die reeds binnen een onderzoek bekend is en naar de verwachting dat, naar ervaringsregels, de voorziene uitoefening van een bepaalde bevoegdheid in aanvulling op en in combinatie met de reeds beschikbare gegevens ingrijpende stelselmatigheid zal opleveren. In de visie van de commissie zal dan ook betrokkenheid van de rechter-commissaris alleen in bijzondere gevallen van onderzoek aan digitale-gegevensdragers of geautomatiseerde werken vereist zijn, en het is zeker niet de bedoeling dat uit voorzorg in veel gevallen een machtiging van de rechter-commissaris zal worden aangevraagd om te voorkomen dat eventuele toevallig in beeld komende gegevens een onderzoek met terugwerkende kracht onrechtmatig zouden maken. Een eventueel onrechtmatigheidsverweer dient te onderbouwen waarom, naar het oordeel van de verdediging, een uitgevoerd onderzoek *redelijkerwijs voorzienbaar* als ingrijpend stelselmatig aangemerkt had moeten worden. (Hierbij moet wel worden aangetekend dat, vanwege de toenemende dataficering, op termijn in toenemende mate sneller dan voorheen sprake zal zijn van ingrijpende stelselmatigheid, zelfs bij traditioneel weinig ingrijpende bevoegdheden; bij een gelijkblijvend niveau van privacybescherming zou dan vaker de rechter-commissaris moeten worden ingeschakeld. Zie hierover nader par. 3.5.)

Hieronder proberen we aan de hand van voorbeelden nader toe te lichten hoe het criterium van (ingrijpende) stelselmatigheid kan worden toegepast op uiteenlopende bevoegdheden, om een eerste invulling te geven aan wat het betekent om, in verschillende situaties, een min of meer volledig beeld van delen van iemands privéleven te krijgen, wanneer daarbij sprake kan

zijn van een ingrijpend beeld in diepe of brede zin, en wat het betekent dat de met deze beelden samenhangende privacyinbreuk op voorhand redelijkerwijs voorzienbaar is.

A. Onderzoek van smartphones bij aanhouding

- Bij een vechtpartij op straat, waarbij meerdere omstanders mogelijk met hun telefoons video-opnamen hebben gemaakt, neemt een opsporingsambtenaar de smartphone van een getuige, die weigert zijn telefoon vrijwillig aan de opsporingsambtenaar te geven, in beslag om te voorkomen dat eventueel bewijsmateriaal verloren gaat. Op de smartphone is de camera-functie op dat moment actief. De opsporingsambtenaar bekijkt de recentst gemaakte video's, voor het geval er een video bij zit waarop de vechtpartij zichtbaar is. Dit is een *niet-stelselmatig* onderzoek: het betreft handmatig bekijken van enkele bestanden, waarbij niet redelijkerwijs voorzienbaar is dat een bepaald aspect van het privéleven van de getuige (of van anderen) min of meer volledig in beeld komt.
- Een drugsklant heeft vrijwillig inzage gegeven in zijn telefoon en berichten laten zien die hij van een dealer heeft ontvangen. Na aanhouding van de verdachte dealer wordt diens smartphone handmatig onderzocht om te controleren of die berichten inderdaad door hem verzonden zijn (door gericht zoeken op het contactadres van de drugsklant of op de specifieke datum en tijdstip waarop de berichten verzonden waren). Weliswaar wordt hier gezocht naar inhoudelijke communicatie, maar door de specifieke gerichtheid van het zoeken en het reeds (via de drugsklant) bekend en vastgelegd zijn van de inhoud van de gezochte berichten levert dit geen stelselmatigheid op. Ook kan de opsporingsambtenaar de in de afgelopen paar dagen laatst gebelde nummers raadplegen, of verder terugzoeken gericht op een specifiek nummer om te onderzoeken of de verdachte dealer contact heeft gehad met een andere bekende dealer. Ook dat betreft *niet-stelselmatig* onderzoek, omdat het beperkt blijft tot handmatig onderzoek van enkele gegevens.
- Een op heterdaad betrapte winkeldief wordt aangehouden. Voor het bewijs van de winkeldiefstal is inbeslagneming van de smartphone niet nodig, maar omdat de winkeleigenaar aangeeft verdachte twee weken ervoor te hebben gezien en toen ook al de indruk te hebben gehad van winkeldiefstal, neemt de opsporingsambtenaar de smartphone in beslag met het oog op het onderzoeken van de locatiegegevens en app-berichten van de twee weken ervoor. Dit is stelselmatig onderzoek, omdat er niet handmatig maar geautomatiseerd wordt gezocht waarbij een in potentie aanzienlijke hoeveelheid gegevens naar voren komt die een beeld geeft van de activiteiten van verdachte in de afgelopen twee weken. De opsporingsambtenaar behoeft voor dit onderzoek dus een bevel van de officier van justitie.
- In de vorige casus wordt, na een bevel van de officier van justitie, de smartphone onderzocht op app-berichten in de afgelopen twee weken. Hierbij blijkt een bericht te zitten waarin verdachte een vriend appte dat hij naar een kliniek moest voor behandeling aan een soa die hij waarschijnlijk had opgelopen bij bezoek aan een prostituée. Het aantreffen van deze gevoelige gegevens (medisch en seksueel leven) maakt het onderzoek *niet ingrijpend* stelselmatig; het was immers niet redelijkerwijs voorzienbaar dat een dergelijk app-bericht in beeld zou komen bij het onderzoek.
- Bij een aanhouding wil de opsporingsambtenaar nagaan of de telefoon bij de verdachte in gebruik is; verdachte zegt dat de telefoon van hem is, terwijl het vermoeden bestaat dat het een gestolen telefoon betreft. Hiertoe kan worden gekeken naar de naam die gebruikt wordt in WhatsApp of in de e-mail; dit is geen stelselmatig onderzoek, omdat het beperkt blijft tot handmatig bekijken van een simpel gegeven.
- Een verdachte van graffiti wordt aangehouden. De smartphone wordt onderzocht om te kijken of er foto's van graffiti-tags op staan. Het geautomatiseerd doorzoeken van de foto's op de zoekterm "graffiti" in bestandsnamen of metadata (die bijvoorbeeld een beeldherkenningsapp op de smartphone automatisch heeft toegevoegd aan foto's) en het vervolgens

bekijken van enkele foto's die daarbij naar voren komen, is *niet stelselmatig*: hierbij valt niet redelijkerwijs te verwachten dat een bepaald aspect van het privéleven van de verdachte min of meer volledig in beeld komt. Ook het gebruik van software die via geautomatiseerde beeldvergelijking zoekt op foto's die sterk lijken op een foto van de graffiti-tag van de verdachte, vormt *geen stelselmatig* onderzoek: het gaat (zolang tenminste de gebruikte software betrouwbaar is en een relatief laag percentage fout-positieven kent, en de zoekopdracht voldoende is afgebakend) om een zeer gerichte zoekactie, waarbij naar verwachting alleen relevante (graffiti)foto's naar boven komen. De zoekactie is weliswaar breed in de zin dat de hele fotobibliotheek wordt doorzocht, maar doordat de gehanteerde methode zeer gericht is en de resultaten beperkt blijven tot wat gezocht wordt, blijft de inbreuk beperkt.

Het handmatig doorkijken door de opsporingsambtenaar van alle foto's om te kijken of daar foto's van graffiti in voorkomen, zal daarentegen sneller *stelselmatig* zijn. Dat is niet het geval als het zoeken beperkt blijft tot het bekijken van een beperkt aantal foto's, bijvoorbeeld de tien meest recente of de foto's gemaakt in het afgelopen uur, om te kijken of de verdachte een graffiti-selfie heeft gemaakt of foto's van collega-graffitispuiters. Dan blijft het onderzoek beperkt en gericht. Er is echter wel sprake van stelselmatigheid als de opsporingsambtenaar handmatig een grotere hoeveelheid foto's bekijkt, bijvoorbeeld om te kijken of er in de afgelopen maanden foto's van graffiti zijn gemaakt. In dat geval bestaat de redelijke kans dat hij kennis kan nemen van veel aspecten van iemands privéleven of *en passant* kan stuiten op intieme of anderszins privacygevoelige foto's. Hoewel het doel van de zoekactie gericht is, kan de opsporingsambtenaar bij de uitvoering gewenst of ongewenst breed kennisnemen van het privéleven van de verdachte. Ook al worden deze gegevens niet vastgelegd, het kennisnemen door een opsporingsambtenaar van alle of een grote hoeveelheid op de smartphone opgeslagen foto's geeft het onderzoek wel een stelselmatig karakter.

- Een verdachte van handel in xtc wordt aangehouden op verdenking van drugshandel. Haar inbeslaggenomen smartphone wordt geautomatiseerd onderzocht op digitale sporen die wijzen op betrokkenheid bij drugshandel, waaronder de geschiedenis van bezochte websites. Dit is een *stelselmatig* onderzoek, omdat het geautomatiseerd zoeken betreft naar gegevens die, bij bezochte webpagina's, redelijkerwijs voorzienbaar meerdere delen van het privéleven betreffen. Het is echter *geen ingrijpend* stelselmatig onderzoek: het valt niet op voorhand aan te nemen dat het zoeken naar bezochte wegpagina's die samenhangen met drugshandel een wezenlijk deel van verdachtes privéleven in kaart zal brengen.
- In de vorige casus wordt de smartphone niet alleen doorzocht op bewijs van drugshandel, maar ook op contacten aan wie zij mogelijk xtc heeft verkocht. Het gaat hierbij om iemand die werkzaam is in de escortbranche, en uit een tap in een ander onderzoek is bekend dat verdachte haar escortpraktijk lijkt te combineren met (vermoede) drugshandel, en dus aan haar cliënten ook xtc verkoopt. Het onderzoek van de contactenlijst op de smartphone betreft in dit geval een *ingrijpend stelselmatig* onderzoek: het is redelijkerwijs voorzienbaar dat personen naar voren komen die met de verdachte tegen betaling seksueel contact hebben gehad, waardoor een wezenlijk deel van het privéleven van cliënten van de verdachte in beeld komt. Het is daarbij redelijkerwijs voorzienbaar dat, als bijvoorbeeld blijkt dat verdachte aan een bepaalde cliënt hoeveelheden xtc heeft geleverd die wijzen op handel door die cliënt, zal worden doorgerechercheerd op mogelijke verdenking van drugshandel door de cliënt, waarbij uit de eventuele zaak tegen de cliënt-verdachte dan zal blijken dat deze seksuele contacten heeft gehad met een escort. De combinatie van gegevens over het seksuele leven van de cliënten en de niet te verwaarlozen kans dat deze informatie bij de omgeving van een cliënt bekend kan raken (waardoor de contextuele integriteit van informatie over de seksuele contacten wordt aangetast), maken dat het onderzoek een ingrijpend stelselmatig karakter krijgt.

B. Onderzoek van gegevens bij een doorzoeking tot onderzoek van gegevens

- Bij een doorzoeking in een bedrijf dat verdacht wordt van belastingfraude, wordt de digitale administratie overgenomen. De overgenomen bestanden worden geïndexeerd en vervolgens geautomatiseerd doorzocht. Afhankelijk van de aard van het bedrijf en de daarmee samenhangende administratie, en van de aard en intensiteit van de zoekactiviteiten, kan dit onderzoek een *stelselmatig* karakter hebben; er zal zelden sprake zijn van ingrijpende stelselmatigheid.
- Bij een doorzoeking van een loods waar vermoed wordt dat synthetische drugs worden geproduceerd, wordt een verdachte aangetroffen met een laptop in zijn tas. De verdachte geeft aan dat het zijn persoonlijke laptop betreft en geeft geen toestemming aan de politie erin te kijken, omdat er, zoals hij zegt, allerlei privégegevens op staan omdat dit de laptop is die hij altijd gebruikt. Voor het onderzoek van de gegevens op de laptop geldt hetzelfde als de verdachte van xtc-handel van wie de smartphone bij aanhouding in beslag is genomen (zie boven). Het handmatig zoeken van enkele bestanden levert een geringe privacyinbreuk op. Het geautomatiseerd doorzoeken aan de hand van zoekvragen als "xtc" is stelselmatig, omdat redelijkerwijs voorzienbaar is dat niet alleen informatie over drugsproductie in beeld kan komen, maar ook de nodige informatie over het uitgaansleven van de verdachte. Het onderzoek zal echter zelden een ingrijpend stelselmatig karakter hebben, omdat niet te voorzien is dat bij het onderzoek een wezenlijk deel van het privéleven van verdachte (of van derden wier persoonsgegevens op de laptop staan) in beeld komt. Alleen als bijvoorbeeld bekend is dat de verdachte ook de secretaris is van de plaatselijke afdeling van een politieke partij (waarvan vermoed kan worden dat de administratie en correspondentie op deze laptop wordt bijgehouden) en de zoekvragen ook naar verwachting resultaten kunnen opleveren over plaatselijke partijleden, of over niet-openbare politieke discussiestukken over de visie op drugsbeleid van de plaatselijke afdeling, is er sprake van ingrijpende stelselmatigheid.

C. Vorderen van gegevens

- Bij een verdachte zijn vijftien kinderporno-afbeeldingen aangetroffen binnen een verzameling van tienduizenden porno-afbeeldingen; hij beweert dat de kinderporno ongemerkt en onbedoeld is binnengekomen bij het geautomatiseerd downloaden uit bepaalde pornobronnen. Technische analyse geeft onvoldoende aanwijzingen of het bezit van de kinderporno als opzettelijk kan worden gekwalificeerd. Om aanvullend bewijs te verzamelen van opzet op bezit, wil de officier van justitie de financiële gegevens bij zijn bank vorderen en (als daaruit blijkt dat er seks-gerelateerde producten of diensten zijn gekocht) aankoopgegevens bij sekswinkels. Het vorderen van bankgegevens brengt normaliter geen ingrijpende stelselmatigheid met zich: het is niet redelijkerwijs voorzienbaar dat daaruit een ingrijpend beeld van iemands privéleven ontstaat. Weliswaar komen naar verwachting gegevens over veel aspecten van iemands leven naar voren, waaronder potentieel enkele wezenskenmerken, maar het betreft veelal metagegevens (contacten, bedragen en omschrijvingen) die een relatief oppervlakkig beeld opleveren. Het vorderen van aankoopgegevens bij een sekswinkel daarentegen is in dit geval wel ingrijpend stelselmatig, omdat dit hier gericht is op het vaststellen van een eventuele pedoseksuele interesse en dat aspect van het seksuele leven van de verdachte normaliter niet in zijn naaste of sociale omgeving bekend zal zijn.

D. Vastleggen telecommunicatie-inhoud

- Het onderscheppen van app-berichten: dit is ingrijpend stelselmatig, omdat app-berichten een vorm van communicatie betreffen die beschermd is onder artikel 13 Gw.

- Het onderscheppen van machine-machine-communicatie (dus gegevensverkeer tussen IoT-apparaten onderling, waarbij niet redelijkerwijs voorzienbaar is dat hiertussen ook mens-mens- of mens-machine-communicatie bij zal zitten). Als het gaat om kort onderscheppen van beperkte functionele gegevens (hoe laat gaat de koffieautomaat aan, als indicatie dat het arrestatieteam kan aanrijden), zal dit niet stelselmatig zijn. Wel is er sprake van stelselmatigheid als het gaat om gedurende een langere periode tappen van IoT-apparaten waardoor, redelijkerwijs voorzienbaar, en als, gelet op het aantal apparaten, de diversiteit in functies en de lengte van de periode waarin het onderlinge gegevensverkeer wordt onderschept, een min of meer volledig beeld kan ontstaan van iemands huiselijk leven. Dergelijk onderscheppen zal niet gauw ingrijpend stelselmatig zijn (omdat de gegevens geen inzicht bieden in de details van gedrag die samenhangen met een wezenlijk deel van iemands privéleven).

E. Stelselmatig overnemen van gegevens uit publiek toegankelijke bronnen

- Op een website worden *real-time streams* getoond van gehackte IoT-camera's (waarbij duidelijk is dat de gebruikers (nog) niet doorhebben dat hun camera gehackt is). Een van de getoonde streams is afkomstig van de webcam in de slaapkamer van een verdachte, die een baan heeft met reguliere werktijden. Indien een opsporingsambtenaar midden op de dag, gedurende tien seconden, deze beelden bekijkt met als doel vast te stellen of een bepaalde kinderpornovideo in deze slaapkamer is opgenomen, is dit *niet stelselmatig*: het is niet te verwachten dat gedurende deze tien seconden de verdachte of een huisgenoot in beeld komt op een manier waarbij een min of meer volledig beeld ontstaat van een bepaald aspect van diens privéleven. Het vervolgens overnemen van de *livestream*-beelden gedurende een week met als doel bewijs van actueel misbruik te vergaren, is daarentegen ingrijpend stelselmatig (diep), omdat een min of meer volledig beeld wordt vastgelegd van een wezenlijk aspect (het intieme leven) van het privéleven van de verdachte (en diens eventuele bedgenoot).
- In een onderzoek naar anarchistisch-radicale nertsenbevrijders worden de gegevens overgenomen van een site waarop een hacktivist de volledige profielen en besloten berichten online heeft gezet van een forum waarop dierenactivisten niet alleen hun eventuele bevrijdingsplannen en -wensen voor nertsen, maar ook hun politieke en ideologische overtuigingen bespreken. Dit is een vorm van ingrijpend stelselmatig onderzoek in diepe zin, omdat het profiel en de besloten berichten een wezenlijk deel van iemands privéleven weergeven. Als de dienst uitgebreide profielen met persoonlijke interesses hanteert en berichten van het afgelopen half jaar bewaart, is het ook ingrijpend stelselmatig in brede zin, aangezien daaruit redelijkerwijs voorzienbaar een aanzienlijk deel van het privéleven naar voren kan komen.

4.2.4. Uitwerking van het normeringscriterium in overige vereisten

In dit rapport is de uitwerking van het voorgestelde normeringscriterium beperkt tot de bevoegde autoriteit die toestemming dient te geven voor de inzet van een bevoegdheid. Zoals opgemerkt in paragraaf 4.2.1 is dat een van de belangrijkste aanknopingspunten in de normering van bevoegdheden. Het is echter niet het enige aanknopingspunt. De wet kent ook andere criteria die kunnen worden verbonden aan de inzet van bevoegdheden, waaronder aanvullende subsidiariteitscriteria en uiteraard het verdenkingscriterium.

Wat betreft **extra subsidiariteitscriteria** kan worden opgemerkt dat dit vooral aan de orde is bij de meest ingrijpende bevoegdheden. Vanzelfsprekend moet de inzet van bevoegdheden altijd voldoen aan de algemene beginselen van subsidiariteit en proportionaliteit, die in het conceptwetsvoorstel met betrekking tot Boek 2 worden gecodificeerd (art. 2.1.2.2). Ook geldt dat een bevoegdheid alleen mag worden uitgeoefend indien dit in het belang van het onderzoek

is (art. 2.1.2.1 lid 2). Voorts gelden voor de afzonderlijke bevoegdheden aanvullende wettelijke toepassingscriteria. Voor ingrijpender bevoegdheden geldt dat deze alleen bij dringende noodzaak kunnen worden toegepast. Met deze extra subsidiariteitseis wordt tot uitdrukking gebracht dat, gegeven de ingrijpendheid van het middel, niet louter de rechtmatigheid van de inzet moet worden getoetst, maar daarbij tevens doelmatigheidsafwegingen in de beoordeling moeten worden betrokken.[65] In dit systeem, waarin een dergelijke extra subsidiariteitseis wordt verbonden aan de meest ingrijpende vormen van inzet van bevoegdheden, past het om, in relatie tot het algemene normeringscriterium, een dergelijke extra subsidiariteitseis te stellen wanneer de inzet van een bevoegdheid ingrijpende stelselmatigheid oplevert – de zwaarste vorm van het drieledige normeringscriterium.

De commissie merkt in dit verband overigens op dat verschillende formuleringen van de betekenis van het vereiste van "dringende noodzakelijkheid" in de memorie van toelichting tot verwarring zouden kunnen leiden. Op pagina 19 van die toelichting wordt het vereiste uitgelegd als een expliciete uitdrukking van de beginselen van proportionaliteit en subsidiariteit, die inhoudt dat toetsende actor (de officier van justitie of de rechter-commissaris) niet kan volstaan met een marginale toetsing. Op pagina 193 van diezelfde toelichting wordt echter, in de toelichting bij het vorderen van "gevoelige" gegevens, het vereiste op een andere manier uitgelegd: "Dit betekent dat de officier van justitie alleen dan tot een bevel tot uitlevering van dergelijke gegevens kan overgaan, indien het onderzoek zonder die gegevens niet verder komt." Deze uitleg komt de commissie ongelukkig voor, omdat deze niet – zoals de algemene uitleg – op doel*matig*heid ziet, maar eerder op doel*treffend*heid: volgens deze uitleg *moet* het middel leiden tot een bijdrage aan het doel, ongeacht of het middel in verhouding staat tot het doel. Aan de ene kant is dat een te ruime uitleg, omdat een proportionaliteitstoets lijkt te ontbreken. Aan de andere kant is het mogelijk ook een te beperkte uitleg, omdat de subsidiariteit wordt uitgelegd als een garantie dat het doel dichterbij komt; het gaat echter om een redelijke en gemotiveerde inschatting van de waarschijnlijkheid dat het onderzoek verder komt, op een manier die in verhouding staat tot de met het middel gepaard gaande kosten. De commissie adviseert dan ook de memorie van toelichting op pagina 193 aan te passen en in lijn te brengen met de algemene uitleg van het begrip.

Aanbeveling 7: inzet van bevoegdheden die ingrijpende stelselmatigheid oplevert is alleen mogelijk als het onderzoek deze inzet dringend vereist. De toelichting moet het criterium van "dringend vereisen" consistent uitleggen als een niet louter marginale doelmatigheidstoets. → *p. 195*

Wat betreft het **verdenkingscriterium** moet worden opgemerkt dat het conceptwetsvoorstel hierin een andere benadering heeft gekozen dan in het huidige wetboek wordt gehanteerd.[66] Deze nieuwe benadering is nog onderwerp van discussie.[67] Aangezien dit een algemeen punt betreft dat de commissieopdracht overstijgt, wordt in dit rapport geen specifieke aandacht besteed aan de vraag of de inzet van bepaalde bevoegdheden betreffende digitale gegevens verbonden zou moeten worden aan een minimale ernst van het strafbare feit waarvoor de bevoegdheid wordt ingezet. In lijn met de algemene benadering in dit rapport ligt het voor de hand om inzet van bevoegdheden die aan het criterium van stelselmatigheid voldoet te verbinden aan een zekere ernst van het strafbaar feit, en inzet van bevoegdheden die ingrijpende

[65] Zie Memorie van toelichting bij het wetsvoorstel met betrekking tot Boek 2, p. 19.
[66] Zie paragraaf 2.3 van de memorie van toelichting bij het conceptwetsvoorstel met betrekking tot Boek 2 over de vereenvoudiging van de verdenkingscriteria.
[67] Zie de consultatieadviezen van de Raad voor de rechtspraak, het OM, de NOvA, de politie, de KMar en het Platform BOD'en, waarin negatief wordt geadviseerd over de voorgestelde vereenvoudiging van de verdenkingscriteria.

stelselmatigheid oplevert te beperken tot ernstige feiten. De precieze vormgeving daarvan kan worden bepaald wanneer de uiteindelijk gekozen systematiek op dit punt in Boek 2 uitgekristalliseerd is.

De commissie wijst daarbij overigens wel op één aspect dat hier van belang is, in verband met haar constatering dat, in een tijdperk van dataficering en volatilisering (par. 4.1), het steeds moeilijker wordt om bij de vormgeving van opsporingsbevoegdheden op voorhand, dus in de wet, een vast beschermingsniveau te koppelen aan een bepaalde bevoegdheid (par. 4.2.1). Dat heeft ook zijn weerslag op de vraag bij welke mate van ernst van strafbare feiten een bepaalde inzet van bevoegdheden aanvaardbaar geacht moet worden: dat is ook moeilijker op voorhand in zijn algemeenheid te bepalen. Voor sommige vormen van (computer)criminaliteit die een relatief lage strafbedreiging kennen, kan soms de inzet van een zwaardere bevoegdheid de enige mogelijkheid zijn om de dader op te sporen. In gevallen waarin er, bijvoorbeeld vanuit maatschappelijke overwegingen, een zwaarwegend belang is om een dergelijk strafbaar feit wel te vervolgen, zou opsporing dan niet mogelijk zijn als de bevoegdheid niet kan worden ingezet voor dit type strafbare feit. Om die reden adviseert de commissie om een vangnetbepaling in te voeren, die bepaalt dat in gevallen van een lichter strafbaar feit dan waarvoor een bevoegdheid is toegelaten, de rechter-commissaris bij een zwaarwegend belang toestemming kan geven voor inzet van de desbetreffende bevoegdheid. Deze vangnetbepaling zou zowel toepassing moeten kunnen vinden bij stelselmatig onderzoek als bij ingrijpend stelselmatig onderzoek.

Aanbeveling 8: inzet van bevoegdheden die stelselmatigheid respectievelijk ingrijpende stelselmatigheid oplevert, kan worden gekoppeld aan een bepaald niveau van ernst van het strafbare feit, conform de algemene gekozen (of te kiezen) systematiek in Boek 2. Daarbij is een vangnetbepaling wenselijk om bij lichtere strafbare feiten de inzet van de bevoegdheid toe te laten met machtiging van de rechter-commissaris, indien een zwaarwegend belang de opsporing van dat feit dringend vordert. → *p. 195*

4.2.5. Overige redenen voor normering

Met het algemene normeringscriterium heeft de commissie zich zoals gezegd[68] geconcentreerd op de inbreuk op het grondrecht op bescherming van de persoonlijke levenssfeer, aangezien dat het meest direct in het geding is bij opsporing in een digitale omgeving. Er zijn echter ook andere redenen voor normering. Privacyinbreuken vormen in die zin een voldoende reden voor het creëren van een expliciete wettelijke grondslag en een bepaald niveau van normering – dat haar weerslag heeft gevonden in het voorgestelde algemene normeringscriterium – maar niet de enige reden daarvoor.

In het systeem van de Wet bijzondere opsporingsbevoegdheden is gekozen voor een wijze van normering waarbij naast inbreuken op grondrechten ook bijzondere risico's voor de integriteit en beheersbaarheid van de opsporing een zelfstandige grondslag voor normering vormen.[69] Dat is bijvoorbeeld bij infiltratie het geval. Hierin stelt de commissie geen wijziging voor; nog steeds zullen risico's voor de integriteit van de opsporing beoordeeld moeten worden door de wetgever bij de vormgeving van bevoegdheden. Onder omstandigheden kan dit ertoe leiden dat een bevoegdheid aan een machtiging van de rechter-commissaris onderworpen moet worden, ook als er geen sprake is van ingrijpende stelselmatigheid. De commissie heeft zich niet specifiek met de vraag bezig gehouden wanneer bepaalde opsporingsbevoegdheden in een digitale omgeving bijzondere risico's voor de opsporing zullen opleveren, in de veronderstelling dat zich hier in een digitale omgeving geen voorzienbare specifieke nieuwe omstandigheden zullen voordoen die tot afwijking van de bestaande regeling zouden nopen. Dit rapport

[68] Zie noot 44.
[69] Zie *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 3.

bevat dus geen adviezen voor normering in het licht van risico's voor de integriteit van de opsporing; de wetgever kan daarin desgewenst de bestaande lijnen doortrekken.

Daarnaast is van belang dat opsporingsbevoegdheden ook inbreuk kunnen maken op andere grondrechten dan de persoonlijke levenssfeer, zoals de vrijheid van meningsuiting, de vrijheid van gedachte, geweten en godsdienst, of de vrijheid van vergadering en vereniging.

Deze grondrechten gaan gepaard met een zelfstandige vorm van normering, veelal op basis van EHRM-rechtspraak. Zo kan een rechterlijke machtiging nodig zijn voor het vorderen van bepaalde gegevens als die gegevens de journalistieke bronbescherming raken, los van de vraag of de gevorderde gegevens een (al dan niet ingrijpende) privacyinbreuk opleveren.[70] Dit betekent dat bij de vormgeving van de normering van bevoegdheden ook rekening moet worden gehouden met de inbreuk op andere grondrechten dan privacy. De invulling van het algemene normeringscriterium – namelijk of een min of meer volledig beeld van bepaalde aspecten van iemands privéleven dan wel een ingrijpend beeld van iemands privéleven kan ontstaan – is daarvoor niet als zodanig geschikt. Dit betekent dat de wetgever, in aanvulling op de normering die geïndiceerd is op basis van het algemene normeringscriterium, ook moet meewegen of de rechtspraak betreffende andere grondrechten dan privacy in bepaalde gevallen tot zwaardere waarborgen zou moeten leiden. Vanwege de beperkte richtinggevendheid van EHRM-rechtspraak voor de specifieke regeling van toekomstige bevoegdheden op wetgevingsniveau (zie par. 4.2.1), heeft de commissie niet specifiek aandacht besteed aan de vraag in welke gevallen in het gemoderniseerde wetboek zwaardere waarborgen op basis van andere grondrechten aangewezen zouden zijn. Er zijn echter wel voorbeelden te bedenken waarin de inbreuk op andere grondrechten tot zware waarborgen noopt. Denkbaar is bijvoorbeeld dat het onderscheppen van IoT-verkeer een ingrijpende inbreuk op grondrechten oplevert als de communicatie tussen apparaten in een samenhangend mediasysteem in een woning wordt onderschept op een manier dat de mediaconsumptie van de bewoner min of meer volledig wordt vastgelegd, inclusief welke tv-programma's, podcasts, YouTube-filmpjes en Netflix-series worden bekeken. Deze informatie raakt direct aan de vrijheid van meningsuiting, waaronder ook de garingsvrijheid van informatie valt, en het stelselmatig in beeld brengen van iemands mediaconsumptie heeft een niet te verwaarlozen verkillend effect op iemands nieuwsgaringsvrijheid. In dit geval is er sprake van ingrijpende inbreuk op grondrechten niet zozeer omdat een ingrijpend beeld van iemands privéleven kan ontstaan als wel omdat het een ingrijpende inbreuk op de vrijheid van meningsuiting betreft, zodat dezelfde voorwaarden zouden moeten gelden als bij ingrijpende stelselmatigheid.

De commissie adviseert de wetgever om in de memorie van toelichting hieraan aandacht te besteden en in regelgeving neer te leggen dat, in gevallen van voorzienbare inbreuken op andere grondrechten waarbij in (grondrechtelijke) rechtspraak een zwaardere normering wordt vereist (in het bijzonder een voorafgaande of tussentijdse rechterlijke toetsing) dan op basis van het algemene normeringscriterium in specifieke toepassingen aan de orde zou zijn, de opsporingsambtenaar en officier van justitie het criterium van (ingrijpende) stelselmatigheid naar analogie moeten toepassen qua bevoegdheidstoedeling en overige vereisten. Hierbij kunnen enkele voorbeelden worden genoemd van onderzoekshandelingen die een niet-ingrijpende privacyinbreuk opleveren maar op gespannen voet staan met bijvoorbeeld de journalistieke bronbescherming of de vrijheid van vergadering. Wanneer uit (grondrechtelijke) rechtspraak in de toekomst zou blijken dat bij inzet van een bepaalde bevoegdheid zwaardere normering (zoals een voorafgaande rechterlijke toetsing) specifiek in de wet zelf geregeld dient te worden – wat op dit moment moeilijk voor concrete gevallen te bepalen valt – dient (vanzelfsprekend) de wet alsdan dienovereenkomstig te worden aangepast.

[70] Zie bijvoorbeeld EHRM 14 september 2010, Sanoma Uitgevers BV t. Nederland, App.nr. 38224/03.

Aanbeveling 9: bij de toelichting op het algemene normeringscriterium en op de kwalificatie van een bepaalde inzet van bevoegdheden als (ingrijpend) stelselmatig dient de wetgever aandacht te besteden aan inbreuken op andere grondrechten dan privacy en in regelgeving neer te leggen dat het criterium naar analogie toegepast moet worden als die inbreuken, conform (grondrechtelijke) rechtspraak, een zwaardere normering indiceren.
→ *p. 195*

4.3. Overige algemene aspecten van normering

Naast de normering van de gegevensvergaring door bovengenoemd algemeen criterium met een driedeling in bevoegde autoriteit (zie verder par. 4.2), kunnen ook op andere manieren waarborgen worden gecreëerd. In de commissie is gesproken over verschillende vormen, die in deze paragraaf worden behandeld.

4.3.1. Rechterlijke toetsing vooraf van cumulatie van bevoegdheden

Inleiding

Bij de wat omvangrijkere strafzaken komt het niet zelden voor dat een rechter-commissaris wordt betrokken bij het opsporingsonderzoek nadat reeds enkele, door de officier van justitie bevolen, bijzondere opsporingsbevoegdheden zijn toegepast. De rechter-commissaris kan in een dergelijke fase van het onderzoek bijvoorbeeld worden benaderd om een machtiging te verlenen tot uitoefening van de bevoegdheid tot het vastleggen van telecommunicatie. In de commissie is gesproken over de vraag of het niet in de rede ligt om de rechter-commissaris in een eerder stadium in het onderzoek te betrekken. Ook bij de cumulatieve inzet van bijzondere opsporingsbevoegdheden waarvoor geen rechterlijke machtiging is vereist, kunnen immers zoveel gegevens worden verkregen over degene ten aanzien van wie deze bevoegdheden zijn toegepast, dat dit samenstel van gegevens een indringend beeld van iemands privéleven geeft.

Waar de commissie een machtiging van de rechter-commissaris nodig acht voor onderzoek – meer precies: een specifieke wijze van uitoefening van een bevoegdheid – waarbij op voorhand redelijkerwijs voorzienbaar een ingrijpend beeld van iemands privéleven kan ontstaan, doet zich de vraag voor of het vereiste van een machtiging van de rechter-commissaris niet ook aangewezen is indien voorafgaand aan de inzet van enkele (elk op zichzelf licht ingrijpende) bevoegdheden redelijkerwijs voorzienbaar is dat het (totaal)resultaat van die bevoegdheden eveneens een dergelijk ingrijpend beeld van iemands persoonlijk leven oplevert.

Positie van de rechter-commissaris in het nieuwe wetboek

In artikel 1.2.4.1, tweede lid, van het conceptwetsvoorstel ter vaststelling van Boek 1 van het nieuwe Wetboek van Strafvordering zijn aard en doel van de bevoegdheidsuitoefening van de rechter-commissaris omschreven: de rechter-commissaris oefent zijn bevoegdheden uit in het belang van de rechtsbescherming en van de volledigheid, de evenwichtigheid en de voortgang van het onderzoek. Toegelicht wordt dat zijn rol tijdens het opsporingsonderzoek met de afschaffing van het gerechtelijk vooronderzoek is veranderd. De rechter-commissaris fungeert niet langer als “onderzoeksrechter”, maar als “rechter in het vooronderzoek”. Daarbij houdt hij toezicht op de rechtmatigheid, evenwichtigheid, volledigheid en voortgang van het opsporingsonderzoek. Wanneer hij via een machtiging toestemming geeft tot toepassing van bepaalde opsporingsbevoegdheden of zelf opsporingsbevoegdheden uitoefent, ressorteert deze bevoegdheidsuitoefening onder de rechtsbeschermende functie die de rechter-commissaris vervult. De ingrijpendheid van de inbreuk op grondrechten maakt dat zijn betrokkenheid bij de bevoegdheidsuitoefening aangewezen is. Daarnaast kan de rechter-commissaris ambtshalve, op vordering van de officier van justitie of op verzoek van de verdediging, onderzoek doen ter

aanvulling van het opsporingsonderzoek. Hoofdstuk 10 van het conceptwetsvoorstel ter vaststelling van Boek 2 geeft hiervoor een regeling. Tezamen met het beoordelen van bezwaren tegen beslissingen van de officier van justitie dient dergelijk optreden van de rechter-commissaris vooral het belang van de evenwichtigheid, volledigheid en voortgang van het onderzoek.

Een aanvullende rol voor de rechter-commissaris bij cumulatie van bevoegdheden?

Het is duidelijk dat de door de commissie voorgestane rol die de rechter-commissaris zal vervullen bij de toepassing van een bevoegdheid waardoor een ingrijpend beeld van iemands privéleven kan ontstaan, aansluit bij de rechtsbeschermende functie die hem door het gemoderniseerde wetboek wordt toebedeeld in het opsporingsonderzoek. De rechter-commissaris beoordeelt in zo'n geval of de voorgenomen ingrijpende wijze van onderzoek, gelet op de ernst van het strafbare feit en de overige onderzoeksmogelijkheden, voldoet aan de beginselen van proportionaliteit en subsidiariteit.

Een eventuele *aanvullende* rol die van de rechter-commissaris een beoordeling van de toelaatbaarheid van de (voorzienbare) effecten van *een verzameling* van bevoegdheden zou vragen, ligt in het verlengde hiervan en moet daarom eveneens in de sleutel van de rechtsbescherming worden geplaatst. De rechter-commissaris zou in zo'n geval beoordelen of de totale privacy-impact van de achtereenvolgende uitoefening van meerdere lichte (heimelijke) bevoegdheden – naar op voorhand redelijkerwijs kan worden voorzien – een ingrijpend beeld van iemands privéleven zou gaan opleveren.

Regeling van een dergelijke bevoegdheid lijkt consistent met het voorstel van de commissie om voor indringend stelselmatig onderzoek door toepassing van één enkele (ingrijpende) bevoegdheid een machtiging van een rechter-commissaris te vereisen. De gedachte is immers dat wanneer overheidsingrijpen door bevoegdheidsuitoefening op enig moment zal leiden tot een indringend beeld van iemands privéleven, een dergelijke machtiging nodig is. Dat kan door toepassing van een enkele bevoegdheid met groot effect. Maar dat indringende beeld kan ook stapsgewijs worden opgebouwd: naarmate met meer bevoegdheden meer gegevens worden verkregen, kan het punt worden bereikt dat bij uitoefening van de volgende bevoegdheid redelijkerwijs voorzienbaar is dat het gehele beeld een indringende inkijk in iemands privéleven geeft. Dit sluit aan op de mozaïektheorie, die het belang onderstreept van het beoordelen van het totale plaatje in plaats van (alleen) de losse steentjes van een onderzoek.[71]

Een aanvullende rol van de rechter-commissaris maakt bovendien een bredere beoordeling van de proportionaliteit en de subsidiariteit van de bevoegdheidsuitoefening mogelijk, namelijk van de gehele set van bevoegdheden. Voor betrokkenheid van de rechter-commissaris bij de besluitvorming over (cumulatieve) toepassing van opsporingsbevoegdheden zou meer in het algemeen ook kunnen pleiten dat ook in strafzaken die uiteindelijk niet aan de zittingsrechter worden voorgelegd, is voorzien in enig rechterlijk toezicht op de uitoefening van bevoegdheden die een ingrijpende inbreuk op iemands persoonlijke levenssfeer kunnen opleveren. En wanneer een omvangrijk opsporingsonderzoek met de inzet van diverse bevoegdheden uiteindelijk wel aan de zittingsrechter wordt voorgelegd, zou een eerdere (intensievere) betrokkenheid van de rechter-commissaris kunnen voorkomen dat op zitting nog lange discussies worden gevoerd over de rechtmatigheid van de toegepaste bevoegdheden.

Tegelijkertijd impliceert een dergelijke betrokkenheid van de rechter-commissaris een fundamentele breuk met de bestaande wettelijke systematiek: die gaat uit – de machtigingsconstructie van het strafrechtelijk financieel onderzoek daargelaten – van toepassingscriteria die gekoppeld zijn aan elke afzonderlijke bevoegdheid. In deze systematiek brengt het feit dat meerdere

[71] Zie noot 60-61 en bijbehorende tekst.

opsporingsbevoegdheden na elkaar of parallel aan elkaar worden toegepast, geen verandering in de voorwaarden voor de inzet mee. Daarbij geldt dat voor de officier van justitie de beginselen van proportionaliteit en subsidiariteit van groot belang zijn bij de afweging of een bevoegdheid in het concrete geval wordt uitgeoefend. Die toets verricht hij per uit te oefenen bevoegdheid, en de officier betrekt hierbij telkens de resultaten van het opsporingsonderzoek die reeds voorliggen. Vooral als het gaat om de lichtere bevoegdheden is het – naar de huidige stand van de techniek – lastig een voorstelling te maken of, en zo, ja wanneer – dat wil zeggen na de (mogelijk parallelle) toepassing van meerdere bevoegdheden – de verkrijging van gegevens redelijkerwijs voorzienbaar een indringend beeld van iemands privéleven zal opleveren. Dat roept ook vragen op over de gevolgen voor de uitvoerbaarheid van de voorziening: zal de officier van justitie in verband met deze onzekerheid de rechter-commissaris daarom niet al snel veiligheidshalve bij zijn onderzoek willen betrekken? In dat geval dringt zich erosie van de systematiek en bovendien een capaciteitsprobleem op (groter nog dan het sowieso te verwachten capaciteitsprobleem, nu in veel wat grotere onderzoeken uit de aard van het opsporingswerk volgt dat op enig moment een indringend beeld ontstaat, zoals opgemerkt in par. 3.5).

Verder verdient aandacht wat de consequenties zullen zijn indien de rechter-commissaris machtiging dient te verlenen voorafgaand aan de uitoefening van *een set* bevoegdheden die redelijkerwijs voorzienbaar een indringend beeld van iemands privéleven zal opleveren. Het lijkt dan in de rede te liggen dat hij ook na uitoefening van die set bevoegdheden machtiging zal moeten verlenen voor de inzet van de daaropvolgende bevoegdheden. Dat zou ervoor kunnen pleiten dat met een soort koepelmachtiging wordt gewerkt waarbij een complete set aan bevoegdheden voor toestemming aan de rechter-commissaris wordt voorgelegd.

Een vraag die verder onder ogen moet worden gezien betreft de beoordelingsmaatstaf voor de rechter-commissaris. Moet hij het standpunt van de officier van justitie het zijne maken en daarop beoordelen of toepassing van de bevoegdheid geoorloofd is? Of beoordeelt hij eerst zelfstandig of wel redelijkerwijs voorzienbaar is dat een indringend beeld wordt verkregen, en zo ja, of daarvoor toestemming wordt gegeven? Als hij oordeelt dat niet redelijkerwijs voorzienbaar een indringend beeld wordt verkregen, kan het benaderen van de rechter-commissaris ook ertoe leiden dat de officier van justitie wordt verteld dat hij gewoon op eigen bevel de bevoegdheid kan uitoefenen. Het toekennen van deze bevoegdheid betekent uiteraard ook dat de rechter-commissaris kan weigeren deze machtiging af te geven. Is daarbij denkbaar dat hij in overleg met de officier van justitie treedt om te bekijken op welke wijze de bevoegdheid om op een minder ingrijpende wijze wordt uitgeoefend? De invloed die de rechter-commissaris daarmee kan uitoefenen op de wijze waarop het opsporingsonderzoek plaatsvindt, is niet onaanzienlijk. De rechter-commissaris zou zich vergaand kunnen bemoeien met de strategie van het opsporingsonderzoek. Dat zou een ontwikkeling zijn die tendeert naar de terugkeer van een (soort) gerechtelijk vooronderzoek. En die ontwikkeling verhoudt zich slecht met het ook in het gemoderniseerde wetboek gehuldigde uitgangspunt dat de officier van justitie het gezag heeft over het opsporingsonderzoek (en dat de situatie van twee kapiteins op één schip moet worden voorkomen).

Conclusie

Uit een oogpunt van consistentie in normeringscriteria valt er veel te zeggen voor een machtigingsconstructie ook in gevallen waarin op voorhand redelijkerwijs voorzienbaar is dat de voorgenomen inzet van *een set* opsporingsbevoegdheden een indringend beeld van iemands privéleven zal opleveren. Als per (nader te bepalen) bevoegdheid betrokkenheid van de rechter-commissaris wordt vereist vanwege bedoeld voorzienbaar effect, zijn er goede redenen om die betrokkenheid ook te realiseren als dat effect vooraf redelijkerwijs te verwachten valt door toepassing van meerdere bevoegdheden of nadat enkele bevoegdheden zijn uitgeoefend.

Niettemin conflicteert een dergelijke regeling dermate met de bestaande en toekomstige normering van opsporingsbevoegdheden en de daarmee samenhangende verantwoordelijkheden en gezagsverhoudingen, dat de commissie voor een op die leest geschoeide bevoegdheid voor de rechter-commissaris binnen de huidige systematiek van normering geen plaats ziet. Een en ander brengt echter wel nadrukkelijk aan het licht dat het huidig wettelijk stelsel geen volledig sluitende regeling kan bieden om naast de enkelvoudige ook de meervoudige inzet van bevoegdheden onder toezicht van de rechter-commissaris te plaatsen wanneer redelijkerwijs voorzienbaar is dat zij door achtereenvolgende toepassing een indringend beeld van iemands privéleven zal opleveren. Die constatering onderschrijft temeer de conclusie van de commissie (zie par. 3.5) dat op (middel)lange termijn het normeren van inbreuken op de privacy anders zal moeten worden ingericht.

4.3.2. Rechterlijke toetsing achteraf

Uit de jurisprudentie van het EHRM vloeit voort dat het ontbreken van rechterlijke machtiging voorafgaand aan de inzet van een inbreukmakende opsporingsbevoegdheid, onder omstandigheden gecompenseerd kan worden door rechterlijke toetsing achteraf. In zijn conclusie bij het genoemde smartphone-arrest concludeert advocaat-generaal Bleichrodt[72] dat het ontbreken van voorafgaande rechterlijke toetsing voor ingrijpende vormen van gegevensonderzoek na inbeslagneming naar huidig recht niet gecompenseerd kan worden geacht door de mogelijkheid van rechterlijke toetsing achteraf. Hij beschrijft twee vormen van rechterlijke toetsing achteraf, die naar zijn mening geen van beide voldoen. De eerste mogelijkheid is de volle toetsing door de zittingsrechter, aan de hand van artikel 359a Sv. Bleichrodt betoogt dat deze mogelijkheid onvoldoende compenseert omdat a. de lat te hoog ligt voor het verbinden van rechtsgevolgen aan een vormverzuim, en b. lang niet alle zaken aan een zittingsrechter worden voorgelegd. De tweede mogelijkheid zou het beklag op grond van artikel 552a Sv zijn, maar die weg staat, in ieder geval op het moment dat Bleichrodt zijn conclusie opstelde,[73] volgens de rechtspraak van de Hoge Raad niet open voor beklag tegen kennisnemen en gebruik van gegevens die zijn ontleend aan een inbeslaggenomen gegevensdrager.

Toetsing door de zittingsrechter

Het beeld dat de zittingsrechter slechts in een beperkt aantal strafzaken betrokken wordt, behoeft enige nuancering. Van alle misdrijven die ter kennis komen van de politie (ruim 900.000[74]) wordt 56% niet in onderzoek genomen, meestal omdat iedere vorm van opsporingsindicatie ontbreekt. In de resterende 44% (dus een kleine 400.000 zaken) wordt wél opsporingsonderzoek gedaan. Daarvan leidt 57% (bijna 230.000 zaken) tot identificatie van één of meerdere verdachten. In 70% (160.000) van die gevallen volgt inzending aan het OM (de resterende 30% wordt op andere wijze afgedaan, zoals met een reprimande of Halt-verwijzing). Van deze ingezonden zaken wordt door het OM ongeveer de helft gedagvaard (80.000), en in 22% (35.000) van de misdrijfzaken wordt een strafbeschikking opgelegd. In ongeveer 15% (ruim 5.000) van die laatste gevallen wordt door de verdachte verzet aangetekend,[75] waarmee de zaak alsnog voor de rechter wordt gebracht. Van het totaal aantal misdrijfzaken waarin onderzoek is gedaan (400.000) komt dus via dagvaarding of na verzet 85.000, oftewel ruim 20% voor de rechter. Dit cijfermatige beeld bevestigt de stelling dat veel opsporingsonderzoeken niet aan rechterlijke toetsing achteraf onderhevig zijn. De vraag is echter of hiermee ook slechts 20%

[72] ECLI:NL:PHR:2016:1047 t/m 1049.
[73] In ECLI:NL:HR:2017:71 lijkt de Hoge Raad de deur voor beklag op grond van artikel 552a Sv over kennisneming en gebruik van gegevens die zijn aangetroffen op een inbeslaggenomen telefoon op een kier te zetten.
[74] Alle genoemde cijfers zijn afkomstig uit de Jaarrapportage Strafrechtketen 2016 van het Ministerie van J&V, https://www.strafrechtketen.nl/onderwerpen/strafrechtketenmonitor/documenten/rapporten/2017/06/28/factsheet-strafrechtketenmonitor-2016 (laatst geraadpleegd 1 juni 2018).
[75] Zie Knigge & Peters 2017.

van alle zaken waarin inbreukmakende opsporingsbevoegdheden zijn ingezet aan de rechter worden voorgelegd. Het is mogelijk dat juist zaken waarin diepgaander opsporingsonderzoek is gedaan uitmonden in een dagvaarding, omdat het om meer ernstige feiten gaat of omdat er meer bewijs is gevonden. Anders gezegd: het is mogelijk dat in de zaken die niet aan de rechter worden voorgelegd relatief vaker sprake zal zijn van een beperkt onderzoek, bijvoorbeeld vanwege de geringere ernst van het feit. Dat laat uiteraard onverlet dat er zaken zijn waarin wél diepgaand onderzoek is gedaan met inzet van inbreukmakende opsporingsbevoegdheden, maar die niet (althans niet met voldoende bewijs) tot een verdachte hebben geleid. Uit de beschikbare cijfers is echter niet af te leiden om hoeveel zaken dat gaat.

Daarnaast is relevant dat in het conceptwetsvoorstel voor Boek 4 wordt voorgesteld de regeling van artikel 359a Sv te herzien. De kern van de voorgestelde wijziging is dat, waar het verbinden van processuele sancties aan onregelmatigheden in de huidige wet als discretionaire bevoegdheid van de rechter is geformuleerd, het conceptwetsvoorstel een meer imperatieve formulering bevat. De bepalingen strekken ertoe een richtsnoer te bieden in welke gevallen aan onrechtmatig handelen processuele sancties dienen te worden verbonden. Daarnaast wordt de reikwijdte van de regeling uitgebreid, onder meer door het loslaten van het vereiste dat de onrechtmatigheid in het voorbereidend onderzoek naar het tenlastegelegde feit moet hebben plaatsgevonden en door het onrechtmatig optreden van anderen dan opsporingsambtenaren en OM (bijvoorbeeld particulieren) onder de regeling te brengen.[76]

Het voorgaande brengt met zich dat toetsing achteraf door de zittingsrechter in het totale stelsel van rechtsbescherming meegewogen moet worden. De waarde die daaraan moet worden toegekend is mede afhankelijk van de vraag op welke wijze de regeling van processuele sancties in het uiteindelijke gemoderniseerde wetboek vorm zal krijgen.

Beklag tegen kennisneming en gebruik en verzoeken tot (gedeeltelijke) teruggave van gegevens

Huidig recht: beklag tegen kennisneming en gebruik van "inbeslaggenomen" gegevens

De huidige wet geeft belanghebbenden – naast de mogelijkheid dat de zittingsrechter de rechtmatigheid van in het vooronderzoek toegepaste bevoegdheden toetst – in een aantal situaties de mogelijkheid om beklag in te dienen bij de raadkamer over verschillende inbreuken die verband houden met gegevens die in de macht van de opsporing zijn geraakt. Beklag is onder de huidige regeling in artikel 552a Sv onder meer[77] mogelijk tegen:[78]

- de kennisneming of het gebruik van gegevens, vastgelegd tijdens een doorzoeking of op vordering verstrekt;
- de kennisneming of het gebruik van gegevens, opgeslagen, verwerkt of overgedragen door middel van een geautomatiseerd werk en vastgelegd bij een onderzoek in zodanig werk;
- de ontoegankelijkmaking van gegevens, aangetroffen in een geautomatiseerd werk, bedoeld in artikel 125o Sv, de opheffing hiervan of het uitblijven van een last tot zodanige opheffing.

Uit een uitspraak van de Hoge Raad van 24 januari 2017 (ECLI:NL:HR:2017:71) lijkt de conclusie getrokken te kunnen worden dat ook geklaagd kan worden over de kennisneming en het gebruik van gegevens die zijn ontleend aan een gegevensdrager die inbeslaggenomen is geweest.

[76] Zie de concept-memorie van toelichting bij Boek 4 (consultatieversie 29 november 2017), p. 85-90.

[77] Beklag is thans ook mogelijk (en vervalt) tegen de vordering van gegevens, de vordering medewerking te verlenen aan het ontsleutelen van gegevens en de vordering gegevens te bewaren en beschikbaar te houden. Beklag is niet mogelijk (en wordt niet gecreëerd) tegen kennisneming en gebruik van gegevens die op andere wijze verkregen zijn.

[78] Zie de concept-memorie van toelichting bij Boek 6 (consultatieversie 29 november 2017), p. 48.

Huidig recht: teruggave "onschuldige" gegevens op gegevensdrager met verboden bestanden?
De raadkamer beslist onder meer over beklag over ex artikel 94 Sv inbeslaggenomen voorwerpen als nog een uitspraak van de zittingsrechter te verwachten is. Dat oordeel is zeer terughoudend: het gaat erom of het belang van de strafvordering nog gediend is met voortzetting van het beslag, waarbij een marginale toets wordt aangelegd.

In de praktijk komt het geregeld voor dat op een inbeslaggenomen gegevensdrager naast verboden gegevens ook niet-verboden (hierna: "onschuldige") gegevens staan waarvan retournering wordt gevraagd, omdat deze gegevens uitsluitend op de inbeslaggenomen drager staan.

Die gegevens kunnen voor de verdachte maar ook voor zijn gezinsleden of voor derden grote (emotionele of economische) waarde hebben. Te denken valt daarbij aan uiteenlopende zaken als onvervangbare familiefoto's, onderwijsproducten als scripties, manuscripten en niet aan de strafzaak gerelateerde (financiële) administraties. Het kan, zeker nu de opslagcapaciteit van dragers nog steeds zeer sterk toeneemt, ook om zeer grote aantallen gegevens gaan. Er doen zich problemen voor wanneer wordt verzocht om teruggave van een gegevensdrager met "onschuldige" bestanden, wanneer op die gegevensdrager ook bestanden zijn aangetroffen die onttrekking of vernietiging vergen, of wanneer wordt verzocht om teruggave van "onschuldige" bestanden die zich bevinden op een inbeslaggenomen gegevensdrager (dat kan ook een volledige computer zijn) waarop ook te onttrekken of vernietigen gegevens voorkomen. Het eerste geval betreft in wezen beklag over het uitblijven van teruggave van het voorwerp, en daarbij zal de hiervoor genoemde terughoudende beoordeling spelen; het tweede wordt soms als subsidiair verzocht bij het beklag strekkende tot teruggave van de drager, maar soms ook zelfstandig.

Of een dergelijk beklag, strekkende tot *teruggave van gegevens* thans mogelijk is staat overigens ter discussie. Het Hof Den Haag heeft – na een contrair requisitoir van het Openbaar Ministerie – recent geoordeeld dat het huidige Nederlandse recht weliswaar geen beroep op de rechter openstelt voor verzoeken om (gedeeltelijke) teruggave van zich op inbeslaggenomen gegevensdragers bevindende gegevens, maar oordeelt dat, gelet op de verplichtingen voortvloeiende uit het EVRM aan betrokkene wel een rechtsingang moet worden geboden, zodat de Nederlandse rechter toch bevoegd is om over het verzoek te oordelen.[79]

Dergelijke verzoeken om gedeeltelijke teruggave van gegevens worden thans regelmatig aan de (straf)rechter ter beoordeling voorgelegd. De rechtspraak laat daarbij nog geen consistente lijn zien.[80] Integendeel, er is een breed scala van beslissingen en redeneringen zichtbaar, die zich in hoofdlijnen tussen twee uitersten bewegen: van "kale" onttrekking van de gehele gegevensdrager[81] tot opdracht aan de politie om (alleen) de strafbare (veelal kinderporno)gegevens van de gegevensdrager te verwijderen en deze drager daarna te retourneren,[82] dan wel (een deel van) de "onschuldige" bestanden te kopiëren en aan klager terug te geven, met onttrekking van de drager met verboden gegevens;[83] soms ook kiest de rechter een tussenoplossing.[84]

---

[79] Hof Den Haag 3 mei 2018, ECLI:NL:GHDHA:2018:1074, onder verwijzing naar onder andere EHRM 30 september 2014, Prezhdarovi t. Bulgarije, App.nr. nr. 8429/05, §49-50.

[80] Zie voor een duidelijke stellingname in de literatuur Van den Bos 2017; zie voor een kritische beschrijving van de huidige regelgeving ook Royer & Oerlemans 2017.

[81] Hof Amsterdam 6 april 2016, ECLI:NL:GHAMS:2016:1274; Rb. Amsterdam 20 oktober 2016, ECLI:NL:RBAMS:2016:8065 (niet gepubliceerd op rechtspraak.nl); Hof Arnhem-Leeuwarden 1 februari 2017, 21-004477-16, ECLI:NL:GHARL:2017:1124 (niet gepubliceerd op rechtspraak.nl). Zie ook Rb. Gelderland (militaire kamer) 19 maart 2018, ECLI:NL:RBGEL:2018:1204.

[82] Rb. Groningen 21 januari 2013, ECLI:NL:RBNNE:2013:BZ9663; in vergelijkbare zin Rb. Rotterdam 15 februari 2017, ECLI:NL:RBROT:2017:1501 en Rb. Rotterdam 20 oktober 2016, ECLI:NL:RBROT:2016:8345.

[83] Rb. Rotterdam 22 november 2017, ECLI:NL:RBROT:2017:9328.

[84] Rb. Rotterdam (MK) 25 januari 2017, ECLI:NL:RBROT:2017:642 (laptop met daarop negen kinderpornobestanden, opdracht aan OM: *of* teruggave laptop na verwijdering kinderporno, *of* niet-kinderpornobestanden van laptop overzetten op een door verdachte/klager aan te leveren gegevensdrager); in hoger beroep van dit vonnis komt het Hof Den Haag 3 mei 2018, ECLI:NL:GHDHA:2018:1074 ook tot een tussenoplossing: er moet een

De keuze voor kale onttrekking volgt wat veelal het standpunt van het Openbaar Ministerie is: dat de opdracht "onschuldige" bestanden af te zonderen voor teruggave zonder de inbeslaggenomen drager een onaanvaardbare werkbelasting betekent voor de beperkte opsporingscapaciteit, terwijl teruggave van de gegevensdrager na verwijderen van de "verboden" bestanden een onmogelijke opgave betekent, omdat volledige verwijdering, zonder dat (versleutelde) verboden restanten op de gegevensdrager achterblijven, vrijwel niet te garanderen is. Bovendien is de gegevensdrager met verboden bestanden – in het geval van kinderpornografie en dierenpornografie – een strafbaar voorwerp. Het bezit van die gegevensdrager is immers zelfstandig strafbaar gesteld.

Het conceptwetsvoorstel voor Boek 6: Wpg in plaats van beklag

In het conceptwetsvoorstel voor Boek 6 zijn alle beklagmogelijkheden over "inbeslaggenomen" gegevens geschrapt, met als argument dat hiervoor het wettelijke regime van de Wet politiegegevens (Wpg) voldoende toegerust is. De concept-memorie van toelichting zegt hierover:

> Alle persoonsgegevens die door de politie in het kader van de uitoefening van haar taak worden verwerkt, vallen onder de in artikel 1 van de Wet politiegegevens (Wpg) gegeven definitie van politiegegevens. Daarmee vallen ook de door opsporingsdiensten in beslag genomen gegevens onder het privacy-regime van deze wet. De Wpg biedt daarmee een ieder over wiens persoon politiegegevens worden verwerkt de mogelijkheid een verzoek tot verbetering, aanvulling, verwijdering, afscherming of markering te doen indien naar zijn oordeel de inbeslaggenomen gegevens niet ter zake dienend zijn, dan wel in strijd met een wettelijk voorschrift worden verwerkt (artikel 28 Wpg). De verantwoordelijke bericht de verzoeker binnen vier weken na ontvangst van het verzoek schriftelijk of, dan wel in hoeverre, hij voldoet aan het verzoek. Dit biedt dus de mogelijkheid om de (verdere) verwerking van de inbeslaggenomen gegevens te beïnvloeden, wat zoals hierboven beschreven vaak het doel is van na inbeslagneming van gegevens gedaan beklag. Een beslissing op een dergelijk verzoek geldt als een beschikking in de zin van de Algemene wet bestuursrecht, waartegen bezwaar en beroep openstaan (artikel 29 Wpg).[85]

Het stelsel van de Wpg biedt dus toegang tot de (bestuurs)rechter, die in individuele gevallen de gegevensverantwoordelijke instantie kan opdragen gegevens ter inzage te geven, te verbeteren, aan te vullen, te verwijderen of af te schermen.

De commissie stelt hierbij vast dat weliswaar het begrip persoonsgegevens door de Autoriteit Persoonsgegevens zeer ruim wordt uitgelegd, maar dat er dus geen rechtsingang bestaat voor gegevens die geen persoonsgegevens zijn (bijvoorbeeld de jaarrekening van een bedrijf). Voorts merkt de commissie op dat de Wpg alleen een ingang biedt voor personen met betrekking tot hun *eigen* persoonsgegevens; indien de "onschuldige" gegevens bijvoorbeeld familiefoto's zijn zonder dat de persoon die deze foto's op een inbeslaggenomen gegevensdrager had staan, zelf ook is afgebeeld of de maker is van deze foto's, is het niet duidelijk of het gaat om deze persoon betreffende persoonsgegevens.

(Gedeeltelijke) teruggave van gegevens?

De commissie merkt voorts op dat het voorgestane Wpg-regime geen oplossing biedt voor het hiervoor beschreven geval waarin wordt verzocht om *teruggave* van *bepaalde* zich op een inbeslaggenomen digitale-gegevensdrager of geautomatiseerd werk bevindende gegevens. Het gaat dan immers niet om "verbetering, aanvulling, verwijdering, afscherming of markering"

belangenafweging plaatsvinden tussen de strafvorderlijke en maatschappelijke belangen bij de onttrekking enerzijds en de persoonlijke belangen van (in dit geval) de verdachte bij behoud dan wel verkrijging van de verzochte gegevensbestanden anderzijds.

[85] Zie de concept-memorie van toelichting bij Boek 6 (consultatieversie 29 november 2017), p. 54.

(art. 28 Wpg) van de desbetreffende gegevens. De concept-memorie van toelichting bij Boek 6 verwijst ter zake naar de praktijk dat de politie c.q. het Openbaar Ministerie als "coulance" bepaalde gegevens van een dergelijke gegevensdrager kan retourneren.[86] De commissie constateert echter dat indien deze "coulance" niet wordt betracht, de belanghebbende als rechtsmiddel het beklag over het niet teruggeven van de inbeslaggenomen gegevensdrager openstaat. Wanneer deze tijdelijk (voor onderzoek) of definitief (noodzaak tot onttrekking aan het verkeer) niet kan worden teruggegeven, heeft de belanghebbende geen rechtsmiddel dat strekt tot teruggave van zijn "onschuldige" gegevens. Wel kan een belanghebbende bij de uiteindelijke verbeurdverklaring of onttrekking hopen op toepassing van de schadevergoedingsbepalingen van artikelen 33c en 36b Sr. Die zijn bedoeld als compensatie voor degene die onevenredig zwaar wordt getroffen door de onttrekking van het gehele voorwerp, maar die artikelen komen niet tegemoet aan de wens om (snel) weer over de gegevens te beschikken. Er is dan namelijk geen rechtsingang ingevolge de Wpg. Bovendien is het de vraag of de strafrechter bij het eindvonnis (dat soms jaren op zich kan laten wachten) dan wel een dergelijk oordeel zal kunnen en mogen vellen.

Het Openbaar Ministerie stelt zich thans op het standpunt dat het wettelijk systeem zich ertegen verzet dat de strafrechter een dergelijke opdracht of bevel tot gedeeltelijke teruggave van gegevens geeft. Indien de Hoge Raad het hiervoor genoemde arrest van het Hof Den Haag,[87] waarin op basis van het EVRM wel in een rechtsingang wordt voorzien, zou bekrachtigen, is codificatie van deze, thans buitenwettelijke, oplossing op zijn plaats. Hoe dan ook vormen de uiteenlopende rechterlijke beslissingen over het wel of niet teruggeven van gegevens dan wel van de geschoonde drager volgens de commissie een argument om te bepleiten dat de wetgever op dit punt tot onderzoek, nadere gedachtenvorming en eventueel regelgeving overgaat, dan wel de keuze een dergelijk rechtsmiddel niet open te stellen grondiger motiveert.

De commissie merkt op dat in de concept-memorie van toelichting bij Boek 6 ook geen beschouwing wordt gewijd aan de verenigbaarheid met het EVRM van de afschaffing van het beklag over de kennisneming en het gebruik van gegevens die zijn ontleend aan een gegevensdrager die in beslag is genomen. In het licht van het voorgaande acht de commissie een dergelijke nadere beschouwing (en waar nodig eventuele heroverwegingen) daaromtrent wel van wezenlijk belang. Dat geldt eens temeer nu opsporing door middel van onderzoek van digitale gegevens de komende decennia alleen maar zal toenemen.

Aanbeveling 10: bij de toelichting op de afschaffing van het beklag over gebruik en kennisneming van "inbeslaggenomen" gegevens (gegevens in de macht van de opsporingsinstanties) dient de wetgever aandacht te besteden aan:
a. de verenigbaarheid van de voorgestelde afschaffing van de beklagregeling voor gedragingen betreffende de kennisneming en het gebruik van gegevens afkomstig van inbeslaggenomen gegevensdragers met de verplichtingen voortvloeiende uit het EVRM; en
b. de bestaande rechtsbeschermingslacune ten aanzien van verzoeken om (gedeeltelijke) teruggave van zich op inbeslaggenomen gegevensdragers bevindende gegevens.
→ *p. 195*

4.3.3. Doelbinding

De normering van gegevensverkrijging en de normering van gegevensgebruik zijn "communicerende vaten". Beide normeringssystemen moeten in samenhang beschouwd worden. Bij het nadenken over de normering van gegevensverkrijgende bevoegdheden moet ook de normering van het gebruik van die gegevens na verkrijging betrokken worden. Deze gedachtegang is ook in het huidige wetboek al zichtbaar. In artikel 126cc Sv is een specifieke regeling opgenomen

[86] Concept-memorie van toelichting bij Boek 6 (consultatieversie 29 november 2017), p. 48.
[87] Hof Den Haag, 3 mei 2018, ECLI:NL:GHDHA:2018:1074.

voor het gebruik van gegevens die zijn verkregen door middel van "ongerichte" en heimelijke onderzoeksmethoden. Bij observatie met behulp van een technisch hulpmiddel dat signalen registreert, het opnemen van vertrouwelijke communicatie, het opnemen van telecommunicatie of het vorderen van gegevens over een gebruiker en het telecommunicatieverkeer met betrekking tot die gebruiker wordt op onselectieve wijze informatie over personen verkregen. In de memorie van toelichting is hierover het volgende opgemerkt:

> De voorgestelde regeling geldt voor processen-verbaal en andere voorwerpen waaraan gegevens kunnen worden ontleend die zijn verkregen door observatie met behulp van een technisch hulpmiddel dat signalen registreert, het onderzoek aan telecommunicatie of het opnemen van communicatie met een technisch hulpmiddel. Voor de toepassing van andere opsporingsbevoegdheden geldt zij niet. De reden hiervan is dat bij de toepassing van genoemde bevoegdheden door het gebruik van een technisch hulpmiddel op ongeselecteerde wijze informatie over personen wordt verkregen. Het is bulkinformatie, die zowel informatie omvat die relevant is, als ook informatie die niet relevant is voor de zaak, betreffende personen die in het geheel niets met de zaak van doen hebben. Het technisch hulpmiddel registreert zonder onderscheid alle signalen die het opvangt. Bij een dergelijke wijze van informatiegaring is het van belang duidelijke regels te stellen over de bewaring en vernietiging.[88]

Artikel 126cc Sv geeft een regeling voor het bewaren en vernietigen van genoemde gegevens. Artikel 126dd Sv bepaalt vervolgens, voor dezelfde categorie gegevens, dat gebruik voor andere doeleinden dan het onderzoek in het kader waarvan de verkrijgende bevoegdheid is ingezet alleen is toegestaan na verkregen toestemming van de officier van justitie. Beide bepalingen zijn in die zin een verzwaring ten opzichte van het regime van de Wpg. Anderzijds kunnen deze bepalingen juist gezien worden als een versoepeling ten opzichte van artikel 125n Sv, waarin is bepaald dat gegevens die tijdens een doorzoeking zijn vastgelegd vernietigd dienen te worden zodra blijkt dat zij van geen betekenis zijn voor het onderzoek.

Als het onderzoek aan digitale-gegevensdragers niet gericht plaatsvindt (in de woorden van de Hoge Raad: als het onderzoek uit meer bestaat dan "het raadplegen van een gering aantal bepaalde op de elektronische gegevensdrager of in het geautomatiseerde werk opgeslagen of beschikbare gegevens"[89]), zal, net als bij de bevoegdheden genoemd in artikel 126cc Sv, bulkinformatie verkregen kunnen worden. Daarbij zal zowel relevante als niet-relevante informatie worden overgenomen, ook over personen die niets met de zaak te maken hebben. Vanuit die parallel zou het niet onlogisch zijn om de gegevens verkregen via stelselmatig onderzoek in digitale-gegevensdragers toe te voegen aan het regime van de artikelen 126cc en 126dd Sv, al dan niet beperkt tot gevallen van heimelijk onderzoek, waarbij in het kader van artikel 126dd Sv enkel die gegevens kunnen worden hergebruikt waarvan is vastgesteld dat die relevant zijn voor een ander strafrechtelijk onderzoek of voor het verkrijgen van inzicht in de betrokkenheid van personen bij misdrijven en handelingen als bedoeld in artikel 10, eerste lid, onderdelen a en b, Wpg. Daarmee zou de inbreuk die wordt gemaakt door het onderzoek aan digitale-gegevensdragers verkleind kunnen worden door de bulkgegevens in het kader van artikel 126cc Sv te bewaren in een afgeschermde omgeving ("digitale kluis"), zonder koppeling met andere bestanden, waarbij alleen met toestemming door een bevoegde autoriteit in het kader van een ander onderzoek een zoekvraag mag worden losgelaten op deze afgeschermde gegevens.

4.3.4. Aanvullende vormen van (systeem)toezicht

Denkbaar is tot slot om aanvullende vormen van toezicht in te stellen. In het wetsvoorstel CC III is recent een aanvullende vorm van toezicht gecreëerd, door de Inspectie Justitie en Veiligheid te belasten met het toezicht op de uitoefening van de bevoegdheid tot het

[88] *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 86.
[89] HR 4 april 2017, o.a. ECLI:NL:HR:2017:584 (Smartphone).

binnendringen in een geautomatiseerd werk (voorgesteld artikel 126nba lid 7 Sv). De Inspectie zal toezien

> op de uitvoering van de voorgestelde bevoegdheid van het onderzoek in een geautomatiseerd werk binnen de grenzen van het bevel van de officier van justitie en de machtiging van de rechter-commissaris. Dit toezicht omvat zowel de gevallen die, in het kader van de door het openbaar ministerie ingestelde strafvervolging jegens een verdachte, aan het oordeel van de rechter worden voorgelegd als de gevallen die niet tot strafvervolging jegens een verdachte leiden. (…) Meer concreet heeft het toezicht betrekking op aspecten als de autorisaties van de bevoegde opsporings-ambtenaren voor de uitvoering van het bevel van de officier van justitie voor het onderzoek in een geautomatiseerd werk, de expertise en kennis van de betrokken opsporingsambtenaren, de inzet van het technische hulpmiddel (kwaliteit en betrouwbaarheid), de vastlegging van gegevens over de werking van het technische hulpmiddel en over de toepassing van onderzoekshandelingen in het geautomatiseerde werk (logging), de beveiliging van de vastgelegde gegevens en het gebruik van de gegevens, inclusief de bewaring en vernietiging daarvan. Het toezicht van de Inspectie VenJ is aldus gericht op het functioneren van het wettelijke systeem rond het onderzoek in een geautomatiseerd werk (systeemtoezicht). Het kader voor het toezicht wordt gevormd door de grenzen van het bevel en de machtiging voor het onderzoek in een geautomatiseerd werk. De oordeelsvorming door de officier of de rechter-commissaris, zoals deze tot uitdrukking komt in het bevel respectievelijk de machtiging, valt buiten dit kader.[90]

In het voorgestelde artikel 126nba lid 7 Sv wordt aldus voorzien in een vorm van systeem-toezicht voor zover het gaat om de uitoefening van de zogenaamde hackbevoegdheid door daartoe aangewezen opsporingsambtenaren.

In hoeverre het OM de regelgeving naleeft bij de uitoefening van zijn taak valt onder het toezicht van de procureur-generaal bij de Hoge Raad.[91] Artikel 122 lid 1 Wet RO bepaalt dat de procureur-generaal bij de Hoge Raad de minister in kennis kan stellen van het feit dat naar zijn oordeel het OM bij de uitoefening van zijn taak de wettelijke voorschriften niet naar behoren handhaaft of uitvoert. Deze bevoegdheid van de procureur-generaal bij de Hoge Raad hangt samen met diens opdracht te waken voor de handhaving en uitvoering van wettelijke voorschriften bij de gerechten zoals omschreven in artikel 121 Wet RO. Daarmee is een juridische grondslag gegeven voor het uitoefenen van toezicht op het OM door de procureur-generaal bij de Hoge Raad. In 2012 is besloten om in dit kader thematische onderzoeken te verrichten naar de wijze waarop het OM zijn taken uitvoert. Hierbij gaat de aandacht telkens uit naar de juridische kwaliteit van de onderzochte taak.[92] Voorstelbaar is dat de procureur-generaal onderzoek zal gaan doen naar de naleving van de wet door het OM bij de uitoefening van de bevoegdheid tot het binnendringen in een geautomatiseerd werk of andere ingrijpende opsporingsbevoegdheden.

Bij de vraag of aanvullend toezicht nodig is, is bovendien relevant dat de Europese Richtlijn 2016/680, die vertaald zal worden in een aangepaste Wpg, het toezicht door de Autoriteit Persoonsgegevens versterkt en verzwaart.[93] Een nieuw element hierin is dat de verwerkings-verantwoordelijke verplicht wordt een "gegevensbeschermingseffectbeoordeling" (*Data*

[90] *Kamerstukken II* 2016/17, 34 372, 6 Nota naar aanleiding van het verslag, p. 81 e.v.

[91] Sinds 1 juni 1999 maakt het parket bij de Hoge Raad als gevolg van de Wet reorganisatie Openbaar Ministerie en instelling landelijk parket (*Stb.* 1999, 194) geen deel meer uit van het Openbaar Ministerie. Zie hierover Fokkens & Kirkels-Vrijman 2011.

[92] Recent zijn kritische toezichtsrapporten verschenen over respectievelijk de naleving van de wet door het Openbaar Ministerie bij het uitvaardigen van strafbeschikkingen (*Beschikt en gewogen* (2014), *Wordt vervolgd: beschikt en gewogen* (2017) en *Beproefd verzet* (2017)) en de naleving van de wet door het Openbaar Ministerie bij het toevoegen van strafvorderlijke, justitiële en politiële gegevens aan het Bopz-dossier (*Gedeelde informatie* (2017).

[93] Zie *Kamerstukken II* 2017/18, 34 889, nr. 2, Wetsvoorstel tot wijziging van de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens ter implementatie van Europese regelgeving over de verwerking van persoonsgegevens met het oog op de voorkoming, het onderzoek, de opsporing en vervolging van strafbare feiten of de tenuitvoerlegging van straffen.

Protection Impact Assessment) op te stellen bij een voorgenomen nieuw soort verwerking die een hoog risico voor de rechten en vrijheden van natuurlijke personen oplevert. Als blijkt uit zo'n effectbeoordeling dat er inderdaad een hoog risico is, of anderszins het gebruik van nieuwe technologieën, mechanismen of procedures waaraan hoge risico's zijn verbonden wordt overwogen, dan verplicht de Richtlijn tot voorafgaande consultatie van de Autoriteit Persoonsgegevens. In artikel 47 van de Richtlijn zijn vervolgens de bevoegdheden van de Autoriteit Persoonsgegevens opgenomen, waaronder de bevoegdheid een gegevensverwerking te verbieden.

De commissie kan niet beoordelen welke betekenis aan de verzwaarde rol van de Autoriteit Persoonsgegevens moet worden toegekend voor het geheel aan waarborgen, en daarmee geen antwoord geven op de vraag of het noodzakelijk is te voorzien in andere vormen van toezicht. De commissie heeft onvoldoende zicht op de gevolgen van de inwerkingtreding van de Richtlijn en de taak van de Autoriteit Persoonsgegevens in relatie tot strafvorderlijk overheidsoptreden en het toezicht binnen de strafrechtsketen zelf. De wijze waarop de Autoriteit Persoonsgegevens deze nieuwe taak zal vormgeven is nog niet bekend. In ieder geval lijkt de introductie van een aanvullende vorm van zaakspecifiek toezicht op gespannen voet te staan met het stelsel van strafvordering, waarin immers het toezicht op strafvorderlijk optreden is "ingebouwd" als onderdeel van de verantwoordelijkheden van het OM en de rechter(-commissaris).

4.3.5. Conclusie

Het overzicht van overige algemene aspecten van normering – dat wil zeggen naast het door de commissie voorgestelde algemene normeringscriterium dat gekoppeld is aan een driedeling in voorafgaande toestemming – geeft een breed scala van waarborgen en vormen van toezicht weer. Het geeft ook aan hoe complex het totale stelsel van waarborgen is, waarbij de nodige vragen bestaan rond rechterlijke toetsing vooraf van cumulatieve inzet van bevoegdheden, rechterlijke toetsing achteraf, doelbinding en aanvullende vormen van toezicht, zoals besproken in deze paragraaf. Deze vragen verdienen beantwoording binnen het moderniseringstraject, met name ook met het oog op beantwoording van de vraag of aanvullende vormen van toezicht nodig zijn naast de van oudsher bestaande en recent ingevoerde vormen. Gelet op de complexiteit van deze vragen, die in samenhang moeten worden bezien, benadrukt de commissie haar conclusie in paragraaf 3.5 dat voor de langere termijn een fundamentele reflectie op het stelsel van toezicht op de opsporing nodig is – een reflectie die de opdracht van de commissie overstijgt maar wel van wezenlijk belang is voor een toekomstbestendig Wetboek van Strafvordering.

Aanbeveling 11: de commissie beveelt aan om bij de benodigde reflectie op het stelsel van toezicht op de gegevensvergaring en -verwerking door opsporingsdiensten (zie Aanbeveling 5), de in deze paragraaf (4.3) behandelde aspecten van normering te betrekken, waaronder vragen rond rechterlijke toetsing vooraf van cumulatieve inzet van bevoegdheden, rechterlijke toetsing achteraf, doelbinding en de diverse aanvullende vormen van (systeem)toezicht. → *p. 195*

4.4. Wetgevingstechniek

Hiervoor in dit rapport refereert de commissie aan "een duivels dilemma". In een tijd waarin digitale opsporingsbevoegdheden zich snel ontwikkelen waardoor zij bij toepassing een steeds grotere impact zullen hebben op de privacy van burgers, komt de klassieke manier van normeren in het strafprocesrecht steeds meer in het gedrang. Op de (middel)lange termijn zal deze normering dan ook anders moeten worden ingericht. Voor de kortere termijn valt nog wel binnen de huidige systematiek te werken, met dien verstande dat op het gebied van de wetgevingstechniek enkele bijstellingen overweging verdienen.

Dergelijke bijstellingen kunnen bijvoorbeeld voorkomen dat al op korte termijn nieuwe fenomenen in de (cyber)criminaliteit niet kunnen worden aangepakt of bepaalde nieuwe technologieën niet kunnen worden ingepast. De belangrijkste bijstelling betreft een normering in het gemoderniseerde wetboek die bestaat uit (tamelijk) abstracte criteria die van geval tot geval moeten en kunnen worden geïnterpreteerd. Een risico van ruimte voor interpretatie is evenwel een gebrek aan uniforme toepassing. Dit kan naar het oordeel van de commissie goeddeels worden ondervangen door een relatief uitgebreide memorie van toelichting waarin uitleg wordt gegeven over de betekenis van de nieuwe criteria. Voorts kunnen richtinggevende voorbeelden illustreren op welke wijze de criteria in de praktijk kunnen worden toegepast. Uiteraard kan in een memorie van toelichting geen uitputtende lijst van voorbeelden worden opgenomen. Een verdere categorisering van gevallen waarvan duidelijk is dat zij onder een bepaald criterium vallen, kan vervolgens wel worden gerealiseerd door interne richtlijnen en procedures. Waar dergelijke "soft law" een belangrijke invulling zal geven aan de wettelijke criteria, zal zij in verband met het kenbaarheidsvereiste openbaar moeten worden gemaakt.

Wil de wetgeving binnen de huidige systematiek nog voldoende ruimte kunnen geven om tijdig op nieuwe ontwikkelingen in te kunnen springen, dan moet naar het oordeel van de commissie ook gedacht worden aan uitbreiding van de mogelijkheden om bij Algemene maatregel van bestuur specifieke eisen te stellen aan bepaalde typen onderzoek of bepaalde typen geautomatiseerde werken of digitale-gegevensdragers. Hier doet zich wel een zeker spanningsveld voor. Wat kan in het licht van het strafvorderlijk legaliteitsbeginsel op een lager niveau worden geregeld, en in hoeverre is het wenselijk bij de totstandkoming van die regelgeving het parlement te betrekken? Er moet voor gewaakt worden dat de kernpunten en de essentiële waarborgen van de bevoegdheidsuitoefening, ook met het oog op het belang van toegankelijke regelgeving, op een te laag niveau regeling zullen vinden. Delegatiegrondslagen moeten zo concreet en nauwkeurig als mogelijk worden geformuleerd, zodat de Raad van State zorgvuldig kan toetsen of de formele wetgever heeft toegestaan dat de voorgestelde voorschriften bij AMvB worden geregeld.

Wat betreft de parlementaire betrokkenheid bij lagere regelgeving volgt uit de Aanwijzingen voor de regelgeving dat bij voorkeur moet worden vermeden dat de vaststelling van bepaalde voorschriften aan een lagere regelgever wordt gedelegeerd en tegelijkertijd wordt vastgelegd dat het parlement bij de regelgeving moet worden betrokken. In een enkel geval valt, aldus deze Aanwijzingen, aan gedelegeerde regelgeving met parlementaire betrokkenheid niet te ontkomen. De commissie kan zich voorstellen dat daarvan sprake kan zijn als het belang van een flexibele normering vereist dat bepaalde eisen aan een integere opsporing of voorschriften die raken aan de grond- en mensenrechten op een lager dan formeel-wettelijk niveau worden geregeld.

Een belangrijke legislatieve constatering is verder dat de voorschriften rondom de verwerking van gegevens in enerzijds het Wetboek van Strafvordering en anderzijds de Wpg en de Wjsg zowel qua wetgevingsproces als inhoudelijk niet naadloos op elkaar zijn afgestemd. Dat maakt het moeilijk om vast te stellen of de normering van de politiële, justitiële en strafvorderlijke gegevensverwerking goed op elkaar aansluit. Dit vraagstuk wordt in toenemende mate prangender, nu ook binnen een regulier opsporingsonderzoek steeds vaker grote databestanden worden "binnengehaald", onderzocht en mogelijk ter beschikking komen voor andere doeleinden dan de concrete strafzaak die daartoe de aanleiding gaf. Naar het oordeel van de commissie is het dan ook onvermijdelijk dat de wetgever zich op korte termijn zal buigen over de vraag of er in de onderlinge wisselwerking tussen deze wetten op bepaalde vlakken geen sprake is van lacunes of doublures en zo ja, op welke wijze en waar dit moet leiden tot nadere aanvulling en afstemming van regelgeving.

Bij een dergelijke integrale beschouwing van de gegevensverwerking in de politiële en justitiële sector is het van belang om de regeling van opsporingsbevoegdheden zuiver te houden,

dat wil zeggen in lijn met het in het Wetboek van Strafvordering gehanteerde opsporingsbegrip. Dit betekent dat quasi-strafvorderlijke onderwerpen niet (althans niet uitsluitend) in Boek 2 van het gemoderniseerde Wetboek van Strafvordering moeten worden geregeld, maar (ook) met *sui generis*-wetgeving zouden kunnen worden genormeerd. Quasi-strafvorderlijke onderwerpen zijn bijvoorbeeld verstoring – waarbij de overheidshandeling niet primair is gericht op waarheidsvinding en vervolging maar primair op het verstoren van strafbare activiteiten (zie ook par. 3.2) – en (grootschalige) niet-persoonsgerichte onderzoeksvormen die zowel een strafvorderlijke als een niet-strafvorderlijke component kunnen hebben (zoals ANPR).

In het voorafgaande is al enkele malen aan de orde gesteld dat het huidige wettelijke stelsel, waarop in het kader van de modernisering wordt voortgebouwd, niet zonder meer toereikend is om te voorzien in een adequaat niveau van toezicht op de uitoefening van onderzoeksbevoegdheden in een digitale omgeving. Er dient dan ook te worden nagedacht over andere of aanvullende vormen van toezicht, waaronder mogelijk ook vormen van toezicht die niet primair zien op individuele zaken of activiteiten maar op meer algemeen niveau van processen en gehanteerde methoden (zie ook par. 4.3.4). Naast de wijze waarop dergelijk toezicht in de wetgeving wordt verankerd, is het vanuit wetgevingstechniek ook van belang om bij het stellen van nadere voorschriften en het inrichten van nieuwe processen in het achterhoofd te houden op welke manier toezicht op de naleving van die voorschriften kan worden uitgeoefend.

Bij het stellen van eventuele (nadere) voorschriften en het inrichten van nieuwe processen zal de wetgever bovendien rekening moeten houden met de in artikel 20 van de Richtlijn politie- en justitiegegevens vastgelegde concepten van *gegevensbescherming door ontwerp* en *gegevensbescherming door standaardinstellingen*. Het gaat dan om regels die de beveiliging van persoonsgegevens optimaliseren of die een beperkte kennisneming waarborgen, zoals een hit-no-hit systeem of het uitgrijzen van geheimhouderinformatie. Het wetsvoorstel tot wijziging van de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens ter implementatie van de Richtlijn politie- en justitiegegevens (2016/680/EU) bevat op dit punt conceptbepalingen die van de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen verlangen. Volgens de commissie zou er door de wetgever ook nagedacht moeten worden over de vraag of vergelijkbare, betrekkelijk abstracte bepalingen een plaats moeten krijgen in het gemoderniseerde Wetboek van Strafvordering. Denkbaar is dat in dergelijke bepalingen de formele wetgever de lagere regelgever opdraagt bij het opstellen van voorschriften die betrekking hebben op de verwerking van persoonsgegevens nadrukkelijk met genoemde concepten rekening te houden.

Voor de wetgever is een geïntegreerde en anticiperende benaderingswijze van voortschrijdende technologie, privacybescherming en strafrechtelijke rechtshandhaving geen gemakkelijke opgave. En die opgave wordt er in de toekomst zeker niet gemakkelijker op, integendeel.

