Platform Modernisering Strafvordering

Beschouwing rapport Commissie-Koops: strafvordering in het digitale tijdperk

Mr. dr. J.J. Oerlemans

1 Inleiding

De iPhone Xs uit september 2018 heeft een processorsnelheid van meer dan 2431 keer[1] de processorsnelheid van de '*Apollo Guidance Computer*' in de Apollo 11 uit 1969. De iPhone Xs bevat bovendien zestien miljoen keer[2] meer opslagruimte dan de Apollocomputer die heeft geholpen de eerste mensen op de maan te zetten. Dit illustreert hoe de rekenkracht en opslagcapaciteit van computers in de laatste decennia explosief zijn toegenomen. Tegenwoordig spelen smartphones ook een belangrijke rol voor het bewijs in strafzaken.[3] Dat komt doordat allerlei gegevens op één apparaat beschikbaar zijn, zoals contactpersonen, foto's en video's. Ook de zoekgeschiedenis op apparaten (zowel op de telefoon zelf als zoekslagen in een web browser) en berichten in *Whatsapp* geven veel prijs over bijvoorbeeld de motieven en activiteiten van een gebruiker van een apparaat en kunnen bijdragen aan bewijs in strafzaken.[4]
Smartphones genereren deze gegevens door handelingen van de gebruiker zelf, maar ook door constant verbinding te maken met de telecomprovider en aanbieders van diverse app-diensten en contact te leggen met wifi- en Bluetooth-verbindingen in de buurt. Niet al het digitale bewijs wordt daarbij verkregen door middel van beslag op gegevensdragers. Ook commerciële aanbieders van 'sensoren' die verbinding met apparaten in de buurt maken en op basis van deze gegevens diensten aanbieden, kunnen bewijs aanleveren in strafzaken.[5] Digitaal bewijs zal een steeds prominentere rol in strafzaken spelen, onder andere om te bepalen waar en wanneer een verdachte zich bevond, zowel in de fysieke als de digitale wereld.[6]
Daarnaast maken socialemediadiensten een stormachtige ontwikkeling door, die van invloed is op het opsporingsproces. In februari 2004 startte Mark Zuckerberg de socialenetwerkdienst 'Thefacebook' met zo'n 1200 gebruikers. Halverwege 2018 waren er 2.2 miljard actieve Facebookgebruikers.[7] Informatie op sociale media biedt een schat aan informatie voor de opsporing. Deze gegevens kunnen bijvoorbeeld bijdragen aan de identificatie van verdachten, de contacten van verdachten in kaart brengen, bijdragen aan de lokalisering van betrokkenen in het opsporingsonderzoek en de publieke communicatie van personen blootleggen.
De uit opsporing verkregen informatie kan bovendien worden opgeslagen en verder worden verwerkt voor opsporingsdoeleinden. Met behulp van data-analysetechnieken zoals '*machine learning*'[8] en '*Big Data*'[9]-analyse kan informatie uit de opgeslagen gegevens

worden verkregen die nieuwe inzichten en sporen voor opsporingsonderzoeken oplevert. Mede door de ontwikkeling van '*cloud computing*'[10] kunnen gegevens – vergeleken met twintig jaar geleden – bovendien voor veel minder geld dan voorheen worden opgeslagen en met veel meer computerkracht dan voorheen worden verwerkt.
Kortom, de technologie dendert voort. Deze ontwikkelingen bieden kansen voor de opsporing, waardoor nieuwe regelingen noodzakelijk kunnen zijn om deze kansen – voor zover wenselijk – te benutten. Tegelijkertijd noodzaakt het tot het opnemen van de nodige waarborgen in het Wetboek van Strafvordering ter bescherming van de betrokkenen in een opsporingsproces. De Commissie modernisering opsporingsonderzoek in het digitale tijdperk (hierna: Commissie-Koops[11]) heeft de opdracht gekregen te onderzoeken 'of de wettelijke regeling van het opsporingsonderzoek, zoals neergelegd in het conceptwetsvoorstel Boek 2, voldoet, of bijstelling dan wel aanvulling behoeft, mede in het licht van de toenemende digitalisering van de criminaliteit en de uitdagingen waaraan de opsporing de komende decennia het hoofd moet bieden'. De Commissie heeft deze opdracht met verve vervuld en kwam tot 72 adviezen om het Wetboek van Strafvordering beter bij de tijd te brengen.
In dit artikel worden niet alle 72 adviezen besproken. Het rapport is te omvangrijk voor een kritische bespreking van alle aanbevelingen in één artikel. Het rapport zelf bevat een heldere samenvatting van de aanbevelingen.[12] Dit artikel richt zich op een bespreking van de nieuw voorgestelde rol van het begrip 'stelselmatigheid' in paragraaf 2 en de aanbevelingen van de Commissie die zich richten op de belangrijkste nieuwe bepalingen in het conceptwetsvoorstel tot wijziging van Boek 2 van het Wetboek van Strafvordering. Paragraaf 3 gaat over het 'stelselmatig vergaren van persoonsgegevens uit open bronnen' en paragraaf 4 over het 'beslag op digitale gegevensdragers'. Paragraaf 5 gaat in op het onderwerp van de 'dataficering van het opsporingsproces'. In paragraaf 6 volgt een slotbeschouwing, waarbij ik inga op de vraag welke bijdrage het rapport heeft geleverd aan de modernisering van het Wetboek van Strafvordering.

2 Nieuwe rol en invulling van het begrip 'stelselmatigheid'

'Stelselmatigheid' is een sleutelbegrip in het rapport van de Commissie-Koops. Het wordt in het rapport geïntroduceerd als een algemeen normeringscriterium voor opsporingsbevoegdheden. In het huidige Wetboek van Strafvordering speelt het begrip stelselmatigheid met name een rol bij de bijzondere opsporingsbevoegdheden van stelselmatige observatie en stelselmatige informatie-inwinning. Als een 'min of meer volledig beeld van bepaalde aspecten van iemands privéleven kan ontstaan', is de toepassing van de opsporingsmethode stelselmatig en moet op bevel van een officier van justitie de betreffende bijzondere opsporingsbevoegdheid worden ingezet. Om te bepalen of daarvan sprake is, geeft de memorie van toelichting op de Wet bijzondere opsporingsbevoegdheden de volgende factoren mee: (1) duur, (2) plaats, (3) frequentie, (4) intensiteit en (5) het gebruik van een technisch hulpmiddel.[13]
De Commissie-Koops voorziet in navolging van de wetgever en de Hoge Raad in een grotere rol voor het criterium door het ook van toepassing te verklaren op andere (deels nieuwe) bevoegdheden, zoals het stelselmatig vergaren van persoonsgegevens uit open

bron, de inbeslagname van gegevensdragers en het vorderen van gegevens. In deze paragraaf wordt eerst het begrip stelselmatigheid als normeringscriterium besproken en daarna het nieuwe criterium van 'ingrijpend stelselmatig'. Daarna volgt een analyse van de voorgestelde driedeling in opsporingsbevoegdheden die daaruit voortvloeit.

2.1 'Stelselmatigheid' als normeringscriterium

De Commissie-Koops verduidelijkt eerst dat van stelselmatigheid sprake is als '*op voorhand redelijkerwijs voorzienbaar* is dat een min of meer volledig beeld van bepaalde aspecten van iemands privéleven kan ontstaan'.[14] De woorden 'op voorhand' uit de definitie doen tot uiting komen dat het gaat om een inschatting. Deze inschatting van de zwaarte van de privacy-inmenging die een opsporingsbevoegdheid met zich brengt moet vooraf worden gemaakt, voor zover deze 'redelijkerwijs voorzienbaar' is 'aan de hand van algemene en contextspecifieke ervaringsregels en van een redelijke inschatting van de omstandigheden van het geval'.[15] Als achteraf blijkt dat de inbreuk op de persoonlijke levenssfeer groter blijkt te zijn, dan maakt dat de privacy-inbreuk niet met terugwerkende kracht stelselmatig.

Bij 'stelselmatigheid' moet de officier van justitie het bevel afgeven voor de inzet van de bijzondere bevoegdheid. Tot op heden is dat het geval bij stelselmatige observatie en stelselmatige informatie-inwinning. Dankzij het arrest van de Hoge Raad over de inbeslagname van smartphones heeft het criterium nu ook in die context een rol gekregen door bij stelselmatigheid het bevel van een officier van justitie te vereisen.[16]

De Commissie-Koops voorziet een nog prominentere rol voor het begrip 'stelselmatigheid' voor de normering van opsporingsmethoden. Het kan volgens de Commissie namelijk voorzien in het omslagpunt tussen 'een geringe inbreuk' op de persoonlijke levenssfeer van betrokkenen in een opsporingsonderzoek en een 'meer dan geringe inbreuk'. Zoals tot op heden ook al het geval is, is voor de toepassing van opsporingsmethoden die een beperkte inbreuk op de persoonlijke levenssfeer van betrokkenen met zich meebrengen niet de toepassing van een bijzondere opsporingsbevoegdheid vereist.[17] Daarvoor volstaat de basis van de algemene opsporingstaak van de politie (art. 3 Polw. 2012 jo. 141-142 Sv).

De Commissie-Koops stelt voor deze algemene normerende werking van het begrip stelselmatigheid in het Wetboek van Strafvordering te expliciteren. Ze tekent daarbij wel aan dat de vijf factoren uit 1996 niet altijd goed werken in een digitale context. Immers, in een kort tijdsbestek van bijvoorbeeld tien minuten kunnen in het digitale tijdperk veel meer persoonsgegevens worden vergaard die een vergaand inzicht geven in het privéleven van een betrokkene, bijvoorbeeld door alle persoonsgegevens die beschikbaar zijn over een persoon op internet vast te leggen en nader te analyseren. De factor 'duur' is daardoor niet goed toepasbaar in de digitale context. De Commissie formuleert daarom een veelvoud van factoren die gebruikt kunnen worden bij het bepalen of al dan niet sprake is van stelselmatigheid bij het onderzoek aan gegevens op een inbeslaggenomen smartphone, bij het vastleggen van persoonsgegevens uit publiekelijk toegankelijke bronnen, het vorderen van gegevens en het vastleggen van inhoudelijke gegevens uit telecommunicatie.[18]

Hieruit blijkt meteen de zwakte van het begrip 'stelselmatigheid' als normeringscriterium;

het is een abstract begrip en krijgt een andere toepassing afhankelijk van de omstandigheden van het geval. Voor betrokkenen in het opsporingsproces en opsporingsambtenaren blijft het daardoor onduidelijk hoe ver opsporingsautoriteiten precies in hun opsporingshandelingen mogen gaan en welke autoriteit (de opsporingsambtenaar, de officier van justitie of de rechter-commissaris) toestemming moet geven voor de inzet van de bevoegdheid.
Uit het rapport blijkt wel dat een deel van de Commissie-Koops aarzelingen heeft bij het van toepassing verklaren van het algemene normeringsprincipe van stelselmatigheid op alle heimelijke bevoegdheden. Het voordeel van een meer toekomstbestendige abstracte wetgeving moet volgens deze leden worden afgewogen tegen de behoefte aan duidelijkheid en toepasbaarheid van zowel de opsporingsinstanties als van degenen die onderwerp van opsporingsonderzoek kunnen zijn. In de visie van deze commissieleden ligt te veel nadruk op het realiseren van een flexibele en toekomstbestendige regeling, waardoor het stelsel in deze vorm tot onwenselijke (rechts)onzekerheid kan leiden.[19] Uiteindelijk heeft de Commissie-Koops er niettemin voor gekozen het criterium van stelselmatigheid deze hoofdrol te geven. Daarbij wordt nog opgemerkt dat rechtszekerheid ook kan worden gefaciliteerd door een uitgebreide memorie van toelichting en nadere uitwerking in lagere richtlijnen en procedures.[20]

