

*Onderzoek aan in beslag genomen
elektronische gegevensdragers en
geautomatiseerde werken ten behoeve van
de opsporing en vervolging van strafbare
feiten*

P.A.M. Mevis

J.H.J. Verbaan

B.A. Salverda



Voorwoord

In opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum van het Ministerie van Veiligheid en Justitie is onderzoek verricht naar de huidige opsporingspraktijk omtrent de inbeslagneming van, en het daaropvolgende onderzoek dat wordt gedaan aan elektronische gegevensdragers en geautomatiseerde werken door opsporingsambtenaren.

In het bijzonder wordt met het onderhavige onderzoek geprobeerd inzicht te verschaffen in het juridisch kader alsmede de bestaande opsporingspraktijk voor zover die betrekking heeft op het onderzoek aan in beslag genomen elektronische gegevensdragers en geautomatiseerde werken. Het onderzoek wordt verricht ten behoeve van een eventuele nadere normering van dergelijk opsporingsonderzoek in het kader van de modernisering van het Wetboek van Strafvordering.

Het betreft een onderzoek dat bestaat uit zowel kwantitatieve als kwalitatieve onderzoeksaspecten.

Het onderzoek is verricht onder leiding en verantwoordelijkheid van prof. mr. P.A.M. Mevis, hoogleraar strafrecht en strafprocesrecht aan de Erasmus Universiteit Rotterdam. De feitelijke onderzoekswerkzaamheden zijn verricht door prof. mr. P.A.M. Mevis, mr. J.H.J. Verbaan (wetenschappelijk medewerker) en mw. mr. B.A. Salverda (wetenschappelijk medewerker).

Het onderzoek is begeleid door een vanwege de opdrachtgever ingestelde begeleidingscommissie onder voorzitterschap van prof. mr. J.H. Crijns, hoogleraar straf- en strafprocesrecht aan de Universiteit Leiden. (De samenstelling van de commissie is in de bijlage opgenomen).

De onderzoeksleiding heeft acht maal vergaderd met de begeleidingscommissie. De onderzoekers spreken jégens de leden van de begeleidingscommissie graag hun dank uit voor hun input in wetenschappelijke en praktische zin en voor de constructieve samenwerking die het uitvoeren van dit onderzoek mede mogelijk maakte.

Tevens danken de onderzoekers de respondenten voor hun nuttige bijdrage aan het onderzoek.

Het onderzoek is in februari 2016 afgesloten.

Inhoudsopgave

Voorwoord.....	3
1. Inleiding.....	6
1.1 Aanleiding voor het onderzoek.....	6
1.2 Probleemstelling en onderzoeksvragen	8
1.3 Afbakening	10
1.4 Uitvoering	11
1.5 Onderzoeksopzet en methodologie	12
1.6 Leeswijzer	13
2. Juridisch kader.....	14
2.1 Inleiding	14
2.2 Verschillende wijzen van het verkrijgen van gegevens ten behoeve van de opsporing	14
2.3 Inbeslagneming van voorwerpen.....	16
2.4 Teruggave van het in beslag genomen voorwerp aan de beslagene	22
2.5 Onderzoek aan in beslag genomen voorwerpen	24
2.6 Doorzoeken van plaatsen ter vastlegging van gegevens	27
2.6.1 Ontsluitingsbevel	30
2.6.2 Gegevens waarover het professioneel verschoningsrecht zich uitstrekt.....	30
2.6.3 Gegevens bij de aanbieder van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst	30
2.6.4 Bewaren en vernietigen van gegevens die tijdens een doorzoeking van een plaats ter vastlegging van gegevens zijn vergaard	31
2.7 Wet bescherming persoonsgegevens en Wet politiegegevens	32
2.8 Het Europees Verdrag voor de Rechten van de Mens	33
2.9 Grondwettelijke bescherming	38
2.10 Recente ontwikkelingen in verband met nader onderzoek aan in beslag genomen elektronische gegevensdragers of geautomatiseerde werken	39
3. Uitwerking en analyse van het onderzoek	45