De commissie meent dat een permanente technisch-juridische adviescommissie waarin de deskundigheid van de verschillende disciplines bij elkaar is gebracht een belangrijke rol kan vervullen om te bevorderen dat tijdig door de wetgever wordt ingespeeld op nieuwe ontwikkelingen. De adviezen van een dergelijke commissie zouden kunnen bijdragen aan het politieke en maatschappelijk draagvlak van nieuwe wetgeving en zouden de wetgever behulpzaam moeten zijn om ervoor te zorgen dat nieuwe ontwikkelingen op een werkbare manier in wetgeving wordt omgezet zodat die wetgeving in de praktijk ook goed is toe te passen. Adviezen zouden op verzoek van de regering of de Staten-Generaal kunnen worden uitgebracht of op eigen initiatief van de technisch-juridische adviescommissie. Denkbaar is voorts dat ook dwarsverbanden worden gelegd met instellingen die zijn belast met vormen van (systeem-) toezicht op de opsporing en vervolging. Een belangrijke meerwaarde van een dergelijke permanente commissie is dat deze in staat is om proactief en tijdig adviezen te geven over wetsaanpassingen die nodig zijn in het licht van technische ontwikkelingen op de middellange termijn, waardoor belangrijke wenselijke wijzigingen tijdig op de agenda worden gezet. Dit geeft zowel

de wetgever als de maatschappij ruimte om de implicaties van technische ontwikkelingen voor wetgeving met voldoende tijd en diepgang te bediscussiëren, waarmee onvoldoende doordachte, ad hoc-aanpassingen kunnen worden voorkomen die ontstaan als ontwikkelingen niet tijdig worden gesignaleerd.

Aanbeveling 12: er wordt een permanente technisch-juridische adviescommissie ingesteld 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. → *p. 195*

5. Doorzoeking, beslag en gegevensvordering

De opdracht van de commissie ziet met name op de Hoofdstukken 7 en 8 van het conceptwetsvoorstel. In dit hoofdstuk van het rapport komen allereerst de onderwerpen van Hoofdstuk 7 van Boek 2 aan de orde. Eerst worden verschillende definities, zoals "gegevens" en "geautomatiseerd werk", besproken (par. 5.1). Vervolgens wordt het nieuw voorgestelde concept van beslag op gegevens aan de orde gesteld (par. 5.2). Een kernonderwerp betreft de vraag hoe het onderzoek van gegevens in of overgenomen uit digitale-gegevensdragers en geautomatiseerde werken moet worden vormgegeven en genormeerd; daarop wordt uitgebreid ingegaan in paragraaf 5.3. Vervolgens worden twee schakelbepalingen voorgesteld voor onderzoek van analoge-gegevensdragers en met het lichaam verbonden gegevensdragers (par. 5.4), waarna de belangrijkste flankerende bevoegdheden – bevriezingsmogelijkheden, biometrische toegangsverschaffing, netwerkzoeking en ontoegankelijkmaking van gegevens – de revue passeren (par. 5.5). Tot slot wordt het vorderen van gegevens behandeld (par. 5.6).

5.1. Terminologie en definities

5.1.1. Gegevens

De in het conceptwetsvoorstel gehanteerde definitie van gegevens luidt als volgt.

> **Artikel 2.1.1.1**
>
> g. gegevens: gegevens als bedoeld in artikel 80quinquies van het Wetboek van Strafrecht; [nieuw]

Deze definitie, die dus ongewijzigd wordt gehanteerd voor de context van Sv, luidt:

> **Artikel 80quinquies Sr**
>
> Onder gegevens wordt verstaan iedere weergave van feiten, begrippen of instructies, op een overeengekomen wijze, geschikt voor overdracht, interpretatie of verwerking door personen of geautomatiseerde werken.

Is de definitie passend en toekomstbestendig?

De definitie van gegevens is algemeen geformuleerd en generiek, en bestaat sinds 1993. In de literatuur wordt de definitie nauwelijks geproblematiseerd.[94]

Een onderdeel in de definitie dat wellicht vragen oproept is het begrip "feiten", zeker in een samenleving die wel wordt gekenschetst als "*post-truth*"[95] en "feitenvrij". Die termen worden vooral gebruikt in relatie tot politiek, maar in bredere zin lijkt het klassieke onderscheid tussen feiten en meningen vaker ter discussie te worden gesteld. In die zin is het begrip "feit" niet onproblematisch. Voor de definitie van gegevens hoeft dat echter geen gevolgen te hebben, omdat het nooit de bedoeling is geweest om een weergave van meningen uit te sluiten van het begrip "gegevens". "Feiten" in de definitie is niet bedoeld in de zin van "objectieve" feitelijkheden (wat dat ook mogen zijn), maar in de zin van elke aanduiding (bijvoorbeeld in de vorm van karakters of symbolen) van de (of beter: een) werkelijkheid, waaronder ook denkbeeldige werkelijkheden.[96] Daarom kan onzes inziens het begrip "feiten" in de definitie ruim

[94] Soms zijn kanttekeningen geplaatst bij het onderdeel "op overeengekomen wijze" (tot 2006: "al dan niet op overeengekomen wijze"), maar die betreffen een theoretische discussie die niet relevant is voor de toekomstbestendigheid.

[95] Oxford Dictionaries koos "post-truth" als woord van het jaar 2016, zie https://en.oxforddictionaries.com/word-of-the-year/word-of-the-year-2016 (laatst geraadpleegd 1 juni 2018).

[96] Zie *Kamerstukken II* 1989/90, 21551, nr. 3 p. 5: Onder feiten worden zowel reële als denkbeeldige gebeurtenissen begrepen.

worden geïnterpreteerd, in de zin dat het zowel zogenoemd "objectieve" als "subjectieve", en zowel reële als denkbeeldige, feitelijkheden omvat. De memorie van toelichting zou dit kunnen verduidelijken.

Een ander onderdeel in de definitie dat vragen kan oproepen is "personen of geautomatiseerde werken". In toenemende mate zullen ook "slimme" apparaten en robots gegevens verwerken; deze zullen echter, in de huidige interpretatie, onder het begrip "geautomatiseerd werk" vallen (zie par. 5.1.3), zodat ook weergaven van instructies aan "slimme" apparaten of robots onder het gegevensbegrip vallen. Mocht (anders dan de commissie adviseert) de wetgever besluiten een differentiatie aan te brengen in het begrip "geautomatiseerd werk" vanwege het erg ruime bereik ervan (zie par. 5.1.3), dan zal mogelijk ook de definitie van "gegevens" dienovereenkomstig moeten worden aangepast.

Verder zien wij geen aanleiding om te denken dat de definitie techniekafhankelijk is of interpretatieproblemen gaat opleveren vanwege technologische ontwikkelingen.

5.1.2. Elektronische gegevensdrager

Het wetsontwerp voert een definitie van "elektronische gegevensdrager" in:

> **Artikel 2.1.1.1**
>
> d. elektronische gegevensdrager: een gegevensdrager die uitsluitend is bestemd voor de opslag van elektronische gegevens; [nieuw]

De memorie van toelichting (p. 101) zegt hierover:

> In hoofdstuk 7 wordt ook de term elektronische gegevensdrager gehanteerd. Een elektronische gegevensdrager is een gegevensdrager waarop elektronische gegevens zijn opgeslagen en die niet onder het begrip geautomatiseerd werk valt. Het verschil tussen een elektronische gegevensdrager en een geautomatiseerd werk is dat een elektronische gegevensdrager niet in staat is zelfstandig bewerkingen uit te voeren. Dit verschil is in de term elektronische gegevensdrager tot uitdrukking gebracht door te benadrukken dat deze uitsluitend is bestemd voor de *opslag* van elektronische gegevens. Alleen in combinatie met een ander apparaat, meestal een geautomatiseerd werk, kunnen de gegevens die op een elektronische gegevensdrager zijn opgeslagen, zichtbaar worden gemaakt. De term elektronische gegevensdrager moet in die zin ruim worden opgevat dat het gaat om gegevensdragers waarop gegevens zijn opgeslagen die langs elektronische weg zichtbaar kunnen worden gemaakt. Hieronder vallen dus ook gegevensdragers waarbij de wijze van opslag magnetisch (harde schijf) of optisch (cd-rom) geschiedt. Een geautomatiseerd werk slaat ook langs elektronische weg gegevens op, maar is daarnaast in staat die gegevens te verwerken en over te dragen (artikel 80sexies Sr).

Is de definitie passend en toekomstbestendig?

Techniekafhankelijkheid en afbakening ten opzichte van "fysieke" dragers

Het is nuttig om een definitie te geven van "elektronische gegevensdragers", nu het onderzoek aan dergelijke dragers nader wordt genormeerd. De definitie lijkt redelijk duidelijk: zoals de memorie van toelichting aangeeft, is het vooral bedoeld om alle dragers (van gegevens die door geautomatiseerde werken worden verwerkt) te omvatten die niet zelf een geautomatiseerd werk zijn. Typische voorbeelden zijn de oude diskette en de huidige usb-stick, alsmede, zoals de memorie van toelichting aangeeft, losse harde schijven, cd-roms en, naar we mogen aannemen, dvd's en geheugenkaarten die in camera's of muziekspelers worden gebruikt.

Door de opsomming van voorbeelden, waaronder cd-rom en harde schijf, ondervangt de toelichting tot op zekere hoogte de techniekafhankelijkheid van de definitie, die immers beperkt is tot "elektronische" gegevensopslag. Aangezien gegevens die door geautomatiseerde werken verwerkt worden behalve elektronisch ook magnetisch of optisch worden opgeslagen, is het belangrijk dat dergelijke vormen van gegevensopslag ook onder de definitie vallen; de

toelichting maakt dat duidelijk. De memorie van toelichting rept echter niet van quantummechanische of biologische opslag (vgl. hieronder), die op middellange termijn ook zullen kunnen voorkomen. Zulke vormen kunnen in de toekomst (via teleologische interpretatie) ook onder de definitie worden geschaard, als de memorie van toelichting een inhoudelijk criterium geeft dat duidelijk maakt dat het de bedoeling is dat ook dergelijke typen gegevensdragers onder het begrip vallen.

De gekozen formulering ("het gaat om gegevensdragers waarop gegevens zijn opgeslagen die langs elektronische weg zichtbaar kunnen worden gemaakt") is daarvoor op zich geschikt, maar te ruim. Allerlei gegevens kunnen immers langs elektronische weg zichtbaar worden gemaakt, als er maar bepaalde apparatuur en programmatuur op worden losgelaten; ook gegevens opgeslagen op papier of in DNA-materiaal kunnen langs elektronische weg op een computerscherm zichtbaar worden gemaakt. Nu is daarvoor wel een bepaald type sensor nodig die gegevens uitleest en omzet in elektronische signalen, maar dat geldt evenzeer voor de cd-rom waarvoor een optische sensor nodig is. Het feit dat in de meeste geautomatiseerde werken een optische lezer voor cd's en dvd's is ingebouwd, in tegenstelling tot lezers van biomateriaal, is niet doorslaggevend; dat zou in de komende decennia immers best kunnen veranderen. Bovendien is de veelal in laptops en smartphones ingebouwde camera, in samenhang met scan-software, ook nu al in staat om geautomatiseerd gegevens van papier in te lezen en zichtbaar te maken op het scherm, zodat papieren gegevensdragers ook onder de definitie lijken te vallen. Hetzelfde geldt voor bijvoorbeeld nummerplaten van auto's, waarop gegevens staan die via ANPR-camera's en bijbehorende software geautomatiseerd worden afgelezen en daarmee elektronisch "zichtbaar" worden gemaakt in het ANPR-systeem.

De toelichting zou daarom een ander materieel criterium moeten geven om aan te duiden welke typen gegevensdragers beoogd worden onder de term te vallen. Het meest relevant is dat het gaat om dragers van gegevens die (primair) door geautomatiseerde werken worden verwerkt (alvorens ze door mensen kunnen worden gebruikt), en niet om dragers van gegevens die (primair) voor directe menselijke waarneming geschikt zijn. Te denken valt daarom aan een omschrijving als "dragers bestemd voor opslag van gegevens die geschikt zijn voor overdracht, interpretatie of verwerking door geautomatiseerde werken". Hiermee wordt aangesloten bij de definitie van gegevens (die zowel gegevens verwerkbaar door personen als gegevens verwerkbaar door geautomatiseerde werken omvat), waarbij in de regeling van gegevens*dragers* een onderscheid wordt gemaakt tussen enerzijds dragers van gegevens die geschikt zijn voor overdracht, interpretatie of verwerking door *personen* (oftewel dragers van gegevens bedoeld voor primair menselijke waarneming) en anderzijds dragers van gegevens die geschikt zijn voor overdracht, interpretatie of verwerking door *geautomatiseerde werken* (oftewel dragers van gegevens primair bedoeld voor waarneming door geautomatiseerde werken).

Aanbeveling 13: de omschrijving van bedoelde gegevensdragers in de memorie van toelichting moet worden aangepast, waarbij het criterium "dragers bestemd voor opslag van gegevens die geschikt zijn voor overdracht, interpretatie of verwerking door geautomatiseerde werken" kan worden gehanteerd. → *p. 195*

Terminologie

De term "elektronische gegevensdrager" is taalkundig ongelukkig: grammaticaal slaat hierin "elektronisch" op de drager en niet op de gegevens. Volgens de spellingregels schrijft men immers een drager van elektronische gegevens als "elektronischegegevensdrager".[97] (Dat in de praktijk deze spellingregel zelden wordt gevolgd, en ook de spellingcorrectie van Word "elektronischegegevensdrager" niet herkent, doet daar niet aan af.) Hoewel, zoals boven

[97] Zie Algemene Nederlandse Spraakkunst (2e druk 1997), p. 682 en 688.

aangegeven, de term elektronisch ook niet echt op de gegevens slaat, maar meer op de verwerkingsbestemming van de gegevens, zal duidelijk zijn dat de meeste *dragers* in elk geval niet "elektronisch" zijn – usb-sticks, geheugenkaarten en harde schijven bestaan primair uit metaal, plastic en andere materialen, en kunnen moeilijk "elektronische voorwerpen" worden genoemd (behalve in zoverre alle materie elektronen bevat, maar in dat opzicht is ook een theekopje "elektronisch"). Aangezien "elektronisch" dus zal slaan op de gegevens, niet de drager, zou de term daarom "elektronischegegevensdrager" moeten luiden. Indien men vindt dat deze term niet ten goede komt aan de leesbaarheid, kan men, in overeenstemming met de grammaticale regels, in plaats hiervan een koppelteken gebruiken: "elektronische-gegevensdrager".

Een meer principiële vraag is of de term "elektronische-gegevensdragers" wel de beste term is, aangezien ook gegevens die (voor verwerking in computers) optisch of quantummechanisch zijn opgeslagen bedoeld worden. Een optie is om de term "computergegevensdrager" te kiezen, aangezien deze uitdrukt waar het om gaat: dragers van gegevens die (primair) door computers worden verwerkt. De term zou ook aansluiten bij de nieuwe definitie van "geautomatiseerd werk", waarin de term "computergegevens" wordt gebruikt (zie par. 5.1.3). Die definitie is echter problematisch vanwege de circulariteit van het "computer"-begrip in de omschrijving (zie par. 5.1.3). Bovendien lijkt de term "computer" langzamerhand uit zwang te raken; men spreekt vooral van een laptop, desktop, tablet, smartphone of andere specifieke verschijningsvormen in plaats van de meer generieke computer, en mogelijk wordt de term over een jaar of twintig alleen nog in historische zin gebruikt.

Een beter alternatief vinden wij "digitale-gegevensdrager". Het begrip "digitaal" wordt in het algemeen gebruikt als aanduiding van computergegevens, en kan ook worden toegepast op optisch of quantummechanisch opgeslagen gegevens: het gaat immers nog steeds om gegevens in de vorm van equivalenten van nullen en enen. Toekomstige (bijvoorbeeld biologische of quantummechanische) vormen van gegevensopslag zullen data overigens niet per se in binaire vorm (nul of één) opslaan; DNA-opslag kan bijvoorbeeld werken met vier eenheden (A, C, T en G). Maar hoewel digitaal vaak geassocieerd wordt met een binair stelsel, duidt de term zelf daar niet op: digitaal is immers afkomstig van "digit", wat etymologisch samenhangt met "vinger", en de term duidt dus eerder op een tientallig dan een tweetallig stelsel. In die zin is de term flexibel genoeg om verschillende rekeneenheden te omvatten. "Digitaal" is al met al generieker, en daarmee toekomstbestendiger, dan "elektronisch". De term heeft ook de voorkeur boven "elektronische-gegevensdrager" bij enkele technische deskundigen van het Privacy & Identity Lab die de commissie consulteerde.

Aanbeveling 14: de term "elektronische gegevensdrager" wordt vervangen door de term "digitale-gegevensdrager". → *p. 195*

Definitie

Er bestaat een onderscheid tussen analoge-gegevensdragers (zoals papier) en digitale-gegevensdragers, en de commissie acht het niet wenselijk om het onderzoek aan inbeslaggenomen papieren volledig hetzelfde te behandelen als het onderzoek aan digitale-gegevensdragers (in plaats daarvan stelt de commissie een schakelbepaling voor, zie par. 5.4). Dit betekent dat het wenselijk is een definitie in het wetboek op te nemen van de "digitale-gegevensdrager", ter onderscheiding van analoge-gegevensdragers. Met de door ons voorgestelde terminologie zou de definitie uit het conceptwetsvoorstel komen te luiden: "een gegevensdrager die uitsluitend is bestemd voor de opslag van digitale gegevens".

Het is de vraag of het nodig is om "uitsluitend" in deze definitie op te nemen. De definitie is bedoeld exclusief te zijn ten opzichte van geautomatiseerde werken: het zijn elkaar uitsluitende begrippen. Maar als een digitale-gegevensdrager gekenmerkt wordt door de eigenschap dat

deze "niet in staat is zelfstandig bewerkingen uit te voeren" (memorie van toelichting, p. 101), dan betekent dit dat gegevensdragers enkel die dragers zijn die geen enkele vorm van programmatuur bevatten. Maar de meeste typische gegevensdragers, zoals een geheugenkaart, een usb-stick en een losse harde schijf, bevatten al enige vorm van software die het schrijven en lezen van de gegevens mogelijk maakt – zogeheten firmware. Op zich doet dergelijke firmware geen afbreuk aan de kwalificatie als gegevensdrager; wezenlijk is immers de *bestemming* van de betreffende dragers als (louter) drager van gegevens. Dat er firmware op een usb-stick staat om lezen en schrijven van gegevens te faciliteren betekent niet dat de bestemming "opslag" wijzigt.

Het is echter mogelijk wel problematisch dat de wat geavanceerdere vormen van gegevensdragers regelmatig encryptiesoftware of andere programmatuur bevatten die de opslag van gegevens verder faciliteert door bepaalde bewerkingen op de gegevens mogelijk te maken. In dat geval is het de vraag of de bestemming nog uitsluitend opslag van gegevens is, en niet ook verwerking van gegevens. In elk geval maakt de constructie de definitie behoorlijk techniekafhankelijk: de kwalificatie van bijvoorbeeld een externe harde schijf of een usb-stick (of toekomstige veelgebruikte equivalenten daarvan) als gegevensdrager is immers afhankelijk van de vraag of de producent bepaalde software meelevert en of die software uitsluitend de opslag van gegevens faciliteert dan wel ook bewerkingen van gegevens toestaat.

Dat betekent dat de gegevensdragers, waaronder typen die de memorie van toelichting noemt als "elektronische gegevensdrager", zodra er "toegevoegde waarde"-programmatuur op staat, niet meer onder de definitie van "digitale-gegevensdrager" vallen maar onder die van "geautomatiseerd werk". In de definitie van dit laatste begrip (zie par. 5.1.3) wordt niet langer gesproken van een cumulatieve eis van opslag, overdracht en verwerking van gegevens, maar van verwerking van gegevens op basis van een programma; die definitie is dus van toepassing op alle gegevensdragers die een vorm van programmatuur bevatten. Dit schept verwarring, omdat wanneer er software op een externe harde schijf of usb-stick staat, dit voor de meeste mensen nog steeds een gegevensdrager en geen computer zal zijn; de juridische kwalificatie komt dan ver af te staan van het normale spraakgebruik.

Ook ontstaat mogelijk een lacune als een drager niet uitsluitend bestemd is voor opslag, maar ook niet onder de definitie van geautomatiseerd werk valt; bij de huidige dragers lijkt dat niet het geval, maar het valt voor de toekomst niet geheel uit te sluiten.

Om te voorkomen dat (toekomstige) dragers van digitale gegevens tussen wal en schip vallen, stelt de commissie daarom voor "uitsluitend bestemd" te vervangen door "bestemd of mede bestemd". Om het begrip af te kaderen van geautomatiseerde werken, kan de clausule worden toegevoegd dat de drager niet zelf een geautomatiseerd werk is. In combinatie met de hierboven voor de memorie van toelichting gesuggereerde omschrijving van bedoelde dragers, adviseert de commissie om de volgende definitie op te nemen.

> **Aanbeveling 15**: de definitie van "digitale-gegevensdrager" luidt: "een gegevensdrager, niet zijnde een geautomatiseerd werk, bestemd of mede bestemd voor de opslag van gegevens die geschikt zijn voor overdracht, interpretatie of verwerking door geautomatiseerde werken". → *p. 195*

Overigens is het niet per se nodig om überhaupt nog een onderscheid te maken tussen digitale-gegevensdragers en geautomatiseerde werken. Het onderzoek aan of in geautomatiseerde werken in het kader van de strafvordering is immers, evenzeer als onderzoek aan of in digitale-gegevensdragers, gericht op de aanwezige gegevens en niet op de (al dan niet aanwezig zijnde) verwerkingscapaciteit van de drager. Nu de commissie aanbeveelt om systematisch digitale-gegevensdragers en geautomatiseerde werken gelijkelijk te behandelen (zie hieronder, kopje "Samenhang met geautomatiseerde werken"), valt er ook iets voor te zeggen om beide

begrippen in één overkoepelend begrip te vatten. (Op zich zou daarvoor ook de term "digitale-gegevensdrager" kunnen worden gehanteerd, die dan zowel dragers met als dragers zonder verwerkingscapaciteit aanduidt; het gaat immers uiteindelijk om de eigenschap van het voorwerp als drager van digitale gegevens.) De commissie acht het verdedigbaar om verschillende begrippen te blijven hanteren, vanwege de historische en verdragsrechtelijke context; in de computercriminaliteitswetgeving en in het Cybercrime-verdrag staan van oudsher immers geautomatiseerde werken (of in verdragstermen computersystemen) voorop in de bepalingen, waarbij alleen secundair wordt verwezen naar gegevensdragers. De wetgever zou er niettemin, in het kader van de modernisering, ook voor kunnen kiezen om één overkoepelend begrip te gaan hanteren.

Voorwerpen met ingebouwde gegevensdragers

Naast usb-sticks en geheugenkaarten, zijn er ook minder typische voorbeelden van digitale-gegevensdragers, bijvoorbeeld een chip in een alledaags voorwerp als een autosleutel waarin gegevens zijn opgeslagen. Er zijn tegenwoordig veel voorwerpen met ingebouwde chips voor (een meestal beperkte vorm van) gegevensopslag. Valt zo'n voorwerp onder de definitie van een digitale-gegevensdrager, en zo ja, is de gegevensdrager dan de chip of de autosleutel? Naar de definitie uit het conceptwetsvoorstel kan alleen de chip een digitale-gegevensdrager zijn; in de door de commissie voorgestelde definitie kan ook de sleutel als geheel als digitale-gegevensdrager worden gezien – deze is immers mede bestemd voor de opslag van gegevens. Dat kan vragen oproepen over de inbeslagneming van een digitale-gegevensdrager en het onderzoek daaraan; valt onder het onderzoek aan de inbeslaggenomen digitale-gegevensdrager dan ook bijvoorbeeld onderzoek aan de sleutel op vingerafdrukken? Naar ons idee past de inbeslagneming systematisch onder de inbeslagneming van voorwerpen. Echter, bij het *onderzoek aan* inbeslaggenomen voorwerpen, dient onderscheid te worden gemaakt tussen onderzoek aan het voorwerp *als voorwerp* (dus onderzoek van de sleutel op vingerafdrukken of andere fysieke sporen) en onderzoek aan het voorwerp als digitale-gegevensdrager (dus onderzoek van de chip op daarin opgeslagen gegevens, die valt onder de regeling betreffende digitale-gegevensdragers).

Gegevensopslag in (synthetisch) biologisch materiaal

Ontwikkelingen in DNA-technologie maken het mogelijk om gegevens in DNA op te slaan. In 2012 slaagden onderzoekers erin een boek van 5,27 megabits (ongeveer 52.000 woorden) op te slaan in DNA, en dit vervolgens weer uit te lezen via DNA-*sequencing*.[98] Het gaat daarbij om synthetisch gegenereerd DNA – niet om het DNA van een persoon. In 2017 publiceerden onderzoekers resultaten van het omzetten van zes bestanden (waaronder een volledig besturingssysteem en een computervirus en een film uit 1895) in DNA – 72.000 stukjes van 200 basenparen. De bestanden konden met DNA-sequencing-technieken foutloos worden uitgelezen uit het DNA. Interessant is ook dat met polymerasekettingreactie (de techniek die ook wordt gebruikt bij het maken van DNA-profielen uit sporenmateriaal) een vrijwel onbeperkte hoeveelheid foutloze kopieën kon worden gegenereerd van de DNA-geëncodeerde bestanden. In theorie kan met deze techniek 215 petabyte (215 miljoen gigabyte) in één gram DNA worden opgeslagen.[99] In plaats van kasten vol harde schijven, zou een enorme kinderpornoverzameling aldus in één reageerbuisje kunnen worden bewaard. In de praktijk zal dat niet zo snel gaan; daarvoor is de technologie nog veel te duur. Ook is het opslaan en uitlezen langzaam. De prijs zal echter gestaag omlaag gaan, en het is voorzienbaar dat vroeger of later ook misdadigers de opslagcapaciteiten van DNA kunnen gaan benutten. Het nieuwe wetboek zal daar rekening mee moeten houden.

[98] Church e.a. 2012.
[99] Service 2017.

De vraag rijst of DNA-materiaal dat wordt gebruikt voor gegevensopslag als een digitale-gegevensdrager kan gelden, en, als dat niet het geval is, of de definitie in dat licht aanpassing behoeft. De voorgestelde definitie lijkt de commissie ruim genoeg om ook biologische opslag te omvatten. DNA-materiaal kan in dit geval – waarbij DNA dus bewust gebruikt wordt om gegevens in op te slaan, te onderscheiden van DNA als natuurlijke drager van gegevens – worden gezien als gegevensdrager, niet zijnde een geautomatiseerd werk, dat bestemd is voor de opslag van gegevens. Deze gegevens zijn geschikt voor interpretatie of verwerking door geautomatiseerde werken, aangezien we de constellatie van apparatuur die gebruikt wordt voor DNA-sequencing kunnen opvatten als een groep van apparaten, waarvan er één of meer op basis van een programma digitale gegevens (de letters A, C, G en T) verwerken.

Met de verdere ontwikkeling van synthetische biologie is het voorstelbaar dat ook andere materialen op een vergelijkbare wijze als opslagmedium voor gegevens kunnen dienen. De redenering hierboven over synthetisch-DNA-opslag geldt dan evenzeer voor andere organische materialen, zoals polymeren, die als gegevensopslagmedium kunnen dienen.

De commissie concludeert dat de voorgestelde definities geen aanpassing behoeven in het licht van biologische gegevensverwerking en -opslag, maar dat het wenselijk is in de toelichting aandacht te besteden aan DNA-materiaal en vergelijkbare organische materialen als potentiële toekomstige digitale-gegevensdrager, zodat de wetsgeschiedenis houvast biedt wanneer dergelijke opslag ergens in de komende decennia praktisch mogelijk wordt. Uit de toelichting zou duidelijk naar voren moeten komen dat de definitie nadrukkelijk beoogt techniek-onafhankelijk te zijn zowel qua opslagmethode als qua opslagmateriaal: het is het *bestemd of mede bestemd zijn* voor de opslag van gegevens die geschikt zijn voor overdracht, interpretatie of verwerking door geautomatiseerde werken dat beslissend is voor het antwoord op de vraag of een voorwerp, stof of substantie als digitale-gegevensdrager wordt aangemerkt, niet de wijze waarop de opslag plaatsvindt of het medium waarop dat gebeurt.

> **Aanbeveling 16**: in de memorie van toelichting dient te worden ingegaan op synthetisch-DNA-materiaal en vergelijkbaar organisch materiaal (waaronder ook synthetisch biologisch materiaal) als gegevensdrager, waarbij beargumenteerd kan worden dat dit onder de definitie van digitale-gegevensdrager valt. Daarbij moet tot uitdrukking worden gebracht dat de definitie van digitale-gegevensdrager beoogt techniek-onafhankelijk te zijn zowel qua opslagmethode als qua opslagmateriaal.
>
> → *p. 196*

Samenhang met geautomatiseerde werken

Een afgrenzingsprobleem is dat een gegevensdrager, naar wij aannemen, ook een apparaat is; volgens de nieuwe definitie van geautomatiseerd werk (zie par. 5.1.3) kan een apparaat ook onderdeel van een geautomatiseerd werk zijn, als het ermee verbonden is of samenhangt. De definitie spreekt immers van een "groep van onderling verbonden of samenhangende apparaten", en het lijkt voor de hand te liggen dat een usb-stick die (op het moment van onderzoek of inbeslagneming) in een geautomatiseerd werk steekt, onderdeel uitmaakt van dat werk. Het is dan immers een vrij duidelijke eenheid. Hetzelfde zou dan gelden voor een apparaat dat draadloos verbonden is met het geautomatiseerde werk – dat is immers een functioneel equivalent van een ingestoken usb-stick of een per kabel aangesloten externe harde schijf. Maar de vervolgvraag is wanneer het externe apparaat nog deel uitmaakt van het geautomatiseerde werk als deze niet feitelijk verbonden is op het moment van onderzoek of inbeslagneming. Zijn het los op een computer liggende usb-stick en de externe harde schijf waarvan de kabel naar de computer los ligt, een zelfstandige gegevensdrager, of onderdeel van het geautomatiseerde werk (als samenhangende groep), of beide? Zijn dragers die in de kast liggen maar draadloos verbonden kunnen worden met een geautomatiseerd werk, zelfstandige dragers of onderdeel van het geautomatiseerde werk, of beide?

Voor de meeste bepalingen heeft dit overigens geen bijzondere gevolgen, aangezien in het conceptwetsvoorstel digitale-gegevensdragers en geautomatiseerde werken qua bevoegdheden veelal op gelijke voet worden behandeld. Er zijn echter wel verschillen; in de artikelen 2.7.4.1.2 en 2.7.4.2.2, die beide de netwerkzoeking betreffen, wordt alleen gesproken over een "elders aanwezig geautomatiseerd werk". Volgens ons is het wenselijk om dit verschil in behandeling op te heffen, en geautomatiseerde werken en digitale-gegevensdragers consistent gelijk te behandelen. Het onderscheid dient geen doel: noch voor het doel van het onderzoek noch voor de rechtsbescherming maakt het immers uit of digitale gegevens op een geautomatiseerd werk of op een digitale-gegevensdrager staan; het gaat om de digitale gegevens zelf en de wijze van onderzoek daarvan.[100]

Aanbeveling 17: in het wetsvoorstel wordt overal consistent gesproken over "geautomatiseerd werk of een digitale-gegevensdrager". → *p. 196*

Een consequentie hiervan is dat in de door de commissie voorgestelde systematiek, in tegenstelling tot de huidige wet, ook onderzoek op afstand toegestaan wordt van digitale-gegevensdragers die niet vallen onder het begrip geautomatiseerd werk. In het in het wetsvoorstel CC III opgenomen artikel 126nba Sv wordt slechts het binnendringen in een geautomatiseerd werk mogelijk gemaakt. Door de gelijke behandeling van geautomatiseerde werken en digitale-gegevensdragers, zou in het commissievoorstel het van afstand binnendringen, evenals de netwerkzoeking, mogelijk moeten worden in digitale-gegevensdragers. De commissie acht dit aanvaardbaar, ten eerste omdat het past in de systematiek (het valt moeilijk in te zien waarom onderzoek op afstand mogelijk moet zijn in geautomatiseerde werken maar niet mogelijk zou moeten zijn in digitale-gegevensdragers), en ten tweede omdat het om een kleine, mogelijk vooral theoretische, uitbreiding gaat. Het is immers (in elk geval op dit moment) technisch niet mogelijk om vanuit een andere locatie een digitale-gegevensdrager te doorzoeken (tenzij deze feitelijk, al dan niet draadloos, verbonden is met een geautomatiseerd werk, maar in dat geval maakt de drager volgens de definitie deel uit van het geautomatiseerde werk). Dat kan in de toekomst anders zijn, maar wanneer het technisch mogelijk zou zijn om op afstand digitale-gegevensdragers uit te lezen, zal zo'n drager al snel onder de definitie van een geautomatiseerd werk vallen. En voor zover dat niet het geval zou zijn, is de uitbreiding tot dit type dragers verdedigbaar vanuit de systematiek van de regeling en het feit dat het onderzoek aan dezelfde voorwaarden moet voldoen als het onderzoek op afstand in een geautomatiseerd werk.

5.1.3. Geautomatiseerd werk

Tot nu toe kent het Wetboek van Strafvordering geen definitie van geautomatiseerd werk, maar heeft de definitie uit het Wetboek van Strafrecht ook daar te gelden. Dit is in de literatuur bekritiseerd,[101] zodat het voorstel om een definitie in het gemoderniseerde wetboek op te nemen instemming verdient.

Artikel 2.1.1.1

e. geautomatiseerd werk: een geautomatiseerd werk als bedoeld in artikel 80sexies van het Wetboek van Strafrecht; [nieuw]

[100] Wel achten wij het relevant om op conceptueel niveau onderscheid te blijven maken tussen dragers van digitale gegevens en dragers van analoge gegevens (zoals papier). Hoewel het voor beide uiteindelijk gaat om de gegevens, en niet om de wijze waarop deze zijn vastgelegd, verschilt het onderzoek van digitale-gegevensdragers in belangrijke opzichten (zoals schaal, wijze van onderzoek en automatiseerbaarheid) van onderzoek van analoge-gegevensdragers. Zie hierover par. 5.4.

[101] Wiemans 2004, p. 238-240.

Deze definitie luidt momenteel nog: "Onder geautomatiseerd werk wordt verstaan een inrichting die bestemd is om langs elektronische weg gegevens op te slaan, te verwerken en over te dragen." Als het wetsvoorstel CC III van kracht wordt, komt deze als volgt te luiden:

> **Artikel 80sexies**
>
> Onder geautomatiseerd werk wordt verstaan een apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerken.

Is de definitie passend en toekomstbestendig?

Techniekafhankelijk?

Een kritiekpunt op de huidige definitie van geautomatiseerd werk in het Wetboek van Strafrecht is dat deze techniekafhankelijk is door gebruik van de term "langs elektronische weg", waardoor computers die op basis van andere computationele technieken werken, zoals quantumcomputers of biologische computers, niet onder de definitie vallen.[102] Nu zijn dergelijke computers al lang in ontwikkeling maar nog redelijk ver van invoering in de markt, maar het valt zeker niet uit te sluiten dat dit laatste ergens in de komende decennia wel zal gebeuren. Op het vlak van quantumcomputers worden de laatste tijd significante vorderingen gemaakt, terwijl ook bio-computers stappen vooruit maken. Belangrijk is daarom dat het begrip en de definitie van geautomatiseerde werken in het gemoderniseerde wetboek ruim genoeg is om ook andere typen computers dan de huidige elektronische-gegevensverwerkers te omvatten. De definitie uit het wetsvoorstel CC III doet dat, door het woord "elektronisch" te vermijden en in plaats daarvan te spreken van "geautomatiseerd" en "computergegevens". De definitie lijkt in dat licht voldoende toekomstbestendig. Wel is het voor de toekomstige rechtszekerheid wenselijk als de memorie van toelichting ook expliciteert dat het de bedoeling is dat ook quantumcomputers en biologische computers, wanneer deze eenmaal op de markt zouden komen, onder de definitie vallen.

Circulair

In het wetsvoorstel CC III is ervoor gekozen om bij de definitie aan te sluiten bij het Cybercrime-verdrag, mede op advies van de Raad van State.[103] De aanbeveling van de Raad om het begrip "computergegevens" niet op te nemen in de definitie, is echter niet overgenomen: het maakt nu deel uit van de omschrijving van wat een geautomatiseerd werk is. Dit is verwarrend, omdat hiermee een zekere circulariteit ontstaat: het begrip "geautomatiseerd werk" is immers, ook door de wetgever, van oudsher bedoeld als synoniem voor "computer" en het is dan onhandig om de term "computer" terug te laten keren in de definitie.[104] Bovendien is onduidelijk wat het begrip "computergegevens" inhoudt; het is niet dezelfde term als het begrip "gegevens" dat elders steeds in de wet wordt gebruikt, en het begrip wordt nergens gedefinieerd of toegelicht. In dat licht valt aan te bevelen, zoals in de literatuur betoogd, om uit het oogpunt van zowel logica als wetssystematiek "computergegevens" in de voorgestelde definitie te vervangen door de term "gegevens".[105] In lijn met de term en de definitie van "digitale-gegevensdrager" ligt het echter meer voor de hand om in de definitie niet de term "gegevens"

[102] Koops & De Roos 2007, p. 24n.

[103] In het ontwerp dat aan de Raad werd voorgelegd, was gekozen voor een definitie ontleend aan Richtlijn 2013/40/EU, die de Raad bekritiseerde omdat de definitie niet alleen het geautomatiseerde werk omvatte maar ook de daarop opgeslagen, verwerkte of overgedragen gegevens.

[104] Als we moeten aannemen dat "computergegevens" gegevens zijn die door computers worden verwerkt en dat computers geautomatiseerde werken zijn, ontstaat een circulaire definitie: "Onder geautomatiseerd werk wordt verstaan een apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch gegevens verwerken die door geautomatiseerde werken worden verwerkt."

[105] Koops e.a. 2016, p. 11.

te hanteren, maar "digitale gegevens" – dat is immers in de kern ook wat geautomatiseerde werken verwerken.

Aanbeveling 18: indien het wetsvoorstel CC III wordt aangenomen, wordt in de definitie van het begrip "geautomatiseerd werk" de term "computergegevens" vervangen door "digitale gegevens". → *p. 196*

Koppeling met Wetboek van Strafrecht of een andere definitie of ander begrip?
De definitie verwijst naar die in het Wetboek van Strafrecht; zoals de memorie van toelichting aangeeft, is het bestendige praktijk om aan het begrip geautomatiseerd werk in het Wetboek van Strafvordering dezelfde betekenis toe te kennen als deze heeft in Wetboek van Strafrecht. Het wetsontwerp consolideert deze praktijk, zonder nadere toelichting.[106] Vanuit systematisch oogpunt is het wenselijk dat begrippen in beide wetboeken zoveel mogelijk dezelfde betekenis hebben; ze geven immers gezamenlijk het strafrecht vorm. Het is echter geen wet van Meden en Perzen; er kunnen redenen zijn om begrippen in het ene wetboek anders te interpreteren dan in het andere wetboek, dan wel om een ander begrip te gebruiken in het Wetboek van Strafvordering om geautomatiseerde werken aan te duiden dan in het Wetboek van Strafrecht. De belangen zijn immers gedeeltelijk verschillend: in het materiële strafrecht is een geautomatiseerd werk vooral een voorwerp dat, via strafbaarstellingen, wordt beschermd om de vertrouwelijkheid, integriteit en toegankelijkheid van gegevens en gegevensverwerkingsprocessen te waarborgen; daarbij is van belang dat geautomatiseerde werken een bepaald type apparaten zijn, bestemd voor zowel de opslag als voor de overdracht en verwerking van gegevens. In het procesrecht is het geautomatiseerd werk vooral een object van onderzoek; hoewel de functies van overdracht en verwerking wel een rol kunnen spelen, is het geautomatiseerde werk voor de opsporing vaak toch vooral een type apparaat waarin veel gegevens liggen opgeslagen.[107]

In die zin is het geautomatiseerde werk in de context van het Wetboek van Strafvordering vooral een bijzonder type digitale-gegevensdrager, namelijk één waarop veelal een grote hoeveelheid data van verschillende aard en uit uiteenlopende contexten ligt opgeslagen. Mogelijk valt er in dat licht iets voor te zeggen om niet, zoals het wetsontwerp doet, een onderscheid te maken tussen apparaten die uitsluitend dienen ter opslag van gegevens ("digitale-gegevensdragers") en apparaten die naast opslag ook gegevens verwerken en overdragen ("geautomatiseerd werk"), maar een onderscheid te maken tussen bijvoorbeeld digitale-gegevensdragers die naar hun aard beperkt zijn in hun capaciteit of in de typen gegevens die zij normaliter bevatten (taakspecifieke gegevensdragers) en digitale-gegevensdragers die naar hun aard een grotere capaciteit hebben of normaliter meerdere typen gegevens bevatten (multifunctionele gegevensdragers). Een keuze voor een ander begrippenkader heeft ingrijpende systematische consequenties voor de voorgestelde regeling, maar het is wel een belangrijke principiële (voor)vraag of binnen de context van opsporing geautomatiseerde werken afgebakend moeten worden ten opzichte van digitale-gegevensdragers, of dat een ander onderscheid passender is. Deze vraag hangt samen met een ander punt: de vraag of de huidige definitie niet te ruim is.

Een ruime definitie – is differentiatie nodig?
Het begrip "geautomatiseerd werk" is heel ruim:

[106] "Omdat deze begrippen inmiddels ook in het Wetboek van Strafvordering een belangrijke plaats zijn gaan innemen, is wenselijk deze begrippen thans ook in het nieuwe wetboek te definiëren, waarbij wordt aangesloten bij de definitie die in het Wetboek van Strafrecht wordt gegeven." Memorie van toelichting, p. 100.
[107] Koops e.a. 2016, p. 126 (waarin de vraag wat nu de kern uitmaakt van geautomatiseerde werken in de context van opsporing beantwoord wordt met "het element van opslag, waarbij de secundaire functionaliteiten van overdracht en verwerking gevolgen hebben voor de manier waarop opgeslagen gegevens onderzocht kunnen worden (vandaar de invoering van steunbevoegdheden als ontsleutelbevel en netwerkzoeking)").

> Steeds meer apparaten vallen tegenwoordig onder het begrip geautomatiseerd werk. Niet alleen een personal computer, laptopcomputer en server vallen hieronder, ook een tablet, smartphone, navigatiesysteem, digitale camera, moderne auto, smart TV en andere "smart" huishoudelijke apparatuur, zoals een smart koelkast, wasmachine of thermostaat vallen onder dit begrip. Dit betekent dat voor zover deze geautomatiseerde werken niet alleen gegevens verwerken maar ook opslaan en de opsporingsdiensten de beschikking willen krijgen over de op die apparatuur opgeslagen gegevens, de bepalingen van dit hoofdstuk van toepassing zijn.[108]

In de memorie van toelichting bij het wetsvoorstel CC III wordt uitgelegd waarom de definitie ook technische apparaten omvat,

> zoals de SCADA-systemen die worden gebruikt bij industriële productiesystemen, navigatiesystemen, televisies, een digitaal fototoestel met Wifi-compatibiliteit of een pacemaker. Deze apparaten vallen ook onder de thans voorgestelde begripsomschrijving. Dit is echter niet zozeer een gevolg van de wens tot verruiming van de omschrijving van het geautomatiseerd werk als wel van de ontwikkeling van de techniek, die ertoe leidt dat steeds meer apparaten beschikken over functies die voorheen waren voorbehouden aan de computer.[109]

Daarbij moet worden bedacht dat naast technische apparaten steeds meer chips zelf (dus los van het apparaat waarin zij zijn ingebed) al voldoen aan de definitie van een geautomatiseerd werk. Men kan op goede gronden betogen dat bijvoorbeeld een NFC-chip (*Near-Field Communication*) (of thans: RFID-chip, *Radio Frequency IDentifier*) die in een OV-chipkaart zit als geautomatiseerd werk moet worden aangemerkt. Een dergelijke contactloze RFID-chip bevat immers naast een elektronische beurs met saldo ook een module die onder meer de laatste tien reistransacties en de laatste twee oplaadtransacties bewaart; het zelfstandig uit zijn geheugen wissen (van gegevens ouder dan de laatste transacties) kan gezien worden als een vorm van verwerken. Dergelijke chips kunnen naast opslag en overdracht van gegevens dus in toenemende mate ook zelf gegevens verwerken.[110]

Bij de ruime begripsomschrijving worden vanuit verschillende hoeken kanttekeningen geplaatst, zowel in relatie tot het wetsvoorstel CC III, omdat de combinatie van de ruime definitie en de nieuwe bevoegdheid tot binnendringen in geautomatiseerde werken betekent dat de politie ook van afstand zou mogen binnendringen in pacemakers en autobesturingssystemen (wat mogelijk veiligheidsrisico's oplevert als er bijvoorbeeld technisch iets mis gaat),[111] als in relatie tot het conceptwetsvoorstel voor het nieuwe Boek 2, waar de bepaling dat elk onderzoek aan inbeslaggenomen geautomatiseerde werken (en digitale-gegevensdragers) een bevel van de officier van justitie vereist, betekent dat ook voor onderzoek van relatief triviale apparaten zoals digitale kassa's een bevel van de officier van justitie nodig is, terwijl de privacyinbreuk van onderzoek van dergelijke apparaten meestal minimaal zal zijn.[112] Vanuit beide gezichtspunten valt te pleiten voor meer differentiatie, dat wil zeggen om – in het algemeen of bij bepaalde bevoegdheden – meer onderscheid aan te brengen tussen soorten apparaten die object van onderzoek zijn.

Een belangrijk argument voor differentiatie is dat de te verwachten privacyinbreuk bij onderzoek in klassieke computers en hedendaagse equivalenten daarvan (zoals smartphone en tablet) aanzienlijk groter zal zijn dan bij onderzoek in apparaten die wel onder de definitie van

[108] Memorie van toelichting, p. 101.
[109] *Kamerstukken II* 2015/16, 34 372, nr. 3, 86. SCADA (*Supervisory Control And Data Acquisition*) duidt op het verzamelen, doorsturen, verwerken en visualiseren van meet- en regelsignalen van verschillende machines in grote industriële systemen.
[110] Zie ook Gerechtshof Den Haag 25 mei 2015, ECLI:NL:GHDHA:2015:1427, waarbij werd geoordeeld dat de NFC-chip op een OV-chipkaart als geautomatiseerd werk in de zin van artikel 80sexies Sr c.q. artikel 138ab Sr diende te worden aangemerkt.
[111] Koops e.a. 2016, p. 13-14 en 53-54.
[112] Consultatiereactie politie, p. 58.

een geautomatiseerd werk vallen maar geen functioneel equivalent zijn van de klassieke computer. Het gaat daarbij niet alleen om de hoeveelheid gegevens, maar vooral ook om de aard ervan: op computers en smartphones (evenals op gegevensdragers die veelal voor reservekopieën worden gebruikt, zoals usb-sticks en losse harde schijven) kunnen allerlei soorten gegevens staan, afkomstig uit verschillende contexten, en veel daarvan zullen ook betrekking hebben op het privéleven van de gebruiker. In dat licht conceptualiseren Koops e.a. computers (en equivalenten daarvan) als een moderne verschijningsvorm van het huis:

> computers zijn inmiddels dermate belangrijke houders van privé-informatie geworden, met allerlei gegevens die vroeger in huis werden bewaard maar inmiddels de burger mobiel vergezellen (fotoalbums, muziek, boeken, dagboeken), dat onderzoek van computers vergelijkbaar is, of zelfs verder gaat, dan een doorzoeking van een woning. (…) Onzes inziens moet de normatieve bescherming van het huisrecht – de plaats waar vroeger al deze gegevens werden bewaard – hier worden doorgetrokken naar computers, althans naar de typen computers waarop burgers tegenwoordig hun persoonlijke leven bij zich dragen: smartphones, tablets en andere draagbare computers (nu in de beperkte zin van het woord 'computer'). We zouden daarbij een onderscheid willen maken tussen 'echte' computers (smartphones en andere persoonlijke computers) enerzijds (waarvoor het huisrecht naar analogie mutatis mutandis zou moeten gelden, en dus rechterlijke toestemming vereist is) en gegevensdragers (en mogelijk gegevensverwerkende apparaten, als een navigatiesysteem of koelkast, die wel een 'geautomatiseerd werk' zijn maar geen functioneel equivalent van de 'echte' computer) anderzijds (waarvoor een bevel van de officier van justitie zou kunnen volstaan). Machtiging van de rechter-commissaris hoeft geen wezenlijke praktische bezwaren op te leveren: zoals een rechter-commissaris per mobiele telefoon toestemming kan geven voor een woningdoorzoeking, kan hij ook per mobiel toestemming geven voor een computerdoorzoeking.[113]

Wanneer we dit inzicht volgen, is de consequentie dat niet alle geautomatiseerde werken gelijk zijn aan elkaar; het begrip omvat zowel apparaten die bij onderzoek het diepst mogelijke inzicht in iemands privéleven kunnen bieden (meer dan een stevige huiszoeking) als apparaten en chips die zeer beperkt gegevens verwerken/overdragen/opslaan. Voor de normering van het onderzoek in (of aan inbeslaggenomen) geautomatiseerde werken kan daarom niet worden volstaan met een regeling die voor alle geautomatiseerde werken (in de huidige definitie) gelijkelijk geldt; zo'n regeling zal te snel onnodig veel bescherming bieden aan relatief triviale apparaten en/of te weinig bescherming bieden aan apparaten waar iemands hele privéleven in kan staan.

Daarom is een nadere vorm van differentiatie nodig. Differentiatie kan op verschillende manieren tot stand komen:

A) inperking van de definitie van "geautomatiseerd werk";
B) splitsing van het begrip "geautomatiseerd werk" in twee of meer (deel)begrippen;
C) handhaving van de ruime definitie in het algemeen, en (waar relevant) differentiatie aanbrengen in de regeling van bevoegdheden tot onderzoek van gegevens in geautomatiseerde werken.

Optie A ligt niet voor de hand. Zoals de wetgever heeft opgemerkt, kan in beginsel elk "slim" apparaat voor de opsporing relevante gegevens bevatten;[114] onder (uitzonderlijke) omstandigheden kan het ook belangrijk zijn een pacemaker of een oog- of oorimplantaat te onderzoeken voor de waarheidsvinding. Als sommige typen apparaten uitgesloten zouden worden van de definitie van geautomatiseerd werk, dan zullen deze onder een ander begrip moeten vallen; feitelijk komt optie A dan neer op optie B.

Voor optie B valt het nodige te zeggen, op basis van de redenering hierboven, namelijk dat er een relevant onderscheid bestaat tussen taakspecifieke apparaten die gegevens opslaan/overdragen/verwerken en generieke computers. Het onderscheid is niet haarscherp, maar in veel

[113] Koops e.a. 2016, p. 80-82.
[114] *Kamerstukken II* 2015/16, 34 372, nr. 3, 86.

gevallen is het wel duidelijk of een apparaat een functioneel equivalent is van de klassieke computer (denk, van klein naar groot, aan: slimme horloges, smartphones, tablets, notebooks, pc's, supercomputers) dan wel een "slim" apparaat dat niet primair de functie heeft van gegevensverwerking, maar een andere functionaliteit heeft waarvoor gegevensopslag, -overdracht en -verwerking faciliterend is (denk aan navigatiesystemen, industriële systemen, digitale camera's met wifi, pacemakers en allerlei andere apparaten uit het Internet der Dingen). Aldus zou het ruime begrip "geautomatiseerd werk" onderverdeeld kunnen worden in twee categorieën, bijvoorbeeld "computers" en "geautomatiseerde apparaten",[115] met een omschrijving die bij "computers" de nadruk legt op hun generieke karakter (apparaten die bestemd zijn voor geautomatiseerde verwerking van gegevens in een in beginsel onbepaald aantal contexten) en die bij "geautomatiseerde apparaten" de nadruk legt op hun taak- of contextspecifieke karakter (apparaten die bestemd zijn voor geautomatiseerde verwerking van gegevens in één of een beperkt aantal specifieke contexten). Bij de regeling van specifieke bevoegdheden zou dan gedifferentieerd kunnen worden tussen beide categorieën, waarbij vanwege de verschillen in privacyinbreuk zwaardere eisen worden gesteld aan onderzoek van "computers" dan aan onderzoek van "geautomatiseerde apparaten"[116]. Naast het ondervangen van de kritiek dat het huidige voorstel te veel apparaten over één kam scheert, zou een dergelijk onderscheid ook als voordeel hebben dat het de rechtszekerheid ten goede komt; burgers (en menig opsporingsambtenaar) zullen immers bij het huidige "geautomatiseerd werk" niet denken aan IoT-apparaten, en de begrippen "computers" en "geautomatiseerde apparaten" sluiten beter aan bij het normale taalgebruik.

Tegen optie B valt in te brengen dat een nieuw onderscheid in soorten geautomatiseerde werken onvermijdelijk nieuwe afbakeningsvragen oproept. Het onderscheid tussen taakspecifiek (één of een beperkt aantal contexten) en generiek (een in beginsel onbepaald aantal contexten) zal in de praktijk niet altijd eenvoudig te maken zijn. Bovendien zullen sommige "slimme" apparaten ongetwijfeld langzamerhand worden uitgebreid met nieuwe functionaliteiten, en op een gegeven moment voor zoveel doeleinden (kunnen) worden gebruikt dat ze een functioneel equivalent van een klassieke computer zijn geworden; het omslagpunt is dan niet precies te bepalen. Ook is, in onze omschrijving van het onderscheid, het begrip "context" niet scherp, en zal nader moeten worden omschreven om houvast te kunnen bieden; het is niet zeker of dat voldoende scherp zou kunnen.[117] Tegelijkertijd kan hiertegen ook worden gesteld dat elk onderscheid (per definitie) afbakeningsvragen oproept, en dat het onderscheid zoals voorgesteld relatief duidelijk lijkt en niet complexer is dan diverse huidige onderscheiden (denk aan: onderzoek aan/in het lichaam, stelselmatig/niet-stelselmatig).

Een alternatief in optie B is om niet te onderscheiden tussen taakspecifieke en generieke computers, maar in de mate waarin de verwerking van gegevens in een apparaat naar zijn aard een privacyinbreuk oplevert, zeg maar "gevoelige" apparaten en "niet-gevoelige" apparaten. Dit sluit aan bij de gedachte van een (geobjectiveerd subjectieve) "redelijke privacyverwachting", een begrip dat een centrale rol speelt in het Amerikaanse privacyrecht, maar (meer

[115] Indien men de term "computer" wil vermijden, is een andere mogelijkheid om het begrip "geautomatiseerd werk" niet als koepelbegrip te hanteren, maar te gebruiken als aanduiding voor de klassieke computer (en equivalenten daarvan), en dit te onderscheiden van het begrip "geautomatiseerd apparaat".

[116] Waarbij voor sommige geautomatiseerde apparaten die vitale of kritieke functies vervullen (zoals pacemakers, autobesturingssystemen of ziekenhuisdiepvriezers) wel zwaardere eisen kunnen worden gesteld in verband met de veiligheid.

[117] Helen Nissenbaum, die privacy benadert vanuit het begrip "contextuele integriteit", omschrijft contexten als "structured social settings characterized by canonical activities, roles, relationships, power structures, norms (or rules), and internal values (goals, ends, purposes)." Nissenbaum 2010, p. 132. Contexten zouden nader kunnen worden omschreven door een opsomming te geven op het abstractieniveau van onderwijs, gezondheid, huishouden, transport, recreatie, politiek, markt, religie, enz.

impliciet) ook in Europa wordt gehanteerd om privacyinbreuken te normeren. Dat levert een iets ander beeld op: klassieke computers (en equivalenten als smartphone en laptop) gaan naar hun aard gepaard met een verwachte ingrijpende privacyinbreuk; de meeste IoT-apparaten gaan dat niet. Sommige IoT-apparaten kunnen wel op voorhand als "gevoelig" worden aangemerkt, zoals de "slimme" koelkast als die geautomatiseerd de inhoud registreert (waarbij de inhoud van een substantiële hoeveelheid suikervrije of koosjere producten, zeker als die een bepaalde continuïteit heeft, samenhangt met gezondheid en religie) of de "slimme" stofzuiger die niet alleen stof maar ook alle gedragingen in de woning registreert.[118] Ook IoT-apparaten die hybride functionaliteiten hebben, of in gevoelige contexten (zoals ziekenhuizen) worden gebruikt, zouden dan onder de "gevoelige" categorie kunnen vallen. Ook hier zijn natuurlijk afbakeningsvragen, maar de ontwikkeling van de afbakening zou aan rechtspraak overgelaten kunnen worden, als de memorie van toelichting voldoende richtinggevende voorbeelden geeft van beide categorieën.

Een variant hiervan, of mogelijk ook een uitwerking, zou kunnen zijn om de notie van "digitaal huisrecht" nader uit te werken, en computers die deel uitmaken van het "digitale huis" te onderscheiden van computers die daar niet onder vallen. Zoals door Koops e.a. betoogd,[119] vallen klassieke computers en hedendaagse equivalenten daarvan, onder een "digitaal huisrecht", en de genoemde voorbeelden van de "slimme" koelkast en "slimme" stofzuiger spelen zich ook af in huiselijke kring. Een "digitaal huisrecht" – mits verder uitgewerkt – zou aldus kunnen dienen als kapstok om het benodigde onderscheid in computers te maken.

De commissie heeft deze opties besproken en is uiteindelijk tot de conclusie gekomen dat een onderscheid in typen geautomatiseerde werken (hoewel waardevol om aan te duiden dat er verschillen bestaan in privacyinbreuk naar gelang de aard van het apparaat of de gegevensdrager) beter niet op voorhand kan worden gemaakt op wetgevingsniveau. Geen van de genoemde opties biedt een scherp, richtinggevend onderscheid; het betreft betrekkelijk open categorieën, zodat sowieso vaak interpretatie nodig zou zijn om te bepalen of een concreet apparaat of gegevensdrager in de "lichte" of de "zware" categorie thuishoort. Er is een grote diversiteit in geautomatiseerde werken, zodat regelmatig discussies nodig zullen zijn of een bepaald type nu in de ene of de andere categorie thuishoort. Bovendien zou de interpretatie ook dynamisch aangepast moeten worden naarmate de technologie voortschrijdt en apparaten of gegevensdragers een ander karakter of andere functionaliteiten krijgen, waarmee de nodige verschuivingen van de ene naar de andere categorie zouden plaatsvinden, wat de rechtszekerheid niet ten goede komt. Onzes inziens is een systeem toekomstbestendiger en robuuster waarin niet het onderscheid in type geautomatiseerd werk of gegevensdrager op voorhand *per definitie* doorslaggevend is voor de normering, maar waarin het één van de factoren is – tussen veel andere – die in samenhang bepalen of een onderzoek in een geautomatiseerd werk of drager een grote of minder grote privacyinbreuk maakt.

Daarom kiezen wij voor optie C: differentiatie vindt plaats op het niveau van bevoegdheden tot onderzoek in of aan geautomatiseerde werken (en digitale-gegevensdragers). Dit past in een van de kernonderdelen van dit advies: het algemene normeringscriterium en de nadruk daarbij op het kijken naar de inhoud – de verwachte privacyinbreuk – en niet naar de gehanteerde techniek of gefixeerde onderscheiden. Bij de normering speelt het onderscheid in typen geautomatiseerd werk (bijvoorbeeld taakspecifiek of generiek; "gevoelig" of "niet-gevoelig") zeker een rol, maar niet per se een doorslaggevende: het gaat erom wat voor beeld kan ontstaan van iemands privéleven, gelet op alle relevante factoren (zie nader par. 4.2).

[118] Zie https://www.nrc.nl/nieuws/2017/07/26/topman-ruikt-kans-zijn-robotstofzuiger-brengt-het-leven-van-bewoners-in-kaart-12242559-a1567914.
[119] Zie boven, noot 113.

Interpretatie en afbakening: wat is één geautomatiseerd werk?

Tot nu toe hebben we vooral gesproken over geautomatiseerde werken alsof deze begrippen één duidelijk aanwijsbaar voorwerp of apparaat aanduiden. De definitie geeft echter geen duidelijke begrenzing aan, aangezien deze is uitgebreid tot een "groep van apparaten". In een netwerkomgeving is dan niet direct duidelijk welke groep van apparaten precies één geautomatiseerd werk constitueert, en waar het ene werk ophoudt en het andere begint als deze een apparaat delen dat in beider groep zit.

Via wifi of bluetooth kan tegenwoordig vrijwel elk apparaat draadloos met een ander apparaat verbonden worden; wanneer apparaten wel of niet één geautomatiseerd werk vormen, is dan ook steeds minder helder te duiden. Mogelijk schiet de definitie van geautomatiseerd werk hierin te kort; in elk geval schiet de toelichting op de definitie te kort door geen richting te geven aan de beantwoording van deze vraag. Een startpunt kan zijn om een apparaat pas als onderdeel van één geautomatiseerd werk aan te merken als er reeds een verbinding bestaat met de andere netwerkapparaten die hangen aan een besturingseenheid, of sporen van zo'n verbinding worden aangetroffen. Zolang een apparaat niet daadwerkelijk verbonden is (of geweest is), moet op basis van de eigen zelfstandige functionaliteiten van dat apparaat worden beoordeeld of het een geautomatiseerd werk is, of een digitale-gegevensdrager, of geen van beide. (Zie hierover ook boven, par. 5.1.2 onder "Samenhang met geautomatiseerde werken".) In de praktijk zal dit overigens weinig uitmaken, aangezien voor de normering het onderzoek van geautomatiseerde werken en digitale-gegevensdragers in het voorstel van de commissie gelijk getrokken wordt. Wel is de vraag wat één geautomatiseerd werk is, van belang voor de registratie van beslag: moeten de inbeslaggenomen voorwerpen als één geautomatiseerd werk, of als meerdere geautomatiseerde werken c.q. digitale-gegevensdragers, worden geregistreerd in het registratiesysteem van inbeslaggenomen goederen? Een praktische benadering is om alle componenten die fysiek verbonden waren op het moment van beslag als één geautomatiseerd werk te registreren, en componenten die niet fysiek verbonden zijn (zoals een niet-verbonden externe harde schijf) als zelfstandig inbeslaggenomen voorwerp; die benadering past echter niet goed bij de ontwikkeling waarbij steeds meer componenten draadloos zijn verbonden. Enige duiding van deze problematiek en een vingerwijzing voor de praktijk in de memorie van toelichting hoe om te gaan met registratie van inbeslaggenomen componenten zou nuttig zijn.

5.2. Beslag op gegevens

In het conceptwetsvoorstel Boek 2 wordt het concept "inbeslagneming van gegevens" geïntroduceerd. Hieronder wordt verstaan (artikel 2.7.3.1.1) het "onder zich nemen van gegevens ten behoeve van de strafvordering" bij de toepassing van enkele (steun)bevoegdheden waarbij het gegevensdragende voorwerp niet in beslag wordt genomen. Hiervan wordt onderscheiden het "kennisnemen" van gegevens, waarvan sprake is als het gegevensdragende voorwerp wel in beslag genomen is. De commissie heeft bezien of deze opzet bijstelling behoeft.

5.2.1. De voorgestelde regeling

Het huidige Wetboek van Strafvordering kent feitelijk drie manieren ter verkrijging (of vergaring) van vastgelegde gegevens:

1. De inbeslagneming van een voorwerp (artikel 94 e.v. Sv) en vervolgens overnemen en/of kennisnemen van de gegevens die zijn opgeslagen op het inbeslaggenomen voorwerp (de gegevensdrager);
2. De doorzoeking ter vastlegging van gegevens (artikel 125i e.v. Sv);
3. Het vorderen van gegevens bij een derde (artikel 126n e.v. Sv).

Strikt genomen zouden bijzondere opsporingsbevoegdheden zoals het opnemen van telecommunicatie, het stelselmatig inwinnen van informatie, het opnemen van vertrouwelijke

communicatie en de nieuwe "hackbevoegdheid" uit het wetsvoorstel CC III[120] ook aangemerkt kunnen worden als een wijze van gegevensverkrijging. Die bevoegdheden laten we hier vooralsnog buiten beschouwing, ook omdat het bij deze bevoegdheden niet altijd gaat om overgenomen gegevens.

In het conceptwetsvoorstel is ervoor gekozen om de wettelijke voorwaarden voor de verschillende manieren van het verkrijgen van overgenomen gegevens meer met elkaar in balans te brengen. Met het oog op het vereenvoudigen van de systematiek en terminologie van het Wetboek van Strafvordering wordt voorgesteld naast inbeslagneming van voorwerpen ook te spreken over inbeslagneming van gegevens: net als voorwerpen worden de gegevens immers onder de beschikkingsmacht van de opsporingsautoriteiten gebracht.

Het conceptwetsvoorstel brengt niet alle vormen van gegevensvergaring onder de noemer "beslag". De inbeslagneming van gegevens is gekoppeld aan een aantal (steun)bevoegdheden. Slechts indien de opsporing bij de uitoefening van deze (steun)bevoegdheden gegevens onder zich neemt ten behoeve van de strafvordering (denk hierbij aan aanhouding, staandehouding, betreden of doorzoeken van plaatsen maar ook de huidige vorderingsbevoegdheden) wordt gesproken over gegevensbeslag. Kenmerkend voor het gegevensbeslag is dat het voorwerp (de gegevensdrager) waarop de gegevens staan of zijn opgeslagen, niet in beslag wordt genomen op grond van artikel 94 e.v. Sv.

De drie manier van het verkrijgen van overgenomen gegevens, zoals hierboven opgenomen, worden in het conceptwetsvoorstel als volgt verwerkt.

1. Na inbeslagneming van een gegevensdrager (het voorwerp) kan de opsporing kennisnemen van de gegevens die eventueel op die gegevensdrager staan. Het conceptwetsvoorstel spreekt in dit geval niet van beslag op gegevens, maar van kennisneming van de gegevens die op de inbeslaggenomen gegevensdrager staan of zijn opgeslagen. Ten aanzien van het kennisnemen van de gegevens die zijn opgeslagen op digitale-gegevensdragers of geautomatiseerde werken worden in het conceptwetsvoorstel nadere regels gesteld in Titel 7.4.
2. De doorzoeking ter vastlegging van gegevens is in het conceptwetsvoorstel opgenomen als de doorzoeking ter inbeslagneming van gegevens. Als de opsporing tijdens de doorzoeking van een plaats gegevens onder zich neemt, is sprake van gegevensbeslag. Nadere regels worden gesteld als sprake is van het beslag op gegevens die zijn opgeslagen op of in een tijdens een doorzoeking aangetroffen digitale-gegevensdrager of geautomatiseerde werk.
3. Het vorderen van gegevens is in het conceptwetsvoorstel opgenomen als een bevel tot uitlevering van gegevens ter inbeslagneming. Als een derde aan het bevel voldoet, dan neemt de opsporing vervolgens de uitgeleverde gegevens in beslag.

De keuze voor het concept van beslag op gegevens heeft een aantal juridische gevolgen. Zo kent het conceptwetsvoorstel een bepaling waarin is geregeld welke gegevens vatbaar zijn voor inbeslagneming (artikel 2.7.3.1.2). Ook is in artikel 2.7.3.1.3 geregeld dat na inbeslagneming van gegevens aan degene bij wie de gegevens in beslag zijn genomen zoveel mogelijk een schriftelijk bewijs van inbeslagneming moet worden uitgereikt, waarin een aanduiding wordt gegeven van de inbeslaggenomen gegevens.

5.2.2. Kritieken op het voorstel

Op de hiervoor geschetste voorgestelde regeling "beslag op gegevens" is tijdens de consultatie van het conceptwetsvoorstel van verschillende zijden kritiek geuit, onder andere door het OM, de politie en de Hoge Raad. Voor een volledige weergave van de kritiek zij verwezen naar de (openbare) consultatieadviezen van die organisaties. Ook in de literatuur is (zeer) kritisch gereageerd op dit onderdeel van het conceptwetsvoorstel.[121]

De meer inhoudelijke punten van de kritiek omvatten onder andere de volgende onderdelen.

[120] *Kamerstukken I* 2016/17, 34 372, A.
[121] Zie onder andere Vellinga-Schootstra 2017 en Stamhuis 2017.

- De meerwaarde van de introductie van "gegevensbeslag" is niet duidelijk.
- Het voorstel breekt met een belangrijk centraal kenmerk van het bestaande begrip beslag, namelijk de omstandigheid dat de beslagene de vrije beschikkingsmacht verliest over het inbeslaggenomen voorwerp. Dat is immers bij gegevens doorgaans niet het geval; die kunnen worden gekopieerd, waarbij de gegevens voor het overige binnen de beschikkingsmacht van de "beslagene" blijven.
- Deze strekking van het beslag-begrip wordt ook buiten strafvordering zo gebruikt, en een wijziging binnen strafvordering doet afbreuk aan die eenduidigheid.
- Een voorwerp is iets tastbaars; een gegeven is dat niet. Het te beschermen belang bij gegevens is ook anders dan bij voorwerpen. Bij voorwerpen is dat vooral de bescherming van het eigendomsrecht. Bij gegevens gaat het om intellectueel eigendom en informationele privacy. Ook zijn gegevens veelal niet op één plek aanwezig, maar op meerdere plekken. Daardoor is de wijze waarop beslag moet worden gelegd wezenlijk anders.
- De definitie is onduidelijk, en de regeling is niet toekomstbestendig door de gebruikmaking van oude begrippen.
- De groep apparaten waarvoor de regeling van Titel 7.4 geldt is te groot.
- Er wordt geen onderscheid gemaakt tussen de verschillende soorten onderzoek. Gewezen wordt op het arrest van de Hoge Raad van 4 april 2017 (ECLI:NL:HR:2017:584) waarin de Hoge Raad wel onderscheid maakt naar de aard van het onderzoek. Er wordt aangedrongen op codificatie van deze lijn van de Hoge Raad, zodat alleen die typen onderzoek waarvoor aanvullende rechtsbescherming nodig is onder de voorgestelde regeling worden gebracht.

5.2.3. Bevindingen commissie

De commissie concludeert, in navolging van de genoemde kritiek, dat de benadering waarbij beslag op gegevens als overkoepelend concept voor het verkrijgen van opgeslagen gegevens ten behoeve van de strafvordering wordt gehanteerd, weinig beloftevol is. Voor beslag geldt van oudsher als belangrijkste kenmerk dat ten aanzien van een object aan de beslagene de beschikkingsmacht wordt ontnomen. Bij strafvorderlijke vergaring van opgeslagen gegevens is dat niet het geval: het gaat daar in de kern in het algemeen om het (laten) maken van kopieën van die gegevens, al dan niet na het inzien daarvan. De gegevens raken daarmee niet buiten de beschikkingsmacht van de betrokkene. Dit onderscheid naar (niet-)exclusieve beschikkingsmacht wordt ook in andere rechtsgebieden gehanteerd. Verder zou het hanteren van het begrip "beslag op gegevens" in het voorgestelde stelsel ook tot een inconsistentie leiden: bij sommige vormen van strafvorderlijke gegevensvergaring zou er namelijk sprake zijn van inbeslagneming van gegevens, terwijl dat in andere situaties waarin gegevens worden verkregen, zoals het vorderen van gegevens, niet het geval is, Voor het maken van dat onderscheid ziet de commissie geen overtuigende verklaring.

Al met al concludeert de commissie dat het begrip "beslag" verwarring wekt en naar het oordeel van de commissie weinig voordelen biedt. De commissie adviseert in plaats van "beslag" andere terminologie te hanteren (zoals het "kennisnemen" en/of "overnemen" van gegevens, zie par. 5.3.1). De commissie is van mening dat de drie voornaamste manieren van het verkrijgen van opgeslagen gegevens die in Hoofdstuk 7 van Boek 2 worden geregeld, in grote mate voldoen voor de opsporing. Daarbij is het niet noodzakelijk dat de verschillende manieren van verkrijging van opgeslagen gegevens één overkoepelde term zoals inbeslagneming krijgen.

1. In het kader van inbeslagneming van een gegevensdrager (het voorwerp) kan de opsporing kennisnemen van de gegevens die op die gegevensdrager staan en deze ook overnemen. Het is gerechtvaardigd dat daarover nadere regels worden gesteld in het geval van digitale gegevensdragers en geautomatiseerde werken (en via een schakelbepaling voor bepaalde gevallen van analoge gegevensdragers, zie par. 5.4).

2. De doorzoeking ter vastlegging van gegevens kan grotendeels behouden blijven. Het kennisnemen van gegevens (zonder vastlegging) is inbegrepen in de doorzoekingsbevoegdheid en hoeft niet zelfstandig te worden genormeerd. Het overnemen betekent dat een kopie van de gegevens wordt gemaakt (bijvoorbeeld door het maken van een image).
3. Het vorderen van gegevens kan een *bevel tot verstrekking van gegevens* worden genoemd. De verstrekte gegevens worden overgenomen en er kan vervolgens kennis van worden genomen.

Aanbeveling 19: het concept van "beslag" op gegevens wordt losgelaten. In plaats van "beslag" kan beter andere terminologie (zie Aanbeveling 20) worden gehanteerd.
→ *p. 196*

5.3. Onderzoek van gegevens in of overgenomen uit digitale-gegevensdragers en geautomatiseerde werken

5.3.1. Terminologie

Inleiding

In het conceptwetsvoorstel voor Boek 2 komt in verschillende hoofdstukken het begrip "vastleggen" of "vastlegging" voor.[122] Tevens wordt in diverse bevoegdheden gesproken over het begrip "kennisnemen" dan wel "kennisneming".[123] Daarnaast wordt in Titel 7.4 van Boek 2 gesproken over het "onderzoek" aan elektronische gegevensdragers en geautomatiseerde werken.

Het begrip "vastleggen" ziet begripsmatig op verschillende typen handelingen. De commissie stelt met instemming vast dat de wetgever met de term "vastleggen" in veel gevallen tot uitdrukking heeft willen brengen dat vastlegging van een (onderzoeks)handeling op een andere dan schriftelijke wijze mogelijk wordt gemaakt zonder dat steeds de wet gewijzigd hoeft te worden. Dit advies ziet dan ook niet op een discussie over deze uitleg van het begrip "vastleggen" in de bepalingen die zien op bevelen, vorderingen en machtigingen.

De voor dit advies relevante vragen zien specifiek op het begrip "vastleggen" in de Hoofdstukken 7 en 8 (hetgeen dan gaat om het vastleggen van gegevens die relevant zijn voor het onderzoek) en meer in het bijzonder:

- de betekenis van het begrip en de verhouding tussen de begrippen "vastleggen/vastlegging", "kennisnemen/kennisneming" en "onderzoek" in de zin van Titel 7.4;
- de bevoegdheden ten aanzien van het onderzoek van/aan een digitale-gegevensdrager en geautomatiseerde werken of de netwerkzoeking en het vastleggen van deze gegevens (in het conceptwetsvoorstel nog opgedeeld in twee afdelingen: onderzoek ter inbeslagneming van gegevens (Afdeling 7.4.1) en onderzoek ter kennisneming van gegevens op een inbeslaggenomen gegevensdrager (Afdeling 7.4.2); merk op dat in de huidig voorgestelde Titel 7.4 de term "vastleggen" dus juist niet wordt gebruikt);

[122] Vastleggen/vastlegging komt voor in de algemene bepalingen over het bevel, de machtiging en de vordering, die vooraf moeten worden "vastgelegd", vastlegging van de waarde van het voorwerp (artikel 2.7.2.4.8), stelselmatige vastlegging van persoonsgegevens uit open bronnen (artikel 2.8.2.4.1), vastleggen van telecommunicatie (artikel 2.8.2.7.1) en vastleggen van vertrouwelijke communicatie (artikel 2.8.2.8.1).

[123] Kennisnemen/kennisneming komt voor in de definitiebepaling van ontoegankelijkmaking van gegevens (artikel 2.1.1.1, onderdeel j), kennisneming van inhoud brieven (artikel 2.7.2.2.10 en artikel 2.7.8.2, eerste lid, onderdeel d), kennisnemen van geschillen door de burgerlijke rechter (artikel 2.7.2.3.5), onderzoek aan geautomatiseerde werken of elektronische gegevensdragers ter kennisneming van gegevens (afdeling 7.4.2), kennisnemen van gegevens na beslag bij verschoningsgerechtigden (par. 7.6.2.2 en 7.6.2.3), en kennisnemen van processtukken door verdachte (artikel 2.10.5.1)

- de nieuwe bevoegdheid tot het stelselmatig vastleggen van persoonsgegevens uit open bronnen (artikel 2.8.2.4.1);
- de bevoegdheid tot het vastleggen van telecommunicatie (artikel 2.8.2.7.1). Hierbij is het begrip "vastleggen" een vervanging van het begrip "opnemen" in artikel 126m Sv;
- de bevoegdheid tot het vastleggen van vertrouwelijke communicatie (artikel 2.8.2.8.1). Ook hier vervangt het begrip "vastleggen" het begrip "opnemen" in artikel 126l Sv.

Voor de beschreven bevoegdheden in de Hoofdstukken 7 en 8 is noch in de wettekst noch in de memorie van toelichting bij het conceptwetsvoorstel uitgelegd wat in dit kader onder het begrip "vastleggen" van de gegevens moet worden verstaan. Evenmin komt in de memorie van toelichting tot uiting wat het verschil is met de tevens in bevoegdheden in de Hoofdstukken 7 en 8 gebruikte begrip "kennisnemen"/"kennisneming".

De verhouding tussen de verschillende begrippen wordt aan de hand van het conceptwetsvoorstel en de memorie van toelichting niet duidelijk. Onduidelijk is of de wetgever heeft beoogd een verschil aan te brengen in de verschillende begrippen. Zo is onduidelijk wat onder "onderzoek" wordt verstaan: is dat zowel "kennisnemen" als "vastleggen"? En bestaat er kennisneming zonder vastlegging en andersom? Er wordt in de memorie van toelichting slechts gesteld dat de term "vastleggen" in het kader van telecommunicatie en vertrouwelijke communicatie (artikelen 2.8.2.7.1 en 2.8.2.8.1) beter aansluit bij de digitale omgeving en dat het *overigens ook opnemen omvat* (p. 253-254), maar een duidelijke uitleg van het begrip ontbreekt. Is de reikwijdte van het begrip gelijk voor al deze bevoegdheden of moet er in de uitleg en reikwijdte van het begrip (of de normering) gedifferentieerd worden naar specifieke bevoegdheden?

Deze vragen hangen samen met de aangrijpingspunten voor normering: bij welke handelingen wordt precies een inbreuk op grondrechten gemaakt die normering behoeft? Voordat we kunnen adviseren over de aangrijpingspunten voor normering, is het nodig om eerst de begrippen helder te krijgen.

Onderzoek, kennisnemen, vastleggen en overnemen

De huidige wet hanteert in de Zevende afdeling Doorzoeking ter vastlegging van gegevens (artikelen 125i tot en met 125o Sv) het begrip "vastleggen van gegevens" als aangrijpingspunt voor normering. Zoals gezegd, wordt in het conceptwetsvoorstel bij het onderzoek aan inbeslaggenomen digitale-gegevensdragers en geautomatiseerde werken (in Afdeling 7.4.2, onderzoek na inbeslagneming van het voorwerp) het "kennisnemen van gegevens" als te normeren handeling gehanteerd. In Afdeling 7.4.1 (feitelijk de vervanger van de huidige doorzoeking ter vastleggingen van gegevens, namelijk de situatie dat de opsporing ter plekke gegevens vastlegt en de apparaten zelf laat staan) wordt gesproken over "onderzoek ter inbeslagneming van gegevens".

Ook in de regeling rondom het beslag op voorwerpen en gegevens bij professioneel verschoningsgerechtigden wordt het begrip "kennisnemen" gehanteerd. Op hoofdlijnen wordt met die laatste regeling beoogd dat niemand kennisneemt van dergelijke informatie, voordat door de rechter-commissaris is vastgesteld dat met betrekking tot die informatie geen beroep op het verschoningsrecht kan worden gedaan (zie de artikelen 2.7.6.2.2.2 en 2.7.6.2.2.3).

Noch het begrip "vastleggen", noch het begrip "kennisnemen", noch het begrip "onderzoek" wordt in een definitiebepaling of in de toelichting verder omschreven. Volgens de commissie zijn duidelijker omschrijvingen van deze begrippen nodig in de memorie van toelichting.

Onder "**kennisnemen**" kan naar de mening van de commissie worden verstaan het waarnemen van gegevens door een persoon, waarbij de gegevens zich tonen in voor menselijke interpretatie vatbare vorm.

"**Vastleggen**" kan worden omschreven als het kopiëren van gegevens uit een externe bron in een systeem van de opsporingsdienst, ongeacht de vraag of de gegevens in de externe bron beschikbaar blijven.[124] Om verwarring te voorkomen met de elders in Boek 2 gebruikte term "vastleggen" in de zin van het op (al dan niet digitaal) schrift stellen van bevelen, vorderingen en machtigingen, stelt de commissie voor om in plaats van "vastleggen" voor het kopiëren van gegevens uit een externe bron de term "**overnemen**" te hanteren. Dit begrip is ook helderder in dit verband, omdat het beter aanduidt dat het gaat om het kopiëren van bestaande gegevens (die dus al ergens zijn vastgelegd). Hierin verschilt het overnemen van gegevens bij onderzoek in of aan digitale-gegevensdragers en geautomatiseerde werken van het vastleggen van (tele)communicatie, aangezien het daarbij gaat om het registreren van signalen die niet (althans niet per se) reeds elders zijn vastgelegd (deze registratie is in dit opzicht vergelijkbaar met het op schrift stellen van bevelen). Voor de artikelen ten aanzien van telecommunicatie en vertrouwelijke communicatie kan daarom de term "vastleggen" gebruikt blijven.

Kennisnemen kan in theorie plaatsvinden zonder overnemen, en omgekeerd kan overnemen plaatsvinden zonder kennisneming. De eerstbedoelde situatie bestaat eruit dat een opsporingsambtenaar wel kennisneemt van gegevens, maar deze niet overneemt in een eigen systeem, omdat de gegevens niet relevant zijn voor het desbetreffende onderzoek of (in spoedsituaties) omdat daarvoor nog geen tijd is geweest. De omgekeerde situatie doet zich voor als langs geautomatiseerde weg een kopie wordt gemaakt, waarbij het ontvangende systeem (een deel van) de vastgelegde gegevens niet presenteert aan een opsporingsambtenaar. Bij gedeeltelijke presentatie kan de selectie ingegeven zijn door geprogrammeerde regels of filters, of doordat delen van de vastgelegde gegevens niet voor directe menselijke interpretatie vatbaar zijn, bijvoorbeeld omdat de gegevens versleuteld zijn.

De term "**onderzoek**" ziet de commissie als een koepelterm voor het geheel aan handelingen dat ten aanzien van gegevens (met inbegrip van handelingen in of aan gegevensdragers die betrekking hebben op de daarin opgeslagen gegevens) wordt uitgevoerd, wat zowel kennisnemen als overnemen omvat (en eventuele tussenstappen zoals voorbewerken of verrijken; zie hieronder voor een schets van het bredere spectrum van onderzoek).

Aanbeveling 20: de memorie van toelichting dient helder uit te leggen wat onder de begrippen "vastleggen", "kennisnemen" en "onderzoek" moet worden verstaan. De term "vastleggen" kan daarbij worden gehanteerd (naast het algemene gebruik voor het op (al dan niet digitaal) schrift stellen van bevelen, vorderingen en machtigingen) voor de heimelijke bevoegdheden tot vastleggen van communicatie. Voor het kopiëren van gegevens uit een externe bron is de term "overnemen" geschikter dan "vastleggen"; dit betreft zowel de doorzoekings- en vorderingsbevoegdheden als de bevoegdheid tot het overnemen van persoonsgegevens uit publiek toegankelijke bronnen (artikel 2.8.2.4.1). De term "onderzoek" kan als koepelterm worden gehanteerd voor het geheel aan handelingen, waaronder kennisnemen en overnemen, met betrekking tot gegevens. → *p. 196*

5.3.2. De formulering van de bevoegdheden

Ten aanzien van het onderzoek aan geautomatiseerde werken en digitale-gegevensdragers wordt wat de commissie betreft niet langer onderscheid gemaakt tussen de situaties waarin de voorwerpen in beslag zijn genomen en die waarin de voorwerpen op de plaats van de doorzoeking of betreding worden onderzocht. Er kan dan één bevoegdheid worden geformuleerd die ziet op beide situaties. Dat kan ook doordat wordt afgestapt van de idee van inbeslagneming van gegevens. De bevoegdheid kan dan als volgt worden omschreven:

[124] Zie bijvoorbeeld de memorie van toelichting bij artikel 125i Sv: "op een gegevensdrager vast te leggen zodat deze ten behoeve van het opsporingsonderzoek gebruikt kunnen worden." *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 18.

> Stelselmatig onderzoek van gegevens in of overgenomen uit een digitale-gegevensdrager of geautomatiseerd werk geschiedt op bevel van de officier van justitie. De officier van justitie beveelt in dat geval dat een opsporingsambtenaar dat onderzoek verricht.

Onder onderzoek wordt in dit verband verstaan het geheel aan handelingen dat ten aanzien van de desbetreffende gegevens wordt uitgevoerd, wat zowel kennisnemen als overnemen kan betreffen (en eventuele tussenstappen zoals voorbewerken of verrijken, zie onder). Het omvat zowel (1) handelingen ten aanzien van de gegevens opgeslagen in de digitale-gegevensdrager of het geautomatiseerde werk zelf, als (2) handelingen ten aanzien van gegevens die zijn overgenomen uit de drager of het werk. In het eerste geval (stelselmatig onderzoek van gegevens *in* een digitale-gegevensdrager of geautomatiseerd werk) kan het onderzoek zowel kennisnemen als het overnemen van de gegevens betreffen. In het laatste geval (stelselmatig onderzoek van gegevens *overgenomen uit* een digitale-gegevensdrager of geautomatiseerd werk) bestaat het onderzoek niet uit overnemen (de gegevens zijn immers reeds overgenomen) maar enkel uit het kennisnemen en eventuele daarop voorbereidende stappen, zoals het geautomatiseerd inzichtelijk en analyseerbaar maken van de gegevens die zijn overgenomen uit digitale-gegevensdragers of geautomatiseerde werken. Voor deze formulering is mede gekozen omdat deze duidelijk maakt dat het genormeerde onderzoek niet beperkt is tot het onderzoek in of aan digitale-gegevensdragers of geautomatiseerde werken zelf, maar zich ook uitstrekt tot het onderzoek aan de uit deze dragers gekopieerde gegevens, zoals de analyse en kennisneming van gegevens in de forensische kopie die tijdens een doorzoeking (of daarna) van een harde schijf is gemaakt.

Voor de regeling van steunbevoegdheden voor dit onderzoek kan in Hoofdstuk 7 een Titel worden ingevoerd met als aanhef “Bevoegdheden met betrekking tot onderzoek van gegevens in of overgenomen uit digitale-gegevensdragers en geautomatiseerde werken”. Het is daarbij denkbaar om “onderzoek van digitale gegevens” te gebruiken als synoniem voor de omslachtige (maar preciezere) formulering “onderzoek van gegevens in of overgenomen uit een digitale-gegevensdrager of geautomatiseerd werk”. Dat maakt het mogelijk om een steunbevoegdheid tot “doorzoeking ter onderzoek van digitale gegevens” te formuleren. De Titel zou dan ook simpeler kunnen luiden: “Bevoegdheden met betrekking tot onderzoek van digitale gegevens”, waarbij de toelichting duidelijk maakt dat “onderzoek van digitale gegevens” bedoeld is als synoniem voor het onderzoek van gegevens in of overgenomen uit digitale-gegevensdragers of geautomatiseerde werken.