2.2 Ingrijpend stelselmatig

De Commissie-Koops introduceert nog een extra dimensie aan het begrip stelselmatig met het nieuwe begrip ‘ingrijpend stelselmatig’. Ingrijpend stelselmatig betekent dat bij de uitoefening van een bevoegdheid op voorhand redelijkerwijs voorzienbaar is dat een ingrijpend beeld van iemands privéleven kan ontstaan.[21] In dat geval is een machtiging van de rechter-commissaris aangewezen bovenop een bevel van de officier van justitie.
De Commissie hanteert de volgende toets voor de invulling van het criterium van ingrijpende stelselmatigheid. Ten eerste is van ingrijpende stelselmatigheid sprake als een min of meer volledig beeld ontstaat van een *wezenlijk deel van iemands privéleven*. De ingrijpendheid bestaat in dat geval uit een diepe (verticale) kijk in iemands privéleven, waarbij een wezenlijk deel naar voren komt. Ten tweede is van ingrijpende stelselmatigheid sprake als een min of meer volledig beeld tot stand komt van *een aanzienlijk deel van iemands privéleven*. De ingrijpendheid bestaat hier uit een brede (horizontale) 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 ook sprake van ingrijpende stelselmatigheid, zo voorziet de Commissie.[22]
Interessant is daarbij de koppeling met de nieuwe notie van de ‘mozaïektheorie van privacy’. De theorie, ontwikkeld in Amerikaanse jurisprudentie, heeft betrekking op de situatie waarbij informatie uit verschillende contexten van iemands leven bij elkaar wordt

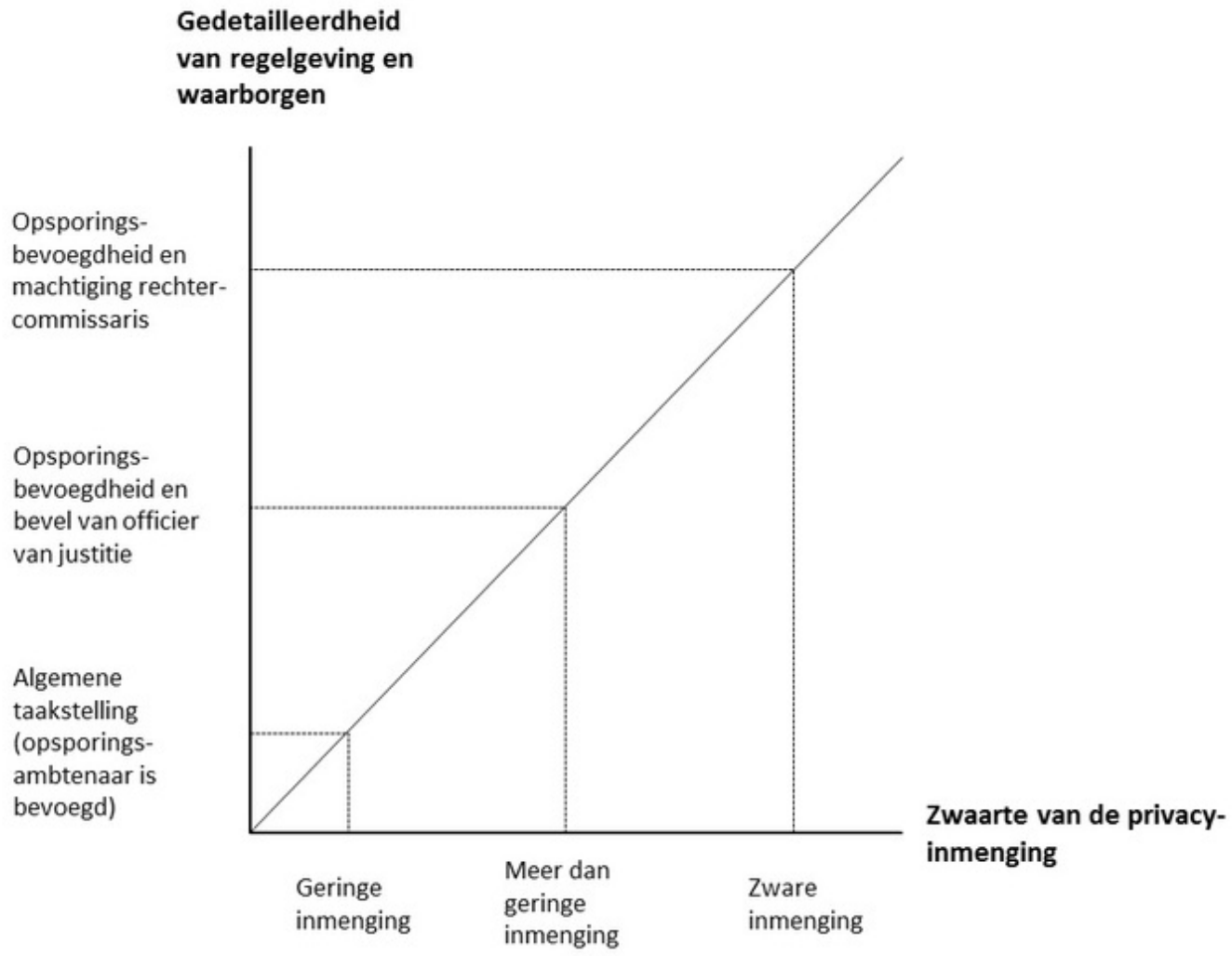
gelegd.[23] Daarbij kan sprake zijn van ingrijpende stelselmatigheid, zonder dat de informatie uit elk van die contexten op zichzelf ingrijpend is. De Commissie-Koops legt deze theorie op een kraakheldere manier uit: 'De mozaïektheorie komt er kort gezegd op neer dat, voor de beoordeling van de mate van een privacyinbreuk, niet moet worden gekeken naar losse steentjes, maar naar het beeld dat ontstaat als je de nodige steentjes bij elkaar legt'.[24]
Bij toepassing van de mozaïektheorie van privacy is het denkbaar dat de gelijktijdige inzet van verschillende bijzondere opsporingsbevoegdheden, zoals het stelselmatig verzamelen van gegevens uit open bron en met stelselmatige informatie-inwinning, de opsporing ingrijpend stelselmatig maakt. Het is ook denkbaar dat de inzet van veel verschillende opsporingsmethoden en bijzondere opsporingsbevoegdheden afzonderlijk slechts een klein deel van het privéleven van een persoon in kaart brengt, maar bij elkaar genomen ingrijpend stelselmatig is. Als deze mozaïektheorie van privacy door de wetgever wordt omarmd, verwacht ik overigens ook dat de rechter-commissaris het een stuk drukker krijgt in de meer grootschalige opsporingsonderzoeken.
De Commissie houdt ten slotte ook als meer concreet criterium aan dat het ingrijpend stelselmatig is als redelijkerwijs voorzienbaar gegevens worden onderzocht die onder het beroepsmatig verschoningsrecht vallen.[25]

2.3 Driedeling in normeringssystematiek

Het criterium van (ingrijpende) stelselmatigheid kan volgens de Commissie-Koops in meer brede zin worden gebruikt om onderscheid te maken tussen (1) geringe, (2) meer dan geringe en (3) zeer ingrijpende inbreuken.[26] De Commissie concludeert dat bij de toepassing van bevoegdheden de belangrijkste waarborg is gelegen in de bevoegde autoriteit die toestemming moet geven voor de uitoefening van de bevoegdheid, respectievelijk de opsporingsambtenaar, officier van justitie en rechter-commissaris.[27] In het huidige Wetboek van Strafvordering en het conceptwetsvoorstel wordt tevens de ernst van het delict gekoppeld aan de inzet van bevoegdheden. Daarbij stelt de Commissie-Koops een vangnetbepaling voor (aanbeveling 8). Met die bepaling is ook bij lichtere strafbare feiten dan voorgeschreven de inzet van de bevoegdheid mogelijk, mits sprake is van een machtiging van de rechter-commissaris en indien een zwaarwegend belang de opsporing van dat feit dit dringend vordert.
Deze driedeling past op zichzelf goed bij het huidige stelsel, waar de normering van opsporingsmethoden sterk samenhangt met de ernst van de inbreuk op de persoonlijke levenssfeer (privacy).[28] De Commissie erkent overigens dat ook andere grondrechten van belang kunnen zijn. De wetgever zal daar volgens de commissie in de memorie van toelichting bij het conceptwetsvoorstel Boek 2 aandacht aan moeten geven.[29] Daarbij zal de wetgever mijns inziens in het bijzonder ook rekening moeten houden met de rechten en plichten die voortvloeien uit het recht op een eerlijk proces op grond van artikel 6 EVRM. Kortom, zwaardere inbreuken op de persoonlijke levenssfeer bij de toepassing van opsporingsmethoden, vergen zwaardere waarborgen in wetgeving. Een (zeer) vergelijkbaar model van de verhouding tussen de zwaarte van privacy-inbreuken en de bevoegde

autoriteiten, heb ik destijds ook in mijn proefschrift geabstraheerd uit de jurisprudentie met betrekking tot artikel 8 (recht op privacy) van het Europees Verdrag voor de Rechten van de Mens (hierna: EVRM) van het Europees Hof voor de Rechten van de Mens (hierna: EHRM).[30] Een verschil is dat ik daaraan heb toegevoegd dat ook de mate van gedetailleerdheid van de regeling dient toe te nemen naarmate de privacy-inmenging zwaarder wordt, zodat de reikwijdte van meer ingrijpende bevoegdheden voldoende kenbaar en voorzienbaar is. De verhouding tussen de zwaarte van privacy-inmenging en de bevoegde autoriteiten zoals de Commissie-Koops voorstelt, in combinatie met het vereiste van een voldoende gedetailleerde regeling, wordt hieronder in Figuur 1 geïllustreerd.