3.1 Inleiding	45
3.2 Kwantitatieve onderzoeksvragen	45
3.2.1 Cijfers over de praktijk van inbeslagneming	46
3.3 Kwalitatieve onderzoeksvragen	51
3.3.1 Autoriteit en gronden	51
3.3.2 Kopiëren van gegevens.....	57
3.3.3 Bewaring van gekopieerde gegevens.....	59
3.3.4 Gegevens waarover het professioneel verschoningsrecht zich uitstrekt.....	61
3.3.5 Gegevens die elders zijn opgeslagen in de cloud of in een netwerk.....	63
3.3.6 Teruggave van elektronische gegevensdragers en geautomatiseerde werken na afronding van het onderzoek	64
3.3.7 Onderzoek aan geautomatiseerde werken zonder formele inbeslagneming	65
3.3.8 Het wissen van bestanden alvorens de gegevensdrager wordt teruggegeven	66
4. Conclusies en observaties.....	69
4.1 Inleiding	69
4.2 Kwantitatieve onderzoeksvragen: cijfers over inbeslagneming, onderzoek en het wissen van gegevens.....	69
4.3 Kwalitatieve onderzoeksvragen: inbeslagneming, onderzoek en gegevensverwerking door opsporingsinstanties	70
4.4 Algemene conclusie	77
Samenvatting.....	80
Summary	84
Literatuurlijst.....	88
Lijst met aangehaalde zaken	90
Bijlage: de begeleidingscommissie	92

1. Inleiding

1.1 Aanleiding voor het onderzoek

Elektronische gegevensdragers (externe harde schijf, usb-stick, geheugenkaart) en geautomatiseerde werken (tablet, laptop, mobiele telefoon, computer, navigatieapparatuur, etc.) zijn een belangrijke bron van informatie voor de opsporing van strafbare feiten.¹ Het gebruik van elektronische gegevensdragers en geautomatiseerde werken is in korte tijd aanzienlijk toegenomen. Technologische ontwikkelingen brengen mee dat steeds grotere hoeveelheden gegevens op eenvoudige wijze (kunnen) worden opgeslagen. Het onderzoek aan bijvoorbeeld een moderne smartphone kan tegenwoordig niet alleen inzicht verschaffen in het telefooncontact dat de betrokkene heeft gehad, maar ook in zijn contactenlijst, de inhoud van communicatie, zijn agenda en de locaties waar de telefoon zich heeft bevonden. In dat licht kan met het onderzoek van daarop vastgelegde gegevens een verregaande inbreuk op de persoonlijke levenssfeer van de betrokkene worden gemaakt. Het belang van bescherming van privéleven kan dan ook niet onbesproken blijven. Ook in het kader van de strafvordering, meer in het bijzonder de opsporing, spelen deze onderwerpen een belangrijke rol.

In de opsporingspraktijk worden dagelijks voorwerpen waarop gegevens zijn opgeslagen, in beslag genomen. Het is vaste jurisprudentie² dat de bevoegdheid om voorwerpen ten behoeve van de waarheidsvinding in beslag te nemen de bevoegdheid omvat om aan in beslag genomen voorwerpen onderzoek te doen. Zulks met inbegrip van in beslag genomen elektronische gegevensdragers of geautomatiseerde werken; ten behoeve van de waarheidsvinding mag (ook) aan in beslag genomen voorwerpen onderzoek worden verricht indien het elektronische gegevensdragers en geautomatiseerde werken betreft.³ Binnen de opsporingspraktijk worden daarin opgeslagen gegevens dan ook onderzocht met de intentie die opgeslagen gegevens (als bewijsmateriaal) te gebruiken in het kader van de waarheidsvinding. De inbeslagneming van elektronische gegevensdragers en geautomatiseerde werken geschiedt meestal niet met het oogmerk de beschikking te krijgen over het desbetreffende voorwerp, als wel om de daarop opgeslagen gegevens te onderzoeken en - indien nodig - veilig te stellen. Daarmee is de inbeslagneming te beschouwen als steunbevoegdheid voor het onderzoek van een elektronische gegevensdrager of in een geautomatiseerd werk en eventueel het veiligstellen van daarin of