In deze nieuwe Titel worden de steunbevoegdheden opgenomen ter gegevensonderzoek (betreden, doorzoeken plaats en woning, enzovoorts), die betrekking hebben op digitale gegevens en – via een in te voeren schakelbepaling (zie par. 5.4.1) – gedigitaliseerde analoge gegevens. Tijdens die betreding of doorzoeking mag gegevensonderzoek plaatsvinden (waaronder kennisnemen of overnemen). De nadruk bij de uitoefening van deze bevoegdheden kan daarbij liggen op het maken van een kopie van de aanwezige gegevens. Hiervoor mag worden kennisgenomen van de gegevens. Op deze handelingen is het algemene normeringscriterium van (indringend) stelselmatig onderzoek, zoals hiervoor genoemd, van toepassing. In geval van betreden of doorzoeken van een besloten plaats en woning zal vaak al minimaal een bevel van de officier van justitie zijn afgegeven, zoals een bevel tot doorzoeking ter inbeslagneming of een bevel tot doorzoeking ter onderzoek van digitale gegevens. Dat bevel kan tegelijk de bevoegdheid omvatten van het doen van stelselmatig onderzoek van digitale gegevens, bijvoorbeeld door een extra aan te kruisen alinea op het bevel. Mutatis mutandis geldt hetzelfde voor doorzoekingen die plaatsvinden met een machtiging van de rechter-commissaris, waarbij de machtiging – indien verwacht wordt dat het beoogde onderzoek een indringend stelselmatig karakter kan hebben en de rechter-commissaris oordeelt dat aan de voorwaarden voor dergelijk

onderzoek is voldaan en dit aangeeft in de machtiging – tegelijk de bevoegdheid kan omvatten tot het doen van indringend stelselmatig onderzoek.

Aanbeveling 21: In Afdeling 7 kan een Titel worden ingevoegd getiteld "Bevoegdheden met betrekking tot onderzoek van gegevens in of overgenomen uit digitale-gegevensdragers en geautomatiseerde werken" of compacter "Bevoegdheden met betrekking tot digitale gegevens", waarin steunbevoegdheden worden geregeld tot onderzoek van digitale gegevens. Daarbij kan één algemene bepaling het onderzoek normeren voor zover dit onderzoek stelselmatig is (waarbij het algemene normeringscriterium van toepassing is voor gevallen van ingrijpende stelselmatigheid). → *p. 196*

5.3.3. Uitwerking: vormen van onderzoek en de normering daarvan

In Titel 7.4 van het conceptwetsvoorstel zijn regels opgenomen voor het onderzoek aan "elektronische gegevensdragers" en geautomatiseerde werken. De strekking van de bepalingen uit deze Titel is dat elk onderzoek aan of in een digitale-gegevensdrager of geautomatiseerd werk slechts plaatsvindt op bevel van de officier van justitie, zowel tijdens een doorzoeking bij onderzoek van een digitale-gegevensdrager of geautomatiseerd werk als bij onderzoek aan een inbeslaggenomen digitale-gegevensdrager of geautomatiseerd werk. Op 4 april 2017 heeft de Hoge Raad drie arresten gewezen over deze problematiek (HR 4 april 2017, ECLI:NL:HR: 2017:584, 588 en 592), waarbij de Hoge Raad onderzoek aan "elektronische gegevensdragers" en geautomatiseerde werken onderscheidt naar de mate van inbreuk op de privacy die het onderzoek maakt. De derde vraag van de opdracht voor de commissie luidt in hoeverre het arrest van de Hoge Raad aanleiding geeft om het voorstel aan te passen.

Een eerste conclusie is dat door niet langer het concept beslag op gegevens te hanteren, niet langer de noodzaak bestaat om de materie in twee verschillende Afdelingen (2.7.4.1.1 voor onderzoek aan aangetroffen apparaten ter inbeslagneming van gegevens en 2.7.4.2.1 voor onderzoek aan apparaten die zelf reeds in beslag zijn genomen) te regelen. De normering komt te gelden voor elk onderzoek aan een digitale-gegevensdrager of geautomatiseerd werk, waarbij het niet uitmaakt of het apparaat in beslag is genomen of blijft staan op de plek van de doorzoeking.

Over de normering hiervan is vervolgens uitgebreid gediscussieerd. Daarbij is door sommigen gesuggereerd dat voor elk onderzoek in of aan smartphones een machtiging van de rechter-commissaris nodig is (omdat smartphones de bescherming van een "digitaal huisrecht" behoeven), terwijl anderen suggereerden dat een machtiging van de rechter-commissaris alleen aangewezen is ten aanzien van gegevens die onder het professioneel verschoningsrecht vallen. Uit de discussie kwam naar voren dat uiteindelijk geen van beide uitersten wenselijk is: in het eerste geval is er sprake van overnormering, in het laatste geval is er sprake van ondernormering. Een complicerende factor hierbij is dat – als men het techniekafhankelijke begrip "smartphone" op wetgevingsniveau wil vermijden – het ingewikkeld, zo niet onmogelijk, is om een steekhoudende afbakening te vinden voor apparaten (zoals smartphones) die naar hun aard aanzienlijk privacygevoeliger zijn dan andere gegevensdragers (zie par. 5.1.3 onder "Een ruime definitie – is differentiatie nodig?"). Er moet dus een criterium worden gevonden aan de hand waarvan kan worden bepaald wanneer een voorafgaande rechterlijke machtiging nodig is, zonder daarbij te vervallen in een aantrekkelijk duidelijk maar onvoldoende genuanceerd criterium als één type apparaat (smartphones) of één type gegevens (verschoningsrecht).

Deze discussie heeft ertoe geleid dat de commissie een algemeen normeringscriterium voorstelt van (ingrijpende) stelselmatigheid (zie par. 4.2), dat in dit advies van toepassing wordt verklaard op het onderzoek aan digitale-gegevensdragers en geautomatiseerde werken. Dit algemene normeringscriterium zou geplaatst kunnen worden als tweede lid bij de voorgestelde bepaling over stelselmatig onderzoek (par. 5.3.2): "Indien het onderzoek als bedoeld in het

eerste lid op voorhand redelijkerwijs voorzienbaar ingrijpend stelselmatig is, kan dit alleen plaatsvinden met machtiging van de rechter-commissaris [en indien het onderzoek dit dringend vereist].” (Een soortgelijke algemene bepaling zou dan ook ergens in Hoofdstuk 8 moeten worden ondergebracht.) Het is ook mogelijk om het algemene normeringscriterium als een algemene bepaling op te nemen in Titel 1.2: “Indien de uitoefening van een bevoegdheid een ingrijpend stelselmatig karakter heeft, is voor deze uitoefening een machtiging van de rechter-commissaris vereist [en kan deze uitoefening alleen plaatsvinden indien het onderzoek dit dringend vereist].” De commissie is binnen het bestek van haar opdracht niet toegekomen aan een gedetailleerde uitwerking hiervan; de systematische uitwerking zal door de wetgever in het vervolgtraject moeten plaatsvinden.

Zoals in par. 5.1.3 onder “Een ruime definitie” is beargumenteerd, wordt bij de voorgestelde normering niet op voorhand een onderscheid gemaakt in soorten geautomatiseerde werken of digitale-gegevensdragers, maar moet het samenstel van factoren worden bekeken dat de voorzienbare mate van privacyinbreuk bepaalt, waarvan het type apparaat slechts één factor is. De vraag die nu voorligt, is op welk moment een (redelijkerwijs voorzienbaar meer dan geringe) privacyinbreuk precies plaatsvindt, oftewel wat het aangrijpingspunt van normering moet zijn.

Zoals hiervoor uitgelegd, zijn kennisnemen en overnemen (vastleggen in de zin van kopiëren) de belangrijkste aspecten van onderzoek. Zowel kennisnemen als vastleggen kunnen worden genormeerd. Dit is bijvoorbeeld gebeurd in de Wet op de economische delicten (hierna: WED), waar in artikel 19 onderscheid wordt gemaakt tussen “inzage” (lid 1) en “kopieën (…) maken” (lid 2). Dit onderscheid speelt geen rol in de feitelijke normering: tot beide handelingen zijn dezelfde functionarissen onder dezelfde voorwaarden bevoegd. Er lijkt in de WED wel een volgordelijkheid te worden verondersteld: eerst inzage, en daarna (eventueel) kopieën maken en meenemen. Zoals hierboven opgemerkt, is die volgorde echter niet noodzakelijk: er zijn ook situaties waarin eerst wordt gekopieerd en vervolgens pas wordt kennisgenomen.

Om beter inzicht te krijgen in het gehele spectrum van onderzoek – met verschillende stappen van kennisnemen en overnemen – onderscheidt de commissie vijf mogelijk relevante, soms overlappende, aangrijpingspunten die bij onderzoek van digitale gegevens aan de orde (kunnen) zijn.

1. Het kennisnemen van gegevens van een digitale-gegevensdrager of geautomatiseerd werk waarover een opsporingsfunctionaris beschikkingsmacht heeft zonder dat het voorwerp in beslag is genomen, bijvoorbeeld tijdens een doorzoeking. Het kennisnemen van gegevens op de drager kan bijvoorbeeld relevant zijn om te beoordelen of het zinvol en proportioneel is een gegevensdrager in beslag te nemen, of om te beoordelen welke selectie van gegevens zou moeten worden overgenomen.
2. Het kennisnemen van gegevens die zijn opgeslagen op een inbeslaggenomen digitale-gegevensdrager of geautomatiseerd werk (zonder deze gegevens eerst over te nemen). Dit kan eventueel in twee stappen gebeuren: eerst het oppervlakkig aftasten van de globale inhoud (om te kijken hoeveel en globaal welk type gegevens het betreft) en vervolgens het kennisnemen van de inhoud van bestanden. Het kennisnemen kan worden ondersteund door geautomatiseerde voorbewerking van de gegevens.
3. Het overnemen van gegevens die op de gegevensdrager of het geautomatiseerd werk staan (oftewel het kopiëren van gegevens van de drager op een systeem van de opsporings-instantie), bijvoorbeeld het overnemen van gegevens tijdens een doorzoeking of bij aanhouding of staandehouding, of het overnemen van gegevens uit een inbeslaggenomen digitale-gegevensdrager of geautomatiseerd werk. Het overnemen kan een selectie betreffen (alleen relevante aangetroffen gegevens) of een integrale kopie van alle gegevens.
4. Het voorbewerken en/of verrijken van gegevens, dat wil zeggen het geautomatiseerd inzichtelijk en analyseerbaar maken van de inhoud van de overgenomen gegevens.

5. Het kennisnemen van de overgenomen gegevens. Dit betreft het kennisnemen van de gegevens die inmiddels in de politiesystemen zijn overgenomen. De oorspronkelijke drager van die gegevens wordt hier dus niet meer gebruikt.

Niet alle momenten zullen zich altijd voordoen; soms ook kunnen stappen in een andere volgorde plaatsvinden. Vaak vinden stappen 1 of 2 niet plaats en worden uit inbeslaggenomen gegevensdragers alle gegevens overgenomen zonder eerst kennis te nemen ervan. Het maken van een image (forensische kopie) van een digitale-gegevensdrager of geautomatiseerd werk, oftewel van een volledige kopie van het geheugen van het apparaat, dan wel van een functionele kopie,[125] kan zowel ter plekke gebeuren (het apparaat wordt niet in beslag genomen) als na inbeslagneming van het apparaat. Soms worden gegevens overgenomen zonder inbeslagneming van de drager, en soms wordt meteen kennisgenomen van overgenomen gegevens zonder het inzichtelijk en analyseerbaar maken van de inhoud.

Kennisnemen en overnemen van gegevens zijn beide handelingen die een inbreuk op de persoonlijke levenssfeer kunnen maken, maar deze inbreuken verschillen wel in karakter. De inbreuk die door kennisnemen wordt gemaakt ziet op het feit dat een persoon *daadwerkelijk* kennisneemt van gegevens, terwijl overnemen vooral inbreukmakend is omdat daarmee een situatie ontstaat waarin herhaaldelijk en door meer personen kennis kan worden genomen van die gegevens en dat gegevens geautomatiseerd kunnen worden gecombineerd met andere overgenomen gegevens.

Waar de aard van de privacyinbreuk aldus verschilt bij deze momenten, zal de mate van inbreuk sterk afhangen van de omstandigheden van het geval. In lijn met de argumentatie die aan het algemene normeringscriterium ten grondslag ligt (par. 4.1 en 4.2), kan moeilijk op voorhand worden gezegd welk moment van doorslaggevende betekenis is voor het bepalen van de privacyinbreuk; dat hangt onder andere af van de drager, de gegevens die erop staan, de voorgenomen zoekacties en het voorziene gebruik van de gegevens.

Dit betekent dat op elk van de genoemde aangrijpingspunten het algemene normeringscriterium van (ingrijpende) stelselmatigheid van toepassing zou moeten zijn en dus op het hele spectrum van "onderzoek" van digitale gegevens. Dat geldt zeker niet alleen voor de laatste stap, waarbij overgenomen gegevens door opsporingsfunctionarissen worden bekeken en gebruikt, maar ook voor de voorgaande stappen. Bij het **eerste aangrijpingspunt** – het aantreffen van een geautomatiseerd werk of digitale-gegevensdrager tijdens een doorzoeking en kennis nemen van enige inhoud daarvan – betekent dit bijvoorbeeld dat, indien een opsporingsambtenaar een voertuig doorzoekt en daarbij de inhoud van een in het voertuig aangetroffen tablet wil bekijken met het oog op beoordeling van de proportionaliteit van het inbeslagneming daarvan (artikel 2.7.2.2.5 j° artikel 2.7.3.2.2 lid 2), hij een bevel van de officier van justitie nodig heeft als het kennisnemen van de inhoud stelselmatig is. Hetzelfde geldt bij het **tweede aangrijpingspunt**, wanneer bijvoorbeeld een opsporingsambtenaar ter plekke handmatig zoekt in een bij een aanhouding inbeslaggenomen smartphone om te beoordelen of bepaalde gegevens overgenomen zouden moeten worden. In beide gevallen is ook een machtiging van de rechter-commissaris aangewezen indien het kennisnemen ingrijpend stelselmatig is. Indien het kennisnemen echter beperkt blijft tot een beperkt aantal gegevens of tot het oppervlakkig aftasten van de globale inhoud (zoals de hoeveelheid gegevens) – bijvoorbeeld om te beoordelen of het om een lege of volle drager gaat of dat bestanden bestaan die betrekking hebben op het voor het onderzoek relevante tijdvak en dus of het maken van een image zinvol is en daarvoor eventueel een bevel van de officier van justitie moet worden gevraagd – blijft dit onder de drempel van stelselmatigheid. Ook als het gaat om kennisneming van een heel gering deel van de inhoud

[125] Het maken van een image (volledige kopie) is bij smartphones veelal niet mogelijk; in die gevallen wordt alleen een *functionele* kopie gemaakt, dat wil zeggen een kopie van de zich op de smartphone bevindende mappen, bestanden en dergelijke, in plaats van een één-op-één-kopie van alle enen en nullen.

(laatste WhatsApp of laatste foto bekijken), als indicatie om vast te stellen of inbeslagneming moet volgen kan dit onder die drempel blijven.

Bij het **derde aangrijpingspunt** – dat in de praktijk veel voorkomt omdat meestal een image of functionele kopie gemaakt wordt van relevante aangetroffen geautomatiseerde werken of digitale-gegevensdragers – is het van belang op te merken dat ook het overnemen zelf aan normering onderhevig is, ook al wordt door opsporingsfunctionarissen nog geen feitelijke kennis genomen of anderszins gebruik gemaakt van de gegevens. Volgens Europese rechtspraak vormt ook het overnemen van (persoons)gegevens reeds een inbreuk op de privacy, ongeacht het verdere gebruik.[126] Ook dit valt dus onder het algemene normeringscriterium.

De leden van de commissie zijn het erover eens dat het maken van een image[127] in beginsel een meer dan geringe privacyinbreuk oplevert. Door het maken van de image beschikt de opsporingsinstantie over de gegevens. Het zijn niet slechts bepaalde gegevens van het apparaat, maar alle gegevens die op het apparaat staan. Het gaat om een in potentie grote hoeveelheid gegevens, veelal van verschillende aard, die bij elkaar veel over iemands privéleven kunnen zeggen. Deze gegevens kunnen bovendien herhaaldelijk en telkens op verschillende manieren worden onderzocht. Ook kunnen de gegevens in andere verbanden dan de onderhavige zaak worden doorzocht wanneer de overgenomen gegevens in politiesystemen worden opgenomen.

Het overnemen van deze gegevens in politiesystemen vormt daarom een meer dan geringe inbreuk, los van het verdere gebruik van de gegevens.[128] Deze benadering sluit ook aan bij de invulling van het begrip stelselmatigheid in de huidige BOB-regeling, waarbij het feit dat achteraf een volledige weergave van de informatie mogelijk is, als een factor wordt meegewogen bij de vraag of er sprake is van stelselmatigheid.[129] De meningen binnen de commissie verschillen echter over de wijze van normering van de bevoegdheid tot het maken van een image. Sommigen binnen de commissie zijn van oordeel dat deze bevoegdheid bij de opsporingsambtenaar moet liggen, en niet op het niveau van de officier van justitie. Dit biedt een oplossing voor situaties waarin een image wordt gemaakt om de gegevens zeker te stellen, maar zonder dat reeds onderzoek aan de gegevens plaatsvindt. Voor het doen van onderzoek aan de gegevens op een later moment dient dan op dat moment het bevel van de officier van justitie te worden gevraagd. Anderen binnen de commissie zien geen reden om af te wijken van de voorgestelde systematiek, waarbij in de regel een bevel van de officier van justitie is vereist wanneer sprake is van stelselmatigheid. De commissie adviseert om deze systematiek hier toe te passen, en adviseert om ook voor het maken van een image als onderzoekshandeling daarom een bevel van de officier van justitie voor te schrijven. De behoefte aan het zekerstellen van gegevens in situaties waarin niet tijdig een bevel van de officier van justitie kan worden verkregen, wordt daarbij ondervangen door de laagdrempelige mogelijkheid om bevriezingsmaatregelen te treffen. Voor het maken van een image als bevriezingsmaatregel is geen (zie par. 5.5.1).

Wel tekent de commissie hierbij aan dat bepaalde digitale-gegevensdragers of geautomatiseerde werken dusdanig weinig privacygevoelige gegevens bevatten, dat het maken van een image van die apparaten geen of slechts een geringe inbreuk op de privacy zal opleveren. Dit is bijvoorbeeld het geval bij apparaten met een geheugenchip waarop slechts één of enkele

[126] Zie onder andere EHRM 26 maart 1987, Leander t. Zwitserland, App.nr. 9248/81, par. 48; EHRM 16 februari 2000, Amman t. Zwitserland, App.nr. 27798/95, par. 69; EHRM 4 december 2008, S. en Marper t. Verenigd Koninkrijk, App.nrs. 30562/04 en 30566/04, par. 73, 75, 84; EHJ 8 april 2014, C-293/12 (Digital Rights Ireland), par. 34.

[127] Of een functionele kopie. In het vervolg van de tekst wordt kortheidshalve alleen gesproken van een image; hieronder moet ook het maken van een (volledige) functionele kopie worden verstaan.

[128] Vgl. EHRM 16 februari 2000, Amman t. Zwitserland, App.nr. 27798/95, par. 69.

[129] Zie *Kamerstukken II* 1998/99, 25 403, nr. 25, p. 5: "Als het gaat om een technisch hulpmiddel dat de beelden op een band opslaat, moet de observatie worden gezien als stelselmatig, omdat dan achteraf een volledige weergave mogelijk is en de beelden systematisch toegankelijk zijn."

typen gegevens, in beperkte hoeveelheid, (kunnen) worden opgeslagen. Het zal ook het geval zijn bij digitale-gegevensdragers of geautomatiseerde werken die nieuw zijn en waarvan op voorhand duidelijk is dat deze nog niet in gebruik (geweest) zijn. Ook als op voorhand duidelijk is dat een apparaat alleen voor specifieke zakelijke doeleinden is gebruikt en daarmee geen of nauwelijks persoonlijke gegevens bevat, zal het overnemen van de volledige inhoud geen of slechts een geringe inbreuk maken. In die gevallen zal de opsporingsambtenaar zelfstandig een image kunnen maken.

In geval van een doorzoeking ter onderzoek van gegevens die plaatsvindt op bevel van een officier van justitie, volstaat het bevel tot doorzoeking voor het maken van een image van ter plaatse aangetroffen dragers; dit kan worden gezien als inbegrepen in de doorzoeking ter onderzoek van gegevens. Voor andere gevallen zal een ander of nieuw bevel van de officier van justitie nodig zijn voor het maken van een image.

De commissie signaleert hierbij dat de privacyinbreuk bij het maken van een image met name wordt veroorzaakt door het feit dat gegevens in politiesystemen worden opgenomen. Daarbij is een volledige weergave van de gegevens mogelijk. In beginsel zijn de gegevens dan ook voor meerderlei gebruik vatbaar, waardoor risico's ontstaan van beveiligingsincidenten of *function creep* waarbij gegevens op onbedoelde manieren gebruikt zouden kunnen worden. Deze risico's kunnen aanzienlijk worden ingeperkt door de gegevens van een image niet over te nemen in de reguliere politiesystemen, maar, met behulp van *Privacy by Design*-implementaties, de image zodanig technisch af te schermen dat de gegevens alleen binnen het kader van het desbetreffende opsporingsonderzoek onderzocht kunnen worden door voor dit onderzoek geautoriseerde functionarissen. Beveiligingsrisico's zijn daardoor beheersbaar. Indien met technisch-organisatorische maatregelen verzekerd kan worden dat gegevens uit een image adequaat afgeschermd blijven, uitsluitend voor het onderhavige onderzoek onderzocht kunnen worden, en de gegevens na afloop van de zaak vernietigd (in de zin van onherstelbaar ontoegankelijk gemaakt) worden, kan het maken van een image als een geringe privacyinbreuk worden gekwalificeerd en geschieden door een opsporingsambtenaar; een onderzoeksbevel is dan alleen nodig voor het (stelselmatig) onderzoek van de gegevens, waaronder de kennisname door de opsporingsambtenaar. Zolang echter dergelijke (voldoende geteste en door een daarvoor gekwalificeerde instantie adequaat bevonden) Privacy by Design-constructies niet aanwezig zijn bij de opsporingsdiensten, zou het maken van een image, behoudens de hiervoor genoemde gevallen, alleen op bevel van een officier van justitie moeten kunnen plaatsvinden.

Het **vierde aangrijpingspunt** van voorbewerken en/of verrijken bereidt voor op het bekijken en analyseren van de gegevens. Hierbij wordt een bestandssysteem met de structuur van de mappen, programma's en bestanden gereconstrueerd, waarbij nog aanvullende metadata kunnen worden gegenereerd om de gegevens (beter) doorzoekbaar te maken. Bij al deze handelingen, die ervoor zorgen dat gegevens inzichtelijk en analyseerbaar worden, is meestal geen menselijke tussenkomst noodzakelijk. De eerste fases (reconstructie van de structuur) vormen op zich geen aanvullende privacyinbreuk, omdat er alleen een globaal overzicht van de inhoud van een image wordt gemaakt dat als zodanig geen zicht biedt op de inhoud van gegevens. Dit is echter wel afhankelijk van het abstractieniveau van het bestandssysteem van de structuur, en het is voorstelbaar dat software wordt gebruikt die een relatief informatierijke inhoudsopgave genereert waarbij uit de metadata toch enig zicht ontstaat op de inhoud (er kunnen bijvoorbeeld bestandsnamen en paden in staan waarin woorden voorkomen die een aanwijzing geven van de inhoud van bestanden, en soms kan er een sterke correlatie bestaan tussen bepaalde subtypen bestanden en bepaalde aspecten van iemands persoonlijke levenssfeer). Ook het geautomatiseerd verrijken van gegevens, bijvoorbeeld op basis van gegevens uit andere bronnen, kan een meer dan geringe privacyinbreuk opleveren. Voor de normering maakt dat echter niet uit, aangezien al deze handelingen alleen zijn toegestaan in gevallen waarvoor toch al een bevel

van de officier van justitie nodig was om de image te maken.[130] Het inzichtelijk maken en voorbereiden van analyse kan daarom, vanuit normeringsperspectief, worden gezien als een verlengstuk van het imagen.

Als er vervolgens onderzoek (in de zin van analyseren en kennisnemen) plaatsvindt aan overgenomen gegevens – het **vijfde aangrijpingspunt** – dan zal ook hier moeten worden beoordeeld wat de voorzienbare mate van inbreuk op de persoonlijke levenssfeer van dit onderzoek aan de overgenomen gegevens is. Als dit stelselmatig is, is een bevel van de officier van justitie nodig; daarbij kan worden volstaan met een eerder gegeven bevel van de officier van justitie (bijvoorbeeld het bevel tot een doorzoeking van een plaats, niet zijnde een woning of kantoor van een verschoningsgerechtigde, of het bevel tot het maken van een image van een bij aanhouding inbeslaggenomen smartphone), indien dat bevel tevens aangeeft dat (en in welke mate) onderzoek aan overgenomen gegevens moet worden gedaan. Als het onderzoek aan overgenomen gegevens redelijkerwijs voorzienbaar ingrijpend stelselmatig is, dan zal de rechter-commissaris een machtiging moeten geven. Indien bij het maken van de image al redelijkerwijs voorzienbaar is dat het onderzoek aan de overgenomen gegevens waarschijnlijk een dergelijke ingrijpende inbreuk gaat maken, dan ligt het voor de hand om de rechter-commissaris om machtiging te vragen voor het maken van de image, die vervolgens uit hoofde van dezelfde machtiging en onderliggend OvJ-bevel ook onderzocht mag worden.

5.3.4. Onderzoek van na inbeslagneming of tijdens netwerkzoeking binnenkomende berichten

Een knelpunt in de opsporing betreft het kennisnemen van nieuwe inhoudelijke gegevens die beschikbaar komen op (of via) een geautomatiseerd werk of digitale-gegevensdrager na de inbeslagname of tijdens een netwerkzoeking. Het meest aansprekende voorbeeld is de inbeslagneming van een telefoon waarbij de opsporing ervoor kan kiezen om de telefoon aan te laten en de verbinding van de telefoon in stand te houden. Hierdoor komen er na het moment van inbeslagneming berichtjes binnen op de telefoon die voor de opsporing direct zichtbaar zijn op het hoofdscherm van de telefoon. Het is voor de opsporing niet duidelijk of en zo ja onder welke voorwaarden kennis mag worden genomen van de inhoud van deze berichten en of de inhoud mag worden gebruikt in het vervolg van het onderzoek.

Er zijn, naast het genoemde voorbeeld van de telefoon, meerdere situaties mogelijk waarin er nieuwe inhoudelijke gegevens binnenkomen na de initiële onderzoekshandeling. Ten eerste verloopt er logischerwijs altijd enige tijd tussen de fysieke handeling van het in beslag nemen (het apparaat onder je nemen) en het op de juiste forensische wijze verbreken van de internetverbinding en het daarop volgende initiële gegevensonderzoek. Daarnaast kan zich de situatie voordoen dat het handhaven van de internetverbinding noodzakelijk is voor het uitvoeren van het gegevensonderzoek of de netwerkzoeking en tijdens dat onderzoek nieuwe berichten binnenkomen; dit laatste zal zich met een zekere waarschijnlijkheid voordoen nu het onderzoek aan inbeslaggenomen gegevensdragers en de netwerkzoeking niet aan korte termijnen zijn gebonden (zie daarover par. 5.5.3 onder “Periode”).

Er kan een onderscheid worden gemaakt tussen pure en voorzienbare (of niet onvoorzienbare) bijvangst. In de situatie dat er een kort, natuurlijk, tijdsverloop is tussen de inbeslagname en het verbreken van de verbinding, evenals in de situatie van een netwerkzoeking die terstond plaatsvindt en van korte duur is, zal er normaliter geen substantieel aantal nieuwe berichten binnenkomen in deze korte periode. Sommigen in de commissie betwijfelen echter of er in deze situaties wel sprake kan zijn van onvoorzienbare bijvangst; bij bijvoorbeeld smartphones kan

[130] Het voorbewerken of verrijken van gegevens levert alleen een meer dan geringe privacyinbreuk op in gevallen waar het om een substantiële hoeveelheid (persoonlijke) gegevens gaat die worden voorbewerkt of verrijkt. Daarvan is geen sprake bij de uitzonderingssituaties waarin het maken van image geen bevel van de officier van justitie behoeft (zoals een zeer beperkte of een nieuwe gegevensdrager).

het immers al snel redelijkerwijs te verwachten zijn dat er berichten zullen binnenkomen, ook in een korte periode. Desondanks acht de commissie dat er in geval van een kort, natuurlijk, tijdsverloop sprake is van pure bijvangst; alle gegevens op het geautomatiseerde werk of de digitale-gegevensdrager maken deel uit van de te onderzoeken gegevens, inclusief de toevallig nieuw binnengekomen berichten, zonder dat daar een extra bevoegdheid of normering voor nodig is. Daarbij geldt dan wel dat het in stand laten van de netwerkverbinding een noodzakelijke voorwaarde is om de onderzoekshandeling met succes te kunnen uitvoeren. Anders gezegd: de bijvangst moet wel echte bijvangst zijn. Zo zal bijvoorbeeld bij het uitlezen van een inbeslaggenomen smartphone het niet altijd noodzakelijk zijn de netwerkverbinding in stand te laten om de inhoud van de smartphone te kunnen onderzoeken; om bijvangst te voorkomen zou daarom de netwerkverbinding na inbeslagneming van een apparaat zo veel mogelijk moeten worden verbroken, tenzij er bijvoorbeeld concrete aanwijzingen zijn dat de inhoud van het apparaat door het verbreken van de netwerkverbinding kan worden gewist of ontoegankelijk kan worden gemaakt.

Van pure bijvangst is mogelijk geen sprake meer bij een langer tijdsverloop, waarbij het doel van de handeling zich weliswaar richt op de reeds (op het moment van de start van de onderzoekshandeling) opgeslagen gegevens maar toch redelijkerwijs voorzienbaar met zich brengt dat er gedurende de substantiële periode ook nieuwe inhoudelijke berichten zullen binnenkomen, waarvan kan worden kennisgenomen en die kunnen worden vastgelegd. In dit verband kan een onderscheid worden gemaakt tussen bijvoorbeeld een server waarop een bedrijfsarchief is opgeslagen enerzijds en een smartphone anderzijds. In dat laatste geval is veel eerder voorzienbaar dat in de tussentijd nieuwe inhoudelijke gegevens zullen binnenkomen dan in dat eerste geval. Ook kunnen zich situaties voordoen waarin de wens bestaat het onderzoek juist mede te richten op het gedurende enige tijd verkrijgen van nieuwe berichten, bijvoorbeeld om reacties op bijvoorbeeld een aanhouding of doorzoeking te volgen; naar huidig recht is dat niet toegestaan op basis van het onderzoek aan inbeslaggenomen geautomatiseerde werken of digitale-gegevensdragers (dat zich immers richt op reeds in de drager opgeslagen gegevens), maar het is een tamelijk veelvoorkomende situatie, en de commissie onderschrijft het opsporingsbelang om dit gedurende enige tijd monitoren van binnenkomende berichten mogelijk te maken. (De vraag is wel of de netwerkzoeking en het onderzoek aan inbeslaggenomen gegevensdragers de aangewezen bevoegdheden zijn om dergelijk monitoren van communicatie mogelijk te maken; zie p. 95.)

Gelet op artikel 13 Gw valt communicatie die zich in de transportfase of bij een aanbieder bevindt en via de aanbieder wordt verkregen, onder de bescherming van het telecommunicatiegeheim (vgl. par. 6.3.2). Deze communicatie kan slechts na voorafgaande machtiging van de rechter-commissaris worden verkregen ten behoeve van opsporing. Dat geldt zowel voor de situatie waarin die gegevens worden gevorderd bij die derde als voor de situatie waarin die stromende communicatie wordt opgenomen met een tap. Dit geldt echter niet voor gegevens die zich bevinden bij de eindgebruiker zelf, bijvoorbeeld op zijn smartphone, en aldaar worden verkregen.

De vraag rijst in dit verband of er bij de kennisname en het vastleggen van nieuwe berichten die binnenkomen op het apparaat van de eindgebruiker na inbeslagneming, of op een apparaat elders tijdens een netwerkzoeking, sprake is van berichten die zijn beschermd onder artikel 13 Gw, zodat een machtiging van de rechter-commissaris vereist is. Het ligt voor de hand dat berichten die via een netwerkzoeking in een geautomatiseerd werk van een aanbieder worden aangetroffen, onder die grondwettelijke bescherming vallen. Maar hoe zit het met berichten die lokaal binnenkomen op het apparaat van de eindgebruiker?

Er zijn verschillende manieren waarop gegevens op het apparaat van de eindgebruiker (of een forensisch verantwoord equivalent daarvan) kunnen binnenstromen. Vaak zal het zo zijn dat de oorspronkelijke gebruiker van het geautomatiseerd werk het apparaat zo heeft ingesteld

dat berichtendiensten (mail, chatberichten) automatisch worden gesynchroniseerd. Wanneer de internetverbinding wordt hersteld, zullen deze berichten verder automatisch binnenstromen. Andere gegevensbronnen worden gesynchroniseerd op het moment dat een applicatie wordt geopend, of op het moment dat er actief om synchronisatie wordt gevraagd. En er zijn omgevingen die vanaf het geautomatiseerde werk te bereiken zijn door actief in te loggen op die omgeving om daar te lezen en te zoeken (alhoewel alles wat kan worden waargenomen op het scherm op dat moment ook lokaal is "opgeslagen" op het fysieke apparaat). Het eerste geval, en wellicht ook het tweede, lijkt meer op een uitbreiding van het gegevensonderzoek op het apparaat. De laatste gevallen neigen meer naar een netwerkzoeking, alhoewel de verschillen (zeker vanuit het perspectief van de gebruiker) relatief zijn. Maakt het bijvoorbeeld uit of de applicatie aanvullend is beschermd met een pincode, of met twee-factor-authenticatie? Voor het gegevensonderzoek is het doorbreken van de beveiliging van het toestel gerechtvaardigd; geldt dat ook voor de beveiliging van de applicatie?

Wanneer de opsporing een actieve rol heeft in het ophalen van de berichten die tot dat moment waren opgeslagen bij een aanbieder of zich in de transportfase bevonden, dan vallen de berichten volgens de commissie onder de bescherming van artikel 13 Gw. Zij beveelt de wetgever aan met voorbeelden in de memorie van toelichting aan te geven welke mate van initiatief van de opsporing ertoe leidt dat deze grondwettelijke bescherming blijft gelden, waaronder in elk geval het na inbeslagneming actief synchroniseren valt. Ook kan worden gedacht aan het inschakelen van een smartphone die ten tijde van de inbeslagneming uit stond en na inschakeling automatisch berichten ophaalt van een server. Te betogen valt ook dat het laten voortduren van een internetverbinding (mede) met het oog op het verkrijgen van na inbeslagneming binnenkomende berichten, voor een periode die langer is dan noodzakelijk voor het onderzoek van de op het moment van inbeslagneming op het apparaat opgeslagen gegevens zelf, een actieve rol oplevert. Voor het verkrijgen van berichten die onder de bescherming van artikel 13 Gw vallen, is een machtiging van de rechter-commissaris nodig (zie par. 5.6.1 onder "Vervanging van enkele "aanbieder"-gerichte bepalingen door een algemene bepaling over het telecommunicatiegeheim").

De volgende vraag die zich opdringt is de vraag of het uitmaakt op welk moment de later binnengekomen berichten worden vastgelegd of daarvan kennis wordt genomen. Er is immers de optie om tijdens een gegevensonderzoek en een eventueel daarop gevolgde netwerkzoeking dit onderzoek of de netwerkzoeking te laten doorlopen en de verbinding met internet in stand te houden, waardoor er direct zicht ontstaat op nieuwe berichten die tijdens dit onderzoek binnenkomen. De overwegingen omtrent deze vraag zijn vergelijkbaar met de overwegingen over de periode dat een netwerkzoeking mag duren; de commissie verwijst in dit verband naar paragraaf 5.5.3, waarin de commissie stelt dat de periode zo lang mag zijn als redelijkerwijs noodzakelijk is om de benodigde gegevens binnen te krijgen, waarbij deze periode beperkt is tot in beginsel enkele dagen; een langere periode is mogelijk, mits deze voldoende wordt gemotiveerd.

Wanneer de opsporing na het initiële onderzoek op een later moment een nieuw gegevensonderzoek of een nieuwe netwerkzoeking noodzakelijk acht, en daarvoor (na verkrijgen van een nieuw bevel, zie par. 5.5.3) de verbinding met internet weer inschakelt, zullen daardoor nieuwe berichten alsnog binnenstromen op het apparaat. Deze gegevens zijn op het moment van onderzoek van de gegevens formeel geen "stromende" gegevens meer, maar "opgeslagen gegevens". Maar afhankelijk van de mate van actieve inmenging moet dit laten binnenstromen van gegevens mogelijk toch worden gezien als een inbreuk op artikel 13 Gw. En daarmee is een machtiging van de rechter-commissaris hiervoor noodzakelijk.

De commissie is het erover eens dat de wetgever het kennisnemen van later binnenkomende berichten mogelijk zou moeten maken, mits dit afdoende is genormeerd (waaronder de eis van

een machtiging van de rechter-commissaris wanneer sprake is van grondwettelijk beschermde communicatie). Het is met het oog op lastenverlichting ook belangrijk dat er niet meerdere bevelen nodig zijn om één enkele opsporingshandeling te verrichten. Maar onder welke bevoegdheid zou het kennisnemen van later binnenkomende berichten nu moeten vallen? In de huidige formulering van de verschillende artikelen in het wetsvoorstel is het nergens goed in te passen. In de formulering van het gegevensonderzoek (nu nog de artikelen 2.7.4.1.1 en 2.7.4.2.1) wordt gesproken over "gegevens die daarin of daarop zijn opgeslagen" en bij de netwerkzoeking (nu nog de artikelen 2.7.4.1.2 en 2.7.4.2.2) gesproken over "naar in dat werk opgeslagen gegevens".

Het kennisnemen van later binnenkomende berichten heeft raakvlakken met de bevoegdheid tot het vastleggen van telecommunicatie. In de formulering van het conceptwetsvoorstel houdt deze bevoegdheid in dat "een opsporingsambtenaar met een technisch hulpmiddel niet voor het publiek bestemde communicatie die plaatsvindt met gebruikmaking van de diensten van een aanbieder van een communicatiedienst, vastlegt" (art. 2.8.2.7.1, eerste lid). De inhoudelijke gegevens die later zijn binnengekomen op het apparaat, zijn daar wel terecht gekomen door gebruikmaking van de dienst van een aanbieder van een communicatiedienst, maar op het moment dat ze op het apparaat staan, is het geen communicatie meer die plaatsvindt via de dienst van de aanbieder. Deze gegevens worden in de situaties van een onderzoek aan een inbeslaggenomen geautomatiseerd werk of digitale-gegevensdrager en van een netwerkzoeking ook niet per se vastgelegd in de zin van artikel 2.8.2.7.1 (dus geregistreerd op het exacte moment van binnenkomen); ze worden veeleer overgenomen (dus gekopieerd) op het moment dat ze na binnenkomst op de drager zijn opgeslagen.

Voor de uitvoering van de tapbevoegdheid is daarnaast het gebruik van een technisch hulpmiddel noodzakelijk. De wet schrijft immers voor dat het vastleggen met een technisch hulpmiddel moet gebeuren. Dit technisch hulpmiddel moet, indien sprake is van het tappen zonder medewerking van de aanbieder, een onder het Besluit technische hulpmiddelen gekeurd technisch hulpmiddel zijn. Deze keuring kan bij een tap niet achteraf plaatsvinden of achterwege blijven. Bij het verkrijgen van de nieuwe berichten via het inbeslaggenomen apparaat of de netwerkzoeking is van de inzet van een (gekeurd) technisch hulpmiddel echter geen sprake. Ook is er geen sprake van middelen die onder het huidige Besluit en de interpretatie daarvan gekeurd kunnen worden (zie in dit verband ook de discussie over de keuring van software in par. 6.6).

Hoewel het onderzoek van na inbeslagneming of tijdens een netwerkzoeking binnengekomen berichten conceptueel wellicht meer verwantschap heeft met tappen dan met onderzoek van opgeslagen gegevens, is de commissie in meerderheid van mening, vanwege genoemde argumenten, dat het verkrijgen van later binnenkomende berichten geregeld zou moeten worden binnen het kader van het gegevensonderzoek aan het apparaat van de eindgebruiker of de daaraan gekoppelde netwerkzoeking. Zij denkt daarbij aan een extra lid in de wetsartikelen van die bevoegdheden, waarbij ook een verwijzing kan worden opgenomen naar de algemene bepaling over grondwettelijk beschermde communicatie waarvoor een machtiging van de rechter-commissaris vereist is (zie par. 5.6.1). Indien dan bijvoorbeeld een tweede netwerkzoeking wordt bevolen omdat men met nieuwe inzichten uit het onderzoek nogmaals onderzoek wil doen en daarbij redelijkerwijs voorzienbaar is dat er ook nieuwe gegevens binnenkomen, zou dan niet zowel een netwerkzoeking als een tapbevel nodig zijn, maar kan een nieuwe netwerkzoeking worden aangevraagd met in dat geval een machtiging van de rechter-commissaris (vgl. par. 5.5.3).

Aanbeveling 22: het wordt mogelijk gemaakt om kennis te nemen van later binnenkomende berichten op in beslag genomen geautomatiseerde werken of van tijdens een netwerkzoeking binnenkomende berichten. Wanneer het gaat om grondwettelijk beschermde

communicatie, is de rechter-commissaris de bevoegde autoriteit. De commissie heeft, om dit mogelijk te maken, een voorkeur voor het uitbreiden van de artikelen over gegevensonderzoek en de netwerkzoeking. → *p. 197*

5.3.5. Notificatie

Artikel 125m lid 1 Sv bevat een notificatieplicht voor het geval een doorzoeking tot vastlegging of ontoegankelijkmaking van gegevens leidt. In die gevallen wordt zo spoedig mogelijk aan de *betrokkenen* schriftelijk mededeling gedaan van deze vastlegging of ontoegankelijkmaking en van de *aard* van de vastgelegde of ontoegankelijk gemaakte gegevens. De mededeling blijft achterwege, indien uitreiking van de mededeling redelijkerwijs niet mogelijk is, en kan worden uitgesteld zolang het belang van het onderzoek zich tegen de mededeling aan de betrokkene verzet. De kring van betrokkenen als bedoeld in artikel 125m Sv is vrij ruim. Dat kan, op grond van het derde lid, de verdachte zijn, maar ook de verantwoordelijke voor de gegevens of de rechthebbende van een plaats waar de doorzoeking heeft plaatsgevonden.

Artikel 125m is in het Wetboek van Strafvordering ingevoegd met de Wet bevoegdheden vorderen gegevens (Stb. 2005, 390). Uit de memorie van toelichting blijkt dat de wetgever voor ogen had om met de notificatieplicht uit artikel 125m Sv aan te sluiten bij de notificatieplicht van artikel 126bb Sv. Daarbij is de volgende toelichting gegeven:

> De mededeling, bedoeld in artikel 125m, behoeft geen uitputtende opgave van alle vastgelegde gegevens te bevatten. Volstaan kan worden met een aanduiding van de aard van de betrokken gegevens, dat wil zeggen met een globale aanduiding, die de betrokken persoon in staat stelt om te beoordelen of zijn rechten (naar zijn oordeel) zijn geschonden.

In het conceptwetsvoorstel is artikel 125m Sv overgenomen in artikel 2.7.3.1.3:

> 1. Indien de uitoefening van de bevoegdheden, bedoeld in de artikelen 2.7.3.2.2, 2.7.4.1.1 tot en met 2.7.4.1.3 en 2.7.8.1, heeft geleid tot de inbeslagneming van gegevens wordt aan degene bij wie de gegevens in beslag zijn genomen zoveel mogelijk een schriftelijk bewijs van inbeslagneming uitgereikt.
>
> 2. Het bewijs van inbeslagneming bevat een aanduiding van de inbeslaggenomen gegevens.
>
> 3. De officier van justitie kan bepalen dat de uitreiking van een schriftelijk bewijs wordt uitgesteld, zolang het belang van het onderzoek zich tegen uitreiking verzet. (…)

Enerzijds is de reikwijdte van deze bepaling qua kring van personen beperkt. Het bewijs van inbeslagneming dient alleen uitgereikt te worden aan degene bij wie, in de terminologie van het conceptwetsvoorstel, de gegevens in beslag zijn genomen. Anderzijds is het bereik van de bepaling groter geworden, doordat de notificatie ziet op alle vormen van "gegevensbeslag" en niet alleen op het overnemen van gegevens na een doorzoeking of de ontoegankelijkmaking van gegevens.

Het tweede lid schrijft daarbij voor dat het bewijs van inbeslagneming een *aanduiding* bevat van de inbeslaggenomen gegevens. Het woord "aanduiding" heeft "de aard" uit artikel 125m Sv vervangen. Uit de concept-memorie van toelichting (p. 188) blijkt dat met het tweede lid geen wijziging is beoogd in de huidige werkwijze van artikel 125m Sv: "omvat dat bewijs een aanduiding van de inbeslaggenomen gegevens. Dit is overeenkomstig de huidige regeling van artikel 125m, eerste lid."

Het voorgestelde artikel 2.7.3.1.3 lid 2 vereist naar de mening van de commissie vanwege bovenstaande uitleg geen uitputtende opgave van alle overgenomen gegevens. De commissie ziet geen aanleiding om "de aard van de gegevens" zoals dat is opgenomen in artikel 125m Sv te vervangen door "een aanduiding van de gegevens" zoals in het conceptwetsvoorstel is gebeurd. Met "aard" is destijds aangesloten bij "the kind of data that has been seized" (beginsel

2 uit de Aanbeveling nr. R (95) 13 van de Raad van Europa).[131] Een vertaling met "aanduiding" ligt volgens de commissie minder voor de hand. Ook op algemeen taalkundige grond lijkt de huidige term "aard" een betere keuze dan aanduiding. Het woord aard beschrijft de gemeenschappelijke eigenschappen of wezenlijke kenmerken die (in dit geval) een set data onderscheiden van andere (sets) data. Dit verhoudt zich vrij nauwkeurig met de uitvoeringspraktijk, waarin overigens ook geen problemen worden ervaren met het woord "aard". Wijziging van "aard" in "aanduiding" kan volgens de commissie in de praktijk aanleiding geven tot hernieuwde discussie over de bedoelde precisie van de omschrijving van de overgenomen gegevens, en dat is niet wenselijk aangezien, zoals de toelichting op artikel 2.7.3.1.3 lid 2 stelt, geen wijziging is beoogd. Een andere begrip ligt dan niet voor hand.

Aanbeveling 23: in artikel 2.7.3.1.3 lid 2 wordt de term "aanduiding" vervangen door de term "aard". → *p. 197*

5.4. Schakelbepalingen

5.4.1. Omzetting analoge naar digitale gegevens en onderzoek daarvan

In de toekomst zullen, meer nog dan nu, de gegevens, die de opsporing onder zich neemt ten behoeve van onderzoek, digitale gegevens zijn. Op dit moment worden echter ook nog geregeld grote hoeveelheden analoge gegevens in beslag genomen: bijvoorbeeld bedrijfsadministraties, papieren brieven en aantekeningen. In principe is er een continuüm in gegevensdragers: zowel de kerf in het kleitablet als een bit op de harde schijf is een vastgelegd gegeven en de betekenis van de kerf is niet anders dan die van de digitale kopie (foto of 3D-scan) van die kerf. Maar wanneer analoge naar digitale gegevens worden omgezet, kán een cesuur in dat continuüm ontstaan: digitalisering opent op het moment van omzetting mogelijkheden voor het onderzoek van gegevens die, door de schaal en de automatisering, aan dat onderzoek een ander karakter kunnen geven. Een digitale zoekslag in duizend gescande en optisch leesbaar gemaakte ordners, of patroonherkenning in honderden handgeschreven dagboekpagina's, kan snel resultaten opleveren, terwijl een menselijke opsporingsambtenaar daaraan maanden zou moeten werken – en dat laatste gebeurt natuurlijk vaak niet omdat de baten daarbij niet tegen de kosten opwegen.

Weliswaar neemt het belang van analoge gegevens af, maar aangezien deze nog steeds voorkomen, adviseert de commissie om tot een consistent systeem te komen en daartoe een schakelbepaling op te nemen, overeenkomstig de scharniermomenten die elders in dit rapport benoemd worden:

1. het moment waarop analoge gegevens in een digitale vorm worden overgenomen,[132] omdat door die digitale vastlegging reeds inbreuk wordt gemaakt op de privacy op een vergelijkbare manier als het overnemen van gegevens uit een digitale-gegevensdrager of een geautomatiseerd werk (zie par. 5.3.3);
2. het moment waarop die aldus digitaal overgenomen gegevens onderzocht gaan worden, hetgeen (ook) een privacyinbreuk oplevert.

Voor wat betreft het eerste moment geldt dat de normering óók gegevens betreft die dus al eerder – in analoge toestand – in de macht van de opsporingsinstantie waren. Een verdergaande inbreuk ontstaat echter doordat de informatie *in digitale vorm* beter en extensief onderzoekbaar

[131] *Kamerstukken II* 1998/99, 26 671, nr. 3, p. 18.

[132] Strikt genomen kan er nog een stap zitten tussen bijvoorbeeld digitaal overnemen door inscannen (om kastruimte te besparen) en het daaropvolgende digitaal leesbaar maken van de tekst (door optische tekenherkenning, vereist voor doorzoekbaarheid), maar die twee stappen worden ook nu veelal reeds gecombineerd. De eerste stap lijkt daarbij van overwegend belang, omdat daarmee de gegevens – direct of indirect – digitaal raadpleegbaar worden.

wordt en daarmee ook potentieel toegankelijk wordt voor een bredere kring. Daarmee wordt de informatie ook kwetsbaarder voor "function creep", alsook voor beveiligingsincidenten.

De situatie en het moment waarop de gegevens van een inbeslaggenomen analoge gegevensdrager worden overgenomen *als* digitale gegevens is overeenkomstig de situatie waarin, en het moment waarop, gegevens die bij een doorzoeking worden aangetroffen op een analoge gegevensdrager en digitaal worden overgenomen, zodat die analoge gegevensdrager niet meer in beslag genomen behoeft te worden (bijvoorbeeld de papieren brief die bij een doorzoeking wordt gefotografeerd en niet wordt meegenomen).

De consistentie vergt dat in de situatie van digitalisering van analoge gegevens voor de normering wordt aangesloten bij de normeringseisen ten aanzien van bevoegdheden en overige voorwaarden die voorgeschreven zijn bij onderzoek van gegevens die van aanvang af als digitale gegevens bestonden. Met een schakelbepaling in de voorgestelde Afdeling 7.2.2 kunnen, aansluitend op de (impliciete) bevoegdheid onderzoek te doen aan inbeslaggenomen voorwerpen (conform bestaande jurisprudentie op basis van artikel 94 j° artikel 95/96 Sv), de bepalingen ter normering van het onderzoek van gegevens in of afkomstig uit digitale-gegevensdragers of geautomatiseerde werken (zowel voor wat betreft het overnemen als het kennisnemen) van overeenkomstige toepassing worden verklaard.

Wat betreft het **overnemen** van analoge gegevens in digitale vorm, geldt dat dit (zolang tenminste niet meteen kennis wordt genomen van de gedigitaliseerde gegevens) vergelijkbaar is met het overnemen van gegevens uit een geautomatiseerd werk of digitale-gegevensdrager, en door de schakelbepaling dienovereenkomstig wordt genormeerd (zie par. 5.3.3 onder "derde aangrijpingspunt"). Uiteraard behoeft daarbij niet voor élke scan of foto die een opsporingsambtenaar van analoog vastgelegde gegevens maakt – na inbeslagneming van de analoge-gegevensdrager of in plaats van inbeslagneming – afzonderlijk toestemming van een andere autoriteit te worden verkregen. Zoals bij de smartphone een volledige image of functionele kopie eigenlijk altijd een officierstoetsing vergt, maar bij een redelijkerwijs voorzienbaar geringe inbreuk (bijvoorbeeld overneming van gegevens op een beperkte geheugenchip in een apparaat) de opsporingsambtenaar zelfstandig bevoegd is (zie par. 5.3.3), wordt ook bij de schakelbepaling voor wat betreft het digitaliseren (als equivalent van overnemen) aangesloten bij de drempel van een meer dan geringe inbreuk. Wat daarbij precies het analoge equivalent is van een beperkte geheugenchip (die onder deze drempel blijft), zal zich in richtlijnen en jurisprudentie moeten uitkristalliseren; de memorie van toelichting kan in elk geval enkele voorbeelden geven van een geringe (inscannen van enkele foto's) en een meer dan geringe (inscannen van een schrift waarin enkele maanden een dagboek is bijgehouden) inbreuk. Hoewel het digitaal overnemen van analoog vastgelegde gegevens aldus een zelfstandige normering krijgt, zal in de praktijk nauwelijks sprake zijn van administratieve lastenverzwaring, omdat bij bijvoorbeeld een bevel tot doorzoeking ter inbeslagneming tegelijk ook de mogelijkheid van een digitaliseringsslag (en het daaropvolgende onderzoek) dekt.

Wat betreft het verdere onderzoek – **analyse en kennisneming** – van de gedigitaliseerde gegevens houdt de schakelbepaling in dat een officier van justitie betrokken moet worden als redelijkerwijs voorzienbaar is dat een min of meer volledig beeld van iemands privéleven ontstaat, of een rechter-commissaris als sprake is van ingrijpende stelselmatigheid. Bij de beoordeling van de voorzienbare omvang van de inbreuk spelen factoren als de omvang van de hoeveelheid gegevens en uiteraard ook de inhoud van de gedigitaliseerde gegevens een rol: ordners met bedrijfsadministratie van een draadnagelfabriek zijn naar verwachting minder privacygevoelig dan ordners met de bedrijfsadministratie van een escortservice of dichtbeschreven bladzijden van een dagboek. Het onderzoek aan gedigitaliseerde, oorspronkelijk analoog vastgelegde, gegevens is door de schakelbepaling in dat opzicht geheel vergelijkbaar met het onderzoek van gegevens die oorspronkelijk in digitale vorm bestonden op het moment dat ze werden overgenomen (zie par. 5.3.3).

Aanbeveling 24: er wordt een schakelbepaling ingevoerd in Afdeling 7.2.2 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 van uit een geautomatiseerd werk of digitale-gegevensdrager overgenomen digitale gegevens. → *p. 197*

5.4.2. Onlosmakelijk met het lichaam verbonden digitale-gegevensdragers en geautomatiseerde werken

Onderzoek aan/in het lichaam (Hoofdstuk 6) en onderzoek met een digitale component (Hoofdstukken 7 en 8) worden in gescheiden regelingen behandeld. Het menselijk lichaam raakt echter langzamerhand steeds meer met (digitale) technologie verweven; denk aan pacemakers, chipimplantaten als onderhuids ingebrachte RFID-chips en cochleair implantaten, en bionische armen en benen die op het zenuwstelsel zijn aangesloten en met hersensignalen kunnen worden aangestuurd. Momenteel zijn dit nog uitzonderingssituaties, maar het is te verwachten dat in de komende decennia het menselijk lichaam steeds meer met digitale technologie verweven raakt.

Dit kan betekenen dat op termijn onderzoek aan/in het lichaam en onderzoek met een digitale component moeilijker uit elkaar te houden zijn. Vooralsnog is het echter mogelijk ze, in elk geval op conceptueel niveau, te blijven onderscheiden, omdat de primair te beschermen rechtsgoederen verschillen. Bij onderzoek aan/in het lichaam is dat de lichamelijke integriteit; bij onderzoek met een digitale component de informationele privacy. De commissie ziet daarom geen reden om voor te stellen de regelingen in Hoofdstuk 6 en Hoofdstukken 7 en 8 te integreren.

Voor digitale-gegevensdragers of geautomatiseerde werken die onlosmakelijk met het lichaam zijn verbonden, stelt de commissie dat het onderzoek daarin of daaraan onder onderzoek aan digitale-gegevensdragers en geautomatiseerde werken valt. Het onderzoek is immers primair gericht op het overnemen van gegevens en niet op het onderzoeken van (voorwerpen gedragen aan of in) het lichaam. Niettemin kan dergelijk onderzoek ook de lichamelijke integriteit raken, afhankelijk van het type technologie en onderzoek. Om die reden stelt de commissie een schakelbepaling voor, die voor onderzoek in of aan onlosmakelijk met het lichaam verbonden digitale-gegevensdragers of geautomatiseerde werken de bepalingen van Titel 6.4 van Boek 2 van overeenkomstige toepassing verklaart. Een dergelijke schakelbepaling is nodig, omdat het onderzoek aan of in de chip niet vanzelf onder onderzoek aan of in het lichaam valt; de commissie stelt immers dat dit onderzoek onder onderzoek aan digitale-gegevensdragers en geautomatiseerde werken valt, en niet *als zodanig* onder onderzoek aan of in het lichaam.

In concreto stelt de commissie voor om bij de normering van onderzoek aan onlosmakelijk met het lichaam verbonden digitale-gegevensdragers of geautomatiseerde werken onderscheid te maken tussen twee typen dragers/werken.

1. Onderhuids geïmplanteerde chips. Dit zijn primair gegevensdragers die, om uiteenlopende redenen, onder de huid zijn geïmplanteerd maar verder niet met een lichaamsonderdeel zijn geïntegreerd. De chips zijn van buiten het lichaam, met een lezer op of met enige afstand van de huid, uitleesbaar. Hoewel de chips niet lichaamseigen zijn, verschillen ze wel van meegedragen voorwerpen in de zin dat geïmplanteerde chips niet (althans niet eenvoudig) thuis te laten zijn. Dit maakt het onderzoek eraan vergelijkbaar met onderzoek aan het lichaam (artikel 2.6.3.1): de inbreuk op lichamelijke integriteit is in deze zin vergelijkbaar met het fouilleren en het schouwen van lichaamsholten van het bovenlichaam. Voor onderzoek aan of in dit type chips stelt de commissie daarom een schakelbepaling voor die artikel 2.6.3.1 van overeenkomstige toepassing verklaart.

Voor de normering betekent dit dat dit type onderzoek, voor zover het qua digitale component blijft onder de drempel van stelselmatigheid (bijvoorbeeld als de chip naar verwachting alleen identificerende of slechts een beperkt aantal gegevens van één type bevat), alleen kan plaatsvinden met bevel van een hulpofficier van justitie. De regeling in artikel 2.6.3.1 bepaalt immers dat onderzoek aan het lichaam plaatsvindt op bevel van de officier van justitie of de hulpofficier van justitie. Dit veronderstelt wel dat de ambtenaar die de chip wil uitlezen ervan op de hoogte is dat de chip zich in het lichaam bevindt; dit zal niet altijd duidelijk zijn, omdat de signalen van de chip in het lichaam niet verschillen van signalen van dezelfde chip buiten het lichaam. In gevallen waarin de opsporingsambtenaar redelijkerwijs kan verwachten dat de chip zich in het lichaam bevindt (wat mede zal afhangen van de stand van de techniek en de mate waarin onderhuids geïmplanteerde chips voorkomen), zal hij een bevel van de (hulp)officier van justitie moeten aanvragen.

2. Met het lichaam geïntegreerde digitale-gegevensdragers of geautomatiseerde werken. Dit zijn bijvoorbeeld oog- of cochleair implantaten, pacemakers en bionische ledematen die met het zenuwstelsel zijn verbonden. Dergelijke gegevensdragers worden in de regel door een arts in het lichaam aangebracht en zijn belangrijk voor het functioneren van het lichaam. Om die redenen maakt het onderzoek aan dergelijke gegevensdragers een grotere inbreuk op de lichamelijke integriteit dan het onderzoek aan onderhuids geïmplanteerde chips. Ook al hoeft voor het uitlezen van dergelijke gegevensdragers niet per se in het lichaam te worden binnengedrongen, de inbreuk op de lichamelijke integriteit is wel vergelijkbaar met de inbreuk van onderzoek in het lichaam, zoals het inwendig schouwen of het verrichten van niet-invasief beeldvormend onderzoek (artikel 2.6.4.1). Voor onderzoek aan dit type digitale-gegevensdragers of geautomatiseerde werken stelt de commissie daarom een schakelbepaling voor die artikel 2.6.4.1 van overeenkomstige toepassing verklaart, met dien verstande dat het onderzoek niet door een arts geschiedt, maar, indien het onderzoek mogelijk negatieve gevolgen voor de veiligheid of de gezondheid van de verdachte heeft, geschiedt onder toezicht van een arts. In de toelichting kan daarbij worden verduidelijkt dat voor dit type onderzoek geen arts nodig is indien de gegevensdrager van buiten het lichaam kan worden uitgelezen en in zijn algemeenheid is vastgesteld (bijvoorbeeld door een medisch-ethische commissie) dat deze vorm van onderzoek van buitenaf geen veiligheids- of gezondheidsrisico's oplevert.

Voor de normering betekent dit dat het uitlezen van met het lichaam geïntegreerde digitale-gegevensdragers of geautomatiseerde werken alleen mogelijk is bij verdenking van een misdrijf waarop naar de wettelijke omschrijving gevangenisstraf van vier jaar of meer is gesteld. Het onderzoek is alleen mogelijk bij verdachten; voor onderzoek bij derden acht de commissie het echter verdedigbaar dat dit wel mogelijk gemaakt wordt voor die gevallen waarin geen arts nodig is (dus wanneer het onderzoek van buiten het lichaam kan plaatsvinden en geen veiligheids- of gezondheidsrisico oplevert) onder vergelijkbare voorwaarden als artikel 2.6.3.1 lid 3 (op bevel van de officier van justitie, indien het onderzoek dit dringend vereist en nadat de derde is gehoord).

De voorgestelde schakelbepaling is niet van toepassing op digitale-gegevensdragers of geautomatiseerde werken die niet onlosmakelijk met het lichaam verbonden zijn, zoals een smartwatch, een stappenteller of een smartphone die verbonden is met op het lichaam aangebrachte sensoren. Het onderzoek aan dergelijke gegevensdragers maakt geen inbreuk op de lichamelijke integriteit. Wel zullen (losmakelijk) met het lichaam verbonden gegevensdragers veelal gegevens over het lichamelijk functioneren bevatten, zoals bloeddruk, hartslag of suikerspiegel. Het feit dat een bepaalde type gegevensdrager met het lichaam verbonden is en als zodanig veelal gegevens over het lichamelijk functioneren bevat, is een relevante factor die moet worden meegenomen in de beoordeling of het onderzoek aan gegevens in of overgenomen uit de gegevensdrager stelselmatigheid of ingrijpende stelselmatigheid oplevert. Dat geldt uit

de aard der zaak ook voor gegevensdragers die onlosmakelijk met het lichaam zijn verbonden: ook daarbij speelt het type gegevensdrager een rol in de beoordeling van de (ingrijpende) stelselmatigheid van het voorgenomen onderzoek aan de digitale-gegevensdrager of het geautomatiseerde werk.

Hersensignalen

In de toekomst zal het vermoedelijk ook mogelijk worden om tot op zekere hoogte hersensignalen van buitenaf uit te lezen. Dat is momenteel al het geval in laboratoriumsituaties. De mogelijkheden van neurotechnologie zullen ongetwijfeld toenemen, al valt de snelheid van de ontwikkelingen moeilijk te voorspellen. De commissie acht het op dit moment te vroeg om uitspraken te doen over een specifieke regeling van hersenonderzoek. De commissie adviseert de wetgever om daar, wanneer de ontwikkelingen dusdanige vormen aannemen dat hersenonderzoek voor opsporingsdoeleinden enigermate realistisch lijkt te worden, wetgeving voor te ontwikkelen. Daarbij hanteert de commissie het uitgangspunt dat onderzoek van hersensignalen een potentieel dermate ingrijpende inbreuk op de privacy en vrijheid van gedachten vormt, dat dit onder de huidige en voorgestelde regeling uitgesloten is voor opsporingsdoeleinden. Alleen met specifieke wetgeving waarbij voldoende waarborgen zijn getroffen, zou dergelijk onderzoek in de toekomst eventueel mogelijk gemaakt kunnen worden.

Een uitzondering hiervoor geldt slechts voor het onderzoek van hersensignalen die puur lichaams*mechanische* functies betreffen; de hersensignalen die bijvoorbeeld een bionische ledemaat aansturen kunnen – voor zover deze worden opgeslagen op een chip – worden uitgelezen conform bovenstaand voorstel over onlosmakelijk met het lichaam verbonden gegevensdragers, bijvoorbeeld in een onderzoek naar opzet indien een bionische arm zwaar letsel heeft veroorzaakt.

Aanbeveling 25: er wordt een schakelbepaling ingevoerd die bepaalt dat voor onderzoek aan of in onlosmakelijk met het lichaam verbonden digitale-gegevensdragers of geautomatiseerde werken de bepalingen uit de Titels 6.3 en 6.4 van Boek 2 van overeenkomstige toepassing zijn, conform bovenstaand voorstel.

Het vastleggen en kennisnemen van hersensignalen (anders dan signalen die puur lichaams*mechanische* functies betreffen) voor opsporingsdoelen is dermate ingrijpend dat dit onder de huidige en voorgestelde wetgeving uitgesloten moet worden geacht; een dergelijke toepassing is alleen mogelijk op basis van eventuele toekomstige specifieke wetgeving met voldoende waarborgen. → *p. 198*

5.5. Flankerende bevoegdheden

5.5.1. Digitale bevriezingsmogelijkheden

Meer dan voorwerpen zijn digitale gegevens dynamisch. Digitale gegevens kunnen zeer snel gewijzigd, verplaatst of verwijderd worden. Het feit dat dit is gebeurd is niet altijd makkelijk waar te nemen of aan te tonen. Opsporingsdiensten moeten daarom snel kunnen acteren in onderzoeken waarbij digitale gegevens een rol spelen. Dit roept de vraag op of er aanvullende wettelijke bevoegdheden nodig zijn om digitale gegevens te kunnen "bevriezen", analoog aan de reeds bestaande bevriezingsbevoegdheden die (van oudsher) bedoeld zijn voor toepassing voorafgaand aan en tijdens fysieke doorzoekingen (artikel 125 Sv en artikel 96 lid 2 Sv).

Bestaande en voorgestelde regeling met betrekking tot het doorzoeken van plaatsen

Bij de doorzoeking van een plaats (voertuig, woning of overige plaats) kunnen de daar aanwezige gegevensdragers worden doorzocht. Daarbij geldt reeds op grond van geldend recht dat diverse maatregelen getroffen kunnen worden om het doel van de doorzoeking veilig te

stellen. Artikel 125 Sv regelt dat maatregelen ter bewaking of afsluiting genomen kunnen worden, dat aanwezigen bevolen kan worden ter plaatse te blijven en af te zien van het gebruik van telecommunicatievoorzieningen. In de fase voorafgaand aan een doorzoeking kunnen de maatregelen van artikel 96 lid 2 Sv worden genomen. In het conceptwetsvoorstel zijn deze mogelijkheden overgenomen (artikelen 2.7.1.1.5 en 2.7.2.2.4) en uitgebreid: de maatregelen kunnen niet alleen genomen worden om voorwerpen veilig te stellen, maar ook om gegevens te bevriezen. Op zichzelf lijken de genoemde maatregelen voldoende ruim geformuleerd om ook het verlies van gegevens te kunnen voorkomen. De vraag is echter of de bevoegdheden om beschermende maatregelen te treffen tijdig beschikbaar zijn. De huidige en voorgestelde regelingen koppelen de bevoegdheid om maatregelen te treffen aan de doorzoeking: de bevoegdheden staan ter beschikking vanaf het moment dat de doorzoeking is aangevangen tot het moment dat het onderzoek ter plaatse is afgelopen (artikel 2.7.1.1.5 lid 1, aanhef). Artikel 2.7.2.2.4 ziet op een iets eerder tijdvak, namelijk vanaf het moment dat feitelijk wordt binnengetreden op de zoekingslocatie tot het moment dat de bevoegde autoriteit ter plaatse is gekomen (en de doorzoeking een aanvang neemt). Het conceptwetsvoorstel biedt geen mogelijkheden om voorafgaand aan het betreden van de te doorzoeken plaats bevriezingsmaatregelen te treffen. Te denken valt aan het fysiek onderbreken van netwerkverbindingen buiten de doorzoekingslocatie, of het gebruik van stoorzenders om draadloze communicatie te blokkeren.

Bestaande en voorgestelde regeling met betrekking tot inbeslaggenomen gegevensdragers

Noch het huidige wetboek, noch het conceptwetsvoorstel bevatten specifieke bevoegdheden die ertoe strekken gegevens op inbeslaggenomen gegevensdragers te bevriezen.

In veel gevallen zijn geautomatiseerde werken voorzien van een beveiliging die ervoor zorgt dat alleen de gebruiker toegang tot de opgeslagen gegevens kan krijgen. Inbeslagneming vindt bij voorkeur dan ook plaats op het moment dat het apparaat “open” staat. Soms is daarvoor vereist dat de gebruiker overrompeld wordt, waarbij bijvoorbeeld zijn telefoon tijdens het gebruik wordt afgenomen of de verdachte bezig is op zijn computer. Veelal zal dit gepaard gaan met diens aanhouding of een doorzoeking. Omdat inbeslagneming een vormvrije handeling is, en ook gepaard kan gaan met de toepassing van proportioneel geweld,[133] kan het gebruik van overrompelingstactieken met daarbij eventueel behorende proportioneel geweldstoepassing geacht worden onderdeel uit te maken van de inbeslagnemingsbevoegdheid.

Na de inbeslagneming van een “open” apparaat is het vervolgens van belang het apparaat open te houden. Vaak zal het voldoende zijn om te zorgen dat bijvoorbeeld het scherm van het toestel met regelmatige intervallen aangeraakt wordt of een muisbeweging detecteert. Deze handelingen kunnen uitgevoerd worden door een opsporingsambtenaar, of door op het apparaat bepaalde software te plaatsen. Door het plaatsen van bepaalde software wordt de gegevensset op het apparaat gewijzigd, maar dit is goed controleerbaar en hoeft daarom geen invloed te hebben op de integriteit van de gegevens. Ook lijkt hiermee geen (of geen substantiële) inbreuk te worden gemaakt op de rechten van de beslagene. Een specifieke wettelijke basis voor dergelijke handelingen (handmatig of softwarematig) acht de commissie dan ook niet nodig.

Bij meer geavanceerde toepassingen kan een apparaat zo geprogrammeerd zijn dat deze alleen “open” blijft zolang het apparaat signalen van buiten ontvangt. Dit kunnen signalen van een ander apparaat zijn (bijvoorbeeld een smartwatch, een geïmplanteerd apparaat of een apparaat dat zich elders bevindt), of van het lichaam van de beslagene. Niet alleen het “open” blijven van een apparaat kan afhankelijk zijn van externe signalen. Het apparaat kan ook zo geprogrammeerd zijn dat het (voor een bepaalde tijd) ontbreken van bepaalde externe signalen

[133] Zie bijvoorbeeld HR 7 september 2004, NJ 2004, 594: De bevoegdheid tot inbeslagneming omvat de bevoegdheid tot het desnoods tegen de wil van betrokkene en met proportioneel geweld openen van diens vuist.

leidt tot het wissen van gegevens op het apparaat of op andere apparaten. Het is daarom van belang maatregelen te kunnen treffen om dit te voorkomen.

Het maken van een image als bevriezingsmaatregel

Een veel toegepaste manier om gegevensverlies of -mutatie te voorkomen is het maken van een 1-op-1 kopie van de gegevens vanaf een gegevensdrager. Zoals hiervoor reeds is besproken, kan het maken van een dergelijke image op zichzelf reeds een meer dan geringe inbreuk maken op de persoonlijke levenssfeer in gevallen waarin het totaal van die gegevens een min of meer volledig beeld geeft van bepaalde aspecten van iemands persoonlijke leven. De inbreuk bestaat eruit dat de gegevens ter beschikking van de opsporing komen. Bij bevriezing is dat echter (nog) niet het geval; de gegevens worden alleen veiliggesteld, maar mogen niet worden onderzocht totdat ze "ontdooid" zijn. Dit brengt met zich dat als voor het maken van een image *als bevriezingsmaatregel* voorzieningen zijn getroffen waardoor geen onderzoek aan de gegevens op de image uitgevoerd kan worden, in die gevallen voor het maken van de image dan geen voorafgaand bevel van de officier van justitie is vereist. Voor het "ontdooien" van de bevroren image, oftewel het vervolgens gebruiken van de image *voor onderzoeksdoeleinden*, is wel een bevel van de officier van justitie vereist (behoudens de in par. 5.3.3 genoemde uitzonderingen voor het maken van een image); voor dit gebruik en het onderzoek aan de gegevens uit de image gelden de voorwaarden als geschetst in paragraaf 5.3.

Conclusie

De commissie staat een algemene en techniek-onafhankelijke regeling voor ogen (naar het voorbeeld van artikel 96 Sv) waarin wordt bepaald dat de opsporingsambtenaar in het kader van een doorzoeking van een plaats of na inbeslagname van een gegevensdrager bevoegd is om, in afwachting van de benodigde toestemming, ten behoeve van het behoud van de gegevens de nodige bevriezingsmaatregelen te nemen om verlies van digitale gegevens te voorkomen. De memorie van toelichting zal een niet-limitatieve opsomming van dergelijke maatregelen moeten bevatten. Hieronder valt ook het maken van een image als bevriezingsmaatregel; daarbij wordt voorgeschreven dat geen onderzoek (anders dan oppervlakkig onderzoek dat nodig is voor de bevriezing zelf) aan bevroren gegevens kan plaatsvinden *op basis van de bevriezingsbevoegdheid* – onderzoek aan bevroren gegevens kan vanzelfsprekend wel plaatsvinden op de grondslag van bevoegdheden tot het onderzoeken van gegevens overgenomen uit geautomatiseerde werken of digitale-gegevensdragers, als aan de daarbij geldende voorwaarden wordt voldaan (par. 5.3.3). Daarnaast kan gedacht worden aan het (voorafgaand aan een doorzoeking of inbeslagneming) in kaart brengen van de aanwezigheid van apparaten, het fysiek onderbreken van netwerkverbindingen, het gebruik van stoorzenders om draadloze communicatie te blokkeren, en het gebruik van software om te voorkomen dat een apparaat zichzelf vergrendelt, al dan niet door het afvangen en reproduceren van signalen van externe bronnen (zoals GPS-signalen of lichaamssignalen).

Aanbeveling 26: in het wetsvoorstel wordt een algemene en technologie-onafhankelijk geformuleerde bevoegdheid opgenomen voor opsporingsambtenaren om in het kader van een doorzoeking of na inbeslagname van een gegevensdrager, in afwachting van de eventueel benodigde bevelen, ten behoeve van het behoud en toegankelijkheid van de gegevens de nodige bevriezingsmaatregelen te mogen nemen. Deze bevoegdheid wordt in de memorie van toelichting toegelicht door middel van een aantal voorbeelden, waarbij aandacht wordt besteed aan het maken van een image als bevriezingsmaatregel. → *p. 198*

5.5.2. Bevoegdheid tot biometrische toegangsverschaffing

Duldplicht

Bij mobiele apparaten die steeds meer zeer gevoelige en onmisbare informatie over de gebruiker bevatten, wordt het belang bij het beveiligen van de toegang tot die apparaten steeds groter. Tegelijk willen mensen dat het apparaat onmiddellijk gebruiksklaar is en niet ellenlange wachtwoorden invoeren of wachten op sms-authenticatie. De leveranciers komen hieraan tegemoet door andere authenticatiemechanismes in te zetten, waarbij alleen de geautoriseerde gebruiker toegang kan krijgen, via biometrische kenmerken die voldoende uniek zijn. De nieuwste toestellen ondersteunen veelal de vingerafdruk, irisscan en gezichtsherkenning. Andere lichaamskenmerken die (in de toekomst) gebruikt zouden kunnen worden zijn geur, bloedvaten in de retina, DNA, bloedsomloop en afdrukken van bijvoorbeeld oor of handpalm. Ook gedragskenmerken zoals stemherkenning, stapherkenning en toetsaanslagritme zijn mogelijk. Deze kenmerken zijn wellicht in de beginfase eenvoudig na te maken, maar hoe verder de leveranciers hun sensoren verbeteren, hoe moeilijker dat wordt. Ook kunnen verschillende biometrische kenmerken samen worden gemeten. Denk aan het meten van de bloedsomloop in combinatie met de vingerafdruk. Of het combineren van kenmerken waardoor het toestel bijvoorbeeld opent met een vingerafdruk maar sluit als het gezicht van verdachte niet in beeld is of er door een onbekende persoon wordt getypt. Daarnaast kan biometrie worden gecombineerd met andere factoren, voor betere beveiliging; naast een wachtwoord kan een tweede factor een *token* zijn. Deze *tokens* worden nu nog buiten het lichaam gedragen (zoals een NFC-chip in een ring), maar kunnen in de toekomst wellicht ook in het lichaam worden geplaatst.

In de praktijk is het niet altijd eenvoudig om toegang te krijgen tot persoonlijke apparaten die in beslag zijn genomen of ter plekke worden onderzocht. Beveiliging is een goede zaak, omdat het voorkomt dat een straatrover, cybercrimineel of toevallige vinder toegang krijgt tot de data. Voor digitale opsporing worden weliswaar steeds nieuwe methodes ontwikkeld om toegang te krijgen tot toestellen, maar biometrische beveiliging levert in toenemende mate problemen op. Dit roept de vraag op welke mogelijkheden er zijn om medewerking af te dwingen aan de toegangsverschaffing via biometrische kenmerken.

Het huidige wetboek kent in het kader van de doorzoekingsbevoegdheden sinds 1993 al de mogelijkheid om iemand die vermoedelijk kennis draagt van de beveiliging van een geautomatiseerd werk, te bevelen toegang te verschaffen tot dat werk (artikel 125k Sv). In het conceptwetsvoorstel (artikel 2.7.4.1.4) wordt dit artikel techniek-neutraler geformuleerd door te spreken van iemand die vermoedelijk "de versleuteling ongedaan kan maken", waarmee niet alleen wachtwoorden maar ook biometrische kenmerken worden bedoeld (memorie van toelichting, p. 206). Daarbij wordt het "ontsleutelbevel" niet alleen van toepassing op geautomatiseerde werken (waar artikel 125k Sv zich toe beperkt), maar ook op digitale-gegevensdragers – een welkome uitbreiding gezien het uitgangspunt dat geautomatiseerde werken en digitale-gegevensdragers qua normering gelijk behandeld moeten worden (zie par. 5.1.2 onder "Samenhang met geautomatiseerde werken"). De formulering is echter enigszins ongelukkig, aangezien het gaat om het ongedaan maken van een beveiliging, die niet per se hoeft te bestaan uit versleuteling (encryptie).

Aanbeveling 27: de term "versleuteling" in artikel 2.7.4.1.4 lid 1 wordt vervangen door de algemenere term "beveiliging", omdat bij toegangsbeveiliging niet per se sprake hoeft te zijn van versleuteling. → *p. 198*

Echter, het bevel mag niet worden gegeven aan verdachten, vanwege het nemo tenetur-beginsel (artikel 125k lid 3 Sv, voorgesteld artikel 2.7.1.1.4) - een aanzienlijke beperking, omdat het veelal alleen de verdachte zal zijn die de (biometrische) beveiliging ongedaan kan maken.

Daarnaast kunnen bepaalde categorieën personen zich verschonen van medewerking, niet alleen beroepsmatige verschoningsgerechtigden, maar ook partners en naaste familieleden (artikel 2.7.6.1.1).

Met de herformulering in artikel 2.7.4.1.4 komt het conceptwetsvoorstel voor een deel tegemoet aan het probleem van biometrische beveiliging, maar de vraag is of meer mogelijk of nodig is.

De commissie heeft overwogen of een bevel tot biometrische toegangsverschaffing ook aan verdachten zou kunnen of moeten worden gegeven. Zonder de discussie over het verplichten van verdachten hun wachtwoorden te geven te heropenen,[134] constateert de commissie dat er een belangrijk verschil bestaat tussen het meewerken in de vorm van het geven van een wachtwoord en meewerken via biometrische toegangsverschaffing. Dit verschil ligt in de kern van het *Saunders*-criterium dat een leidende rol speelt in de interpretatie van het nemo teneturbeginsel. Volgens dit criterium is het beginsel niet van toepassing op "the use in criminal proceedings of material which may be obtained from the accused through the use of compulsory powers but which has an existence independent of the will of the suspect such as, inter alia, documents acquired pursuant to a warrant, breath, blood and urine samples and bodily tissue for the purpose of DNA testing."[135] Het criterium is daarbij niet per se, of niet alleen, of iets onafhankelijk van de wil van de verdachte *bestaat*, maar vooral ook of iets onafhankelijk van de wil van de verdachte kan worden *verkregen*. Wachtwoorden bestaan op zich onafhankelijk van de wil van de verdachte (die ze immers niet enkel met zijn wil kan veranderen), maar kunnen niet onafhankelijk van de wil van de verdachte worden verkregen – ze kunnen alleen worden verkregen als de verdachte dat wil of als diens wil, onder substantiële dwang, wordt gebroken. Vooral vanwege dat laatste is een decryptiebevel aan verdachten nauwelijks te sanctioneren zonder het nemo tenetur-beginsel aan te tasten.

Bij biometrie ligt dit anders. Biometrisch materiaal bestaat onafhankelijk van de wil van de verdachte en kan ook, met lichte dwang (het vastpakken van een vinger, het open houden van een ooglid), onafhankelijk van de wil van de verdachte worden verkregen; daarin verschilt het niet van bloed of lichaamsmateriaal dat gedwongen kan worden afgenomen. Dit geldt op het eerste gezicht misschien niet voor biometrische gedragskenmerken, zoals manier van lopen of wijze van toetsaanslagen, waarbij de verdachte een meer actieve vorm van medewerking moet verlenen. In het systeem van de Nederlandse wet wordt echter aangenomen dat vergelijkbare methoden die een meer of minder actieve vorm van medewerking vergen, zoals sorteerproeven, Oslo-confrontaties, schrijfproeven en urineonderzoek verenigbaar zijn met het nemo teneturbeginsel,[136] zodat dit voor gedragsgebaseerde biometrische kenmerken evenmin een beletsel hoeft te vormen.

De commissie constateert dat biometrische kenmerken meer verwant zijn aan lichaamsmateriaal en handelingen als schrijfproeven dan aan wachtwoorden, en dat het nemo teneturbeginsel niet in de weg hoeft te staan aan een bevel aan verdachten om mee te werken aan biometrische toegangsverschaffing. Deze conclusie is recent ook getrokken door de Noorse wetgever, die in 2017 een bevoegdheid heeft ingevoerd om eenieder, inclusief verdachten, te bevelen mee te werken aan toegangsverschaffing tot een geautomatiseerd werk door biometrische authenticatie, en zo nodig dwang te gebruiken om de authenticatie te bewerkstelligen als de geadresseerde weigert.[137]

---

[134] Een discussie die terecht is afgesloten met het besluit om in het wetsvoorstel computercriminaliteit III geen decryptiebevel voor verdachten in te voeren, zie *Kamerstukken II* 2015/16, 34 372, nr. 3, p. 6 en de analyse in Koops 2012.

[135] EHRM 17 december 1996, App.nr. 9187/91 (Saunders t. Verenigd Koninkrijk), §69.

[136] Zie Koops 2000, p. 44-45; vgl. artikel 2.6.5.5.1 uit het conceptwetsvoorstel: de officier van justitie kan bevelen dat de verdachte een tekst moet opschrijven ten behoeve van een handschriftvergelijkend onderzoek.

[137] Artikel 199 Noors Wetboek van Strafvordering. Zie Bruce 2017, die op p. 29 aangeeft dat deze bevoegdheid het nemo tenetur-beginsel niet aantast (behoudens grove vormen van geweld die artikel 3 EVRM schenden).

Toch acht de commissie een bevel tot medewerking aan biometrische ontsluiting aan verdachten niet nodig en daarmee ook onwenselijk. De reden hiervoor is gelegen in de mogelijke sanctionering in geval van niet-medewerking. Het weigeren mee te werken zou, in geval van een bevel, strafbaar zijn op grond van artikel 184 Sr (maximum drie maanden gevangenisstraf). De dreiging van drie maanden gevangenisstraf zal verdachten er niet vaak toe zetten om mee te werken, wanneer daarmee potentieel significant bewijsmateriaal ontsloten zou worden, zeker als het misdrijven betreft met hogere gevangenisstraffen. Dit impliceert dat een alternatief de voorkeur verdient boven vervolging op basis van artikel 184 Sr: afgedwongen toegangsverschaffing. Het gedwongen dulden van biometrische ontsluiting vormt een relatief lichte inbreuk op de lichamelijke integriteit. Wel is de privacyinbreuk potentieel groot, doordat door afgedwongen medewerking mogelijk veel privacyrelevante gegevens worden ontsloten. Zoals Bruce echter opmerkt,[138] wordt deze privacyinbreuk niet veroorzaakt door het bevel tot meewerken aan toegangsverschaffing, maar door de bevoegdheden tot doorzoeking en onderzoek van gegevens. De legitimatie van de privacyinbreuk ligt dus in de grondslag van deze laatste bevoegdheden. Bij de inbreuk op de lichamelijke integriteit stelt (vanzelfsprekend) artikel 3 EVRM grenzen aan de mate van dwang die mag worden uitgeoefend. Een vinger mag met enige kracht worden vastgepakt en op de sensor gehouden, ook als de verdachte tegenstribbelt; een ooglid mag worden opengehouden voor de irisscanner. De beginselen van proportionaliteit en subsidiariteit normeren hierbij de mate van dwang die in concrete gevallen aanvaardbaar is.

De vraag van het afdwingen van biometrische ontsluiting speelt niet alleen bij verdachten, maar ook bij niet-verdachten, aan wie conform het conceptwetsvoorstel, een bevel kan worden gegeven tot meewerken aan biometrische ontsluiting. De dreiging van artikel 184 Sr zal veelal voldoende zijn voor niet-verdachte personen om mee te werken. Er kunnen zich echter gevallen voordoen waarin geadresseerden, om hun moverende redenen, niet meewerken en het risico van vervolging op basis van artikel 184 Sr op de koop toe nemen. Voor het traditionele ontsleutelbevel is deze situatie aanvaard; er zijn immers weinig alternatieven voorhanden om medewerking af te dwingen als iemand niet een wachtwoord wil geven. Bij biometrische beveiliging ligt dit anders: in plaats van (of naast) een vervolging voor niet meewerken aan een ambtelijk bevel, zou ook de toegangsverschaffing fysiek afgedwongen kunnen worden, door het vastpakken van de vinger en deze op de sensor plaatsen, of door een ooglid open te houden voor de iris-sensor. Dit maakt inbreuk op de lichamelijke integriteit, maar op een niet al te ingrijpende manier.

Daarom stelt de commissie voor om biometrische toegangsverschaffing ook door anderen dan de verdachte, onder dwang, mogelijk te maken.[139] Vanwege de relatief geringe maar niet verwaarloosbare inbreuk op de lichamelijke integriteit zou deze mogelijkheid alleen met een bevel van de officier van justitie moeten kunnen plaatsvinden.

Voor professioneel verschoningsgerechtigden geldt dat naar huidig recht het verschoningsrecht niet absoluut is; met toestemming van de rechter kan dit in (zeer) bijzondere gevallen worden doorbroken. Voor zover in dergelijke (zeer) bijzondere gevallen gegevens van professioneel verschoningsgerechtigden kunnen worden verkregen, ligt het in het verlengde daarvan voor de hand dat ook afgedwongen toegangsverschaffing in deze gevallen mogelijk zou moeten zijn, onder dezelfde voorwaarden als voor het verkrijgen van gegevens zelf. Ten aanzien van niet-professioneel verschoningsgerechtigden (zoals naaste verwanten of echtgenoten) acht de commissie het toepassen van afgedwongen biometrische ontsluiting verdedigbaar; zij kunnen zich weliswaar verschonen van medewerking aan het overhandigen van gegevens, maar zij moeten wel doorzoekingen en andere vormen van gegevensvergaring door opsporingsdiensten dulden. Ook voor hen ligt het in het verlengde daarvan in de rede dat zij biometrische ontsluiting

[138] Bruce 2017, p. 29.
[139] Zoals ook in Noorwegen het geval is, zie noot 137.

moeten dulden, onder dezelfde voorwaarden als die gelden voor het verkrijgen van gegevens bij hen.