Figuur 1: Verhouding tussen de zwaarte van privacy-inmenging en bevoegde autoriteiten



3 Stelselmatig vergaren van gegevens uit open bronnen

Het verzamelen en verwerken van gegevens uit een voor eenieder toegankelijke bron (‘open bron’) is volgens de politie een vast onderdeel van het politiewerk. Het wordt gebruikt bij opsporing, ‘*crowd control*’, evenementen en tijdens crisissituaties.[31] Mensen publiceren vrijwillig grote hoeveelheden persoonsgegevens op websites en sociale media. Ook andere personen, bedrijven of instellingen publiceren gegevens over personen op internet. Binnen een opsporingsonderzoek kan de politie deze gegevens bijvoorbeeld gebruiken ter identificatie van verdachten, getuigen en personen waarmee een verdachte

(online) in contact staat. De gegevens kunnen ook mogelijk bewijs opleveren van strafbare feiten (denk aan opruiing) op basis van uitlatingen van de verdachte op internet.[32]
Bij het verzamelen van persoonsgegevens vindt een inmenging met het recht op privacy plaats (meer specifiek met het recht op bescherming van persoonsgegevens). De wetgever acht het wenselijk dat bij het stelselmatig verzamelen van gegevens omtrent een persoon uit open bron een (nieuwe) bevoegdheid wordt ingezet. Daartoe is het volgende voorstel gedaan in het conceptwetsvoorstel Boek 2:

Stelselmatige vastlegging van persoonsgegevens uit open bronnen
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.*

De Commissie-Koops geeft enkele aanbevelingen met betrekking tot de voorgestelde regeling binnen de context van het opsporingsproces.[33] In deze paragraaf wordt de definitie van een open bron en de uitleg van het begrip ‘stelselmatig’ bij openbronnenonderzoek besproken. Daarnaast komt in deze paragraaf de inzet van zogenoemde ‘*crawlers*’ en ‘*scrapers*’ in verhouding tot de nieuwe bevoegdheid aan bod, alsmede de vraag op welke wijze de nieuwe bevoegdheid zich onderscheidt van stelselmatige observatie.

3.1 Het begrip open bron

Het is van belang het begrip ‘open bron’ goed af te bakenen, omdat de term de indruk kan geven dat het vergaren van gegevens ‘vrij’ of ‘onbeperkt’ is. Bij het overnemen van gegevens uit open bron vindt echter een privacy-inbreuk plaats die een aparte grondslag in de wet behoeft.[34] Tegen deze achtergrond moet de introductie van de bevoegdheid worden gezien, waarbij een officier van justitie een bevel afgeeft tot het *stelselmatig* vergaren van persoonsgegevens uit open bron voor een periode van maximaal drie maanden bij delicten die worden bedreigd met een gevangenisstraf van één jaar of meer.

De Commissie beveelt aan dat de wetgever in de memorie van toelichting op het conceptwetsvoorstel Boek 2 meer informatie geeft over het begrip 'open bron'. In de praktijk kan er namelijk onduidelijkheid over bestaan wat de reikwijdte daarvan is. Daar speelt bijvoorbeeld de vraag of registratie op een socialemediawebsite is toegestaan bij openbronnenonderzoek en betaling is toegestaan om toegang te krijgen tot gegevens. In het rapport geeft de Commissie-Koops hier meer duidelijkheid over.
Open bronnen kenmerken zich volgens de Commissie door het feit dat in beginsel eenieder er toegang toe kan verkrijgen. Een open bron omvat volgens de commissie ook het *deep web*; het gedeelte van het internet dat niet geïndexeerd is door zoekmachines, maar dat wel feitelijk toegankelijk is bij bezoek van de betreffende website. Hetzelfde geldt voor het *dark web*, het gedeelte van internet waarvan de IP-adressen van servers verborgen zijn en dat alleen toegankelijk is via speciale software, zoals de Tor-browser.[35]
Ook betaaldiensten zonder nadere toegangscontrole, zoals toegang tot LexisNexis, de Kamer van Koophandel of integrale bestanden die op de markt tegen betaling beschikbaar zijn, vallen volgens de commissie onder het begrip 'open bron'. Voor zover die toegang gebonden is aan een account, moet het verkrijgen van een account een (semi)geautomatiseerd proces zijn, waarbij niet bepaalde groepen worden uitgesloten van registratie. Het is wellicht vanzelfsprekend, maar de Commissie merkt op dat het verzamelen van gegevens langs irreguliere wegen, bijvoorbeeld door gebruikmaking van een technische truc, niet valt onder het overnemen van gegevens uit publiek toegankelijke bronnen.[36]
Open bronnen staan dus tegenover afgeschermde bronnen, die zich kenmerken doordat een internetgebruiker er uitdrukkelijk voor kiest andere internetgebruikers al dan niet toe te laten tot de bron. Daarbij kan gedacht worden aan profielgegevens van een gebruiker van Facebook, waarbij de gebruiker slechts toegang geeft tot de informatie op zijn profiel na het accepteren van een vriendschapsverzoek.[37]

3.2 Het begrip stelselmatig in een online context

De Commissie-Koops wijst er terecht op dat 'stelselmatig' in deze context een andere betekenis heeft dan bijvoorbeeld stelselmatige observatie in de fysieke wereld. In een online omgeving is het namelijk mogelijk met een korte, eenmalige actie een grote hoeveelheid persoonsgegevens te vergaren. Aspecten als duur (tien minuten) en frequentie (eenmalig) spelen dan in het geheel geen rol, terwijl de inbreuk op de persoonlijke levenssfeer substantieel kan zijn. De privacy-inbreuk blijft volgens de Commissie-Koops beperkt bij het raadplegen van nieuwsbronnen of vlogs waarbij het de bedoeling is deze inhoud wereldkundig te maken en als de politie gericht zoekt op sociale media naar mogelijke getuigen bij een incident.[38]
De hamvraag is dan wat 'stelselmatig' is. De Commissie-Koops noemt daarbij in totaal *zeventien* (!) factoren die kunnen worden gebruikt om stelselmatigheid in te vullen. Deze factoren kunnen geclusterd worden tot de volgende vier aspecten: (1) omvang en type van de (over te nemen) gegevens, (2) aard van de bron, (3) wijze van zoeken en (4) het gebruik van de gegevens en de mogelijke impact op de persoon.[39] Met deze invulling van de norm

wordt aangesloten bij de voorgestelde algemene norm van stelselmatigheid. Hoewel een deel van de Commissie-Koops van mening is dat ingrijpende stelselmatigheid niet aan de orde kan zijn bij het overnemen van persoonsgegevens uit publiek toegankelijke bronnen, wordt toch geadviseerd voor openbronnenonderzoek het algemene normeringscriterium te hanteren, inclusief de optie van 'ingrijpende stelselmatigheid'.[40]
Ondanks deze handvatten vermoed ik dat de opsporingspraktijk moeite zal hebben de factoren in de praktijk toe te passen.[41] Mogelijk komen bij de uitvoering van de nieuwe bevoegdheid concrete toepassingen naar boven waarvoor standaard wel of geen bevel tot het stelselmatig verzamelen van gegevens uit open bronnen hoeft te worden verkregen. De vraag blijft dan wel bestaan of de nieuwe regeling voldoende voorzienbaar voor burgers is, omdat het moeilijk te duiden is wanneer een officier van justitie het bevel moet afgeven. Mogelijk wordt dit risico gemitigeerd als uit geopenbaard beleid of uit gepubliceerde jurisprudentie meer concrete normen boven komen drijven. Mijns inziens past het normeringscriterium goed bij deze bevoegdheid, gezien de grote verscheidenheid aan toepassingen, waarbij in meer of mindere mate een inbreuk plaatsvindt op de persoonlijke levenssfeer van de betrokkenen.

3.3 Inzet van crawlers en scrapers

De Commissie-Koops gaat ook in op de vraag in hoeverre de inzet van *crawlers* is toegestaan op basis van de algemene opsporingstaak van de politie (art. 3 Polw. 2012 jo. 141-142 Sv) of op basis van de nieuwe bevoegdheid tot het stelselmatig verzamelen van gegevens omtrent personen uit open bron, maar geeft hierop geen duidelijk antwoord.
Een *crawler* is kortgezegd een programma dat binnen ingestelde condities (zoals welke bronnen moeten worden doorzocht en op welke woorden of andere zoektermen moet worden doorzocht) gegevens van internet verzamelt, zoals webpagina's die voldoen aan de criteria, en deze vervolgens indexeert. Als daarbij ook gegevens worden vastgelegd, wordt gesproken van een '*scraper*'. De Commissie geeft aan dat het met software bijvoorbeeld mogelijk is alle gesprekken in een bepaald chatkanaal vast te leggen en later te doorzoeken of via de zogenoemde API ('*Application Programming Interface*') van Twitter automatisch gegevens van Twittergebruikers vast te leggen.[42]
Er is geen strafrechtelijke jurisprudentie over de inzet van *crawlers* en *scrapers* beschikbaar, wat op zichzelf al iets zegt over de huidige kenbaarheid en voorzienbaarheid van de opsporingsmethode.[43] Binnen het bestuursrecht zijn drie uitspraken van de Rechtbank Amsterdam beschikbaar, waaruit blijkt dat de gemeente Amsterdam een *scraper* heeft ingezet om webpagina's van Airbnb vast te leggen om na te gaan of een bewoner ten onrechte zijn woonboot meer dan het toegestaan aantal dagen verhuurde.[44] De Rechtbank Amsterdam achtte de inzet van het middel rechtmatig op grond van de algemene onderzoeksbevoegdheid in artikel 3:2 van de Algemene wet bestuursrecht (Awb).[45]
De wetgever hint er in de memorie van toelichting van het conceptwetsvoorstel voor Boek 2 op dat, wanneer gebruik wordt gemaakt van een *webcrawler* voor de vastlegging van gegevens, al snel een verdergaande privacy-inbreuk plaatsvindt (en de inbreuk dus stelselmatig is).[46] In dat geval is de inzet van de nieuw voorgestelde bijzondere

opsporingsbevoegdheid op zijn plaats. Het wordt in de memorie van toelichting van het conceptwetsvoorstel niet helder gemaakt of een *crawler* of *scraper* ook als 'technisch hulpmiddel' wordt aangemerkt zoals wordt bedoeld in het Besluit technische hulpmiddelen. Hier vallen doorgaans andere middelen onder, zoals middelen die worden gebruikt voor stelselmatige observatie of de hackbevoegdheid.[47]
De Commissie-Koops gebruikt ook hier het normeringscriterium van stelselmatigheid en stelt dat, afhankelijk van de privacy-inmenging die daarbij naar verwachting plaatsvindt, de inzet van de nieuwe bevoegdheid op zijn plaats is, omdat het dan als stelselmatig kan worden gekwalificeerd. De Commissie-Koops neemt dus niet de positie in dat altijd sprake is van stelselmatigheid bij de inzet van een *crawler* of *scraper*. Het gevaar bestaat daardoor dat het voor de opsporingspraktijk niet voldoende duidelijk is welke grondslag in strafvordering gepast is bij het gebruik van dergelijke instrumenten.[48] Mijns inziens moet ook aan de inzet van de bevoegdheid van stelselmatige observatie worden gedacht als het middel voor een langere duur persoonsgegevens van dezelfde bron verzamelt (zie verder paragraaf 3.4).
Gezien de hoeveelheid gegevens die door de inzet van een *scraper* doorgaans wordt verwerkt, is het binnen het kader van het conceptwetsvoorstel Boek 2 naar mijn mening passend het criterium van stelselmatigheid bij gebruik van een *scraper* toe te passen. De privacy-inmenging is daarbij zwaarder dan bij een *crawler*, omdat bij een *scraper* veel meer persoonsgegevens worden opgeslagen. Het heeft mijn voorkeur dat de wetgever in de memorie van toelichting de knoop doorhakt en uitlegt of de inzet van de nieuwe bevoegdheid is vereist bij de inzet van deze middelen.[49]

3.4 Onderscheid met stelselmatige observatie

Het stelselmatig vastleggen van gegevens omtrent personen onderscheidt zich volgens de memorie van toelichting op het conceptwetsvoorstel van stelselmatige observatie in de zin dat het volgen of waarnemen bij observatie een '*realtime*' element in zich heeft. De aanwezigheid, het gedrag of de bewegingen van de persoon worden *realtime* gevolgd of waargenomen en daarmee feitelijk vastgelegd. Bij het onderzoek in open bronnen gaat het daarentegen vooral om 'historische' gegevens die reeds aanwezig en beschikbaar zijn.[50]
De Commissie-Koops kan zich – terecht vind ik – grotendeels vinden in deze toelichting.[51] Volgens de Commissie bestaat echter onduidelijkheid of de bevoegdheid tot stelselmatige observatie dan wel het stelselmatig verzamelen van persoonsgegevens moet worden ingezet als bijvoorbeeld een '*lifelog-blog*' of een uitzending op een live-streamingdienst als '*periscope*' van een verdachte wordt gevolgd. Ook Stol en Strikwerda (2018) geven aan dat het onderscheid tussen het verzamelen van 'historische' en 'toekomstige gegevens' niet duidelijk is. De Commissie-Koops beveelt de wetgever dan ook aan het onderscheid tussen het stelselmatig vastleggen van persoonsgegevens uit open bron en stelselmatig observatie beter uit te leggen.[52]
Toch begrijp ik deze onduidelijkheid niet goed. Voordat in een opsporingsonderzoek het besluit wordt genomen gebruik te maken van een bepaalde publiekelijk toegankelijke bron, moet een inschatting worden gemaakt of daarbij historische of toekomstige gegevens

worden verzameld. Bij het aangedragen voorbeeld wordt gedrag van mensen gevolgd of waargenomen en heeft het een '*realtime*' element in zich, waardoor er mijns inziens sprake is van observatie.