¹ Daar waar in dit rapport gesproken wordt van ‘gegevensdragers’ wordt bedoeld ‘elektronische gegevensdragers en geautomatiseerde werken’.

² Zie o.a. HR 20 februari 2007, ECLI:NL:HR:2007:AZ3564, NJ 2008, 113, m.nt. T.M. Schalken onder NJ 2008, 115; HR 8 mei 2001, ECLI:NL:HR:2001:AB1517, NJ 2001, 479 en HR 29 maart 1994, ECLI:NL:HR:1994:AD2076, NJ 1994, 537, m.nt. T.M. Schalken onder NJ 1994, 577.

³ G.J.M. Corstens & M.J. Borgers, *Het Nederlands strafprocesrecht*, Deventer: Wolters Kluwer, 2014, p. 541, HR 29 maart 1994, ECLI:NL:HR:1994:AD2076, NJ 1994, 537, m.nt. T.M. Schalken onder NJ 1994, 577 en HR 8 mei 2001, ECLI:NL:HR:2001:AB1517, NJ 2001, 479.

daarop opgeslagen gegevens. Het in beslag nemen van dergelijke voorwerpen geschiedt met toepassing van de gewone inbeslagnemingsbevoegdheden. Omdat vervolgens onderzoek kan en mag worden gedaan aan de in beslag genomen elektronische gegevensdragers en geautomatiseerde werken, mag in beginsel zonder enige begrenzing kennis worden genomen van alle gegevens die op de betreffende gegevensdragers en werken zijn verwerkt. Een opsporingsambtenaar tot inbeslagneming bevoegd, mag daarmee zonder toestemming of machtiging van de officier van justitie of de rechter-commissaris onderzoek doen aan door hem in beslag genomen elektronische gegevensdragers en in geautomatiseerde werken, kennis nemen van de daarop opgeslagen gegevens en deze kopiëren of vastleggen ten behoeve van het opsporingsonderzoek. (Daarbij moet wel worden bedacht dat inbeslagneming vaak tijdens het doorzoeken ter inbeslagneming plaatsvindt; de opsporingsambtenaar, niet zijnde (hulp)officier van justitie en zelfs de (hulp)officieren van justitie zijn maar beperkt bevoegd tot zodanig doorzoeken). De wetgeving bevat nauwelijks regels over deze wijze van vergaren, verzamelen en vastleggen van gegevens. De bestaande regelgeving heeft hoofdzakelijk betrekking op het in beslag nemen van de voorwerpen zelf. De normering is daardoor verbonden met de inbeslagneming en niet met het daarop volgend onderzoek van de daarin opgenomen gegevens.

Tegelijkertijd bestaat ten aanzien van het vorderen van gegevens, waarbij een inbreuk op de persoonlijke levenssfeer wordt gemaakt, wel een strikte normering in specifieke wettelijke bepalingen. De normering in die regeling is – anders dan bij de inbeslagneming – deels gebaseerd op de aard van de gegevens die gevorderd worden. De ‘ruimte’ in regeling en normering met betrekking tot het onderzoek aan in beslag genomen voorwerpen waarop gegevens zijn opgeslagen enerzijds en de regulering van het vorderen van gegevens anderzijds lijken zich aldus niet goed met elkaar te verhouden.