Aanbeveling 28: in het wetsvoorstel wordt een bevoegdheid opgenomen op basis waarvan de officier van justitie kan bevelen toegang tot een biometrisch beveiligd geautomatiseerd werk of digitale-gegevensdrager te verschaffen, met een duldplicht voor zowel verdachten als niet-verdachten, waaronder ook niet-professioneel verschoningsgerechtigden. Artikel 2.7.4.1.4 moet dienovereenkomstig worden aangepast, waarbij in het geval van biometrische beveiliging, in afwijking van het eerste lid, geen bevel tot medewerking wordt gegeven maar een duldplicht bestaat. Ten aanzien van professioneel verschoningsgerechtigden is afgedwongen biometrische ontsluiting niet uitgesloten, maar dient de afgedwongen biometrische ontsluiting met dezelfde waarborgen te worden omgeven als het kennisnemen van gegevens die onder het verschoningsrecht vallen. → *p. 198*

Hierbij kan in de memorie van toelichting worden aangegeven dat onder biometrische beveiliging verstaan wordt een beveiliging op basis van biometrische gegevens, zoals bedoeld in voorgesteld artikel 1 onder s van de Wpg,[140] alsook het gebruik van *tokens* die op of in het lichaam worden gedragen, zoals een geïmplanteerde chip.

Heimelijk verkregen biometrische gegevens

Naast een duldplicht ten aanzien van biometrische toegangsverschaffing, is er nog een mogelijkheid. Voor het verkrijgen van toegang tot bijvoorbeeld een smartphone kan gebruik worden gemaakt van vingerafdrukken die al in het bezit van zijn van de opsporingsinstantie of die met het oog daarop worden vergaard. Ook met een scherpe foto (bijvoorbeeld van een gelaat of iris) kan toegang worden verkregen, afhankelijk van hoe de biometrische sensor is afgesteld. Het heimelijk vergaren van dergelijke biometrische kenmerken maakt inbreuk op de privacy. De vraag is of dat een meer dan geringe inbreuk betreft. Het maken van een enkele foto van een verdachte wordt (in de context van observatie) niet gezien als een meer dan geringe inbreuk;[141] het afnemen van een enkele vingerafdruk op een publiek toegankelijke plaats maakt naar het oordeel van de commissie evenmin een meer dan geringe privacyinbreuk. Voor lichaamsmateriaal ligt dat anders, omdat uit dit materiaal via het DNA tal van persoonskenmerken kunnen worden afgeleid. Mede daarom is in de regeling van DNA-onderzoek een specifieke bepaling opgenomen, die het mogelijk maakt om DNA-onderzoek te verrichten aan celmateriaal op inbeslaggenomen voorwerpen of dat op andere wijze verkregen is (artikel 151b lid 4 Sv en het voorgestelde artikel 2.6.5.7.1 lid 5).

In Hoofdstuk 6 van het conceptwetsvoorstel met betrekking tot Boek 2 wordt in navolging daarvan nu ook een specifieke regeling getroffen voor het verrichten van onderzoek aan andere biometrische gegevens (te weten vingerafdrukken en handpalmafdrukken) buiten medeweten van de verdachte of wanneer de verdachte niet meewerkt of vermist is. In die gevallen is een bevel van de officier van justitie vereist.[142] De bepaling in artikel 2.6.5.4.2 lid 3 luidt als volgt:

[140] Artikel 1 onder s van het wetsvoorstel tot aanpassing van de Wpg, *Kamerstukken II* 2017/18, 34 889, nr. 2, luidt: "biometrische gegevens: persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische, of gedragskenmerken van een natuurlijke persoon op grond waarvan de eenduidige identificatie van die persoon mogelijk is of bevestigd wordt, zoals afbeeldingen van het gezicht of dactyloscopische gegevens".

[141] Zie bijvoorbeeld ook HR 18 april 2017, ECLI:NL:HR:2017:725, NJ 2017/457, m.nt. B.F. Keulen.

[142] Zie artikel 2.6.5.4.2 lid 3. Een dergelijke regeling is ook opgenomen voor handschrift- en stemvergelijkend onderzoek in artikel 2.6.5.5.1 lid 2.

> In afwijking van het eerste lid kan de officier van justitie, indien het in het belang van het onderzoek is dat de vingerafdrukken of handpalmafdrukken van de verdachte buiten zijn medeweten worden verkregen, of indien de verdachte zich tegen de afname van zijn vingerafdrukken of handpalmafdrukken verzet of vermist is, het vergelijkend onderzoek laten verrichten aan de vingerafdrukken of handpalmafdrukken die op een in beslag genomen voorwerp aanwezig zijn of op andere wijze verkregen zijn, mits voldoende zekerheid bestaat dat die vingerafdrukken of handpalmafdrukken van hem afkomstig zijn.

Het heimelijk verzamelen van materiaal ten behoeve van biometrische toegangsverschaffing vertoont overeenkomsten met het verkrijgen van vingerafdrukken of handpalmafdrukken in het belang van het onderzoek. De methode is immers vergelijkbaar, alleen het doel verschilt: vergelijkend onderzoek onderscheidenlijk biometrische ontsluiting. Daarom ligt het voor de hand om voor heimelijke vergaring van biometrische gegevens ter ontsluiting van een geautomatiseerd werk of een digitale-gegevensdrager een vergelijkbare regeling te treffen als voor vergelijkend onderzoek van vinger- of handpalmafdrukken, met een expliciete wettelijke basis en een bevel van de officier van justitie.

Aanbeveling 29: er wordt een bevoegdheid ingevoerd 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, worden gebruikt ten behoeve van de ontsluiting van een digitale-gegevensdrager of een geautomatiseerd werk. Deze bevoegdheid zou ondergebracht kunnen worden in artikel 2.7.4.1.4. → *p. 198*

Biometrie van overleden personen

Een laatste vraagpunt is of er een regeling nodig is voor situaties waarin de gebruiker van het apparaat is overleden, maar nog een bruikbare vingerafdruk of ander biometrisch kenmerk heeft. Het recht op lichamelijke integriteit werkt in beginsel door na overlijden.[143] Het lichaam van overledenen kan dan ook rekenen op rechtsbescherming (zie bijvoorbeeld artikel 150 Sr), in overeenstemming met de menselijke waardigheid. Het gebruiken van de vinger van een overledene voor biometrische toegangsverschaffing lijkt ons echter een geringere inbreuk op de menselijke waardigheid dan het onderzoek dat bij opsporing aan het lichaam van overledenen kan worden verricht. In het conceptwetsvoorstel van Boek 2 staat in Hoofdstuk 6 een bepaling over onderzoek aan overledenen (met name betreffende de sectie; zie artikel 2.6.6.1 in samenhang met de Wet op de lijkbezorging en memorie van toelichting, p. 38-40 en 156-159). In tegenstelling tot dat onderzoek aan overledenen, dat de menselijke waardigheid raakt omdat sectie of ander geneeskundig onderzoek veelal gepaard gaat met het aantasten van het lichaam, vormt het gebruik van een biometrisch kenmerk, met name een vingerafdruk, geen aantasting van het lichaam, maar slechts een beperkte aanraking. In dat licht zou de bevoegdheid dan ook gebaseerd kunnen worden op artikel 3 Politiewet 2012 (hierna: PW 2012).[144]

Aanbeveling 30: in de memorie van toelichting kan worden gewezen op de mogelijkheid dat, met inachtneming van respect voor de menselijke waardigheid, een biometrisch kenmerk van het lichaam van een overledene kan worden afgenomen op basis van de algemeen taakstellende artikelen, zoals artikel 3 Politiewet 2012. → *p. 198*

[143] *Kamerstukken II* 1978/79, 15 463, nr. 2, p. 5-6, zie Zuiderveen Borgesius en Korteweg 2009, p. 215. Deze auteurs pleiten meer algemeen voor erkenning van privacybescherming na overlijden (p. 223). Zie ook *Kamerstukken II* 2007/08, 31 415, nr. 1, p. 24 en *Kamerstukken II* 2009/10, 32 168, nr. 3, p. 19.

[144] "De politie heeft tot taak in ondergeschiktheid aan het bevoegd gezag en in overeenstemming met de geldende rechtsregels te zorgen voor de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven."

5.5.3. Netwerkzoeking

Met de toename van de rol van internet in het maatschappelijk leven en het mobieler worden van de apparaten waarmee we toegang tot het internet hebben, is de behoefte toegenomen om accountgegevens, berichtgeschiedenis, notities en mediabestanden beschikbaar te hebben op meerdere apparaten en soms ook te delen met anderen. Tegelijk zijn opslag en verbindingen goedkoper geworden en is de technologie beschikbaar gekomen voor virtualisatie en gedistribueerde opslag. Daarmee werd "de cloud" een consumentenproduct. De instellingen van een toestel worden online opgeslagen, evenals foto's en video's, e-mails, chats, agenda en eventueel een volledige reservekopie. De gebruiker van het apparaat weet daarbij niet (meer) wat op het apparaat staat en wat alleen in de cloud is opgeslagen. Zolang zijn internetverbinding werkt, is er voor de gebruiker eigenlijk geen verschil. Alle gezochte informatie komt onmiddellijk in beeld.

De politie heeft sinds jaar en dag de mogelijkheid om voorwerpen (waaronder dus ook geautomatiseerde werken en digitale-gegevensdragers) in beslag te nemen en ze te onderzoeken (artikel 94 e.v. Sv, inmiddels met inachtneming van het smartphone-arrest van de Hoge Raad). Tijdens een doorzoeking (onder leiding van de officier van justitie of rechter-commissaris) kan de politie ook geautomatiseerde werken en digitale-gegevensdragers doorzoeken om te bepalen of ze relevant zijn voor de waarheidsvinding. Indien nodig kunnen er tijdens de doorzoeking ook gegevens worden vastgelegd die op de plaats van de doorzoeking op een gegevensdrager zijn opgeslagen of vastgelegd (op grond van het huidige artikel 125i Sv).

Tevens bevat het huidige wetboek al de bevoegdheid tot een netwerkzoeking: tijdens een doorzoeking (van een woning, bedrijf of voertuig) is het mogelijk om onderzoek te doen in een geautomatiseerd werk dat op een andere plaats staat (het huidige artikel 125j Sv). Relevant met betrekking tot deze bevoegdheid is Aanbeveling 17 in par. 5.1.2 onder "Samenhang met geautomatiseerde werken" om de netwerkzoeking ook mogelijk te maken in digitale-gegevensdragers die zich elders bevinden (en dus niet langer alleen in geautomatiseerde werken).

Deze bevoegdheid komt thans minder tot zijn recht dan in de praktijk gewenst is, terwijl informatie die belangrijk is voor de opsporing in toenemende mate online (en dus elders) is opgeslagen. Het belangrijkste knelpunt is dat de effectiviteit sterk wordt beperkt door jurisdictieproblemen. Bij uitstek bij de toepassing van deze bevoegdheid speelt de onduidelijkheid van de locatie van data een wezenlijke rol, een onduidelijkheid die nog versterkt wordt doordat grote partijen veelal niet willen of kunnen verklaren waar de data van hun gebruikers precies liggen opgeslagen. Dit algemene knelpunt van jurisdictie valt buiten de opdracht van de commissie, maar is in dit verband wel belangrijk om nogmaals te benadrukken (zie verder par. 3.1). Een tweede probleem is de beperkte periode gedurende welke de bevoegdheid kan worden ingezet, namelijk gedurende de doorzoeking. Vaak blijkt pas na onderzoek van een in beslag genomen geautomatiseerd werk dat deze niet de gezochte informatie bevat, maar dat deze informatie elders wel is opgeslagen. Vanwege het beperkte toepassingsbereik, is de voornaamste toepassing van de netwerkzoeking nu om tijdens een doorzoeking bij een bedrijf, met ondersteuning van de ICT-afdeling, data veilig te stellen van een server die het bedrijf huurt in een datacentrum elders.

In het conceptwetsvoorstel is de netwerkzoeking in twee artikelen opgenomen.[145] De eerste bepaling is opgenomen in Afdeling 7.4.1 "Onderzoek ter inbeslagneming van gegevens" en betreft feitelijk een overname van het huidige artikel 125j Sv. Het gaat in deze Afdeling om onderzoek aan elektronische gegevensdragers of geautomatiseerde werken zonder deze apparaten zelf in beslag te nemen. Wel kunnen de gegevens die op de apparaten zijn opgeslagen in beslag worden genomen, aldus het voorstel. Ter inbeslagneming van gegevens kan de officier

[145] Gezien de adviezen van de commissie over onder meer het beslag op gegevens is het goed mogelijk dat de artikelen zullen worden heroverwogen en misschien zelfs samengevoegd.

van justitie bevelen dat vanaf de plaats waar dit onderzoek wordt verricht, nader onderzoek wordt gedaan in een elders aanwezig geautomatiseerd werk:

> **Artikel 2.7.4.1.2 [artikel 125j]**
>
> 1. In geval van onderzoek als bedoeld in artikel 2.7.4.1.1 kan de officier van justitie bevelen dat een opsporingsambtenaar ter inbeslagneming van gegevens vanaf de plaats waar de opsporingsambtenaar het onderzoek verricht, nader onderzoek doet in een elders aanwezig geautomatiseerd werk naar in dat werk opgeslagen gegevens.
>
> 2. Het onderzoek reikt niet verder dan voor zover de personen die plegen te werken of te verblijven op de plaats waar het onderzoek plaatsvindt, vanaf die plaats, met toestemming van de rechthebbende tot het geautomatiseerde werk, daartoe toegang hebben.
>
> 3. Artikel 2.7.4.1.1, tweede en derde lid, is van overeenkomstige toepassing

Het tweede artikel waarin de netwerkzoeking wordt voorgesteld is opgenomen in Afdeling 7.4.2 "Onderzoek ter kennisneming van gegevens". Deze Afdeling ziet op de situaties waarin een elektronische gegevensdrager of een geautomatiseerd werk in beslag is genomen. Aan de inbeslaggenomen apparaten kan onderzoek worden gedaan ter kennisneming van de gegevens die daarop zijn opgeslagen. Ook bij dit onderzoek wordt de netwerkzoeking mogelijk gemaakt (waarin het conceptwetsvoorstel dus alleen over geautomatiseerde werken spreekt):

> **Artikel 2.7.4.2.2 [nieuw]**
>
> 1. In geval van onderzoek als bedoeld in artikel 2.7.4.2.1, eerste lid, kan de officier van justitie bevelen dat een opsporingsambtenaar ter kennisneming van gegevens vanaf de plaats waar de opsporingsambtenaar het onderzoek verricht, nader onderzoek doet in een elders aanwezig geautomatiseerd werk naar in dat werk opgeslagen gegevens.
>
> 2. Het nader onderzoek reikt niet verder dan voor zover de persoon onder wie het geautomatiseerd werk in beslag is genomen met toestemming van de rechthebbende tot het elders aanwezig geautomatiseerd werk, daartoe toegang heeft.
>
> 3. Artikel 2.7.4.2.1, tweede lid, is van overeenkomstige toepassing.

Is de regeling duidelijk?

Uit de wetsgeschiedenis blijkt dat de wetgever met de netwerkzoeking heeft bedoeld justitie dezelfde toegangsmogelijkheid te geven die de rechthebbende op het geautomatiseerd werk elders heeft geschapen voor de persoon of personen die plegen te werken of verblijven op de plaats van de doorzoeking. In de memorie van toelichting op artikel 125j Sv wordt dit de "dubbele band" genoemd.[146] Dit aspect moet in de nieuwe artikelen ook worden vertaald naar de situatie buiten de doorzoeking. In de voorgestelde tekst is dat nog niet helemaal gebeurd.

In geval van artikel 2.7.4.1.2 komt dit doordat de netwerkzoeking nu kan worden losgekoppeld van de plaats van de doorzoeking (de "plaats waar de opsporingsambtenaar het onderzoek verricht" is niet per se "de plaats waar de doorzoeking plaatsvindt" die nu in artikel 125j Sv wordt genoemd), een voor de opsporing welkome uitbreiding van de bevoegdheid. In plaats van het aanknopen bij de plaats van de doorzoeking, is ervoor gekozen aan te knopen bij de plaats waar de opsporingsambtenaar het onderzoek uitvoert. Dat zal vaak de plaats zijn waar op dat moment een doorzoeking plaatsvindt, zoals een woning of bedrijf. In dat geval volstaat de formulering van het voorgestelde tweede lid: "Het onderzoek reikt niet verder dan voor zover de personen die plegen te werken of te verblijven op de plaats waar het onderzoek plaatsvindt, vanaf die plaats, met toestemming van de rechthebbende tot het geautomatiseerde werk, daartoe toegang hebben".

[146] *Kamerstukken II* 1989/90, 21 551, nr. 3, p. 27.

Maar het nader onderzoek kan ook plaatsvinden na een aanhouding of staandehouding, op een plaats waar de rechthebbende niet pleegt te werken of te verblijven, zoals op straat of in een winkel. In de praktijk zal dan veelal worden overgegaan tot het in beslag nemen van het apparaat, waarna op grond van Afdeling 7.4.2 een netwerkzoeking kan plaatsvinden na inbeslagneming van het geautomatiseerde werk. Het is echter denkbaar dat op grond van Afdeling 7.4.1 direct ter plekke, op een plaats waar de rechthebbende geen bepaalde band mee heeft, een netwerkzoeking plaatsvindt. In dat geval adviseert de commissie aan te sluiten bij de rechten van de persoon (of groep van personen) die gebruiker is of was van het geautomatiseerd werk dat (of de digitale-gegevensdrager die) wordt doorzocht. Er zal wel een sterke proportionaliteitstoets gelden als het geautomatiseerde werk tevens in gebruik was bij niet-betrokken derden. Hier zal wel rekening mee moeten worden gehouden in de toetsing van proportionaliteit en subsidiariteit. In de memorie van toelichting kan bijvoorbeeld worden uitgelegd dat het mogelijk is dat een netwerkzoeking plaatsvindt nadat een onderzoekssubject via een bibliotheekcomputer heeft ingelogd op een elders aanwezig geautomatiseerd werk (bijvoorbeeld op sociale media of een e-mailaccount), maar dat het daarbij niet proportioneel is om een netwerkzoeking uit te voeren op elders aanwezige geautomatiseerde werken (of digitale-gegevensdragers) met accounts van niet-betrokkenen die toevallig ook gebruik hebben gemaakt van die bibliotheekcomputer.

Aanbeveling 31: de voorwaarde in het tweede lid van het voorgestelde artikel 2.7.4.1.2 dient beter aan te sluiten bij de mogelijkheid dat de netwerkzoeking plaatsvindt op een afwijkende plaats. Bijvoorbeeld: “In geval van een doorzoeking of betreding van een plaats reikt het onderzoek niet verder dan voor zover de personen die plegen te werken of te verblijven op de plaats van de doorzoeking of betreding, vanaf die plaats, met toestemming van de rechthebbende tot het geautomatiseerde werk of de digitale-gegevensdrager, daartoe toegang hebben. In overige gevallen reikt het onderzoek niet verder dan voor zover de gebruiker van het geautomatiseerde werk dat, of de digitale-gegevensdrager die, wordt onderzocht, met toestemming van de rechthebbende tot dat geautomatiseerde werk of die digitale-gegevensdrager, daartoe toegang heeft.” → *p. 199*

In de praktijk vindt de doorzoeking ter vastlegging van gegevens en de netwerkzoeking regelmatig plaats bij een datacentrum of een andere professionele partij. Dergelijke bedrijven hebben tegenwoordig veel faciliteiten om van afstand toegang te verschaffen ten behoeve van bijvoorbeeld onderhoud, en slechts beperkte faciliteiten om fysiek toegang te verschaffen. Tot nu toe moest de doorzoeking op zo’n locatie voortduren zo lang als het duurde om de gewenste gegevens van of vanuit een server vast te leggen. De opsporingsambtenaar moest tijdens het overnemen van de gegevens ook fysiek op die locatie aanwezig blijven om aan de wet te voldoen. De commissie constateert dat de koppeling tussen de rechthebbende op gegevens en de fysieke locatie van die gegevens in de gedigitaliseerde en gevirtualiseerde wereld achterhaald is. Nu, maar zeker in de toekomst, zullen de meeste gezochte gegevens zich niet meer fysiek in de omgeving van het subject maar ergens in de cloud bevinden. De commissie adviseert derhalve de wetgever om in dergelijke gevallen de mogelijkheid tot een doorzoeking ter plaatse te behouden maar daarnaast het uitvoeren van het onderzoek van afstand mogelijk te maken.

Aanbeveling 32: wanneer een (rechts)persoon waar een doorzoeking plaatsvindt, de opsporing de mogelijkheid biedt om van afstand de doorzoeking (en daarop volgend eventueel een netwerkzoeking) uit te voeren of voort te zetten, moet dit gelijk gesteld worden met een doorzoeking bij de (rechts)persoon zelf. → *p. 199*

Bij het voorgestelde artikel 2.7.4.2.2 doet zich evenals bij artikel 2.7.4.1.2 een probleem voor. In artikel 2.7.4.2.2 staat dat het onderzoek niet verder reikt dan zover de persoon onder wie het geautomatiseerd werk in beslag is genomen met toestemming van de rechthebbende tot het elders aanwezig geautomatiseerd werk, daartoe toegang heeft. Dit kan tot problemen leiden wanneer degene onder wie het apparaat in beslag is genomen, niet de gebruiker is van het apparaat. Het is dan meer in lijn met de uitleg van het huidige artikel, om ook daar uit te gaan van de band tussen de (normale) gebruiker van het apparaat en het doel van de netwerkzoeking dan dat de persoon centraal komt te staan die het apparaat toevallig in handen had op het moment dat het in beslag werd genomen. Enkele voorbeelden om dit te illustreren.

- Soms is een apparaat in gebruik (geweest) bij meerdere personen die allen hun eigen accounts (bijvoorbeeld e-mail of cloud-opslag) raadplegen.
- Wanneer een apparaat in beslag wordt genomen tijdens een doorzoeking van een woning of bedrijfspand, is op voorhand niet altijd duidelijk van wie het is, en het kan best een ander zijn dan degene onder wie het in beslag is genomen.
- Op een plaats delict kan een toestel worden aangetroffen dat van zowel een slachtoffer, een dader als een getuige kan zijn.

Het in gebruik zijn geweest van het geautomatiseerd werk bij een bepaald persoon kan blijken uit het feit dat er vanuit het geautomatiseerde werk is ingelogd op het mail-, chat- of sociale-media-account van die persoon.

Aanbeveling 33: de restrictie in het tweede lid van artikel 2.7.4.2.2 wordt gewijzigd in: "Het nader onderzoek reikt niet verder dan voor zover de gebruiker van het geautomatiseerd werk dat, of de digitale-gegevensdrager die, in beslag is genomen met toestemming van de rechthebbende tot het elders aanwezig geautomatiseerd werk of digitale-gegevensdrager, daartoe toegang heeft." → *p. 199*

De commissie realiseert zich dat het mogelijk is dat iemand maar kortstondig of eenmalig gebruik heeft gemaakt van het geautomatiseerd werk, of dat hij een onrechtmatige gebruiker is van het geautomatiseerde werk (zoals na diefstal). Ook in die gevallen kan het noodzakelijk zijn om de netwerkzoeking uit te voeren en is er geen goede reden om een netwerkzoeking bij voorbaat uit te sluiten. Hier zal wel rekening mee moeten worden gehouden in de toetsing van proportionaliteit en subsidiariteit. In de memorie van toelichting kan bijvoorbeeld worden uitgelegd dat het mogelijk is dat een netwerkzoeking plaatsvindt nadat een onderzoekssubject heeft ingelogd op een elders aanwezig geautomatiseerd werk (bijvoorbeeld op sociale media of een e-mailaccount) via een door hem gestolen smartphone, om toegang te krijgen tot het account van het onderzoekssubject, maar dat het in principe niet proportioneel is om de netwerkzoeking uit te voeren ten aanzien van accounts van de oorspronkelijke (rechtmatige) gebruiker.

Periode

Deze subparagraaf behandelt het vraagstuk gedurende welke periode de netwerkzoeking mag voortduren of herhaaldelijk mag worden uitgevoerd.

De bevoegdheid tot netwerkzoeking is van oudsher bedoeld voor het verkrijgen van historische gegevens: het gaat om in het elders aanwezige werk opgeslagen gegevens. Nu de bevoegdheid van netwerkzoeking in het conceptwetsvoorstel niet meer is beperkt tot de doorzoeking van een plaats en ook niet tot geautomatiseerde werken die tijdens een doorzoeking worden aangetroffen, rijst de vraag hoe lang de netwerkzoeking zou mogen duren en hoe veel tijd er tussen doorzoeking, inbeslagneming en de netwerkzoeking mag zitten. Het bespreken van dit discussiepunt hangt samen met het meer algemene vraagstuk over het vastleggen en kennisnemen van inhoudelijke gegevens die binnenkomen na de inbeslagname van het apparaat

waaraan het onderzoek plaatsvindt of tijdens de doorzoeking ter vastlegging van gegevens (zie par. 5.3.4).

Binnen de commissie is discussie gevoerd over de vraag hoe lang de netwerkzoeking mag voortduren vanaf het begin van die netwerkzoeking. De commissie is daarbij van oordeel dat de netwerkzoeking zo lang mag duren als redelijkerwijs noodzakelijk is om alle benodigde gegevens binnen te krijgen. Daarbij wordt wel aanbevolen te benoemen dat de duur van de netwerkzoeking in beginsel niet langer zou mogen zijn dan enkele dagen. Daarvan kan onder omstandigheden worden afgeweken, maar als er meer tijd nodig is om de netwerkzoeking in redelijkheid zorgvuldig uit te voeren, dan moet dit nader worden gemotiveerd.

Aanbeveling 34: de duur van de netwerkzoeking wordt in de memorie van toelichting zodanig uitgelegd dat de netwerkzoeking zo lang mag duren als voor het initiële onderzoek redelijkerwijs noodzakelijk is om alle benodigde gegevens binnen te krijgen. Deze periode is wel in beginsel begrensd tot enkele dagen; zijn er omstandigheden die een langere duur noodzakelijk maken, dan moet dit worden gemotiveerd. → *p. 199*

Een andere vraag is of er een voorschrift moet gelden over wanneer de netwerkzoeking moet zijn aangevangen. Deze vraag geldt met name voor de situatie waarin geautomatiseerde werken in beslag zijn genomen. Het wettelijk inperken van het moment waarop een netwerkzoeking mogelijk is tot "terstond na" de inbeslagname of tot een andere specifieke periode wordt door de opsporingsinstanties als onwenselijk beschouwd; het levert hetzelfde probleem op als de huidige beperking tot het moment van de doorzoeking, namelijk dat niet altijd terstond duidelijk is dat mogelijk relevante gegevens elders zijn opgeslagen. De inzichten die resulteren uit het onderzoek aan de (via onderzoek aan het geautomatiseerde werk of de digitale-gegevensdrager) verkregen gegevens, die niet altijd kort na de inbeslagname beschikbaar zijn, zouden daarom ook het startpunt moeten kunnen zijn voor het aanvragen van een bevel tot netwerkzoeking. Dat maakt het mogelijk om gericht te werk te gaan. Het zou in dat licht ook mogelijk moeten zijn om de netwerkzoeking juist op een later moment aan te vangen dan het initiële onderzoek aan het geautomatiseerde werk of de digitale-gegevensdrager zelf.

Overwogen is of er een maximum gesteld zou moeten worden aan de periode die verstrijkt tussen het moment van inbeslagname van een geautomatiseerd werk en het onderzoeken daarvan. In de praktijk worden soms grote hoeveelheden gegevensdragers in beslag genomen (tientallen telefoons zijn bij een onderzoek naar een drugsdealer geen uitzondering), waardoor het de digitaal specialist behoorlijk wat tijd kost deze op forensische wijze veilig te stellen en dit te documenteren. Het stellen van een maximumtermijn zou er ook in kunnen resulteren dat gegevens van alle in beslag genomen gegevensdragers snel integraal worden overgenomen, teneinde binnen de termijn te blijven. Dat komt de proportionaliteit van het onderzoek niet altijd ten goede. Als bijvoorbeeld het (al dan niet ontlastend) bewijs al gevonden wordt in een van de eerste veiliggestelde telefoons, is het wellicht niet noodzakelijk alle gegevens van de andere telefoons over te nemen. Hoewel sommige commissieleden het standpunt innemen dat er een beperkte en concrete maximumtermijn moet worden gesteld, adviseert de commissie, gelet op de genoemde deze argumenten, om geen vaste termijn te stellen waarbinnen inbeslaggenomen gegevensdragers moeten zijn onderzocht. De termijn moet een redelijke zijn, die afhangt van de omstandigheden van het geval; daarbij is de situatie op het moment van beslag bepalend, omdat dit moment de toestand reflecteert waarin de gezochte gegevens zich bevonden op het moment van de onderzoekshandeling die leidde tot beslag. Later binnengekomen of binnenkomende gegevens mogen worden gebruikt conform en onder de voorwaarden genoemd in paragraaf 5.3.4 (waarbij met name aandacht nodig is voor de beperking tot pure bijvangst en de voorwaarden als de opsporing een actieve rol heeft in het ophalen van onder artikel 13 Gw

beschermde berichten) en mits deze vallen binnen de redelijke termijn waarbinnen de netwerkzoeking dient plaats te vinden.

Het zijn vooral de beginselen van subsidiariteit en proportionaliteit de redelijke termijn begrenzen waarbinnen een netwerkzoeking op basis van later onderzoek aan een inbeslaggenomen geautomatiseerd werk of digitale-gegevensdrager kan worden gebaseerd. Indien er bijvoorbeeld een maand is verstreken voordat een inbeslaggenomen smartphone wordt onderzocht, terwijl de smartphone naar redelijke maatstaven ook al na een week onderzocht had kunnen worden, vervalt de grondslag om op basis van het late onderzoek in de smartphone een netwerkzoeking uit te voeren – er is immers een substantiële kans dat in het elders aanwezige geautomatiseerde werk inmiddels meer (en mogelijk aanzienlijk meer) gegevens aanwezig zijn dan op het moment van de oorspronkelijke inbeslagname van de smartphone. Een verlengde zoeking is dan niet meer subsidiair en proportioneel, omdat deze naar redelijke maatstaven eerder had kunnen plaatsvinden. Dit betekent dat bij een aanzienlijke periode tussen het moment van inbeslagneming en het moment van onderzoek aan het inbeslaggenomen geautomatiseerde werk, de opsporingsambtenaren moeten kunnen motiveren waarom dat onderzoek aanzienlijk later is uitgevoerd en waarom het proportioneel is om, ook in het licht van eventueel nieuw aanwezige gegevens in het geautomatiseerde werk elders, alsdan alsnog een netwerkzoeking uit te voeren.

Aanbeveling 35: er wordt geen vaste maximale termijn gesteld voor het moment waarop een netwerkzoeking kan aanvangen na inbeslagname. Er wordt tevens geen vaste maximale termijn gesteld voor het aanvangen van het onderzoek aan een in beslag genomen geautomatiseerd werk of digitale-gegevensdrager. Het gaat in beide gevallen om een redelijke termijn, die begrensd wordt door de beginselen van proportionaliteit en subsidiariteit. De voorwaarden genoemd in Aanbeveling 22 en bijbehorende tekst zijn daarbij van toepassing. → *p. 199*

Ten slotte is gesproken over de wens van de opsporing om een netwerkzoeking nogmaals te laten plaatsvinden als er uit andere bronnen nieuwe informatie bekend is geworden voor het opsporingsteam. Dit levert afhankelijk van de context van het geval enige spanning op met de oorspronkelijke bedoeling van de netwerkzoeking (zijnde het overnemen van gegevens die op het moment van een onderzoekshandeling niet ter plekke maar elders zijn opgeslagen). Wanneer het om een historische dataverzameling gaat, die onveranderd is gebleven (een reservekopie van de administratie van een verdachte die in voorarrest zit), dan zijn er naar verwachting geen nieuwe gegevens beschikbaar gekomen. Maar als er op het geautomatiseerd werk elders door het verloop van tijd nieuwe informatie is opgeslagen (bijvoorbeeld door derden in een cloud-omgeving), dan was deze ten tijde van de initiële netwerkzoeking nog niet opgeslagen. Opsporingsinstanties geven aan dat deze gegevens vaak cruciaal zijn voor het onderzoek; het betreft bijvoorbeeld gesprekken die gaan over de aanhouding van verdachte of de doorzoeking van zijn woning. Vanwege de spanning die zo'n gebeurtenis oplevert wordt er dan wel eens meer gezegd dan de bedoeling was, zo is de ervaring met telefoontaps. De commissie adviseert daarom toch zo'n herhaalde netwerkzoeking mogelijk te maken, op basis van een nieuw bevel. Overwogen is of dit nieuwe bevel per definitie door een hogere autoriteit zou moeten worden getoetst. De commissie is van mening dat dat niet noodzakelijk is, omdat het van de omstandigheden van het geval afhangt of het redelijkerwijs te verwachten is dat er (substantiële) nieuwe gegevens in het geautomatiseerde werk elders zullen worden aangetroffen. Zij beveelt daarom aan ook hier de driedeling van het algemene normeringscriterium te hanteren. Als het herhaalde onderzoek naar verwachting ingrijpend stelselmatig zal zijn, dan is een machtiging van de rechter-commissaris noodzakelijk; anders volstaat een bevel van de officier van justitie.

Indien er geen sprake is geweest van inbeslagneming van het desbetreffende geautomatiseerd werk, is tevens een bevel of machtiging nodig voor een nieuwe doorzoeking van de plaats van waaruit de eerste netwerkzoeking heeft plaatsgevonden. De commissie adviseert te bepalen dat de officier van justitie (of de rechter-commissaris) bij zo'n opvolgende netwerkzoeking de reikwijdte van het bevel bepaalt, waaronder de periode gedurende welke het bevel mag worden uitgevoerd.

Aanbeveling 36: het moet mogelijk zijn een herhaalde netwerkzoeking uit te voeren op grond van een nieuw bevel. De daartoe bevoegde autoriteit wordt bepaald aan de hand van het algemene normeringscriterium. In het bevel tot uitvoering van een herhaalde netwerkzoeking moet de reikwijdte van het bevel worden beschreven, waaronder de periode gedurende welke het bevel geldig is. → *p. 199*

Forensische apparatuur gebruiken voor de netwerkzoeking

In de voorgestelde artikelen met betrekking tot de netwerkzoeking staat dat de opsporingsambtenaar vanaf de plaats waar hij of zij het onderzoek verricht, nader onderzoek doet in een elders aanwezig geautomatiseerd werk naar in dat werk opgeslagen gegevens. De gebruiker van het geautomatiseerd werk of de personen die plegen te werken of te verblijven op de plaats van doorzoeking moeten rechtmatig toegang hebben gehad tot het geautomatiseerd werk elders. Maar niet is bepaald dat het onderzoek daadwerkelijk met het (al dan niet in beslag genomen) initiële geautomatiseerde werk zou moeten plaatsvinden.

Een dergelijke verplichting vinden we ook niet in het huidige artikel 125j Sv. Wanneer nu een netwerkzoeking plaatsvindt bij een bedrijf, wordt er samen met de ICT-afdeling besloten wat de forensisch en economisch optimale manier is om de benodigde gegevens veilig te stellen. De systeembeheerder weet over het algemeen goed welke gegevens waar staan en hoe ze het beste kunnen worden overgenomen. De systeembeheerder zal soms zelf inloggen op de locatie elders om samen met de opsporingsambtenaar de gegevens te selecteren en deze weg te schrijven naar een opslagmedium dat door de opsporingsambtenaar is meegenomen. Maar het gebeurt ook dat via de laptop van de opsporingsambtenaar toegang wordt verkregen tot het bedrijfsnetwerk om via dat netwerk in te kunnen loggen op een andere locatie en bepaalde gegevens over te nemen. Op die manier kan het hele proces worden gelogd en kan er meteen een controlegetal (hashwaarde) worden berekend van de overgenomen gegevens.

Dit onderlinge overleg en kiezen op welke wijze de gegevens het beste kunnen worden veiliggesteld, gebeurt minder vaak bij een netwerkzoeking vanuit een woning. In dat geval is degene die zou kunnen assisteren bij de netwerkzoeking veelal de verdachte zelf. En hij, noch zijn apparatuur, kunnen in beginsel worden vertrouwd met het bewaren van de integriteit van het bewijs. Toch wordt meestal het geautomatiseerde werk van de verdachte gebruikt voor het uitvoeren van de netwerkzoeking in een woning, soms omdat de inloggegevens niet kunnen worden overgenomen uit het geautomatiseerd werk, maar soms ook omdat digitaal specialisten het gevoel hebben dat ze daarmee buiten de bevoegdheid zouden treden. Er zijn echter commerciële producten beschikbaar die speciaal zijn ontwikkeld voor het uitvoeren van een forensisch integere "cloud-doorzoeking". Overigens is de ervaring van de digitale recherche dat officieren van justitie en rechters-commissarissen hierbij het advies van de digitaal specialist volgen; zij worden dus niet op juridische gronden beperkt in welke apparatuur zij mogen gebruiken bij de netwerkzoeking.

Met name wanneer het gaat om een netwerkzoeking na beslag, is het vanuit het perspectief van een effectieve en zuivere opsporing onwenselijk om verplicht te zijn het "verdachte" geautomatiseerde werk te moeten gebruiken, om de volgende redenen.

- Zodra het geautomatiseerd werk verbinding maakt met het internet, kan een van afstand gegeven wiscommando worden ontvangen en uitgevoerd.

- Als een apparaat verbinding maakt met internet, kunnen allerlei apps gaan synchroniseren en daarmee data binnenhalen waarvoor geen toestemming is gegeven.
- Het gebruiken van het inbeslaggenomen geautomatiseerde werk zal wijzigingen aanbrengen die mogelijk belangrijke data overschrijven (denk aan logs). Dit is vanuit forensisch oogpunt onwenselijk.
- Het handmatig via de interface van een telefoon doorzoeken van grote hoeveelheden data (bijvoorbeeld chat of mailhistorie) kost te veel handelingen en geeft kans op het maken van fouten.
- Het gebruik van een geteste opstelling voor het veiligstellen van precies die gegevens waartoe de gebruiker met toestemming van de rechthebbende toegang had is de enige onderzoeksmethode die goede, forensische logging van de onderzoekshandelingen mogelijk maakt.

De opsporing zou in voorkomende gevallen dus gebruik moeten kunnen maken van forensische apparatuur in plaats van het inbeslaggenomen apparaat. Maar de keuze voor het uitvoeren van de netwerkzoeking met een speciaal daarvoor ingericht apparaat mag niet leiden tot een uitbreiding van de bevoegdheid. In de memorie van toelichting moet dan ook nadrukkelijk worden opgenomen dat indien voor de uitoefening van een netwerkzoeking een ander apparaat wordt gebruikt dan het oorspronkelijke geautomatiseerde werk, er dus niet méér toegang mag worden verworven dan bij onderzoek vanaf het oorspronkelijke geautomatiseerde werk het geval zou zijn geweest. Het is dan ook een voorwaarde dat het beslag op het inbeslaggenomen geautomatiseerde werk nog voortduurt gedurende de netwerkzoeking.

Aanbeveling 37: de commissie beveelt aan om toe te lichten dat de netwerkzoeking ook met forensische onderzoeksapparatuur kan plaatsvinden, waarbij niet méér toegang mag worden verworven dan bij onderzoek vanaf het oorspronkelijke geautomatiseerde werk het geval zou zijn. → *p. 199*

Afbakening

Zoals eerder in dit hoofdstuk (par. 5.3.4) aan bod kwam, heeft de voorgestelde netwerkzoeking raakvlakken met een aantal (heimelijke) bevoegdheden. Doordat er een veelheid aan technieken bestaat om informatie gedistribueerd op te slaan en in het wetboek wordt geprobeerd zo techniekonafhankelijk mogelijk te reguleren, kan dit ook niet anders. Steeds zal moeten worden gekeken naar de handelingen die moeten worden verricht om kennis te kunnen nemen van de gezochte informatie en welke bevoegdheden de opsporingsambtenaar legitimeren deze handelingen uit te voeren. Het kan ook voorkomen dat een feitelijke handeling onder meerdere bevoegdheden gelegitimeerd is. Er zal dan ook per geval door de opsporingsambtenaar en de officier van justitie (en eventueel de rechter-commissaris) beoordeeld moeten worden welke bevoegdheden op die feitelijke handelingen in de desbetreffende context van toepassing zijn. Dat is in het huidige Wetboek van Strafvordering niet anders.

In paragraaf 5.3.4 over later binnenkomende berichten werd al gesproken over de aangrenzende interceptiebevoegdheid. Een andere belangrijke afbakening van de netwerkzoeking is die ten opzichte van de bevoegdheid om (van afstand) binnen te dringen in een geautomatiseerd werk, voorgesteld artikel 126nba Sv (wetsvoorstel CCIII). Wellicht ten overvloede merken we op dat de handelingen die onder de netwerkzoeking vallen, onder omstandigheden ook kunnen worden uitgevoerd ter (voorbereiding op de) uitvoering van een bevel op grond van artikel 126nba Sv. Maar wat is de reikwijdte van de netwerkzoeking, en wanneer wordt het noodzakelijk om de bevoegdheid van artikel 126nba Sv in te zetten?

Een eerste onderscheid is dat de netwerkzoeking alleen mag worden uitgevoerd wanneer er voorafgaand een doorzoeking, een inbeslagname, of een onderzoek van het geautomatiseerd

werk bij aanhouding of staandehouding heeft plaatsgevonden. De netwerkzoeking mag bovendien alleen betrekking hebben op elders opgeslagen gegevens als er een rechtmatige band bestaat tussen de gebruiker en deze gegevens, terwijl de bevoegdheid omschreven in artikel 126nba Sv de opsporingsambtenaar laat binnendringen in elk geautomatiseerd werk dat bij de verdachte in gebruik is, dus ook geautomatiseerde werken waar hij niet rechtmatig toegang toe heeft. Deze bevoegdheid is ook niet beperkt tot opgeslagen gegevens.

Bij de netwerkzoeking mag de opsporingsambtenaar alleen op min of meer dezelfde wijze inloggen als de gebruiker. Het kan zijn dat er gebruik wordt gemaakt van geautomatiseerde handelingen, maar vanuit het perspectief van de beheerder van het account (bijvoorbeeld Google) wordt er "gewoon ingelogd". De 126nba-bevoegdheid legitimeert het gebruik van andere methodes om te kunnen binnendringen in het geautomatiseerd werk.

Is deze regeling afdoende genormeerd?

Zoals eerder aangegeven, wordt de netwerkzoeking nu vaak gebruikt bij het vastleggen van bedrijfsadministraties. De officier van justitie is bij de doorzoeking van een bedrijf de bevoegde autoriteit, ook als zich opgeslagen communicatie onder de gegevens bevindt.

De commissie acht het voorstelbaar dat de netwerkzoeking een bevoegdheid wordt waar vaker een beroep op zal worden gedaan, nu deze wordt uitgebreid naar de situatie waarin een geautomatiseerd werk in beslag is genomen en situaties waarbij na aanhouding of staandehouding een geautomatiseerd werk ter plekke wordt onderzocht. De bevoegdheid zal regelmatig tot lastige afwegingen leiden in sfeer van bevoegdheid (de afbakening) en proportionaliteit, alsmede territorialiteit. Daarnaast zullen de gegevens die worden onderzocht mogelijk communicatie bevatten, waarvan een deel onder omstandigheden kan vallen onder de bescherming van artikel 13 Gw.

Aanbeveling 38: op de netwerkzoeking zou hetzelfde algemene normeringscriterium van toepassing moeten zijn als op het onderzoek van gegevens in of overgenomen uit een geautomatiseerd werk of digitale-gegevensdrager. Wanneer daarbij berichten worden onderzocht die zijn toevertrouwd aan een derde en die worden beschermd onder artikel 13 Gw, is altijd een machtiging van de rechter-commissaris vereist (vgl. par. 6.3.4).

→ *p. 199*

Ten slotte

De mogelijkheid om onder voorwaarden onderzoek te kunnen doen in een geautomatiseerd werk of digitale-gegevensdrager elders is belangrijk voor de opsporingspraktijk. Dit komt doordat er in het algemeen steeds meer data worden gegenereerd en bewaard, maar deze steeds minder op het geautomatiseerde werk dat een verdachte bij zich draagt worden opgeslagen, en steeds meer in de cloud. Dit blijkt ook uit dagelijks bij opsporingsinstanties binnenkomende vragen en verzoeken, waarbij vooral het probleem naar voren komt dat momenteel geen in de wet geregelde mogelijkheid bestaat om elders opgeslagen gegevens via een netwerkzoeking te verkrijgen na inbeslagname van een geautomatiseerd werk of buiten de context van een doorzoeking ter vastlegging van gegevens. Het is evident dat de wetgever met het onderhavige wetsvoorstel dit gat wenst te dichten. Nu de noodzaak om ook na beslag een netwerkzoeking te kunnen doen zich vrijwel dagelijks voordoet en het gebrek aan een wettelijke bevoegdheid tot onwenselijke complicaties leidt, acht de commissie het onverantwoord om te wachten met deze wetgeving tot de inwerkingtreding van het nieuwe Wetboek van Strafvordering. De commissie adviseert dan ook nadrukkelijk om de mogelijkheid een netwerkzoeking uit te kunnen voeren na de inbeslagname of bij onderzoek van een geautomatiseerd werk of digitale-gegevensdrager na aanhouding of staandehouding zo spoedig mogelijk in te voeren.

Aanbeveling 39: de wettelijke uitbreiding van de mogelijkheid tot een netwerkzoeking na beslag en in situaties van aanhouding en staandehouding is op korte termijn dringend wenselijk, waarbij het moderniseringstraject niet kan worden afgewacht. → *p. 200*

5.5.4. Ontoegankelijk maken

Het begrip ontoegankelijk maken

Wanneer de politie illegale inhoud aantreft op een server of een in beslag genomen gegevensdrager, dan is het om het strafbare feit te beëindigen of andere strafbare feiten te voorkomen soms noodzakelijk om zeker te stellen dat anderen daar niet meer van kunnen kennisnemen. Voorbeelden zijn kinderpornografische afbeeldingen, lijsten met gehackte inloggegevens, schadelijke malwareprodukten, lijsten met creditcardnummers en CVC-codes. In het conceptwetsvoorstel wordt in zo'n geval gesproken van ontoegankelijk maken (Titel 7.5). Dit begrip "ontoegankelijk maken" wordt nader uitgelegd in de definitiebepaling.

> **Artikel 2.1.1.1. definitiebepaling**
>
> j. ontoegankelijkmaking van gegevens: het treffen van voorlopige maatregelen ter voorkoming van de verdere kennisneming, gebruikmaking of verspreiding van die gegevens of het verwijderen van gegevens uit een geautomatiseerd werk of van een elektronische gegevensdrager, met behoud van die gegevens ten behoeve van de strafvordering. [artikel 126o,[147] tweede lid]

In de memorie van toelichting (p. 102) is over de definitiebepaling het volgende opgenomen:

> De definitie van ontoegankelijkmaking van gegevens is overgenomen uit het huidige artikel 125o, tweede lid. Het begrip wordt binnen het kader van Boek 2 gebruikt in Hoofdstuk 7. In de definitie is verduidelijkt dat het bij de ontoegankelijkmaking van gegevens gaat om het treffen van voorlopige maatregelen. Ontoegankelijkmaking van gegevens is een tijdelijke maatregel die is bedoeld om bepaalde gegevens buiten de beschikkingsmacht van de betrokkene te brengen. Tot definitieve vernietiging van ontoegankelijk gemaakte gegevens kan alleen de rechter besluiten.

Ontoegankelijk maken is dus bedoeld als een voorlopige, tijdelijke maatregel. De rechter beslist later pas over de gegevens (vernietiging of ongedaanmaking).[148]

De bevoegdheid tot het ontoegankelijk maken van gegevens is opgenomen in Titel 7.5 van Boek 2. Het kan door de officier van justitie worden bevolen aan de opsporingsambtenaar voor gegevens op een in beslag genomen geautomatiseerd werk of gegevensdrager, gegevens op een geautomatiseerd werk dat, of gegevensdrager die, is onderzocht en gegevens die werden aangetroffen tijdens een netwerkzoeking.

> **Artikel 2.7.5.1 (na onderzoek gegevensdrager)**
>
> 1. Indien bij een onderzoek aan een elektronische gegevensdrager of in een geautomatiseerd werk als bedoeld in Titel 7.4 gegevens worden aangetroffen met betrekking tot welke of met behulp waarvan het strafbare feit is begaan of die van zodanige aard zijn dat het ongecontroleerde bezit ervan in strijd is met de wet of het algemeen belang, kan de officier van justitie bevelen dat een

[147] Hierbij merkt de commissie op dat abusievelijk wordt verwezen naar artikel 126o; dat moet zijn: 125o.

[148] Dit gebeurt bij de einduitspraak als er vervolgd wordt voor de strafbare inhoud of als de officier van justitie een separate vordering tot vernietiging aan de rechtbank voorlegt. Ook kan de tijdelijke maatregel worden opgeheven wanneer er geen strafvorderlijk belang meer is bij ongedaanmaking (zie art. 2.7.5.1, vierde lid). Er bestaat echter, in het huidige conceptwetsvoorstel voor Boek 6, geen mogelijkheid tot beklag tegen de ongedaanmaking. Vgl. in dit verband ook de opmerkingen van de commissie over beklag in par. 4.3.2 onder "Beklag tegen kennisneming en gebruik".

opsporingsambtenaar die gegevens ontoegankelijk maakt voor zover dit noodzakelijk is ter beëindiging van het strafbare feit of ter voorkoming van nieuwe strafbare feiten.

Het ontoegankelijk maken van gegevens kan ook worden bevolen aan een aanbieder van een communicatiedienst[149] voor gegevens die hij opslaat of doorgeeft.

Artikel 2.7.5.2 (opgenomen in wetsvoorstel CC III)

1. In geval van verdenking van [een misdrijf als omschreven in artikel 67, eerste lid,] kan de officier van justitie aan een aanbieder van een communicatiedienst als bedoeld in [artikel 138e] het bevel richten om terstond alle maatregelen te nemen die redelijkerwijs van hem kunnen worden gevergd om bepaalde gegevens die worden opgeslagen of doorgegeven, ontoegankelijk te maken, voor zover dit noodzakelijk is ter beëindiging van een strafbaar feit of ter voorkoming van nieuwe strafbare feiten.

Als de gegevens niet langer ontoegankelijk hoeven te blijven, dan bepaalt de officier van justitie of de rechter-commissaris dat de ontoegankelijkmaking ongedaan moet worden gemaakt (nadruk toegevoegd):

Artikel 2.7.5.1

4. Zodra het belang van de strafvordering zich niet meer verzet tegen de opheffing van de ontoegankelijkmaking, bepaalt de officier van justitie dan wel de rechter-commissaris, indien deze de ontoegankelijkmaking heeft bevolen, **dat de ontoegankelijkmaking ongedaan** wordt gemaakt.

Alleen de rechter kan beslissen dat de gegevens uiteindelijk worden vernietigd (nadruk toegevoegd):

Artikel 2.7.5.3

1. Bij een afzonderlijke rechterlijke beslissing op een met redenen omklede vordering van de officier van justitie kan worden bevolen dat ontoegankelijk gemaakte gegevens **worden vernietigd** indien het gegevens betreft:

a. met betrekking tot welke of met behulp waarvan een strafbaar feit is begaan;

b. die van zodanige aard zijn dat het ongecontroleerde bezit ervan in strijd is met de wet of het algemeen belang, voor zover de vernietiging noodzakelijk is ter voorkoming van nieuwe strafbare feiten. (…)

5. Indien het gerecht de vordering afwijst, beveelt het dat de **ontoegankelijkmaking van de gegevens ongedaan** wordt gemaakt.

Is het begrip voldoende duidelijk?

De manier waarop het ontoegankelijk maken van gegevens en met name het ongedaan maken van ontoegankelijkmaking is omschreven in het conceptwetsvoorstel, komt niet goed overeen met de technische handelingen in de praktijk. In deze paragraaf onderzoeken we wat er zou gebeuren als zo'n bevel wordt gegeven.

De bevoegdheid om gegevens ontoegankelijk te maken is al langer beschikbaar, namelijk in de situatie van de doorzoeking ter vastlegging van gegevens (en eventueel de daarop volgende netwerkzoeking) en is geregeld in artikel 125o Sv. Nieuw in het conceptwetsvoorstel is de mogelijkheid om ook ontoegankelijkmaking van gegevens op een voorwerp dat in beslag is genomen te bevelen.

Wanneer een geautomatiseerd werk of gegevensdrager in beslag wordt genomen, en tijdens het onderzoek blijkt dat er bepaalde gegevens op staan waarvan de officier van justitie niet wil dat die de verdachte ter hand worden gesteld, zullen deze niet van de gegevensdrager worden

[149] Zie hierover ook par. 5.6.1.

gehaald. Het voorwerp is buiten de beschikkingsmacht van de verdachte en daarmee zijn de gegevens de facto ontoegankelijk gemaakt. Voorwaarde is wel dat het voorwerp niet verbonden wordt met het internet, omdat dan nooit uit te sluiten is dat een derde toegang heeft tot de gegevens.

De officier van justitie zal het beslag op het voorwerp laten voortduren. Pas als door de rechter het besluit tot vernietiging van de gegevensdrager of de gegevens daarop is genomen, gaat de opsporingsambtenaar over tot het zo goed mogelijk uitvoering geven aan die opdracht. Er wordt in dat geval dus geen tijdelijke maatregel getroffen, anders dan het veilig opbergen van de gegevensdrager.

Als de drager van de gegevens echter *buiten* de beschikkingsmacht van de opsporing blijft, zoals wanneer na een doorzoeking het geautomatiseerd werk achterblijft bij de verdachte of in een datacentrum, moet mogelijk wel een maatregel worden genomen waarbij een deel van de gegevens op de drager (namelijk de legale inhoud) beschikbaar blijft en een ander deel (de illegale inhoud) feitelijk ontoegankelijk wordt voor derden.

De meest voor de hand liggende en effectieve manier om ervoor te zorgen dat bepaalde gegevens of bestanden niet langer beschikbaar zijn voor kennisname door derden is om ze definitief te wissen (*wipen*). Een dergelijke wismaatregel kan niet ongedaan worden gemaakt. en is in die zin dus ook geen tijdelijke maatregel zoals de toelichting op ontoegankelijkmaking wel impliceert. Als een derde dat wel zou kunnen, waren de gegevens immers niet deugdelijk ontoegankelijk gemaakt. Een alternatief kan zijn de desbetreffende gegevens in situ te versleutelen op een dusdanige wijze dat ontsleuteling daarvan alleen (praktisch) mogelijk is met medewerking van de ontoegankelijkmakende autoriteit.

Voorafgaand aan deze handeling zal een (forensische) kopie van de gegevens worden gemaakt. Op deze manier blijven de gegevens beschikbaar voor de waarheidsvinding, kan later worden bewezen welke gegevens precies zijn gewist en kunnen de gegevens worden teruggegeven indien de rechter daartoe beslist.

Wanneer de gegevens die ontoegankelijk moeten worden gemaakt, gewoon bestanden in een map zijn, zoals Word-documenten of foto’s op een usb-stick, dan is het wissen en later retourneren van de gewiste gegevens veelal wel uitvoerbaar. Wanneer de gegevens echter zijn opgenomen zijn in een databankomgeving, dan is dat een stuk lastiger. Helemaal wanneer deze databank na het moment van veiligstellen van de gegevens door moet blijven werken en nieuwe gegevens zal gaan bevatten.

Stel bijvoorbeeld dat er onderzoek wordt gedaan naar een server waarop een internet-forum draait. Een van de berichten op dat forum bevat illegaal materiaal. Als de beheerder een betrouwbare partij is dan zal aan hem een verwijderbevel worden gericht. Maar in andere gevallen zal de opsporingsambtenaar die het bericht ontoegankelijk wil maken terwijl de rest van het forum in de lucht blijft, toegang willen krijgen tot de beheeromgeving met de juiste rechten om wijzigingen aan te brengen in deze databank. Hij kan het bericht dan veiligstellen en vervolgens verwijderen. Als de rechter later besluit dat deze actie ongedaan moet worden gemaakt, dan is het niet mogelijk exact dezelfde gegevens op de oude plek terug te zetten; de structuur van de databank zal immers inmiddels veelal zijn gewijzigd. Er kan wel een nieuw bericht met dezelfde inhoud worden gemaakt dat mogelijk ook qua plaats en vorm zo goed mogelijk lijkt op de oorspronkelijke, maar dat is iets anders dan ongedaan maken.

Er kan soms tijdens het onderzoek aan een server een reservekopie worden gemaakt van de hele databank. Die zou dan na een rechterlijke uitspraak weer kunnen worden teruggezet en werken zoals op het moment van ontoegankelijk maken. Maar die reservekopie zal dan geen wijzigingen van na die datum bevatten en voor de eigenaar waarschijnlijk niet bruikbaar zijn.

Het kan ook voorkomen dat het niet mogelijk is om bepaalde gegevens selectief te wissen van een gegevensdrager of geautomatiseerd werk. Bijvoorbeeld als de software waar de gegevens mee kunnen worden ingezien geen (permanente) wisfunctie heeft, er niet selectief

kan worden gewist (alleen een grotere hoeveelheid gegevens) of wanneer de opsporingsambtenaar niet de benodigde (technische) rechten heeft. In zo'n geval is ontoegankelijk maken geen optie en zal er toch worden aangedrongen op beslag op de drager of het wissen (of anderszins ontoegankelijk maken, zoals door versleuteling) van meer of alle gegevens. De toetsing van de proportionaliteit verdient in dergelijke gevallen bijzondere aandacht.

Wanneer de illegale gegevens in een online account of een online reservekopie staan, moet er een netwerkzoeking worden gedaan om ze te vinden. Tijdens een netwerkzoeking in een (gedeeld) account op bijvoorbeeld Google of Dropbox is de opsporingsambtenaar bij het wissen afhankelijk van de mogelijkheden die de software biedt. Vaak zijn verwijderingsacties gedurende een periode van bijvoorbeeld 30 dagen terug te draaien door de rechthebbenden. Indien mogelijk zal er dan een bevel aan de aanbieder tot ontoegankelijkmaking op grond van artikel 2.7.5.2 worden gedaan. Als de opgeslagen gegevens inzichtelijk zijn voor de aanbieder, dan kan hij daar gevolg aan geven door bijvoorbeeld een bepaalde afbeelding te verwijderen. Steeds vaker echter is de opslag versleuteld op een wijze waardoor de aanbieder er zelf ook niet meer bij kan. Dan kan er alleen worden gevorderd dat het hele account wordt gesloten. Of de opsporingsambtenaar kan proberen vanuit het account het gekoppelde e-mailadres en het wachtwoord te veranderen om de gebruiker(s) buiten te sluiten. Ook in deze gevallen verdient de toetsing van de proportionaliteit bijzondere aandacht.

Wanneer de rechter oordeelt dat gegevens definitief moeten worden vernietigd, dan speelt het probleem dat wissen van bepaalde digitale gegevens vaak complex en soms onmogelijk is. De passage in de memorie van toelichting van het conceptwetsvoorstel (p. 236 e.v.) over het vernietigen van gegevens van verschoningsgerechtigden onderstreept het belang van een realistische weergave van de manier waarop gegevens ontoegankelijk gemaakt zouden moeten worden als bedoeld in Titel 7.5. De aard van de ontoegankelijkmaking vereist dat gegevens die ontoegankelijk zijn gemaakt ook daadwerkelijk ontoegankelijk blijven. De huidige voorgestelde tekst van 2.7.5.2 vereist slechts dat een aanbieder gegevens ontoegankelijk maakt. De tekst vereist niet dat deze er zorg voor draagt of zich inspant dat de gegevens ook daadwerkelijk ontoegankelijk blijven. Hoewel dit uit de aard van de bevoegdheid afgeleid zou kunnen worden verdient het naar het oordeel van commissie de voorkeur om dit ook expliciet in de wettekst op te nemen. Dit kan eenvoudig worden bereikt door in lid 1 achter "ontoegankelijk te maken" "en te houden" in te voegen.

Aanbeveling 40: in de memorie van toelichting wordt meer geabstraheerd van de daadwerkelijk te nemen maatregelen voor ontoegankelijkmaking. Het gaat om de functie: de gegevens worden buiten de beschikkingsmacht van verdachte en derden gebracht. De officier van justitie bepaalt de wijze waarop dat gebeurt. Wanneer de gegevens moeten worden teruggegeven zal vaak niet letterlijk een "ongedaanmakings"-actie volgen, maar zullen de veiliggestelde gegevens worden geretourneerd in een vorm die zoveel mogelijk het functioneel equivalent is van de oorspronkelijke staat waarin de gegevens zich bevonden.

De tekst van artikel 2.7.5.2 wordt aangepast om duidelijk te maken dat de geadresseerde gegevens niet alleen ontoegankelijk moet *maken*, maar ook ontoegankelijk moet *houden*. → *p. 200*

Beklag en de belangen van derden

Zoals al in paragraaf 4.3.2 aangestipt, is de visie van de commissie dat de wetgever zich niet onder verwijzing naar de Wpg kan beperken tot afschaffing van elke vorm van beklag van belanghebbenden voor wat betreft gebruik en kennisneming van gegevens. Eenzelfde lacune doet zich voor ten aanzien van de ontoegankelijkmaking en de vernietiging van gegevens, nu slechts is voorzien in een appelmogelijkheid voor de belanghebbende tegen de afzonderlijke

beslissing tot vernietiging. Er staan geen andere rechtsmiddelen open, wat problematisch is in situaties waarin geen eindbeslissing wordt genomen over de ontoegankelijk gemaakte gegevens, bijvoorbeeld als de hoofdzaak niet voor de rechter komt en als de officier een separate vordering tot definitieve vernietiging van de gegevens achterwege laat. In die gevallen wordt de tijdelijke maatregel *de facto* een permanente maatregel, zonder een bewuste beslissing over het permanent worden van de ontoegankelijkmaking. De commissie verwijst in dit verband naar haar opmerkingen over het belang van beklag (par. 4.3.2), die hier mutatis mutandis ook gelden.

Een hieraan deels gerelateerd punt dat in dit verband in het bijzonder aandacht behoeft betreft de situatie dat de ontoegankelijkmaking van gegevens de belangen van derden raakt. Weliswaar bestaat in de fysieke wereld ook reeds de mogelijkheid dat beslag op een goed derden raakt, bijvoorbeeld wanneer een auto in beslag wordt genomen terwijl deze door meerdere mensen wordt gebruikt, maar verwevenheid en meerbruikbaarheid van gegevens is veel meer voorkomend en lastiger te ontwarren dat het fysieke equivalent. Het is niet mogelijk een sluitend overzicht te geven van gevallen waarin de belangen van derden door ontoegankelijkmaking onevenredig zouden worden geschaad. Wel kunnen een aantal voorbeelden worden gegeven.

Het kan bijvoorbeeld zo zijn dat een *library* als open source beschikbaar is die veelvuldig gebruikt wordt bij de bouw van malware, maar ook legitieme toepassingen heeft. Het ontoegankelijk maken (zo dit al lukt bij open-broncode) zou dan ook verdere legitieme toepassing onmogelijk maken. Ook kan worden gedacht aan een misdadiger die gestolen gegevens heeft opgeslagen (verstopt) in een databank waartoe hij onrechtmatig toegang heeft gekregen. Als deze databank door de “gehackte” derde wordt gebruikt voor bedrijfskritische bezigheden, bijvoorbeeld het bedrijven van een webwinkel, zou deze mogelijk onevenredig worden getroffen wanneer de databank langere tijd (voor hem) ontoegankelijk zou worden gemaakt. Ook minder technische voorbeelden zijn denkbaar: als een bepaalde groep een radicaliserende of haatzaaiende houding baseert op een bepaalde tekst met religieuze relevantie voor een veel grote groep mensen die de radicaliserende interpretatie van die tekst niet delen, zou het systematisch onbeschikbaar maken van dergelijke tekst derden schaden in hun legitieme bezigheden.

Steeds meer ook werken meerdere mensen samen aan gedeelde documenten; Wikipedia is een formeel georganiseerde variant daarvan, maar ook steeds meer werk wordt gedaan via gedeelde bestandverwerking, zoals etherpad of Google Docs. Het is zeker niet onvoorstelbaar dat het eenvoudigweg ontoegankelijk maken van dergelijke documenten of accounts consequenties heeft voor onbetrokken derden. Men zou bijvoorbeeld kunnen denken aan een samenwerkingsverband van onderzoekers die een zwakte in een besturingssysteem onderzoeken en hun inzichten via zo’n service met elkaar delen. Het enkele feit dat ook voor slechte doeleinden te gebruiken technische informatie wordt aangetroffen, betekent niet dat de gebruikers van die informatie misdadige intenties hebben of dat het gerechtvaardigd zou zijn hun toegang tot die gegevens te beëindigen. Daarbij moet ook worden bedacht dat door de oneindige realiseerbaarheid en (gelijktijdige) herbruikbaarheid van gegevens ook geen sprake hoeft te zijn van een rechtstreekse samenwerking tussen verdachte en derden; ook vierden en vijfden kunnen verder hebben gebouwd aan documenten die tussen verdachten en derden tot stand zijn gekomen.

Dit alles heeft tot gevolg dat de consequenties van een ontoegankelijkmaking groter kunnen zijn, en de onmiddellijke inzichtelijkheid ervan kleiner, dan bij fysiek beslag het geval is. Derhalve zou in de praktijk niet altijd op dezelfde wijze uitvoering moeten worden gegeven een ontoegankelijkmaking als aan een beslag. Een nauwkeuriger afweging is noodzakelijk opdat de belangen van niet betrokken derden beter inzichtelijk zijn en afgewogen kunnen worden.

Aanbeveling 41: een officier of de rechter-commissaris moet bij de beslissing tot (handhaving van) ontoegankelijkmaking de belangen van derden bij een ontoegankelijk expliciet en onderbouwd meenemen in deze beslissing. Een vingerwijzing daartoe zou moeten worden opgenomen in de memorie van toelichting. → *p. 200*

5.6. Vorderen van gegevens

Het conceptwetsvoorstel bevat, afgezien van de terminologie van beslag op gegevens en een aanpassing aan de wetgevingssystematiek van het wetsvoorstel, inhoudelijk grotendeels dezelfde bevoegdheden tot het vorderen van gegevens als het huidige wetboek. In het conceptwetsvoorstel wordt overigens gesproken over het bevelen tot uitlevering van gegevens; in dit rapport zullen wij de term "vorderen van gegevens" gebruiken. De commissie heeft zich in relatie tot Afdeling 7.3.3 van het conceptwetsvoorstel geconcentreerd op twee aspecten van de regeling van gegevensvordering: het onderscheid tussen vorderingen aan aanbieders van communicatiediensten en vorderingen aan anderen (par. 5.6.1), en de normering van gegevensvorderingen, zowel in het algemeen (par. 5.6.2) als in relatie tot verkeersgegevens in het bijzonder (par. 5.6.3).

5.6.1. Vorderen van gegevens in relatie tot grondwettelijk beschermde communicatie

Het conceptwetsvoorstel maakt, evenals het huidige wetboek, bij de bevoegdheden tot het vorderen van gegevens onderscheid tussen vorderingen aan aanbieders van communicatiediensten en vorderingen aan anderen. Het onderscheid is vooral van belang in verband met de bescherming van het telecommunicatiegeheim, omdat bij aanbieders opgeslagen communicatie zich in de transportfase bevindt en daarmee de inhoud van deze communicatie aanspraak kan maken op grondwettelijke bescherming onder artikel 13 Gw (vgl. ook par. 6.3.2). De manier waarop deze bescherming tot uitdrukking komt in het conceptwetsvoorstel, is volgens de commissie echter mogelijk niet toekomstbestendig vanwege het potentieel uit de pas lopen van de in Sv gehanteerde definitie van communicatieaanbieders in relatie tot de reikwijdte van artikel 13 Gw. Daarnaast kan de regeling volgens de commissie op sommige punten worden vereenvoudigd. In deze paragraaf worden op deze punten voorstellen gedaan.

Vervanging van enkele "aanbieder"-gerichte bepalingen door een algemene bepaling over het telecommunicatiegeheim

Voor een goed begrip van de term "aanbieder" in het Wetboek van Strafvordering is het van belang voor ogen te houden dat er een onderscheid bestaat tussen:

1. aanbieders van openbare telecommunicatiediensten en -netwerken in de zin van de Telecommunicatiewet (Tw);
2. aanbieders van communicatiediensten en -netwerken in de zin van het huidige artikel 126la Sv.

Ad 1: In de Tw wordt onder *openbaar* verstaan een openbare elektronische communicatiedienst die voor iedereen beschikbaar is. Ook is er sprake van een openbare elektronische communicatiedienst als die toegankelijk is voor leden van een bepaalde groep als (vrijwel) iedereen lid kan worden van die groep. Besloten diensten, zoals een bedrijfsnetwerk dat niet toegankelijk is voor anderen dan werknemers van het bedrijf, vallen buiten de definitie.[150]

[150] Een *openbaar telecommunicatienetwerk* is in de Tw gedefinieerd als: "elektronisch communicatienetwerk dat geheel of hoofdzakelijk wordt gebruikt om openbare elektronische communicatiediensten aan te bieden, waaronder mede wordt begrepen een netwerk, bestemd voor het verspreiden van programma's voor zover dit aan het publiek geschiedt" Een *openbare telecommunicatiedienst* is in de Tw gedefinieerd als: "een elektronische communicatiedienst die beschikbaar is voor het publiek". Een *elektronische communicatiedienst* is in de Tw gedefinieerd als: "een gewoonlijk tegen vergoeding aangeboden dienst die geheel of hoofdzakelijk bestaat in het overbrengen van signalen via elektronische communicatienetwerken, waaronder telecommunicatiediensten en transmissiediensten op netwerken die voor omroep worden gebruikt, doch niet de dienst waarbij met behulp van elektronische communicatienetwerken en -diensten overgebrachte inhoud wordt geleverd of redactioneel wordt gecontroleerd. Het omvat niet de diensten van de informatiemaatschappij zoals omschreven in artikel 1 van de notificatierichtlijn

Aanbieders van openbare telecommunicatiediensten en -netwerken moeten voldoen aan de voorschriften van Hoofdstuk 13 Tw en lagere regelgeving[151]. Een van de voorschriften is dat de diensten van deze categorie aanbieders aftapbaar moeten zijn voor de opsporing en inlichtingen- en veiligheidsdiensten. Daarnaast dienen zij aan strenge beveiligingsvoorschriften te voldoen, die zijn neergelegd in het Besluit bewaren gegevens telecommunicatie. Het Agentschap Telecom ziet toe op de naleving van de voorschriften uit de Tw en het Besluit.

Onder deze categorie aanbieders vallen de grote (mobiele) telefonie- en internetaanbieders. Hostingaanbieders vallen veelal niet onder deze categorie aanbieders.

Ad 2: Het huidige artikel 126la Sv[152] en het voorgestelde artikel 2.1.1.1 definiëren de aanbieder van communicatiediensten als:

> de natuurlijke persoon of rechtspersoon die in de uitoefening van een beroep of bedrijf aan de gebruikers van zijn dienst de mogelijkheid biedt te communiceren met behulp van een geautomatiseerd werk, of gegevens verwerkt of opslaat ten behoeve van een zodanige dienst of de gebruikers van die dienst (….).

De communicatiedienst hoeft niet openbaar te zijn. Deze categorie aanbieders omvat de aanbieders in de zin van de Tw, maar bijvoorbeeld ook niet-openbare bedrijfsnetwerken, communicatie faciliterende webdiensten en socialenetwerksites. Deze categorie aanbieders bevat derhalve een veel grotere groep dan de Tw-aanbieders.

Voor zover de aanbieders in deze categorie niet tevens aanbieder in de zin van de Tw zijn, geldt dat zij niet verplicht aftapbaar hoeven te zijn. Wel dienen zij in beginsel uitvoering te geven aan vorderingen van politie en justitie: als een aanbieder aftapbaar is, moet aan een tapvordering uitvoering worden gegeven en als een aanbieder gegevens heeft opgeslagen, moet aan een vordering gegevensverstrekking uitvoering worden gegeven.

In de memorie van toelichting bij het conceptwetsvoorstel wordt het begrip aanbieder beperkt tot de "natuurlijke persoon of rechtspersoon (…) die een beroep of bedrijf uitoefent waarvan de *hoofdactiviteit* bestaat uit het aan andere personen bieden van de mogelijkheid om met elkaar te communiceren met behulp van een geautomatiseerd werk."[153] Dit is beperkter dan de benadering van de grondwetgever bij de herziening van artikel 13 Gw, waarin de reikwijdte zich ook uitstrekt tot bedrijfsnetwerken en dienstaanbieders die een communicatiedienst als neven- of ondergeschikte dienst aanbieden (zie par. 6.3.2).

De vaststelling of degene aan wie wordt overwogen om een vordering te doen onder de definitie van een artikel 126la Sv-aanbieder valt, is thans en ook in het conceptwetsvoorstel bepalend voor de vraag welk vorderingsregime van toepassing is. Het vorderingsregime in Hoofdstuk 7 en de bevoegdheden in Hoofdstuk 8 van het wetsvoorstel betreffen de grotere categorie aanbieders van artikel 126la Sv en niet slechts de Tw-aanbieders. Er bestaan in Hoofdstuk 7 echter bij enkele bevoegdheden verschillen in normering indien de bevoegdheid wordt uitgeoefend ten aanzien van een 126la-aanbieder ten opzichte van de situatie waarin deze wordt uitgeoefende ten aanzien van een ander.

---

die niet geheel of hoofdzakelijk bestaan uit het overbrengen van signalen via elektronische communicatienetwerken."

[151] Onder andere Regeling Aftappen, Besluit Aftappen, Besluit bewaren gegevens telecommunicatie en andere afleverstandaarden.

[152] In wetsvoorstel CCIII worden de definities aanbieder en gebruiker van een communicatiedienst verhuisd naar de artikelen 138e en 138f Sv. De inhoud van de definitie wijzigt niet ten opzichte van 126la Sv.

[153] Memorie van toelichting, p. 99 (cursivering toegevoegd).

Dit is in de eerste plaats het geval bij gegevensvorderingen: vergelijk artikel 2.7.3.3.5 en het huidige artikel 126ng lid 2 Sv (met betrekking tot communicatie-inhoud[154] die wordt gevorderd van 126la-aanbieders), waar naast een vordering van de officier van justitie ook machtiging door de rechter-commissaris is voorgeschreven, met het algemene artikel 2.7.3.3.3 en het huidige artikel 126nd Sv, waar alleen de vordering van de officier van justitie volstaat. Daarnaast verschillen de bepalingen ook qua extra subsidiariteitseis ("dringend" belang in art. 2.7.3.3.5) en qua reikwijdte: de vordering van communicatie-inhoud gericht aan een 126la-aanbieder is slechts mogelijk voor zover klaarblijkelijk de gegevens van de verdachte afkomstig zijn, voor hem bestemd zijn of op hem betrekking hebben, of tot het begaan van het strafbare feit hebben gediend, of met betrekking tot die gegevens het strafbare feit is begaan (art. 2.7.3.3.5). (Bij de beperking tot gegevens afkomstig van of bestemd voor de verdachte neemt de commissie overigens aan dat dit ook omvat gegevens die van of naar apparaten worden gestuurd die plaatsvervangend zijn voor de verdachte, gelet op het in het conceptwetsvoorstel gehanteerde communicatiebegrip[155]. Dit zou in de toelichting verhelderd moeten worden.)

Blijkens de wetsgeschiedenis van het toekomstige artikel 13 Gw is het echter niet nodig om onderscheid te maken tussen 126la-aanbieders en andere derden die berichtenverkeer onder zich hebben. In het conceptwetsvoorstel wordt echter vanwege de inzichtelijkheid gekozen voor een afzonderlijke bepaling voor het bevel tot uitlevering van gegevens aan een aanbieder van een communicatiedienst.[156]

Dit verschil is onwenselijk, omdat de definitie van 126la-aanbieders mogelijk uit de pas loopt of kan gaan lopen met de grondwettelijke interpretatie van derde-transporteurs (zie par. 6.3.2: onder aanbieders in de zin van artikel 13 Gw "moeten dus ook degenen die berichtfuncties aanbieden als nevengeschikte dienst tot deze derden gerekend worden", wat afwijkt van de memorie van toelichting bij het conceptwetsvoorstel dat zich beperkt tot communicatiediensten als hoofdactiviteit).

Het onderscheid tussen 126la-aanbieders en overige derde-transporteurs speelt niet alleen een rol bij gegevensvordering, maar ook bij de bepalingen betreffende doorzoeking en beslag. In navolging van het huidige artikel 125la Sv bepaalt artikel 2.7.4.1.3 dat indien een onderzoek ter vastlegging van gegevens of een netwerkzoeking plaatsvindt op een geautomatiseerd werk van een aanbieder, dit alleen kan plaatsvinden als het belang van het onderzoek dit dringend vereist en met machtiging van de rechter-commissaris, en dat alleen kennis kan worden genomen van de inhoud van communicatie van of voor de verdachte of die over de verdachte of het strafbare feit gaat. Een vergelijkbare bepaling is te vinden in Afdeling 7.4.2 voor het onderzoek ter kennisneming van gegevens (zie artikel 2.7.4.2.3) opgeslagen op een bij een aanbieder inbeslaggenomen digitale-gegevensdrager of geautomatiseerd werk. Door het gebruik van de term "aanbieder" met de in de memorie van toelichting gegeven uitleg, zijn deze artikelen beperkt tot bedrijven voor wie het aanbieden van een communicatiedienst een hoofdactiviteit is. Zoals gezegd strekt het grondwettelijke telecommunicatiegeheim, in de voorgestelde grondwetswijziging, echter verder, en zou ook communicatie-inhoud die middels

[154] Voor het geval de wetgever zou besluiten (in afwijking van het commissievoorstel hieronder) dit artikel te handhaven, wijst de commissie erop dat de formulering in de tekst in het wetsvoorstel ongelukkig is gekozen. Artikel 2.7.3.3.5 spreekt van "gegevens *met betrekking tot* niet voor het publiek bestemde communicatie" (cursivering toegevoegd). Deze omschrijving wekt verwarring omdat "met betrekking tot" meer de associatie wekt met verkeersgegevens (of andere metadata) dan met inhoud van communicatie. Deze afbakening is minder scherp dan de huidige clausule "gegevens die zijn opgeslagen in het geautomatiseerde werk van de aanbieder en niet voor deze bestemd of van deze afkomstig zijn". De commissie adviseert, indien dit artikel zou worden gehandhaafd, om deze huidige clausule te gebruiken, of een scherpere omschrijving te hanteren als "gegevens bestaande uit inhoud van niet voor het publiek bedoelde communicatie".

[155] Zie noot 169 en bijbehorende tekst.

[156] Memorie van toelichting, p. 48.

doorzoeking en beslag wordt verkregen bij "nevendienst"-aanbieders op dezelfde bescherming moeten kunnen rekening als communicatie-inhoud verkregen bij "hoofddienst"-aanbieders.

Hoewel het (nog) geen geldend recht is, moet wel rekening gehouden worden met de mogelijkheid dat artikel 13 Gw wordt aangepast conform het thans in eerste lezing aangenomen wetsvoorstel. Het is ook mogelijk dat bij tweede lezing van het wetsvoorstel tot aanpassing van artikel 13 Gw nieuwe voorbeelden worden gegeven, of een verdere invulling wordt gegeven aan de reikwijdte ten aanzien van aanbieders die niet vallen onder de klassieke openbare telecomaanbieders waar artikel 13 Gw zich van oudsher op richtte of dat concreter afgrenzing van inhoud van communicatie en verkeersgegevens wordt geformuleerd. Op dit moment valt daarom niet volledig te definiëren hoever het grondwettelijke telecommunicatiegeheim precies reikt.

Nu is het mogelijk om in het gemoderniseerde Wetboek van Strafvordering een eigen keuze te maken in de reikwijdte, maar het lijkt de commissie beter om in plaats van een zelfstandige afbakening in Sv, die mogelijk uit de pas kan gaan lopen met de afbakening die in het kader van artikel 13 Gw wordt gehanteerd, rechtstreeks aan te sluiten op artikel 13 Gw zelf. Dit kan door, bijvoorbeeld in de titel met algemene bepalingen voor Hoofdstuk 7 (Titel 7.1), een algemene bepaling op te nemen die de normering van het onderzoek van communicatie-gerelateerde gegevens koppelt aan het grondwettelijke telecommunicatiegeheim, zonder op voorhand vast te leggen hoever dat telecommunicatiegeheim precies strekt.

Conceptueel is dit de eenvoudigste en meest toekomstbestendige benadering. Strafvordering volgt hiermee de Grondwet, en laat het aan de rechtspraktijk over om de reikwijdte van artikel 13 Gw te bepalen (en waar relevant in de toekomst te laten mee-ontwikkelen met technische ontwikkelingen). Praktisch gezien lost dit niet alle afbakeningsproblemen op: er zal de nodige rechtsonzekerheid blijven welke communicatie precies onder de bescherming van artikel 13 Gw valt; de grondwetgever laat dat aan de lagere rechtsontwikkeling over, en het zal een tijd duren voordat rechters piketpalen hebben geslagen om de reikwijdte van artikel 13 Gw af te bakenen voor nieuwe(re) technologieën en diensten. Dit is echter onvermijdelijk voor een wetboek dat beoogt voor langere tijd houdbaar te zijn: gezien de voortdurende ontwikkelingen in het communicatielandschap, niet alleen in technologisch opzicht maar ook qua markt en bedrijfsmodellen, is het niet mogelijk om op enig moment een precieze afbakening te geven van wat onder grondwettelijk beschermde telecommunicatie valt; gehanteerde begrippen moeten een aanzienlijke mate van abstractie hebben, die het toelaat om de begrippen dynamisch te interpreteren aan de hand van de beschikbare interpretatiemethoden (waaronder de grammaticale, historische en teleologische). In dat licht zal het helpen als in de memorie van toelichting enig houvast wordt geboden door voorbeelden te geven van wat in ieder geval onder het telecommunicatiegeheim valt, en door te verwijzen naar relevante passages uit het wetsvoorstel ter herziening van artikel 13 Gw.

Aanbeveling 42: de artikelen 2.7.3.3.5, 2.7.4.1.3 en 2.7.4.2.3 worden geïntegreerd in één algemene bepaling (bijvoorbeeld in Titel 7.1): "Indien de uitoefening van een bevoegdheid als genoemd in Titel 7.3 of Titel 7.4 betrekking heeft op gegevens die beschermd worden door het telecommunicatiegeheim als bedoeld in artikel 13 Grondwet, kan het onderzoek alleen plaatsvinden indien het belang van het onderzoek dit dringend vereist en na een daartoe verleende machtiging van de rechter-commissaris. Het onderzoek kan alleen betrekking hebben op a. gegevens die van de verdachte afkomstig zijn, voor hem bestemd zijn of op hem betrekking hebben, of tot het begaan van het strafbare feit hebben gediend; of b. gegevens met betrekking tot welke het strafbare feit is begaan." (Hierbij dient in de toelichting te worden verhelderd dat de beperking onder a. (gegevens afkomstig van of bestemd voor de verdachte) ook omvat gegevens die van of naar apparaten worden gestuurd die plaatsvervangend zijn voor de verdachte.) → *p. 200*

Overige "aanbieder"-gerichte bepalingen

De vraag ligt vervolgens voor of er specifieke bepalingen zijn waarin het begrip aanbieder in de zin van 126la-aanbieders wel gehandhaafd zou moeten worden. Het begrip "aanbieder" komt in Hoofdstuk 7 naast de reeds genoemde bepalingen voor in de volgende artikelen.

- Artikel 2.7.3.3.2 lid 2: een bevel zo spoedig mogelijk gegevens te verschaffen over andere aanbieders die bij de communicatie betrokken waren, in het kader van de bevoegdheden vluchtige gegevens te laten bevriezen (thans artikel 126ni Sv). Hoewel de bevriezingsbevoegdheid een algemeen karakter heeft en (dus) evenzeer aanbieders als anderen betreft, is het nuttig deze bepaling te handhaven omdat het een specifieke implementatie betreft van een bepaling uit het Cybercrime-verdrag (artikel 17 lid 1 onder b).
- Artikel 2.7.3.3.4 lid 1: dit bepaalt dat een gegevensvordering (art. 2.7.3.3.3) alleen kan worden gericht aan een aanbieder van een communicatiedienst als het (kort gezegd) geen communicatie-inhoud betreft, waarvoor de specialis van artikel 2.7.3.3.5 bestemd is. Nu de commissie aanbeveelt artikel 2.7.3.3.5 te laten vervallen ten faveure van een algemene bepaling, heeft artikel 2.7.3.3.4 lid 1 geen functie meer: er is geen specifieke regeling nodig voor bevelen aan aanbieders van communicatiediensten als zodanig. Het bevel van artikel 2.7.3.3.3 kan gewoon worden gericht aan aanbieders (en andere derden), waarbij de voorgestelde algemene bepaling betreffende het telecommunicatiegeheim aanvullende eisen stelt indien de vordering gegevens betreft die onder artikel 13 Gw vallen.
- Artikel 2.7.3.3.4 lid 2 van dit artikel bevat een bevoegdheid voor de opsporingsambtenaar om nummer en soort dienst te vorderen. Aangezien dit samenhangt met de overeenkomstige bepaling in artikel 2.7.3.3.3 lid 3, waar artikel 2.7.3.3.4 lid 2 ook naar verwijst, kan deze bepaling worden geïntegreerd in artikel 2.7.3.3.3 lid 3 door toevoeging aldaar van "het nummer en de soort dienst van een gebruiker van een communicatiedienst" onder een nieuwe letter f.
- Artikel 2.7.3.3.4 lid 3 bevat een bevoegdheid om van een communicatieaanbieder te vorderen dat deze door bestandsvergelijking een nummer of andere gebruikersgegevens achterhaalt. Deze mogelijkheid tot bestandsanalyse moet blijven bestaan.[157]
- Artikel 2.7.3.3.6 lid 4: dit betreft een bevel tot uitlevering van toekomstige gegevens (thans artikel 126ne Sv). Voor het vorderen van gegevens wordt in het algemeen de periode gesteld op één maand, terwijl voor een vordering gericht aan een aanbieder de periode op drie maanden wordt gesteld. Hoewel dit onderscheid op het eerste oog inconsistent kan lijken, is het verklaarbaar vanwege het feit dat de bevoegdheid om te tappen naar een periode van maximaal drie maanden wordt opgetrokken, en het ligt dan voor de hand om dat ook voor verkeersgegevens te doen (ook omdat deze veelal gelijktijdig met vastgelegde communicatie worden meegeleverd). Voor aanbieders van communicatiediensten is de langere termijn daarom logisch. Dat geldt echter niet voor alle overige derden van wie gegevens (niet beperkt tot verkeersgegevens, maar alle mogelijke gegevens) worden gevorderd; voor hen is er geen reden de huidige termijn van artikel 126ne Sv op te trekken naar drie maanden. Hier moet het onderscheid dus ook worden gehandhaafd.

Samenvattend stelt de commissie voor dat het onderscheid tussen 126la-aanbieders en niet-126la-aanbieders in veel gevallen kan worden vervangen door een algemene bepaling die verwijst naar het telecommunicatiegeheim, maar dat voor de bestandsanalyse, de onverwijlde gedeeltelijke verstrekking van verkeersgegevens en de vordering van toekomstige gegevens,

[157] In par. 7.1 wordt het voorstel besproken om een nieuwe bevoegdheid in te voeren waarbij van derden een analyse kan worden gevorderd. Daar lijkt deze bevoegdheid bij te passen. Afhankelijk van de formulering van dit nieuw te vormen artikel moeten worden gekeken of voor het vorderen van de bestandsanalyse bij een aanbieder een aparte formulering noodzakelijk blijft, die aansluit bij de specifieke bepaling daarover in de Telecommunicatiewet.

specifieke bepalingen wenselijk blijven voor 126la-aanbieders. In deze bepalingen kan de term aanbieder van een communicatiedienst daarbij worden gehandhaafd met de invulling zoals die in de toelichting is gegeven, namelijk dat de communicatiedienst een hoofdactiviteit is. Deze bepaling zijn immers specifiek gericht op wat van oudsher de klassieke telecommunicatieaanbieders zijn en omvatten daarmee de voor deze bepalingen noodzakelijke (mobiele)telefonie- en internetaanbieders.