4 Beslag op digitale gegevensdragers

Het leggen van beslag op gegevensdragers met daarop opgeslagen gegevens is een ingewikkeld onderwerp met vele flankerende onderwerpen, waarover al veel is geschreven.[53] De Commissie-Koops heeft de voorgestelde regelingen in afdeling 7.4.2 uit het conceptwetsvoorstel over 'onderzoek ter kennisneming van gegevens' uitvoerig geanalyseerd en komt in totaal tot 26 aanbevelingen op dit onderwerp. Daarbij wordt bijvoorbeeld ook ingegaan op het voorstel tot 'beslag op gegevens'[54] en wordt een nieuwe regeling voorgesteld voor onderzoek aan 'op het lichaam verbonden gegevensdragers', zoals pacemakers en een oog- of oorimplantaat.[55]
In deze paragraaf ga ik alleen in op de aanbevelingen van de Commissie-Koops met betrekking tot de voorwaarden voor het beslag op gegevensdragers en het daaropvolgende onderzoek van de opgeslagen gegevens op deze gegevensdragers.[56] In de kern gaat het over de vraag welke autoriteit bevoegd is beslag te leggen en onderzoek op de opgeslagen gegevens te verrichten, gezien de ernst van de privacy-inbreuk die deze handelingen op de persoonlijke levenssfeer van de betrokkenen met zich meebrengen. Daarnaast ga ik kort in op het voorstel met betrekking tot het kennisnemen van inkomende berichten op inbeslaggenomen gegevensdragers, de netwerkzoeking en in hoeverre de (al dan niet gedwongen) ontsleuteling van gegevensdragers is toegestaan.

4.1 Bevoegde autoriteiten voor beslag en onderzoek van gegevens

In 2014 besliste het Amerikaanse Hooggerechtshof in de zaak *California v. Riley* dat voor het in beslag nemen van een telefoon van een verdachte na een arrestatie een '*warrant*' (rechterlijk bevel) is vereist.[57] Mobiele telefoons zijn niet 'zomaar een voorwerp dat vatbaar is voor inbeslagname'. Aan de praktische bezwaren van de opsporing hadden rechters ook geen boodschap. De rechters overwegen op p. 28 van de uitspraak:

> 'Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life" (…). The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple – get a warrant.'

Mede naar aanleiding van deze '*landmark case*' in de Verenigde Staten is in Nederland een discussie op gang gekomen. In Nederland denken de wetgever en Hoge Raad heel anders over de wenselijke bescherming die moet worden gegeven aan moderne mobiele telefoons (*smartphones*). In artikel 2.7.4.2.1 van het conceptwetsvoorstel wordt voorgesteld dat een

bevel van een officier van justitie is vereist als onderzoek wordt gedaan aan 'een inbeslaggenomen elektronische gegevensdrager of in een inbeslaggenomen geautomatiseerd werk' (zoals een smartphone). In 2017 heeft de Hoge Raad bovendien in het 'smartphone-arrest' bepaald dat een bevel van een officier van justitie is vereist als het onderzoek 'zo verstrekkend is dat een min of meer compleet beeld is verkregen van bepaalde aspecten van het persoonlijk leven van de gebruiker van de gegevensdrager of het geautomatiseerde werk'.[58]
De Commissie-Koops bouwt voort op de ingezette lijn van de wetgever en de Hoge Raad. De Commissie stelt – in navolging van de nieuwe rol voor het begrip stelselmatigheid – de volgende bevoegdheid voor:

> '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.'[59]

Slechts voor ingrijpende vormen van 'stelselmatig onderzoek' aan een digitale gegevensdrager of geautomatiseerd werk is volgens de Commissie een machtiging van een rechter-commissaris noodzakelijk.[60] In andere gevallen is het bevel van een officier van justitie voldoende. De Commissie-Koops geeft in haar rapport aan dat het onderzoek *slechts in uitzonderingsgevallen* zeer ingrijpend is.[61] Dat is bijvoorbeeld het geval wanneer kennis wordt genomen van geheimhoudercommunicatie. De Commissie komt niet tot andere concrete voorbeelden waarbij van ingrijpende stelselmatigheid sprake zou zijn.
Ter invulling van het criterium van stelselmatigheid geeft de Commissie-Koops ook enkele voorbeelden.[62] Tijdens de doorzoeking bij een bedrijf waarbij de gehele administratie wordt overgenomen, geïndexeerd en vervolgens automatisch wordt doorzocht, acht de Commissie bijvoorbeeld een bevel van een officier van justitie voldoende, omdat daarbij stelselmatig onderzoek op de opgeslagen gegevens wordt uitgevoerd.[63] De aard van de digitale gegevensdrager is volgens de Commissie als factor aan te merken om de ernst van de inbreuk op de persoonlijke levenssfeer te bepalen.[64] De Commissie-Koops legt verder in het rapport uit dat de wijze waarop kennis wordt genomen van de gegevens uit een geautomatiseerd werk de zwaarte van de privacy-inbreuk (en stelselmatigheid) beïnvloedt. Het *kennisnemen* van gegevens op een computer tijdens een doorzoeking acht de Commissie bijvoorbeeld minder vergaand dan het *overnemen* van gegevens uit een geautomatiseerd werk. En het nader verwerken van de overgenomen gegevens en mogelijk verrijken van de gegevens met andere gegevenssets die eerder zijn verworven, is een factor die de privacy-inmenging zwaarder maakt.
De Commissie levert in het rapport een waardevolle bijdrage aan de nadere invulling van begrippen als 'digitale gegevensdrager' en wat het kennisnemen en vastleggen van gegevens in de context van artikel 2.7.4.2.1 en verder behelst.[65] Ook begrijp ik dat de zwaarte van de privacy-inmenging bij de inbeslagname en het nadere onderzoek aan de gegevens op een gegevensdrager per situatie verschilt. Toch ben ik het meer principieel niet eens met de aangelegde drempel wanneer sprake is van een beperkte, meer dan

beperkte en ingrijpende inbreuk op de persoonlijke levenssfeer bij de inbeslagname van 'persoonlijke computers', zoals een smartphone.
Royer en ik hebben eerder (in 2017) uiteen gezet dat wij bij het doorzoeken van gegevens op een inbeslaggenomen smartphone een machtiging van een rechter-commissaris gepast vinden (behoudens uitzonderingen).[66] Mijn inschatting is dat veel generatiegenoten – en de '*millennials*' daarna – het met ons eens zullen zijn dat het kennisnemen van foto's, berichten of bezochte webpagina's op een smartphone een *ingrijpende bevoegdheid* is, waarbij toestemming van een rechter-commissaris op zijn plaats is. '*My phone is my castle*',[67] wordt ook wel door de Amerikanen gezegd. Deze uitdrukking geeft een meer eigentijdse indruk van de zwaarte van de privacy-inmenging.
Als gevolg van het smartphone-arrest lijkt nu de norm ontwikkeld dat het kennisnemen van foto's op een smartphone doorgaans een beperkte privacy-inbreuk is, waarvoor slechts toestemming van een opsporingsambtenaar nodig is.[68] Het conceptwetsvoorstel en de ontwikkelde norm van de Hoge Raad liggen daarmee ver uiteen met de privacybeleving die veel burgers ervaren bij de inbeslagname van persoonlijke computers.[69] In plaats van het criterium van stelselmatigheid kan beter worden aangesloten bij het (oude) normeringcriterium van de zwaarte van de inbreuk op de persoonlijke levenssfeer, waarbij het doorzoeken van gegevens op een inbeslaggenomen smartphone als een ernstige inbreuk op de persoonlijke levenssfeer van de betrokkene wordt beschouwd.
Waarom zou het niet mogelijk zijn een regeling te creëren voor het beslag en onderzoek van gegevens op geautomatiseerde werken waarbij – behoudens enkele uitzonderingen – een machtiging van een rechter-commissaris is vereist? Het type geautomatiseerd werk waaraan dan moet worden gedacht, zoals een smartphone, laptop, PC en tablet computer, kan daarbij best in de memorie van toelichting worden beschreven. Het is spijtig dat de Commissie in het rapport weinig ruimte geeft voor deze alternatieve visie.[70]

4.2 Uitlezen van inkomende berichten

De Commissie-Koops signaleert een belangrijk probleem voor de opsporingspraktijk, namelijk dat de politie zich niet goed raadt weet met de vraag in hoeverre kennis mag worden genomen van inkomende berichten op het inbeslaggenomen apparaat. Steeds vaker wordt '*live data forensics*' toegepast, waarbij het apparaat aan blijft staan, terwijl digitaal forensisch onderzoek plaatsvindt of actief gegevens die elders staan opgeslagen worden opgehaald. Deze handelswijze wordt noodzakelijk geacht, omdat (1) batterijen en opslagmedia vaak niet meer verwijderd kunnen worden zonder de apparatuur te beschadigen, (2) versleuteling in werking kan treden of wordt geactiveerd en (3) steeds meer gegevens (zoals berichtengeschiedenis, foto's en notities) worden opgeslagen in de cloud en niet meer op het apparaat zelf.[71]
Het kennisnemen of overnemen van de inhoudelijke berichten op een geautomatiseerd werk is bijvoorbeeld mogelijk bij synchronisatie van programma's (*apps*) op het apparaat. De kennisname is ook mogelijk door actief in te loggen in accounts en gegevens op te halen van aanliggende geautomatiseerde werken (servers van de aanbieder van een dienst). De commissie onderschrijft het opsporingsbelang om gedurende enige tijd het monitoren van

binnenkomende berichten mogelijk te maken. 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 en is een machtiging van een rechter-commissaris noodzakelijk.[72] Onder zo'n actieve rol valt in elk geval het na inbeslagneming actief synchroniseren van de apps op een smartphone, aldus de Commissie. Ook kan worden gedacht aan het inschakelen van een smartphone die ten tijde van de inbeslagneming uit stond en na inschakeling automatisch berichten (zoals e-mail- en chatberichten) ophaalt van een server.
De Commissie stelt dan ook voor om een extra lid toe te voegen aan de regeling voor het gegevensonderzoek aan het apparaat van de eindgebruiker of de daaraan gekoppelde netwerkzoeking (art. 2.7.5.1 en art. 2.7.5.2 van het conceptwetvoorstel Boek 2). Dit voorstel, inclusief voorgestelde waarborg van een machtiging van de rechter-commissaris, acht ik ook wenselijk.