Het Wetboek van Strafvordering bevat verder een aantal nadere regelingen die betrekking hebben op het vastleggen van op een elektronische gegevensdrager of in een geautomatiseerd werk opgeslagen gegevens, zoals de regeling omtrent de ontsleuteling, de bescherming van het professioneel verschoningsrecht, de bescherming van vertrouwelijke elektronische communicatie, de notificatie, het bewaren en vernietigen van niet-relevante gegevens en het ontoegankelijk maken van gegevens met betrekking tot welke of met behulp waarvan het strafbare feit is gepleegd.⁴ Maar al deze bepalingen zijn beperkt tot de situatie dat tijdens een doorzoeking van een plaats onderzoek wordt gedaan naar gegevens, die zijn opgeslagen op een elektronische gegevensdrager of in een geautomatiseerd werk.⁵ De gehele zevende afdeling van Titel IV van Boek 1 Sv is van toepassing op de vastlegging van gegevens gedurende de doorzoeking en daarmee tot die situatie van doorzoeking beperkt. Deze regelingen zijn daarmee niet van toepassing indien het onderzoek plaatsvindt

⁴ Zie artikel 125k Sv, artikel 125l Sv, artikel 125la Sv, artikel 125m Sv, artikel 125n Sv en artikel 125o Sv.

⁵ Artikel 125i Sv.

en de gegevens worden vastgelegd op bijvoorbeeld het politiebureau na inbeslagneming (buiten doorzoeking) van de gegevensdrager of het geautomatiseerde werk.

Ten aanzien van de inbeslagneming van elektronische gegevensdragers en geautomatiseerde werken zijn niet alle onderwerpen gedetailleerd in het Wetboek van Strafvordering geregeld. Soms is sprake van nadere invulling door lagere regelgeving, door middel van een aanwijzing of instructie, maar dat is niet in alle gevallen zo. De bevoegdheid tot het onderzoeken van in beslag genomen voorwerpen is niet separaat voorzien in het Wetboek van Strafvordering maar ligt als gezegd volgens de rechtspraak in de bevoegdheid tot inbeslagneming besloten. Ook blijkt de rechtspraak bestaat onduidelijkheid over de precieze voorwaarden voor, en grenzen aan de toepassing van (onderdelen van) diverse bevoegdheden.

Bij deze stand van zaken is, onder meer, inzicht in de huidige opsporingspraktijk wenselijk. Met het onderhavige onderzoek wordt geprobeerd inzicht te verschaffen in de bestaande opsporingspraktijk. Daarmee wordt beoogd bij te dragen aan de uitwerking van het in de Contourennota over de modernisering van het Wetboek van Strafvordering aangekondigde voornemen tot nadere normering van het onderzoek aan in beslag genomen elektronische gegevensdragers en geautomatiseerde werken.⁶ De focus van het onderhavige onderzoek ligt primair op een inventarisatie van het geldende juridisch kader en een beschrijving van de huidige praktijk, in het bijzonder die in de fase van het opsporingsonderzoek, ten aanzien van de inbeslagneming van elektronische gegevensdragers en geautomatiseerde werken en het onderzoek naar en gebruik van de gegevens die daarop zijn opgeslagen.

1.2 Probleemstelling en onderzoeksvragen

Naar aanleiding van het bovenstaande heeft de opdrachtgever de volgende probleemstelling voorgelegd:

Wat is er bekend over de inbeslagneming van en het daaropvolgende onderzoek dat wordt gedaan aan elektronische gegevensdragers en in geautomatiseerde werken door opsporingsambtenaren?

Bovenstaande algemene vraagstelling is uitgewerkt in een aantal onderzoeksvragen. Het gaat daarbij vooral om een analyse van het juridisch kader alsmede de inbeslagnemingspraktijk en het daaropvolgende onderzoek dat aan elektronische gegevensdragers en in geautomatiseerde werken wordt verricht door opsporingsambtenaren. De onderzoeksvragen zijn opgedeeld in een tweetal blokken.

⁶ *Kamerstukken II 2015/16*, 29 279, nr. 278, p. 63.