Aanbeveling 43: artikel 2.7.3.3.4 lid 1 kan komen te vervallen, terwijl lid 2 kan worden geïntegreerd in artikel 2.7.3.3.3 lid 3. De bepalingen betreffende bestandsanalyse, de onverwijlde gedeeltelijke verstrekking van verkeersgegevens en de vordering toekomstige gegevens kunnen worden gehandhaafd, inclusief de toelichting dat dit ziet op aanbieders voor wie de communicatiedienst een hoofdactiviteit is. → *p. 200*

Het begrip "aanbieder" komt tevens voor in artikel 2.7.5.2. Dit betreft het nieuw in te voeren artikel 125p Sv uit het wetsvoorstel CC III en betreft het vorderen aan een aanbieder gegevens ontoegankelijk te maken (thans gebaseerd op art 54a Sr). Nu het wetsvoorstel CC III thans nog voorligt in de Eerste Kamer, acht de commissie het onwenselijk op dit specifieke punt advies uit te brengen. Wel adviseert de commissie de wetgever om te beoordelen of deze bevoegdheid beperkt dient te blijven tot deze categorie aanbieders. Het is de vraag of onder de in artikel 138e omschreven aanbieders wel alle hosting-aanbieders vallen (inclusief hosting-aanbieders voor wie het aanbieden van een communicatiedienst niet een hoofdactiviteit is). Zo niet, dan heeft artikel 125p Sv mogelijk een beperktere reikwijdte dan artikel 54 Sr zoals aangepast in het wetsvoorstel CC III (dat immers ziet op een "tussenpersoon die een communicatiedienst verleent bestaande in de doorgifte of opslag van gegevens die van een ander afkomstig zijn", wat wel duidelijk hosting-aanbieders omvat).

Aanbeveling 44: de wetgever moet beoordelen of de categorie aanbieders als bedoeld in artikel 2.7.5.2 voldoende aansluit op de categorieën tussenpersonen in artikel 54 Sr, en waar nodig deze bepalingen beter op elkaar afstemmen. → *p. 200*

5.6.2. Normering van het vorderen van gegevens in het algemeen

De huidige regeling van het vorderen van gegevens bevat een driedeling: identificerende gegevens kunnen worden gevorderd door een opsporingsambtenaar, "gewone" gegevens op bevel van de officier van justitie, en bijzondere categorieën (zogenoemde "gevoelige") gegevens met machtiging van de rechter-commissaris. Het conceptwetsvoorstel hanteert een vergelijkbare driedeling samenhangend met de aard van de gevorderde gegevens, maar koppelt de vordering van "gevoelige" gegevens niet langer aan een machtiging van de rechter-commissaris; wel geldt een zwaarder verdenkingscriterium (tweejaarsmisdrijven in plaats van eenjaarsmisdrijven) en een aanvullende subsidiariteitseis (dringendheid) (zie art. 2.7.3.3.3).

Vanuit systematische overwegingen stelt de commissie voor om in plaats van de in artikel 2.7.3.3.3 gehanteerde driedeling de meer abstracte driedeling van het algemene normeringscriterium te hanteren, en bij vorderingen van gegevens waarbij sprake is van ingrijpende stelselmatigheid een machtiging van de rechter-commissaris te vereisen, in lijn met de voorgestelde invulling van het algemene normeringscriterium (zie par. 4.2.3). Dit verhoogt de onderlinge consistentie van de regeling van opsporingsbevoegdheden ten aanzien van digitale gegevens. Qua verstrekkendheid kan het vorderen van gegevens immers vergelijkbaar zijn met het onderzoek van gegevens in of overgenomen uit een geautomatiseerd werk: de ingrijpendheid hangt vooral af van hoeveel en welke gegevens een opsporingsinstantie uit welke bron vordert respectievelijk zoekt of vastlegt. De commissie wijst op een mogelijk gebrek aan consistentie indien verschillende vormen van normering van toepassing zijn op een doorzoeking ter onderzoek van

digitale gegevens bij een derde enerzijds en op de vordering van gegevens aan die derde anderzijds – in beide situaties kunnen immers exact dezelfde gegevens in beeld komen. Weliswaar zullen bij doorzoeking eerder volledige gegevensdragers in beslag worden genomen dan wel images worden gemaakt van gegevensdragers, terwijl vorderingen meer gericht zijn op bepaalde gegevens, maar de wet staat er niet aan in de weg om grote datasets te vorderen (waaronder integrale datasets indien dit proportioneel is in situaties waarin de gevorderde vanwege de inrichting van zijn systemen niet in staat is bepaalde selecties te maken; vgl. par. 7.1), vergelijkbaar met het integraal overnemen van gegevens uit een geautomatiseerd werk of digitale-gegevensdrager.

Een ander voordeel van het algemene normeringscriterium ten opzichte van de categorische aanduiding van bepaalde soorten gegevens in artikel 2.7.3.3.3 is dat de mate van inbreuk op de persoonlijke levenssfeer bij gevorderde gegevens niet *alleen* afhangt van de aard van de gegevens, maar ook van de hoeveelheid, de context en de wijze waarop de gegevens worden onderzocht en gebruikt. Om die reden kan het derde deel van de driedeling – de meest ingrijpende vorm – niet vereenzelvigd worden met "gevoelige" gegevens als zodanig, maar moet eerder worden gekeken naar het totale beeld dat redelijkerwijs voorzienbaar ontstaat van iemands privéleven bij uitoefening van een bevoegdheid (zie par. 4.2.2). Zo levert het vorderen van enkele "gevoelige" gegevens om een alibi te verifiëren – bijvoorbeeld de lijst met aanwezigen op de bijeenkomst van het bijbelleesclubje, of de notulen van de bewonersverenigingsvergadering waarin staat dat mevrouw Lindemans niet aanwezig was omdat zij haar been heeft gebroken – niet per se een ingrijpende inbreuk op iemands privéleven op. De commissie acht de contextspecifieke, meer integrale beoordeling van het beeld van iemands privéleven daarom een adequatere maatstaf dan de kale maatstaf of het wel of niet om "gevoelige" gegevens gaat. Dat is ook meer in lijn met de regeling van onderzoek van gegevens in of overgenomen uit geautomatiseerde werken of digitale-gegevensdragers, waarbij geen specifieke wettelijke eis wordt gesteld voor het onderzoek naar "gevoelige" gegevens; ook in dit opzicht acht de commissie het relevant om de onderlinge consistentie van de regeling van de verschillende vormen van gegevensonderzoek (beslag, doorzoeking en vordering, zie par. 5.2.3) voor ogen te houden.

Sommigen in de commissie hebben twijfels geuit over het op gegevensvorderingen van toepassing verklaren van het derde deel van het normeringscriterium – ingrijpende stelselmatigheid gekoppeld aan een machtiging van de rechter-commissaris – vanwege de moeilijke bepaalbaarheid van dit criterium en mogelijk daarmee gepaard gaande uitvoeringsproblemen (zie ook par. 6.2, p. 136). Niettemin acht de commissie het wenselijk het algemene normeringscriterium wel toe te passen op de bevoegdheid gegevens te vorderen. De reden daarvoor is, als gezegd, deels gelegen in systematische overwegingen – het verhoogt de onderlinge consistentie en daarmee de systematiek van de regeling van opsporingsbevoegdheden. Deels is de reden echter ook inhoudelijk: er zijn situaties waarin het vorderen van gegevens een dermate ingrijpende inbreuk op iemands persoonlijke levenssfeer oplevert, omdat een ingrijpend beeld van zijn privéleven wordt blootgelegd, dat het redelijk is dit alleen toe te staan als een rechter-commissaris daartoe heeft gemachtigd. Dat betreft – evenals bij onderzoek van gegevens in of overgenomen uit geautomatiseerde werken en digitale-gegevensdragers – alleen uitzonderlijke gevallen; het inschakelen van de rechter-commissaris zal geen automatisme moeten (of kunnen) worden, maar alleen aangewezen zijn indien redelijkerwijs voorzienbaar een ingrijpend beeld van iemands privéleven ontstaat. Dat zal bij gegevensvorderingen vrijwel alleen in de diepe variant aan de orde zal zijn (bijvoorbeeld wanneer gegevens van een internetpornodienstaanbieder worden gevorderd om te beoordelen of iemand pedoseksuele interesse heeft), en alleen in hoogst uitzonderlijke gevallen in de brede variant (zie par. 4.2.2 over diep en breed). Dat laatst zou het geval kunnen zijn als een grote hoeveelheid gegevens van een mega-

databezitter worden gevorderd, waardoor een relatief scherp zicht kan worden verkregen op uiteenlopende aspecten van iemands privéleven.

Voor wat betreft het eerste gedeelte van het algemene normeringscriterium – de vraag of er sprake is van stelselmatigheid – stelt de commissie dat de huidige beperking voor opsporingsambtenaren om (zonder bevel van de officier van justitie) alleen identificerende gegevens te kunnen vorderen, redelijk is. Voor andere vorderingen is een bevel van de officier van justitie vereist, mede in verband met het feit dat enige inspanning wordt gevraagd van een derde (die bij identificerende gegevens per definitie gering is maar bij andere gegevens niet per se gering hoeft te zijn).

Aanbeveling 45: op de bevoegdheid tot het vorderen van gegevens wordt het algemene normeringscriterium van toepassing verklaard. De toelichting kan daarbij aangeven dat er slechts in uitzonderlijke gevallen sprake zal zijn van ingrijpende stelselmatigheid, grotendeels beperkt tot de "diepe" variant. → *p. 201*

5.6.3. Normering van de bevoegdheid tot het vorderen van verkeersgegevens

Terminologie: verkeersgegevens en metadata

Het Besluit vorderen gegevens telecommunicatie geeft in artikel 2 een opsomming van "verkeersgegevens", de gegevens die op grond van het huidige Wetboek van Strafvordering zijn aan te merken als gegevens over een gebruiker van een communicatiedienst en het communicatieverkeer met betrekking tot die gebruiker, als bedoeld in artikel 126n, eerste lid, tweede volzin, artikel 126u, eerste lid, tweede volzin, en artikel 126zh, eerste lid, tweede volzin, Sv, die op grond van die artikelen kunnen worden opgevraagd. Het betreft de gegevens waarvoor voorheen de Wet bewaarplicht telecommunicatiegegevens gold.

Ook het conceptwetsvoorstel benoemt in de memorie van toelichting "verkeersgegevens" die in artikel 2.8.2.7.1 lid 5 nader worden omschreven als *de bij algemene maatregel van bestuur aangewezen gegevens over de gebruiker* (het nummer of een andere aanduiding waarmee de individuele gebruiker van de communicatiedienst wordt geïdentificeerd of de naam en, voor zover bekend, het adres van de gebruiker) *en over het communicatieverkeer van die gebruiker* gedurende de periode waarin uitvoering wordt gegeven aan het bevel. Blijkens de memorie van toelichting (p. 255-256) is met het wetsvoorstel bedoeld aan te sluiten bij het huidige stelsel.

Verkeersgegevens in deze beperkte zin (namelijk de specifiek in het Besluit vorderen gegevens telecommunicatie aangewezen gegevens) vormen een deelverzameling van verkeersgegevens in brede zin (alle gegevens betreffende elektronische communicatie, met uitzondering van de inhoud van die communicatie[158]). Deze laatste, brede, zin is die waarin veelal over verkeersgegevens wordt gesproken, in de literatuur alsook in beleid. Daarbij wordt niet altijd scherp voor ogen gehouden dat het vorderen van verkeersgegevens als bedoeld in het Wetboek van Strafvordering beperkt is tot verkeersgegevens in enge zin, en een aantal van de in de literatuur of het debat vaak genoemde gegevens, zoals URL's, daar niet onder vallen.

Om verwarring te voorkomen, wordt in dit rapport verder de term "verkeersgegevens" gebruikt in de enge zin (dus de bij AMvB aangewezen gegevens) en de verwante (maar bredere) term "metadata" voor verkeersgegevens in brede zin.[159]

[158] De definitie van verkeersgegevens (in deze brede zin) vergt een conceptuele afbakening ten opzichte van de inhoud van communicatie. Voor een consistent uitgewerkte en onderbouwde definitie van het begrip verkeersgegevens, zie Fischer 2010.

[159] De term "metadata" betekent "gegevens over gegevens" en is feitelijk een breder begrip dan verkeersgegevens in ruime zin. In deze paragraaf wordt de term echter gebruikt in de zin van gegevens over elektronische communicatie.

De normering van vorderingen van metadata en verkeersgegevens

Van oudsher worden metadata minder beschermd dan communicatie-inhoud. Historisch is dat verklaarbaar omdat de gegevens op een envelop (meestal) minder zeggen over iemands privéleven dan de inhoud van de brief in de envelop, en het feit dat mevrouw A met mijnheer B belt (meestal) minder zegt over hun privéleven dan wat ze met elkaar bespreken. Met de ontwikkeling in telecommunicatiemiddelen en -mogelijkheden is echter het informatiegehalte van metadata gaandeweg groter geworden. Ten eerste is de hoeveelheid metadata enorm veel groter dan de gegevens over briefverkeer of telefoongesprekken in de 20e eeuw. Waar mensen vroeger hooguit een tiental berichten op een dag met enkele personen uitwisselden, gaan er nu regelmatig tientallen berichten per uur heen en weer met veel verschillende communicatiepartners. Ten tweede zijn er meer typen metadata bijgekomen: niet alleen gegevens over ontvanger, verzender, tijdstip en de (vaste) plaats van ontvanger of verzender, maar ook mobiele locatiegegevens, gegevens over typen berichten die worden uitgewisseld (bijvoorbeeld aan de hand van het gebruikte protocol of Internetpoorten),[160] en metadata die momenteel niet onder verkeersgegevens vallen zoals gegevens over Internetgebruik (bijvoorbeeld bezochte URL's). Ten derde komt er informatie bij over communicatie die apparaten zelf genereren. Ten vierde, en als belangrijkste, de mogelijkheden zijn sterk toegenomen om uit deze grote hoeveelheid beschikbare metadata patronen te herkennen en nieuwe informatie af te leiden, die meer zegt dan alleen met wie iemand hoe vaak communiceert.

Ton Siedsma (werkzaam bij Bits of Freedom) voerde in 2013 een experiment uit om een week lang al zijn metadata (dus ruimer dan de categorie "verkeersgegevens" uit Sv) van zijn bel-, mail- en browseverkeer te laten verzamelen en die vervolgens door onderzoekers te laten analyseren. Een artikel in *de Correspondent* gaf op basis daarvan een profiel van hem, dat opmerkelijk gedetailleerd is: zijn leeftijd, dat hij pas is afgestudeerd, zijn dagritme, wie zijn vriendin en zus is, zijn interessesferen, dat hij vermoedelijk christelijk is, zijn (voorgenomen) aankopen, dat hij veel weet van technologie en burgerrechten, wat hij voor werk doet en waar hij zich binnen zijn baan mee bezig houdt, en dat hij in de avonduren vaak doorwerkt, wie er in twee verschillende vriendengroepen zitten en met wie hij beroepsmatig veel contact heeft.[161] Dit was in 2013. Anno 2018 zal de hoeveelheid communicatie zeker niet afgenomen zijn, en zijn de mogelijkheden om informatie uit metadata af te leiden zeker niet minder geworden. In 2024 zullen de mogelijkheden om informatie uit metadata af te leiden naar verwachting nog ruimer zijn, en in de daaropvolgende jaren naar verwachting mogelijk nog verder toenemen.

Gezien deze ontwikkelingen is in de wetenschap in de afgelopen vijftien jaar[162] het onderscheid in privacygevoeligheid tussen inhoud en metadata steeds meer ter discussie gesteld. De overheersende mening in de wetenschap is dat het onderscheid achterhaald is, en dat het vergaren van metadata qua privacyinbreuk niet *intrinsiek* minder ingrijpend is dan het vergaren van communicatie-inhoud, en dat zeker in de Internetcontext regelmatig evenveel of zelfs meer uit metadata valt af te leiden dan uit inhoud.[163]

---

[160] Het TCP/IP-protocol werkt met verschillende Internetpoorten, die samenhangen met bepaalde applicaties. Sommige applicaties zijn specifiek en hangen samen met inhoud, zoals poortnummer 4242 voor medische bestanden, of poort 9212 voor het Financial Information eXchange protocol. Zie Koops & Smits 2014, p. 42-43.

[161] Dimitri Tokmetzis, 'Hoe je onschuldige smartphone bijna je hele leven doorgeeft aan de geheime dienst', *de Correspondent* 20 december 2013.

[162] Zie reeds Asscher en Ekker 2003, p. 104: "Zowel in de discussie over de technische aspecten van verkeersgegevens als in de juridische debatten worden vraagtekens geplaatst bij de wénselijkheid om nog onderscheid te maken tussen de inhoud van communicatie en de verkeersgegevens" en Hes 2003, p. 18: "Ook zou de dynamiek in de technologie kunnen leiden tot een continue herdefinitie van de scheidslijn tussen inhoud en verkeersgegevens en derhalve aan voortdurend 'achterlopende' wetgeving."

[163] Zie bijvoorbeeld Koops & Smits 2014, p. 133 (de term "verkeersgegevens" gebruikend in de ruime zin van metadata: "wanneer men alle verkeersgegevens heeft behorend bij iemands Internetgebruik over een periode van

In wetgeving en beleid wordt daarentegen nog steeds een normatief onderscheid gemaakt tussen inhoud en verkeersgegevens in enge zin.[164] Dat is begrijpelijk, omdat het wettelijke begrip van verkeersgegevens beperkter is dan de categorieën metadata die in het debat veelal als voorbeeld worden gebruikt, en uit de bij AMvB momenteel aangewezen categorieën verkeersgegevens een minder scherp beeld opleveren van iemands privéleven dan bij de ruimere categorie metadata het geval is.

Het conceptwetsvoorstel zelf verwijst echter niet specifiek meer naar het Besluit, maar regelt via artikel 2.7.3.3.11 de mogelijkheid bij AMvB nadere regels te stellen, waaronder blijkens de memorie van toelichting (p. 201) het Besluit vorderen gegevens telecommunicatie valt. Hierop zou volgens de commissie in de memorie van toelichting nader moeten worden ingegaan. Het valt immers niet te voorzien hoe de AMvB er over tien of twintig jaar uitziet; de AMvB zou in de toekomst uitgebreid kunnen worden met andere typen metadata dan de huidige verkeersgegevens. In dat geval is het mogelijk dat uit deze gegevens alsdan wel een scherper, en mogelijk ingrijpend, beeld van iemands privéleven afgeleid zou kunnen worden.

Voor een wetboek dat bedoeld is toekomstbestendig te zijn, rijst de vraag of het normatieve onderscheid tussen inhoud en verkeersgegevens op langere termijn te handhaven is als een principieel, systematisch onderscheid. Weliswaar wordt het begrip "verkeersgegevens" momenteel in beperkte zin gebruikt, maar de mogelijkheid bestaat dat in de toekomst meer typen metadata als "verkeersgegevens" worden aangewezen, waardoor het begrip "verkeersgegevens in enge zin" dichter in de buurt zou komen bij het begrip "verkeersgegevens in brede zin", oftewel metadata. Bovendien is denkbaar dat de huidige typen verkeersgegevens in de toekomst een scherper beeld van iemands privéleven gaan opleveren, als communicatiepatronen nog verder intensiveren. Levert in dat licht het vastleggen en kennisnemen van de inhoud van communicatie intrinsiek, dus per definitie, een grotere inbreuk op dan het vorderen van verkeersgegevens, en als men vindt dat dat nog steeds het geval is, is dit dan ook nog het geval in 2030?

In lijn met de algemene constatering dat traditionele scheidslijnen vervagen en dat een duurzame regeling moet werken met meer algemene criteria die flexibel kunnen worden ingevuld, stelt de commissie dat, in elk geval voor de middellange termijn, geen principieel onderscheid kan worden volgehouden tussen inhoud en verkeersgegevens dan wel metadata. In sommige gevallen zal het tappen van communicatie maar een beperkt beeld van iemands privéleven

een paar uur 'is het vrij gemakkelijk geworden de inhoud van al die verschillende (internet) activiteiten te duiden, zonder daadwerkelijk de inhoud te kennen'") en p. 138 ("Wanneer alles over Internet gaat, in complexe en uitwisselbare patronen, is de consequentie ook dat alles wat met telecommunicatie te maken heeft – vanuit de in Hoofdstuk 5 geschetste argumentatie – inhoud wordt. Misschien zouden we dan ook moeten constateren dat het begrip 'verkeersgegevens' zijn langste tijd gehad heeft. (…) Verkeersgegevens zijn dermate verknoopt met communicatiepatronen, dat het vaak mogelijk is dat kennis van de verkeersgegevens gepaard gaat met kennis van de strekking van wat er wordt gecommuniceerd. (…) Vanuit de hiervoor genoemde redenering dat verkeersgegevens behorend bij Internet als inhoud moeten worden beschermd, is dan de conclusie dat verkeersgegevens en inhoud altijd samenvallen vanuit de ratio van het correspondentiegeheim"). Vgl. ook General Counsel voor de NSA, Stewart Baker: "metadata absolutely tells you everything about somebody's life. If you have enough metadata, you don't really need content", geciteerd in Wisman 2015, p. 83, die zelf ook constateert: "the separation of metadata and content data is increasingly irrelevant", evenals Felten 2013, p. 1: "It is no longer safe to assume that this "summary" or "non-content" information is less revealing or less sensitive than the content it describes."

Zie ook memorie van toelichting bij Boek 2, p. 255: "Het vastleggen van telecommunicatie levert de opsporing *slechts* de inhoud van de communicatie op. Met behulp van de verkeersgegevens kan de opsporing de communicatie beter duiden" (cursivering toegevoegd).

[164] Er zijn wel rechterlijke uitspraken die de toegenomen privacygevoeligheid van verkeersgegevens erkennen, zie bijvoorbeeld EHJ 8 april 2014, C‑293/12 and C‑594/12 (*Digital Rights Ireland*), §27: "Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them."

opleveren (bijvoorbeeld als iemand een bepaalde telefoon beperkt en slechts voor één bepaald, zakelijk doel gebruikt); in andere gevallen zal uit gevorderde verkeersgegevens dan wel metadata een tamelijk scherp en mogelijk ook breed beeld van iemands privéleven af te leiden zijn (bijvoorbeeld als de gegevens al het telefoon- en internetverkeer van een intensieve sociale media-gebruiker gedurende drie maanden betreffen). Het valt daarom op middellange termijn moeilijk vol te houden dat voor het vastleggen van inhoud van communicatie (ook die niet onder het telecommunicatiegeheim valt) intrinsiek wel een rechterlijke machtiging nodig is en voor het vorderen van verkeersgegevens intrinsiek niet. Het zal van de omstandigheden van het geval (zoals duur, type apparaat waarmee wordt gecommuniceerd, intensiteit van communicatiegedrag) afhangen hoe ingrijpend de inbreuk op het privéleven feitelijk is.

Volgens de commissie moet daarom niet alleen de normering van het vastleggen van communicatie-inhoud flexibeler worden door, als hierboven aangegeven, het algemene normeringscriterium te hanteren (zie par. 6.3.4); ook op het vorderen van verkeersgegevens en overige metadata zou dat criterium van toepassing moeten zijn.

Voor de vormgeving van bevoegdheden betekent dit het volgende. De commissie heeft hiervoor geadviseerd om het onderscheid tussen vorderingen aan aanbieders en vorderingen aan andere derden in zijn algemeenheid (met enkele specifieke uitzonderingen) te laten vervallen (par. 5.6.1). Het vorderen van verkeersgegevens en overige metadata – evenals overige gegevens die niet onder het telecommunicatiegeheim vallen – valt dus onder het algemene vorderingsregime. Dit kan plaatsvinden door een opsporingsambtenaar waar het bepaalde identificerende data betreft (artikel 2.7.3.3.3 lid 3 met daarin ingevoegd artikel 2.7.3.3.4 lid 2) en door de officier van justitie in geval van stelselmatigheid,[165] met machtiging van de rechter-commissaris in geval van ingrijpende stelselmatigheid. De precieze grens zal daarbij, zoals steeds bij het algemene normeringscriterium, in richtlijnen en rechtspraak nader moeten worden geduid en kan mee-evolueren met techno-sociale ontwikkelingen in het communicatiegebruik.

Daarbij stelt de commissie wel voor om toe te lichten dat de huidige categorie verkeersgegevens – dus de gegevens aangewezen in het Besluit vorderen gegevens telecommunicatie – niet onder ingrijpende stelselmatigheid vallen, en dus door de officier van justitie kunnen worden gevorderd, gelet op de relatief beperkte categorieën verkeersgegevens die hier momenteel zijn aangewezen. De toelichting zou daarbij wel duidelijk moeten maken dat, bij eventuele toekomstige uitbreiding van de AMvB, bezien moet worden of het nog steeds gerechtvaardigd is dat voor vordering van deze verkeersgegevens per definitie geen rechterlijke machtiging nodig is.

Aanbeveling 46: het vorderen van metadata wordt, vallend onder de algemene bevoegdheid gegevens te vorderen, verbonden aan het algemene normeringscriterium. Daarbij wordt toegelicht dat de bij AMvB aangewezen verkeersgegevens (het Besluit vorderen gegevens telecommunicatie) niet onder ingrijpende stelselmatigheid vallen (tenzij in de toekomst het Besluit zou worden uitgebreid met andere typen metadata, in welk geval de kwalificatie van ingrijpendheid moet worden herbeoordeeld). → *p. 201*

[165] In dit geval wordt het eerste deel van het algemene normeringscriterium – de geringe inbreuk – op wetgevingsniveau al specifiek ingevuld door bepaalde categorieën gegevens aan te wijzen. Het is op zich mogelijk om dit te veralgemeniseren, in lijn met het algemene normeringscriterium, maar bij het vorderen van gegevens speelt mee dat er ook een bepaalde inspanning wordt verwacht van de gevorderde om de gegevens te leveren, wat een reden is om de vordering van andere dan de identificerende gegevens aan de officier van justitie toe te delen.

6. Heimelijke bevoegdheden

In Hoofdstuk 8 van het conceptwetsvoorstel zijn – naast enkele nieuwe bevoegdheden – de huidige bijzondere opsporingsbevoegdheden opgenomen. Dit zijn bevoegdheden die in beginsel heimelijk worden uitgeoefend, dat wil zeggen zonder dat de betrokkene daar weet van heeft. In dit hoofdstuk van het rapport wordt allereerst aandacht besteed aan de naamgeving van Hoofdstuk 8 (par. 6.1), waarna de normering van de heimelijke bevoegdheden in het algemeen aan de orde komt (par. 6.2). De commissie heeft zich in het licht van haar opdracht geconcentreerd op de bevoegdheden ten aanzien van communicatie (vastleggen van telecommunicatie en van vertrouwelijke communicatie, par. 6.3) en de twee nieuw voorgestelde bevoegdheden van het overnemen van persoonsgegevens uit publiek toegankelijke bronnen (par. 6.4) en stelselmatige locatiebepaling (par. 6.5). Tot slot worden aanbevelingen gedaan ten aanzien van de regeling van technische hulpmiddelen die bij de uitoefening van heimelijke bevoegdheden kunnen worden ingezet (par. 6.6).

6.1. Terminologie

De titel van Hoofdstuk 8 luidt "Heimelijke bevoegdheden". De term "heimelijke bevoegdheden" vervangt de huidige term "bijzondere opsporingsbevoegdheden". De memorie van toelichting bij het conceptwetsvoorstel (p. 9 en 56) geeft daartoe de volgende redenen:

> Zoals ook uit het opschrift van deze Hoofdstukken voortvloeit, is het in het huidige wetboek gehanteerde terminologische onderscheid tussen bijzondere opsporingsbevoegdheden en "gewone" opsporingsbevoegdheden niet gehandhaafd. Van de bijzondere opsporingsbevoegdheden kan eigenlijk niet worden gezegd dat zij bijzonder zijn. Bijvoorbeeld stelselmatige observatie, thans als een bijzondere opsporingsbevoegdheid geclassificeerd, behoort tot het gewone opsporingswerk. Bovendien kan een beperkte observatie plaatsvinden op basis van algemene taakstellende bepalingen. In dat geval gaat het om een opsporingsactiviteit die geen grondslag vindt in een wettelijke bevoegdheid die als bijzondere opsporingsbevoegdheid is geclassificeerd. In het verleden zijn de bevoegdheden tot het vorderen van gegevens als bijzondere opsporingsbevoegdheden aangemerkt. Ook deze bevoegdheden zijn allerminst bijzonder, en hebben veel gemeen met de "gewone" bevoegdheden tot het bevelen van de uitlevering van voorwerpen. Verder is het, om redenen die in paragraaf 9 uiteen worden gezet, gewenst om bevoegdheden met betrekking tot gegevens samenhangend te bezien en te regelen. Om al deze redenen wordt afgestapt van de term bijzondere opsporingsbevoegdheden. Om redenen die in paragraaf 10 uiteen zijn gezet, wordt voor de klassieke bijzondere opsporingsbevoegdheden de term "heimelijke bevoegdheden" gehanteerd.
>
> (…) De term "bijzondere opsporingsbevoegdheden" wordt in het nieuwe wetboek niet meer gebruikt. De bevoegdheden die zijn opgenomen in de regeling zijn namelijk op zichzelf en ook in relatie tot de andere bevoegdheden uit Boek 2 niet bijzonder, maar hebben wel het centrale kenmerk dat zij heimelijk worden uitgeoefend, wat wil zeggen dat de persoon ten aanzien van wie de bevoegdheid wordt uitgeoefend vooraf van deze uitoefening geen kennis heeft en dat hem daarvan pas later mededeling wordt gedaan. Vandaar dat als opschrift voor dit Hoofdstuk is gekozen voor de term "heimelijke bevoegdheden".

Op dit voorstel is in de consultatie de nodige kritiek gekomen. Het belangrijkste kritiekpunt is dat deze naamgeving lijkt te impliceren dat bevoegdheden uit andere Hoofdstukken nooit heimelijk kunnen worden uitgeoefend. Daarnaast zijn het OM en de zitten magistratuur van mening dat het woord heimelijk een negatieve connotatie heeft.

Als men het Hoofdstuk heimelijke bevoegdheden overziet, dan kan de conclusie niet anders luiden dan dat in dat hoofdstuk de bevoegdheden regeling vinden die in beginsel slechts

heimelijk worden uitgeoefend, dus zonder dat de desbetreffende persoon daar weet van heeft. Dat is naar het oordeel van de commissie inderdaad het centrale kenmerk van bevoegdheden zoals tappen, infiltratie en observatie. (Hierbij dient wel te worden opgemerkt dat de heimelijkheid van deze bevoegdheidstoepassingen altijd een tijdelijke is. Zodra het onderzoek het toelaat, zal de heimelijkheid van de handelingen moeten worden opgeheven.) Bevoegdheden die niet in Hoofdstuk 8 zijn opgenomen, zijn in de regel bevoegdheden die in beginsel *openlijk* worden uitgeoefend. Denk hierbij aan beslag, betreden en doorzoeken. Het feit dat deze bevoegdheden niet in Hoofdstuk 8 zijn opgenomen, betekent echter niet dat deze bevoegdheden *nooit* heimelijk uitgeoefend kunnen worden. Een goed voorbeeld hiervan is het DNA-onderzoek (artikel 2.6.5.7.1), maar ook het vergelijkend onderzoek van vinger- of handpalmafdrukken kan bijvoorbeeld onder omstandigheden heimelijk worden uitgevoerd (artikel 2.6.5.4.2 leden 3 en 4). Ook kan bij een doorzoeking bij, of een gegevensvordering aan, een beroepsmatige gegevensverwerker geheimhouding worden bevolen (artikel 2.7.3.1.4), wat betekent dat deze bevoegdheden ten opzichte van de verdachte heimelijk kunnen worden uitgeoefend. Om die reden luidt de titel van Hoofdstuk 7 dan ook niet "Openlijke bevoegdheden", maar "Bevoegdheden met betrekking tot voorwerpen en gegevens". Dit geeft ook aan dat de indeling van bevoegdheden in verschillende Hoofdstukken in Boek 2 geen volledige symmetrie kent: bevoegdheden zijn gegroepeerd rond een bepaald centraal kenmerk (vrijheid in Hoofdstuk 5, lichaam in Hoofdstuk 6, voorwerpen en gegevens in Hoofdstuk 7 en heimelijkheid in Hoofdstuk 8), maar daarbij bestaat geen harde één-op-één-relatie tussen deze kenmerken en de bevoegdheden. Ook bij doorzoekingsbevoegdheden kan immers de vrijheid van personen worden beperkt (artikel 2.7.1.1.5); zo ook kunnen bevoegdheden met betrekking tot lichaam, voorwerpen of gegevens onder omstandigheden heimelijk worden uitgeoefend.

Dat heimelijk een negatieve connotatie zou hebben, is (ten dele) juist, maar datzelfde geldt voor andere in het wetboek gehanteerde begrippen; vrijheidsbeneming heeft, in een democratische rechtsstaat, ook geen positieve connotatie[166]. Bovendien is heimelijkheid niet per definitie negatief: naast de pejoratieve betekenis "stiekem" heeft het ook de meer neutrale betekenis "in het geheim", en geheimen zijn zeker niet per definitie negatief.

De commissie beveelt aan om in de memorie van toelichting bovenstaande uitgangspunten te benadrukken, om het belangrijkste kritiekpunt op de naamgeving weg te nemen.

Aanbeveling 47: in de memorie van toelichting wordt nader toegelicht dat het feit dat een bevoegdheid niet staat opgenomen in Hoofdstuk 8, niet betekent dat deze nooit heimelijk kan worden uitgeoefend. → *p. 201*

6.2. Normering van heimelijke bevoegdheden

De heimelijke bevoegdheden in Hoofdstuk 8 kennen elk hun eigen normering, zoals ook de huidige bijzondere opsporingsbevoegdheden elk specifiek zijn genormeerd, op basis van een inschatting per bevoegdheid hoe ingrijpend deze is en wat in dat licht adequate voorwaarden zijn waaronder deze mag worden uitgeoefend. Zoals toegelicht in paragraaf 4.2.1, is de visie van de commissie echter dat bij onderzoek in een digitale omgeving het in de 21e eeuw steeds moeilijker wordt om op voorhand en in abstracto te kunnen bepalen welke mate van inbreuk een bepaalde bevoegdheid maakt. Er is steeds minder logische samenhang tussen een bepaald deel van het privéleven en een bepaalde bevoegdheid die dat deel van het privéleven blootlegt, terwijl bij bevoegdheden ook de bandbreedte groter wordt van de mogelijke ernst van privacyinbreuken. Het zal dan ook veelal van de context afhangen of bij de uitoefening van een bevoegdheid op voorhand redelijkerwijs voorzienbaar is dat een geringe, een meer dan geringe

[166] Wellicht is dit reden geweest om in het conceptwetsvoorstel in de aanhef van Hoofdstuk 5 het neologisme "vrijheidsbenemening" te hanteren?

of een zeer ingrijpende inbreuk op de privacy zal worden gemaakt. Om die reden heeft de commissie een algemeen normeringscriterium voorgesteld, dat gehanteerd kan worden bij de diverse vormen van onderzoek van gegevens in of overgenomen uit een geautomatiseerd werk of een digitale-gegevensdrager en bij bevoegdheden tot vorderen van gegevens (zie hfd. 0). In de hierna volgende paragrafen motiveert de commissie voorts waarom het algemene normeringscriterium ook van toepassing zou kunnen en moeten zijn op de heimelijke bevoegdheden van het vastleggen van telecommunicatie en vertrouwelijke communicatie (zie par. 6.3.4), stelselmatig overnemen van gegevens uit publiek toegankelijke bronnen (zie par. 6.4.5) en stelselmatige locatiebepaling (zie par. 6.5.3).

Vanuit de visie dat de mate van inbreuk door een bevoegdheid minder goed op voorhand en in abstracto bepaalbaar is, past het – ook vanuit systematische overwegingen – om deze lijn door te trekken en het algemene normeringscriterium ook in zijn algemeenheid op de heimelijke bevoegdheden in Titel 8.2 van toepassing te verklaren. Hoewel niet alle bevoegdheden naar hun aard primair in een digitale omgeving worden uitgeoefend, zullen – vanwege de verwevenheid van de fysieke en de online wereld en de immer toenemende dataficering (par. 2.2.3) – bij elke bevoegdheid in meer of mindere mate digitale gegevens een rol kunnen (gaan) spelen. Daarbij moet men, voor een wetboek dat bedoeld is toekomstbestendig te zijn en qua gehanteerde systematiek ten minste tien of twintig jaar na inwerkingtreding houdbaar zou moeten zijn, rekening houden met mogelijke ontwikkelingen over een lange termijn waarbij het moeilijk te voorzien is hoe ingrijpend de uitoefening van bevoegdheden – ook die op dit moment naar hun aard nog weinig ingrijpend lijken – in de toekomst kan uitpakken. Juist daarom is een algemeen normeringscriterium, dat contextspecifiek wordt ingevuld en waarvan de interpretatie dynamisch kan mee-evolueren met technisch-sociale ontwikkelingen, geschikt voor een systematische regeling van opsporingsbevoegdheden in een digitaal tijdperk.

Een deel van de commissie heeft aarzelingen bij het van toepassing verklaren van het algemene normeringsprincipe op de bevoegdheid tot het vorderen van gegevens en alle heimelijke bevoegdheden. Zij erkennen dat een dergelijke benadering de toekomstbestendigheid van het nieuwe wetboek zou vergroten. Mocht in de toekomst blijken dat als gevolg van een toenemende dataficering het gebruik van deze bevoegdheden een grotere privacyinbreuk zou gaan maken dan in het verleden bij het formuleren van de voorwaarden voor de toepassing van deze bevoegdheden was voorzien, dan is door deze wijze van inrichten geen (nadere) wetswijziging nodig om de benodigde rechtsbescherming te realiseren. Deze leden zien echter een fundamenteel verschil tussen enerzijds het onderzoek aan meer persoonsgebonden computers (zoals pc's, laptops, smartphones en tablets) en anderzijds bevoegdheden waarmee gegevens bij derden worden opgevraagd of waarmee gegevens betreffende bewegingen, gedragingen of uitlatingen in een specifieke context worden vergaard. Genoemde geautomatiseerde werken kenmerken zich door het feit dat bij (uitvoerig) onderzoek daarin vaak direct een vrij scherp en volledig beeld verkregen kan worden van verschillende aspecten van iemands persoonlijke leven (althans voor zover het computers voor persoonlijk gebruik betreft). Die scherpte en volledigheid ontbreekt volgens deze leden over het algemeen bij de toepassing van andere bevoegdheden, zoals stelselmatige observatie, locatiebepaling en onderzoek in publiek toegankelijke bronnen.

Het voordeel van een meer toekomstbestendige abstracte wetgeving moet worden afgewogen tegen de behoefte van zowel de opsporingsinstanties als van degenen die onderwerp van opsporingsonderzoek kunnen zijn, aan duidelijkheid en toepasbaarheid. Het voorgestelde stelsel is zodanig abstract dat er, in de visie van de genoemde commissieleden, te veel nadruk ligt op het eerstgenoemde belang ten koste van het laatstgenoemde belang, waardoor het stelsel in deze vorm tot onwenselijke (rechts)onzekerheid kan leiden.

Andere leden van de commissie stellen daartegenover dat ook bij bevoegdheden tot het vorderen van gegevens en tot het vergaren van gegevens betreffende bewegingen, gedragingen

of uitlatingen in specifieke contexten onder omstandigheden wel degelijk redelijkerwijs voorzienbaar een ingrijpend beeld van iemands privéleven kan ontstaan; het feit dat het om (soms hoge) uitzonderingsgevallen zal gaan, doet daar niet aan af. Het belang van toekomstbestendigheid – ook met het oog op het feit dat de voorgestelde regeling op zijn vroegst pas over enkele jaren in werking treedt, en dat in de tussentijd en na inwerkingtreding de datificering vermoedelijk verder zal voortschrijden – alsook de belangen van consistentie en van een systematische regeling wegen zwaar voor deze leden. Zij onderstrepen daarbij dat rechtszekerheid ook kan worden gefaciliteerd door een uitgebreide memorie van toelichting en nadere uitwerking in lagere richtlijnen en procedures (zie par. 4.4). Aangezien de inwerkingtreding van het gemoderniseerde wetboek niet van vandaag op morgen zal geschieden, is er bovendien de nodige tijd om de abstracte criteria uit te werken voor veelvoorkomende situaties en de praktijk voor te bereiden op de nieuwe systematiek.

De commissie stelt daarom voor het algemene normeringscriterium op alle heimelijke bevoegdheden in Titel 8.2 van toepassing te verklaren. Dat wil niet zeggen dat bij elke bevoegdheid steeds in elk geval een complexe afweging nodig is om te bepalen of de beoogde inzet van een bevoegdheid stelselmatigheid of ingrijpende stelselmatigheid oplevert. De wetgevingstechnische voorkeur voor tamelijk abstracte regelingen dient gepaard te gaan met handvatten om de rechtszekerheid en uitvoerbaarheid te waarborgen, in de vorm van relatief uitgebreide toelichtingen met richtinggevende voorbeelden, alsook in de vorm van uitwerkingen in lagere regelgeving en praktijkrichtlijnen (zie par. 4.1 en 4.4). Dit betekent dat waar het algemene normeringscriterium op *wetgevingsniveau* altijd van toepassing is, de mogelijkheid bestaat in de *toelichting* ten aanzien van veelvoorkomende vormen van uitoefening van bepaalde bevoegdheden aan te geven of, en onder welke omstandigheden, er wel of niet sprake is van (ingrijpende) stelselmatigheid.

Met heldere voorbeelden, maatstaven en argumenten kan richting worden geven aan praktijk en jurisprudentie ten aanzien van bepaalde toepassingen van bevoegdheden. (In die lijn stelt de commissie onder andere voor om bij de bevoegdheden tot het vorderen van gegevens in de toelichting duidelijk te maken dat het vorderen van de huidige catalogus van verkeersgegevens in enge zin geen ingrijpende stelselmatigheid oplevert, zie par. 5.6.3.) De commissie acht het bijvoorbeeld denkbaar dat in de memorie van toelichting wordt aangegeven dat ingrijpende stelselmatigheid voor bepaalde bevoegdheden, zoals stelselmatige observatie en bevoegdheden ten aanzien van een besloten plaats, op dit moment niet aan de orde is, gezien de huidige stand van de techniek. Dat laat de mogelijkheid open om in de toekomst het criterium anders te interpreteren, wanneer bij die bevoegdheden wel veel meer mogelijk wordt en de inzet ingrijpend stelselmatig kan worden.

Naast het algemene normeringscriterium, dat bevoegdheden met name normeert gelet op het belang van de bescherming van de persoonlijke levenssfeer, kunnen er ook andere redenen zijn voor een bepaald niveau van normering. Naast het van toepassing verklaren van het algemene normeringscriterium op alle bevoegdheden in Titel 8.2, kan de wetgever in dat verband specifieke eisen (blijven) stellen bij bepaalde bevoegdheden in Titel 8.2, zoals bij infiltratie in verband met mogelijke risico's voor de integriteit van de opsporing of bij toepassing van bevoegdheden waarbij journalistieke bronbescherming in het geding is (zie par. 4.2.5).

Aanbeveling 48: het algemene normeringscriterium wordt van toepassing verklaard op alle bevoegdheden in Titel 8.2. In de memorie van toelichting kan daarbij ten aanzien van veelvoorkomende vormen van uitoefening van bepaalde bevoegdheden worden uitgelegd of, en onder welke omstandigheden, er wel of niet sprake is van (ingrijpende) stelselmatigheid, waarbij bij bepaalde (vormen van uitoefening van) bevoegdheden kan worden aangegeven dat er, gelet op de huidige stand van de techniek, geen sprake is van ingrijpende stelselmatigheid. → *p. 202*

6.3. Communicatie-gerelateerde bevoegdheden

De communicatie-gerelateerde bevoegdheden bestaan uit het vastleggen van telecommunicatie (hierna ook: tappen) en het vastleggen van vertrouwelijke communicatie (hierna ook: direct afluisteren), alsook bevoegdheden tot het vorderen van communicatie-gerelateerde gegevens (metadata of verkeersgegevens). Deze laatste zijn – vanwege de indeling van bevoegdheden in Hoofdstukken 7 en 8 van het conceptwetsvoorstel – reeds behandeld in paragraaf 5.6. Hier concentreren we ons op de eerstgenoemde bevoegdheden, waarbij we voor een goed begrip van de materie eerst aandacht besteden aan de definitie van de begrippen "vastleggen" en "communicatie" (par. 6.3.1) en aan de reikwijdte van het grondwettelijke telecommunicatiegeheim (par. 6.3.2), om vervolgens de systematiek (par. 6.3.3) en normering (par. 6.3.4) te bespreken.

6.3.1. Definities

Vastleggen

Bij de bevoegdheden tot het vastleggen van telecommunicatie en vertrouwelijke communicatie kan de vraag gesteld worden wat specifiek in het kader van deze bevoegdheden het begrip "vastleggen" inhoudt. In de thans geldende wetgeving wordt niet het begrip "vastleggen" maar het begrip "opnemen" gebruikt. Dit begrip wordt, in een interpretatie uit de praktijk, uitgelegd als een passief begrip. Je mag bij wijze van spreken alleen op de "record"-knop drukken, maar verder niets doen.

Gelet op de toename van versleuteling is het slechts "passief opnemen" niet meer effectief. Vanwege de toename in (van eind tot eind) versleutelde communicatie is het wenselijk om bij interceptie gebruik te maken van "ontsleuteldozen" in de lawful intercept (LI)-infrastructuur van de aanbieder. Met deze technische middelen kan de gegevensstroom tijdens de tap al van versleuteling worden ontdaan. Onder de enge definitie van "passief opnemen" is dat echter niet mogelijk. Mag, met de introductie van het begrip "vastleggen", onder deze beide bevoegdheden nu ook het meer dan passief opnemen van de communicatie worden verstaan?

In de toelichting bij artikel 2.8.2.5.1[167] lijkt dit te worden bedoeld. Uit deze toelichting blijkt dat wordt gewerkt aan technische hulpmiddelen die het mogelijk maken om versleutelde telecommunicatie te ontsleutelen en vast te leggen. Tevens staat in de toelichting opgenomen dat het gebruik van deze technische hulpmiddelen valt onder de bevoegdheid bedoeld in artikel 2.8.2.7.1, de tap dus. Met het oog op de authenticiteit van de ontsleutelde vastgelegde communicatie, dienen deze technische hulpmiddelen wel te voldoen aan de eisen gestelde in het Besluit technische hulpmiddelen.

Hoewel deze passage helder genoeg is voor wat betreft de relatie met technische hulpmiddelen, zou de memorie van toelichting bij artikel 2.8.2.7.1 zelf ook nadrukkelijker moeten benoemen dat bij het vastleggen de hier bedoelde hulpmiddelen kunnen worden ingezet, met de expliciete toelichting dat dit inhoudt dat het vastleggen van de communicatie geschiedt onder gelijktijdige ontsleuteling van de signalen. Aangezien hier de signalen bij de registratie van de communicatie een bewerking ondergaan, is de betrouwbaarheid van deze registratie cruciaal. In dat verband is het belangrijk dat er eisen worden gesteld aan de technische hulpmiddelen; over de vraag hoe die eisen het beste kunnen worden gesteld, verwijst de commissie naar haar opmerkingen over technische hulpmiddelen in het algemeen (par. 6.6).

[167] "In het Besluit technische hulpmiddelen zijn eisen gesteld aan de technische hulpmiddelen die bij de uitoefening van verschillende heimelijke bevoegdheden kunnen worden ingezet. Onderdeel b is nieuw. Dit onderdeel heeft betrekking op *de technische hulpmiddelen die dienen ter ontsleuteling van versleutelde communicatie die wordt vastgelegd door middel van de in artikel 2.8.2.7.1 omschreven bevoegdheid* (vastleggen telecommunicatie)". Memorie van toelichting, p. 238 (cursivering toegevoegd).

Aanbeveling 49: in de toelichting op artikel 2.8.2.7.1 wordt verduidelijkt dat de term "vastleggen" in dit verband ook inhoudt dat al tijdens het vastleggen aan ontsleuteling kan worden gedaan, met verwijzing naar de dienovereenkomstige passage in de toelichting ten aanzien van technische hulpmiddelen. → *p. 196*

Communicatie

Noch in de definitiebepalingen van Boek 1 noch in die van Boek 2 komt het begrip "communicatie" voor. In het normale spraakgebruik duidt communicatie (in de zin waarin het gebruikt wordt in de context van opsporing) op een "verbinding" of op een "(gelegenheid tot) uitwisseling van gedachten, het geestelijk met elkaar verkeren".[168] De memorie van toelichting (consultatieversie, p. 253) combineert beide betekenissen door telecommunicatie in het kader van het inbreuk maken op het voorgestelde telecommunicatiegeheim – de memorie van toelichting bij dat voorstel parafraserend[169] – te definiëren als:

> de uitwisseling van gegevens tussen twee of meer personen die in beslotenheid plaatsvindt met behulp van een door een derde beheerd communicatiemiddel. De inhoud kan bestaan uit geluid, tekst of beeld en de gegevensuitwisseling kan ook plaatsvinden tussen een persoon en een apparaat dat vervangend is voor een persoon of instantie.

Zonder de specifieke aspecten van heimelijkheid en communicatiemiddel, levert dit als werkdefinitie van communicatie op: *uitwisseling van gegevens tussen personen onderling en/of tussen een persoon en een apparaat dat vervangend is voor een persoon of instantie*[170].

Deze definitie blijkt in de praktijk echter niet (meer) te voldoen als beschrijving van alle stromende (*streaming*) gegevens, van gegevens in enige transportfase, die relevant kunnen zijn voor strafrechtelijk onderzoek. Deze beschrijving sluit namelijk gegevens uit die worden overgedragen door een persoon naar zichzelf of zijn eigen apparaat (bijvoorbeeld mail versturen aan zichzelf, bestanden opslaan in de cloud, wachtwoord invoeren om in te loggen op eigen apparaat of beveiligde opslag in de cloud, inspreken voicerecorder; hierna: "zelfcommunicatie"). Dergelijke gegevens zijn door de wetgever zelfs uitdrukkelijk uitgesloten bij toepassing van artikel 126l Sv; overigens niet (expliciet) omdat deze nooit vastgelegd zouden mogen worden,

[168] Zie Dikke van Dale: "1. kennisgeving, m.n. van … familiegebeurtenissen; 2. verbinding (… in communicatie staan met …); 3. (gelegenheid tot) uitwisseling van gedachten, het geestelijk met elkaar verkeren". Vgl. Wikipedia, https://nl.wikipedia.org/wiki/Communicatie: "Communicatie is een activiteit waarbij levende wezens betekenissen uitwisselen door op elkaars signalen te reageren. Het Latijnse woord communicare slaat terug op "iets gemeenschappelijk maken". Deze pagina gaat over interactie tussen mensen. (Er bestaat ook diercommunicatie en plantencommunicatie.) Communicatie is behalve een sociale activiteit, ook het resultaat van het contact: de optelsom van wederzijdse betekenisgevingen, ook wel communicatie-effect genoemd. (…) De essentie van communicatie is dat een of meer zenders en ontvangers binnen een zekere tijdsduur geregeld van rol wisselen en daarbij betekenissen aan elkaar overdragen."

[169] *Kamerstukken II* 2013/14, 33 989, nr. 3, p. 11: "Communicatie betekent uitwisseling van informatie van welke aard en in welke vorm dan ook tussen een verzender en een of meer ontvangers. In deze toelichting wordt op diverse plaatsen het begrip «bericht» gebruikt als een veel voorkomende vorm van communicatie. Te denken valt bijvoorbeeld aan een e-mailbericht of een sms-bericht. Ook de uitwisseling van informatie met een computer van een instantie valt onder communicatie."

Dit is weer een variatie op de memorie van toelichting bij het wetsvoorstel bijzondere opsporingsbevoegdheden, *Kamerstukken II* 1996/97, 25 403, nr. 3 p. 36: "Onder vertrouwelijke communicatie valt bijvoorbeeld een in beslotenheid gevoerd gesprek, een niet openbaar e-mailbericht, of niet voor het publiek bestemd radioverkeer. Ook het gebruik van een geldautomaat, waarbij een persoon met behulp van zijn bankpas communiceert met de computer van de bank, valt onder dit begrip. Onder communicatie valt niet het invoeren van gegevens voor eigen gebruik in een PC. Er is alleen sprake van communicatie als er gegevensuitwisseling is met een ander. Of die ander een persoon is of een apparaat dat vervangend is voor een persoon of een instantie, is niet van belang. Het gaat erom dat er interactie is tussen twee of meer partijen."

[170] Het begrip "instantie" is niet nader geduid, maar ziet op een (rechts)persoon of andere organisatie.

maar omdat hier geen sprake is van communicatie, uitwisseling tussen meer personen.[171] Het is niet duidelijk of de wetgever bedoeld heeft dat dergelijke "berichtenuitwisseling met zichzelf" dermate privacygevoelig is dat deze überhaupt niet heimelijk vastgelegd zou mogen worden, of juist minder privacygevoelig is dan communicatie en daarom op basis van een andere bevoegdheid (zoals stelselmatige observatie van gedrag) zou kunnen worden vastgelegd (zie hierover verder par. 6.3.3).

Ook wordt in deze definitie "autonome" berichtenoverdracht van en tussen apparaten uitgesloten (zijn de auto die signalen ontvangt van de GPS-satelliet en verzendt naar de autoproducent, en de ijskast die dat doet naar de slimme meter, nog wel een "apparaat dat vervangend is voor een persoon"?).

De strafvorderlijke benadering van communicatie wijkt hiermee af van de materieelstrafrechtelijke benadering. De wetgever heeft in de Wet computercriminaliteit voor de artikelen 139a tot en met 139e Sr aangesloten bij de definitie in de Wet op de telecommunicatievoorzieningen. "Telecommunicatie" is daarin: "iedere overdracht, uitzending of ontvangst van gegevens van welke aard ook door middel van kabels, langs radio-elektrische weg of door middel van optische of andere elektro-magnetische systemen." Daarbij wordt in de memorie van toelichting opgemerkt:

> Hoewel in deze definitie mede wordt gesproken van «overdracht van gegevens», is om iedere onduidelijkheid te vermijden in de begripsbepalingen waar nodig nog toegevoegd «of andere gegevensoverdracht door een geautomatiseerd werk». De terminologie «overdracht van gegevens» in samenhang met het woord «telecommunicatie» duidt immers primair op overdracht van gegevens op afstand, tussen personen onderling, tussen personen en computers of tussen computers onderling. Met de toevoeging «overdracht van gegevens» wordt evenwel mede bedoeld het gegevensverkeer over korte afstand, bij voorbeeld tussen een computer en het daarop aangesloten beeldscherm. Het is niet in overeenstemming met het gewone taalgebruik te achten ook deze overdracht van gegevens aan te duiden als telecommunicatie.[172]

Hier wordt dus het begrip communicatie in wezen gedefinieerd als: "iedere overdracht, uitzending of ontvangst van gegevens van welke aard ook*"*.

Europeesrechtelijk ligt een ontwerp-richtlijn op het gebied van elektronische communicatie voor, waarin communicatie sec wordt aangeduid als "elke overdracht van signalen".[173] Het begrip signalen draagt een verwijzing in zich naar het informatiekarakter van de overgedragen gegevens, de be-teken-is.

Er zijn dus verschillende definities van het begrip communicatie. Daar kunnen nog specifieke omschrijvingen aan worden toegevoegd wanneer het gaat om de open of besloten sfeer van communicatie[174], en het al of niet gebruik van een intermediair (zoals een toegangsaanbieder of aanbieder van webmail of een chatdienst). Dát is met name relevant voor de vraag of en in welke mate inbreuk wordt gemaakt op enig communicatiegeheim (zie par. 6.3.2).

De eis van voorzienbaarheid van inbreuken op de persoonlijke levenssfeer vergt dat begrippen waarop strafvorderlijke bevoegdheden zien, zoals het begrip communicatie, voldoende helder

[171] *Kamerstukken II* 1996/97, 25403, nr. 3, p. 35-36.
[172] *Kamerstukken II* 1989/90, 21 551, nr. 3 p. 7.
[173] De definitie in de concept-Richtlijn tot vaststelling van het Europees wetboek voor elektronische communicatie betreft weliswaar niet het strafvorderlijk domein en geeft geen afzonderlijke definitie van communicatie, maar uit de definitie van "elektronische communicatienetwerk" blijkt dat daaronder neutraal wordt verstaan: *het overbrengen van signalen* of, als het gaat over persoonlijke communicatie: *uitwisseling van informatie* tussen personen (art. 2 onder 4 en 5). Zie http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=comnat:COM_2016_0590_FIN (laatst geraadpleegd 1 juni 2018).
[174] Van open tot besloten: een spandoek bij een demonstratie, een mailwisseling, een PGP-telefoongesprek, iemand die in zichzelf praat.

geduid worden. Hoewel het in beginsel ook mogelijk is het begrip communicatie te laten vallen en slechts te werken met een begrip als *"overdracht van gegevens/signalen"*, waaronder dan ook communicatie valt, acht de commissie het wenselijk het begrip communicatie te handhaven, deels om verband te houden met de historische context en deels vanwege artikel 13 Gw, dat een specifieke bescherming van (gemedieerde) communicatie behelst waar het Wetboek van Strafvordering bij moet aansluiten.

Dit betekent dat, hoewel aan elke definitie inherent is dat toekomstige ontwikkelingen kunnen meebrengen dat deze definitie ontoereikend wordt, een adequate definitie van het begrip communicatie nodig is. Bij een definitie ligt de keuze voor om a) een relatief beperkt begrip van communicatie te handhaven (dat aansluit bij het normale spraakgebruik) en bepaalde bevoegdheden ook toepasbaar te verklaren op *"overige overdracht van gegevens"*, waaronder "zelfcommunicatie"; of b) het begrip communicatie ruimer te definiëren als bijvoorbeeld "*elke overdracht van gegevens tussen personen en/of apparaten"* of *"elke overdracht van gegevens"* of *"elke overdracht van signalen"*.

Bij de eerste optie heeft de commissie overwogen communicatie te definiëren als "de uitwisseling van gegevens tussen personen en/of apparaten die personen vervangen." Dit sluit aan bij de "gewone" betekenis (gegevensuitwisseling tussen personen en/of persoonsvervangende apparaten). Vanwege de sterke toename in "zelfcommunicatie" – het uitwisselen van gegevens met zichzelf via de communicatie-infrastructuur, zoals het heen en weer zenden van gegevens naar de cloud – is het ook mogelijk om de definitie uit te breiden met "gemedieerde zelfcommunicatie", oftewel de uitwisseling van gegevens van een persoon met zichzelf voor zover deze uitwisseling plaatsvindt met behulp van een door een derde beheerd communicatiemiddel (sturen van een mail aan jezelf, verkeer van/naar een cloud-opslagdienst). Daarmee blijft echter het uitwisselen van berichten buiten de (tele)communicatie-infrastructuur om, buiten de definitie van communicatie; dit heeft als consequentie dat het onderscheppen van bijvoorbeeld een wachtwoord door een bug in een toetsenbord niet onder "vastleggen van communicatie" valt (omdat het wachtwoord geen vorm van communicatie is). Dat zou ondervangen kunnen worden door de overdracht van gegevens tussen een persoon en een eigen apparaat (een apparaat dat staat voor diezelfde persoon, zoals een computer) óók aan te merken als "zelfcommunicatie" en daarmee alle vormen van "zelfcommunicatie" onder het communicatiebegrip te laten vallen. Daarmee wordt echter de band met het normale spraakgebruik losser. Een alternatief voor de oprekking van het communicatiebegrip is om zelfcommunicatie buiten de definitie te houden, maar in de regeling van bevoegdheden een bepaling op te nemen als: voor de toepassing van bevoegdheden wordt uitwisseling van gegevens met zichzelf gelijkgeschakeld met communicatie. Nadeel daarvan is weer dat voor de burger de voorzienbaarheid van de reikwijdte van een bevoegdheid minder duidelijk wordt, omdat bevoegdheden die op het oog zien op het vastleggen van communicatie dan ook worden toegepast op het vastleggen van niet-communicatie. Daarmee wordt in zekere zin alsnog via een omweg de reikwijdte van het communicatiebegrip opgerekt ten opzichte van het normale spraakgebruik.

Hoewel de commissie het voordeel van aansluiten op het normale spraakgebruik waardevol acht, heeft zij uiteindelijk niet voor deze benadering gekozen. De reden daarvan is niet alleen dat de betekenis minder helder wordt door linksom (in de definitie zelf) of rechtsom (door toepassingsverklaring in de bevoegdheid), ook zelfcommunicatie (al dan niet gemedieerd) onder het communicatiebegrip te brengen. Een andere en zwaarderwegende reden is dat het naar verwachting, gezien de ontwikkeling van het Internet of Things, in toenemende mate moeilijk zal zijn om vast te stellen wanneer een apparaat precies persoonsvervangend is voor de doeleinden van het communicatiebegrip. Is het via Internet hoger zetten van de thermostaat een vorm van uitwisseling van een bericht met een apparaat dat een persoon vervangt? Dat kan nog betoogd worden als men het begrip zelfcommunicatie op enige wijze onderbrengt bij communi-

catie, maar als het hoger zetten geautomatiseerd gebeurt door een slimme assistent op de smartphone van een gebruiker (die diens persoonlijke voorkeuren geleerd heeft), is er dan nog steeds sprake van uitwisseling tussen persoonsvervangende apparaten? Valt de uitwisseling van signalen tussen twee zelfrijdende auto's onder communicatie door persoonsvervangende apparaten? Hoewel het op zich mogelijk is om alle apparaten in het Internet of Things te zien als vervangend voor een persoon, zijn we dan ver verwijderd van de oorspronkelijke betekenis van het communicatiebegrip als "uitwisseling van gedachten, het geestelijk met elkaar verkeren".

Daar komt bij dat met de toename van mens-machine- en machine-machine-communicatie, veel berichtenverkeer niet langer neerkomt op inhoudelijke gedachte-uitwisseling, maar op het "kale" overbrengen van signalen. Er gaan signalen over communicatie-infrastructuren, en of de signalen juridisch wel of niet toe te rekenen zijn aan een bepaalde persoon of instantie is (thans) op het moment dat deze kunnen worden afgetapt op technisch niveau nauwelijks of niet te onderscheiden. Dit heeft praktisch als gevolg dat wanneer in het berichtenverkeer berichten tussen zowel apparaten onderling als tussen apparaten en personen opgevangen worden, het nauwelijks haalbaar zal zijn om daar bij het onderscheppen zinvol onderscheid tussen te maken.

Daarom concludeert de commissie dat de tweede optie de voorkeur verdient: een brede definitie van communicatie die alle overdracht van gegevens tussen personen of apparaten omvat. Dit is de helderste en meest consistente benadering, die de bovengenoemde afbakeningsproblemen vermijdt. Hiermee wordt ook aangesloten bij de strafbaarstelling van aftappen in artikel 139c Sr, dat elke vorm van gegevensoverdracht tussen personen en geautomatiseerde werken en binnen geautomatiseerde werken omvat, wat de onderlinge systematiek binnen het strafrecht versterkt. In deze benadering speelt in de strafvorderlijke regeling van het vastleggen van communicatie-inhoud naast de klassieke rechtsgoederen van het beschermen van gedachte-uitingen en het telecommunicatiegeheim ook een (nieuw) rechtsgoed een rol, dat van integriteit en vertrouwelijkheid van computersystemen – een rechtsgoed dat de Duitse grondwettelijke rechter bescherming heeft toegekend door een nieuw grondrecht (op bescherming van integriteit en vertrouwelijkheid van computersystemen) te onderkennen, in aanvulling op de klassieke grondrechten van huisrecht en telecommunicatiegeheim.[175] Dit sluit goed aan bij het communicatielandschap van de 21e eeuw, waarin zelfcommunicatie en machine-machine-communicatie een belangrijke plaats innemen.

Aanbeveling 50: het wetsvoorstel moet een definitie van het begrip communicatie omvatten, waarbij een brede definitie wenselijk is: communicatie is elke overdracht van gegevens tussen personen of apparaten. Hieronder valt ook gegevensoverdracht binnen geautomatiseerde werken en gegevensoverdracht van personen met zichzelf.

→ *p. 202*

Door de sterke uitbreiding van het begrip communicatie komt veel meer dan nu het geval is onder bereik van de bevoegdheden tot vastleggen van communicatie, waaronder gegevensoverdracht tussen apparaten. Gekoppeld met de opkomst van het Internet of Things betekent dit dat een aanzienlijk groter deel van het leven dan voorheen onder de reikwijdte van de tap of direct afluisteren komt te vallen. Dit roept vragen op over de normering en de daarbij te hanteren criteria. Hierop komen we in het navolgende terug, maar eerst kijken we naar één van de relevante criteria voor normering: artikel 13 Grondwet (hierna: Gw). Niet alle vormen van gegevensoverdracht vallen onder het grondwettelijke telecommunicatiegeheim. Om nader te omschrijven in welke gevallen sprake is van door de Grondwet beschermde communicatie, is het daarom van belang de reikwijdte van artikel 13 Gw nader in kaart te brengen.

[175] BVerfG 27 februari 2008, 1 BvR 370/07, ECLI:DE:BVerfG:2008:rs20080227.1bvr037007, beschikbaar op http://www.bverfg.de/e/rs20080227_1bvr037007.html (laatst geraadpleegd 1 juni 2018).

6.3.2. Het grondwettelijke telecommunicatiegeheim

Recent is de voorgestelde grondwetswijziging ter zake artikel 13 Gw in beide Kamers met algemene stemmen aangenomen,[176] zodat artikel 13 Gw na instemming van de Kamers in tweede lezing zal komen te luiden:

> **Artikel 13**
>
> 1. Ieder heeft recht op eerbiediging van zijn brief- en telecommunicatiegeheim.
>
> 2. Beperking van dit recht is mogelijk in de gevallen bij de wet bepaald met machtiging van de rechter of, in het belang van de nationale veiligheid, door of met machtiging van hen die daartoe bij de wet zijn aangewezen.

Vooruitlopend op inwerkingtreding en uitgaande van de verwachting dat de tekst aldus zal komen te luiden, kan op grond van de wetsgeschiedenis het volgende worden gezegd over de vormen van communicatie die met deze bepaling beschermd worden en de mogelijke inbreuken daarop. Daarbij beperken we ons tot hetgeen voor de modernisering van het Wetboek van Strafvordering relevant is, hetgeen betekent dat alleen wordt gekeken naar de verticale bescherming: inbreuken die door de overheid worden gemaakt.

De discussie over betekenis en reikwijdte van de bepaling concentreert zich met name op de betekenis voor en van telecommunicatie; aan de brief worden weinig woorden gewijd,[177] omdat in wezen het beschermingsniveau van de telecommunicatie wordt verhoogd tot het beschermingsniveau van de brief.[178]

Artikel 13 Gw heeft te gelden als specialis van met name artikel 10 Gw (dat de persoonlijke levenssfeer beschermt) en is van toepassing als aan drie criteria is voldaan:[179]

a. er wordt gebruik gemaakt van een communicatiemiddel;
b. een derde is belast met transport en/of opslag; en
c. er is sprake van gerichtheid op een of meer ontvangers.

De achterliggende gedachte is, om in de fase waarin een betrokken derde toegang heeft tot de aan hem ter verzending toevertrouwde boodschap, bescherming te bieden tegen heimelijke inzage daarvan door de overheid.[180] De verzonden inhoud is in die fase kwetsbaar, want onderweg van de ene door de artikelen 10 of 12 Gw beschermde privésfeer naar de andere en – buiten controle/beschikkingsmacht of zicht van de verzender – daarbij in handen van een derde.[181]

In het bijzonder van belang is de parlementaire bespreking van:

I. de reikwijdte van het begrip telecommunicatie;
II. het onderscheid tussen inhoud en verkeersgegevens;
III. de afzender en geadresseerde, mede in relatie tot communicatie tussen apparaten (IoT);
IV. de vraag wie als derde is aan te merken.

(I) Uitdrukkelijk kiest de (Grond)wetgever in dit artikel niet voor bescherming van een algemeen "communicatiegeheim" (dat ook zou zien op bijvoorbeeld opname van vertrouwe-

[176] *Handelingen II* 2016/17, 69-11, *Handelingen I* 2016/17, 35-4, Wet van 17 augustus 2017, *Stb.* 2017, 334.
[177] Voor de definitie wordt verwezen naar de Postwet 2009: "de op een fysieke drager aangebrachte geadresseerde schriftelijke mededelingen" en de uitleg voor die wet en het huidige artikel 13 Gw, waaronder ook open stukken en algemene mededelingen vallen, mits geadresseerd.
[178] *Kamerstukken II* 2013/14, 33 989, nr. 3 p. 10.
[179] *Kamerstukken II* 2013/14, 33 989, nr. 3 p. 12-16, en passim, onder meer *Handelingen II* 2016/17, 67-3, p. 10.
[180] *Kamerstukken II* 2013/14, 33 989, nr. 3 p.14-15, 24, *Kamerstukken II* 2014/15, 33 989, nr. 6, p. 5.
[181] *Kamerstukken II* 2013/14, 33 989, nr. 3 p. 10, *Kamerstukken II* 2014/15, 33 989, nr. 6 p. 5-6, *Handelingen II* 2016/17, 67-3, p. 9. De overheid was in de tijd dat het recht geformuleerd werd tevens de derde aan wie werd toevertrouwd; hoewel aan die geschiedenis (en de privatisering van de instellingen) wel af en toe gerefereerd wordt (onder meer Advies Raad van State, *Kamerstukken II* 2013/14, 33 989, nr. 4, p. 2), wordt daar voor de uitleg van de huidige bepaling niet meer naar verwezen.

lijke rechtstreekse communicatie),[182] maar voor bescherming van de communicatie die verloopt via een *middel* waarbij de communicatie aan een derde wordt toevertrouwd en, onder verwijzing naar de etymologie, het overbrengen van informatie op afstand.[183] Het begrip is bewust ruimer dan wetten en verdragen die zien op *elektronische* telecommunicatie, om mogelijk toekomstige niet-elektronische communicatie mede te omvatten.[184]

De beschermde telecommunicatie heeft niet alleen betrekking op "stromende" gegevens, maar ook op opslag door de betrokken derde, voor, tijdens en na de transportfase; maatgevend is dat de derde-transporteur toegang heeft tot de inhoud.[185]

(II) Technische verkeersgegevens/metadata vallen niet onder artikel 13 Gw, tenzij het gaat om metadata die zelf inhoud zijn/bevatten (zoals de onderwerpregel van e-mailberichten). Erkend wordt dat verkeersgegevens inzicht kunnen geven in de privésfeer, maar tegen deze inbreuk wordt beschermd door artikel 10 Gw/artikel 8 EVRM.[186]

Artikel 13 beschermt de inhoud, dat is: informatie, gevoelens en gedachten die de verzender beoogt over te brengen.[187] Wel wordt erkend dat sprake is van een grijs gebied wat de onderscheiding inhoud/verkeersgegevens betreft, maar daarin heeft uiteindelijk de wetgever of de rechter het laatste woord.[188]

Een motie met de strekking ook verkeersgegevens te beschermen onder het telecommunicatiegeheim is in de Tweede Kamer ontraden en verworpen.[189] In de Eerste Kamer motiveert de Minister dit nog eens: hiertegen pleiten praktische redenen (elke keer de rechter om toestemming vragen zou grote consequenties hebben voor strafrechtelijk onderzoek) en logische redenen (aansluiten bij de systematiek).[190]

(III) Wezenlijk is dat sprake is van informatie die gericht is aan een of meer afzonderlijk te bepalen ontvangers (ook de mail van zender aan zichzelf, ook spam, niet een klassieke tv-uitzending). Ongerichte communicatie valt niet onder artikel 13 Gw, maar onder de vrijheid van meningsuiting (artikel 7 Gw).[191]

Zender en ontvanger kunnen apparaten zijn, en boodschappen kunnen automatisch gegenereerd zijn, maar – hoewel niet uitdrukkelijk in een definitie benoemd – wordt daarachter wel een persoon verondersteld, ook als die niet aanstonds kenbaar is.[192] In het kader van IoT meldt de Minister – die overigens wil "wegblijven van voorbeelden" om techniekonafhankelijk te

[182] *Kamerstukken II* 2014/15, 33 989, nr. 6 p. 5; die directe communicatie wordt beschermd door artikel 10 Gw, of – in de woning – artikel 12 Gw.
[183] *Kamerstukken II* 2013/14, 33 989, nr. 3, p. 9.
[184] *Kamerstukken II* 2013/14, 33 989, nr. 3, p. 9-10; genoemd wordt o.m. de Telecommunicatiewet.
[185] *Kamerstukken II* 2013/14, 33 989, nr. 3, p. 10, 14, *Handelingen II* 2016/17, 67-3, p. 14, *Handelingen I* 2016/17, 34-5, p. 7.
[186] *Kamerstukken II* 2013/14, 33 989, nr. 3, p.18, 19, 23.
[187] *Kamerstukken II* 2013/14, 33 989, nr. 3, p. 39.
[188] *Kamerstukken II* 2013/14, 33 989, nr. 3, p. 19-20.
[189] *Kamerstukken II* 2016/17, 33 989, nr. 13 en *Handelingen II* 2016/17, 67-3, p. 9 en 69-12.
[190] *Handelingen I* 2016/17, 34-5, p. 7.
[191] *Kamerstukken II* 2013/14, 33 989, nr. 3, p. 16. Over de vraag wanneer iets ongericht is valt overigens ook weer te twisten: is een Twitterbericht gericht tot volgers of tot het publiek?
[192] *Kamerstukken II* 2013/14, 33 989, nr. 3, p. 11: "Communicatie betekent uitwisseling van informatie van welke aard en in welke vorm dan ook tussen een verzender en een of meer ontvangers. … Ook de uitwisseling van informatie met een computer van een instantie valt onder communicatie. … Of die ander een persoon is of een apparaat dat vervangend is voor een persoon of een instantie, is niet van belang. Het gaat erom dat er interactie is tussen twee of meer partijen." En *ibidem*, p. 16: Het kan gaan om het gericht zijn van de communicatie aan natuurlijke personen maar ook om berichten aan – én van – organisaties, instellingen en andere entiteiten. Tegenwoordig wordt veel van apparaat naar apparaat gecommuniceerd, terwijl de persoon achter de verzender en ontvanger wellicht niet direct kenbaar zijn."

blijven – dat een door de ijskast in opdracht van de eigenaar opgestuurd geadresseerd bericht hetzelfde behandeld moet worden als een door de eigenaar zelf per brief aan een supermarkt gericht boodschappenlijstje, en dus beschermd wordt onder artikel 13 Gw.[193] Daarentegen valt overdracht van bijvoorbeeld locatiegegevens door een auto naar de fabrikant kennelijk niet onder artikel 13 Gw; maar wel onder de persoonlijke levenssfeer, want de Minister ziet het als "oprekken" om dit aan te merken als bericht: het gaat erom of de eigenaar/gebruiker weet dat de auto dit doet, of het zijn bedoeling is dat dit verstuurd wordt en of er sprake is van inhoud.[194] "De intentie van de persoon die het bericht verstuurt moet zijn om het bericht te laten versturen. Dus wanneer twee apparaten met elkaar communiceren levert dit niet automatisch een bericht op."[195]

(IV) Artikel 13 Gw gaat uit van derden aan wie berichten worden toevertrouwd; daaronder vallen alle aanbieders in de zin van de Telecommunicatiewet en de Postwet 2009, maar ook aanbieders van niet-openbare telecommunicatiediensten (bedrijfsnetwerken, private koeriers): "op enig moment in het proces dient sprake te zin van transport van communicatie".[196] Blijkens deze omschrijving, de diverse voorbeelden[197] en de discussie in de Kamers[198] moeten dus ook degenen die berichtfuncties aanbieden als nevengeschikte dienst tot deze derden gerekend worden.

Duidelijk is dat het grondwettelijke communicatiegeheim ziet op een begrip communicatie dat beperkter is dan het door de commissie voorgestelde communicatiebegrip. De grondwetgever beperkt de bescherming tot uitwisseling van berichten tussen personen (of instanties) en tussen een persoon en een apparaat dat een persoon (of instantie) vervangt; daarbij wordt de inhoud van communicatie gekoppeld aan informatie, gevoelens en gedachten die de verzender beoogt over te brengen. "Zelfcommunicatie" valt hier wel onder voor zover het berichten (aan zichzelf) betreft die aan een derde worden toevertrouwd, maar berichtenuitwisseling binnen een computersysteem valt er niet onder. Ook machine-machine-communicatie en IoT-communicatie valt binnen de reikwijdte van het telecommunicatiegeheim wanneer er sprake is van een door de gebruiker van het apparaat bewust bedoelde verzending van een bericht, maar niet wanneer de verzending niet toe te rekenen valt aan een bewuste keuze van de apparaatgebruiker. Een en ander heeft consequenties voor de normering van het vastleggen van communicatie-inhoud binnen Strafvordering (zie onder, par. 6.3.4).

6.3.3. De systematiek van het strafvorderlijk onderzoek van communicatie

Bovenstaande analyse van het begrip communicatie en de grondwettelijke reikwijdte van het telecommunicatiegeheim betekenen, in samenhang met technische ontwikkelingen zoals het IoT, dat enige reflectie nodig is op de afbakening van communicatie ten opzichte van (wat we gemakshalve noemen) non-communicatie, en op de systematiek van de regeling van communicatie-gerelateerde bevoegdheden.

Communicatie is een bijzondere vorm van gedrag. Vastlegging van de inhoud van communicatie vergt zelfstandige normering ten opzichte van vastlegging van niet-communicatief gedrag a) omdat communicatie inzicht kan geven in gedachten, en omdat het delen van gedachten tussen mensen bijzondere bescherming behoeft, b) vanwege het grondwettelijke telecommunicatiegeheim, c) vanwege het belang van de bescherming van integriteit en vertrouwelijkheid

[193] *Handelingen II* 2016/17, 67-3, p. 11.
[194] *Handelingen II* 2016/17, 67-3, p. 12, 11.
[195] *Handelingen I* 2016/17, 34-5, p. 6.
[196] *Kamerstukken II* 2013/14, 33 989, nr. 3, p. 13, *Kamerstukken II* 2014/15, 33 989, nr. 6, p. 5.
[197] *Kamerstukken II* 2013/14, 33 989, nr. 3, p. 16: invullen van een formulier op een website valt eronder, alsook chatten in een besloten chatgroep.
[198] *Handelingen I* 2016/17, 34-5, p. 6: "Facebook of welke andere organisatie ook".

van computersystemen, en d) omdat bij onderscheppen van telecommunicatie steunbevoegdheden nodig zijn, waaronder een regeling voor afdwingbare medewerking van communicatie-aanbieders.

Er bestaan bevoegdheden voor observatie van fysiek gedrag (in het bijzonder artikel 126g Sv, stelselmatige observatie) en vastleggen van communicatief gedrag (onder andere artikelen 126m en 126l Sv) van een persoon. Deze bevoegdheden moeten naadloos op elkaar aansluiten. In de huidige regeling – die doorwerkt in het conceptwetsvoorstel bij gebreke van een specifiek voorstel hieromtrent – bestaat onduidelijkheid (en mogelijk een lacune in de wetgeving) omtrent bijvoorbeeld het onderscheppen van wachtwoorden via een keylogger: dit is expliciet uitgesloten van de bevoegdheid van artikel 126l Sv (direct afluisteren) omdat het geen communicatie betreft.[199] Onduidelijk is echter of het onder de bevoegdheid van stelselmatige observatie valt; dat is in theorie (in andere plaatsen dan een woning) mogelijk,[200] maar in de praktijk moeilijk omdat een keylogger niet alleen non-communicatie maar met enige waarschijnlijkheid ook communicatie opvangt, terwijl stelselmatige observatie onder artikel 126g Sv niet (mede) gericht mag zijn op het opnemen van de inhoud van communicatie. Ook kent stelselmatige observatie geen steunbevoegdheid voor het binnentreden in woningen om een keylogger te plaatsen. Het tussen wal en schip vallen van bepaalde vormen van gegevensoverdracht, bijvoorbeeld binnen geautomatiseerde werken, is onwenselijk. In het voorstel van de commissie wordt dit opgelost door de voorgestelde brede definitie van communicatie, waardoor het plaatsen van een keylogger onder de bevoegdheid tot het opnemen van vertrouwelijke communicatie (126l Sv, artikel 2.7.2.8.1) valt, inclusief het onderscheppen van wachtwoorden en andere vormen van gegevensoverdracht die niet vallen onder het oude communicatiebegrip.

Het vastleggen van gegevens die niet worden overgedragen tussen personen of apparaten – waarbij te denken valt aan het opvangen van geluiden die iemand of een apparaat maakt zonder de bedoeling te hebben dat deze door iemand of een apparaat worden opgevangen, zoals het op een bankje in het park in zichzelf praten of het maken van geluiden tijdens een dutje aldaar – is dan mogelijk, zoals ook onder de huidige regeling, op basis van de bevoegdheid tot stelselmatige observatie. Inzet van een middel waarbij redelijkerwijs voorzienbaar is dat zowel communicatief als niet-communicatief gedrag wordt vastgelegd, wordt gebaseerd op de zwaarste bevoegdheid (dus niet stelselmatige observatie maar een tap of direct afluisteren, of een andere relevante bevoegdheid waarbij communicatie-inhoud kan worden vastgelegd, zoals stelselmatig inwinnen van informatie, of een combinatie van deze bevoegdheden).

Een volgend systematisch onderscheid is dat communicatie-inhoud door de opsporing kan worden vastgelegd *ex nunc* of *ex tunc*. Hiermee bedoelen we het onderscheid tussen het vastleggen van real-time- of toekomstige gegevens (*ex nunc*) en het overnemen van eerder gegenereerde (historische) gegevens (*ex tunc*).[201] Dit onderscheid lijkt voldoende robuust en

[199] Zie boven, noot 171.

[200] Waarbij het wel de vraag is of de inhoud van ingetikte "zelfcommunicatie" zoals wachtwoorden – die blijkens de wetsgeschiedenis niet onder "communicatie" valt – als "gedrag" valt te kwalificeren. Het feit *dat* iemand aan het tikken is, is duidelijk gedrag; maar *wat* zij aan het tikken is, is eerder een uiting van gedachten en lijkt in die zin meer op communicatie dan op gedrag. In dit opzicht sluiten de concepten gedrag en communicatie, zoals gebruikt in de huidige wetssystematiek, niet naadloos op elkaar aan: er bestaat een tussencategorie van gedachte-uitingen die niet (als zodanig) bedoeld zijn voor anderen. In de vorige eeuw kende het Wetboek een dergelijke tussencategorie in de vorm van de geschriftenbescherming (waarbij geschriften bij een huiszoeking zwaarder werden beschermd dan andere objecten in de woning), maar deze is in 2000 afgeschaft.

[201] Dit onderscheid hangt van oudsher samen met het onderscheid tussen stromende en opgeslagen gegevens, maar valt er niet mee samen. Klassiek wordt het onderscheppen van gegevens in real time geassocieerd met het onderscheppen van stromende gegevens, en het vastleggen van historische gegevens met het onderscheppen van opgeslagen gegevens. Met de komst van cloud-technologie verliest het onderscheid tussen stromende en opgeslagen gegevens echter sterk aan relevantie: in de cloud opgeslagen gegevens zijn in potentie voortdurend in beweging. Ook heeft de traditionele vorm van opslag van gegevens op een gegevensdrager in toenemende mate

toekomstbestendig, omdat het een conceptueel (en niet een technisch) onderscheid aanduidt, namelijk naar het moment van het vastleggen van gegevens: gegevens die op het moment dat het vastleggen door de opsporingsdienst begint al waren gegenereerd en vastgelegd door de gebruiker, vallen onder historische gegevens; gegevens die vanaf het moment dat het vastleggen door de opsporingsdienst begint, door de gebruiker worden gegenereerd, ontvangen en vastgelegd of verzonden, vallen onder real-time/toekomstige gegevens. Voor het vastleggen *ex nunc* zijn de klassieke bevoegdheden van de tap en direct afluisteren bestemd, voor het vastleggen *ex tunc* gelden de klassieke doorzoekings-, beslag- en vorderingsbevoegheden. Van belang daarbij is dat het telecommunicatiegeheim niet alleen op het eerste van toepassing is (waar het van oudsher vooral op ziet) maar ook bij het laatste aan de orde kan zijn, namelijk als historische gegevens bij of via een derde-transporteur worden verkregen.[202]

Dit brengt ons bij een derde systematisch onderscheid. Dit is het normatieve onderscheid tussen gegevens die door artikel 13 Gw worden beschermd en gegevens die niet onder de reikwijdte van die bepaling vallen. (Deze laatste kunnen wel grondwettelijk beschermd zijn, maar dan onder artikel 10 Gw; ze worden dan niet *als communicatie* beschermd maar als privacyrelevante gegevens.) Dit onderscheid werkt als gezegd door in het bovenstaande conceptuele onderscheid tussen vastlegging *ex nunc* en *ex tunc*. In beide gevallen kan er sprake zijn van het telecommunicatiegeheim, maar niet noodzakelijkerwijs. Zoals in paragraaf 6.3.2 is geconstateerd, is het grondwettelijk communicatiegeheim niet van toepassing op alle vormen van gegevensoverdracht die *ex nunc* wordt vastgelegd, en evenmin op alle vormen van historische communicatie die *ex tunc* wordt vastgelegd – daarvan is alleen sprake waar het berichten betreft die worden verkregen bij of via de aanbieder. In de door de commissie voorgestelde benadering (zie ook onder) sluit Sv aan bij de systematiek van artikel 13 Gw, die communicatie beschermt voor zover deze kwetsbaar is vanwege de beschikkingsmacht van een aanbieder. Het verkrijgen *via* de aanbieder hangt samen met deze kwetsbaarheid (en valt dus onder artikel 13 Gw); het verkrijgen *buiten* de aanbieder *om* (dus bij de eindgebruiker) hangt niet samen met deze kwetsbaarheid (en valt dus buiten artikel 13 Gw).[203]

Op basis van bovenstaande onderscheiden kunnen we, met inachtneming van het feit dat communicatie-inhoud niet alleen via passieve registratie door tap of direct afluisteren, maar ook via interactieve bevoegdheden als stelselmatig inwinnen van informatie kan worden verkregen, de bevoegdheden als volgt in schema brengen. (Dit schema is niet bedoeld als een uitputtend overzicht van alle opsporingsbevoegdheden, maar als hulpmiddel om de onderlinge relatie tussen de belangrijkste communicatie-gerelateerde bevoegdheden te verhelderen.)