4.3 De netwerkzoeking

De netwerkzoeking werd in de memorie van toelichting op de Wet computercriminaliteit I nog omschreven als 'de meest vergaande bevoegdheid tot onderzoek in geautomatiseerde werken'.[73] De reden daarvoor is dat het (destijds) de mogelijkheid gaf tijdens een huiszoeking onderzoek te doen in 'een elders aanwezig geautomatiseerd werk', voor zover dit redelijkerwijs nodig is om de waarheid aan de dag te brengen. Dat wil zeggen dat onder de bevoegdheid van een netwerkzoeking toegang mag worden verschaft en onderzoek mag worden gedaan op aangesloten computers die vanaf de plek van de doorzoeking bereikbaar zijn, voor zover de verdachte of een andere rechthebbende daartoe ook toegang heeft.[74]
In 2006 is de regeling in artikel 125j Sv van de netwerkzoeking uitgebreid, waardoor de bevoegdheid van de netwerkzoeking bij *alle* doorzoekingen mag worden ingezet. Daarmee is het ook mogelijk gemaakt tijdens een doorzoeking in een kantoor, bijvoorbeeld door toegang te verschaffen tot een e-mailserver in een datacentrum dat vanaf de plek van de doorzoeking (digitaal) bereikbaar is. In de memorie van toelichting op het conceptwetsvoorstel Boek 2 maakte de wetgever duidelijk dat de reikwijdte van de netwerkzoeking ook strekt tot bijvoorbeeld de webmail van een verdachte.[75]
De Commissie-Koops wijst erop dat de doorzoeking ter vastlegging van gegevens en de netwerkzoeking op dit moment vaak plaatsvindt bij een datacentrum of een andere professionele partij. Dergelijke bedrijven hebben tegenwoordig faciliteiten om op afstand toegang te verschaffen tot gegevens ten behoeve van bijvoorbeeld onderhoud, terwijl er slechts beperkte faciliteiten zijn om fysiek toegang tot de gegevens te verschaffen. Ik neem aan dat deze faciliteiten ook door of voor opsporingsinstanties kunnen worden ingezet.
De Commissie-Koops maakt ook duidelijk dat bij particulieren een '*cloud-doorzoeking*' kan plaatsvinden – eventueel met behulp van commerciële forensische software – via de accounts van een verdachte. In de praktijk komt het steeds vaker voor dat de gegevens die voor opsporingsonderzoek relevant zijn, elders dan op het inbeslaggenomen geautomatiseerd werk beschikbaar zijn.[76] 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'.[77]

De Commissie-Koops wijst er terecht op dat de netwerkzoeking alleen mag worden uitgevoerd tijdens een doorzoeking. De netwerkzoeking mag bovendien alleen betrekking hebben op elders opgeslagen gegevens als er een rechtmatige band bestaat tussen de gebruiker en deze gegevens.[78]
De opsporingspraktijk heeft er behoefte aan ook gegevens in de cloud in andere gevallen (na inbeslagname en in situaties van aanhouding en staandehouding), op een later moment en op afstand veilig te stellen. De Commissie adviseert daarom in het Wetboek van Strafvordering in de mogelijkheid te voorzien om het uitvoeren van het onderzoek van gegevens op afstand mogelijk te maken.[79] Met de voorgestelde wijzigingen door de Commissie-Koops wordt ook een herhaalde netwerkzoeking op een later moment (op afstand) mogelijk, waarbij dus ook gegevens uit Apple's '*iCloud*' of andere gegevens via accounts van de verdachte op afstand veilig kunnen worden gesteld. Het zou daarbij ook mogelijk moeten zijn om achteraf actief in te loggen op een account om de gegevens op te halen. Het account moet wel in gebruik zijn geweest bij de verdachte, hetgeen kan blijken uit het feit dat er vanuit het geautomatiseerde werk is ingelogd op het e-mail-, chat- of socialemedia-account van die persoon.[80]
Daarmee lijkt de voorgestelde regeling tot wijziging van de netwerkzoeking op de hackbevoegdheid, omdat op afstand toegang wordt verkregen tot een geautomatiseerd werk.[81] De opsporingshandeling ligt echter in het verlengde van de doorzoeking en de ratio van de netwerkzoeking, waardoor het logisch is aan te sluiten bij de netwerkzoeking. Een machtiging van een rechter-commissaris is noodzakelijk, als berichten worden aangetroffen tijdens een netwerkzoeking in een geautomatiseerd werk van een aanbieder.[82] Mijns inziens is de waarborg van een machtiging van een rechter-commissaris bij een netwerkzoeking te allen tijde wenselijk.[83]
Volgens de Commissie is de nood tot het mogelijk maken van deze opsporingshandelingen zo hoog, dat deze zo snel mogelijk in werking moeten treden en dus niet kan worden afgewacht op de implementatie van het conceptwetsvoorstel in het Wetboek van Strafvordering.[84]

4.4 Ontsleuteling van gegevensdragers

De versleuteling van gegevensdragers door verdachten en de mogelijkheden op afstand de inhoud van gegevensdragers te wissen vormen een belangrijk probleem binnen de opsporingspraktijk.[85] De versleuteling vindt doorgaans plaats met de toepassing van een cijfercode of wachtwoord.[86] Nieuwe mobieltjes ondersteunen ook vaak de mogelijkheid het apparaat te openen met een vingerafdruk, irisscan of door middel van gezichtsherkenning. In de Wet computercriminaliteit III is uiteindelijk afgezien van de mogelijkheid verdachten te verplichten de beveiliging van geautomatiseerde werken ongedaan te maken door het

afgeven van een wachtwoord onder dreiging van een gevangenisstraf, omdat de maatregel in strijd met het nemo-teneturbeginsel wordt geacht.[87] Voor het toegang geven op basis van biometrie, zoals door middel van de vingerafdruk, irisscan en gezichtsherkenning, ligt dit echter anders omdat het dan om – kort gezegd – lichaamsonafhankelijk materiaal gaat. De afgifte daarvan is al eerder niet in strijd geacht met het nemo-teneturbeginsel, afgeleid uit artikel 6 EVRM.[88] Met lichte dwang, zoals het opleggen van de vinger bij de vingerafdrukscanner of bij het houden van de smartphone voor het gezicht van de verdachte, kan soms toegang tot het apparaat worden verschaft.[89] Daarbij mag uiteraard geen excessief geweld worden toegepast.

Bij een wachtwoord moet een geestesinspanning worden geleverd om het wachtwoord te produceren. Het onderscheidt zich daarmee van lichaamsonafhankelijk materiaal. De Commissie-Koops en bijvoorbeeld ook Van Toor (2017) zijn van mening dat het verplicht ongedaan maken van de beveiliging door middel van een vingerafdruk, irisscan en gezichtsherkenning van de verdachte – voor zover proportioneel en subsidiair – juridisch haalbaar is.

De Commissie-Koops acht de introductie van een *bevel* aan verdachten tot medewerking aan biometrische ontsluiting niet nodig. De dreiging bij het niet-naleven van een bevoegd ambtelijk gegeven bevel van maximaal drie maanden gevangenisstraf (art. 184 Sr) zal volgens de Commissie 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 strafbedreigingen.[90]

Wel stelt de Commissie voor om biometrische toegangsverschaffing onder (lichte) dwang mogelijk te maken voor verdachten én voor anderen dan de verdachte, als zijnde een 'duldplicht'.[91] Een bevel van de officier van justitie zou daarbij voldoende moeten zijn, gezien de 'niet-verwaarloosbare' inbreuk op de lichamelijke integriteit. Bood stelt echter dat de voorgestelde regeling in aanbeveling 28 van de Commissie te kort door de bocht is en 'gemakkelijk kan leiden tot een regeling die niet EVRM-proof is'.[92] Dit voorstel verdient daarom wellicht nog nadere bestudering. Ik verwacht echter dat, voordat de wetgever daaraan toekomt, eerst gerechten hierover uitspraak moeten doen naar aanleiding van verweren van advocaten op dit punt.

5 'Dataficering' van het opsporingsproces

In hoofdstuk 2 en 3 van het rapport geeft de Commissie een beknopte schets van het digitale landschap en de intensieve processen van gegevensverwerking bij de politie. In algemene zin vindt een digitalisering van het dagelijks leven plaats en de daarmee gepaard gaande toename in de vastlegging en het hergebruik van gegevens. De Commissie stelt vast dat gedragingen van personen op internet (bijvoorbeeld op socialemediadiensten) en de fysieke wereld (vastlegging door sensoren zoals camera's en wifi- en Bluetoothverbindingen) in steeds toenemende mate digitaal worden vastgelegd en uitgewisseld of gereproduceerd kunnen worden. De politie maakt daarbij in toenemende mate gebruik van de gegevens die bij private bedrijven beschikbaar zijn.

Deze tendens van de 'digitalisering en de beschikbaarheid van gegevens' (dataficering) voor het opsporingsproces noopt volgens de Commissie niet tot aanpassingen aan het

Wetboek van Strafvordering. De Commissie-Koops volstaat slechts met de aanbeveling dat de wetgever aandacht dient 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'.[93]

Een grondiger analyse zou volgens de Commissie de onderzoeksopdracht overstijgen. Het is begrijpelijk dat de Commissie geen aanbevelingen doet over de modernisering van wetgeving met betrekking tot andere politietaken, zoals de handhaving van de openbare orde, en andere wetgeving, zoals de Wet politiegegevens. Dat betekent echter niet dat gegevensverwerkingen bij de politie met een uitwerking in de opsporing als onderwerp terzijde moet worden geschoven. Gegevensverwerkingen bij de politie kunnen namelijk van invloed zijn op de opsporing en daarmee op strafvordering. Gezien de snelle ontwikkelingen op het gebied van data-analyse en het potentieel van 'data science' voor de politie, is het *juist* een onderwerp dat behandeld dient te worden in het kader van 'strafvordering in het digitale tijdperk'.
In deze paragraaf wordt eerst uitgelegd aan welke regeling bij gegevensverwerkingen met een uitwerking in de opsporing kan worden gedacht. Daarna wordt ingegaan op het vermeende gebrek aan toezicht bij bepaalde gegevensverwerkingen door de politie.