Allereerst een blok dat zich richt op de kwantitatieve onderzoeksvragen welke met name betrekking hebben op cijfers over het onderzoek, de inbeslagneming en het wissen van gegevens. Het tweede blok besteedt aandacht aan de kwalitatieve onderzoeksvragen waarbij het accent ligt op de gegevensverwerking door opsporingsambtenaren.

I. Kwantitatieve onderzoeksvragen

- A) Zijn er cijfers bekend over hoe vaak een opsporingsambtenaar een mobiele telefoon, laptop, computer, usb-stick etc. in beslag neemt (i) op grond van een zelfstandige inbeslagnemingsbevoegdheid (zoals artikelen 95, 96, 96a en 96b Sv) en (ii) tijdens een doorzoeking van een plaats door een officier van justitie (artikel 96c Sv) of door een rechter-commissaris (artikel 110 Sv)? Zo ja, wat zeggen deze cijfers?
- B) Zijn er cijfers bekend over hoe vaak een opsporingsambtenaar onderzoek verricht aan een smartphone, computer etc. zonder dat deze in beslag wordt genomen?
- C) Zijn er cijfers bekend over hoe vaak bestanden van een smartphone, computer etc. worden gewist voordat deze worden teruggegeven aan de beslagene?

II. Kwalitatieve onderzoeksvragen

- 1. Wie beslist dat aan de in beslag genomen gegevensdragers of het in beslag genomen geautomatiseerde werk onderzoek mag worden gedaan en dat de daarop of daarin opgeslagen gegevens mogen worden vastgelegd?
- 2. Worden gegevens gekopieerd voor verder onderzoek? Zo ja, alle gegevens ('image' maken) of alleen een deel daarvan? In geval van een deel, waarom een/dat deel en niet alle gegevens?
- 3. Wat wordt gedaan met de gekopieerde gegevens? Hoe en hoe lang worden ze bewaard?
- 4. Wat wordt er gedaan als opsporingsinstanties gegevens van een geheimhouder (professioneel verschoningsgerechtigde) tegenkomen?
- 5. Wordt er ook gekeken naar gegevens die via de in beslag genomen smartphone, computer of tablet toegankelijk zijn en zijn opgeslagen in de cloud (denk aan Gmail, Dropbox, Picasa etc.)? Zo ja, worden deze gegevens ook gekopieerd/vastgelegd?
- 6. Wat gebeurt er met de gegevensdragers / het geautomatiseerde werk indien het onderzoek daaraan is afgerond (teruggeven aan beslagene, deponeren bij Domeinen Roerende Zaken, anders)? Indien beslag wordt voortgezet, op welke grond?
- 7. Komt het voor dat door een opsporingsambtenaar onderzoek wordt verricht aan een smartphone, computer etc. zonder dat deze in beslag wordt genomen?

Zo ja, wordt van dergelijk onderzoek proces-verbaal gemaakt? Worden bij dergelijk onderzoek door de opsporingsambtenaar ook gegevens vastgelegd (gekopieerd) ten behoeve van de opsporing?

8. Komt het voor dat bestanden van een smartphone, computer etc. worden gewist voordat deze worden teruggegeven aan de beslagene? Als bestanden worden gewist, wie beslist daarover? Worden alle bestanden gewist of alleen de in de ogen van de opsporingsambtenaar ‘illegale content’? Wordt de verdachte daarvan in kennis gesteld?

1.3 Afbakening

Het onderhavige onderzoek omvat een studie naar de uitvoering in de praktijk omtrent inbeslagneming. Het onderzoek omvat zowel juridische als empirische componenten. De uitvoering van een dergelijk onderzoek is logischerwijs niet mogelijk zonder de nodige afbakeningen.