Een systematisch (maar niet uitputtend bedoeld)[204] overzicht van de bevoegdheden ziet er als volgt uit:

---

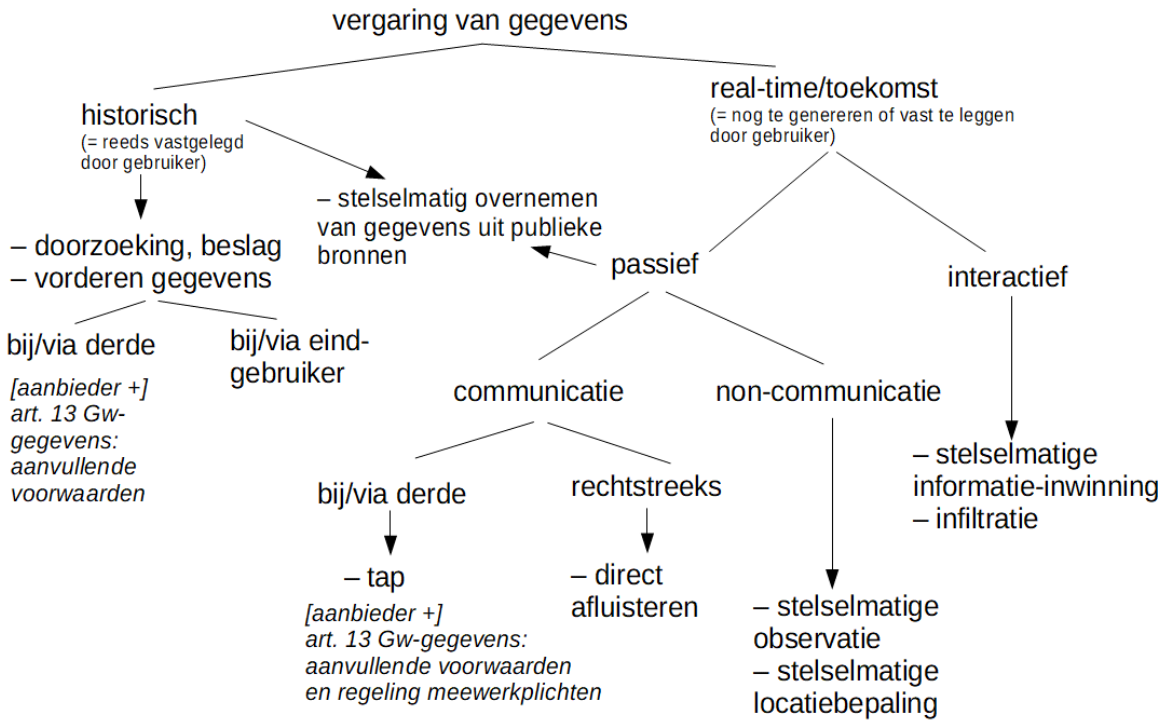
een dynamisch karakter, omdat gegevens die via een app op de smartphone of tablet worden opgeslagen zowel binnen het apparaat als in een cloud-omgeving kunnen worden opgeslagen. Uit de expertbijeenkomst "Opsporing en toekomstige technologie" die de commissie op 24 november 2017 organiseerde, kwam dan ook naar voren dat het onderscheid tussen opgeslagen en stromende gegevens problematisch is. Om die reden hanteert de commissie dan ook niet het begrippenpaar stromend—opslag maar het begrippenpaar real-time—historisch.

[202] Zie boven, noot 185 en bijbehorende tekst.

[203] Dit is vergelijkbaar met de bestaande benadering van bijvoorbeeld voicemail: deze valt onder de grondwettelijke bescherming als een opgeslagen voicemailbericht wordt verkregen via de aanbieder (bijvoorbeeld met een tap of vordering), maar niet als deze wordt verkregen tijdens een doorzoeking bij de eindgebruiker (ook niet als deze nog steeds (ook) in de beschikkingsmacht van de aanbieder ligt).

[204] Zo kan bijvoorbeeld onder de vergaring van real-time/toekomstige (communicatie)gegevens ook het vastleggen van binnenkomende berichten op een inbeslaggenomen geautomatiseerd werk, zoals smartphone of laptop, vallen (zie par. 5.3.4).

Figuur 1. Schema van opsporingsbevoegdheden



De door de commissie voorgestelde ruime definitie van communicatie en bovenstaande beschouwing over de afbakening van communicatie ten opzichte van non-communicatie hebben implicaties voor de normering van communicatie-gerelateerde bevoegdheden. Deze implicaties zijn deels verwerkt in de beschouwing over het vorderen van gegevens in relatie tot grondwettelijke beschermde communicatie (par. 5.6.1) en worden voor het overige in de volgende paragraaf behandeld ten aanzien van het vastleggen van communicatie.

6.3.4. Normering van de bevoegdheden tot vastleggen van telecommunicatie en vertrouwelijke communicatie

De voorgestelde benadering breidt de reikwijdte van de bevoegdheden tot het vastleggen van telecommunicatie en vertrouwelijke communicatie (artikelen 126l en 126m Sv) uit met diverse vormen van gegevensoverdracht (zelfcommunicatie, gegevensverkeer tussen apparaten). Dit betekent dat meer gegevensoverdracht onder de reikwijdte komt van bevoegdheden die van oudsher als zeer ingrijpend worden aangemerkt en altijd een machtiging van de rechter-commissaris behoeven.

De commissie adviseert om differentiatie aan te brengen in de normering van deze bevoegdheden. In lijn met de algemene constatering in dit advies dat traditionele scheidslijnen vervagen en minder goed kan worden bepaald welke bevoegdheden *per definitie* het meest ingrijpend zijn, stelt de commissie dat het vastleggen van (tele)communicatie niet in alle gevallen dermate ingrijpend zal zijn dat daarvoor een rechterlijke machtiging nodig is. Vanzelfsprekend is dat wel het geval voor de communicatie die onder het telecommunicatiegeheim valt. Zoals reeds vermeld omvat communicatie tegenwoordig (en in de IoT-toekomst steeds meer) ook berichtenverkeer tussen apparaten onderling – dat niet onder het telecommunicatiegeheim valt – alsook de uitwisseling van qua inhoud relatief triviaal berichtenverkeer tussen personen en machines. Ook constateert de commissie dat het onderscheid tussen communicatie-inhoud en metadata, zeker op middellange termijn, minder verdedigbaar is als een normatief onderscheid

met *intrinsiek* verschillende beschermingsniveaus, en dat het vaker van de omstandigheden van het geval zal afhangen of het kennisnemen van communicatie-inhoud meer of minder zicht geeft op iemands privéleven dan de informatie die uit metadata zijn af te leiden (zie par. 5.6.3).

Om die redenen adviseert de commissie het algemene normeringscriterium ook toe te passen op de bevoegdheden tot tappen en direct afluisteren. Het eerste deel van het criterium – de geringe inbreuk – zal zich daarbij zelden voordoen, maar is niet uitgesloten; evenals het uitlezen van een simpele chip met weinig gegevens in een apparaat als niet-stelselmatig wordt gekarakteriseerd (par. 5.3.3), zal ook het onderscheppen van de gegevens tussen een dergelijke chip en een lezer (gesteld dat deze draadloze communicatie van afstand te onderscheppen zou zijn) een niet-stelselmatig karakter hebben. Ook het onderscheppen van berichten tussen een robotstofzuiger en sensoren in de muur gedurende korte tijd zal slechts een geringe privacyinbreuk opleveren. Dit zijn vooral theoretische voorbeelden; in vrijwel alle gevallen zal het tappen of direct afluisteren een bevel van de officier van justitie behoeven, en vaak – maar niet altijd – ook een machtiging van de rechter-commissaris.

Evenals bij de doorzoekings- en vorderingsbevoegdheden (par. 5.6.1) stelt de commissie voor een algemene bepaling op te nemen in Hoofdstuk 8 die het vastleggen van communicatie die onder het telecommunicatiegeheim valt, bindt aan het vereiste van een machtiging van de rechter-commissaris en – zoals in de artikelen 126m en 126l Sv – aan zwaardere subsidiariteits- en verdenkingscriteria. Hieronder valt het vastleggen van de inhoud van communicatie (tussen personen of tussen een persoon en een persoonsvervangend apparaat) die verloopt via een derde die belast is met transport en/of opslag (zie par. 6.3.2).

Het telecommunicatiegeheim beschermt echter alleen communicatie die via een derde-transporteur plaatsvindt; het onderscheppen van directe communicatie tussen personen betreft ook een ingrijpende privacyinbreuk (daarom kennen de artikelen 126m en 126l Sv ook dezelfde normering). In het beschermingsniveau van communicatie tussen mensen beoogt de commissie geen verandering aan te brengen. Het vastleggen van niet-openbare gerichte communicatie die tussen mensen plaatsvindt via een derde en het vastleggen van vertrouwelijke directe communicatie tussen mensen moeten als ingrijpend stelselmatig worden gekenmerkt. Het gaat daarbij immers om wat communicatie van oudsher bij uitstek inhoudt: de besloten onderlinge uitwisseling van gedachten.

Voor communicatie tussen mensen en apparaten (voor zover niet onder het telecommunicatiegeheim vallend) en tussen apparaten onderling zal het van diverse factoren – zoals de duur, het type apparaat, de aard van de gegevens die normaliter met zo'n apparaat worden uitgewisseld, de gebruiksfrequentie – afhangen of het vastleggen daarvan stelselmatig of ingrijpend stelselmatig is. Wat de aard van de gegevens betreft, kan daarbij gesteld worden dat wanneer de (zelf-)communicatie samenhangt met gedachte-uitingen – zoals sommige commando's aan een AI-persoonlijke assistent, of het inspreken van tekst op een voicerecorder – het vastleggen daarvan onder ingrijpende stelselmatigheid kan vallen, als redelijkerwijs voorzienbaar is dat het gesprokene een ingrijpend beeld van iemands privéleven oplevert. Dat is niet het geval als bij commando's aan een persoonlijke AI-assistent om een liedje harder of zachter te zetten, evenmin als bij het inspreken van een voicerecorder door een accountant van een (deel van) het jaarverslag van een bedrijf. Het is echter wel het geval als bij de opsporingsinstantie bekend is dat iemand een dagboek bijhoudt met behulp van op zijn voicerecorder ingesproken teksten, of als uit het onderzoek gebleken is dat iemand met veelvuldig privacygevoelige vragen stelt aan zijn persoonlijke assistent ("Alexa, wat zijn de eerste symptomen van dementie?", "Alexa, welke partij is voor belastingverlaging voor middeninkomens?"). Veelal zal overigens niet direct op voorhand redelijkerwijs voorzienbaar zijn dat bij het vastleggen van vertrouwelijke mens-machine-communicatie een ingrijpend beeld van iemands privéleven kan ontstaan; wanneer echter tijdens bijvoorbeeld het uitoefenen van de bevoegdheid tot direct afluisteren gericht op iemands zelf- of machine-communicatie blijkt dat dit wel het geval is,

zou het laten voortduren van het onderzoek alleen kunnen plaatsvinden als alsnog een machtiging van de rechter-commissaris is verkregen.

Hoewel het flexibele normeringscriterium ruimte voor interpretatie openlaat en vragen zal oproepen wanneer nu precies sprake is van ingrijpende stelselmatigheid (buiten de duidelijke situaties van communicatie tussen personen en het telecommunicatiegeheim), acht de commissie deze flexibele benadering beter verdedigbaar voor een wetboek dat beoogt een duurzame systematiek te hebben, dan een rigide benadering die in de wet op voorhand categorieën communicatie aanwijst waarvoor een rechterlijke machtiging nodig is en daarmee andere categorieën uitsluit. Een dynamische interpretatie die mee kan evolueren met de (aanzienlijke) ontwikkelingen in het telecommunicatie-ecosysteem zal op langere termijn werkbaarder zijn dan een technologie-specifieke aanwijzing van bepaalde soorten communicatie. Daarbij is goed denkbaar dat, naast richtinggevende voorbeelden in de memorie van toelichting, voor bepaalde veelvoorkomende vormen van communicatie richtlijnen worden ontwikkeld die aan de praktijk de benodigde rechtszekerheid bieden, en die relatief eenvoudig aangepast of uitgebreid kunnen worden zodra technische ontwikkelingen daartoe nopen.

Aanbeveling 51: het vastleggen van communicatie en het vastleggen van vertrouwelijke communicatie (Afdelingen 8.2.7 en 8.2.8) wordt verbonden aan het algemene normeringscriterium. Daarbij wordt een algemene bepaling opgenomen: "Indien het onderzoek bedoeld in deze afdeling betrekking heeft op communicatie die beschermd wordt door het telecommunicatiegeheim als bedoeld in artikel 13 Gw, kan het onderzoek alleen plaatsvinden indien het belang van het onderzoek dit dringend vereist en na een daartoe verleende machtiging van de rechter-commissaris."

In de toelichting wordt vermeld dat het heimelijk vastleggen van niet-openbare communicatie die tussen mensen plaatsvindt via een derde of het vastleggen van vertrouwelijke directe communicatie die tussen mensen plaatsvindt als ingrijpend stelselmatig wordt aangemerkt. Voor het vastleggen van communicatie tussen personen en apparaten zou de toelichting relevante factoren moeten benoemen die relevant zijn voor de beoordeling van (ingrijpende) stelselmatigheid, en richtinggevende voorbeelden kunnen geven, in de lijn van de hierboven gedane suggesties. → *p. 203*

6.4. Stelselmatig overnemen van persoonsgegevens uit publiek toegankelijke bronnen

Het conceptwetsvoorstel bevat een regeling voor (wat het conceptwetsvoorstel noemt) "het vastleggen van persoonsgegevens uit open bronnen". De voorgestelde regeling luidt als volgt:

Artikel 2.8.2.4.1

1. In geval van verdenking van een misdrijf waarop naar de wettelijke omschrijving gevangenisstraf van een jaar of meer is gesteld, kan de officier van justitie bevelen dat een opsporingsambtenaar stelselmatig, met een technisch hulpmiddel, persoonsgegevens uit open bronnen vastlegt.

2. Het bevel tot stelselmatige vastlegging van persoonsgegevens uit open bronnen wordt gegeven voor een periode van ten hoogste drie maanden. De geldigheidsduur kan telkens voor een periode van ten hoogste drie maanden worden verlengd.

3. Bij of krachtens algemene maatregel van bestuur worden regels gegeven omtrent:
a. de autorisatie van de opsporingsambtenaren die kunnen worden belast met de uitvoering van het bevel, bedoeld in het eerste lid;
b. de geautomatiseerde vastlegging van gegevens over de uitvoering van het bevel, bedoeld in het eerste lid.

6.4.1. Inleiding – relatie tussen opsporing en andere politietaken

Gelet op de opdracht van de commissie en de reikwijdte van het Wetboek van Strafvordering, bespreken we hier het doen van onderzoek in en het stelselmatig overnemen van gegevens[205] uit publiek toegankelijke bronnen (met name internetbronnen) in situaties waarin er sprake is van een verdenking van een strafbaar feit[206]. Dergelijk onderzoek heeft in de politiepraktijk een bredere toepassing dan alleen binnen de kaders van strafvordering. Immers, ook bij andere taken die de politie uitvoert, worden (persoons)gegevens vanaf het internet overgenomen. De voorbeelden lopen uiteen van het monitoren van online uitingen van wapenvergunninghouders, tot het beoordelen van de risico's rond een voetbalwedstrijd, het monitoren ter beveiliging van grote evenementen, het verkrijgen van een informatiepositie ten behoeve van terrorismebestrijding, het controleren van de achtergrond van vluchtelingen en de invulling van de hulpverleningstaak (zoals vermissingen en dreigen met zelfdoding).

De grondslag die hiervoor wordt gehanteerd zijn de algemene taakstellende artikelen. Bij gebreke van een specifieke wettelijke grondslag betekent dit dat het onderzoek moet worden beëindigd zodra de drempel van de "meer dan geringe inbreuk" in beeld komt.

In de huidige praktijk worden allerlei maatschappelijke vraagstukken bij de politie neergelegd, zonder dat in de wet voorzien is in een passend bijbehorend juridisch kader. In dit rapport wordt alleen geadviseerd over een regeling in het Wetboek van Strafvordering, maar de commissie wijst erop dat de wetgever ook voor het overnemen van persoonsgegevens uit publiek toegankelijke bronnen in het kader van andere politietaken een normerend kader zou moeten stellen, dat bij voorkeur zo veel mogelijk zou moeten aansluiten bij de terminologie en voorwaarden die binnen strafvordering worden gehanteerd.

Het is wenselijk op relatief korte termijn een wettelijke regeling te treffen voor het overnemen van persoonsgegevens uit publiek toegankelijke bronnen in het kader van zowel de strafrechtelijke handhaving van de rechtsorde als de overige politietaken, aangezien er momenteel de nodige onduidelijkheid, en daarmee rechtsonzekerheid, bestaat over wat precies onder publiek toegankelijke bronnen moet worden verstaan en onder welke voorwaarden een eventuele meer dan geringe inbreuk zou mogen plaatsvinden.

Aanbeveling 52: de commissie adviseert de wetgever voor de taken van de politie die niet vallen onder de regeling in Strafvordering een bredere regeling te treffen die een grondslag biedt voor het overnemen van persoonsgegevens uit publiek toegankelijke bronnen. Daarbij zouden in ieder geval zoveel mogelijk vergelijkbare terminologie en (bij soortgelijke toepassingen) vergelijkbare voorwaarden als binnen de strafvorderlijke regeling moeten worden gehanteerd. De commissie adviseert bovendien om deze regeling, inclusief het voorliggende artikel uit het wetsvoorstel, snel tot stand te brengen, en niet te wachten tot de inwerkingtreding van het nieuwe Wetboek van Strafvordering.

→ *p. 204*

6.4.2. Definitie en reikwijdte van het begrip "publiek toegankelijke bron"

De definitie

In het hierboven weergegeven artikel is de "open bron" een belangrijk kernbegrip, als aanduiding van het type informatiebron waar deze opsporingsbevoegdheid op ziet. In de memorie van toelichting (p. 245) wordt de volgende omschrijving van het begrip "open bron" gegeven.

[205] De bevoegdheid is beperkt tot het overnemen van persoonsgegevens. Waar in deze par. Stelselmatig overnemen van persoonsgegevens uit publiek toegankelijke bronnen wordt gesproken van het "overnemen van gegevens" wordt in dit verband het overnemen van persoonsgegevens bedoeld.

[206] Of een redelijk vermoeden dat in georganiseerd verband ernstige misdrijven worden beraamd of gepleegd en in geval van aanwijzingen van een terroristisch misdrijf. Zie daarvoor de koppeling met artikel 2.8.6.1.

> Kenmerkend voor een open bron is het feit dat er een onbeperkte kring van personen toegang kan verkrijgen en er geen tussenkomst van een derde nodig is om toegang te verkrijgen. De registratie, het aanmaken van een profiel of de betaling zijn formaliteiten en geschieden vaak volledig geautomatiseerd. Dit in tegenstelling tot besloten of afgeschermde bronnen of websites waarbij bijvoorbeeld een uitnodiging of goedkeuring vereist is om toegang te krijgen. De aard of het doel van de open bron is niet relevant, doorslaggevend is of de open bron door een ieder gebruikt kan worden.

Open bronnen kenmerken zich dus doordat in beginsel eenieder er toegang toe kan verkrijgen en dat voor zover toegang gebonden is aan een account, het verkrijgen van een account een (semi-)geautomatiseerd proces is waarbij niet bepaalde groepen worden uitgesloten van registratie. Open bronnen staan dus tegenover afgeschermde bronnen, die zich kenmerken doordat er een controle plaatsvindt op wie degene is die toegang wil hebben tot de bron.

Hierna zal worden ingegaan op de precieze invulling van het begrip: wanneer is een bron "open", en wanneer niet? Voorafgaand daaraan is het echter noodzakelijk goed te kijken naar de gehanteerde definitie. In de uitvoeringspraktijk, maar ogenschijnlijk ook in het gewone spraakgebruik, is een bepaalde uitleg van de term "open bron" gegroeid die minder specifiek is dan van de regeling die thans wordt voorgesteld. "Open bron" heeft in dat gebruik namelijk geresulteerd in een connotatie van "vrij" of "onbeperkt" om te gebruiken. Dit resulteert in een uitleg dat de politie geen bevoegdheden nodig zou hebben om deze gegevens te verzamelen en (verder) te verwerken. Dit is gezien het voorstel tot een nieuwe bevoegdheid, maar ook gezien het reeds bestaande wettelijk kader voor de taakuitvoering van de politie en de bescherming van de persoonlijke levenssfeer, niet terecht.

Ook buiten de politie is het een vaak gehoord argument dat als iets op internet staat, het door eenieder ongelimiteerd gebruikt kan worden op een wijze waarop men dat zelf wil. Men hanteert daarbij vaak het argument dat het de burger die het betreft immers zelf de heeft gepubliceerd. Dat is niet terecht, om uiteenlopende redenen. Zo worden veel gegevens op het internet gepubliceerd door een ander dan de persoon over wie de gegevens gaan. Bovendien hebben veel mensen, wanneer zij gegevens op het internet zetten, niet de bedoeling om ze daarmee *ongelimiteerd* ter beschikking te stellen aan alle andere mensen op de wereld, waaronder de overheid. Ook worden er gegevens soms niet bewust op internet gezet, maar als onbedoeld gevolg van handelingen die een ander doel hadden. Bijvoorbeeld het delen van locatiegegevens door een hardloop-app. Gegevens kunnen, door ze te combineren met andere gegevens, weer nieuwe informatie opleveren, waar de betrokkene zich ook niet van bewust is. Dit gebeurt vaak door derden, ook commercieel, door partijen waarmee betrokkene geen enkele (rechts)relatie heeft of zelfs maar weet van hun bestaan. Een voorbeeld daarvan is het onder een pseudoniem posten op een forum, dat door het gebruik van dezelfde avatar op een andere website aan je echte identiteit gekoppeld worden. Het enkele feit dat gegevens op internet staan, betekent dus geenszins dat zij doelbewust ongelimiteerd zijn prijsgegeven aan anderen.

Zelfs als iemand wel de intentie heeft om zijn gegevens ter beschikking te stellen aan wie dan ook, dan legitimeert dat nog niet zonder meer het op een structurele en stelselmatige wijze kennisnemen en overnemen daarvan door de politie. Ook daarvoor moet er een gelegitimeerd doel zijn dat binnen de taakstelling valt.

De commissie is dus van oordeel dat de term "open bron" een onbedoelde en ongewenste suggestie in zich heeft als zou een dergelijke bron een rechtenvrije omgeving zijn. De commissie stelt daarom voor de term "publiek toegankelijke bron" te gebruiken, die taalkundig dichter bij de aard van de soort bronnen ligt. Deze term wijst – anders dan de term "open bron", die aan lijkt te sluiten op de juridische status van de gegevens binnen de bron – op de *feitelijke toegankelijkheid* van de gegevens. Dit sluit ook aan bij de benadering in het Cybercrime-verdrag, waar *publicly available* de gebruikte hoofdterm is, en niet de term *open source*. Taalkundig brengt dit inherent een andere notie met zich dan het woord "open". *Publiek*

toegankelijk geeft volgens de commissie beter weer dat er weliswaar geen beperkingen vooraf bestaan wat betreft de feitelijke beschikbaarheid van de gegevens, maar dat het gebruik van de gegevens niet geheel regelvrij is.

Hiermee kan tevens beter onderscheid worden gemaakt tussen enerzijds de feitelijke kwalificatie (namelijk voor het publiek toegankelijk) en anderzijds de kwalificatie *openbaar*, die een juridische component in zich draagt. Een gegeven dat geheel openbaar is, wordt dan gezien als een gegeven dat al geopenbaard is voor het brede publiek. Dit maakt het ook mogelijk om te praten over verschillen tussen intentie en feitelijkheid, iets wat in de huidige praktijk tot spraakverwarring leidt, en wat voor het juridisch gevoel een groot verschil maakt.

Het zou bij gebruikmaking van de nu reeds gebruikte term ("open bron"), bij het introduceren van een nieuwe bevoegdheid met mogelijkheden en beperkingen, moeizaam kunnen zijn dit nieuwe stelsel te laten landen in de uitvoeringspraktijk. Ook om deze reden is een andere term wenselijk. Hiervan zal een belangrijke signaalfunctie uitgaan dat er in het juridisch kader iets veranderd is, hetgeen de uitvoeringspraktijk zal helpen bij de gewaarwording ervan.

Aanbeveling 53: in het conceptwetsvoorstel wordt de term "open bronnen" vervangen door "publiek toegankelijke bronnen". → *p. 203*

Reikwijdte van het begrip

Wanneer is er dan sprake van een "publiek toegankelijke bron", en wanneer niet? De toelichting bij het voorstel geeft hier enig inzicht in, maar roept ook enige afbakeningsvragen op. Voor deze afbakening zijn volgens de commissie enkele te onderscheiden aspecten van belang, waarbij de vraag of in enige mate een beveiliging wordt doorbroken prominent is. Deze paragraaf gaat op dergelijke aspecten in.

In principe zijn alle bronnen die op een geautomatiseerd werk staan dat bereikbaar is vanaf het internet, die gepubliceerd (in geval van een webpagina) of gedeeld (in geval van bestanden delen) zijn en niet voorzien zijn van een beveiliging, publiek toegankelijk. Daarnaast zijn bronnen publiek toegankelijk wanneer er geen effectieve controle plaatsvindt bij het verstrekken van toegang (bijvoorbeeld in geval van chatomgevingen). Er zijn grensgevallen bekend rondom de vraag of het de bedoeling was van de beheerder van die computer dat een bron daadwerkelijk feitelijk toegankelijk is voor het publiek. Denk bijvoorbeeld aan gevallen waarbij informatie gepubliceerd is, maar nog niet aan het publiek bekend is gemaakt door het plaatsen van een hyperlink. Deze informatie kan dan worden gekregen door een slimmigheid die niet bedoeld is door degene die de website maakte. Een inmiddels klassiek voorbeeld is dat je door de URL tweedekamer.nl/miljoennenota2010.html handmatig te wijzigen in tweedekamer.nl/miljoennenota2011.html informatie kunt waarnemen die niet bedoeld was openbaar te zijn, maar in principe voor eenieder (die het trucje kent) toegankelijk is. Een ander voorbeeld is het raadplegen van een hele database door opeenvolgende nummers van records in de URL te zetten. Voor geoefende internetrechercheurs zijn dit soort trucjes bekend, en ze worden ook gedeeld en gepubliceerd in de gemeenschap van journalisten en onderzoekers die zich bezig houden met online gegevensvergaring (vaak aangeduid als de "OSINT community").

De term publiek toegankelijk betekent dus niet dat de pagina te vinden moet zijn door een zoekmachine. Er zijn veel plaatsen op het internet die bijvoorbeeld niet door zoekmachines willen worden geïndexeerd (dit geven zij dan aan in een bestandje robots.txt, dat door crawlers van zoekmachines wordt gelezen), maar wel degelijk voor eenieder toegankelijk zijn. De wens om bepaalde content niet te laten indexeren is dan ingegeven uit praktische of commerciële overwegingen. Een variant hiervan betreft de situatie waar via de gebruikersvoorwaarden van een website is aangegeven dat opsporingsdiensten zich geen toegang mogen verschaffen, maar dat andere personen allemaal welkom zijn. Zo zijn er meer bronnen waar wel staat *vermeld* dat

zij bestemd zijn voor een bepaalde kring van personen, maar waarbij die beperking niet door een *feitelijke toegangscontrole* wordt bewerkstelligd.

Bovenstaande gaat over vraag of de inhoud van een specifieke pagina wel of niet publiek toegankelijk is. Een andere vraag is of een bepaalde pagina (met publiek toegankelijke gegevens) door het publiek gevonden kan worden met bepaalde startinformatie. Een voorbeeld daarvan is "andersom zoeken". Een telefoongids geeft de mogelijkheid om bij een naam een nummer te vinden. Maar een derde die genoeg informatie uit die database heeft kunnen overnemen, kan daarmee de dienst aanbieden dat bij een ingevoerd nummer de naam geeft. Een ander voorbeeld: in het domeinnaamsysteem kun je alleen een domeinnaam opzoeken en dan kennisnemen van de actuele houder van die ene domeinnaam. Maar als een derde partij voldoende informatie uit dit register heeft kunnen opslaan, kunnen ze je bij een houder alle domeinen geven die hij heeft geregistreerd. Of de dienst kan de gegevens van eerdere houders aan je tonen.

Telkens zal moeten worden afgewogen in hoeverre een bron die beschikbaar is voor geautomatiseerde vergaring van gegevens ook daadwerkelijk publiek toegankelijk is. Daartoe biedt de toelichting (p. 245) nu het volgende als richtsnoer.

> Indien tijdens het opsporingsonderzoek bijvoorbeeld een wachtwoord van een emailaccount bekend wordt, maakt dit niet dat de emailaccount daarmee een open bron is geworden. Tot slot kan bij het raadplegen van open bronnen geen sprake zijn van het doorbreken of ontwijken van beveiliging, het aanwenden van technische ingrepen, valse signalen of valse sleutels om toegang te verkrijgen tot de open bron. Dit zijn vormen van afscherming waarmee kennelijk beoogd wordt om de gegevens slechts voor een bepaalde (beperkte) groep personen beschikbaar te stellen.

Hierbij wordt impliciet aangehaakt bij de strafbaarstelling van computervredebreuk in artikel 138ab Sr. Volgens de commissie raakt dit de kern van wat als "publiek toegankelijke bron" gezien kan worden, en het is daarom raadzaam om de link met de in artikel 138ab Sr specifiek genoemde strafbare vormen van computervredebreuk explicieter te maken in de toelichting. Dit verheldert twee aspecten.

Ten eerste wordt hiermee aangehaakt bij het criterium dat in 1993 is gehanteerd voor de strafbaarstelling: computervredebreuk was alleen strafbaar als daarbij "enige beveiliging" werd doorbroken, waarbij is vastgesteld dat dat een "minimum"-niveau van beveiliging is: er moet een minimale vorm van toegangscontrole zijn, die meer is dan een "pro forma"-beveiliging die bestaat uit een bordje "verboden toegang". Dat verklaart waarom bronnen die via robots.txt, Algemene Voorwaarden of beginpagina's voorwaarden stellen aan de toegang ("verboden toegang voor zoekmachines", "geen toegang voor politie", "deze pagina is alleen bestemd voor inwoners van Amsterdam", "Bent u boven de 18? Klik dan hier") maar geen *feitelijke* toegangscontrole hanteren, een publiek toegankelijke bron zijn: ze kennen alleen een "pro forma-beveiliging". Het *deep web* – het gedeelte van het internet dat niet geïndexeerd is door zoekmachines, maar dat wel feitelijk toegankelijk is als je de website bezoekt – is dus ook een publiek toegankelijke bron: het kent als zodanig geen minimaal niveau van beveiliging. Het criterium betekent ook dat bronnen die financiële drempels kennen voor de toegang maar niet anderszins aan toegangscontrole onderworpen zijn, zoals toegang tot LexisNexis, de Kamer van Koophandel of integrale bestanden die op de markt tegen betaling beschikbaar zijn, een publiek toegankelijke bron zijn, ook als de financiële drempel dusdanig is dat niet iedereen het zich zou kunnen veroorloven.

Ten tweede verheldert de koppeling met de strafbaarstelling van computervredebreuk dat het bij het overnemen van gegevens uit publiek toegankelijke bronnen niet primair om een intrinsiek kenmerk van de bron zelf gaat, maar om de *wijze van toegang*. Het betreft 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[207]. Een voorbeeld kan dit verhelderen. Het Kadaster is een bron die, tegen betaling, voor eenieder toegankelijk is. Deze bron geldt echter alleen als publiek toegankelijke bron wanneer de gegevens via de reguliere weg (in het genoemde geval dus tegen betaling) worden verkregen; het verzamelen van gegevens uit een dergelijke bron langs *irreguliere* wegen, bijvoorbeeld door gebruikmaking van een technische truc, valt niet onder het overnemen van gegevens uit publiek toegankelijke bronnen.

Het houdt ook in dat een publiek toegankelijke webpagina waarop iemand onrechtmatig verkregen gegevens (bijvoorbeeld accountgegevens of vertrouwelijke stukken die iemand door hacken heeft verkregen) heeft geplaatst, als publiek toegankelijke bron geldt wanneer deze pagina op een normale wijze wordt bezocht; de politie heeft er immers toegang toe zonder drempel of toegangscontrole. (Dat dit een potentieel grote privacyinbreuk kan betekenen, doet daar niet aan af – de aard van de gegevens is een kwestie die de *normering* van het onderzoek in de publiek toegankelijke bron beïnvloedt, niet de definitie of afbakening ervan.)

Een vergelijkbare redenering is van toepassing op toegang tot gegevens op het *dark web*, het gedeelte van het *deep web* waartoe alleen toegang kan worden verkregen met speciale software, instellingen of autorisatie zoals Tor.[208] Men zou dan kunnen redeneren dat dergelijke software onder een "technische ingreep" valt, en daarmee dat het *dark web* geen publiek toegankelijke bron is. Wij hanteren echter een andere redenering: het feit dat gegevens alleen met bepaalde software toegankelijk zijn, vormt nog geen beveiliging van deze gegevens in de zin dat er enige vorm van toegangscontrole plaatsvindt. Eenieder kan de benodigde software downloaden en gebruiken. In die zin is er geen conceptueel verschil tussen Tor en andere browsers, en tussen het *dark web* en het geïndexeerde web: de toegang vindt niet plaats door een technische *ingreep* (zoals bedoeld in artikel 138ab Sr), maar met een technisch *hulpmiddel* in de maatschappelijke zin van het woord. In feite treedt op het *dark web* dezelfde situatie op als die op het internet bestond voordat er toereikende zoekmachines waren (midden jaren '90). Men moest of het adres van de webpagina of service weten of er komen via verzamelpagina's zoals "startpagina".

Daarom valt het overnemen van gegevens uit het *dark web* onder onderzoek in een publiek toegankelijke bron, voor zover de gegevens niet anderszins aan toegangscontrole met een minimale beveiliging onderworpen zijn.

Ook indien websites voor (volledig) gebruik van de site voorschrijven dat je een account aanmaakt, waarna je, net als alle andere gebruikers, de site kunt betreden en kennis kunt nemen van de inhoud daarvan, is er geen sprake van een beveiliging. De inhoud die je kunt zien nadat je bent ingelogd met een "nep-account" is publiek toegankelijk. Daarentegen valt het verkrijgen van toegang tot sociale media via het aanmaken van een nep-account waarmee wordt gepoogd vrienden te worden van verdachte personen, niet onder dit type onderzoek. Daarmee beoog je immers toegang te krijgen tot gegevens die niet voor eenieder toegankelijk zijn, maar enkel voor "vrienden". De onderhavige bevoegdheid kan dan niet worden gebruikt; waar relevant kunnen daarvoor wel andere bevoegdheden, zoals stelselmatig inwinnen van informatie of pseudokoop, worden ingezet.

Aan de hand van het bovenstaande moet dus, voorafgaand aan de inzet van de onderhavige bevoegdheid, worden vastgesteld of de te benaderen bron wel of niet publiek toegankelijk is. Er is geen "tussencategorie"; bij twijfel zal dus de officier van justitie moeten worden geraadpleegd.

Na de vaststelling dat sprake is van een publiek toegankelijke bron, komt men toe aan vragen rondom de omgang met de gegevens in die bron, met name de inbreuk op de persoonlijke levenssfeer. Op die vragen wordt hierna ingegaan.

---

[207] Deze laatste categorie ontbreekt in de toelichting, maar hoort er wel bij. Het hebben van een account of het gebruiken van een zogenaamde internet*nickname* is overigens in zichzelf nog geen valse hoedanigheid.

[208] https://en.wikipedia.org/wiki/Dark_web (laatst geraadpleegd 1 juni 2018).

Aanbeveling 54: in de memorie van toelichting kan de reikwijdte van het begrip "publiek toegankelijke bron" nader worden ingevuld door explicieter aan te knopen bij de strafbaarstelling van computervredebreuk, zoals in bovenstaande omschreven. Daarnaast kan in de memorie van toelichting worden verhelderd dat men in een onderzoek allereerst zou moeten vaststellen of er sprake is van een publiek toegankelijke bron. Pas als dat het geval is en deze bevoegdheid dus in beginsel zou kunnen worden ingezet, komen de afwegingen op het gebied van de inbreuk op de persoonlijke levenssfeer aan de orde.

→ *p. 203*

6.4.3. Stelselmatigheid en de normering van overnemen van gegevens uit publiek toegankelijke bronnen

Beperking tot overnemen[209] van gegevens

De bevoegdheid zoals geformuleerd in het conceptwetsvoorstel ziet enkel op het vastleggen (in de zin van overnemen) van gegevens; het enkel kennisnemen van persoonsgegevens uit publiek toegankelijke bronnen valt er niet onder. Het idee daarbij is dat het kennisnemen van persoonsgegevens uit publiek toegankelijke bronnen mogelijk wel inbreuk maakt op de persoonlijke levenssfeer, maar dat die inbreuk altijd een geringe zal zijn. Het gaat immers, ten eerste, om persoonsgegevens waar eenieder kennis van kan nemen. Ten tweede is bij het kennisnemen door een persoon niet achteraf – zoals bij overnemen het geval is – een volledige reproductie van het waargenomene mogelijk, en zijn er navenant minder risico's van verdere verspreiding van de gegevens zoals die bij overnemen in politiesystemen aanwezig kunnen zijn. De commissie kan zich vinden in dit idee en sluit zich aan bij de beperking van de normering van het onderzoek in publiek toegankelijke bronnen tot het *overnemen* van persoonsgegevens daaruit. Dit sluit ook aan bij de lijn die de commissie heeft uitgezet ten opzichte van de inbreuk die het overnemen van digitale gegevens in politiesystemen oplevert (par. 5.3.3).

Het overnemen van (digitale) gegevens

Hoewel het niet expliciet wordt gesteld, ziet de nieuwe bevoegdheid met name op het overnemen van *digitale* gegevens. Dat geldt sowieso voor het overnemen van gegevens van internet, maar ook voor het inkopen van bestanden die op de markt beschikbaar zijn, zal gelden dat deze gegevens vrijwel altijd in digitale vorm zullen worden verkregen. Denkbaar is dat bestanden worden ingekocht op analoge dragers die op de markt beschikbaar zijn; daarop ziet deze bevoegdheid volgens de commissie niet (dit zal gewoon op basis van artikel 3 PW 2012 kunnen). Alleen wanneer dergelijke analoog overgenomen gegevens zouden worden gedigitaliseerd, zou de bevoegdheid van toepassing worden, als het digitaal overnemen van deze gegevens stelselmatig is; de memorie van toelichting zou kunnen toelichten dat voor die (waarschijnlijk hoogst zelden voorkomende) gevallen dan de schakelbepaling van Hoofdstuk 7 (de omzetting van analoge naar digitale gegevens, zie par. 5.4.1) van analoge toepassing is en de digitaliseringsslag (als deze stelselmatigheid oplevert) dan valt onder het stelselmatig overnemen van gegevens uit publiek toegankelijke bronnen. (Wetssystematisch zou een schakelbepaling kunnen worden opgenomen in artikel 2.8.2.4.1, maar omdat het om hoogst uitzonderlijke situaties gaat, kan volgens de commissie een opmerking in de toelichting volstaan.)

Daarbij moet verder worden opgemerkt dat, mede omdat de commissie adviseert om de clausule "met een technisch hulpmiddel" te herformuleren (par. 6.4.4), de onterechte indruk zou kunnen ontstaan dat de bevoegdheid ook potentieel van toepassing zou kunnen zijn op het "overnemen" van gegevens uit de publieke ruimte. Te denken valt aan het noteren van een kenteken, het noteren van een beschrijving van een zichtbare tatoeage of het maken van een

[209] Zoals in par. 5.3.1 toegelicht, stelt de commissie voor in dit verband de term "overnemen" te gebruiken in plaats van de in het conceptwetsvoorstel gehanteerde term "vastleggen".

foto daarvan, het noteren van straatnaam en huisnummer, het noteren van het merk en opgedrukte teksten van kledingstukken, het fotograferen of anderszins vastleggen van het framenummer van een voertuig, enzovoorts. Ongeacht of het overnemen van gegevens nu op analoge wijze gebeurt (het maken van aantekeningen in een notitieblokje) of op digitale wijze (het maken van foto's of het maken van aantekeningen in een smartphone of laptop), fungeert de publieke ruimte bij deze handelingen niet als "publiek toegankelijke bron" zoals bedoeld in artikel 2.8.2.4.1. Gegevens uit de publieke ruimte worden in de genoemde voorbeelden niet "overgenomen" in de zin van het kopiëren van gegevens uit bestaande bestanden (wat het geval is bij internetbronnen en andere publiek toegankelijke bronnen, zoals op de markt beschikbare gegevensbestanden); ze worden eerder "vastgelegd" in de zin van het *registreren* van gegevens. Dit valt onder de dagelijkse handelingen die op basis van artikel 3 PW 2012 kunnen (blijven) plaatsvinden, dan wel – als bij het vastleggen de drempel van stelselmatigheid wordt gehaald – onder stelselmatige observatie.

Aanbeveling 55: in de memorie van toelichting kan worden verduidelijkt dat de bevoegdheid niet ziet op het inkopen van analoge gegevens (met verwijzing naar de schakelbepaling in geval deze gegevens worden gedigitaliseerd). Ook kan worden verduidelijkt dat de bevoegdheid niet ziet op het overnemen van gegevens uit de publieke ruimte, omdat dit valt onder artikel 3 PW 2012 dan wel onder bevoegdheden die het vastleggen (registreren) van gegevens uit de publieke ruimte normeren, zoals stelselmatige observatie. → *p. 203*

Definitie van "stelselmatig" in deze bepaling

De normering van het overnemen van gegevens uit publiek toegankelijke bronnen wordt gekoppeld aan het "stelselmatig" overnemen van gegevens. De term "stelselmatig" is in het huidige Wetboek van Strafvordering ingevoerd bij de Wet bijzondere opsporingsbevoegdheden, waarbij de nadruk lag op de fysieke wereld; de term dient daarin in belangrijke mate om de ingrijpendheid van ingezette middelen te duiden. Bijvoorbeeld bij stelselmatige observatie, waar duur, intensiteit, plaats, methode en frequentie van de observatie kernelementen zijn in de vaststelling van de stelselmatigheid en de mate waarin de persoonlijke levenssfeer wordt geacht te zijn aangetast. Deze invalshoek is niet altijd goed toepasbaar op de online wereld. Weliswaar is het ook in de online wereld mogelijk om de duur en frequentie als criterium te gebruiken voor de mate waarin een maatregel als inbreukmakend kan worden beoordeeld, maar de uitwerking ervan kan radicaal verschillen. In de online wereld, anders dan doorgaans in een offline omgeving, is het gemakkelijk voor te stellen dat met een korte, eenmalige actie een grote hoeveelheid persoonsgegevens wordt vergaard. Aspecten als duur (tien minuten) en frequentie (eenmalig) spelen dan in het geheel geen rol, terwijl de inbreuk op de persoonlijke levenssfeer substantieel is. Daarom is het belangrijk om nader te bepalen wat onder "stelselmatigheid" in deze nieuwe context kan of moet worden verstaan.

Het conceptwetsvoorstel beoogt met het criterium "stelselmatig" een regeling te treffen voor de vastlegging van gegevens die verder gaat dan de "geringe inbreuk op de persoonlijke levenssfeer" (memorie van toelichting, p. 59). Het vastleggen van persoonsgegevens uit publiek toegankelijke bronnen waarbij niet een meer dan geringe inbreuk op de persoonlijke levenssfeer wordt gemaakt, blijft mogelijk op basis van de taakstellende bepalingen, zoals artikel 3 PW 2012. De aard van de onderzoeksvraag en de aard van de bron zijn van grote invloed op de vraag of van stelselmatigheid sprake zal zijn. Enkele voorbeelden waarin er, behoudens uitzonderlijke omstandigheden, niet snel sprake zal zijn van stelselmatigheid, zijn volgende situaties:

- wanneer na een incident de politie gericht op sociale media zoekt naar mogelijke getuigen van dat incident;

- wanneer de politie algemene informatie wil vergaren over een locatie of buurt en daarbij in beginsel niet uit is op het overnemen van persoonsgegevens;
- wanneer de politie (bijvoorbeeld de wijkagent) contact zoekt met aanspreekpunten van organisaties of zeer actieve buurtbewoners;
- wanneer er onderzoek wordt gedaan op websites van rechtspersonen en sociale-media-pagina's van rechtspersonen;
- wanneer er onderzoek wordt gedaan op de webpagina's van nieuwsmedia, openbare blogs en vlogs die duidelijk bedoeld zijn om gegevens wereldkundig te maken.

Daar waar de taakstellende bepalingen (zoals artikel 3 PW 2012) niet meer voldoende grondslag bieden voor het overnemen van persoonsgegevens, biedt de voorgestelde bepaling de mogelijkheid om, onder nadere voorwaarden, toch gegevens vast te leggen.

In het kader van (stelselmatige) observatie is het criterium "stelselmatig" het sleutelbegrip aan de hand waarvan wordt beoordeeld of er sprake is van een "meer dan geringe inbreuk". Bij de voorliggende nieuwe bepaling voor het vastleggen van persoonsgegevens van het internet is een soortgelijke toepassing beoogd. In de toelichting (p. 246) wordt gesteld:

> Voor het begrip stelselmatig wordt aansluiting gezocht bij het begrip stelselmatig in de bepalingen inzake stelselmatige observatie en stelselmatige inwinning van informatie. Het vastleggen van de persoonsgegevens op het publiek toegankelijke deel van het internet wordt stelselmatig als met de vastgelegde gegevens, na analyse, een min of meer volledig beeld kan worden verkregen van bepaalde aspecten van het persoonlijk leven van betrokkene. (…) Van stelselmatigheid kan ook sprake zijn door bij herhaling geautomatiseerd en methodisch te zoeken in informatiebronnen naar bepaalde persoonsgegevens en de gevonden persoonsgegevens vervolgens vast te leggen. Niet iedere geavanceerde zoekactie waarmee op een geautomatiseerde wijze methodisch en grootschalig gegevens worden gezocht en vastgelegd uit open bronnen, is per definitie stelselmatig. De inzet van dergelijke zoektechnologie om te achterhalen wie op of rond een bepaald tijdstip op of nabij een plaats delict is geweest, kan bijvoorbeeld plaatsvinden op basis van de algemene bevoegdheidsbepaling. Doel noch resultaat van deze gerichte geavanceerde zoekactie is een min of meer volledig beeld van bepaalde aspecten van het persoonlijk leven van betrokkene vast te leggen.

De passage kan enige verwarring wekken omtrent het gehanteerde criterium, omdat naast het inhoudelijke criterium (een min of meer volledig beeld) ook de manier van zoeken (bij herhaling geautomatiseerd en methodisch zoeken) wordt genoemd, een procedureel criterium dat meer aansluit bij de betekenis van "stelselmatig" in het algemene spraakgebruik. Bij nadere beschouwing wordt echter duidelijk dat alleen het inhoudelijke criterium geldt: niet elke vorm van bij herhaling methodisch zoeken is immers "stelselmatig" in juridische zin; dat is alleen het geval als een min of meer volledig beeld van bepaalde aspecten van het persoonlijk leven van betrokkene kan worden verkregen. Dit is in lijn met de manier waarop de wetgever bij de Wet BOB het begrip stelselmatig heeft toegelicht: dat is van toepassing als door de voorgenomen wijze van observatie of inwinnen van informatie een min of meer volledig beeld van bepaalde aspecten van iemands privéleven kan ontstaan.[210] De wijze van zoeken speelt dus wel een rol, maar alleen voor zover deze wijze samenhangt met de factoren (zoals bij observatie de duur, frequentie en intensiteit) die van invloed zijn op de verwachting dat een min of meer volledig beeld kan ontstaan.

Gevolg hiervan is dat de kernvraag is wanneer bij het overnemen van persoonsgegevens uit publiek toegankelijke bronnen een "meer dan geringe inbreuk" plaatsvindt. Het is dan van doorslaggevend belang dat nadere invulling wordt gegeven aan de factoren die van invloed zijn op de verwachting dat een min of meer volledig beeld van aspecten van iemands privéleven kan ontstaan.

[210] *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 26.

Aanbeveling 56: de toelichting moet verduidelijken dat, voor de beoordeling of sprake is van "stelselmatigheid", het inhoudelijke criterium wordt gehanteerd van het "min of meer volledige beeld", en niet de manier van zoeken. → *p. 194*

Gaat het om de verwachting vooraf of het resultaat achteraf?

Een belangrijke vraag voor de praktijk is de vraag op welk moment beoordeeld moet worden of er sprake is of kan zijn van een meer dan geringe inbreuk. Moet dat voorafgaand aan het moment waarop je gegevens gaat overnemen? Of tijdens het overnemen, wanneer geconstateerd wordt dat het beeld stelselmatig kan worden? Of op het moment dat de gegevens verzameld en geanalyseerd zijn en blijkt dat er een min of meer volledig beeld is verkregen van aspecten van het persoonlijke leven?

De vraag wat als "stelselmatig" gezien moet worden, moet worden beoordeeld aan de hand van de informatie die *vooraf* beschikbaar is: het gaat erom dat de privacyinbreuk redelijkerwijs voorzienbaar is. Dat blijkt (impliciet) uit de toelichting: "Het vastleggen van de persoonsgegevens op het publiek toegankelijke deel van het internet wordt stelselmatig als met de vastgelegde gegevens, na analyse, een min of meer volledig beeld *kan worden verkregen* van bepaalde aspecten van het persoonlijk leven van betrokkene" (memorie van toelichting, p. 246, cursivering toegevoegd).

De toelichting is echter niet eenduidig. Elders valt te lezen: "bij de stelselmatige observatie (…) kan op grond van de algemene taakstellende bepalingen – en in de toekomst op basis van de algemene bevoegdheidsbepaling – geobserveerd worden en is een bevel van de officier van justitie pas noodzakelijk indien de observatie een stelselmatig karakter *krijgt*" (memorie van toelichting, p. 60, cursivering toegevoegd). Dit suggereert dat de beoordeling van stelselmatigheid pas gaande de uitvoering zou plaatsvinden, op het moment dat een opsporingsambtenaar merkt (of zou moeten merken) dat de handeling op dat moment een meer dan geringe inbreuk oplevert.

Volgens de commissie is dat niet de bedoeling van het wettelijke systeem. De inzet van bevoegdheden wordt altijd vooraf bepaald en genormeerd: de bevoegde autoriteiten beoordelen of de middelen die zij *willen gaan* inzetten onder een bepaalde bevoegdheid vallen en of aan de voorwaarden van die bevoegdheid is voldaan. Bij de uitvoering kan vervolgens blijken dat aan een voorwaarde niet, of niet meer, is voldaan, bijvoorbeeld als bij een netwerkzoeking (artikel 125j Sv) in een geautomatiseerd werk op afstand wordt gezocht en bestanden worden vastgelegd waarvan de opsporingsambtenaar verwacht, op basis van de bestandsnamen, dat die "redelijkerwijs nodig zijn om de waarheid aan de dag te brengen" en bij opening van een bestand blijkt dat het geen relevante informatie voor het onderhavige onderzoek bevat. Voor dergelijke gevallen gelden soms specifieke regels (zoals in dit geval: vernietigen van het bestand zodra blijkt dat het geen betekenis heeft voor het onderzoek, artikel 125n, eerste lid, Sv) of algemene regels (zoals het kunnen doorrechercheren op bijvangst, maar ook het verbod op *détournement de pouvoir*: de bevoegdheid mag niet zijn ingezet in de hoop bijvangst te krijgen). Soms blijkt tijdens de uitoefening van een bevoegdheid (bijvoorbeeld op grond van de taakstellende artikelen) dat een zwaardere bevoegdheid nodig is; die moet alsdan worden aangevraagd, al kan in urgente gevallen soms alvast met de uitoefening worden begonnen. Dat zijn uitzonderingsgevallen: in de regel wordt de inzet van bevoegdheden vooraf bepaald. De vraag of bij onderzoek in een publiek toegankelijke bron sprake is van stelselmatigheid, moet dan ook steeds op voorhand worden beantwoord, aan de hand van op dat moment beschikbare informatie en de beoogde inzet van het middel, met inachtneming van de ervaringen met resultaten van de inzet van een dergelijk middel in eerdere gevallen. Bij twijfel zou de opsporingsambtenaar ervoor kunnen kiezen om eerst een oppervlakkige zoekslag te maken, om een eerste beeld te krijgen van wat een uitgebreide zoekslag op zou kunnen leveren.

Ook bij uitoefening van deze methode kan het echter voorkomen dat op voorhand niet te voorzien is dat een min of meer volledig beeld van bepaalde aspecten van iemands privéleven ontstaat, maar dat dit wel blijkt te gebeuren gedurende de uitoefening. Op dat moment zou de zoekactie (op basis van het taakstellend artikel) moeten stoppen, waarbij de gevonden informatie naar huidig recht als bijvangst kan worden gebruikt. Daarbij moet wel worden aangetekend dat bij het stelselmatig overnemen van gegevens uit publiek toegankelijke bronnen vaak minder tussenstappen in het onderzoeksproces mogelijk zijn. Dit kan betekenen dat pas op een later moment dan bij klassiek rechercheren het geval zou zijn duidelijk wordt dat de grens van stelselmatigheid nabij komt of mogelijk zelfs al is bereikt. De beoordeling zou in dat licht dus moeten plaatsvinden op het proces, niet het resultaat, waarbij dat proces zodanig ingericht zou moeten zijn dat naar redelijke verwachting voldoende herijkingspunten in het onderzoeksproces zitten om op tijd te kunnen constateren of stelselmatigheid is bereikt of bereikt zal gaan worden.

Is eenmaal vastgesteld dat de grens van stelselmatig overnemen is bereikt en het wenselijk is om op dezelfde voet door te gaan met zoeken in publiek toegankelijke bronnen, dan moet op dat moment een bevel van de officier van justitie worden aangevraagd en aan de overige voorwaarden van het stelselmatig overnemen van persoonsgegevens uit publiek toegankelijke bronnen worden voldaan. Tot slot komt, indien de zonder gebruikmaking van een specifieke bevoegdheid uit een publiek toegankelijke bron verkregen gegevens gebruikt worden in een concrete strafzaak, onder de huidige regeling aan de rechter (achteraf) wettelijk het oordeel toe of de toepassing van de opsporingsmethode rechtmatig is geweest. Daarbij is niet alleen het daadwerkelijke resultaat van de inzet beslissend, maar vooral ook het resultaat dat daarvan op voorhand redelijkerwijs mocht worden verwacht.[211]

Aanbeveling 57: de toelichting moet verduidelijken dat vooraf een inschatting moet worden gemaakt en vastgelegd over de te verwachten inbreuk op de persoonlijke levenssfeer, en tevens moet de toelichting handvatten geven over hoe die inschatting gemaakt kan worden (zie "Hoe geef je invulling aan de (vooraf te vervullen) toets op de mate van inbreuk?" hieronder). De toelichting moet daarbij ingaan op het leerstuk van bijvangst in het kader van de bevoegdheid tot het overnemen van persoonsgegevens uit publiek toegankelijke bronnen. → *p. 194*

De inzet van crawlers

Bijzondere aandacht hierbij verdient de materie van het (grootschalig) "crawlen" van het internet. Een crawler is een geautomatiseerd proces dat binnen gestelde condities (zoals welke bronnen moeten worden doorzocht en op welke woorden of andere zoektermen moet worden doorzocht) al dan niet met gebruik van inloggegevens, als ware hij een gewone gebruiker, contact maakt met bronnen die via het internet toegankelijk zijn. De werking is afhankelijk van het type bron. Wanneer het gaat om webpagina's, zullen deze worden geladen en worden de daarop vastgelegde gegevens vergeleken met de zoekcriteria. De webpagina's die niet voldoen aan de criteria, worden niet opgeslagen. Wat wel voldoet aan de criteria wordt overgenomen (vastgelegd in een politiesysteem). Maar als het bijvoorbeeld gaat over het zoeken in chatomgevingen, dan zal geautomatiseerd verbinding worden gemaakt met een chat-server en daar aangemeld worden op een kanaal om vervolgens alle gesprekken in dat kanaal te volgen en eventueel te selecteren welke gesprekken eruit moeten worden opgeslagen (bijvoorbeeld alleen de gesprekken die plaatsvinden tijdens de aanwezigheid van het subject). Een andere manier om geautomatiseerd informatie te vergaren uit publiek toegankelijke bronnen is door gebruik te maken van een speciale interface die een platform, zoals Twitter, zelf aanbiedt. Er worden

[211] Zie bijvoorbeeld HR 13 november 2012, ECLI:NL:HR:2012:BW9338, NJ 2013/413, m.nt. Borgers en ECLI:NL:PHR:2015:1029 (gevolgd door HR in ECLI:NL:HR:2015:1815) over observatie.

dan vragen gesteld via de zogenaamde API (Application Programming Interface). De informatie die daarop terugkomt wordt geselecteerd op relevantie en de selectie wordt vastgelegd. In de overgenomen informatie kunnen zodanige persoonsgegevens zitten dat er sprake is van stelselmatigheid.

De inzet van een crawler kan enerzijds, wanneer de crawler wordt voorzien van beperkingen, de inbreuk op de persoonlijke levenssfeer beperken, met name bij een korte loopduur. Anderzijds is de gecompliceerdheid of fijnmazigheid van de vooraf te maken inschatting over de te verwachten privacyinbreuk moeilijk te verwerken in een crawler. Ook is tussentijdse aanpassing naar bevind van zaken nauwelijks mogelijk. Bovendien is het mogelijk dat zelfs indien vooraf beperkingen aan een crawler worden meegegeven, bij langere loopduur de uiteindelijke datasets niet veel afwijken van onbeperkte crawlers; dit zal mede afhangen van het gebruikte type crawler. De commissie adviseert hierop in de toelichting bij het conceptwetsvoorstel nader in te gaan. Daarbij dient, in het kader van de vereisten van proportionaliteit en subsidiariteit, ingegaan te worden op de inspanningsverplichting om de crawler te beperken wanneer dat technisch mogelijk is.

Indien crawlers op basis van het onderhavige artikel ingezet kunnen worden, is vooraf beoordeling nodig van de mate van privacyinbreuk die redelijkerwijs voorzienbaar is bij het vergaren van gegevens met de crawler. Daarop is het stelselmatigheidscriterium van toepassing. Indien vervolgens bij het zoeken in de vergaarde dataset wordt vastgesteld dat sprake is van een grotere privacyinbreuk dan was voorzien, moet de crawler bij hernieuwde inzet worden aangepast dan wel toestemming van de juiste autoriteit worden gevraagd.

De voorgaande tekst gaat over de inbreuk op de persoonlijke levenssfeer die plaatsvindt door het *overnemen* van persoonsgegevens. Voorafgaand aan het overnemen van persoonsgegevens worden door de crawler echter grote hoeveelheden gegevens doorzocht op relevantie. Een bijzonder aspect aan de inzet van een crawler is dus dat er ook een (kleine) inbreuk op de persoonlijke levenssfeer plaatsvindt ten aanzien van de personen wier gegevens door de crawler zijn onderzocht, maar niet zijn overgenomen. Het betreft gegevens die op een in beginsel onbeperkte hoeveelheid plaatsen op het internet kunnen worden aangetroffen. Hier is dus, in de terminologie van paragraaf 5.3.3, geen sprake van kennisnemen of overnemen, maar van een zekere vorm van geautomatiseerd onderzoek zonder dat het desbetreffende gegeven ooit door de ogen van een agent worden gezien of ooit wordt opgeslagen op een politiesysteem.

De inbreuk op de persoonlijke levenssfeer die wordt gemaakt met het geautomatiseerd doorzoeken van publiek toegankelijke internetgegevens is van een andere aard[212] dan bij de eerder genoemde inbreuken die samenhangen met de gegevens betreffende specifieke personen of strafbare feiten. Hier is sprake van onderzoek dat zich richt op een gegevensverzameling die in beginsel niet in een rechtstreeks verband staat tot het strafbare feit of de onderzochte persoon (vaak de verdachte), maar tegelijkertijd wel veel gegevens bevat over personen die eveneens niet in relatie staan tot enig strafbaar feit. Bij geautomatiseerd internetonderzoek is vaak pas bij het overnemen van de door de crawler als relevant beoordeelde gegevens sprake van een afbakening van de gegevens in relatie tot een verdachte of een strafbaar feit.

In de bestaande en voorgestelde regelgeving, maar ook in dit rapport, worden onderzoeksbevoegdheden en de inzetvoorwaarden gekoppeld aan de mate van inbreuk op de persoonlijke levenssfeer van *specifieke personen*. Er is echter geen regeling voor inbreuken die niet ten aanzien van specifieke personen plaatsvinden, maar op bovengenoemde wijze betrekking hebben op niet-afgebakende groepen. Daarnaast is van belang dat de bevoegdheden ten aanzien van gegevensdragers en geautomatiseerde werken de handelingen normeren onder de noemer van het doen van "onderzoek" aan de gegevens, waarbij onderzoek in elk geval omvat het

[212] Deze andersoortige inbreuk komt dus ook niet "tussen" de geringe inbreuk en de meer dan geringe inbreuk op iemands persoonlijke levenssfeer in te staan; het gaat om een ander type inbreuk.

"kennisnemen" en "overnemen" van gegevens. Bij het onderhavige artikel wordt specifiek het "overnemen" van persoonsgegevens gereguleerd, en niet het (daaraan voorafgaande) geautomatiseerde (door)zoeken van internetgegevens. Dit roept de vraag op of het geautomatiseerd *doorzoeken* van internetgegevens, zonder dat deze worden overgenomen, specifieke regeling behoeft.

De beperking van de regeling tot *overnemen* is volgens de commissie verklaarbaar door de aard van de gegevensbronnen. Bij de onderhavige bevoegdheid is het aangrijpingspunt de *publiek toegankelijke bron*, waarbij de feitelijke toegankelijkheid voor eenieder een doorslaggevend criterium is. De feitelijke toegankelijkheid is een startpunt, en het daadwerkelijk verschaffen van *toegang* tot de gegevens (en dus nog niet het kennisnemen of overnemen) met als uiteindelijk doel het (wel genormeerde) overnemen van gegevens, is voor de commissie reden om de daarmee gepaard gaande inbreuk op de persoonlijke levenssfeer als gering te bestempelen. Een precedent hiervoor kan gevonden worden bij het toepassen van ANPR (Automatic Number Plate Recognition). Daarbij was bepaald dat het geautomatiseerd scannen van de kentekengegevens en het daaruit enkel *overnemen* van de hits (dus de gezochte kentekens) was toegestaan op basis van de bestaande regelgeving, namelijk artikel 3 PW 2012. De inbreuk op de persoonlijke levenssfeer van de eigenaars van de niet-overgenomen kentekens (de no-hits) werd als klein beschouwd. Door het toenmalige College Bescherming Persoonsgegevens is in 2012 vastgesteld dat er voor het in brede zin *overnemen* van de no-hits geen wettelijke grondslag bestond. Daarvoor is vervolgens een wetsvoorstel tot stand gebracht, om alsnog in die wettelijke grondslag te voorzien. Daarmee is primair gekozen voor het regelen van het breed *overnemen* van alle kentekengegevens die bepaalde geselecteerde camera's passeren. De reeds bestaande toepassing, namelijk het *scannen* van kentekens voorafgaand aan het vastleggen (van enkel de hits) kon, en kan nog steeds, vallen onder artikel 3 PW 2012. Er is dus geen specifieke regeling nodig geacht voor het scannen (zonder overnemen) van de kentekengegevens.

Ook in het voorgestelde artikel (2.8.2.4.1) in het conceptwetsvoorstel wordt het stelselmatig *vastleggen* (in onze terminologie: overnemen) van persoonsgegevens uit publiek toegankelijke bron als aanknopingspunt gekozen, en niet het daaraan voorafgaande *doorzoeken* van de publiek toegankelijke bron. In de nieuwe Wet op de inlichtingen- en veiligheidsdiensten 2017 is eveneens het stelselmatig *verzamelen* van gegevens uit open bron geregeld; ook daar ziet de regeling dus op het overnemen van gegevens, niet op de fase daaraan voorafgaand.

De commissie is om deze redenen van oordeel dat tijdens de fase van het geautomatiseerd doorzoeken van publiek toegankelijke internetgegevens, voorafgaand aan de fase van het kennisnemen of overnemen van die gegevens, geen sprake is van een meer dan geringe inbreuk op de persoonlijke levenssfeer, en dat dit dus toegestaan is op basis van de taakstellende artikelen. De commissie beveelt aan dit expliciet te benoemen in de toelichting op het wetsvoorstel.

Aanbeveling 58: in de toelichting moet in het kader van de inzet van crawlers nader worden ingegaan op de voorzienbaarheid van de privacyinbreuk, proportionaliteit en subsidiariteit, in relatie tot de wijze van inrichting van de crawler (zoals loopduur, zoekbereik en andere aangebrachte beperkingen). De commissie beveelt tevens aan dat in de toelichting expliciet wordt gemaakt dat bij de inzet van crawlers in de fase van het (geautomatiseerd) doorzoeken van internetgegevens, voorafgaand aan het overnemen van de gegevens, geen sprake is van een meer dan geringe inbreuk. → *p. 203*

Hoe geef je invulling aan de (vooraf te vervullen) toets op de mate van inbreuk?

Zoals geconstateerd, zijn de in het kader van stelselmatige observatie ontwikkelde factoren voor de klassieke invulling van "stelselmatigheid", zoals duur, frequentie en plaats, lang niet altijd even relevant bij de bepaling van de mate van inbreuk van internetonderzoek. Dit wordt ook in

de memorie van toelichting erkend, waarin enkele aanknopingspunten worden gegeven voor de relevante factoren:

> het verschil zit vooral in de *wijze van zoeken*, de *hoeveelheid* gegevens waarin gezocht kan worden en de *geavanceerde manier* waarop resultaten vastgelegd worden. (…) Ook kunnen in korte tijd *veel meer* en *meer diverse* gegevens doorzocht worden *dan handmatig* in dezelfde tijd en met dezelfde omvang ooit mogelijk zou zijn. [p. 59]
>
> Afhankelijk van de *te gebruiken zoektechnologie*, *het doel* van de zoekactie en *de hoeveelheid en aard* van de historische persoonsgegevens die in open bronnen worden gedeeld, kan daardoor bij een *geavanceerde* éénmalige vastlegging van gegevens al sprake zijn van stelselmatigheid doordat in de gevonden gegevens een min of meer volledig beeld besloten ligt van bepaalde aspecten van het persoonlijk leven van betrokkene. [p. 246]

Het is voor de praktijk wenselijk om deze factoren meer systematisch op een rijtje te zetten. De factoren die van invloed zijn op de vraag of het overnemen van persoonsgegevens uit publiek toegankelijke bronnen naar verwachting stelselmatig zal zijn, zijn volgens de toelichting:

- de hoeveelheid gegevens;
- de aard van de gegevens;
- de diversiteit van gegevens;
- de geavanceerdheid van het gebruikte technisch hulpmiddel (handmatig zoeken met een klassieke zoekmachine, of geautomatiseerd zoeken en combineren van gegevens, of geautomatiseerde veredeling van gegevens?);
- het doel van de zoekactie (gericht op vastlegging van enkele simpele feiten, of breder);
- de manier van zoeken (persoonsgericht en beperkt, of niet gericht op specifieke personen en beperkt; tegenover: persoonsgericht en diep; niet gericht op specifieke personen maar diep).

Dit is een nuttige lijst die al veel relevante factoren omvat. Volgens de commissie kan deze lijst echter nog worden uitgebreid en verfijnd, alsook duidelijker geclusterd. Met aanvullingen van de commissie zijn de volgende clusters factoren relevant:

1) Omvang en type van de (over te nemen) gegevens:

- de hoeveelheid gegevens;
- de aard van de gegevens;
- de diversiteit van gegevens;
- deze factoren hangen mede samen met de mate waarin vooraf bekend is hoeveel en hoe de persoon zich manifesteert in publiek toegankelijke bronnen (in de praktijk: op het internet).

2) Aard van de bron:

- de aard van de locatie waarop de gegevens te vinden zijn; sommige bronnen zijn naar hun aard zeer openbaar (de krant), andere helemaal niet (de inhoud van privé-opslagruimte die toevallig niet beveiligd was);
- de menselijke bron van de gegevens (heeft de betrokkene deze zelf op internet geplaatst, of hebben anderen dat gedaan?);
- het doel waarmee de gegevens in eerste instantie zijn vergaard of gepubliceerd; is bijvoorbeeld expliciet of, gezien de context, impliciet duidelijk dat de gegevens op internet zijn geplaatst met het oog op brede verspreiding, of juist niet met het oog op kennisneming door een brede of onbeperkte kring;
- de plaats van de gegevens (welke privacyverwachting bestaat bij de locatie van de gegevens: staan ze direct zichtbaar op een platform met een breed publiek, of op een obscure webpagina?);
- de feitelijke bekendheid van de gegevens (zijn de gegevens in een brede groep verspreid? Als het gevoelige gegevens betreft, is dit de eerste openbaarmaking? Of zijn er (inmiddels) vele bronnen die er mededeling over hebben gedaan?)

3) Wijze van zoeken:
- de geavanceerdheid van het gebruikte technisch hulpmiddel (handmatig zoeken met een klassieke zoekmachine, of geautomatiseerd zoeken en combineren van gegevens, of geautomatiseerde veredeling van gegevens?);
- het doel van de zoekactie (gericht op het overnemen van enkele simpele gegevens, of breder);
- de manier van zoeken (persoonsgericht en beperkt, of niet gericht op specifieke personen en beperkt; tegenover: persoonsgericht en diep; niet gericht op specifieke personen maar diep);
- de specificiteit van de zoekvraag (wordt een algemene of heel specifieke vraag gesteld, wordt de zoekvraag op voorhand toegespitst aan de hand van reeds in een onderzoek bekende gegevens, en gaat het om "gesloten vragen" of om "open vragen"? Dit hangt samen met de manier van zoeken, maar is niet hetzelfde);
- de samenhang tussen de zoekvraag en het onderhavige strafbare feit (is de zoekvraag direct en specifiek gericht op dit feit, of breder?).

4) Het gebruik van gegevens en de mogelijke impact op de persoon:
- de mate waarin (door een crawler of opsporingsambtenaar onderzochte) gegevens worden overgenomen en de selectiviteit die daarbij wordt gehanteerd (worden gegevens alleen beperkt en gericht overgenomen in politiesystemen, of is er juist sprake van een brede en weinig selectieve overneming van wat is aangetroffen?);
- de in het onderzoek reeds bekende informatie (hoeveel steentjes zal de zoekactie toevoegen aan het reeds bestaande beeld?);
- de combinatie van gegevens uit verschillende bronnen (bijvoorbeeld het combineren van internetzoekresultaten met op de markt ingekochte bestanden met persoonsgegevens).

De commissie is zich ervan bewust dat de veelheid van relevante aspecten en het brede spectrum van de mate van inbreuk in concrete gevallen kan leiden tot lastige afwegingen voor de opsporingsambtenaar en de officier van justitie. Dit is echter inherent aan de diversiteit van bronnen op het internet. Er is zoveel informatie over zoveel aspecten van de levens van zoveel personen, informatie die op zoveel verschillende wijzen te benaderen valt, allemaal vanuit het kantoor van de opsporingsambtenaar, dat dit zich niet laat vatten in een beperkte set aspecten die meegewogen moeten worden. De commissie heeft nagedacht over het hanteren van een kortere lijst aspecten, maar heeft daar van afgezien omdat dit een te grofmazig afwegingskader zou opleveren, dat in voorkomende gevallen teveel ten koste van de rechtsbescherming zou kunnen gaan.

Bij al de genoemde factoren gaat het om de redelijke voorzienbaarheid *vooraf*. Niet alles is daarbij even goed te voorzien: de manier van zoeken kan vanzelfsprekend wel vooraf worden bepaald (en vervolgens weer aangepast afhankelijk van de uitkomsten van het begin van de zoekactie), maar de hoeveelheid, de plaats en de aard van gegevens die in beeld komen zullen niet altijd vooraf goed kunnen worden ingeschat. De opsporingsambtenaren zullen moeten afgaan op wat reeds bekend is over de persoon en over diens manifestatie op internet, en vervolgens op basis van algemene ervaringsregels moeten inschatten of de voorgenomen zoekvragen met enige waarschijnlijkheid kunnen leiden tot een min of meer volledig beeld van bepaalde aspecten van iemands privéleven. In twijfelgevallen zou het uitgangspunt moeten zijn dat aan de voorwaarden van stelselmatig overnemen van persoonsgegevens uit publiek toegankelijke bronnen moet worden voldaan en een bevel worden aangevraagd, zoals ook de toelichting (p. 60) aangeeft. Een andere mogelijkheid is dat de opsporingsambtenaar ervoor kiest om eerst een oppervlakkige zoekslag te maken, om een eerste beeld te krijgen van wat een

uitgebreide zoekslag op zou kunnen leveren. Hierbij zal hoe dan ook moeten worden geaccepteerd dat deze afweging – achteraf gezien – soms onjuist zal blijken te zijn geweest.

Aanbeveling 59: de memorie van toelichting moet explicieter handvatten bieden voor de factoren die van invloed zijn op "stelselmatigheid", door een uitgebreider en inzichtelijker overzicht te bieden van deze factoren. De boven genoemde factoren kunnen daarvoor als leidraad dienen. → *p. 203*

6.4.4. Technisch hulpmiddel

In het conceptwetsvoorstel wordt de bevoegdheid gedefinieerd als met een technisch hulpmiddel persoonsgegevens uit open bronnen vastleggen. Het is echter onwenselijk om dit onderzoek te beperken tot het overnemen "met een technisch hulpmiddel". Hierdoor lijkt de bevoegdheid immers beperkt tot "zoeken op internet", waarbij meer of minder geavanceerde zoekprogramma's worden gebruikt. Onder het stelselmatig overnemen van persoonsgegevens uit publiek toegankelijke bronnen valt echter ook het verzamelen van gegevens uit andere dan direct toegankelijke internetbronnen, bijvoorbeeld van bestanden die tegen betaling op de markt verkrijgbaar zijn. Het inkopen van publiek beschikbare bestanden valt niet onder het gebruik van een "technisch hulpmiddel". Dit moet echter wel onder de voorgestelde bevoegdheid vallen, omdat deze bestanden – afhankelijk van aard en omvang – ook een min of meer volledig beeld van iemands privéleven kunnen opleveren. Daarnaast kan het juist ook de combinatie van internetgegevens en gegevens uit andere publiek beschikbare bestanden zijn die tot stelselmatigheid leidt.

Daarom zou het gebruik van een technisch hulpmiddel niet in de definitie van de bevoegdheid moeten staan. Omdat het wel wenselijk is om eisen te kunnen stellen – vooral met het oog op de integriteit en authenticiteit van de overgenomen resultaten – kan beter een zin worden toegevoegd aan lid 1: "Hierbij kan gebruik worden gemaakt van een geautomatiseerde wijze van overnemen. Bij algemene maatregel van bestuur kunnen eisen worden gesteld aan deze wijze van overnemen." Het voorgestelde artikel 2.8.1.5.1 (huidig artikel 126ee Sv) is dan niet van toepassing bij deze bevoegdheid. De commissie acht het in plaats daarvan wel noodzakelijk dat er eisen (kunnen) worden gesteld aan de wijze van overneming, in verband met de integriteit en authenticiteit van de overgenomen gegevens. Dit is onder meer van belang voor de toetsbaarheid en *equality of arms* in een eventueel strafproces. In dit verband is ook de bredere discussie relevant over de toepassing van het Besluit technische hulpmiddelen op software (zie daarover par. 6.6).

Aanbeveling 60: artikel 2.8.2.4.1, eerste lid, wordt aangepast door herformulering van de voorwaarde "met een technisch hulpmiddel". → *p. 203*

6.4.5. Normering

Het aanknopingspunt voor de bevoegdheid is het omslagpunt tussen niet-stelselmatig en stelselmatig overnemen van persoonsgegevens uit publiek toegankelijke bronnen. In lijn met de gekozen benadering van een driedeling voor de normering van het onderzoek van gegevens in of overgenomen uit geautomatiseerde werken of digitale-gegevensdragers (zie par. 4.2 en 5.3.3), stelt de commissie ook bij de bevoegdheid tot overnemen van persoonsgegevens uit publiek toegankelijke bronnen een getrapt stelsel van toestemmingsvereisten voor:

- niet-stelselmatig overnemen kan plaatsvinden door opsporingsambtenaren;
- voor stelselmatig overnemen is een bevel officier nodig;
- ingrijpend stelselmatig overnemen vergt een machtiging van de rechter-commissaris.

Voor stelselmatig overnemen geldt in het conceptwetsvoorstel een verdenkingscriterium van een misdrijf waarop minimaal een jaar gevangenisstraf is gesteld en is een bevel van de officier

van justitie nodig. Dat is in lijn met andere bevoegdheden, zoals stelselmatige observatie en stelselmatige inwinning van informatie, al geldt voor de laatstgenoemde bevoegdheid een hoger verdenkingscriterium.

Ook bij het overnemen van persoonsgegevens uit publiek toegankelijke bronnen kan echter diep in iemands persoonlijk leven worden gekeken, gegeven wat er allemaal op internet (en in publiek beschikbare bestanden) over personen te vinden is. De toelichting stelt dat zelf ook: "Met persoonsgegevens uit open bronnen kunnen opsporingsinstanties zich snel een vrij volledig en accuraat beeld vormen van een persoon, zowel in het heden als het verleden." (memorie van toelichting, p. 59) Het overnemen van persoonsgegevens uit publiek toegankelijke bronnen zal in de meeste gevallen minder ingrijpend zijn dan onderzoek in geautomatiseerde werken of onderzoek van communicatie. Maar dit hoeft niet altijd zo te zijn.

De vraag moet daarom worden gesteld of er ook nadere normering nodig is voor gevallen waarin in redelijkheid voorzienbaar een ingrijpende inbreuk op iemands privacy plaatsvindt. De commissie ziet qua potentiële privacyinbreuk in beginsel geen verschil tussen verschillende typen van het vergaren van verzamelingen van gegevens; het hangt in principe van het concrete geval af hoe groot de privacyinbreuk van de inzet van een bepaalde bevoegdheid naar verwachting zal zijn. Bij het overnemen van persoonsgegevens uit publiek toegankelijke bronnen zijn de te onderzoeken gegevens naar hun aard echter wel anders dan bij de inzet van andere bevoegdheden; het betreft immers gegevens die feitelijk reeds voor eenieder toegankelijk zijn. Zoals eerder gezegd, betekent dit niet dat de gegevens onbeperkt gebruikt mogen worden. Het betekent echter wel dat een *ingrijpende* inbreuk op de persoonlijke levenssfeer niet snel zal plaatsvinden door het doen van onderzoek in de desbetreffende bron door de opsporingsinstantie. Die ingrijpende inbreuk heeft in beginsel al plaatsgevonden door het *publiceren* van het desbetreffende gegeven op het internet, en niet door het doen van *onderzoek* daarnaar. Het is echter in uitzonderingsgevallen denkbaar dat het overnemen van persoonsgegevens uit publiek toegankelijke bronnen zelf ingrijpend van aard wordt. Wanneer daar sprake van kan zijn, wordt hieronder toegelicht.

Het overnemen van persoonsgegevens is "ingrijpend stelselmatig" als op voorhand redelijkerwijs voorzienbaar is dat een min of meer volledig beeld van een wezenlijk deel van iemands privéleven kan ontstaan (diep), dan wel een min of meer volledig beeld op verscheidene aspecten van iemand privéleven (breed). Hoewel een deel van de commissie van mening is dat "ingrijpende stelselmatigheid" niet aan de orde kan zijn bij het overnemen van persoonsgegevens uit publiek toegankelijke bronnen, wordt in dit rapport geadviseerd om wel het algemene normeringscriterium hanteren, met name om redenen van consistentie (met de algemene lijn in dit rapport dat het minder dan voorheen mogelijk is om op voorhand een zekere rangorde aan te brengen in bevoegdheden in termen van intrinsieke mate van ingrijpendheid), alsook omdat er wel situaties denkbaar zijn waarin inzet van deze bevoegdheid een ingrijpende inbreuk maakt op de persoonlijke levenssfeer.

Zoals in de algemene paragraaf over de driedeling is opgemerkt, is het daarbij wel belangrijk te benadrukken dat "ingrijpend stelselmatig" bij dit type onderzoek een uitzondering zal zijn. Bij overnemen van persoonsgegevens uit publiek toegankelijke bronnen zal dat alleen in zeer uitzonderlijke situaties voorkomen, minder nog dan bij bijvoorbeeld onderzoek van smartphones, vanwege het publiek toegankelijke karakter van de gegevens. Desalniettemin valt niet uit te sluiten dat het overnemen van persoonsgegevens uit publiek toegankelijke bronnen ingrijpende stelselmatigheid kan opleveren, gezien de grote hoeveelheid gegevens die (nu al, maar zeker over tien jaar) over uiteenlopende aspecten van iemands leven online te vinden zijn. Ingrijpende stelselmatigheid zal daarbij alleen het geval zijn als (redelijkerwijs voorzienbaar) gegevens worden overgenomen die door anderen dan de betrokkene zelf online zijn gezet en die duidelijk een privékarakter hebben, en waarbij zoekvragen worden gehanteerd waarbij (ook) in bronnen wordt gezocht waarvan bekend is dat die veelal dergelijke gegevens bevatten. Dit

kan het geval zijn als (ook) wordt gezocht in bronnen met gehackte gegevens die door de hacker (of een ander) online zijn gezet en de zoekvraag naar verwachting zal leiden tot het overnemen van privacygevoelige gegevens uit dergelijke bronnen waarbij die gegevens een ingrijpend beeld van iemands privéleven betreffen. Denk bijvoorbeeld, in een onderzoek naar kindermishandeling, aan het gedurende twee weken overnemen van beelden van een *nannycam* uit de kinderslaapkamer die via een *livestream* worden uitgezonden op een door een hacktivist opgezette webpagina met onbeveiligde camera's (de "diepe" variant); in een moordonderzoek met een ongeïdentificeerd slachtoffer die een weinig voorkomende tatoeage op haar borst heeft, het met een crawler overnemen van alle foto's van vrouwen met een soortgelijke tatoeage op de borst waarbij ook in wraakporno-sites wordt gezocht (en waarbij vanwege de foutmarge van de beeldherkenningssoftware ook foto's van derden zullen worden overgenomen) ("diep"); of, in een kinderporno-onderzoek, het overnemen van het volledige profiel en de besloten chats van een klant van een relatiebemiddelingsdienst, die online zijn gezet door een hacktivist die deze dienst gehackt heeft ("diep" en mogelijk ook "breed").

Deze voorbeelden illustreren dat het om uitzonderlijke situaties gaat, waarbij met name *combinaties* optreden van a) zoekvragen en een onderzoeksdoel waarbij naar verwachting ook gegevens zullen worden overgenomen die naar hun aard aanzienlijk privacygevoelig zijn, en b) onderzoek wordt gedaan in typen bronnen waarin naar ervaringsregels veelal gegevens te vinden zijn die door anderen dan betrokkenen online zijn gezet.

Wanneer bij het overnemen van persoonsgegevens uit publiek toegankelijke bronnen gebruik wordt gemaakt van gegevensbescherming door ontwerp en gegevensbescherming door standaardinstellingen (*Data Protection by Design and by Default*), zal het risico kunnen worden verminderd dat redelijkerwijs voorzienbaar gegevens worden overgenomen uit publiek toegankelijke bronnen die een ingrijpend beeld van iemands persoonlijke leven opleveren. Zo kunnen crawler-instellingen beperkt worden tot bepaalde typen bronnen, of kunnen bronnen met gehackte gegevens en wraakporno-achtige webpagina's worden uitgesloten. Ook kunnen met crawlers vergaarde gegevens worden afgezonderd in een afgeschermde omgeving zonder koppeling met politiesystemen, waarbij alleen gegevens uit deze omgeving worden overgenomen in politiesystemen die via gerichte zoekvragen in beeld zijn gekomen en relevant zijn bevonden voor het desbetreffende onderzoek (en waarbij wel, omwille van toetsbaarheid, de vergaarde gegevens wel in de afgeschermde omgeving, de "kluis", bewaard blijven tot na afloop van de zaak, zonder dat deze gegevens gebruikt kunnen worden voor andere doeleinden).

Evenals bij "stelselmatigheid" vindt ook de beoordeling van "ingrijpend stelselmatig" vooraf plaats, op basis van de beschikbare informatie in het dossier, de voorgenomen wijze van onderzoek, en de overige hierboven genoemde factoren die van invloed zijn op de mate van privacyinbreuk. Wel kan het voorkomen dat gaande het onderzoek blijkt dat het voorgenomen overnemen van persoonsgegevens uit publiek toegankelijke bronnen niet "gewoon" stelselmatig is maar ingrijpend stelselmatig wordt, bijvoorbeeld als onverwacht informatie naar voren komt dat de betrokkene regelmatig een praatgroep voor gokverslaafden bezoekt, terwijl alleen zijn partner – maar niet zijn vrienden, collega's of werkgever – weet heeft van zijn gokverslaving. In dergelijke gevallen zou, als het onderzoek in publiek toegankelijke bronnen naar verwachting informatie kan opleveren die samenhangt met deze gokverslaving en deze informatie relevant kan zijn voor het onderzoek en dus naar verwachting overgenomen zal worden, het onderzoek stilgezet moeten worden en pas kunnen worden voortgezet als alsnog een machtiging van de rechter-commissaris wordt verkregen. Als daarentegen de gokverslaving niet relevant is voor het onderzoek, en het ook niet redelijkerwijs te verwachten valt – gelet op de te hanteren zoekvragen en het gebruik van de eventuele resultaten – dat het verdere onderzoek nieuwe informatie zal opleveren die het zicht op dit deel van het leven van de verdachte vergroot en daarmee het beeld van dit aspect verder inkleurt – zal het voort te zetten onderzoek niet ingrijpend stelselmatig zijn.

Aanbeveling 61: op de bevoegdheid van overnemen van persoonsgegevens uit publiek toegankelijke bronnen is het algemene normeringscriterium van toepassing. De toelichting op "stelselmatigheid" en "ingrijpende stelselmatigheid" is te vinden in par. 4.2.2 en 5.3.3, die voor deze bevoegdheid nader wordt ingekleurd door de toelichting in deze paragraaf. → *p. 203*

6.4.6. Verhouding met andere bevoegdheden

De verhouding tussen bevoegdheden vergt aandacht. Het valt buiten de reikwijdte van dit rapport om op de onderlinge verhouding tussen alle bevoegdheden in te gaan, maar de commissie signaleert wel dat meer duidelijkheid geboden is, om de praktijk voldoende houvast te geven. Een voorbeeld hiervan is de verhouding tussen het overnemen van persoonsgegevens uit publiek toegankelijke bronnen en stelselmatige observatie. De toelichting (p. 60) zegt daarover:

> Stelselmatige observatie ziet op het stelselmatig volgen van een persoon of stelselmatig diens aanwezigheid of gedrag waarnemen. Hoewel open bronnen indicaties kunnen bevatten voor de aanwezigheid of het gedrag van een persoon (bijvoorbeeld met foto's of berichten op sociale media) neemt de opsporingsambtenaar niet zelf het gedrag of de aanwezigheid van de persoon waar. Het volgen of waarnemen in de zin van het huidige artikel 126g (artikel 2.8.2.1.1) heeft een "realtime" element in zich. De aanwezigheid, het gedrag of de bewegingen van de persoon worden in geval van stelselmatige observatie "realtime" gevolgd of waargenomen en daarmee feitelijk vastgesteld, al dan niet met behulp van een technisch hulpmiddel. Bij het onderzoek in open bronnen gaat het daarentegen vooral om "historische" gegevens die reeds aanwezig en beschikbaar zijn. Om deze reden is een afzonderlijke wettelijke grondslag van het onderzoek in open bronnen noodzakelijk en gewenst.

Hoewel dit een redelijke afbakening lijkt, miskent het dat steeds meer gedrag real-time via het internet is waar te nemen. Ook zonder dat Eggers' *The Circle* realiteit wordt, is live-streaming van camerabeelden al een gevestigde praktijk, die naar verwachting alleen maar zal toenemen. Fenomenen als *lifelogging*[213] en *quantified self*[214] stellen het onderscheid tussen real-time observatie en internetonderzoek van historische gegevens ter discussie: onderzoek van iemands publiek toegankelijke *lifelog*-blog levert veelal dezelfde soorten informatie op als door fysieke observatie kan worden verkregen (zij het dat waarschijnlijk aanzienlijk meer en gedetailleerder informatie naar voren komt, bijvoorbeeld over iemands slaappatronen). Zeker nu het overnemen van persoonsgegevens uit publiek toegankelijke bronnen wordt voorgesteld als een bevoegdheid die over een bepaalde periode (tot drie maanden, verlengbaar) wordt uitgeoefend, gaat het niet enkel om het overnemen van historische gegevens, maar ook om het overnemen van gegevens die worden gegenereerd na het afgeven van het bevel. Dit roept vragen op of het stelselmatig volgen van bepaalde blogs en live-camerabeelden als stelselmatige observatie of als onderzoek in een publiek toegankelijke bron moet worden gezien.