5.1 Gegevensverwerkingen met een uitwerking in de opsporing

Hildebrandt (2016) heeft in haar preadvies voor de Nederlandse Juristen Vereniging al eerder nadrukkelijk aandacht gevraagd voor de dataficering in de opsporing en de inzet van systemen ('*agents*') ter analyse van deze gegevens in het opsporingsproces.[94] In het rapport van de Commissie wordt niet naar het preadvies verwezen of op de aanbevelingen ingegaan.
Het is echter ontegenzeggelijk dat de politie gebruikmaakt van data-analysetechnieken ter uitvoering van haar taken, inclusief de opsporingstaak. Daarbij kan gedacht worden aan '*predictive mapping*' en '*predictive identification*'. Bij *predictive mapping* wordt het 'waar' en 'wanneer' van criminaliteit in kaart gebracht. Bij *predictive identifcation* worden personen of groepen aangewezen als potentiële daders of slachtoffers.[95] Das en Schuilenburg (2018) betogen in hun artikel over *predictive policing* en strafvordering dat dit soort gegevensverwerkingen onderdeel uit kan maken van de opsporing en daarmee van strafvordering. Zij merken op dat 'wanneer een voorspelling wordt gegenereerd met het doel burgers te selecteren die mogelijk betrokken (zullen) zijn bij strafbare feiten, deze selectie uiteindelijk leidt tot een verdenking en nadere strafvorderlijke ingrepen (bijvoorbeeld de aanhouding van de geselecteerde burger)'.[96]
Das en Schuilenburg bevelen aan dat bij de modernisering van het Wetboek van Strafvordering moet worden overwogen een afzonderlijke grondslag op te nemen voor het gebruik van voorspellende instrumenten in de fase vóór de verdenking.[97] Een officier van

justitie zou mijns inziens het bevel tot het gebruik ervan kunnen toetsen op het doel, de noodzaak, de proportionaliteit en subsidiariteit, en de bewaartermijn van de gegevens aangeven. Daarnaast moet het Wetboek van Strafvordering ervoor zorgen dat het gebruik van data-analysetechnieken met betrekking tot de opsporing met waarborgen wordt omkleed ter bescherming van de betrokkenen. Tot op zekere hoogte is over het gebruik van data-analyse transparantie vereist, moeten de data-analysetechnieken voor de verdediging uitlegbaar worden, zouden de data-analysetechnieken aan bepaalde kwaliteitseisen moeten voldoen en is een zorgplicht voor het gebruik van dergelijke technieken noodzakelijk.[98] Hoe die regeling in het Wetboek van Strafvordering er precies uit moet zien, vergt nader onderzoek. De Commissie-Koops had hier een bijdrage aan kunnen leveren door hierover een heldere aanbeveling te doen, maar daar is het helaas niet van gekomen.

Het bovenstaande in aanmerking genomen komt het vreemd voor dat de Commissie-Koops wél nadrukkelijk wijst op een in de opsporingspraktijk gemiste (vergaande) bevoegdheid, namelijk 'het vorderen van data-analyse door derden' ten behoeve van de opsporing. Met de voorgestelde bevoegdheid moeten derden, zoals banken, telecommunicatiebedrijven en openbaarvervoersvervoerinstellingen, op vordering van een officier van justitie of (bij ingrijpende stelselmatigheid) de rechter-commissaris, gegevensanalyses uitvoeren voor de politie.[99] De bevoegdheid zou noodzakelijk zijn om bijvoorbeeld in het kader van publiek-private samenwerking analyses ten behoeve van de opsporing uit te voeren. De Commissie geeft aan dat in de praktijk de betrokken partijen 'zich beperkt voelen' door civiele aansprakelijkheid, privacywetgeving en civiel overeengekomen geheimhoudingsverplichtingen.[100] Als de introductie van een dergelijk vergaande nieuwe bevoegdheid serieus wordt overwogen, worden hopelijk ook de nodige waarborgen daarbij in overweging genomen.

5.2 Nieuwe toezichthouder voor de politie

Opsporingsonderzoeken leiden niet altijd tot een strafzaak, waarbij de zittingsrechter de rechtmatigheid van het opsporingsproces toetst, inclusief de daaraan voorafgaande en tijdens het onderzoek uitgevoerde gegevensverwerkingen.[101] Hildebrandt schreef hierover in haar preadvies (2016, p. 175):

> 'Het gevolg hiervan is minstens dat allerhande vormen van monitoring en ander onderzoek, al dan niet gebaseerd op data-gestuurde risico-analyses, de rechter niet zullen bereiken en dus door anderen getoetst moeten worden. Juist bij toenemende inzet van politie-*agents* moet in een rechtsstaat de aanvechtbaarheid worden gekoesterd en veilig gesteld van de beslissingen die – grotendeels onder de radar – door (of op basis van) dergelijke systemen worden genomen.'

Hildebrandt (2016), Buruma (2016) en Schermer (2017) zijn opvallend eensgezind over de wenselijkheid van een nieuwe vorm van toezicht die ook nadrukkelijk de rechtmatigheid van de gegevensverwerkingen door de politie onder leiding van het Openbaar Ministerie in

het opsporingsproces toetst.[102]
De Commissie-Koops wijst in het rapport slechts op de rol van de Autoriteit Persoonsgegevens en de Inspectie Justitie en Veiligheid als toezichthouder. Ze geeft daarbij de voorzichtige aanbevelingen mee dat 'de memorie van toelichting aandacht dient te besteden aan het systeem van toezicht op de langere termijn en extern toezicht' en 'de nodige reflectie noodzakelijk is op het stelsel van toezicht op de gegevensvergaring en -verwerking door opsporingsdiensten'.[103] Het gaat hier niet alleen over toetsing van de rechtmatigheid van de bepalingen omtrent gegevensverwerking uit de Wet politiegegevens, maar bij data-analyse met een uitwerking op strafvordering ook over een rechtmatigheidstoets op andere aspecten (in de toekomst mogelijk ook met betrekking tot nieuwe bepalingen over gegevensverwerkingen of de nieuwe bevoegdheid hieromtrent in het Wetboek van Strafvordering).[104]

6 Slotbeschouwing

De Commissie-Koops heeft een waardevolle bijdrage geleverd aan het project Modernisering Strafvordering door verbeteringen voor te stellen met betrekking tot het conceptwetsvoorstel Boek 2. De Commissie heeft een grondige en systematische analyse gedaan van de voorgestelde regelingen en aandacht besteed aan de relevante maatschappelijke ontwikkelingen. De wetgever doet er goed aan alle 72 aanbevelingen uit het rapport serieus mee te nemen in het wetgevingsproces. De nieuwe rol en invulling van 'stelselmatigheid' is bovendien waardevol om de zwaarte van de privacy-inmenging en bijpassende autoriteit in te vullen. Het nieuwe normeringscriterium loopt als een rode draad door het rapport voor de normering van bijzondere opsporingsbevoegdheden, zoals openbronnenonderzoek, het beslag op digitale gegevensdragers, het vorderen van gegevens en onderzoek aan (tele)communicatie.
Toch is het criterium van stelselmatigheid naar mijn mening niet voor alle opsporingshandelingen even geschikt. In sommige gevallen kan bij de normering van opsporingsmethoden beter voor duidelijkheid worden gekozen met een vooraf ingevulde inbreuk op de persoonlijke levenssfeer en bijbehorende autoriteit om het bevel voor de opsporingshandeling te geven. Ik doel daarbij in het bijzonder op het beslag op bepaalde gegevensdragers en de inzet van *scrapers* ten behoeve van de opsporing. De Commissie-Koops gaat in plaats daarvan mee met de ruime normen die in de praktijk zijn ontwikkeld en achteraf door de rechtspraak zijn goedgekeurd of bijgestuurd. Daarbij worden suggesties gedaan voor een zeer genuanceerde invulling van het criterium afhankelijk van de verschillende omstandigheden van het geval, waarbij met tal van factoren rekening moet worden gehouden. Het is echter belangrijk dat ook de maatschappij, bij monde van de wetgever, zich uitspreekt en beslissingen neemt over belangrijke zaken, zoals de wenselijke wettelijke bescherming bij het onderzoek van gegevens in een smartphone en de vraag of *scrapers* op grote schaal (persoons)gegevens mogen verzamelen. Ook geeft een regeling voor opsporingsmethoden zonder stelselmatigheid als normeringscriterium de reikwijdte van een opsporingsbevoegdheid duidelijker aan en biedt daarmee meer rechtszekerheid voor alle betrokkenen in het strafproces.
In dit artikel heb ik opnieuw betoogd dat de zwaarte van de privacy-inmenging bij de

inbeslagname van en het onderzoek op smartphones ernstig is en dat simpelweg kan worden gekozen voor een vereiste machtiging van een rechter-commissaris (behoudens enkele uitzonderingen bij wet). Zeker voor de jongere generaties zijn opsporingshandelingen met betrekking tot smartphones, PC's en laptops, waarbij de bijbehorende gegevens al dan niet in de cloud zijn opgeslagen, zeer privacy-intrusief. Het arrest van de Hoge Raad en het voorstel van de Commissie-Koops houden hier mijns inziens onvoldoende rekening mee en leggen een onduidelijk criterium aan om de ernst van de privacy-inmenging te bepalen. De aanbeveling een wetsvoorstel voor het beslag op gegevensdragers en openbronnenonderzoek al eerder naar de Tweede Kamer te sturen ondersteun ik daarom ten volle. Hopelijk bestaat daarbij ook nog ruimte voor een debat over het alternatief van een eenvoudiger regeling met een duidelijke bevoegde autoriteit voor de inbeslagname en het onderzoek van gegevens op bovengenoemde gegevensdragers en de inzet van *scrapers*.
Daarnaast is de uitwerking over de 'dataficering van de opsporing' en in het bijzonder het gebruik van data-analysetechnieken in het rapport ondermaats gebleven. Een commissie die zich buigt over 'strafvordering in het digitale tijdperk' zou ook hierover uitgebreid moeten adviseren, waarbij kan worden voortgebouwd op adviezen die hier al eerder over zijn gegeven. Het advies had zich moeten richten op concrete suggesties voor strafprocessuele waarborgen bij de verwerking van gegevens binnen het opsporingsproces, inclusief het daaraan gerelateerde vermeende gebrek aan toezicht. In plaats daarvan worden slechts voorzichtige aanbevelingen gedaan en een nieuwe vergaande bevoegdheid voorgesteld om een bevel tot data-analyses bij derden ten behoeve van de opsporing mogelijk te maken. Tegenover al het potentieel dat data-analyse voor de politie biedt, moet voldoende bescherming voor de betrokken burgers staan. Op dit punt is het rapport niet in balans.
Het is echter geenszins mijn bedoeling dit artikel over het rapport van de Commissie-Koops in mineur af te sluiten. De bovenstaande kritiek doet niet af aan de waarde en het belang van de voorstellen van de Commissie. Over het geheel genomen heeft de Commissie-Koops een mooie en waardevolle prestatie geleverd, waar de wetgever – getuige de 72 aanbevelingen gericht op het Wetboek van Strafvordering – concreet mee uit te voeten kan.

Noten

1 Berekend op basis van de 2,49 Ghz processorsnelheid van de Apple A12-chip vergeleken met de 1,024 Mhz chip in de Apollo 11-computer. Daarbij is nog geen rekening gehouden met het aantal kernen (zes) in de A12-chip die tot extra kracht en efficiëntie leiden.

2 Berekend op basis van de 512Gb opslagruimte in de iPhone Xs (uitgebreide optie), vergeleken met de 32kb opslag in de Apollo 11-computer.

3 Volgens Henseler maken smartphones 80 procent van het digitaal bewijs uit in strafzaken: J. Henseler, 'De (R)evolutie van Digitaal Bewijs', lectorale rede 21 november 2017, Hogeschool Leiden, p. 13 (hierna: Henseler 2017).