Die afbakening is vorm gegeven middels de definiëring van de volgende begrippen:

<i>Elektronische gegevensdrager</i>	Voorwerpen die louter bedoeld zijn om gegevens op te slaan, maar waarvoor andere apparatuur nodig is om die gegevens ook daadwerkelijk te kunnen waarnemen. Hierbij kan worden gedacht aan: een usb-stick, een externe harde schijf, een SD-kaart etc.
<i>Geautomatiseerd werk</i>	Apparatuur die 'zelfstandig' gegevens kan opslaan, verwerken en overdragen. Hierbij kan worden gedacht aan: een laptop, een tablet, een smartphone, een computer, maar ook aan een slimme thermostaat en andere huishoudelijke apparaten etc., voor zover deze apparaten gegevens opslaan.

De omschrijving van geautomatiseerd werk wijkt in letterlijke zin af van de definitie zoals die is neergelegd in artikel 80sexies Wetboek van Strafrecht.⁷ De omschrijving die in het kader van dit onderzoek is gehanteerd is enigszins aangepast ten opzichte van artikel 80sexies Sr om verwarring bij de respondenten ten aanzien van geautomatiseerde werken te voorkomen. Die bepaling spreekt namelijk over ‘inrichting die bestemd is om’, met het oog op de praktijk is gekozen voor de meer gebruikelijke term ‘apparatuur’. Waar aangewezen worden in het rapport andere begrippen op de betreffende plaats in een voetnoot gedefinieerd.

⁷ Artikel 80sexies Sr luidt: Onder geautomatiseerd werk wordt verstaan een inrichting die bestemd is om langs elektronische weg gegevens op te slaan, te verwerken en over te dragen.

Ten aanzien van de kwalitatieve vragen moet worden geconstateerd dat het aantal afgenomen interviews voor de beantwoording van de onderzoeksvraag niet groot is. Binnen de – ook qua tijd en middelen – begrensde opdracht, kon maar een beperkt aantal interviews worden afgenomen. Om die reden moesten keuzes gemaakt worden en is in overleg met de begeleidingscommissie een selectie gemaakt op functioneel niveau binnen de politie-eenheden. Bij de bijzondere opsporingsdienst is geen onderscheid gemaakt naar het functionele niveau.

Met de intentie om een meer volledig, representatief en betrouwbaar beeld van de praktijk te schetsen is getracht om spreiding over de politieregio's in acht te nemen. De nationale politie en het Openbaar Ministerie hebben toestemming verleend voor het onderzoek. Er zijn 22 opsporingsambtenaren in verschillende rangen en functies, verspreid over de politieregio's geïnterviewd. Daartoe behoren de afdelingen digitale opsporing van de regionale eenheden Amsterdam en Haaglanden. Ook zijn digitale rechercheurs en wijkagenten uit die politieregio's geïnterviewd, tevens zijn politieambtenaren van de Dienst Landelijke Recherche van de landelijke eenheid geïnterviewd. Verder zijn er interviews afgenomen met officieren van justitie van zowel het Landelijk Parket als arrondissementsparketten. Daarnaast is er ook een bezoek gebracht aan het Nederlands Forensisch Instituut (hierna: NFI). Tijdens dit bezoek hebben de onderzoekers inzicht kunnen verkrijgen in diverse werkprocessen ten aanzien van het doen van onderzoek aan in beslag genomen voorwerpen. Bovendien is gesproken over diverse aspecten die raken aan de werkzaamheden die worden verricht door het NFI, zoals het doen van destructief onderzoek⁸, ontsleuteling, als ook de omvang van het aantal in beslag genomen voorwerpen en de verschillende soorten gegevensdragers waaraan onderzoek wordt verricht. Tot slot zijn ook opsporingsambtenaren van de FIOD en een medewerker van de Koninklijke marechaussee geïnterviewd. Bij de bijzondere opsporingsdiensten, zoals de FIOD, geldt een afwijkende praktijk ten opzichte van de reguliere opsporing bestaan met betrekking tot onder andere het besluit wel of niet tot inbeslagneming van gegevensdragers over te gaan. Ditzelfde geldt voor de Koninklijke marechaussee.