Aanbeveling 62: de wetgever dient in de memorie van toelichting meer helderheid te scheppen over de afbakening met andere bevoegdheden, zoals stelselmatige observatie. → *p. 203*

[213] https://en.wikipedia.org/wiki/Lifelog (laatst geraadpleegd 1 juni 2018).
[214] https://en.wikipedia.org/wiki/Quantified_Self (laatst geraadpleegd 1 juni 2018).

6.5. Stelselmatige locatiebepaling

In de opsporingspraktijk wordt al sinds geruime tijd gebruik gemaakt van locatiebepalingsmiddelen. Wanneer dat op een niet-stelselmatige wijze gebeurt, biedt artikel 3 PW 2012 een afdoende grondslag. Er is echter nog geen bevoegdheid voorhanden voor het *stelselmatig* inzetten van locatiebepalingsmiddelen. De voorgestelde regeling is blijkens de toelichting onder meer ingegeven door het feit dat de jurisprudentie geen duidelijke lijn heeft vastgesteld over de inzet van technische middelen ter locatiebepaling, in het bijzonder de stille sms en de IMSI-catcher. De toelichting (p. 61) wijst op een enkele uitspraak waar in algemene zin is gezegd dat er een specifieke wettelijke regeling nodig is.[215] In andere uitspraken werd de inzet van dergelijke plaatsbepalingsmiddelen goedgekeurd omdat het een geringe inbreuk op de privacy werd geacht. In de jurisprudentie is geen duidelijke lijn te destilleren over het omslagpunt van "niet-stelselmatig" naar "stelselmatig".

De voorgestelde regeling biedt een specifieke wettelijke grondslag voor stelselmatige locatiebepaling, en luidt als volgt:

> **Artikel 2.8.2.10.1 [nieuw]**
>
> 1. Ter uitvoering van een bevel tot uitoefening van een bevoegdheid als bedoeld in afdeling 8.2.1 tot en met afdeling 8.2.8 kan de officier van justitie bevelen dat een opsporingsambtenaar stelselmatig en met een technisch hulpmiddel de locatie bepaalt van de persoon ten aanzien van wie de bevoegdheid wordt uitgeoefend.
>
> 2. Het bevel tot stelselmatige locatiebepaling wordt gegeven voor een periode van ten hoogste een maand. De geldigheidsduur kan telkens voor een periode van ten hoogste een maand worden verlengd.
>
> 2. [sic] Het bevel vermeldt, naast de gegevens, bedoeld in artikel 2.8.1.1.1, tweede lid:
> a. ter uitvoering van welke bevoegdheid de locatiebepaling wordt uitgeoefend;
> b. een aanduiding van de aard van het technische hulpmiddel.

Voor de beoordeling van deze regeling en de mate waarin de inzet van deze bevoegdheid inbreuk maakt op de persoonlijke levenssfeer, is het van belang om vast te stellen dat het hier enkel gaat om het *vaststellen van de locatie* van de betrokkene. Het betreft een steunbevoegdheid: de locatiebepaling dient ter uitvoering van een andere bevoegdheid, bijvoorbeeld het kunnen uitvoeren van (stelselmatige) observatie. Deze bevoegdheid is dus met nadruk *niet* bedoeld voor het volgen van gedrag van de betrokkene.

6.5.1. Is deze regeling duidelijk?

Deze regeling neemt in ieder geval de in de jurisprudentie ontstane onduidelijkheid weg over de vraag of wel of niet een wettelijke bepaling nodig is. Een tweetal aspecten van deze regeling behoeft echter een nadere blik: het omslagpunt tussen niet-stelselmatig en stelselmatig, en het bevestigen van een technisch hulpmiddel op de persoon.

Het "omslagpunt" tussen niet-stelselmatig en stelselmatig

Deze regeling betreft als gezegd een steunbevoegdheid die gekoppeld is aan de heimelijke bevoegdheden genoemd in het eerste lid. Het gaat daarbij om de bevoegdheden stelselmatige observatie, bevoegdheden ten aanzien van een besloten plaats (inkijken), pseudokoop of -dienstverlening, stelselmatig overnemen van persoonsgegevens uit publiek toegankelijke bronnen, stelselmatige inwinning van informatie, infiltratie, het vastleggen van telecommunicatie en het vastleggen van vertrouwelijke communicatie. Indien het voor de toepassing van die bevoegdheden nodig is met een technisch hulpmiddel stelselmatig de locatie vast te stellen van de verdachte of een andere persoon, kan deze steunbevoegdheid ingezet worden. Alhoewel deze

[215] Hof Den Bosch 20 juni 2013, ECLI:NL:GHSHE:2013:2579.

steunbevoegdheid is ingegeven door jurisprudentie rond de stille sms en de IMSI-catcher, kan hij, gelet op de formulering van de bevoegdheid, ook uitgevoerd worden met behulp van andere plaatsbepalingsmethoden. De bepaling is immers techniekonafhankelijk geformuleerd. (Als het de bedoeling van de wetgever is de locatiebepaling in dit artikel te beperken tot stille sms en IMSI-catchers, zou de toelichting dit veel strikter en explicieter moeten weergeven.)

Het voorgestelde artikel lost het gebrek aan een specifieke wettelijke grondslag op, maar geeft geen duidelijkheid over het omslagpunt tussen niet-stelselmatig en stelselmatig. Het gaat daarbij om de inhoudelijke inschatting dat een "meer dan geringe inbreuk" op de persoonlijke levenssfeer wordt gemaakt door de inzet van de plaatsbepalingsmiddelen. In de memorie van toelichting staat dat de rechtspraak, net als nu, dat omslagpunt zal moeten bepalen. Dat is juist, maar er zou voor gekozen kunnen worden om op dit punt wel al de toelichting aan te vullen met criteria op basis waarvan wordt bepaald wanneer er sprake is van "stelselmatigheid". Dat geeft de rechtspraak meer houvast. In dat kader kan gedacht worden aan criteria als duur en frequentie, maar ook aan criteria die afhangen van de methode van plaatsbepaling en het voorgenomen of voorziene gebruik van de locatiegegevens.

Een peilbaken op een auto wordt op dit moment gebruikt als steun bij stelselmatige observatie. De tekst van artikel 2.8.2.10.1 sluit niet uit dat voor de uitvoering van die bevoegdheid een peilbaken wordt gebruikt; het artikel is immers technologieonafhankelijk geformuleerd. Het is dan mogelijk dat het gebruik van een peilbaken ter locatiebepaling gekoppeld wordt aan de (gelijktijdige) inzet van een tweede locatiebepalingsmethode, bijvoorbeeld via de mobiele telefoon. Bij de auto leg je vooral de bewegingen in het verkeer vast, en bij locatiebepaling middels de telefoon kun je specifiekere gegevens vastleggen, zoals binnen een gebouw. (Dit hangt overigens weer nader af van de gebruikte techniek: GPS of wifi-locatiebepaling via de telefoon levert nauwkeurige informatie op dan de stille sms of de IMSI-catcher.[216] Daarbij moet wel worden aangetekend dat het verschil in precisie tussen deze technieken geleidelijk afneemt; met de komende generatie mobiele telefonie, 5G, kan mogelijk de locatie van een mobiele telefoon in stedelijke omgevingen ook met een stille sms of IMSI-catcher veel preciezer kan worden bepaald, in zeer dichte gebieden mogelijk tot op een meter nauwkeurig, omdat er veel meer *nodes* zijn.[217])

Er is hier geen sprake van stapeling van bevoegdheden, maar het gebruiken van twee methoden binnen één bevoegdheid. Een dergelijke gecombineerde inzet van twee methoden levert een verdergaande inbreuk op dan het kiezen van één van deze methoden. Het gelijktijdig inzetten van twee methoden betekent zeker niet automatisch dat het onderzoek "stelselmatig" van aard is,[218] maar het kan er wel voor zorgen dat er sneller sprake is van een meer dan geringe inbreuk dan bij de inzet van één methode omdat de combinatie een fijnmaziger inzicht in de locatie kan opleveren.

Het koppelen van de gegenereerde locatiegegevens aan andere gegevens vindt niet plaats op grond van deze bevoegdheid. Het betreft immers een steunbevoegdheid die niet ziet op het vastleggen van gedrag, maar op het bepalen van de locatie ten behoeve van het uitoefenen van een andere bevoegdheid. In de toelichting kan verduidelijkt worden hoe in dit verband met de locatiegegevens dient te worden omgegaan.

---

[216] Koops, Newell & Škorvánek 2019.

[217] Hakkarainen e.a. 2015, p. 3: "ultradense networks seem capable of very precise UN [user nodes] localization with an accuracy that may very well be below one meter." Vgl. https://www.rcrwireless.com/20180517/5g/five-ways-kt-5g-at-the-olympics-tag6-tag99 (laatst geraadpleegd 1 juni 2018). In (landelijke) omgevingen waar een minder zwaar (verwacht) bandbreedtegebruik is, zullen *nodes* verder uit elkaar liggen, waardoor de precisie hetzelfde of mogelijk zelfs lager kan uitvallen dan bij 4G-telecommunicatie.

[218] En heeft dus geen rechtstreekse gevolgen voor de normering van de inzet, zoals het adiëren van de rechter-commissaris. De normering komt verderop in deze paragraaf aan de orde.

Aanbeveling 63: de regeling betreffende stelselmatige locatiebepaling is helder, waarbij het aan de rechter is om het omslagpunt tussen niet-stelselmatigheid en stelselmatigheid vast te stellen. In de toelichting moet wel meer aandacht worden besteden aan de criteria die van invloed zijn op (het bereiken van) dat omslagpunt en de omgang met vastgelegde locatiegegevens wanneer de gezochte locatie afdoende is bepaald. → *p. 204*

Bevestigen van een technisch hulpmiddel op de persoon

In de memorie van toelichting bij het nieuwe Boek 2 van het Wetboek van Strafvordering (p. 240) staat de volgende passage, waarin gesuggereerd wordt dat er bij het binnendringen van de telefoon en het activeren van de GPS geen sprake is van het bevestigen van een technisch hulpmiddel op de persoon.

> De opsporing kan bijvoorbeeld een smartphone van afstand benaderen en vervolgens via GPS aan plaatsbepaling doen. Uit de memorie van toelichting bij het genoemde wetsvoorstel *(CCIII)* volgt dat een smartphone niet een technisch hulpmiddel is dat op een persoon is bevestigd. Er wordt namelijk gebruik gemaakt van een voorwerp dat de persoon al bij zich heeft voor een ander doel. Dat is van belang voor de nu toegelichte bepaling. Indien gebruik wordt gemaakt van een voorwerp dat een persoon al bij zich heeft voor een ander doel, is geen sprake van het bevestigen op een persoon in de zin van deze bepaling.

Dit wekt verwarring op, omdat het in tegenspraak lijkt met eerdere uitspraken van de wetgever,[219] en dient te worden verduidelijkt in de toelichting. Voor de toepassing van beide steunbevoegdheden is van belang dat duidelijkheid bestaat over dit punt: vormt een smartphone en/of (de bij uitoefenen van de hackbevoegdheid daarop geplaatste) software *een technisch hulpmiddel dat wordt bevestigd op de persoon*? Volgens de commissie is het geldend recht (en de bedoeling van de wetgever) dat locatietrackers niet op het lichaam of in voorwerpen die op het lichaam worden gedragen, mogen worden bevestigd zonder toestemming van de persoon; dit vanwege de lichamelijke integriteit. Dat staat duidelijk op p. 27 van de toelichting op het wetsvoorstel CCIII, die instemmend verwijst naar de Wet BOB op dit punt.[220] Het verbod geldt dus ook voor locatietracking middels een aansteker die iemand bij zich draagt, en in het verlengde van de aansteker dus ook voor de bij zich gedragen smartphone.

Aangezien dat geldend recht is, heeft de wetgever in CCIII hierop een wettelijke uitzondering gecreëerd door wel toe te staan dat locatietrackers worden geplaatst in geautomatiseerde werken die iemand bij zich draagt; die uitzondering geldt hierbij dus alleen voor de specifieke bevoegdheid van binnendringen in een geautomatiseerd werk op afstand.

Vervolgens schept de wetgever bij Boek 2 verwarring door de laatste zin ("Indien gebruik wordt gemaakt van een voorwerp dat een persoon al bij zich heeft voor een ander doel, is geen sprake van het bevestigen op een persoon in de zin van deze bepaling") die in strijd is met het voorbeeld van de aansteker. Onze interpretatie is dat de wetgever bij Boek 2 (en waarschijnlijk ook in het wetsvoorstel CCIII) heeft willen duidelijk maken dat als softwarematig locatie wordt bepaald via een apparaat dat iemand toch al bij zich draagt, dat apparaat geen technisch hulpmiddel is in de zin de wet *voor zover het het vereiste van het Besluit technische hulpmiddelen betreft*. Het lijkt de commissie logisch dat het niet de bedoeling is dat het geautomatiseerde werk dat iemand bij zich draagt, aan dat besluit moet voldoen. Maar dat betekent niet dat de (op de smartphone geplaatste) software niet meer een op de persoon

[219] "In de wet is bepaald dat een technisch hulpmiddel niet op een persoon wordt bevestigd, tenzij met diens toestemming (artikelen 126g, derde lid, en 126o, derde lid, Sv). In de memorie van toelichting bij de Wet bijzondere opsporingsbevoegdheden is destijds aangegeven dat bevestiging op een persoon inhoudt: op of aan het lichaam of de kleding. *Daaronder valt ook plaatsbepalingsapparatuur die wordt aangebracht in een aansteker of pen die in of op de kleding wordt gedragen* (*Kamerstukken II* 1996/97, 25 403, nr. 3)." *Kamerstukken II* 2015–2016, 34 372, nr. 3, p. 27 (cursivering toegevoegd).

[220] Zie vorige noot.

bevestigd hulpmiddel betreft dat inbreuk maakt op de lichamelijke integriteit (door het gebruik van het lichaam voor het traceren van de locatie), waarvoor een expliciete wettelijke basis nodig is. Die basis wordt met het wetsvoorstel CCIII gecreëerd voor het op afstand binnendringen in smartphones of andere geautomatiseerde werken, maar in het conceptwetsvoorstel wordt geen basis geschapen voor andere vormen van het plaatsen van locatietrackers op apparaten die iemand bij zich draagt; daarvoor blijft de bestaande lijn rond de aansteker gelden.

Aanbeveling 64: de passage in de toelichting dient te worden verduidelijkt, opdat geen misverstand bestaat over het bevestigen van een technisch hulpmiddel op het lichaam.
→ *p. 204*

6.5.2. De reikwijdte

Het OM heeft in de consultatie aandacht gevraagd voor de koppeling van deze bevoegdheid aan de heimelijke bevoegdheden. Het OM stelt zich op het standpunt dat deze koppeling losgelaten moet worden, en noemt met name twee voorbeelden:

1. stelselmatige locatiebepaling ten behoeve van aanhouding van de verdachte;
2. stelselmatige locatiebepaling gekoppeld aan vordering toekomstige verkeersgegevens.

De aanhouding

Aan de locatiebepaling ten behoeve van de aanhouding van een verdachte is in de memorie van toelichting aandacht besteed. De aanhouding is iets waarvoor de locatiebepaling in beginsel niet stelselmatig hoeft te worden verricht; in beginsel kan een of enkele keren voldoende zijn. Een niet-stelselmatige locatiebepaling op basis van artikel 3 PW 2012 zou dan ook voldoende moeten zijn voor dit doel.

Het OM stelt zich op het standpunt dat dit in voorkomende gevallen onvoldoende kan zijn voor aanhoudingen. Dit komt mede door de onduidelijkheid over het “omslagpunt”; hoe vaak mag je een middel inzetten voordat het “stelselmatig” wordt?

De commissie is van oordeel dat één of enkele succesvolle sms’jes[221] in de meeste gevallen voldoende moeten zijn voor de aanhouding. Wanneer de sms’jes zijn verzonden en daarmee de locatie van de betrokkene is vastgesteld, zal doorgaans tot aanhouding over kunnen worden gegaan, zonder dat van stelselmatigheid sprake is. Er is pas sprake van stelselmatigheid wanneer redelijkerwijs voorzienbaar een (zeer) groot aantal plaatsbepalingen moet worden gedaan alvorens de verdachte daadwerkelijk kan worden aangehouden. Dat zal in de praktijk niet snel gebeuren, al zijn er wellicht omstandigheden denkbaar dat toch de drempel van stelselmatigheid toch zal worden bereikt. Wanneer de verdachte bijvoorbeeld langdurig in beweging is, bijvoorbeeld in een voertuig, kan het nodig zijn om een groot aantal plaatsbepalingen uit te voeren alvorens tot aanhouding over te kunnen gaan. Ook is denkbaar dat de verdachte zich in een gebied bevindt waar weinig zendmasten zijn, en de locatiebepaling dus minder nauwkeurig is, waardoor de locatiebepaling zich over een lange periode uitstrekt voordat de locatie met voldoende precisie kan worden bepaald om de verdachte aan te houden. Ook dan kan het gevolg zijn dat een grote hoeveelheid locatiebepalingen moet worden uitgevoerd, voordat tot aanhouding kan worden overgegaan. Hoewel het hier om enigszins gezochte voorbeelden gaat, lijkt het voor de systematiek wenselijk rekening te houden met de mogelijkheid dat er gevallen bestaan waarin het nodig is om deze bevoegdheid op stelselmatige wijze toe te kunnen passen ten behoeve van aanhoudingen.

[221] Met een succesvol sms’je wordt gedoeld op de situatie dat contact wordt gemaakt met het toestel van de verdachte, op zodanige wijze dat er een locatiebepaling tot stand komt. Als het toestel bijvoorbeeld is uitgeschakeld, heeft een stille sms niet het gewenste effect: er zal dan geen plaatsbepaling mogelijk zijn.

Aanbeveling 65: de steunbevoegdheid van stelselmatige locatiebepaling moet mogelijk worden gemaakt voor aanhouding. → *p. 204*

De toekomstige verkeersgegevens

Wat betreft de verkeersgegevens heeft het OM aangegeven zich af te vragen of er onder het nieuwe wetboek nog gebruik kan worden gemaakt van plaatsbepaling via het vorderen van toekomstige verkeersgegevens. Deze bevoegdheid is in het nieuwe Boek 2 opgenomen in artikel 2.7.3.3.6, eerste lid. Het probleem zit hem in de beschikbaarheid van de verkeersgegevens: als de verdachte zelf niet actief gebruik maakt van het toestel door te bellen of te sms'en, worden er door de provider geen verkeersgegevens vastgelegd. Een tap levert dan ook geen verkeersgegevens op. Het toestel kan dan niet gevolgd worden, tenzij er een stille sms wordt verzonden: alleen dan ontstaat er een verkeersgegeven. De stille sms laat de telefoon alleen maar pingen, en er is een tap of vordering toekomstige verkeersgegevens nodig om vervolgens het locatiegegeven te verkrijgen. Indien het (zoals het conceptwetsvoorstel nu luidt) niet toegestaan is om stelselmatig stille sms'jes te verzenden ten behoeve van de vordering toekomstige verkeersgegevens, zou die methode in die redenering dus niet gebruikt kunnen worden voor stelselmatige locatiebepaling om toekomstige verkeersgegevens te genereren. Men zou kunnen veronderstellen dat dit een lacune oplevert in het systeem van bevoegdheden om stelselmatige locatiebepaling te kunnen toepassen.

De commissie is echter van oordeel dat er geen lacune is. In het hierboven genoemde geval worden de (toekomstige) verkeersgegevens gevorderd niet ten behoeve van inzicht in het communicatiepatroon van verdachte maar ten behoeve van de locatiebepaling, waarbij noch de verkeersgegevens noch de locatiebepaling een doel op zich zijn; ze zijn beide nodig ten behoeve van een ander opsporingsdoel, bijvoorbeeld een stelselmatige observatie. De stelselmatige locatiebepaling, in de vorm van de stille sms, kan in dit geval dus worden ingezet als steunbevoegdheid voor die stelselmatige observatie. Daarbij is er geen beletsel om naast de stelselmatige observatie ook de bevoegdheid tot vorderen van (toekomstige) verkeersgegevens toe te passen.[222] Het maken van de gevraagde koppeling is derhalve niet nodig.

Aanbeveling 66: in de toelichting wordt verduidelijkt dat stelselmatige locatiebepaling als bedoeld in artikel 2.8.2.10.1 geen formele steunbevoegdheid hoeft te zijn van de vordering toekomstige verkeersgegevens, om van de beschreven methode gebruik te kunnen maken in combinatie met een vordering toekomstige verkeersgegevens. → *p. 204*

6.5.3. Is deze regeling afdoende genormeerd?

Relatie met huisrecht?

Het gebruik van technische hulpmiddelen ten behoeve van locatiebepaling kan zich uitstrekken tot achter de muren van het huis van betrokkene. Dit zal in toenemende mate het geval zijn als van nauwkeuriger methoden gebruik gemaakt wordt. Het huisrecht komt bijzondere bescherming toe, en dit roept derhalve de vraag op of de inzet van deze bevoegdheid zwaarder genormeerd dient te worden wanneer de mogelijkheid bestaat dat de locatie in huis wordt vastgesteld.

Er lijkt geen rechtstreekse schending van artikel 12 Gw aan de orde te zijn. In een vergelijkende studie hebben Koops et al.[223] de rechtspraak in verschillende landen bezien. Zo heeft het Duitse Bundesgerichtshof overwogen dat GPS-tracking geen strijd oplevert met het

[222] Vanzelfsprekend kan de vordering toekomstige verkeersgegevens ook uitgeoefend worden voor andere doelen dan locatiebepaling; daarop is de bovenstaande passage niet van toepassing.
[223] Koops, Newell & Škorvánek 2019, p. 19-20.

constitutionele recht op onschendbaarheid van de woning, en het EHRM heeft overwogen dat GPS-surveillance in zijn aard te onderscheiden is van andere vormen van *surveillance*, omdat die andere vormen meer informatie bloot leggen over het gedrag, de meningen of gevoelens van de betrokkene. Met GPS worden enkel de kale locatiegegevens bij de woning vastgelegd, maar niet wat betrokkene zegt, doet, of anderszins uit middels zijn gedrag.

In een eerdere publicatie van Koops en Prinsen[224] is ingegaan op wat de term "binnentreden" uit artikel 12 Gw betekent in het licht van moderne technieken. Vastgesteld is dat het vooral ging om fysiek binnentreden, maar dat bijvoorbeeld ook het stelselmatig naar binnen kijken als inbreuk op het huisrecht zou moeten worden gekenschetst. Echter, of het nu gaat om het hacken van een computer in huis, het onderscheppen van informatie uit de slimme koelkast, het gebruiken van een richtmicrofoon of visueel middel voor observatie: de moderne en (op dat moment toekomstige) middelen om van buitenaf een inbreuk te plegen op het huisrecht, werden in die publicatie allemaal geplaatst in de sleutel van het verkrijgen van informatie over wat er in het huis gezegd of gedaan wordt.

Daarvan is geen sprake bij het gebruiken van plaatsbepaling. Enkel de aanwezigheid van een persoon of voorwerp kan in grovere of gedetailleerdere mate worden vastgesteld. Het gaat alleen om de "kale locatiegegevens", zoals zij eerder werden genoemd. De inbreuk op de persoonlijke levenssfeer is, met het enkel vaststellen van de aanwezigheid in huis, naar het oordeel van de commissie niet zodanig dat een aanvullende normering nodig is.

Indringend stelselmatig?

Er zouden ook bij deze bevoegdheid omstandigheden kunnen zijn die leiden tot een situatie waarin sprake is van *ingrijpende stelselmatigheid* (zie par. 4.2). In dat geval is er aanleiding voor aanvullende normering. Van belang is om vast te stellen dat op twee manieren sprake kan zijn van ingrijpende stelselmatigheid; daar waar wordt doorgedrongen in wezenskenmerken van een persoon (diep), maar ook daar waar in brede zin zodanig veel informatie wordt verkregen over diverse aspecten van het persoonlijk leven (breed) dat er om die reden sprake is van ingrijpendheid.

De commissie is van oordeel dat gegenereerde locatiegegevens een *indicatie* kunnen geven van de aard van de activiteit van een persoon, maar die gegevens zullen altijd ruimte open laten voor interpretatie. Een regelmatig bezoek aan bijvoorbeeld een bordeel kan betekenen dat betrokkene klant is, maar kan ook betekenen dat hij pooier is, of een pakketbezorger. En als hij klant is, geven de locatiegegevens nog geen intieme details bloot op dezelfde indringende wijze die videobeelden, geluidsfragmenten of gegevens van een gegevensdrager kunnen bewerkstelligen. Belangrijker nog is dat de locatiebepaling niet voor het vaststellen van gedrag dient: het is een steunbevoegdheid ten dienste van andere bevoegdheden. Het dient enkel om de locatie vast te stellen, bijvoorbeeld om te kunnen observeren. Het is dan niet de locatiebepaling, maar de observatie waarmee gedrag wordt vastgelegd, die een mogelijk ingrijpende privacyinbreuk maakt. Dit alles pleit niet voor een verzwaarde normering voor inzet van de steunbevoegdheid.

Bovendien zal er, zoals hierboven bij de passage over aanhouding reeds uiteen gezet, in veel gevallen überhaupt geen sprake zijn van stelselmatigheid van de locatiebepaling: in de meeste gevallen zullen immers één of enkele succesvolle sms'jes voldoende zijn. Het betreft een steunbevoegdheid die normaliter niet lang hoeft te worden ingezet om tot het hoofddoel over te kunnen gaan. De gevallen waarin dergelijke kortdurende inzet niet voldoende is (en er dus bij wijze van uitzondering toch sprake kan zijn van stelselmatigheid), zijn gevallen waarin de verdachte onderweg is in de auto, of gevallen waarin de locatiebepaling niet nauwkeurig genoeg is om de verdachte snel exact te lokaliseren teneinde over te gaan tot de aanhouding of de observatie. In beide gevallen is moeilijk voorstelbaar dat sprake kan zijn van *ingrijpendheid*; er

[224] Koops & Prinsen 2005.

is immers geen sprake van aanwezigheid op gevoelige locaties, omdat dat eenvoudigweg niet kan worden vastgesteld. Dit, gekoppeld aan het vereiste van de *redelijkerwijs voorzienbare* ingrijpendheid, leidt tot de conclusie dat een voorzienbare, ingrijpend stelselmatige locatiebepaling een vrijwel niet voorkomende situatie zal zijn. Slechts wanneer redelijkerwijs voorzienbaar is dat de locatiebepaling een zeer precies en langdurig karakter zou krijgen alvorens over gegaan kan worden tot het hoofddoel van de locatiebepaling (te weten de aanhouding, observatie of andere heimelijke bevoegdheid), kan eventueel sprake zijn van ingrijpende stelselmatigheid.

De commissie verwacht dat dergelijke indringende inbreuken op de persoonlijke levenssfeer in de praktijk zeer uitzonderlijk zullen zijn, en bovendien niet goed voorzienbaar. Een bevel van de officier van justitie is dus normaliter voldoende voor het meer dan incidenteel verkrijgen van locatiegegevens. Desalniettemin kan voor de echte uitzonderingsgevallen aangesloten worden bij het algemene normeringscriterium (zie par. 4.2), dat regelt dat in geval van voorzienbare, indringend stelselmatige inbreuken de rechter-commissaris toestemming moet geven.

Aanbeveling 67: deze bevoegdheid wordt gekoppeld aan het algemene normeringscriterium, waarbij in hoge uitzonderingsgevallen, in voorzienbare situaties van indringende stelselmatigheid, de rechter-commissaris toestemming moet geven. → *p. 204*

6.6. Technische hulpmiddelen

6.6.1. Definitie

In het huidige Wetboek van Strafvordering reguleert artikel 126ee Sv het gebruik van bepaalde technische hulpmiddelen in de opsporing. In het artikel wordt de reikwijdte van het begrip technisch hulpmiddel (in de strafvorderlijke zin) ingeperkt tot hulpmiddelen gebruikt bij de uitvoering van in het artikel zelf limitatief opgesomde bevoegdheden. Voorts dient artikel 126ee Sv als kapstokbepaling voor nadere regulering van technische hulpmiddelen bij inzet van de in dit artikel benoemde bevoegdheden bij AMvB.

In het conceptwetsvoorstel is een bepaling opgenomen met betrekking tot technische hulpmiddelen die worden gebruikt in het kader van een aantal heimelijke bevoegdheden, het voorgestelde artikel 2.8.1.5.1. Dit artikel vervult dezelfde functie als artikel 126ee Sv.

Artikel 2.8.1.5.1 [artikel 126ee]

Bij algemene maatregel van bestuur worden regels gesteld over:

a. de opslag, verstrekking en plaatsing van de technische hulpmiddelen, bedoeld in artikel 2.8.2.1.1, derde lid, artikel 2.8.2.4.1, eerste lid, artikel 2.8.2.8.1, eerste lid en artikel 2.8.2.10.1, eerst lid, alsmede van de technische hulpmiddelen, bedoeld in artikel 2.8.2.7.1, eerste lid, voor zover het bevel, bedoeld in artikel 2.8.2.7.1, vijfde of zesde lid, ten uitvoer wordt gelegd zonder medewerking van de betrokken aanbieder;
b. de opslag, verstrekking en plaatsing van de technische hulpmiddelen die dienen ter ontsleuteling van versleutelde communicatie die wordt vastgelegd op grond van artikel 2.8.2.7.1, eerste lid;
c. de technische eisen waaraan de hulpmiddelen, bedoeld in onderdelen a en b voldoen, onder meer met het oog op de onschendbaarheid van de vastgelegde waarnemingen; toevoeging wetsvoorstel CCIII) of, in geval van toepassing van artikel 126nba, 126uba of 126zpa, de vastgelegde gegevens, en met het oog op het voorkomen van misbruik door derden;
d. de controle op de naleving van de eisen, bedoeld in onderdeel c;
e. de instellingen die de registratie van signalen aan een technische bewerking onderwerpen;
f. de wijze waarop de bewerking, bedoeld in onderdeel e, plaatsvindt met het oog op de controleerbaarheid achteraf, alsmede de waarborgen waarmee deze is omgeven en de mogelijkheden voor een tegenonderzoek.

Uit de memorie van toelichting bij het conceptwetsvoorstel blijkt dat artikel 126ee Sv inhoudelijk nagenoeg ongewijzigd is overgenomen in artikel 2.8.1.5.1. Zowel in de huidige als in de concepttekst ziet het artikel op de technische hulpmiddelen die worden ingezet bij de uitoefening van de bevoegdheden stelselmatige observatie, opnemen vertrouwelijke communicatie en het zonder medewerking van de aanbieder opnemen van telecommunicatie.

Alleen onderdeel b, dat ziet op de opslag, verstrekking en plaatsing van technische hulpmiddelen ter gebruik van ontsleuteling van versleutelde communicatie die verloopt via aanbieders van een communicatiedienst, is toegevoegd. Ook de nieuwe heimelijke bevoegdheden stelselmatig overnemen van persoonsgegevens uit publiek toegankelijke bronnen (artikel 2.8.2.4.1) en stelselmatige locatiebepaling (artikel 2.8.2.10.1) zijn toegevoegd aan onderdeel a. In bovenstaande tekst is in onderdeel c ook de wijziging van het wetsvoorstel CC III verwerkt.

Afgezien van de inperking van de reikwijdte van het technisch hulpmiddel begrip schept het artikel weinig duidelijkheid over wat daaronder wel of niet moet worden verstaan.

6.6.2. De lagere regeling

De huidig geldende AMvB, het Besluit technische hulpmiddelen strafvordering (hierna: het besluit), is op 1 januari 2007 in werking getreden en vindt zijn grondslag in artikel 126ee Sv. Het besluit stelt procedurele eisen aan de opslag, de verstrekking, de plaatsing, de controle en de verwijdering van de technische hulpmiddelen (artikelen 5 tot en met 9 van het besluit). Voorts stelt het besluit (in de artikelen 10-15) technische eisen waaraan technische hulpmiddelen in de zin van 126ee Sv dienen te voldoen.

Ook het besluit biedt niet onmiddellijk verdere duidelijkheid over wat onder een “technisch hulpmiddel” moet worden verstaan; het bevat geen definitie of omschrijving. De Nota van Toelichting bij het huidige besluit maakt wel meer duidelijk: het besluit ziet alleen op technische hulpmiddelen die gegevens registreren en op een gegevensdrager vastleggen (ook omschreven als “vastgelegde waarnemingen”). Enkel zintuigversterkende apparaten – die dus niet registreren – vallen er niet onder.

Of iets een technisch hulpmiddel is als bedoeld in artikel 126ee Sv hangt mede af van de context, van het gebruik. Ter illustratie: een richtantenne die gebruikt wordt voor communicatie tussen twee uiteen liggende gebouwen heeft een andere context dan dezelfde richtantenne die gebruikt wordt om datastromen op te vangen die tussen twee andere antennes heen en weer gaan. Het eerste is niet een technisch hulpmiddel in de zin van 126ee Sv, het tweede mogelijk wel.

Ondanks de focus op klassieke technische hulpmiddelen is het besluit niet beperkt tot technische hulpmiddelen die beeldsignalen of geluidssignalen registeren. Er zijn blijkens de Nota van Toelichting ook andere soorten signalen denkbaar. Het voorbeeld dat wordt gegeven is de aanslag van een toets op het toetsenbord van een computer.

Ook softwarematige hulpmiddelen zijn niet uitgesloten van toepasselijkheid van het besluit, zoals kan worden afgeleid uit de Nota van Toelichting. Daarmee is niet gezegd dat de huidige regeling volstaat, zeker niet nu software een steeds vaker gehanteerd hulpmiddel wordt.

6.6.3. Algemene overwegingen ten aanzien van technische en andere hulpmiddelen

Een probleem dat zich in de praktijk voordoet is dat er een duidelijk verschil bestaat tussen een technisch hulpmiddel in de zin van artikel 2.8.1.5.1 (artikel 126ee Sv) en een apparaat dat in normaal (technisch) maatschappelijk spraakgebruik ook wel een “technisch (hulp)middel” wordt genoemd. Veel hard- en software die functies uitvoeren ter ondersteuning van menselijke processen kunnen in het gewone spraakgebruik een technisch hulpmiddel worden genoemd.

Het kenmerkende onderscheid tussen technische hulpmiddelen in de zin van artikel 126ee Sv en andere hulpmiddelen van technische aard die in de opsporing kunnen worden gebruikt, is het feit dat de artikel 126ee Sv-hulpmiddelen gegevens *genereren*. Daarvan zijn te onderscheiden technische voorzieningen die *bestaande* gegevens kopiëren (vergaren), bijvoorbeeld

software waarmee gegevens op internet worden gezocht en overgenomen. De technische hulpmiddelen in de zin van artikel 126ee Sv zijn in wezen vervangend voor een opsporingsambtenaar. De waarneming van een opsporingsambtenaar, die gebeurtenissen waarneemt en daarvan ambtsedig proces-verbaal opmaakt, wordt vervangen door waarneming door een apparaat. Net zoals aan opsporingsambtenaren betrouwbaarheidseisen worden gesteld, worden eisen gesteld aan technische hulpmiddelen die soortgelijke waarnemingen doen en vastleggen.

Dit verschil betekent echter niet per definitie dat geen betrouwbaarheidseisen zouden moeten worden gesteld aan hulpmiddelen van technische aard waarmee geen nieuwe gegevens worden gegenereerd maar bestaande gegevens worden overgenomen. Hetzelfde geldt voor hulpmiddelen van technische aard waarmee gegevens worden verwerkt. Het toenemende gebruik van software als instrument van gegevensvergaring en -analyse, noodzakelijk om het groeiende datavolume te kunnen hanteren, betekent dat ook op het terrein van de verzameling en analyse van bestaande gegevens menselijk handelen plaats maakt voor "handelen" door technologie.

De mate waarin aan dergelijke hulpmiddelen wettelijke eisen moeten worden gesteld is mede afhankelijk van de vraag of de handelingen die een hulpmiddel uitvoert herhaalbaar zijn. Als de handeling herhaalbaar is, kan de betrouwbaarheid van de resultaten immers worden getoetst door de handeling te herhalen en beide resultaten te vergelijken. Of een geautomatiseerde onderzoekshandeling herhaalbaar is, hangt daarbij mede af van de vraag in welke context de handeling is uitgevoerd.

In een omgeving die volledig onder controle staat van de opsporingsdienst, zal een geautomatiseerde handeling in veel gevallen eenvoudig herhaald kunnen worden. Als de handeling echter (al dan niet deels) heeft plaatsgevonden in een externe omgeving, zoals het geval is bij het gebruik van crawlers op het internet, zal een herhaling van de handeling op een later moment een ander resultaat kunnen opleveren. Hetzelfde geldt voor handelingen waarvoor gebruik wordt gemaakt van hulpmiddelen waarvan onderdelen ("componenten" in de terminologie van het huidige besluit) onder controle van derden staan.

Daardoor kan in die gevallen op basis van de vergelijking van resultaten geen definitieve uitspraak worden gedaan over de betrouwbaarheid van het eerste resultaat. Het ligt daarom voor de hand om aan niet-herhaalbare onderzoekshandelingen die gegevens genereren bepaalde eisen te stellen die zien op de integriteit en authenticiteit van de vastlegging van wat door de gebruikte middelen is waargenomen.

Voor niet-herhaalbare geautomatiseerde datavergaringen zou het Wetboek van Strafvordering algemene betrouwbaarheids- en uitlegbaarheidseisen moeten stellen (vgl. ook par. 3.4.2). Gelet op de diversiteit van toepassingen is het niet werkbaar om dergelijke eisen standaard te verbinden, zoals in het bestaande regime van artikel 126ee Sv gebeurt, aan een voorafgaande toetsing. Het gaat simpelweg om te veel typen software, die bovendien regelmatig aangepast en geüpdatet moeten worden in verband met technische ontwikkelingen (bijvoorbeeld als weer een nieuwe (versie van) een app of smartphone op de markt komt). In plaats van toetsing vooraf, zou nader verkend kunnen worden of, en zo ja onder welke voorwaarden, een toetsing achteraf door de rechter(-commissaris) voldoende waarborgen kan bieden voor de betrouwbaarheid van gebruikte technische middelen.

Voor zover het gegevensverwerkingen of -analyses betreft die binnen de opsporingsdiensten worden uitgevoerd, gelden de eisen van de Wpg. Deze wet stelt op dit moment geen eisen aan bij verwerking gehanteerde hulpmiddelen. Meer en meer echter worden, mede door de toenemende hoeveelheden data binnen onderzoeken, allerlei hulpmiddelen gebruikt bij het analyseren en visualiseren van data en relaties tussen data. Visualisatie en representatie kunnen belangrijk hulpmiddelen zijn om complexe zaken meer begrijpelijk en inzichtelijk te maken, maar kunnen het (ook juist daardoor) moeilijker maken de juistheid van de representatie te bevragen en toetsen en om de mogelijkheden van alternatieve verklaringen gevisualiseerd of

gerepresenteerd te zien. Dit betekent dat het gebruik van dergelijke hulpmiddelen significante invloed kan hebben op de te verkrijgen resultaten van onderzoek of de waardering daarvan.

Met het toenemend gebruik van dergelijke hulpmiddelen en hun effect op de opsporing ligt het niet voor de hand het gebruik ervan geheel ongereguleerd te laten. Aan de andere kant zou een rigide, al te specifieke regulering voor een te strak keurslijf kunnen zorgen, waardoor niet met de snelle ontwikkeling van dergelijke hulpmiddelen kan worden meegegaan. Daarom zou gedacht kunnen worden aan een algemene eis van toetsbaarheid van de betrouwbaarheid van de gebruikte middelen en hun resultaten, evenals aan bepaalde minimumeisen aan de kennis en vaardigheid van gebruikers van dergelijke hulpmiddelen.

Aanbeveling 68: aangezien de wijze waarop technische hulpmiddelen op dit moment worden gereguleerd voor het gebruik van software minder houdbaar is, moet een toekomstige regeling rekening houden met de specifieke eigenschappen van software en het effect dat die hebben op daaraan te stellen eisen. Er kan onderscheid worden gemaakt tussen technische hulpmiddelen die bewijs of informatie genereren en technische hulpmiddelen die reeds bestaande gegevens overnemen. De mate waarin de met hulpmiddelen van die laatste categorie verrichte handelingen herhaalbaar zijn, zou mede moeten bepalen welke regels voor die categorie hulpmiddelen zouden moeten worden gesteld.

Hulpmiddelen voor gegevensverwerking, -analyse of -presentatie vallen naar het oordeel van de commissie niet onder het Wetboek van Strafvordering maar onder de Wpg. De commissie geeft in overweging bij de herziening van de Wpg, gezien het toenemend belang van dergelijke hulpmiddelen in de opsporingsketen, enige algemene regels te stellen met betrekking tot gebruikte hulpmiddelen voor gegevensverwerking, -analyse of -presentatie, zoals een algemene eis van toetsbaarheid van de betrouwbaarheid van resultaten die met gebruikmaking van dergelijke hulpmiddelen worden verkregen of gepresenteerd. → *p. 204*

6.6.4. Toekomstige hulpmiddelen

De commissie heeft, met hulp van verschillende experts in een technische sessie, ook gekeken naar toekomstige ontwikkelingen op het gebied van opsporingsondersteunende hulpmiddelen en naar de vraag of deze ook gereguleerd zouden moeten worden. Daarbij is onder ander aandacht geschonken aan velden zoals de inzet van dieren of andere biologische hulpmiddelen en de inzet van robotische hulpmiddelen, en hybride vormen daarvan. Gezien de weidsheid van de nu nog onvoldoende concreet te voorziene ontwikkelingen en hun uiteenlopende aard, is het voor de commissie niet mogelijk om hierover gerichte adviezen te formuleren.

Wel lijkt het raadzaam dat, wanneer dergelijke hulpmiddelen in de toekomst meer regulier worden ingezet, tijdig te bezien of nadere regulering alsdan noodzakelijk is. In zijn algemeenheid zal daarbij moeten worden aangesloten bij de lijn die ook in de huidige adviezen zichtbaar is. Een algemene eis van uitlegbaarheid of toetsbaarheid zal daar deel van uitmaken, met specifieke aandacht voor hulpmiddelen die op een niet-herhaalbare wijze gegevens vastleggen.

Aanbeveling 69: indien biologische en/of robotica-gebaseerde hulpmiddelen in de toekomst meer concrete vormen aannemen, moet op dat moment worden bezien of en in hoeverre nadere regulering van het gebruik van deze middelen noodzakelijk is. Aan de inzet van dergelijke middelen zouden alsdan eisen kunnen worden gesteld die een vergelijkbaar niveau van betrouwbaarheid garanderen als bij klassieke technische hulpmiddelen het geval is. → *p. 204*

7. Nieuwe bevoegdheden en onderwerpen

Een onderdeel van het eerste deel van de opdracht van de commissie betreft de vraag of het "pakket" van bevoegdheden in Boek 2, waaronder de nieuwe bevoegdheden uit het wetsvoorstel computercriminaliteit III, voldoende toekomstbestendig is met het oog op de technologische ontwikkelingen. Voor zover de commissie in staat is de ontwikkelingen in de periode tot circa 2030 te overzien, en met inachtneming van de fundamentele aandachtspunten die de commissieopdracht overstijgen (waaronder geautomatiseerde data-analyse, par. 3.4), heeft zij over het algemeen geen substantiële lacunes in het pakket van bevoegdheden geconstateerd. De combinatie van de verschillende bevoegdheden in Hoofdstukken 7 en 8 van Boek 2 lijkt voldoende aanknopingspunten te bieden voor het opsporingsonderzoek in de komende tien, vijftien jaar. Ongetwijfeld zullen op onderdelen aanpassingen nodig zijn, maar die zullen in de verwachting van de commissie grotendeels goed inpasbaar zijn in de systematiek van het totaalpakket van bevoegdheden.

Op één onderdeel signaleert de commissie echter wel een tekortkoming in het pakket van bevoegdheden: het gebrek aan de mogelijkheid om te vorderen van private partijen dat zij een data-analyse uitvoeren (par. 7.1). Daarnaast wijst de commissie op geautomatiseerde gezichtsherkenning als een belangrijke ontwikkeling voor de komende decennia, waar specifiek aandacht voor nodig is (par. 7.2).

7.1. Data-analyse door private partijen

7.1.1. Achtergrond: analyse door een derde partij

De huidige wetgeving ten aanzien van het vorderen van gegevens geeft alleen de mogelijkheid om welbepaalde gegevens of bestanden te vorderen bij houders van die gegevens. Er bestaat (uitzonderingen daargelaten[225]) nu geen mogelijkheid om van de vermoedelijke houder te vragen/vorderen om gegevens te analyseren, vergelijken of combineren teneinde nieuwe gegevens te verkrijgen,[226] terwijl daar steeds meer behoefte aan is. In deze paragraaf wordt daarom onderzocht in hoeverre het introduceren van een bevoegdheid tot het vorderen van data-analyse wenselijk en mogelijk is.

Nu er steeds meer data worden vastgelegd door allerlei partijen, levert het vorderen van één welbepaald gegeven vaak een zeer incompleet beeld op, terwijl het vorderen van het uitleveren van een heel bestand vaak veel te veel data oplevert. Deze gegevens zijn niet allemaal relevant voor de onderzoeksvraag en de opsporingsdienst heeft er geen behoefte aan. Maar zo'n bestand zal, met het oog op eventuele nieuwe onderzoeksvragen, vaak bewaard blijven. Dit resulteert in een onnodige inbreuk op de privacy van betrokkenen.

Wanneer een bestand dat van belang is voor opsporing ook gegevens bevat van niet-verdachte personen, dan zal het beginsel van proportionaliteit hogere eisen stellen aan de motivering ten aanzien van het toepassen van de bevoegdheden.[227] Dit zal er regelmatig toe leiden dat bestanden niet gevorderd kunnen worden op basis van de huidige wetgeving en er dan feitelijk geen opsporing kan plaatsvinden. In de huidige informatiemaatschappij beschikken grote bedrijven (denk aan banken en techbedrijven zoals Google, Facebook en Apple) over zeer

[225] Bijvoorbeeld het Besluit bijzondere vergaring nummergegevens telecommunicatie, *Stb.* 2002, 31 (laatst gewijzigd *Stb.* 2013, 49) dat telecommunicatiedienst aanbieders verplicht een nummer van een subject te achterhalen door middel van analyse van hun bestanden.
[226] Zie de Aanwijzing opsporingsbevoegdheden 2014, par. 2.10, http://wetten.overheid.nl/BWBR0035498/2014-09-01#Circulaire.divisie2_Circulaire.divisie2.10 (geraadpleegd 1 juni 2018).
[227] Ibid.

veel informatie, in zulke grote verzamelingen dat het ook technisch onmogelijk is dat de opsporing deze bestanden volledig over zou nemen ter analyse.

Een derde argument voor het laten uitvoeren van analyses op bestanden door derde partijen is dat het hun eigen data zijn die zij heel goed kennen en over het algemeen (bij grotere partijen) op een fraude- of marketingafdeling de middelen voorhanden zijn om een degelijke analyse uit te kunnen voeren. Voor de opsporingsinstantie is het analyseren van deze data veel moeilijker.

In de opsporingspraktijk wordt ook nu al regelmatig gebruik gemaakt van onderzoek dat is verricht door particuliere partijen. Snel opeenvolgende, met name technische, ontwikkelingen maken de wereld steeds complexer, waardoor het onmogelijk is dat de overheid alle specialismes in eigen huis ontwikkelt en behoudt. Publiek-private samenwerking heeft het afgelopen decennium een enorme vlucht genomen. De toename van kennis en macht van (grote) bedrijven leidt ook tot een grotere maatschappelijke verantwoordelijkheid. Sommige bedrijven geven aan vrijwillig te willen samenwerken met de overheid, helemaal waar het hun eigen domein betreft. Maar zij voelen zich door de mogelijke civiele aansprakelijkheid, privacywetgeving en civiel overeengekomen geheimhoudingsverplichtingen beperkt. Een wettelijke bevoegdheid om het uitvoeren van analyses door een derde of de gezamenlijke uitvoering daarvan te vorderen, kan een deel van deze bezwaren wegnemen.

7.1.2. Voorbeelden

In deze paragraaf wordt een aantal geanonimiseerde voorbeelden gegeven van onderzoeken met data-analyse door derden, die met de huidige regels niet of nauwelijks mogelijk zijn.

Casus bestandsvergelijking vervoersbedrijf

Op een aantal stations is brand gesticht. Het vermoeden bestaat dat het één en dezelfde dader betreft. Het openbaar vervoerbedrijf besluit door middel van (big data) analyse te proberen de dader te achterhalen. Een grote variëteit aan data wordt gebruikt om tot hypotheses te komen en deze te toetsen. Hierbij kan gedacht worden aan data van vervoerbewijzen (OV-chipkaarten), data van de tijdstippen van de incidenten, data over de trajecten waarop de incidenten plaatsvonden, data van de controles voordat een incident had plaatsgevonden, data over boetes, stationslocaties, agressiemeldingen, mogelijke routes, data over reizigers die hetzelfde traject als verdachte(n) aflegden, camerabeelden, data van controlepoortjes, data over afwijkend reisgedrag, sociale-media-data, en informatie die door conducteurs genoteerd werd.

Er is door de NS een geïntegreerde analyse uitgevoerd, waarbij verschillende databronnen aan elkaar gekoppeld zijn om incidenten te plotten op tijd en locatie en daaromheen van zoveel mogelijk informatie te voorzien. Er heeft *text mining* plaatsgevonden om te zien welke informatie er naar boven komt bij bepaalde zoektermen. En er is een “strangeness”-analyse uitgevoerd om op basis van de OV-kaart-data het (afwijkende) reisgedrag van de vervoersbewijsnummers in kaart te brengen.[228]

Uiteindelijk komt de NS op deze manier tot de identiteit van de waarschijnlijke dader. De politie kan het resultaat van het interne onderzoek, de wijze waarop de analyses hebben plaatsgevonden en de onderliggende gegevens die betrekking hebben op de verdenking vorderen.

Indien de houder hier niet zelf ervoor gekozen had om onderzoek te doen, zou de opsporing de bestanden hebben moeten vorderen en zelf de analyse hebben moeten uitvoeren om tot het gewenste resultaat te kunnen komen. Dit zijn enorme bestanden met alle kaart- en reisgegevens van heel veel Nederlanders. Uitlevering vragen van deze gegevens over zoveel onverdachte personen lijkt een buitenproportioneel brede inbreuk op de privacy. Daarnaast is de kans groot dat de verwerker van de gegevens ze niet wil verstrekken, vanwege reputatieschade of aansprakelijkheid.

[228] Zie *Tijdschrift voor de Politie* jrg. 79, 9 oktober 2017, p. 40 e.v.

Die afweging is mogelijk anders als er geen brand is gesticht maar er bijvoorbeeld mensen voor de trein zijn geduwd. Dan weegt het opsporingsbelang zwaarder, maar dat doet niet af aan de onwenselijkheid de gegevens van vrijwel de hele Nederlandse bevolking te vorderen. Het heeft de voorkeur om alleen de relevante informatie op basis van analyse te vorderen. Dit leidt tot een beperktere inbreuk op de privacy.

Casus FIOD

Banken verrichten op basis van hun complianceverplichtingen nu ook transactiemonitoring. Hierbij krijgen zij vaak zicht op bepaalde fiscale fraude als BTW-carrouselfraude, toeslagenfraude, uitkeringsfraude of subsidiefraude. Dit zijn allemaal vormen van bestandsanalyse. De uitkomsten van de analyse die de banken, veelal verplicht, al uitvoeren binnen hun huidige bedrijfsvoering kunnen gemeld worden aan de Financial Intelligence Unit. Opsporingsinstanties zouden in het geval van terrorismefinanciering bijvoorbeeld een bank willen vragen een bepaald profiel mee te nemen in hun analyse. Nu bestaat die wettelijke vorderingsbevoegdheid niet.

Casus vragen naar een identiteit op basis van kenmerken bij Google

Er is een dode baby gevonden in een meer. Uit de kleding die de baby droeg is af te leiden dat de moeder waarschijnlijk van Bulgaarse afkomst is. De baby ligt maximaal 10 uur in het water. Dan zou de vraag gesteld kunnen worden: is er gedurende dit tijdvak langs de oevers van dit meer een smartphone actief geweest met als taalinstelling Bulgaars (en mogelijk eerder actief in Bulgarije) van een vrouw die het belangstellingsprofiel had van een zwangere vrouw. Op advies van digitaal specialisten wordt deze vraag gesteld aan Google, omdat de kans dat de vrouw een Android-toestel zou hebben gehad relatief groot wordt ingeschat. Google zou deze vraag op basis van een relatief simpele bestandsanalyse kunnen uitvoeren.

Casus opvolgende analyseslagen uitvoeren Facebook

Er is een minderjarige seksueel misbruikt door een volwassen man, die haar groomde vanuit een Facebookprofiel dat leek toe te behoren aan een minderjarige jongen. Uit sociale-mediaonderzoek komt een heel netwerk van onecht ogende Facebookprofielen naar boven. Het vermoeden is dat meerdere personen tientallen Facebookprofielen besturen die elkaar geloofwaardigheid moeten geven, maar ook gebruikt worden om intieme contacten met andere minderjarigen te leggen. Uit publiek toegankelijke bronnen valt niet te herleiden welke profielen echt zijn en welke niet. De computer van de inmiddels aangehouden verdachte zit op slot.

De vraag die dan gesteld zou kunnen worden aan Facebook is: help ons bij het vinden van gelieerde accounts die ook intieme contacten leggen met minderjarigen, zodat deze minderjarigen kunnen worden gewaarschuwd en er nader onderzoek kan worden gedaan naar medeverdachten. Als je deze gegevens middels vorderen zou willen verkrijgen, dan zou dat ten minste de volgende stappen bevatten:

- alle identificerende kenmerken van het verdachte account;
- ID's van andere accounts die gebruik maken van dezelfde identificerende gegevens;
- voor zover niet overeenkomend met de eerste verdachte, de identificerende gegevens van hem bevriende accounts;
- van alle verdachte accounts in deze groep (accounts van de verdachte en accounts van mogelijke andere verdachten) de inhoud en contactenlijst;
- van verdachte accounts die gezien de inhoud en contactenlijst wellicht contact hebben met echte minderjarigen de inhoud van gesprekken om te beoordelen of er sprake was van grooming;
- de identificerende gegevens van de accounts van de potentiele minderjarige slachtoffers zodat met hen contact kan worden gezocht.

Als al deze tussenstappen gevorderd zouden moeten worden, dan kost dat veel tijd en brengt het wellicht de persoonsgegevens van niet-betrokken derden in beeld, terwijl de fraudeafdeling bij Facebook al bij de eerste bevraging kan zien wat het antwoord is.

7.1.3. Voorstel van de commissie-Mevis

Op basis van bovenstaande argumentatie acht de commissie het wenselijk dat een bevoegdheid wordt geïntroduceerd om data-analyse door derde partijen te vorderen. Dat er behoefte bestaat aan een bevoegdheid om beter en proportioneel gebruik te maken van informatie die beschikbaar is bij derden, is niet nieuw. De commissie-Mevis stelde al in mei 2001, in haar *Rapport van de Commissie Strafvorderlijke gegevensvergaring in de Informatiemaatschappij*, dat een bevoegdheid om het bewerken van data te kunnen vorderen nodig was. Ook voorspelde men dat het belang van een dergelijke bevoegdheid in de toekomst steeds groter zou worden. De dataficering van de samenleving, de mogelijkheid deze data te analyseren en de ontwikkelingen in de kunstmatige intelligentie hebben deze voorspelling bewaarheid.

De commissie-Mevis deed een concreet tekstvoorstel,[229] dat voor zover relevant luidde:

> **Artikel 126ng**
>
> 1. In geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, dat gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert, kan de officier van justitie, indien het belang van het onderzoek dit dringend vordert, van degene van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot gegevens die ten tijde van de vordering zijn opgeslagen in een geautomatiseerd werk, vorderen dat hij deze gegevens bewerkt en de daardoor verkregen gegevens verstrekt.
>
> 2. De vordering kan slechts gedaan worden na voorafgaande schriftelijke machtiging, op vordering van de officier van justitie te verlenen door de rechter-commissaris. (…)
>
> 5. De officier van justitie kan, gelet op het belang van het onderzoek, in de vordering bepalen dat degene tot wie de vordering is gericht, deze bewerking in overeenstemming met de aanwijzingen van de opsporingsambtenaar uitvoert.
>
> 6. De officier van justitie doet van de vordering proces-verbaal opmaken, waarin hij vermeldt:
> a. (…) een zo exact mogelijke beschrijving van de wijze waarop de bewerking is uitgevoerd. (…)

Het kabinet heeft destijds positief gereageerd op het advies van de commissie-Mevis, maar voorzag problemen bij het vragen aan een derde partij om een analyse uit te voeren. De voorkeur van het kabinet ging uit naar een algemene bevoegdheid om (grote) bestanden te laten analyseren door de opsporingsambtenaar zelf. Aan de bezwaren vanuit de bescherming van persoonsgegevens zou tegemoet worden gekomen door de analyse zoveel mogelijk langs geautomatiseerde weg, in een zogenoemde "black box",[230] te laten plaatsvinden, waarna alleen de resultaten van de analyse ten behoeve van opsporing zouden worden bewaard. Overige gegevens dienden te worden vernietigd.[231]

Voor het uitvoeren van grote bestandsanalyses is echter nadien geen specifieke regeling tot stand gekomen, zodat er, in tegenstelling tot de aanbeveling van de commissie-Mevis, geen

[229] Rapport van de Commissie Strafvorderlijke gegevensvergaring in de Informatiemaatschappij, mei 2001, p. 67-68.

[230] Het idee daarachter was niet dat onbekend zou blijven hoe het resultaat van de analyse tot stand was gekomen (zoals tegenwoordig vaak wordt bedoeld met de term "black box"), maar dat voorkomen moest worden dat de gegevens van derden die tijdens de analyse zouden worden verwerkt, maar niet in het resultaat zouden voorkomen, ter beschikking van de opsporing zouden komen. Tijdens de analyse zouden ze in een gescheiden systeem moeten blijven en na afloop worden vernietigd.

[231] *Kamerstukken II* 2001/02, 28 366, nr. 1.

mogelijkheid is geschapen om gegevens te vorderen die via bestandsanalyse worden geïdentificeerd uit grote databestanden van derde partijen.[232] Dat maakt het privacybezwaar van het vorderen van grote bestanden er niet kleiner op, integendeel: het leidt tot de hierboven beschreven onwenselijke situatie dat onnodig veel gegevens moeten worden gevorderd of dat, vanwege de disproportionaliteit van zo'n vordering, überhaupt geen gegevens kunnen worden gevorderd, ook als de gezochte gegevens zelf geen bijzonder grote privacyinbreuk zouden opleveren. Gekoppeld met de hierboven gesignaleerde sterk toegenomen hoeveelheid en complexiteit van databestanden bij derde partijen, waardoor het vorderen van gehele bestanden veelal een disproportionele privacyinbreuk zal opleveren, ziet de commissie aanleiding te adviseren om een voorstel in de lijn van dat van de commissie-Mevis in het toekomstige wetboek over te nemen.

7.1.4. Vormgeving en normering van de voorgestelde bevoegdheid

De tekst van het Mevis-voorstel biedt een prima vertrekpunt voor een bevoegdheid data-analyse door derden te vorderen. De verdenkings- en subsidiariteitscriteria zouden daarbij moeten worden aangepast aan de algemene lijn in het wetsvoorstel (zie daarover par. 4.2.4). Voor wat betreft de bevoegde autoriteit stelt de commissie dat het Mevis-voorstel, waarin alleen met machtiging van de rechter-commissaris data-analyses door derden kunnen worden gevorderd, te zwaar is. Er zijn immers ook de nodige gevallen van eenvoudig uit te voeren koppelingen tussen twee bestanden, die noch qua privacyinbreuk noch qua gevraagde inspanning door de derde partij ingrijpend zijn. De enkele omstandigheid dat van een derde een bepaalde analyse wordt gevergd, maakt de vordering niet per definitie ingrijpender dan de vordering van bepaalde gegevens zelf; de benodigde inspanning om bepaalde gegevens te produceren, rechtstreeks of via een bepaalde bewerkingsslag, zal immers sterk afhangen van de omvang en inrichting van de databestanden bij de derde.

Daarom stelt de commissie ook hier het algemene normeringscriterium voor, met dien verstande dat het feit dat van een derde partij een bepaalde inspanning wordt gevraagd, meegewogen moet worden. Naarmate een bevoegdheid meer inspanningen vergt van de derde is er een hogere autoriteit nodig die over de toepassing kan beslissen. Als uitgangspunt geldt daarbij dat naarmate de handelingen meer inspanning vergen van de derde van wie de medewerking wordt gevorderd en verder afliggen van zijn normale activiteiten, de wettelijke regeling zwaardere voorwaarden dient te bevatten.[233] Dit betekent dat een bestandsanalyse niet door een opsporingsambtenaar zelf kan worden bevolen; de afweging of de gevraagde inspanning van een derde kan worden verlangd, moet bij de officier van justitie worden belegd.

De bevoegde autoriteit is daarom de officier van justitie of, wanneer het gaat om op voorhand voorzienbare ingrijpende stelselmatigheid, de rechter-commissaris. Het feit dat het ook gaat om de mogelijke belasting van de bedrijfsvoering van de organisatie aan wie wordt gevraagd extra inspanning te verrichten om te komen tot een voor de opsporing bruikbaar resultaat, is een aanvullende factor die inzet van de rechter-commissaris kan rechtvaardigen. Weliswaar zullen de ter uitoefening van de vordering gemaakte kosten conform de gebruikelijke regeling (op basis van artikel 592 Sv) moeten worden vergoed, maar ook dan kan er bij een meer dan beperkte inspanning sprake zijn van een substantiële inbreuk op de normale bedrijfsvoering die een rechterlijke toetsing vooraf rechtvaardigt.

Samenvattend stelt de commissie voor om als bevoegde autoriteit de officier van justitie aan te wijzen wanneer de gevraagde analyse naar verwachting geen substantiële inbreuk op de normale bedrijfsvoering oplevert en er geen sprake is van ingrijpende stelselmatigheid. Een

[232] Het heeft mogelijk wel invloed gehad op artikel 126hh Sv, waarbij in geval van terreuronderzoek grote databestanden kunnen worden gevorderd om daar zelf analyses op uit te voeren.
[233] Zie ook *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 4 (Memorie van toelichting bij Wetsvoorstel bevoegdheden vorderen gegevens).

machtiging van de rechter-commissaris is vereist wanneer de gevraagde analyse een ingrijpend stelselmatig karakter draagt *of* wanneer de analyse een substantiële inbreuk op de normale bedrijfsvoering van het bedrijf vergt.

Wat een dergelijke inbreuk is, zal vooral afhangen van de bewerking die nodig is om de benodigde gegevens te produceren en de mate waarin deze bewerking binnen de normale bedrijfsvoering uitvoerbaar is; de mate van bewerking zal daarbij niet alleen afhangen van de zoekvraag, maar ook van de inrichting van de bestanden en de capaciteiten van de derde partij. Veelal zal een simpele koppeling tussen twee bestanden om een overeenkomst te vinden, een beperkte inbreuk opleveren; een bewerking waarbij vijf databanken gekoppeld moeten worden waarin allemaal verschillende zoeksleutels worden gebruikt, zal een grotere inbreuk op de bedrijfsvoering betekenen. Bij grotere bedrijven zal een analyse op eigen data door de fraude-afdeling meestal met betrekkelijk weinig inspanning kunnen worden uitgevoerd; die inspanning zal vaak geringer zijn dan de inspanning die moet worden verricht om enorme bestanden te kopiëren, veilig over te brengen naar het opsporingsdomein, en daar op speciale hardware en software door data-specialisten inzichtelijk en toegankelijk te maken alvorens deze kunnen worden geanalyseerd. Kleinere bedrijven zullen daarentegen een relatief grotere inspanning moeten leveren om bewerkingen uit te voeren op hun databestanden, zodat voor hen een gevraagde data-analyse sneller een grotere inbreuk op de bedrijfsvoering kan opleveren. Bij grote bedrijven zal een dergelijke data-analyse vaker voorkomen en daarmee makkelijker kunnen worden georganiseerd zonder substantiële invloed op het normale bedrijfsproces. De memorie van toelichting kan in deze lijn enkele voorbeelden geven van wat onder een substantiële inbreuk op de bedrijfsvoering moet worden verstaan, waarna in de jurisprudentie het criterium zich verder zal kunnen uitkristalliseren. Daarnaast zullen ook afspraken gemaakt kunnen worden met veel-bevraagde sectoren, zoals de banken en de telecommunicatieaanbieders, over welke inspanningen van hen kunnen worden verwacht bij vaker voorkomende typen van gevorderde data-analyse.

7.1.5. Afbakening ten opzichte van “gewone” gegevensvordering

De voorgestelde bevoegdheid tot data-analyse gaat verder dan een “gewone” vordering tot verstrekking van gegevens, omdat er een extra handeling – namelijk een bepaalde bewerking – wordt vereist. Dat betekent echter niet dat elke vorm van bewerking, of elke handeling die verder gaat dan het simpelweg opzoeken van een bepaald gegeven in een databestand, onder “data-analyse” valt. Het zal regelmatig voorkomen, ook nu al, dat voor een eenvoudige bevraging van gegevens een eenvoudige analyse plaats moet vinden, zoals het opzoeken in een administratie welk bestand op een server de juiste camerabeelden bevat. Ook kan het bij sommige NAW-verstrekkingen voorkomen dat eerst in een bestand van telecomnummer naar klantnummer wordt gezocht en daarna bij dat klantnummer de NAW-gegevens worden opgezocht in een ander bestand. Dergelijke meervoudige zoekhandelingen, die samenhangen met de manier waarop de gevorderde de gegevenshuishouding precies heeft ingericht, vallen gewoon onder de traditionele vordering van gegevens.

Bij data-analyse gaat het om bewerkingen die verder gaan dan meervoudige zoekhandelingen, bijvoorbeeld het integraal met elkaar vergelijken van alle gegevens in één dataset met alle gegevens in een andere dataset, om gegevens te identificeren die in beide datasets voorkomen. In de kern is het belangrijkste verschil tussen een “gewone” gegevensvordering en een data-analysevordering dat bij het eerste uiteindelijk gegevens worden geleverd die als zodanig ergens geregistreerd staan (hoewel meerdere handelingen nodig kunnen zijn om deze gegevens uit de databestanden te lichten), terwijl bij het laatste “nieuwe” gegevens worden geleverd, dat wil zeggen gegevens die nog niet *als zodanig* bij de gevorderde geregistreerd stonden. De scheidslijn tussen deze twee valt overigens niet haarscherp te trekken, aangezien de vraag of een gegeven “als zodanig” al geregistreerd staat of nieuw gegenereerd wordt, samenhangt met

de precieze inrichting van de gegevenshuishouding in het desbetreffende geval. In jurisprudentie zal waar nodig deze scheidslijn zich nader kunnen uitkristalliseren.

7.1.6. Controleerbaarheid van de gevraagde analyse

Indien de houder van gegevens gevraagd wordt een bewerkingsslag uit te voeren, doet zich voorts de vraag voor naar de betrouwbaarheid van deze bewerking en de uitkomsten daarvan. Dit speelt met name wanneer een analyse van data van een derde wordt gevorderd waarbij de zoekopdracht moet worden geïnterpreteerd of selecties moeten worden gemaakt. Deze vraag komt op bij data-analyses maar wordt normaliter niet gesteld bij het "gewoon" vorderen van databestanden van die dezelfde derden. Dat is niet helemaal terecht: deze derde heeft immers ook die bestanden samengesteld en daar bewerkingen op uitgevoerd in het kader van zijn eigen bedrijfsvoering en zal ook, afhankelijk van de inrichting van zijn gegevenshuishouding, een zekere beoordelingsmarge hebben om te bepalen welke gegevens nu precies onder de gevorderde gegevens vallen. De beoordelingsmarge zal, in het geval van een gevraagde bewerking, wel groter kunnen zijn dan bij de gemiddelde traditionele gegevensvordering het geval is. Om die reden is het van belang om, vergelijkbaar met de traditionele gegevensvordering, in de wettekst op te nemen dat het bevel tot data-analyse "een zo nauwkeurig mogelijke aanduiding van de bewerking" bevat die wordt bevolen. Afhankelijk van het geval zal dit een simpele aanduiding kunnen zijn, of een zeer gedetailleerde omschrijving van de gevraagde analyse; dat is niet anders dan bij het "gewoon" vorderen van gegevens, waarbij de specificiteit van de aanduiding ook afhangt van de omstandigheden van het geval.

Bij uitgevoerde analyses kan het in eerste instantie wenselijk lijken dat de volledige oorspronkelijke datasets bewaard worden, om de controleerbaarheid van de gemaakte analyses te verzekeren. In de inleiding is echter al beschreven dat databestanden steeds vaker veel te groot zijn om integraal over te nemen; ze zullen dus ook veel te groot zijn om volledig bewaard te worden. Wanneer een bank of Facebook op een bepaalde datum een analyse uitvoert op haar totale informatiesystemen, is het onmogelijk te eisen een kopie van het totale systeem te bewaren naar de stand van dat moment. Bovendien is het bij gewone gegevensvorderingen ook niet het geval dat oorspronkelijke datasets worden bewaard, terwijl daarbij evenzeer vragen kunnen spelen van de betrouwbaarheid van gemaakte selecties (bijvoorbeeld om te controleren of de gevorderde wel daadwerkelijke alle gevorderde gegevens heeft geleverd, en bijvoorbeeld geen fouten heeft gemaakt bij de interpretatie van de vordering).

Het gaat dus niet om de vraag of een analyse herhaalbaar is, maar om de eisen die worden gesteld aan de aantoonbare kwaliteit van de analyse. In het Mevis-voorstel wordt dit punt ondervangen door het voorgestelde vijfde lid, op basis waarvan de officier van justitie in zijn vordering kan bepalen dat de opsporing aanwijzingen kan geven over hoe de analyse moet worden uitgevoerd en hoe die moet worden vastgelegd. Dat biedt de mogelijkheid om hierbij voorwaarden aan de uitvoering te stellen, ook ten aanzien van de controleerbaarheid. Zo kan bijvoorbeeld gevraagd worden de exacte werkwijze bij de analyse te beschrijven in een rapportage of om de analyse door een tweede persoon te laten controleren of herhalen. Deze voorwaarden kunnen ook bepalen dat de werkzaamheden onder toezicht of door een opsporingsambtenaar of een aangewezen deskundige plaats dienen te vinden. Daarbij zal een rol spelen of een analyse wordt gevorderd van grote, ervaren bedrijven van wie regelmatig gegevens(-analyses) worden gevorderd, dan wel het een houder van een dataset betreft die minder ervaren is of minder betrouwbaar wordt geacht; in het laatste geval ligt het voor de hand dat de opsporing een grotere rol speelt, bijvoorbeeld door te ondersteunen met hardware, software en datatechnici waarbij het bedrijf alleen toegang hoeft te verlenen tot de benodigde data, zonder dat de (bruto) data worden overgenomen in politiesystemen. De officier van justitie heeft de ruimte om de voorwaarden aan te passen aan de specifieke casus, waarbij naast betrouwbaarheid ook afwegingen van proportionaliteit en subsidiariteit ten aanzien van de uitvoering een rol spelen.

De commissie adviseert in dit licht ook dit onderdeel van het Mevis-voorstel over te nemen. Door aldus in de wettelijke bevoegdheid de mogelijkheid op te nemen van het vorderen van een bewerkingsslag, die in het ene uiterste volledig wordt uitgevoerd door de houder en die, in het andere uiterste, volledig wordt uitgevoerd door, of onder direct toezicht staat van, opsporingsambtenaren, kan afhankelijk van de omstandigheden van het geval een goede balans worden gevonden ten aanzien van de proportionaliteit, betrouwbaarheid, controleerbaarheid, kostenverdeling en technische mogelijkheden van de opsporingsinstantie en van de houder.

Ten aanzien van de verlangde controleerbaarheid van de analyse kan tot slot onderscheid worden gemaakt naar de benodigde bewijskracht. Als in de eerder beschreven casus van het kinderlijkje de bevraging bij Google leidt naar één telefoon met één gebruikster, en uit een DNA-test blijkt dat deze vrouw de moeder van het kind is, dan zal de bewijsconstructie voornamelijk gebaseerd worden op het DNA-onderzoek. De analyse was dan meer richtinggevend voor het onderzoek. In een geval waarin de uitkomsten van de analyse als direct bewijs moeten dienen, zullen er mogelijk zwaardere eisen aan de controleerbaarheid moeten worden gesteld. Dit is een aandachtspunt dat meegenomen kan worden bij uitvoering van Aanbeveling 3 betreffende geautomatiseerde data-analyse en uitlegbaarheid van strafvorderlijke beslissingen (par. 3.4.2).

7.1.7. Flankerende bepalingen

Om de bevoegdheid tot data-analyse door derden goed te kunnen uitoefenen, zijn twee flankerende bepalingen nodig. Ten eerste moet de officier van justitie vooraf vragen kunnen (doen) stellen over de (opbouw van de) data en de inspanning die een bedrijf moet plegen om een bepaalde analyse uit te voeren. Dit stelt de officier van justitie in staat om te beoordelen of een vordering van data-analyse überhaupt zinvol is, en of, en zo ja welke, voorwaarden moeten worden verbonden aan de vordering met het oog op de controleerbaarheid. Tevens stelt dit de officier van justitie in staat een bevel zo eenduidig mogelijk te formuleren, opdat het weinig ruimte laat voor eigen interpretatie. Het maakt ook de beoordeling van proportionaliteit en subsidiariteit mogelijk. Zelfs een schijnbaar eenvoudige vraag als “kunt u alle betalingen aanleveren van uw rekeninghouders naar een bepaalde bankrekening van een derde bank?” zal door sommige banken immers eenvoudig kunnen worden geleverd, terwijl dit bij anderen niet gaat.

Het voorgestelde artikel 2.7.3.3.3 lid 4 geeft de opsporingsambtenaar de bevoegdheid om aan de houder van data relatief eenvoudige ja/nee-vragen te stellen om vast te stellen of de houder informatie heeft over een bepaald subject en het dus zinvol is een vordering te doen. De vraagbevoegdheid en informatieverplichting ten behoeve van het analysebevel zijn hiermee vergelijkbaar maar zouden verder dienen te gaan om de officier van justitie in staat te stellen de hierboven beschreven beoordelingen te maken. Bij de bevoegdheid tot data-analysevordering zou een vergelijkbaar lid kunnen worden ingevoerd met de strekking dat de officier van justitie, voor zover noodzakelijk voor de vordering van de data-analyse, degene die daarvoor redelijkerwijs in aanmerking komt kan bevelen inlichtingen te verstrekken over de inrichting van de gegevenshuishouding en de bewerkingen die nodig zijn om de bedoelde analyse uit te voeren.

Een tweede punt is dat het kan voorkomen dat de opsporingsinstantie in de vraagstelling ook politiegegevens moet verstrekken die noodzakelijk zijn om de gevraagde analyse voldoende gericht te kunnen uitvoeren. Het is daarom belangrijk dat de houder kan worden verplicht om in het kader van toepassing van dit artikel verkregen informatie geheim te houden en te vernietigen. Dit zal in het gemoderniseerde wetboek worden geregeld via artikel 2.7.3.1.4 (nu artikel 126bb lid 5 Sv).

Aanbeveling 70: er wordt een bevoegdheid ingevoerd voor de officier van justitie om, met een zo nauwkeurig mogelijke aanduiding van de gevraagde bewerking, data-analyse door derden te vorderen, met machtiging van de rechter-commissaris wanneer de gevraagde analyse een ingrijpend stelselmatig karakter draagt of wanneer de analyse een

substantiële inbreuk op de normale bedrijfsvoering van de gevorderde oplevert. Het desbetreffende voorstel van de commissie-Mevis kan daarbij als uitgangspunt dienen, aangepast aan de systematiek van het gemoderniseerde wetboek en conform bovenstaande voorstellen voor normering en flankerende bepalingen. → *p. 205*

7.2. Geautomatiseerde gezichtsherkenning

7.2.1. Inleiding

Geautomatiseerde gezichtsherkenning kent globaal twee vormen. Ten eerste het herkennen van gezichten als gezicht, met inbegrip van de gelaatsuitdrukking, wat relevant is voor bijvoorbeeld het inschatten van bepaalde gemoedstoestanden (emotiedetectie, agressiedetectie). Ten tweede het herkennen van gezichten als identificatiemiddel, waarbij het gezicht fungeert als een bepaald type biometrie. Het eerste type is relevant in het kader van handhaving van de openbare orde, maar niet direct voor opsporing. In de context van dit rapport richten wij ons daarom op het tweede type: gezichtsherkenning ter identificatie van individuen.

Binnen de politie wordt op dit punt overigens niet gesproken over "gezichtsherkenning", maar over "gelaatsvergelijking". Hoewel dat een accuratere term is, zoals hierna wordt toegelicht, hanteren wij hier nog "gezichtsherkenning" omdat dit in het debat vooralsnog de meest gebruikte term is.

Behalve herkenning op basis van gezichten, is herkenning ook mogelijk op basis van andere persoonlijke kenmerken, zoals tatoeages, stemmen of een looppatroon. De commissie acht de hieronder beschreven afwegingen in beginsel ook toepasselijk op dergelijke vormen van identificatie, maar beperkt zich hier tot gezichtsherkenning. Dit vanwege het feit dat gezichtsherkenning naar het oordeel van de commissie de komende jaren met afstand de meest voorkomende vorm van (geautomatiseerde) herkenning zal zijn ten behoeve van de opsporing.

7.2.2. Huidig proces

Voor gezichtsherkenning is een afbeelding van een gezicht nodig (meestal een foto, maar in de toekomst wellicht ook bewegend beeld) en bepaalde software. Van het afgebeelde gezicht worden kenmerken op gestandaardiseerde wijze vastgelegd, bijvoorbeeld de vorm van het gezicht en de afstand tussen enkele vaste punten in het gezicht. Die kenmerken kunnen dan vergeleken worden met de kenmerken van een ander gezicht waarvan een afbeelding op dezelfde wijze is verwerkt.

De software genereert vervolgens een score die weergeeft in welke mate de kenmerken overeenkomen. De software geeft vanzelfsprekend de afbeeldingen weer die de grootste overeenkomst vertonen. Er wordt door de software geen standpunt ingenomen over de vraag of twee vergeleken gezichten van dezelfde persoon zijn. Er worden dus geen gezichten "herkend": er worden gezichten (gelaten) vergeleken. Als de software een hoge score oplevert, bekijken specialisten de afbeeldingen om te zien of er naar hun oordeel sprake kan zijn van een match. Ook zij geven geen definitief oordeel of het wel of niet dezelfde persoon betreft; zij geven wel aan of er naar hun oordeel veel overeenkomsten zijn. De gelaatsvergelijking of gezichtsherkenning leidt dus niet tot een definitief "ja" of "nee" – er moet altijd worden doorgerechercheerd om te kunnen vaststellen of het daadwerkelijk om dezelfde persoon gaat.

De kwaliteit van de afbeelding bepaalt in grote mate de kans op een succesvolle vergelijking. Omstandigheden als de hoek en de kwaliteit van de opname, hoeveelheid licht, maar ook petjes of andere obstakels, hebben een grote invloed op gezichtsherkenning. Op dit punt wordt technische vooruitgang geboekt, zoals het ontwikkelen van software die het gefotografeerde gezicht kan "draaien" zodat de vergelijking beter kan worden uitgevoerd.

Hoewel gezichtsherkenning technisch nog niet op grote schaal met voldoende nauwkeurigheid mogelijk is, heeft de techniek zich de afgelopen jaren wel snel ontwikkeld. Daarbij verbetert de software waarmee de gezichtsvergelijking wordt uitgevoerd, wat leidt tot een

grotere betrouwbaarheid van de uitkomsten. De verwachting is dat binnen afzienbare tijd meer toepassingen, zowel voor private als publieke actoren, op de markt zullen komen.

7.2.3. Verschillende (huidige en toekomstige) toepassingen

Gezichtsherkenning kan op verschillende manieren worden toegepast voor de opsporing (en binnen andere domeinen). Deze paragraaf brengt in algemene zin die verschillende toepassingen in beeld. Niet al die toepassingen worden op dit moment gebruikt binnen de Nederlandse opsporingsorganisaties. Daar zijn verschillende redenen voor, bijvoorbeeld de stand van de techniek, de mate waarin toepassingen toegelaten zijn binnen het huidige wet- en regelgevingskader, het ontbreken van de noodzaak in de huidige praktijk, of een combinatie van dergelijke factoren. Voor een goed overzicht over de materie en gelet op de wens om toekomstbestendige wetgeving te hebben, benoemt de commissie wel de verschillende mogelijke toepassingen, ook als er op dit moment geen concrete wens is om die toepassingen mogelijk te maken of te gebruiken.

In de eerste plaats is van belang dat er bij gezichtsherkenning sprake is van een “linkerkant” en een “rechterkant” van de vergelijking. De linkerkant betreft het gezicht of de gezichten die je wil vergelijken, bijvoorbeeld om de bijbehorende identiteit vast te stellen. De rechterkant betreft het vergelijkingsmateriaal, namelijk gezichten waarvan je over meer informatie beschikt, zoals de identiteit.

Aan zowel de linker- als de rechterkant van de vergelijking kunnen verschillende sets gezichten worden geplaatst. Er kan aan beide zijden sprake zijn van één (1) specifiek gezicht, maar er ook kan sprake zijn van een set gezichten, bijvoorbeeld een bekende dadergroep. Een dergelijke set wordt aangeduid met de letter “s”. Daarnaast kan aan beide zijden van de vergelijking sprake zijn van een bredere set gegevens zoals een gehele database. Die wordt aangeduid met de letter “n”.

Staat in de linkerkant van de vergelijking een “1”, dan geeft dit aan dat de identiteit van die ene specifieke persoon wordt gezocht. De rechterkant van het schema bepaalt dan met welke set gegevens wordt geprobeerd die identificatie te bewerkstelligen; dit kan één persoon zijn (1), een bepaalde, vastomlijnde groep (s) of een meer onbepaalde, in potentieel grote groep (n).

Staat in de linkerkant van de vergelijking een “s”, dan geeft dit bijvoorbeeld aan dat er binnen een bepaalde verzameling personen (de “s”) wordt gezocht naar bepaalde bekenden, zoals verdachten. De “s” staat dan bijvoorbeeld voor alle personen op een bepaald plein of station.

Staat in de linkerkant van de vergelijking een “n”, dan betreft het een soortgelijke toepassing, maar minder gericht, bijvoorbeeld wanneer op alle locaties waar camera’s hangen onder alle gefilmde mensen (de “n”) gezocht zou worden naar bekenden, zoals verdachten.

Schematisch zijn dan de volgende vergelijkingen mogelijk.

Links	*Rechts*	*Omschrijving vergelijking*
1	1	Is dit de persoon die we denken dat het is?
1	s	Zit deze persoon in de bekende dadergroep?
1	n	Wie is deze persoon?
s	1	Is degene die we zoeken aanwezig op dit plein?
s	s	Zijn de mensen die we gericht zoeken aanwezig op dit plein?
s	n	Zijn er op dit plein bekende verdachten of veroordeelden aanwezig?
n	1	Is degene die we zoeken aanwezig op een van de locaties waar camera’s hangen?
n	s	Zijn de mensen die we gericht zoeken aanwezig op een van de locaties waar camera’s hangen?
n	n	Zijn er bekende verdachten of veroordeelden aanwezig op een van de locaties waar camera’s hangen?

7.2.4. Toepassing binnen de opsporing

Binnen de opsporing wordt op dit moment hoofdzakelijk gebruik gemaakt van geautomatiseerde gezichtsherkenning voor twee doeleinden:

1. het verifiëren van de identiteit van een verdachte of veroordeelde, en
2. om te bezien of (nieuwe) verdachten of veroordeelden reeds voorkomen in de strafrechtsketendatabank, bedoeld in artikel 27b, vierde lid, Sv juncto artikel 2, onderdeel g, van het Besluit identiteitsvaststelling verdachten en veroordeelden.

Het eerste voorbeeld betreft de situatie waarin er bij een bepaalde persoon reeds een identiteit wordt vermoed, en waarbij de geautomatiseerde vergelijking wordt gebruikt om te bevestigen of het inderdaad de desbetreffende persoon is. Dit betreft een "1-op-1"-vergelijking.

De tweede toepassing kan bijvoorbeeld gaan om een van een winkelier ontvangen foto van een winkeldief. Die foto wordt dan vergeleken met bekende verdachten of veroordeelden. Dit kan zowel een "1-op-s"-vergelijking zijn, wanneer vermoed wordt dat de desbetreffende persoon deel uitmaakt van een bepaalde subset van verdachten, zoals een bepaalde groep lokale veelplegers. Het kan ook een "1-op-n"-vergelijking zijn wanneer een dergelijk vermoeden er niet is en in een bredere, meer onbepaalde kring wordt gezocht. Zie voor de huidige praktijk een recent artikel in NRC.[234]

De grondslag voor deze tweede vorm van vergelijking ligt, wanneer vergeleken wordt met de databank van verdachten en veroordeelden, in artikel 55c, vierde lid, Sv. Deze bepaling regelt dat de in de databank opgenomen foto's van aangehouden verdachten en van veroordeelden ook kunnen worden verwerkt voor het voorkomen, opsporen, vervolgen en berechten van strafbare feiten en het vaststellen van de identiteit van een lijk. De inhoud van dit artikellid blijft ook bij het gemoderniseerde wetboek gehandhaafd.[235]

Een dergelijke "1-op-n"-vergelijking is op dit moment ook mogelijk met als referentiedatabank (dus aan de rechterkant) de databank met gezichten van vreemdelingen. Daarvoor geldt echter een andere juridische grondslag, met extra waarborgen, zoals een machtiging van de rechter-commissaris.

In het hierboven genoemde NRC-artikel is te lezen dat de politie experimenteert met software die gezichten in een opgenomen video van mensenmassa's herkent. Dit kan in de toekomst dus wellicht een van de manieren zijn waarbij de "s" in de linkerkant van de vergelijking staat, dus zodanig dat een video van de mensenmassa geautomatiseerd wordt vergeleken met een referentiedatabank van een of meerdere personen.

7.2.5. De indringendheid van de geautomatiseerde gezichtsherkenning

Betoogd kan worden dat het toepassen van gezichtsherkenning inbegrepen is in de rechtmatige uitoefening van enige bevoegdheid tot (al dan niet stelselmatige) observatie: daarbij mogen immers met gebruik van technische hulpmiddelen personen worden geobserveerd, en vastgelegde beelden mogen worden geanalyseerd. Ook vindt bij observatie van oudsher al (menselijke) gezichtsherkenning plaats doordat een observerende opsporingsambtenaar op basis van het geheugen personen kan herkennen in de omgeving van de geobserveerde persoon.

Daar kan tegenin worden gebracht dat door geautomatiseerde gezichtsherkenning de schaal en mogelijk ook het karakter van observatie verandert, omdat het herkennen van personen uit het geheugen een beperkte reikwijdte heeft, terwijl het geautomatiseerd herkennen van perso-

[234] https://www.nrc.nl/nieuws/2018/02/19/politiesoftware-scant-gezichten-van-verdachten-a1592781 (laatst geraadpleegd 1 juni 2018).