4 Zie bijvoorbeeld Rb. Rotterdam 16 mei 2017, ECLI:NL:RBROT:2017:4101. De zoekslagen 'met terpentine overgieten', 'oorzaak uitgebrande slaapkamer', 'terpentine brand' en 'man steekt dakloze die aan het slapen is in brand' op de smartphone van de verdachte waren bijvoorbeeld belangrijk in een moordzaak. En zie bijvoorbeeld Rb. Noord-Nederland 9 maart 2017, ECLI:NL:RBNNE:2017:843 en Rb. Midden-Nederland 3 januari 2017, ECLI:NL:RBMNE:2017:93 waarbij een verdachte via WhatsApp prijslijsten van drugs en 'aanbiedingen van de maand' naar zijn clientèle stuurde. Ook speelde de inhoud van Whatsapp-berichten en e-mailberichten op zogenoemde '*Pretty Good Privacy*-telefoons' een belangrijke bewijsrol bij een moordzaak (Rb. Amsterdam 19 april 2018, ECLI:NL:RBAMS:2018:2504).

5 Zie bijvoorbeeld Rb. Zeeland-West-Brabant 28 juni 2016, ECLI:NL:RBZWB:2016:3865 (doodslag in het verkeer) en Rb. Midden-Nederland 17 december 2013, ECLI:NL:RBMNE:2013:7258 (moord), waarbij Bluetooth-gegevens van sensoren langs de weg een belangrijke bewijsrol in strafzaken hebben gespeeld.

6 Zie ook Henseler 2017, p. 48.

7 Zie www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ (laatst geraadpleegd op 25 oktober 2018).

8 'Machine learning' gaat over de ontwikkeling van algoritmen en technieken voor het bouwen van computersystemen die automatisch verbeteren op basis van ervaringsregels. Zie voor een heldere uitleg van machine learning en aanverwante begrippen: L. Colonna, *Legal Implications of Data Mining* (diss. Stockholm University), 2016.

9 De term 'Big Data' wordt op veel verschillende wijzen uitgelegd. Meer algemeen wordt de term gebruikt voor datasets waarvan de omvang groter is dan de capaciteit van reguliere database software waarmee de data kunnen worden ontsloten, opgeslagen, gemanaged en geanalyseerd (McKinsey Global Institute, 'Big Data: The next frontier for innovation, competition and productivity', 2011, p. 1). De WRR geeft geen definitie van Big Data in zijn rapport 'Big Data in een vrije en veilige samenleving' (nr. 94, p. 21 (2016)), maar beschrijft in plaats daarvan de volgende drie hoofdkenmerken van Big Data: (1) Data: het gaat om grote hoeveelheden gestructureerde en ongestructureerde data uit verschillende bronnen; (2) Analyse: de analyse is '*data-driven*', zoekt geautomatiseerd naar correlaties, waarbij de grootste potentie wordt verwacht van '*realtime*' en voorspellende analyses; en (3) Gebruik: de analyses moeten leiden tot '*actionable knowledge*' (ingrepen in de realiteit op basis van bestandsanalyses).

10 'Cloud computing' is het uitbesteden van gegevensbeheer of computerapplicaties aan een dienstverlener, met gedistribueerde opslag en in beginsel zonder regie over de locatie (B.J. Koops e.a., 'Misdaad en opsporing in de wolken', TILT/WODC 2012, p. 18).

11 Commissie modernisering opsporingsonderzoek in het digitale tijdperk, *Regulering van*

opsporingsbevoegdheden in een digitale omgeving, s.l. 2018 (hierna: Commissie-Koops 2018).

12 Zie Commissie-Koops 2018, p. 192-205.

13 *Kamerstukken II* 1996/97, 25403, 3, p. 26-27.

14 Commissie-Koops 2018, p. 38.

15 Commissie-Koops 2018, p. 38.

16 HR 4 april 2017, ECLI:NL:HR:2017:592, *NJ* 2017/230 m.nt. T. Kooijmans, r.o. 3.4.

17 Zie HR 19 december 1995, ECLI:NL:HR:1995:ZD0328, *NJ* 1996, 249 m.nt. Schalken, *Kamerstukken II* 1996/97, 25403, 3, p. 110 en 115 en HR 20 januari 2009, ECLI:NL:HR:2009:BF5603, *NJ* 2009, 225 m.nt. Borgers, HR 13 november 2012, ECLI:NL:HR:2012:BW9338, *NJ* 2013, 413 m.nt. Borgers, HR 1 juli 2014, ECLI:NL:HR:2014:1562, *NJ* 2015/115 m.nt. P.H.P.H.M.C. van Kempen en HR 4 april 2017, ECLI:NL:HR:2017:592, *NJ* 2017/230 m.nt. T. Kooijmans.

18 Zie Commissie-Koops 2018, p. 45-48.

19 Commissie-Koops 2018, p. 136.

20 Commissie-Koops 2018, p. 137.

21 Commissie-Koops 2018, p. 39.

22 Commissie-Koops 2018, p. 39.

23 De Commissie verwijst daarbij naar *United States v. Maynard*, 615 F.3d 544, 558 (D.C.Cir. 2010) en twee '*concurring opinions*' in een zaak van het Amerikaanse Hooggerechtshof: *United States v. Jones*, 565 U.S. 400 (2012), 417-18 (Sotomayor, concurrence), 428-31 (Alito, concurrence).

24 Commissie-Koops 2018, p. 40.

25 Commissie-Koops 2018, p. 42.

26 Zie aanbeveling 6 van de Commissie-Koops 2018, p. 41.

27 Commissie-Koops 2018, p. 33.

28 Commissie-Koops 2018, p. 33.

29 Aanbeveling 9, Commissie-Koops 2018, p. 73.

30 J.J. Oerlemans, *Investigating cybercrime* (diss. Leiden), Amsterdam: Amsterdam University Press 2017, p. 78 (hierna: Oerlemans 2017).

31 Zie bijvoorbeeld het persbericht op politie.nl, 'Sociale media vast onderdeel van politiewerk', 27 maart 2013.

32 Zie bijvoorbeeld Rb. Overijssel 4 oktober 2018, ECLI:NL:RBOVE:2018:3656. De verdachte riep op Facebook op tot een 'Project X 2'-feest met minimaal 50.000 mensen. Hij wilde het 'Project X-feest' dat in 2012 in Haren volledig uit de hand liep nog eens 'dunnetjes overdoen'. Hij maakte zich daarmee volgens de rechtbank schuldig aan het delict opruiing. Zie ook Rb. Rotterdam 13 maart 2018, ECLI:NL:RBROT:2018:5367 waarbij een verdachte werd veroordeeld voor opruiing vanwege het maken en verspreiden – o.a. via YouTube – van filmpjes voor een terroristische organisatie, waarop executies en een 'kill-list' waren te zien. Zie ten slotte ook Rb. Amsterdam 29 mei 2018, ECLI:NL:RBAMS:2018:3934 voor een veroordeling voor opruiing na een uit de hand gelopen 'Zwarte Pietendiscussie' op Facebook.

33 Openbronnenonderzoek ten behoeve van de handhavings- en hulpverleningstaak, bijvoorbeeld bij grote evenementen, is door de Commissie verder niet onderzocht. Wel wordt in aanbeveling 52 het advies meegegeven hier ook een regeling voor te treffen.

34 Commissie-Koops 2018, p. 156. Zie ook Oerlemans 2017, p. 169-170. De Commissie-Koops geeft er, net als ik eerder in mijn proefschrift heb betoogd, de voorkeur aan te spreken over 'publiekelijk toegankelijke bronnen' (aanbeveling 53), omdat dit beter weergeeft 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.

35 Commissie-Koops 2018, p. 155. Zie hierover ook CTIVD-rapport nr. 55 (2018), p. 10.

36 De Commissie-Koops maakt daarbij een vergelijking met de grenzen die door de delictsomschrijving van computervredebreuk worden gesteld (zie aanbeveling 54, p. 154-156).

37 Zie meer uitgebreid over de definitie: Commissie-Koops 2018, p. 152-156.

38 Zie Commissie-Koops 2018, p. 157-158.

39 Zie Commissie-Koops 2018, p. 163-164.

40 Commissie-Koops 2018, p. 166.

41 De Commissie onderkent dit op p. 164. Maar de Commissie kon het naar eigen zeggen niet eenvoudiger maken, omdat het zou 'afdoen aan de veelzijdigheid van beschikbare bronnen op het internet en het anders te grofmazig zou worden'.

42 Commissie-Koops 2018, p. 160-161.

43 In één witwaszaak (Rb. Noord-Holland 10 maart 2017, ECLI:NL:RBNHO:2017:1940) wordt wel opgemerkt dat 'darknet markets zijn veiliggesteld door het darkwebmonitor project'. Dat is mogelijk met een *scraper* en daarbij is teruggezocht op de activiteiten van gebruikers van de handelsplaatsen.

44 Rb. Amsterdam 5 april 2017, ECLI:NL:RBAMS:2017:2123, Rb. Amsterdam 15 februari 2018, ECLI:NL:RBAMS:2018:780 en Rb. Amsterdam 27 juni 2018, ECLI:NL:RBAMS:2018:4442.

45 Zie Rb. Amsterdam 27 juni 2018, ECLI:NL:RBAMS:2018:4442, r.o. 21.

46 MvT conceptwetsvoorstel Boek 2, p. 247.

47 Zie hierover ook Commissie-Koops 2018, p. 175-178. Het data-analysesysteem 'Hansken' van het Nederlands Forensisch Instituut werd overigens ook niet als technisch hulpmiddel beschouwd. Zie Rb. Amsterdam 19 april 2018, ECLI:NL:RBAMS:2018:2504, r.o. 7.3.

48 Zie ook W. Stol & L. Strikwerda, 'Online vergaren van informatie voor opsporingsonderzoek. Een beknopte evaluatie van voorgestelde wetgeving', *Tijdschrift voor Handhaving* 2018, nr. 1-2, p. 17 (hierna: Stol & Strikwerda 2018).

49 Zie ook Commissie-Koops 2018, p. 162 (aanbeveling 58).

50 Zie p. 60 van de toelichting op het conceptwetsvoorstel wijziging Boek 2. Zie ook het handige schema op p. 148 van het rapport van de Commissie-Koops voor het onderscheid in het vergaren van gegevens.

51 Zie ook Oerlemans 2017, p. 143-144.

52 Aanbeveling 62.

53 Zie o.a. F.P.E. Wiemans, *Onderzoek van gegevens in geautomatiseerde werken* (diss. Tilburg), Nijmegen: Wolf Legal Publishers 2004 en meer recent R. van den Bosch, 'Privacy in het digitale tijdperk: over de rechtmatigheid van het onderzoek aan een in beslag genomen smartphone', *TPWS* 2016/48, afl. 17, p. 47-50, E. Gritter, 'Opsporing in de digitale wereld: het onderzoek van in beslag genomen gegevensdragers', *Delikt en Delinkwent* 2016/43, afl. 7, p. 493-503, S. Royer & J.J. Oerlemans, 'Naar een nieuwe regeling voor beslag op gegevensdragers', *Computerrecht* 2017/200, afl. 5, p. 277-284 (hierna: Royer & Oerlemans 2017), E.F. Stamhuis, 'Een ongeschikt concept', *Strafblad* 2017, (50), p. 360-366, F. Vellinga-Schootstra, 'Inbeslagneming van voorwerpen en gegevens', *Rechtsgeleerd Magazijn THEMIS* 2017, afl. 6, p. 334-343 en J.S. Nan, 'Een moderne inbeslagneming van voorwerpen', *Platform Modernisering Strafvordering* 2018-1.