De resultaten van de interviews geven een breed beeld van wat er in de dagelijkse praktijk zoal voorkomt, zonder de pretentie dat dit beeld volledig representatief is.

1.4 Uitvoering

Het onderzoek is in de eerste plaats uitgevoerd door na te gaan of in de data- en bedrijfsprocesssystemen van de politie gegevens bewaard worden die antwoord op de kwantitatieve onderzoeksvragen kunnen geven. De datasystemen van de politie bleken

⁸ Met destructief onderzoek wordt bedoeld het onderzoek aan een voorwerp waarbij onherstelbare beschadigingen aan het voorwerp worden aangebracht. Dergelijk onderzoek kan soms nodig zijn als het niet mogelijk is om toegang te krijgen tot het geautomatiseerde werk.

slechts beperkt inzicht te kunnen verschaffen. Ten behoeve van de beantwoording van de kwalitatieve onderzoeksvragen is eerst een verzameling gemaakt van de wettelijke regelingen, achterliggende literatuur en jurisprudentie. Op grond daarvan zijn vervolgens vragenlijsten opgesteld ten behoeve van interviews binnen de politieorganisatie.

1.5 Onderzoekopzet en methodologie

In dit onderzoek is gebruik gemaakt van verschillende methoden van onderzoek.

Ten aanzien van de kwantitatieve onderzoeksvragen is onderzocht of in de data- en bedrijfsprocessystemen van de politie gegevens worden bewaard die antwoord kunnen geven op deze vragen. Daarvoor is contact opgenomen met de Dienst Landelijke Recherche en de afdeling Digitale Opsporing van verscheidene regionale eenheden binnen de nationale politie. Bij het Bureau Managementinformatie (BMI, onderdeel van de nationale politie) is de vraag uitgezet naar het aantal malen dat de bevoegdheid tot inbeslagneming is toegepast op telefoons en computers en de daarbij in beslag genomen hoeveelheden telefoons en computers. De landelijke cijfers van de jaren 2012, 2013 en 2014 zijn door het BMI aangeleverd en worden door de onderzoekers in hoofdstuk 3 weergegeven. Bij het waarderen van deze cijfers dient een belangrijk voorbehoud te worden gemaakt met betrekking tot de volledigheid daarvan. Dit is deels omdat verschillende registratiesystemen worden gehanteerd (onder andere BVH, Summ-IT⁹) en deels omdat feitelijke registratie niet in alle gevallen lijkt plaats te vinden. Bij de registratie van de in beslag genomen voorwerpen in de kennisgeving van inbeslagneming worden dezelfde soort voorwerpen niet altijd op eenzelfde wijze omschreven. Uit de opgemaakte kennisgevingen van inbeslagneming kunnen dan ook niet op eenvoudige wijze de exacte cijfers geaggregeerd worden.

Ten aanzien van de kwalitatieve vragen zijn eerst de wettelijke regelingen, achterliggende literatuur en jurisprudentie verzameld en geanalyseerd. Vervolgens is, onder meer, op grond van die analyse gewerkt met het afnemen van interviews binnen de politieorganisatie om een zo goed als mogelijk antwoord te geven op de kwalitatieve onderzoeksvragen. Door de onderzoekers is een vragenlijst voor de af te nemen interviews opgesteld. De vragen zijn geformuleerd in overleg met de begeleidingscommissie. De vragenlijsten zijn gedifferentieerd en afgestemd op de te ondervragen respondenten. Vervolgens is overgegaan op het afnemen van de interviews met betrokkenen. De resultaten van de interviews geven een breed beeld van wat er in de dagelijkse praktijk zoal voorkomt, zonder de pretentie dat dit beeld volledig representatief is. Op basis van het voorgaande kon het aantal af te nemen interviews beperkt blijven en is in die interviews de focus met name gelegd op inventarisatie van de politiepraktijk.