[235] Dit wordt niet in het nieuwe wetboek zelf geregeld maar in een wet die de regels over het verwerken van gegevens in de strafrechtsketen zal bevatten en waarin de Wjsg en de Wpg zullen opgaan. In afwachting van die wet zal de inhoud van dit artikellid worden opgenomen in een tijdelijke algemene maatregel van bestuur waarin de huidige regels worden neergelegd over de verwerking van gegevens die door de uitoefening van strafvorderlijke bevoegdheden zijn verkregen. Zie de toelichting op artikel 1.10.7 van het conceptwetsvoorstel Boek 1.

nen onafhankelijk is van de individuele observant en potentieel een groot bereik heeft, afhankelijk van welke gezichten vergeleken worden (de linkerkant: "1", "s" of "n"?), en de omvang van de referentiedatabank waarmee zij vergeleken worden (de rechterkant: "1", "s" of "n"?). Waar spontane herkenning van personen eerder uitzondering dan regel zal zijn, kan de identificatie van personen met geautomatiseerde gezichtsherkenning eerder regel dan uitzondering worden (wederom afhankelijk van de reikwijdte van de gebruikte datasets aan zowel linker- als rechterkant). Dit is zeker het geval bij de "n-op-n"-vergelijking, namelijk daar waar *alle* vastgelegde gezichten vergeleken worden met een gehele, meer onbepaalde referentiedatabank, maar kan ook het geval zijn bij vergelijkingen van "s-op-n", "n-op-s" of "s-op-s", en mogelijk ook bij "n-op-1"-vergelijkingen, afhankelijk van het toepassingsbereik van deze vergelijkingen. Dit betekent dat de indringendheid van observatie kan toenemen als daarbinnen geautomatiseerde gezichtsherkenning wordt gebruikt.

In dit verband is voor dit rapport in het bijzonder de normering van het identificeren van personen binnen (stelselmatige) observatie een relevant onderwerp. Het toepassen van geautomatiseerde gezichtsherkenning bij de observatie van een verdachte sluit direct aan op de doelstelling van de observatie: het in kaart brengen van de handelingen en contacten van de geobserveerde persoon. Daarvoor is als zodanig geen aanvullende normering nodig. Wel zal het gebruik van geautomatiseerde gezichtsherkenning een factor zijn die meeweegt in de beoordeling of er sprake is van stelselmatigheid (zie par. 5.3.3): de drempel zal sneller worden gehaald, ook bij kortdurende observaties, omdat een bepaald aspect van het persoonlijk leven van de verdachte sneller in kaart kan worden gebracht, namelijk met wie hij allemaal contact heeft. Ook kan het gebruik van geautomatiseerde gezichtsherkenning, als de referentiedatabank groot is,[236] leiden tot indringende stelselmatigheid wanneer de observatie en de gezichtsherkenning continu en gedurende meerdere weken plaatsvindt. Gedurende een langere periode zal de verdachte immers met veel mensen, in verschillende contexten contact hebben, zodat een groot deel van zijn persoonlijke netwerk in kaart wordt gebracht. Daarmee kan een indringend beeld, in de brede zin van een min of meer volledig beeld van meerdere delen van iemands privéleven, ontstaan. De commissie adviseert in dat licht om het gebruik van gezichtsherkenning om personen te identificeren met wie een geobserveerde verdachte interacteert, als factor mee te wegen in de beoordeling of er sprake is van (ingrijpende) stelselmatigheid.

Aanbeveling 71: in de memorie van toelichting moet aandacht worden besteed aan het gebruik bij observatie van geautomatiseerde gezichtsherkenning om personen te identificeren met wie de geobserveerde interacteert, waarbij dit gebruik als factor dient mee te wegen bij de beoordeling of er sprake is van (ingrijpende) stelselmatigheid. → *p. 205*

7.2.6. Het bestaande juridische kader

De commissie constateert dat de huidige toepassingen van gezichtsherkenning worden gebaseerd op bestaande wettelijke grondslagen, waarvan het genoemde artikel 55c, vierde lid, Sv een belangrijk voorbeeld is. De commissie acht het daarnaast goed mogelijk dat er toepassingen zijn van geautomatiseerde gezichtsherkenning die slechts een geringe inbreuk op de persoonlijke levenssfeer maken, waarvoor de taakstellende artikelen als basis kunnen dienen.

De commissie constateert daarbij dat de desbetreffende regelgeving niet gemaakt is met als doel het reguleren van gezichtsherkenning. De genoemde bepalingen komen uit een tijd waarin gezichtsherkenningstechnologie nog niet beschikbaar was. De toepassingen van gezichtsherkenning kunnen dus weliswaar getoetst worden aan bestaande regels, en onder omstandigheden

[236] Bijvoorbeeld als deze niet alleen mensen met een strafblad bevat maar ook bijvoorbeeld (potentiële) getuigen, of als foto's van sociale netwerken worden gebruikt in een referentiedatabank.

daaronder ook rechtmatig worden uitgeoefend, maar dat neemt niet weg dat er rondom gezichtsherkenning geen gerichte wettelijke grondslagen zijn opgesteld, en dat over toepassingen hiervan in de strafvordering ook nog weinig maatschappelijk of politiek debat is gevoerd.

De sterke ontwikkeling van de technische mogelijkheden rondom gezichtsherkenning en de nog te verwachten toekomstige mogelijkheden, waarbij in technische zin steeds sneller en massaler gezichtsvergelijking mogelijk kan worden, betekenen dat de indringendheid van de inbreuk op de persoonlijke levenssfeer van personen bij de toepassing van geautomatiseerde gezichtsherkenning zeer kan toenemen. Deze toenemende indringendheid is aanleiding om zeer zorgvuldig om te gaan met het inzetten van nieuwe mogelijkheden tot gezichtsherkenning, bijvoorbeeld door een uitvoerig besluitvormingsproces plaats te laten vinden conform hetgeen daarover is gezegd in de visie op sensing van het kabinet[237]. Hoe breder en ongerichter de toepassing van gezichtsvergelijking dan is, des te zwaarder de toets zal moeten zijn over de toelaatbaarheid daarvan. De commissie acht het, wederom vanwege de toenemende indringendheid, dan ook denkbaar dat in de toekomst een specifieke regeling nodig is.

De commissie vindt dat er op dit moment nog onvoldoende duidelijk is over de wensen en behoeften van de opsporing, de maatschappij en de politiek voor wat betreft de inzet van geautomatiseerde gezichtsherkenning binnen de opsporing die verder gaat dan de huidige toegestane vormen van gerichte gezichtsherkenning. De commissie acht het daarom niet binnen haar opdracht passen om hier op dit moment nader inhoud aan te geven. Vanwege de snel voortschrijdende technologie acht de commissie het raadzaam om op dit vlak te starten met visievorming en maatschappelijk debat. Daarbij kan aandacht worden besteed aan diverse relevante aspecten, zoals de vraag welk beeldmateriaal onder welke omstandigheden gebruikt mag worden voor gezichtsvergelijking, waarmee vergeleken mag worden, in welke gevallen er toestemming nodig is van een hogere autoriteit en welke bewaartermijnen worden gehanteerd. Ook is van belang hoe wordt omgegaan met “hits” en “no-hits”, mede gelet op de constatering dat de vraag wat een “hit” is, gecompliceerder ligt dan bij sommige andere technieken, aangezien de gelaatsvergelijking slechts een bepaalde score oplevert voor de mate van waarschijnlijkheid van een match en de technologie, zeker in ongecontroleerde omstandigheden zoals opnames van bewegende mensen in de publieke ruimte, een niet-verwaarloosbaar percentage fout-positieven zal kennen.

Aanbeveling 72: de commissie adviseert het kabinet om te starten met visievorming en maatschappelijk en politiek debat te entameren over de inzet van geautomatiseerde gezichtsherkenning binnen de opsporing. → *p. 205*

[237] *Kamerstukken II* 2015-16, 29 628, nr. 594.

8. Samenvatting, conclusies en aanbevelingen

In dit hoofdstuk geven we een overzicht van de bevindingen van het rapport in de vorm van een samenvatting van de belangrijkste bevindingen en conclusies, met verwijzing naar de aanbevelingen die door de tekst heen zijn gedaan. Deze verwijzingen zijn aanklikbaar, zodat de lezer (althans in de digitale versie van dit rapport) eenvoudig naar de desbetreffende aanbeveling kan navigeren en kennis kan nemen van de bijbehorende analyse en context.

8.1. Inleidende beschouwingen

hfd. 1 De commissie modernisering opsporingsonderzoek in het digitale tijdperk is ingesteld om te adviseren over de toekomstbestendigheid van het "pakket" van bevoegdheden in het conceptwetsvoorstel Boek 2 van het gemoderniseerde Wetboek van Strafvordering, en van de klassieke manier van normeren in het strafprocesrecht, in een digitale context. Specifieke onderdelen van de opdracht betroffen de werkbaarheid van de voorgestelde bepalingen over "inbeslagneming" van gegevens en de gevolgen van het smartphone-arrest van de Hoge Raad (ECLI:NL:HR: 2017:584) voor de voorgestelde regeling. Het gemoderniseerde wetboek treedt naar verwachting pas over een aantal jaren in werking en zou dan idealiter qua systematiek minstens tien tot vijftien jaar moeten meegaan. De commissie kan echter niet verder vooruitkijken dan ongeveer 2030, vanwege de onvoorzienbaarheid van technische ontwikkelingen op (middel)lange termijn. Het rapport kent ook andere beperkingen, in verband met de relatief beperkt beschikbare tijd voor het advies in combinatie met de complexiteit van de materie. Het rapport biedt daarom geen uitputtende antwoorden, noch kant en klare wetteksten; het advies richt zich meer op grote lijnen, systematiek, handvatten en concepten. De samenstelling van commissie (vertegenwoordigers van opsporingsdiensten, Openbaar Ministerie, zittende magistratuur, advocatuur en wetenschap) brengt met zich mee dat niet altijd is gestreefd naar consensus, maar naar voorstellen die een redelijke middenweg bewandelen gelet op de uiteenlopende belangen en visies die bij de discussies in de commissie naar voren zijn gekomen.

hfd. 2 Het rapport bevat een grove schets van de **contouren van het huidige digitale landschap** en voorzienbare grote ontwikkelingen daarin. Dit hoofdstuk kan de minder technisch georiënteerde lezer enig houvast bieden voor de techno-sociale context waarin de analyses en adviezen in het rapport kunnen worden geplaatst. De enorme digitalisering van alle aspecten van het dagelijks leven biedt zowel kansen voor de opsporing (er zijn meer data beschikbaar, en grootschalige dataopslag en geautomatiseerde data-analyse bieden nieuwe mogelijkheden) als bedreigingen (bijvoorbeeld door toegenomen versleuteling of jurisdictieproblemen bij opslag van data in de cloud). Daarbij is een steeds verdergaande automatisering van de leefomgeving te verwachten, waarbij steeds meer data worden gegenereerd en opgeslagen ("dataficering"), vaak ook in een ander land. Technologische ontwikkelingen volgen elkaar snel op, zodat ze moeilijk te vangen zijn in vaste juridische kaders. Het digitale landschap wordt bevolkt door nieuwe (internationale) partijen (zoals platforms), en bestaande partijen krijgen een andere rol (zoals burgers of bedrijven die actief bijdragen aan opsporing). De fysieke wereld en de digitale wereld raken steeds meer verknoopt tot een gemengde werkelijkheid, wat betekent dat bij de regulering van digitale opsporingsbevoegdheden rekening moet worden gehouden met de verwevenheid van de fysieke leefwereld en digitale gegevens.

hfd. 3 Alvorens verbetervoorstellen te doen voor de bevoegdheden in Boek 2, signaleert de commissie diverse aandachtspunten die suggereren dat een **bredere reflectie nodig** is dan enkele aanpassingen in het conceptwetsvoorstel. Sommige onderwerpen die de commissieopdracht overstijgen, zoals jurisdictie, vergen zelfstandig en dringend aandacht, waarbij internationaal

overleg nodig is over grensoverschrijdende opsporing. Andere aandachtspunten hebben implicaties voor de houdbaarheid van een gemoderniseerd wetboek op de (middel)lange termijn. Zo heeft het verschuiven van klassieke doelen van strafvordering (niet alleen of altijd primair gericht op vervolging, maar ook of hoofdzakelijk gericht op het beëindigen van een strafbaar feit) op langere termijn gevolgen voor het strafvorderlijk systeem als geheel en de normering daarvan (zie Aanbeveling 1). De commissie benadrukt het belang van:

- een integrale visie op de normering van zowel gegevensvergaring als -gebruik, waarbij Sv en Wpg in samenhang moeten worden bezien (zie Aanbeveling 2);
- het ontwikkelen van een visie op geautomatiseerde data-analyse binnen strafvordering, met eventueel expliciteren van de impliciete eis van uitlegbaarheid van strafvorderlijke beslissingen (zie Aanbeveling 3);
- reflectie op de systematiek van normering; aangezien het vanwege de "dataficering" steeds eenvoudiger is aspecten van het privéleven scherp in beeld te brengen, is voorzienbaar dat meer betrokkenheid van de rechter-commissaris nodig is, wat op korte termijn capaciteitsuitbreiding veronderstelt en op langere termijn de systematiek van normering onder druk zet (zie Aanbeveling 4); en
- reflectie op het stelsel van toezicht vooraf en achteraf, mede omdat lang niet alle zaken uiteindelijk voor de rechter komen en omdat bij digitale opsporing ook vaak gegevens in beeld komen van derden (niet-verdachten) (zie Aanbeveling 5).

Na deze signalering van fundamentele aandachtspunten heeft de commissie vervolgens geprobeerd om in de rest van het rapport, binnen de bestaande kaders en binnen de beperkingen van haar opdracht, voorstellen te doen om de werkbaarheid en toekomstbestendigheid van de regeling van opsporingsbevoegdheden in een digitale context te bevorderen.

8.2. Algemene benadering in normering

§4.1 Het advies over de regulering van opsporingsbevoegdheden in Boek 2 is gestoeld op een algemene benadering in normering. De wetgever moet rekening houden met een wereld waarin de digitalisering tot in de haarvaten is doorgedrongen, waarbij maatschappelijke processen door alle datastromen in een versnelling raken en grenzen van ruimte en tijd vervluchtigen. De consequentie daarvan is dat vastomlijnde concepten en ankerpunten weinig houvast bieden. Dit betekent dat toekomstbestendige wetgeving voldoende techniek-onafhankelijk moet zijn. De commissie adviseert daarom in de nieuwe wet tamelijk **abstracte concepten** op te nemen, waarbij – om rechtszekerheid te bevorderen – de memorie van toelichting door heldere voorbeelden, maatstaven en argumenten duidelijk moet maken hoe die concepten in de huidige en toekomstige praktijk uitwerken.

Een belangrijke waarborg tegen inbreuken op de privacy (persoonlijke levenssfeer) wordt vaak gevonden in de autoriteit die toestemming moet geven voor die inbreuk: een zwaardere inbreuk vergt een hogere autoriteit. Opsporingsambtenaren mogen over het algemeen (uitzonderingen, zoals spoedgevallen, daargelaten) zelfstandig handelen als sprake is van geen of een geringe inbreuk; bij een meer dan geringe inbreuk is veelal de officier van justitie bevoegd, en bij zeer ingrijpende inbreuken de rechter-commissaris. Voor de vormgeving van toekomstige opsporingsbevoegdheden zijn in dit verband van rechtspraak van het Europees Hof voor de Rechten van de Mens alleen de grote lijnen bruikbaar, omdat de Europese rechtspraak casuïstisch is en de uitspraken (vanwege de lange doorlooptijd) veelal betrekking hebben op oude, soms achterhaalde technieken.

§4.2 In het digitale tijdperk is het moeilijker om op voorhand een vast beschermingsniveau te koppelen aan een bepaalde bevoegdheid: de ernst van de inbreuk hangt vooral af van de context. De commissie trekt hieruit de conclusie dat het nieuwe wetboek moet werken met abstracte normering, die per geval kan worden geïnterpreteerd, waarbij het wenselijk is deze normering

in het hele stelsel van bevoegdheden door te voeren. De commissie stelt in dat licht een **algemeen normeringscriterium** voor van **(ingrijpende) stelselmatigheid**, dat in brede zin kan worden gebruikt om onderscheid te maken tussen geringe, meer dan geringe en zeer ingrijpende inbreuken en het daarmee (in de regel) samenhangende onderscheid tussen opsporingsambtenaar, officier van justitie en rechter-commissaris als bevoegde autoriteit (zie Aanbeveling 6).

Stelselmatigheid is als criterium breder toepasbaar dan bij de enkele huidige bijzondere opsporingsbevoegdheden waarin het begrip voorkomt; het wordt ook (impliciet) gehanteerd in het smartphone-arrest. Volgens de commissie is het, door de abstracte invulling, breed bruikbaar. De betekenis van "stelselmatig" is daarbij niet die van het normale spraakgebruik (waarin het veelal ziet op een herhaalde actie), maar kent een specifieke juridische invulling: de uitoefening van een bevoegdheid is stelselmatig als daarbij *op voorhand redelijkerwijs voorzienbaar een min of meer volledig beeld van bepaalde aspecten van iemands privéleven* kan ontstaan (vgl. Aanbeveling 56). "Op voorhand redelijkerwijs voorzienbaar" geeft aan dat de vraag of uitoefening van een bevoegdheid stelselmatig is vóór de inzet wordt beoordeeld, en geobjectiveerd is: het gaat om wat een opsporingsfunctionaris redelijkerwijs zou moeten voorzien, aan de hand van algemene en context-specifieke ervaringsregels en van een redelijke inschatting van de omstandigheden van het concrete geval (vgl. ook Aanbeveling 57). Bij de interpretatie van het begrip "stelselmatig" kan deels worden aangesloten bij bestaande rechtspraak (bijvoorbeeld rond stelselmatige observatie), maar de invulling moet worden aangepast en uitgebreid, omdat bij digitaal onderzoek plaats en duur weinig relevante factoren zijn, terwijl bijvoorbeeld type drager, hoeveelheid gegevens en automatisering van het onderzoek relevante factoren zijn voor stelselmatigheid in een digitale context. Voor stelselmatige inzet van bevoegdheden is in beginsel de officier van justitie de bevoegde autoriteit.[238]

Voor aanwijzing van de rechter-commissaris als beslissende autoriteit stelt de commissie *ingrijpende stelselmatigheid* als criterium voor. Dit betekent dat op voorhand redelijkerwijs voorzienbaar is dat een *ingrijpend* beeld van iemands privéleven kan ontstaan. Ingrijpend kan daarbij "diep" zijn, als het een min of meer volledig beeld van een *wezenlijk* deel van iemands privéleven betreft (veelal maar niet per se samenhangend met iemands medische, seksuele, religieuze, politieke of etnische identiteit), of "breed", als een min of meer volledig beeld ontstaat van een significant aantal aspecten van iemands privéleven, waardoor een *aanzienlijk* deel van iemands privéleven wordt blootgelegd. Ingrijpende stelselmatigheid is altijd aan de orde als redelijkerwijs voorzienbaar is dat te onderzoeken gegevens vallen onder het professioneel verschoningsrecht. Daarbuiten is het lastig factoren aan te duiden die in alle gevallen wijzen op ingrijpende stelselmatigheid. Een ingrijpend beeld van iemands privéleven zal veelal samenhangen met zogenoemde "gevoelige" gegevens, maar lang niet altijd zullen gevoelige gegevens een ingrijpend beeld opleveren – dat hangt af van de hoeveelheid, aard en overige contextuele factoren. Volgens de commissie zal stelselmatige ingrijpendheid daarom een uitzondering zijn: de rechter-commissaris zal slechts in bijzondere gevallen behoeven te beslissen (al zal die betrokkenheid in de toekomst wel kunnen of moeten toenemen vanwege de genoemde "dataficering").

(Ingrijpende) stelselmatigheid is door zijn abstractie bruikbaar als breed toepasbaar criterium voor de regulering van opsporingsbevoegdheden in het digitale tijdperk. Een deel van de commissie heeft aarzelingen bij het breed toepasbaar verklaren van het criterium in verband met de behoefte aan duidelijkheid en toepasbaarheid (zie p. 136). De commissie beseft dan ook dat het door de abstractie geconcretiseerd zal moeten worden om bruikbaar te zijn in de praktijk. Dit betekent dat in de memorie van toelichting heldere voorbeelden, maatstaven en argumenten gegeven moeten worden om richting te geven aan praktijk en jurisprudentie, voor uiteenlopende toepassingen van bevoegdheden die voor de komende jaren relevant zijn. De commissie geeft

[238] De wetgever kan in bepaalde, specifieke gevallen eventueel een opsporingsambtenaar aanwijzen als bevoegde autoriteit.

daartoe in dit rapport de nodige aanzetten met voorbeelden en argumenten. Vervolgens kunnen rechtspraktijk en rechtsontwikkeling het abstracte criterium verder vorm geven.

De wet kent naast de bevoegde autoriteit ook andere criteria voor de inzet van bevoegdheden. De commissie adviseert om steeds wanneer uitoefening van een bevoegdheid redelijkerwijs voorzienbaar ingrijpende stelselmatigheid oplevert, voor te schrijven dat de inzet ook dringend vereist is (zie Aanbeveling 7). Evenzo ligt het voor de hand de inzet van bevoegdheden die (ingrijpende) stelselmatigheid opleveren, te koppelen aan bepaalde verdenkingscriteria (dat wil zeggen een niveau van ernst van het strafbare feit). Daarbij merkt de commissie op dat het moeilijk is op voorhand in zijn algemeenheid te bepalen bij welke mate van ernst van strafbare feiten toepassing van een bevoegdheid nog aanvaardbaar is. De commissie adviseert daarom een vangnetbepaling in te voeren, met de strekking dat de rechter-commissaris machtiging kan geven voor inzet van een bevoegdheid voor een lichter strafbaar feit dan waarvoor een bevoegdheid in het algemeen is toegelaten (zie Aanbeveling 8).

Het rapport gaat uit van de gedachte dat privacybescherming het meest direct in het geding is bij opsporing in een digitale omgeving en bevat geen specifieke adviezen over andere grondslagen voor normering dan privacyinbreuken, zoals risico's voor de integriteit en beheersbaarheid van de opsporing. Wel adviseert de commissie de wetgever aandacht te besteden aan inbreuken op andere grondrechten dan privacy, met name in gevallen waarin (grondrechtelijke) rechtspraak aangeeft dat inzet van een bevoegdheid zwaardere normering, zoals voorafgaande instemming van de rechter, vereist; daartoe kan worden vastgelegd dat in die gevallen het criterium van (ingrijpende) stelselmatigheid per analogie van toepassing is (zie Aanbeveling 9).

§4.3 Naast het voorgestelde algemene normeringscriterium heeft de commissie kort **overige algemene aspecten van normering** besproken, wat een breed scala van waarborgen en vormen van toezicht betreft. Het totale stelsel van waarborgen is complex en doet vragen rijzen rond rechterlijke toetsing vooraf van cumulatieve inzet van bevoegdheden, rechterlijke toetsing achteraf, mogelijkheden en beperkingen van beklag (zie daarover Aanbeveling 10), doelbinding en aanvullende vormen van (systeem)toezicht. Deze vragen verdienen beantwoording binnen het moderniseringstraject, met name ook met het oog op beantwoording van de vraag of aanvullende vormen van toezicht nodig zijn naast de van oudsher bestaande en recent ingevoerde vormen. De commissie benadrukt in dit verband het belang voor de langere termijn van een fundamentele reflectie op het stelsel van toezicht (zie Aanbeveling 11).

§4.4 Hoewel de commissie niet is toegekomen aan het ontwikkelen van een fundamentele visie op **wetgevingstechniek** in het licht van digitale ontwikkelingen, heeft zij hieraan wel een korte beschouwing gewijd, waarbij onder andere wordt gewezen op het belang van verankering van de beginselen van gegevensbescherming door *ontwerp* en door *standaardinstellingen*. Daarnaast geeft de commissie in overweging een permanente technisch-juridische adviescommissie in te stellen, die de wetgever proactief en tijdig adviseert in het licht van technisch-sociale ontwikkelingen op de middellange termijn; aldus kunnen nieuwe ontwikkelingen tijdig worden gesignaleerd en grondig worden besproken zodat de wetgever deze tijdig en adequaat kan verwerken (zie Aanbeveling 12).

8.3. Doorzoeking, beslag en gegevensvordering

§5.1 Ten aanzien van de bevoegdheden rond doorzoeking, beslag en gegevensvorderingen – zoals geregeld in Hoofdstuk 7 van Boek 2 – heeft de commissie eerst de gehanteerde **definities** besproken. De definitie van *gegevens* geeft geen interpretatieproblemen. Voor wat betreft *elektronische gegevensdragers* (art. 2.1.1.1) adviseert de commissie de omschrijving in de memorie van toelichting iets aan te passen (zie Aanbeveling 13), de term te vervangen door het iets generiekere "digitale-gegevensdrager" (zie Aanbeveling 14) en de clausule "uitsluitend bestemd" in de definitie aan te passen (zie Aanbeveling 15). De aangepaste definitie is ruim

genoeg om eventueel nieuwe opslagmedia (zoals synthetisch DNA) te omvatten, wat in de toelichting kan worden benoemd (zie Aanbeveling 16). Een digitale-gegevensdrager kan ook een apparaat zijn; het zal niet altijd duidelijk zijn of een apparaat een digitale-gegevensdrager of een geautomatiseerd werk is. Aangezien het normatief geen verschil maakt of gegevensonderzoek een geautomatiseerd werk dan wel een digitale-gegevensdrager betreft, stelt de commissie voor om bij alle bevoegdheden digitale-gegevensdragers en geautomatiseerde werken hetzelfde te behandelen (zie Aanbeveling 17).

De definitie van *geautomatiseerd werk* (artikel 2.1.1.1), zoals gewijzigd in het wetsvoorstel Computercriminaliteit III, is grotendeels toereikend, maar kent een zekere circulariteit omdat het verwijst naar "computergegevens"; dit kan beter worden vervangen door "digitale gegevens" (zie Aanbeveling 18). Het begrip geautomatiseerd werk is heel ruim en bevat apparaten variërend van simpele chips met bepaalde ingebouwde software, tal van "slimme" apparaten in het Internet der Dingen en pacemakers tot klassieke computers, servers en smartphones. Differentiatie binnen deze ruime groep apparaten lijkt wenselijk. Op basis van een analyse van diverse mogelijkheden, concludeert de commissie uiteindelijk dat een onderscheid op wetgevingsniveau onwenselijk is (omdat elk onderscheid lastige afbakeningsvragen oproept); waar relevant kan in de regeling van bevoegdheden tot onderzoek van digitale gegevens worden gedifferentieerd naar het type geautomatiseerd werk (zie uitgebreid par. 5.1.3 onder "Een ruime definitie – is differentiatie nodig?").

§5.2 Vervolgens zijn de bevoegdheden in Hoofdstuk 7 van Boek 2 besproken. Het conceptwetsvoorstel introduceert het begrip "inbeslagneming van" of **"beslag op" gegevens** voor het onder de beschikkingsmacht van de opsporing brengen van gegevens. De commissie deelt de kritiek uit de consultatiereacties en de literatuur op dit begrip (zie par. 5.2.2) en concludeert dat het begrip beslag verwarring wekt en geen voordelen heeft. De commissie adviseert dan ook het begrip "beslag op gegevens" los te laten en andere terminologie te hanteren (Aanbeveling 19).

§5.3 **Handelingen ten aanzien van gegevens** bestrijken een breed spectrum (zie voor een overzicht in par. 5.3.3). De (vanuit het oogpunt van normering gezien) belangrijkste stappen daarbij zijn het *overnemen* van gegevens en het *kennisnemen* van gegevens (het waarnemen van gegevens door een persoon, waarbij de gegevens zich tonen in voor menselijke interpretatie vatbare vorm). (Volgens de commissie is "overnemen" in dit kader een betere term voor het kopiëren van gegevens uit een externe bron dan de term "vastleggen", die overigens wel gebruikt kan blijven bij de heimelijke bevoegdheden tot het vastleggen – inclusief gelijktijdige ontsleuteling, zie Aanbeveling 49 – van communicatie.) Voor het geheel aan handelingen dat ten aanzien van gegevens wordt uitgevoerd, kan de term *onderzoek* worden gebruikt, wat zowel kennisnemen als overnemen en eventuele tussenstappen zoals voorbewerken of verrijken omvat. De commissie adviseert in de memorie van toelichting een duidelijke uitleg op te nemen van deze begrippen (Aanbeveling 20).

Voor stelselmatig onderzoek van gegevens in of overgenomen uit een geautomatiseerd werk of een digitale-gegevensdrager kan daarbij een overkoepelende bepaling worden geformuleerd, die tezamen met steunbevoegdheden kan worden geplaatst in een Titel "Bevoegdheden met betrekking tot onderzoek van gegevens in of overgenomen uit digitale-gegevensdragers en geautomatiseerde werken" (zie Aanbeveling 21). Bij elk van de (deels overlappende) stappen bij het onderzoek is het algemene normeringscriterium van (ingrijpende) stelselmatigheid van toepassing. Bijzondere aandacht vergt het maken van een image (het overnemen van alle gegevens uit een drager, nog zonder kennisneming); er zijn dragers die zo weinig privacygevoelige informatie bevatten, dat het maken van een image slechts een geringe inbreuk op de persoonlijke levenssfeer vormt, maar in het algemeen ziet de commissie het maken van een

image[239] als een meer dan geringe privacyinbreuk, vooral doordat gegevens in politiesystemen worden opgenomen; in dat geval is (in beginsel, behoudens eventuele wettelijk te regelen uitzonderingen) een bevel van de officier van justitie op zijn plaats.

Een knelpunt in de opsporing is of het toelaatbaar is van **nieuwe inhoudelijke gegevens** kennis te nemen die binnenkomen op of via een geautomatiseerd werk of digitale-gegevensdrager na inbeslagname of tijdens een netwerkzoeking – bijvoorbeeld wanneer een inbeslaggenomen maar nog niet onderzochte telefoon niet uitgezet mag worden omdat deze dan automatisch wordt vergrendeld en er vervolgens nog berichtjes binnenkomen. De commissie meent dat wat binnenkomt in de korte, natuurlijke, periode tussen inbeslagneming en het uitschakelen van de verbinding pure bijvangst is, waarvoor geen extra bevoegdheid of normering nodig is. Anders ligt het wanneer sprake is van een langere, substantiële, periode waarin voorzienbaar berichten binnenkomen of zelfs het onderzoek zich mede richt op die nieuw binnenkomende berichten. Afhankelijk van de mate waarin de opsporingsdienst actief bijdraagt aan het binnenhalen van dergelijke nieuwe berichten, wordt mogelijk inbreuk gemaakt op (het toekomstige) artikel 13 Gw en is een machtiging van de rechter-commissaris nodig. In zijn algemeenheid meent de commissie dat de wetgever het kennisnemen van later binnenkomende berichten mogelijk moet maken, mits dit afdoende wordt genormeerd. Daarbij moet worden aangesloten bij de normering van gegevensonderzoek aan het apparaat van de eindgebruiker of de daaraan gekoppelde netwerkzoeking (zie Aanbeveling 22).

Bij het gegevensonderzoek wordt de notificatieplicht van het huidige artikel 125m Sv overgenomen in artikel 2.7.3.1.3; de commissie stelt hierbij voor om de tekstuele wijziging ("aanduiding" in plaats van "aard") terug te draaien, omdat geen inhoudelijke wijziging is beoogd (Aanbeveling 23).

§5.4 Bevoegdheden ten aanzien van gegevens zijn zowel toepasbaar op digitale gegevens (gegevens opgeslagen op digitale-gegevensdragers) als op **analoge gegevens** (gegevens opgeslagen op analoge-gegevensdragers, zoals papier). De commissievoorstellen, bijvoorbeeld ten aanzien van het algemene normeringscriterium in relatie tot het onderzoek van gegevens, richten zich alleen op digitale gegevens; voor analoge gegevens kan de huidige (voorgestelde) regeling blijven bestaan ten aanzien inbeslagneming van voorwerpen (zoals papier) en het kopiëren van gegevens (bijvoorbeeld het fotograferen van de inhoud van een brief tijdens een doorzoeking). Analoge gegevens kunnen echter – en zullen ook veelal – worden gedigitaliseerd; daardoor worden ze (vanwege het gemak om digitale gegevens te delen of op afstand te benaderen) toegankelijk voor een bredere kring én wordt de doorzoekbaarheid wezenlijk anders. De commissie adviseert daarom een *schakelbepaling* op te nemen, die voor (aanvankelijk analoog opgeslagen) gedigitaliseerde gegevens de normering voor wat betreft het overnemen en het verdere onderzoek van digitale gegevens van overeenkomstige toepassing verklaart (zie Aanbeveling 24).

Ook wijst de commissie op de toenemende verwevenheid van het **menselijk lichaam** met digitale technologie. Op termijn zijn bevoegdheden betreffende onderzoek aan het lichaam en bevoegdheden met een digitale component daarom moeilijker uit elkaar te houden; de regelingen hebben echter een zelfstandig bestaansrecht omdat de beschermde belangen, lichamelijke integriteit respectievelijk informationele privacy, verschillen. Het onderzoek in of aan onlosmakelijk met het lichaam verbonden digitale-gegevensdragers of geautomatiseerde werken ziet de commissie primair als een onderzoek van digitale gegevens (dat dus wordt genormeerd via de bevoegdheden in Hoofdstuk 7). Omdat dergelijk onderzoek echter tegelijk ook de lichamelijke integriteit kan raken, stelt de commissie een tweede schakelbepaling voor, die de bepalingen van Titel 6.3 en 6.4 van Boek 2 van overeenkomstige toepassing verklaart, waarbij qua

[239] Als onderzoekshandeling. Het maken van een image als bevriezingsmaatregel (waarbij gegevens niet kunnen worden onderzocht tot ze, met de daarvoor relevante toestemming, worden ontdooid) vormt slechts een geringe inbreuk.

normering onderscheid wordt gemaakt tussen enerzijds onderhuids geïmplanteerde chips en anderzijds digitale-gegevensdragers of geautomatiseerde werken die met het lichaam of lichaamsfuncties zijn geïntegreerd, zoals pacemakers. Het vastleggen en kennisnemen van hersensignalen die niet puur lichaamsmechanische functies betreffen, acht de commissie echter uitgesloten onder de huidige en nu voorgestelde wetgeving. (Zie Aanbeveling 25)

§5.5 Naast de kernbepalingen rond het onderzoek van digitale gegevens en de bijbehorende schakelbepalingen, heeft de commissie ook enkele flankerende bevoegdheden geanalyseerd. Ten eerste betreft dat **bevriezingsmaatregelen**, die nodig kunnen zijn omdat digitale gegevens dynamisch zijn en snel gewijzigd of verwijderd kunnen worden. De formulering van de bevriezingsmaatregelen in de artikelen 2.7.1.1.5 en 2.7.2.2.4 lijkt ruim genoeg, maar de bevoegdheden zijn pas beschikbaar vanaf het moment van doorzoeking of binnentreden. Dat sluit *voorafgaande* bevriezingsmaatregelen uit, zoals het fysiek onderbreken van netwerkverbindingen of gebruik van stoorzenders. Daarbij ontbreken bevoegdheden ter bevriezing van gegevens op inbeslaggenomen gegevensdragers; de noodzaak voor dergelijke bevriezing neemt echter sterk toe, omdat ook gegevens op inbeslaggenomen gegevensdragers op allerlei manieren gewijzigd of ontoegankelijk gemaakt kunnen worden (zie par. 5.5.1). Volgens de commissie is daarom een meer algemene, techniek-onafhankelijke regeling wenselijk voor bevriezingsmaatregelen in het kader van doorzoekingen of inbeslagneming van gegevensdragers; de memorie van toelichting moet daarbij een (niet-limitatieve) opsomming van dergelijke maatregelen geven (zie Aanbeveling 26).

Een tweede flankerende bevoegdheid betreft mogelijkheden om **beveiliging ongedaan te maken**. Het huidige artikel 125k Sv wordt in het nieuwe artikel 2.7.4.1.4 uitgebreid tot een ontsleutelbevel voor geautomatiseerde werken én gegevensdragers; daarbij is een iets ruimere formulering wenselijk (ongedaan maken van *beveiliging*, niet van *versleuteling*, Aanbeveling 27). Een dergelijk bevel mag niet worden gegeven aan de verdachte vanwege het nemo teneturbeginsel. Dit beginsel staat er echter niet aan in de weg dat biometrische kenmerken, die immers onafhankelijk van de wil van de verdachte bestaan, ook onafhankelijk van diens wil – zo nodig onder slechts lichte dwang – kunnen worden verkregen (door een vinger op de sensor te leggen of een oog even open te houden). De commissie beveelt aan dat de officier van justitie kan bevelen toegang tot een biometrisch beveiligd geautomatiseerd werk of digitale-gegevensdrager te verschaffen, met een duldplicht voor zowel verdachten als niet-verdachten, waaronder ook niet-professioneel verschoningsgerechtigden. De beginselen van proportionaliteit en subsidiariteit en artikel 3 EVRM begrenzen daarbij de zo nodig uit te oefenen dwang. Ten aanzien van professioneel verschoningsgerechtigden acht de commissie afgedwongen toegangsverschaffing niet uitgesloten, maar dit kan alleen plaatsvinden in dezelfde gevallen en onder dezelfde voorwaarden als die gelden voor het kennisnemen van gegevens die onder het professioneel verschoningsrecht vallen (zie Aanbeveling 28).

Een andere manier om biometrische gegevens te verkrijgen ter ontsluiting van een geautomatiseerd werk of een digitale-gegevensdrager, is het heimelijk vergaren hiervan, zoals het heimelijk maken van een gelaatsfoto of het kopiëren van een achtergelaten vingerafdruk. Dit is vergelijkbaar met het heimelijk vergaren van vinger- of handpalmafdrukken voor vergelijkend onderzoek (art. 2.6.5.4.2 lid 3), en de commissie stelt daarom voor in dit verband een vergelijkbare regeling te treffen (Aanbeveling 29). Afname van biometrische kenmerken van overledenen kan volgens de commissie worden gebaseerd op de taakstellende artikelen; de inbreuk op de menselijke waardigheid is hierbij kleiner dan bij het in artikel 2.6.6.1 voorziene onderzoek aan overleden personen (zie Aanbeveling 30).

De derde besproken flankerende bevoegdheid is de **netwerkzoeking** – het in het kader van doorzoeking en beslag onderzoeken van elders opgeslagen gegevens. Dit wordt steeds belangrijker, omdat informatie in toenemende mate elders (met name in de cloud) ligt opgeslagen. (De inzetbaarheid van de bevoegdheid wordt daarbij sterk beperkt door jurisdictieproblemen, maar

dat valt buiten de opdracht van de commissie.) De voorgestelde regeling bevat ten opzichte van het huidige artikel 125j Sv een belangrijke en nuttige uitbreiding om een netwerkzoeking ook vanaf een inbeslaggenomen gegevensdrager of geautomatiseerd werk te kunnen uitvoeren. De formulering in artikel 2.7.4.1.2 en artikel 2.7.4.2.2 vergt wel aandacht, omdat het bestaande criterium van de "dubbele band" (die de zoeking beperkt tot reguliere en rechtmatige verbindingen) nog onvoldoende is vertaald naar situaties waarin de netwerkzoeking plaatsvindt elders dan op de plaats van een doorzoeking (zie Aanbeveling 31 en Aanbeveling 33). Ook is het nuttig om te expliciteren dat een (rechts)persoon bij wie een doorzoeking plaatsvindt, de opsporing de mogelijkheid kan bieden om van afstand de doorzoeking, en daarbij eventueel een netwerkzoeking, uit te voeren of voort te zetten, als zijnde vergelijkbaar met een doorzoeking bij de (rechts)persoon zelf (Aanbeveling 32). Evenzo kan worden toegelicht dat de netwerkzoeking niet in alle gevallen vanaf het onderzochte geautomatiseerde werk zelf hoeft te worden verricht (omdat dit soms risico's voor de forensisch verantwoorde veiligstelling van gegevens met zich brengt), maar ook met forensische onderzoeksapparatuur kan plaatsvinden, zolang niet méér toegang wordt verworven dan vanaf het oorspronkelijke apparaat het geval zou zijn (Aanbeveling 37).

De netwerkzoeking is van oudsher in tijd begrensd doordat deze tijdens een doorzoeking plaatsvindt. Nu de netwerkzoeking ook zal zijn toegestaan buiten doorzoekingen, is de vraag hoelang deze mag duren en hoeveel tijd mag verlopen tussen een doorzoeking of inbeslagneming en een netwerkzoeking. Een en ander hangt samen met het vraagstuk van later, na beslag, binnenkomende gegevens (par. 5.3.4). De commissie meent dat de netwerkzoeking zo lang mag duren als redelijkerwijs noodzakelijk is om alle benodigde gegevens binnen te krijgen. De commissie adviseert wel dat de netwerkzoeking in beginsel niet langer mag duren dan enkele dagen; zijn er omstandigheden die een langere duur noodzakelijk maken, dan moet dit worden gemotiveerd (Aanbeveling 34). Daarentegen is het volgens de commissie niet wenselijk om een vaste maximale termijn te stellen waarbinnen een netwerkzoeking moet beginnen na inbeslagname van een geautomatiseerd werk; het hangt van het geval af hoe snel een inbeslaggenomen drager redelijkerwijs kan worden onderzocht – als een groot aantal geautomatiseerde werken en digitale-gegevensdragers in beslag is genomen, kunnen deze die niet allemaal tegelijk en terstond worden onderzocht. Daarom kan ook moeilijk een maximale termijn worden gesteld waarbinnen onderzoek aan een in beslag genomen geautomatiseerd werk of digitale-gegevensdrager moet plaatsvinden. Het gaat in beide gevallen om een redelijke termijn, die begrensd wordt door de beginselen van proportionaliteit en subsidiariteit (zie Aanbeveling 35).

De wens van de opsporing om een netwerkzoeking opnieuw te kunnen uitvoeren op basis van later bekend geworden informatie, levert spanning op met de oorspronkelijke bedoeling van de netwerkzoeking: onderzoek van gegevens die zich ten tijde van een onderzoekshandeling elders bevinden en aldaar reeds zijn opgeslagen. Omdat gegevens die pas na een eerste netwerkzoeking beschikbaar komen volgens opsporingsinstanties wel cruciaal kunnen zijn, adviseert de commissie zo'n herhaalde netwerkzoeking mogelijk te maken, maar alleen op basis van een nieuw bevel daartoe. De officier van justitie of rechter-commissaris moet bij zijn beslissing de reikwijdte daarvan bepalen, waaronder de periode waarvoor het bevel geldig is (zie Aanbeveling 36).

De normering van de netwerkzoeking moet hetzelfde zijn als bij het onderzoek in of aan een geautomatiseerd werk of digitale-gegevensdrager zelf. Het voorgestelde algemene normeringscriterium is dus ook hier toepasbaar, met speciale aandacht voor situaties waarin berichten worden onderzocht die door het grondwettelijke telecommunicatiegeheim worden beschermd (Aanbeveling 38).

Omdat gegevens inmiddels steeds vaker elders liggen opgeslagen en de netwerkzoeking daarom een belangrijkere rol vervult dan voorheen, vraagt de praktijk van de opsporing dringend om de voorgestelde uitbreidingen van de netwerkzoeking na beslag en in situaties van

aanhouding en staandehouding. De commissie adviseert in dat licht deze aanpassingen – vooruitlopend op het moderniseringstraject – spoedig in te voeren (Aanbeveling 39).

De vierde flankerende bevoegdheid is **ontoegankelijkmaking** van gegevens, een voorlopige maatregel die vooral bedoeld is om de beschikbaarheid en verdere verspreiding van (vermoedelijk) strafbare gegevens te voorkomen. De manier waarop ontoegankelijkmaking en de eventuele ongedaanmaking daarvan in de toelichting worden omschreven, strookt echter niet altijd met wat in de praktijk realistisch is en zou in dat licht moeten worden aangepast. Daarbij kan ook worden verduidelijkt dat het voorgestelde ontoegankelijkmakingsbevel aan een aanbieder niet alleen inhoudt de gegevens ontoegankelijk te *maken*, maar ook deze ontoegankelijk te *houden*. (Zie Aanbeveling 40.) Bijzondere aandacht bij ontoegankelijkmaking – immers bedoeld als voorlopige maatregel – is nodig voor een eindoordeel over de strafbaarheid van de ontoegankelijk gemaakte gegevens, en het waar nodig teruggeven van "onschuldige" gegevens. De commissie vraagt aandacht voor situaties waarin geen eindbeslissing wordt genomen over de ontoegankelijk gemaakte gegevens (bijvoorbeeld als de hoofdzaak niet voor de rechter komt en als de officier een separate vordering tot definitieve vernietiging van de gegevens achterwege laat) en voor het expliciet en onderbouwd meewegen van belangen die derden kunnen hebben bij ontoegankelijk gemaakte gegevens (zie Aanbeveling 41).

§5.6 Naast onderzoek van gegevens in of overgenomen uit gegevensdragers in het kader van doorzoeking en inbeslagneming, is het vorderen van gegevens een belangrijke manier om opgeslagen gegevens te verkrijgen. De commissie heeft zich geconcentreerd op twee aspecten van de regeling van gegevensvordering.

Het eerste aspect is het **onderscheid tussen** vorderingen aan **aanbieders** van communicatiediensten en vorderingen aan **anderen**. Dit onderscheid is vooral van belang in verband met de bescherming van het grondwettelijke telecommunicatiegeheim. De definitie van communicatieaanbieders in het conceptwetsvoorstel en de toelichting daarop (aanbieders voor wie een communicatiedienst een hoofdactiviteit is) wijkt af van de reikwijdte van (het toekomstige) artikel 13 Gw (dat ook ziet op bedrijfsnetwerken en aanbieders voor wie de communicatiedienst een nevenactiviteit is). Hoewel de grondwetswijziging nog niet heeft plaatsgevonden, en bij behandeling van wetsvoorstel tot aanpassing van artikel 13 Gw nog nadere invulling aan de reikwijdte kan worden gegeven, acht de commissie het onwenselijk – en onnodig – om binnen Sv een regeling te treffen die uit de pas kan lopen met de reikwijdte van de bescherming van telecommunicatie onder (het toekomstige) artikel 13 Gw. De commissie adviseert daarom diverse bepalingen betreffende vorderingen aan aanbieders van een communicatiedienst te vervangen door een algemene bepaling die de normering van onderzoek van communicatie-inhoud koppelt aan het grondwettelijke telecommunicatiegeheim, zonder zelf vast te leggen tot waar dat telecommunicatiegeheim precies strekt (Aanbeveling 42). Sommige bepalingen moeten echter behouden blijven, waarbij de term "aanbieder van een communicatiedienst", vanwege de specifieke strafvorderlijke context, kan worden gehandhaafd (zie Aanbeveling 43). Bij de vordering aan aanbieders om gegevens ontoegankelijk te maken adviseert de commissie de wetgever te beoordelen of de voorgestelde reikwijdte ruim genoeg is om ook hostingaanbieders voor wie communicatie geen hoofdactiviteit is, te omvatten (Aanbeveling 44).

Het tweede aspect betreft de **normering** van gegevensvorderingen, zowel in het algemeen als in relatie tot verkeersgegevens in het bijzonder. De huidige en voorgestelde regeling van het vorderen van gegevens (in het conceptwetsvoorstel bevelen tot uitlevering van gegevens genoemd) maken een normatief onderscheid tussen identificerende gegevens, "gewone" gegevens en bijzondere categorieën (zogenoemde "gevoelige") gegevens. Volgens de commissie hangt de mate van inbreuk op de persoonlijke levenssfeer bij gevorderde gegevens echter niet alleen af van de *aard* van de gegevens, maar vooral ook van de hoeveelheid, de context en de wijze waarop de gegevens worden onderzocht en gebruikt. Bepaalde gegevensvorderingen kunnen een vérgaande inbreuk op de persoonlijke levenssfeer betekenen, maar dat is zeker niet bij elke

vordering van gevoelige gegevens het geval. De commissie stelt in dat licht voor om in plaats van de in artikel 2.7.3.3.3 gehanteerde driedeling de meer abstracte driedeling van het algemene normeringscriterium te hanteren. Dit verhoogt ook de onderlinge consistentie van de regeling van opsporingsbevoegdheden ten aanzien van digitale gegevens: qua verstrekkendheid kan het vorderen van gegevens immers vergelijkbaar zijn met het onderzoek van gegevens in of overgenomen uit een geautomatiseerd werk: de ingrijpendheid hangt vooral af van hoeveel en welke gegevens je uit welke bron vordert respectievelijk zoekt of vastlegt. Vanuit systematische overwegingen adviseert de commissie om bij vorderingen van gegevens waarbij sprake is van ingrijpende stelselmatigheid een machtiging van de rechter-commissaris te vereisen, in lijn met de voorgestelde invulling van het algemene normeringscriterium. De toelichting kan daarbij aangeven dat er slechts in uitzonderlijke gevallen sprake zal zijn van ingrijpende stelselmatigheid, grotendeels beperkt tot de "diepe" variant. Voor vorderingen van "gewone gegevens" die niet beperkt zijn tot identificerende gegevens, is een bevel van de officier van justitie op zijn plaats, mede in verband met het feit dat enige inspanning wordt gevraagd van een derde. (Zie Aanbeveling 45.)

De normering van het vorderen van **verkeersgegevens**, als bijzonder geval van de algemene gegevensvordering, vergt aandacht omdat in de literatuur en het maatschappelijk debat steeds vaker de vraag wordt gesteld of het nog wel zinvol is een normatief onderscheid te maken tussen de inhoud van communicatie en metadata. Het is daarbij echter belangrijk om voor ogen te houden dat metadata (alle gegevens betreffende elektronische communicatie, met uitzondering van de inhoud) een veel ruimer begrip is dan verkeersgegevens in enge zin (namelijk de specifiek in het Besluit vorderen gegevens telecommunicatie aangewezen gegevens). In het debat wordt niet altijd beseft dat het vorderen van verkeersgegevens als bedoeld in het Wetboek van Strafvordering beperkt is tot verkeersgegevens in enge zin, en dat een aantal in het debat vaak genoemde gegevens, zoals URL's, daar niet onder vallen. De commissie deelt het inzicht dat uit metadata een tamelijk scherp beeld van iemands persoonlijk leven kan ontstaan, maar acht dat bij de thans aangewezen categorieën verkeersgegevens niet het geval. De mogelijkheid bestaat echter dat in de toekomst meer typen metadata als "verkeersgegevens" worden aangewezen, en wellicht kunnen – als communicatiepatronen nog verder intensiveren – de huidige typen verkeersgegevens in de toekomst scherper zicht bieden op iemands privéleven. Omdat niet voorzienbaar is welke data in bijvoorbeeld 2030 als "verkeersgegevens" zijn aangewezen en in welke mate die zicht bieden op iemands privéleven, adviseert de commissie om in zijn algemeenheid het vorderen van metadata qua normering hetzelfde te behandelen als het vorderen van gegevens in het algemeen, en dus te verbinden aan het algemene normeringscriterium. Daarbij moet wel worden toegelicht dat de bij algemene maatregel van bestuur aangewezen verkeersgegevens niet onder ingrijpende stelselmatigheid vallen, met de kanttekening dat, als in de toekomst deze AMvB zou worden uitgebreid met andere typen metadata, de kwalificatie van ingrijpendheid moet worden herbeoordeeld. (Zie Aanbeveling 46.)

8.4. Heimelijke bevoegdheden

§6.1 In het kader van de bevoegdheden in Hoofdstuk 8 van het conceptwetsvoorstel merkt de commissie allereerst op dat door de titel "Heimelijke bevoegdheden" de onterechte indruk zou kunnen ontstaan dat alleen de bevoegdheden in dit hoofdstuk heimelijk kunnen worden uitgeoefend. Dat is niet het geval – soms ook kunnen bevoegdheden uit bijvoorbeeld Hoofdstuk 6 of Hoofdstuk 7 heimelijk worden toegepast. De toelichting zou dit moeten verduidelijken (Aanbeveling 47).

§6.2 Vervolgens is gekeken naar de **normering** van heimelijke bevoegdheden in het algemeen. In het conceptwetsvoorstel kent elke bevoegdheid zijn eigen normering, op basis van een inschatting hoe ingrijpend deze bevoegdheid in zijn algemeen is en wat in dat licht adequate

waarborgen zijn. Er is echter steeds minder logische samenhang tussen een bepaald deel van het privéleven en een bepaalde bevoegdheid die dat deel van het privéleven blootlegt; ook kan in het digitale tijdperk bij bevoegdheden de bandbreedte groter zijn van de mogelijke ernst van privacyinbreuken. Het is dan ook vooral contextafhankelijk of bij de uitoefening van een bevoegdheid op voorhand redelijkerwijs voorzienbaar is dat een geringe, een meer dan geringe of een zeer ingrijpende inbreuk op de privacy zal worden gemaakt. Daarom, alsmede vanuit systematische overwegingen, is het wenselijk de in dit rapport voorgestelde lijn van het algemene normeringscriterium door te trekken naar de heimelijke bevoegdheden.

Niet alle bevoegdheden worden naar hun aard primair in een digitale omgeving uitgeoefend, maar bij elke bevoegdheid kunnen – vanwege dataficering en de verwevenheid van de fysieke en de online wereld – digitale gegevens een rol (gaan) spelen. Voor een wetboek dat bedoeld is toekomstbestendig te zijn en qua systematiek een tijd na inwerkingtreding houdbaar moet zijn, moet men bovendien rekening houden met ontwikkelingen op lange termijn, waardoor op dit moment nauwelijks in te schatten is hoe ingrijpend een bevoegdheid in de toekomst kan uitpakken. Juist daarom is een algemeen normeringscriterium, dat contextspecifiek wordt ingevuld en waarvan de interpretatie dynamisch kan mee-evolueren met technisch-sociale ontwikkelingen, geschikt voor een systematische regeling van opsporingsbevoegdheden in een digitaal tijdperk. De commissie adviseert daarom het algemene normeringscriterium van toepassing te verklaren op alle heimelijke bevoegdheden in Titel 8.2. Daarbij is het wel van belang de behoefte aan toekomstbestendigheid niet overmatig te benadrukken ten koste van de behoefte aan duidelijkheid en toepasbaarheid (zie p. 136). Rechtszekerheid zal moeten worden gefaciliteerd door een uitgebreide memorie van toelichting en nadere uitwerking in lagere richtlijnen en procedures; ook zal er voldoende ruimte moeten worden geschapen om de praktijk voor te bereiden op de nieuwe systematiek. Daarbij zal de rechtszekerheid met name ook worden bevorderd door in de memorie van toelichting ten aanzien van veelvoorkomende vormen van uitoefening van bepaalde bevoegdheden uit te leggen of, en onder welke omstandigheden, er wel of niet sprake is van (ingrijpende) stelselmatigheid, waarbij bij bepaalde (vormen van uitoefening van) bevoegdheden kan worden aangegeven dat er, gelet op de huidige stand van de techniek, geen sprake is van ingrijpende stelselmatigheid. (Zie Aanbeveling 48.)

§6.3 Vervolgens zijn enkele bevoegdheden nader geanalyseerd, te beginnen met de **communicatie-gerelateerde bevoegdheden** (tappen en direct afluisteren). De commissie acht het opnemen van een heldere definitie van “communicatie” belangrijk, mede gelet op de opkomst van het Internet der Dingen en spraakgestuurde bediening van apparaten. Er is, naast klassieke communicatie tussen personen, steeds meer mens-machine- en machine-machine-communicatie, waardoor de afbakening van “communicatie”, zowel conceptueel als feitelijk, lastig te maken is indien een beperkte (persoonsgebonden) definitie wordt gebruikt. Na een analyse van diverse mogelijke definities, concludeert de commissie dat een brede definitie wenselijk is: communicatie is elke overdracht van gegevens tussen personen of apparaten. Hieronder valt ook gegevensoverdracht binnen geautomatiseerde werken en gegevensoverdracht van personen met zichzelf (Aanbeveling 50).

De voorgestelde definitie is ruimer dan de huidige en in het conceptwetsvoorstel voorgestane invulling van het begrip, en bestrijkt ook meer soorten (tele)communicatie dan de aan derden voor transport toevertrouwde communicatie die onder de reikwijdte van (het toekomstige) artikel 13 Gw valt. Dit heeft gevolgen voor de normering van het tappen en direct afluisteren.

In lijn met de in dit advies voorgestane algemene benadering van normering, stelt de commissie voor het vastleggen van telecommunicatie en het vastleggen van vertrouwelijke communicatie (Afdelingen 8.2.7 en 8.2.8) te verbinden aan het algemene normeringscriterium. Daarbij wordt (evenals bij het vorderen van gegevens, zie Aanbeveling 42 hierboven) een algemene bepaling opgenomen die voor het vastleggen van communicatie die beschermd wordt door artikel 13 Gw, een machtiging van de rechter-commissaris en dringendheid vereist. Voor wat

betreft niet onder artikel 13 Gw beschermde communicatie, moet worden gekeken naar de redelijkerwijs voorzienbare inbreuk die een tap of direct afluisteren oplevert. Het heimelijk vastleggen van niet-openbare communicatie die tussen mensen plaatsvindt via een derde en het vastleggen van vertrouwelijke directe communicatie tussen mensen moet in elk geval als ingrijpend stelselmatig worden aangemerkt. Voor het vastleggen van communicatie tussen personen en apparaten zou de toelichting relevante factoren en voorbeelden moeten benoemen die relevant zijn voor de beoordeling van (ingrijpende) stelselmatigheid (waarbij kan worden aangeknoopt bij de voorbeelden die de commissie geeft in par. 4.2.3 en 6.3.4). (Zie Aanbeveling 51.)

§6.4 De commissie heeft een uitgebreide beschouwing gewijd aan de voorgestelde nieuwe bevoegdheid tot het **stelselmatig overnemen van persoonsgegevens uit publiek toegankelijke bronnen**, vooral ook om te verhelderen hoe deze nieuwe bevoegdheid moet worden geïnterpreteerd. De commissie vindt "publiek toegankelijke bron" een betere term dan het in het conceptwetsvoorstel gehanteerde "open bron" (Aanbeveling 53) en beveelt aan in de memorie van toelichting de reikwijdte van dit begrip nader in te vullen door explicieter aan te knopen bij de strafbaarstelling van computervredebreuk (zie de analyse in par. 6.4.2, Aanbeveling 54). De bevoegdheid ziet niet op het inkopen van analoge gegevens (wel geldt de schakelbepaling als ingekochte gegevens worden gedigitaliseerd, zie Aanbeveling 24 hierboven), noch op het overnemen van persoonsgegevens uit de publieke ruimte (Aanbeveling 55). Een nadere toelichting over de afbakening met andere bevoegdheden, zoals stelselmatige observatie, is welkom (Aanbeveling 62). Naast verheldering, adviseert de commissie één onderdeel in artikel 2.8.2.4.1, eerste lid, aan te passen, omdat het overnemen van persoonsgegevens niet per se hoeft te gebeuren met een "technisch hulpmiddel" als bedoeld in het Besluit technische hulpmiddelen; wel zouden in verband met de integriteit en authenticiteit van de overgenomen resultaten bij algemene maatregel van bestuur eisen kunnen worden gesteld aan de wijze van overnemen (Aanbeveling 60).

Wat de normering van het overnemen van persoonsgegevens uit publiek toegankelijke bronnen betreft, stelt de commissie in lijn met de algemene benadering het algemene normeringscriterium voor (Aanbeveling 61). Het feit dat persoonsgegevens via een publiek toegankelijke bron beschikbaar zijn, is weliswaar relevant voor het vaststellen van de privacyinbreuk, maar geen doorslaggevende factor om te stellen dat het om een beperkte inbreuk gaat. Er zijn veel gegevens over personen beschikbaar die door anderen online zijn gezet, en niet altijd is er bij publieke toegankelijkheid sprake van een (bewuste of door de betrokkene bedoelde) openbaarmaking in een brede kring. Soms worden bijvoorbeeld beelden van gehackte webcamera's (waaronder mogelijk *nannycams* in de kinderslaapkamer) op een webpagina via een livestream uitgezonden zonder dat de betrokkene daarvan weet heeft. Om die reden kan het overnemen van persoonsgegevens uit publiek toegankelijke bronnen onder (zeer uitzonderlijke) omstandigheden zelfs een vérgaande privacyinbreuk betekenen en ingrijpende stelselmatigheid opleveren. Voor het bepalen van het omslagpunt tussen niet-stelselmatigheid en stelselmatigheid zou de memorie van toelichting explicieter handvatten moeten bieden door een uitgebreider en inzichtelijker overzicht te bieden van de factoren die van invloed zijn op "stelselmatigheid" (zie de aanzet daartoe in par. 6.4.3 onder "Hoe geef je invulling aan de (vooraf te vervullen) toets op de mate van inbreuk?", Aanbeveling 59). Daarbij is ook aandacht nodig voor de inzet van crawlers (zie Aanbeveling 58).

De commissie signaleert dat de voorgestelde strafvorderlijke bevoegdheid tot het stelselmatig overnemen van persoonsgegevens uit publiek toegankelijke bronnen slechts één onderdeel van het politiewerk betreft, terwijl dit type onderzoek evenzeer relevant is voor andere taken. De commissie adviseert de wetgever daarom een bredere regeling te treffen die ook andere politietaken omvat (zoals handhaving van de openbare orde), waarbij vergelijkbare voorwaarden als binnen de strafvorderlijke regeling voor de hand liggen. Vanwege het grote

belang van dit type onderzoek en de rechtsonzekerheid die momenteel bestaat bij gebreke van een wettelijke regeling, adviseert de commissie bovendien om deze regeling, evenals het voorliggende artikel uit het wetsvoorstel, snel tot stand te brengen, vooruitlopend op het moderniseringstraject (Aanbeveling 52).

§6.5 De andere in het conceptwetsvoorstel voorgestelde nieuwe heimelijke bevoegdheid betreft **stelselmatige locatiebepaling**, als steunbevoegdheid bij diverse andere bevoegdheden. De voorgestelde regeling is helder, maar evenals bij publiek toegankelijke bronnen kunnen de criteria die van invloed zijn op (het bereiken van) het omslagpunt van stelselmatigheid nader worden toegelicht; dat geldt ook voor de omgang met vastgelegde locatiegegevens wanneer de gezochte locatie afdoende is bepaald (Aanbeveling 63). Sommige elementen vragen ook om verduidelijking in de toelichting, zoals de passage over het bevestigen van een technisch hulpmiddel op het lichaam (Aanbeveling 64) en een verduidelijking dat stelselmatige locatiebepaling ook (via de band van een andere bevoegdheid) kan worden in gezet in combinatie met een vordering toekomstige verkeersgegevens (Aanbeveling 66).

Het gebruik van stelselmatige locatiebepaling om een te arresteren verdachte te lokaliseren zal meestal slechts een beperkte privacyinbreuk opleveren; het valt echter (in elk geval theoretisch) niet uit te sluiten dat daarbij soms de drempel van stelselmatigheid wordt bereikt. De commissie adviseert daarom de steunbevoegdheid van stelselmatige locatiebepaling ook mogelijk te maken ter aanhouding van een verdachte (Aanbeveling 65).

Voor de normering sluit de commissie aan bij het algemene normeringscriterium, waarbij voor deze bevoegdheid slechts in hoge (vooralsnog tamelijk theoretische) uitzonderingsgevallen sprake zou kunnen zijn van indringende stelselmatigheid (Aanbeveling 67).

§6.6 Bij de uitoefening van heimelijke bevoegdheden wordt uiteraard gebruik gemaakt van de nodige technologie. Voor sommige **technische hulpmiddelen** worden, via het Besluit technische hulpmiddelen strafvordering, bepaalde eisen gesteld in verband met de betrouwbaarheid van de met die middelen vastgelegde resultaten. Deze algemene maatregel van bestuur is van oudsher vooral gericht op fysieke hulpmiddelen zoals camera's; de regeling is minder houdbaar voor het gebruik van software. Een toekomstige regeling die eisen stelt aan de betrouwbaarheid van technische hulpmiddelen, zal rekening moeten houden met de specifieke eigenschappen van software. Er kan daarbij onderscheid worden gemaakt tussen technische hulpmiddelen die bewijs of informatie genereren en technische hulpmiddelen die reeds bestaande gegevens overnemen. De mate waarin de met hulpmiddelen van die laatste categorie verrichte handelingen herhaalbaar zijn, zou mede moeten bepalen welke regels voor die categorie hulpmiddelen zouden moeten worden gesteld. De commissie geeft daarnaast in overweging bij de herziening van de Wpg, gezien het toenemend belang van technische hulpmiddelen in de opsporingsketen, enige algemene regels te stellen voor het gebruik van hulpmiddelen voor gegevensverwerking, -analyse of -presentatie, zoals een algemene eis van toetsbaarheid van de verkregen resultaten (Aanbeveling 68). Verder vooruitkijkend valt ook te verwachten dat biologische en/of roboticagebaseerde hulpmiddelen op termijn meer concrete vormen aannemen; op dat moment zou de wetgever moeten bezien of nadere regulering van deze middelen noodzakelijk is, om een vergelijkbaar niveau van betrouwbaarheid te garanderen als bij klassieke technische hulpmiddelen het geval is (Aanbeveling 69).

8.5. Nieuwe bevoegdheden en onderwerpen

§7.1 Een onderdeel van de commissieopdracht betreft de vraag of het "pakket" van bevoegdheden in Boek 2 voldoende toekomstbestendig is met het oog op de technologische ontwikkelingen. Voor zover de commissie in staat is de ontwikkelingen in de periode tot circa 2030 te overzien, en met inachtneming van de fundamentele aandachtspunten die de commissieopdracht overstijgen, heeft zij over het algemeen geen substantiële lacunes in het pakket van bevoegdheden

geconstateerd. Ongetwijfeld zullen op onderdelen aanpassingen nodig zijn, maar die zullen naar verwachting grotendeels goed inpasbaar zijn in de systematiek van Boek 2.

Op één onderdeel signaleert de commissie echter wel een tekortkoming in het pakket van bevoegdheden: het gebrek aan de mogelijkheid om te **vorderen** van private partijen dat zij een **data-analyse** uitvoeren. De wet kent geen mogelijkheid om van een partij te vorderen gegevens te analyseren, vergelijken of combineren teneinde nieuwe gegevens te verkrijgen. Daar is echter steeds meer behoefte aan, gezien de sterk toegenomen hoeveelheid en complexiteit van databestanden bij derde partijen, waardoor het vorderen van gehele bestanden veelal een disproportionele privacyinbreuk zal opleveren. Vaak zou een analyse ook redelijkerwijs gevraagd kunnen worden van (in elk geval) grote partijen, die zelf ook veelal dergelijke analyses uitvoeren, bijvoorbeeld voor fraudebestrijding (zie par. 7.1.1 en 7.1.2). De commissie-Mevis heeft hierover in 2001 al een voorstel voor gedaan, dat de wetgever, onder verwijzing naar een alternatief, niet heeft overgenomen; voor dat alternatief is echter nadien geen regeling tot stand gekomen. De commissie acht het tegen deze achtergrond raadzaam een bevoegdheid in te voeren voor de officier van justitie om, met een zo nauwkeurig mogelijke aanduiding van de gevraagde bewerking, data-analyse door derden te vorderen. Daarbij is een machtiging van de rechter-commissaris nodig wanneer de gevraagde analyse een ingrijpend stelselmatig karakter draagt of wanneer de analyse een substantiële inbreuk op de normale bedrijfsvoering van de gevorderde oplevert. Het desbetreffende voorstel van de commissie-Mevis kan daarbij als uitgangspunt dienen, aangepast aan de systematiek van het gemoderniseerde wetboek en met inachtneming van de door de commissie voorgestelde normering en flankerende bepalingen (Aanbeveling 70).

§7.2 Een tweede punt betreft niet zozeer een lacune als wel een tot nog toe onderbelicht onderwerp: **geautomatiseerde gezichtsherkenning**. Dit is volgens de commissie een belangrijke ontwikkeling voor de komende decennia waar specifiek aandacht voor nodig is. Deels is dit onderwerp relevant voor het conceptwetsvoorstel: de memorie van toelichting moet aandacht besteden aan het gebruik bij observatie van geautomatiseerde gezichtsherkenning om personen te identificeren met wie de geobserveerde interacteert, waarbij dit gebruik als factor dient mee te wegen bij de beoordeling of er sprake is van (ingrijpende) stelselmatigheid (Aanbeveling 71). Daarnaast is het onderwerp in bredere zin relevant, omdat er in de komende decennia tal van toepassingen van geautomatiseerde gezichtsherkenning mogelijk zijn (zie par. 7.2.3 voor een overzicht), die verder kunnen gaan dan de relatief beperkte huidige toepassingen die mogelijk zijn op bestaande wettelijke grondslagen. De commissie constateert daarbij dat huidige regelgeving niet gemaakt is met als doel het reguleren van gezichtsherkenning. Toepassingen van gezichtsherkenning kunnen weliswaar worden getoetst aan bestaande regels, en onder omstandigheden ook binnen die regels rechtmatig worden uitgeoefend, maar voor gezichtsherkenning zijn geen gerichte wettelijke grondslagen opgesteld. Ook is er over toepassingen hiervan in de strafvordering nog weinig maatschappelijk of politiek debat gevoerd. De commissie adviseert het kabinet daarom te starten met visievorming en maatschappelijk en politiek debat te entameren over de inzet van geautomatiseerde gezichtsherkenning binnen de opsporing (Aanbeveling 72).

8.6. Ter afsluiting

Bovenstaande conclusies en aanbevelingen zouden de indruk kunnen wekken dat het conceptwetsvoorstel op veel punten te wensen overlaat. Die indruk is onterecht. De commissie heeft bij het begin van haar werk geconstateerd dat het conceptwetsvoorstel op veel punten goed in elkaar zit en veel nuttige onderdelen bevat om het wetboek bij de tijd te brengen in het licht van technische ontwikkelingen. De vele goede punten van het conceptwetsvoorstel worden echter niet benoemd in dit rapport – de opdracht van de commissie was immers om verbetervoorstellen

te doen, zodat de analyse en de voorstellen zich hebben gericht op onderdelen die minder geslaagd waren. Daarnaast is tijdens het werk van de commissie gebleken dat in de praktijk van digitale opsporing doorlopend nieuwe vragen rijzen, waarop in het onderhavige conceptwetsvoorstel, evenmin als in de huidige wet, niet altijd duidelijke antwoorden te vinden zijn. Regelmatig roepen onderdelen van bepalingen interpretatievragen op in het licht van nieuwe (versies van) uitvoeringsmethoden of andere technische ontwikkelingen; daarbij komen ook niet zelden lacunes in de wet naar voren. In deze zin is het werk van de commissie een voortzetting van het werk dat is gedaan in de aanloop naar het conceptwetsvoorstel: het betreft een grote onderhoudsbeurt, die om de zoveel tijd nodig is om de wetgeving rond opsporingsbevoegdheden bij de tijd te brengen, zodat deze weer even mee kan.

Het advies van de commissie is dan ook zeker geen eindpunt. Het is het begin van een vervolgtraject, waarin niet alleen de voorstellen – die zich veelal eerder op grote lijnen richten dan op concrete tekstvoorstellen – moeten worden geconcretiseerd en uitgewerkt, maar waarbij ook ongetwijfeld nieuwe vragen zullen rijzen en mogelijk weer nieuwe lacunes zullen worden gesignaleerd. Juist omdat de wetgeving die opsporingsbevoegdheden reguleert geen rustig bezit is, en dat ook niet kan zijn in het digitale tijdperk, heeft de commissie zich geconcentreerd op de grote lijnen, de belangrijkste gehanteerde concepten en de systematiek van de regeling van opsporingsbevoegdheden. Als de fundamenten en het casco stevig in elkaar zitten, is de kans aanzienlijk groter dat het gebouw langere tijd meekan, waarbij het benodigde klein en groot onderhoud ervoor kan zorgen dat het gebouw bij de tijd blijft.

De commissie denkt dat haar voorstellen betreffende de definities, concepten en systematiek, alsmede de voorgestelde algemene benadering voor de normering van opsporingsbevoegdheden, zicht bieden op een goede fundering en casco voor Boek 2 van het gemoderniseerde wetboek in een digitale context. Dit komt de toekomstbestendigheid van de voorgestelde regeling ten goede.

Niettemin heeft de commissie er in haar rapport ook op gewezen dat het vasthouden aan bepaalde bestaande kaders (zoals het in zelfstandige trajecten behandelen van Sv en Wpg, of het huidige toezichtskader) vragen oproept over de toekomstbestendigheid op (middel)lange termijn. In dat licht adviseert de commissie om niet alleen Hoofdstukken 7 en 8 van Boek 2 te moderniseren langs de lijnen van het conceptwetsvoorstel en de verbetervoorstellen daaromtrent uit dit rapport, maar ook om enig bodemonderzoek uit te voeren, om te verzekeren dat de aan te brengen fundamenten ook daadwerkelijk voldoende verankering bieden voor de regulering van opsporingsbevoegdheden in een digitale omgeving.

Bibliografie

Asscher, L.F. en A.H. Ekker (red.) (2003), *Verkeersgegevens. Een juridische en technische inventarisatie*, Amsterdam, Otto Cramwinckel Uitgever.

van den Bos, J. (2017), 'Strafrechtelijke beslissingen inzake in beslag genomen gegevensdragers', *Trema* 2017/10.

Bruce, I. (2017), 'Forced biometric authentication – on a recent amendment in the Norwegian Code of Criminal Procedure', *Digital Evidence and Electronic Signature Law Review*, jrg. 14, p. 26-30.

Church, G. M., Y. Gao & S. Kosuri (2012), 'Next-Generation Digital Information Storage in DNA', *Science* 16 augustus 2012, DOI: 10.1126/science.1226355.

Devroe, E. e.a. (2017), *Toezicht op strafvorderlijk overheidsoptreden*, Leiden: Universiteit van Leiden/NSCR/WODC, https://www.wodc.nl/onderzoeksdatabase/2686-toezicht-en-controle.aspx.

Felten, E.W. (2013), Written Testimony, United States Senate, Committee on the Judiciary Hearing on Continued Oversight of the Foreign Intelligence Surveillance Act, October 2, 2013, http://www.cs.princeton.edu/~felten/testimony-2013-10-02.pdf.

Fischer, J.C. (2010), *Communications Network Traffic Data. Technical and Legal Aspects*, diss. TU/e.

Floridi, L. (ed.) (2014), *The Onlife Manifesto: Being Human in a Hyperconnected Era*, Springer.

Fokkens, J.W. & N.N. Kirkels-Vrijman (2011), 'De procureur-generaal bij de Hoge Raad en het Openbaar Ministerie', in: A.G. Bosch e.a. (red.), *Twee eeuwen Openbaar Ministerie 1811-2011*, Den Haag: Sdu, p. 191- 212.

Franken, H.J. e.a. (2000), *Eindrapport Commissie Grondrechten in het Digitale Tijdperk*, Rotterdam: Phoenix & Den Oudsten.

Gelok, M.F. & W.M. de Jong (red.), *Volatilisering in de economie*, serie *Voorstudies en achtergronden* V98, Den Haag: Sdu.

Hakkarainen, A. e.a. (2015), 'High-Efficiency Device Localization in 5G Ultra-Dense Networks: Prospects and Enabling Technologies', Vehicular Technology Conference (VTC Fall), 2015 IEEE 82nd, doi: 10.1109/VTCFall.2015.7390965.

Hes, R. (2003), 'Verkeersgegevens in nieuwe generaties telecommunicatiesystemen', in: L.F. Asscher en A.H. Ekker (red.), *Verkeersgegevens. Een juridische en technische inventarisatie*, Amsterdam, Otto Cramwinckel Uitgever, p. 12-40.

Hotson, G. e.a. (2016), 'Individual finger control of a modular prosthetic limb using high-density electrocorticography in a human subject', *Journal of Neural Engineering*, vol. 13 nr. 2, doi: 10.1088/1741-2560/13/2/026017.

van den Hoven, J. e.a. (2016), *Licht op de digitale schaduw. Verantwoord innoveren met big data, Rapport van de expertgroep Big data en privacy aan de minister van Economische Zaken*, https://www.rijksoverheid.nl/documenten/rapporten/2016/10/04/licht-op-de-digitale-schaduw-verantwoord-innoveren-met-big-data.

IDC (2012), *The Digital Universe In 2020: Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East*, december 2012, https://www.emc.com/collateral/analyst-reports/idc-the-digital-universe-in-2020.pdf.

Knigge, G. & M. Peters (2017), *Beproefd verzet. Over de naleving van de wet door het openbaar ministerie bij de afhandeling van het verzet tegen een OM-strafbeschikking*, Den Haag.

Koops, B.J. (2000), *Verdachte en ontsleutelplicht: hoe ver reikt nemo tenetur?*, Deventer: Kluwer 2000.

Koops, B.J. & M. Prinsen (2005), 'Glazen woning, transparant lichaam. Een toekomstblik op huisrecht en lichamelijke integriteit', *Nederlands Juristenblad* 80 (12), p. 624-630.

Koops, B.J. (2006a), 'Should ICT Regulation Be Technology-Neutral?', in: Koops et al. (eds.), *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners*, The Hague: T.M.C. Asser Press 2006, p. 77-108.

Koops, B.J. (2006b), *Tendensen in opsporing en technologie. Over twee honden en een kalf*, oratie Tilburg, Nijmegen: Wolf Legal Publishers, 55 p.

Koops, B.J. & Th. de Roos (2007), 'Materieel strafrecht en ICT', in: B.J. Koops (red.), *Strafrecht en ICT*, 2e druk, Den Haag: Sdu 2007, p. 23-75.

Koops, B.J. (2011), 'Forgetting Footprints, Shunning Shadows. A Critical Analysis of the "Right to Be Forgotten" in Big Data Practice', 8 *SCRIPTed* (3), p. 229-256.
Koops, B.J. (2012), *Het decryptiebevel en het nemo-teneturbeginsel. Nopen ontwikkelingen sinds 2000 tot invoering van een ontsleutelplicht voor verdachten?*, Meppel/Den Haag: Boom Lemma / WODC.
Koops, B.J. (2014), 'On legal boundaries, technologies, and collapsing dimensions of privacy', 3 *Politica e Società* (2), p. 247-264.
Koops, B.J. & M.E.A. Goodwin (2014), *Cyberspace, the cloud, and cross-border criminal investigation. The limits and possibilities of international law*, The Hague/Tilburg: WODC/TILT, https://ssrn.com/abstract=2698263.
Koops, B.J. & J.M. Smits, m.m.v. F. van der Kroon (2014), *Verkeersgegevens en artikel 13 Grondwet. Een technische en juridische analyse van het onderscheid tussen verkeersgegevens en inhoud van communicatie*, Oisterwijk: Wolf Legal Publishers, http://alexandria.tue.nl/repository/books/772741.pdf.
Koops, B. J. (2016), 'Megatrends and Grand Challenges of Cybercrime and Cyber-Terrorism Policy and Research', in: B. Akhgar & B. Brewster (red.), *Combatting Cybercrime and Cyberterrorism. Challenges, Trends and Priorities*, Springer 2016, p. 3-15.
Koops, B.J., C. Conings & F. Verbruggen (2016), *Zoeken in computers naar Nederlands en Belgisch recht. Welke plaats hebben 'digitale plaatsen' in de systematiek van opsporingsbevoegdheden?*, Preadvies Nederlands-Vlaamse Vereniging voor Strafrecht 2016, Oisterwijk: Wolf Legal Publishers.
Koops, B.J. (2017), 'Digitaal huisrecht', *92 Nederlands Juristenblad* (3), p. 183-187.
Koops, B.J., B.C. Newell & I. Škorvánek (2019), 'Location tracking by police: New Frameworks for Preserving Geolocational Privacy', *UC Irvine Law Review* (te verschijnen), https://ssrn.com/abstract=3142165.
Kosinski, M., D. Stillwell & Thore Graepel (2013), 'Private traits and attributes are predictable from digital records of human behavior', *Proceedings of the National Academy of Sciences* 110 (15), p. 5802-5805. https://doi.org/10.1073/pnas.1218772110.
Lindemann, M. & D.A.G. van Toor (2018), 'Protection of a suspect's privacy in criminal procedures', *Ars Aequi* 2018/05, p. 376-384.
Nissenbaum, H. (2010), *Privacy in Context. Technology, Policy, and the Integrity of Social Life*, Stanford, CA: Stanford UP.
Odinot, G., D. de Jong, J.B.J. van der Leij, C.J. de Poot, E.K. van Straalen (2012), *Het gebruik van de telefoon- en internettap in de opsporing*, Den Haag/Meppel: WODC / Boom Lemma, https://www.wodc.nl/onderzoeksdatabase/effectiviteit-van-tappen.aspx.
Royer, S. & J.J. Oerlemans (2017), 'Naar een nieuwe regeling voor beslag op gegevensdragers', *Computerrecht* 2017/5.
Schermer, B.W. (2017), 'Het gebruik van Big Data voor opsporingsdoeleinden: tussen Strafvordering en Wet politiegegevens', *Tijdschrift voor Bijzonder Strafrecht en handhaving* 2017(4).
Service, Robert F. (2017), 'DNA could store all of the world's data in one room', Science 2 maart 2017, doi:10.1126/science.aal0852, http://www.sciencemag.org/news/2017/03/dna-could-store-all-worlds-data-one-room.
Seshu, C. (2008), 'Quantum key distribution', in: Global E-Security 4th International Conference, ICGeS 2008, London, UK, June 23-25, 2008, Proceedings, p. 207.
Stamhuis, E.F. (2017), 'Een ongeschikt concept', *Strafblad* (50), p. 360-366.
Vellinga-Schootstra, F. (2017), 'Inbeslagneming van voorwerpen en gegevens', *Rechtsgeleerd Magazijn Themis* (6), p. 334-343.
de Vries, I. (2017), 'Big Data', in: M. den Hengst, T. ten Brink en J. ter Mors (red.), *Informatiegestuurd politiewerk in de praktijk*, Deventer: Vakmedia.
Wetenschappelijk Raad voor het Regeringsbeleid (WRR) (2016), *Big Data in een vrije en veilige samenleving*, Amsterdam University Press.
Wiemans, F.P.E. (2004), *Onderzoek van gegevens in geautomatiseerde werken* (diss. Tilburg), Nijmegen: Wolf Legal Publishers 2004.
Wisman, T. (2015), 'Privacy: Alive and Kicking. Case Note *Digital Rights Ireland: Joined Cases C-293/12 and C-594/12, 8 April 2014*', *European Data Protection Law* (1), p. 80-84.
Zuiderveen Borgesius, F.J. & D.A. Korteweg (2009), 'E-mail na de dood: juridische bescherming van privacybelangen', *Privacy & Informatie* (5), p. 212-224.

Bijlage I. Samenstelling van de commissie

De Commissie modernisering opsporingsonderzoek in het digitale tijdperk is ingesteld bij besluit van de toenmalige Minister van Veiligheid en Justitie voor de periode 1 juni 2017 tot 1 januari 2018.[240] Bij besluit van de Minister van Justitie en Veiligheid en de Minister voor Rechtsbescherming van 18 december 2017 is de periode verlengd tot 1 mei 2018.[241]

1. Dhr. Prof. dr. E.J. Koops (voorzitter), Tilburg University
2. Dhr. Mr. R.J. Verbeek (secretaris), Directie Wetgeving en Juridische Zaken, Ministerie van Justitie en Veiligheid
3. Dhr. R. Greidanus, LL.M. (adjunct-secretaris), Tilburg University (tot eind december 2017)
4. Dhr. N. van Buiten, LL.M. (adjunct-secretaris), Tilburg University (vanaf januari 2018)
5. Dhr. Mr. dr. B.W. Schermer, Universiteit Leiden
6. Mevr. Mr. M.J. Grapperhaus, Gerechtshof 's-Hertogenbosch
7. Dhr. Mr. A. Kuijer, Gerechtshof Den Haag en Kenniscentrum Cybercrime
8. Mevr. Mr. D. van der Ven-Laheij, Openbaar Ministerie
9. Mevr. Mr. A.M. van Hoorn, Openbaar Ministerie
10. Dhr. Mr. T. Dieben, Nederlandse orde van advocaten
11. Mevr. Mr. E. van den Bosch, Nederlandse orde van advocaten
12. Dhr. Mr. P.C. Verloop, Nederlandse orde van advocaten
13. Dhr. Mr. M. Goos, Politie
14. Mevr. Mr. M. Viersma, Politie
15. Dhr. Mr. M. Zoetekouw, Politie
16. Dhr. Mr. E. Franken, Platform Bijzondere opsporingsdiensten
17. Dhr. Drs. M. van Barneveld, Platform Bijzondere opsporingsdiensten (tot eind december 2017)
18. Dhr. Mr. J. Koelewijn, Platform Bijzondere opsporingsdiensten (vanaf januari 2018)
19. Dhr. Mr. E.E. Gillissen, Directie Rechtshandhaving en criminaliteitsbestrijding, Ministerie van Justitie en Veiligheid
20. Dhr. Mr. F.J.E. Krips, Directie Wetgeving en Juridische Zaken, Ministerie van Justitie en Veiligheid

[240] *Staatscourant* 12 juli 2017, nr. 39081.
[241] *Staatscourant* 28 december 2017, nr. 73969.

Bijlage II. Uitgangspunten voor de uitvoering van de opdracht

Uitgangspunten voor de inhoud van de opdracht (het wetboek – inhoudelijk):

1. De regeling van opsporing in het wetboek moet zo simpel zijn als mogelijk, en zo complex als nodig.
2. De regeling van opsporing moet zo technologie-onafhankelijk zijn als mogelijk (in verband met duurzaamheid), en zo technologie-specifiek als nodig (in verband met rechtszekerheid).
3. De regeling van opsporing moet in hoge mate technologie-onafhankelijk zijn qua leidende concepten en systematiek, maar mag technologie-specifiek zijn in de regeling van bepaalde concrete bevoegdheden.
4. Bij het streven naar toekomstbestendigheid en voldoende mate van technologie-onafhankelijkheid van het wetboek hanteert de commissie een horizon van tien tot vijftien jaar vanaf nu. Verder kijkt de commissie in meer algemene zin naar momenteel voorzienbare technische ontwikkelingen die de komende 25 jaar op ons af kunnen komen, om te signaleren of deze ingrijpende consequenties zouden kunnen hebben voor de systematiek.
5. Opsporingsbevoegdheden moeten met vergelijkbare waarborgen worden omgeven naar de mate van gelijkheid, en met verschillende waarborgen naar de mate van ongelijkheid.
6. Naarmate de privacyinbreuk van een bevoegdheid groter is, moeten er meer waarborgen zijn. Bij het vaststellen van de mate van inbreuk, is het onderscheid in typen privacy naar persoonsgegevens, lichaam, huis en communicatie niet van overwegende betekenis, hoewel het wel een rol kan spelen.

Uitgangspunten voor de inhoud van de opdracht (het wetboek – procedureel):

7. De commissie streeft in haar advies, binnen de kaders van haar opdracht, naar een zo omvattend mogelijke regeling voor Boek 2 in het kader van Modernisering Strafvordering. Onderdelen die urgent om wetsaanpassing vragen, hoeven echter niet te wachten op het daarmee samenhangende wetgevingstraject.
8. Niet alles hoeft in het wetboek zelf te worden geregeld (denk aan lagere regelgeving, richtlijnen, andere wetten, andere vormen van regulering), maar substantiële inbreuken op grondrechten bij de opsporing van strafbare feiten wel, in verband met het vereiste van voorzienbaarheid bij wet.

Uitgangspunten voor het proces (de commissie):

9. De kwaliteit van het advies staat voorop en mag niet (overmatig) lijden onder tijdsdruk.
10. Het advies richt zich in elk geval op de systematiek van de regeling in de Hoofdstukken 7 en 8 van Boek 2 (structuur, concepten, manier van regelen) en op de invulling van details die sterk samenhangen met deze systematiek. Overige details zullen worden meegenomen voor zover dit mogelijk is binnen de tijd die de commissie tot haar beschikking heeft.
11. De commissie streeft naar consensus (en dus naar compromissen). Compromissen mogen evenwel niet leiden tot vage voorstellen.
12. De commissie streeft zoveel mogelijk naar concrete voorstellen, maar hoeft niet alle problemen op te lossen. Waar, na voldoende discussie, geen zicht blijkt op een oplossing(srichting) waar de commissie achter kan staan, wordt dit als probleempunt in het advies gesignaleerd.