54 De Commissie-Koops (2018, p. 82-83) adviseert in aansluiting op het betoog van Stamhuis (2017) en Vellinga-Schootstra (2017) de overkoepelende regeling voor 'beslag op gegevens' los te laten en grotendeels aan te sluiten bij de bestaande regelingen voor het verkrijgen van opgeslagen gegevens in strafvordering.

55 Zie paragraaf 5.2 van het rapport van de Commissie-Koops.

56 De aanbevelingen met betrekking tot de klachtregeling en teruggave van gegevensdragers worden in dit artikel dus niet behandeld. Zie hierover p. 55-59 van het rapport van de Commissie-Koops.

57 U.S. Supreme Court, 25 juni 2014, *Riley v. California*, 573 U.S. (2014). Voor deze zaak werd in het Amerikaanse strafprocesrecht al aangenomen dat over het algemeen een warrant is vereist voor de inbeslagname en kennisname van opgeslagen gegevens op computers. Zie O.S. Kerr, *Computer Crime Law*, 2nd edition, American Casebook Series, West Academic Publishing 2010, p. 309.

58 HR 4 april 2017, ECLI:NL:HR:2017:584, 588 en 592, *Ars Aequi* 2017/9, p. 730-735 m.nt. L. Stevens, r.o. 3.4.

59 Commissie-Koops 2018, p. 86.

60 Commissie-Koops 2018, p. 87-88.

61 Commissie-Koops 2018, p. 44.

62 Commissie-Koops 2018, p. 45-48.

63 Commissie-Koops 2018, p. 47.

64 Commissie-Koops 2018, p. 76-79.

65 Zie Commissie-Koops 2018, p. 76-79 en p. 84-86.

66 Royer & Oerlemans 2017, p. 279.

67 M.D. Ricciuti & K.D. Parker, 'My Phone Is My Castle: Supreme Court Decides that Cell Phones Seized Incident to Arrest Cannot Be Subject to Routine Warrantless Searches', *Boston Bar Journal* 2014, nr. 4.

68 Zie HR 10 juli 2018, ECLI:NL:HR:2018:1121 en Hof Arnhem-Leeuwarden 14 juli 2017, ECLI:NL:GHARL:2017:6069.

69 Royer & Oerlemans 2017, p. 280.

70 Zie in deze zin wel Commissie-Koops 2018, p. 136 waarin wordt aangegeven dat een deel

van de leden het van toepassing verklaren van het criterium van stelselmatigheid bij het onderzoek aan meer persoonsgebonden computers (zoals pc's, laptops, smartphones en tablets) niet wenselijk vindt.

71 A.A. Hilberink & M. van Delden, 'De forensische kant van digitaal onderzoek', *Strafblad* 2017/4.

72 Commissie-Koops 2018, p. 94. De wetgever zou dan in de MvT duidelijk moeten maken wat een 'actieve rol behelst'.

73 *Kamerstukken II* 1989/90, 21551, 3, p. 27. De hackbevoegdheid in art. 126nba Sv heeft deze plek nu van de netwerkzoeking overgenomen, aangezien de hackbevoegdheid op heimelijke wijze wordt toegepast en na een hack nog andere opsporingshandelingen kunnen plaatsvinden, naast het overnemen van relevante gegevens.

74 Zie art. 125j Sv.

75 Zie de MvT op het conceptwetsvoorstel Boek 2, p. 203. Technisch gezien wordt toegang verschaft tot de server waar e-mailberichten van een verdachte liggen opgeslagen.

76 Commissie-Koops 2018, p. 109.

77 Commissie-Koops 2018, p. 111.

78 Commissie-Koops 2018, p. 116.

79 Commissie-Koops 2018, aanbeveling 31-33. De commissie doet in totaal negen aanbevelingen in het kader van de netwerkzoeking, waarvan een volledige bespreking buiten het bestek van dit artikel valt.

80 Commissie-Koops 2018, p. 112.

81 Commissie-Koops 2018, p. 116. De nieuwe hackbevoegdheid uit art. 126nba Sv maakt het op afstand binnendringen in *elk* geautomatiseerd werk mogelijk, dus ook in geautomatiseerde werken waar de verdachte niet rechtmatig toegang toe heeft. Deze bevoegdheid is ook niet beperkt tot opgeslagen gegevens in een geautomatiseerd werk. Zie over de hackbevoegdheid ook J.J. Oerlemans, 'Wet computercriminaliteit III: meer handhaving op internet', *Strafblad* 2017, afl. 15, p. 350-359.

82 Zie Commissie-Koops 2018, p. 93-94.

83 De wenselijkheid van de waarborg van het vereiste van een machtiging van een rechter-commissaris heb ik uiteengezet in mijn dissertatie met verwijzing naar de ernstige privacyinmenging in de zin van art. 8 EVRM (Oerlemans 2017, p. 276-278).

84 Commissie-Koops 2018, p. 117 en aanbeveling 39.

85 Zie ook P.A.M. Mevis, J.H.J. Verbaan & B.A. Salverda, 'Onderzoek aan in beslag genomen elektronische gegevensdragers en geautomatiseerde werken ten behoeve van de opsporing en vervolging van strafbare feiten', Erasmus/WODC 2016.

86 Overigens lijkt een 4-cijferige pincode nog eenvoudig te kraken, maar een sterk wachtwoord niet. Zie P. Rosenzweig, 'iPhones, the FBI, and Going Dark', lawfareblog, 4 augustus 2015. Beschikbaar op: https://www.lawfareblog.com/iphones-fbi-and-going-dark (laatst geraadpleegd op 25 oktober 2018).

87 Zie de Kamerbrief van 4 januari 2016 (*Kamerstukken II* 2015/16, 26643, 383). Zie hierover uitgebreid B.J. Koops, *Het decryptiebevel en het nemo-teneturbeginsel. Nopen ontwikkelingen sinds 2000 tot invoering van een ontsleutelplicht voor verdachten?*, WODC 2012, nr. 305, Den Haag: Boom Lemma uitgevers 2012.

88 Zie EHRM 17 december 1996, nr. 9187/91 (*Saunders t. Verenigd Koninkrijk*), par. 69. Zie ook D.A.G. van Toor, 'De vergrendelde smartphone als object van strafvorderlijk onderzoek', *Computerrecht* 2017/2, afl. 1, p. 3-11 (hierna: Van Toor 2017).

89 Commissie-Koops 2018, p. 105.

90 Commissie-Koops 2018, p. 106.

91 Aanbeveling 28, p. 107. In deze paragraaf worden niet alle aanbevelingen omtrent dit onderwerp besproken. Zie daarvoor aanbeveling 27-30 in par. 5.3.2.

92 A. Bood, 'Geef ze een vinger … Gedwongen ontgrendeling van een smartphone en het nemo tenetur-beginsel', *NJB* 2018/1880, afl. 36, p. 2744-2748.

93 Commissie-Koops 2018, p. 28 (aanbeveling 3).

94 M. Hildebrandt, 'Data-gestuurde intelligentie in het strafrecht', in: E.M.L. Moerel, J.E.J. Prins, M. Hildebrandt, T.F.E Tjong Tjin Tai, G-J. Zwenne & A.H.J. Schmidt, *Homo Digitalis*, Handelingen 146e NJV vergadering 2016, Deventer: Kluwer 2016, p. 137-240 (hierna: Hildebrandt 2016). Zie ook de kritische bespreking van het preadvies door Y. Buruma, 'De criminele homo digitalis', *NJB* 2016/1073, afl. 22, p. 1534-1541 (hierna: Buruma 2016). Eerder, in 2007, schreef Schermer een proefschrift over (software) agents en het strafrecht: B.W. Schermer, *Software Agents, Surveillance, and the Right to Privacy: a Legislative Framework for Agent-enabled Surveillance* (diss. Leiden), Leiden: Leiden University Press 2007.

95 A. Das & M.B. Schuilenburg, 'Predictive policing: waarom bestrijding van criminaliteit op basis van algoritmen vraagt om aanpassing van het strafprocesrecht', *Strafblad* 2018/4, p. 19-26, op p. 21 (hierna: Das & Schuilenburg 2018).

96 Das & Schuilenburg 2018, p. 24. Zie in dit kader ook Hildebrandt 2016, p. 172-175 en p.

193-194.

97 Zie eerder in dit kader ook Schermer 2007, p. 211. Interessant is daarbij ook de overweging van A-G Knigge over de opsporing van strafbare feiten op basis van gegevens afkomstig uit 'Automatic Number Plate Recognition' (ANPR). Hij overweegt dat 'wel opmerking verdient dat de Wpg niet de meest aangewezen plaats is om de uitvoering van de politietaak te normeren, zeker niet voor zover het daarbij gaat om de opsporing van strafbare feiten. Daarvoor hebben we het Wetboek van Strafvordering' (HR 9 september 2014, ECLI:NL:PHR:2014:1963, concl. A-G Knigge, punt 4.7).

98 Zie bijvoorbeeld ook Hildebrandt 2016 en B.W. Schermer, 'Het gebruik van Big Data voor opsporingsdoeleinden: tussen Strafvordering en Wet politiegegevens', *Tijdschrift voor Bijzonder Strafrecht & Handhaving* 2017, nr. 4, p. 207-216.

99 Commissie-Koops 2018, p. 183-187 (aanbeveling 70).

100 Commissie-Koops 2018, p. 180.

101 De noodzaak van voldoende toezicht hangt samen met de tendens dat ook de verstoring van de criminaliteit een prominentere plek krijgt, naast het vergaren van bewijs teneinde een persoon bij schuld een passende straf op te leggen. De Commissie-Koops (2018, p. 24) stipt deze tendens en de gevolgen ervan voor toezicht slechts kort aan.

102 Buruma en Schermer pleiten daarbij voor een Commissie van Toezicht voor de Politie, vergelijkbaar met de Commissie van Toezicht voor de Inlichtingen- en Veiligheidsdiensten.

103 Commissie-Koops 2018, p. 31 en 62 (aanbevelingen 5 en 11). Zie over het vermeende gebrek aan toezicht ook M. Samadi, 'Het toezicht op de strafvorderlijke overheid: een modern artikel 359a Sv?', *Platform Modernisering Strafvordering* 2018-6 en E. Devroe, M. Malsch, J. Matthys & G. Minderman, *Toezicht op strafvorderlijk overheidsoptreden*, Den Haag: WODC 2017.

104 A-G Knigge merkte in zijn conclusie (HR 9 september 2014, ECLI:NL:PHR:2014:1963, concl. A-G Knigge, punt 4.7) over het gebruik van gegevens van ANPR-camera's voor de opsporing op dat het CBP (nu de Autoriteit Persoonsgegevens) 'niet de eerst aangewezen instantie is om te beoordelen of een bepaalde opsporingsmethode voldoet aan de eisen van proportionaliteit'.

Trefwoorden: **digitale opsporing, openbronnenonderzoek, beslag, data-analyse, big data**