⁹ BVH staat voor 'Basisvoorziening Handhaving'. Summ-IT is een politieregistratiesysteem.

Voorafgaand aan het interview is de toezegging gedaan dat alles vertrouwelijk wordt besproken en in het rapport niet met naam en toenaam verwezen zal worden naar specifieke respondenten. De interviews zijn auditief geregistreerd zodat informatie correct kon worden verwerkt.

De verzamelde data en gegevens zijn geanalyseerd en vervolgens is door middel van de interviews verdiepende betekenis gegeven aan bovengenoemde analyse.

1.6 Leeswijzer

Uit het voorgaande vloeit de volgende leeswijzer voor het rapport voort. In dit inleidende hoofdstuk is een beschrijving gegeven van de aanleiding voor het onderzoek, de vraagstelling en de wijze van onderzoek. In hoofdstuk 2 wordt het juridisch kader besproken. Daarbij wordt aandacht besteed aan de relevante wettelijke bepalingen uit het Wetboek van Strafvordering. Ook komt de inbeslagneming in het kader van bijzondere wetten zijdelings aan bod. Tevens wordt gekeken naar verdragsrechtelijk en grondwettelijk beschermde rechten zoals deze neergelegd in het Europees Verdrag voor de Rechten van de Mens (hierna: EVRM) en de Grondwet. Ook de rechtspraak van het Europees Hof voor de Rechten van de Mens (hierna: EHRM) in het kader van het recht op privéleven komt aan bod, naast rechtspraak van de Hoge Raad en lagere rechtspraak in Nederland. Hoofdstuk 3 doet verslag van het onderzoek dat is gedaan naar de praktijk van inbeslagneming aan de hand van zowel de kwantitatieve gegevens, maar voornamelijk aan de hand van de kwalitatieve gegevens. Er wordt aandacht besteed aan de praktijk van inbeslagneming en de praktische aspecten van het nader onderzoek aan gegevensdragers. Verder worden verschillende knelpunten met betrekking tot de inbeslagneming van elektronische gegevensdragers en geautomatiseerde werken besproken. Het geheel wordt in hoofdstuk 4 met een slotbeschouwing en enige conclusies afgesloten.

2. Juridisch kader

2.1 Inleiding

Zoals in het voorgaande hoofdstuk is weergegeven, worden voorafgaand aan de bespreking van de resultaten van het onderzoek naar de praktijk van het in beslag nemen van geautomatiseerde werken en elektronische gegevensdragers en het nader onderzoek daaraan (hoofdstuk 3), in dit hoofdstuk de wettelijke regelingen met betrekking tot het in beslag nemen van voorwerpen (een begrip waaronder ook de geautomatiseerde werken en elektronische gegevensdragers kunnen worden gebracht) en relevante jurisprudentie uiteengezet. In dat kader wordt in dit hoofdstuk een schets gegeven van de bestaande Nederlandse regelgeving op dit gebied. Naast de inbeslagneming van voorwerpen, meer in het bijzonder gegevensdragers en geautomatiseerde werken, wordt stilgestaan bij de bepalingen die onderdeel uitmaken van de regeling van het doorzoeken van een plaats ter vastlegging van gegevens. Die regeling biedt de mogelijkheid om gedurende een doorzoeking van een plaats de aldaar aanwezige elektronische gegevensdragers en geautomatiseerde werken te onderzoeken en de gegevens die daarop zijn opgeslagen vast te leggen.

Bij de beschrijving van de afzonderlijke bepalingen wordt ook ingegaan op de relevante aanwijzingen van het Openbaar Ministerie en eventueel aanvullend beleid. Bovendien wordt stilgestaan bij rechtspraak met betrekking tot die bepalingen. Voor wat betreft de jurisprudentie wordt in het bijzonder stil gestaan bij uitspraken die betrekking hebben op het gebruik van de bevoegdheid, waarbij geautomatiseerde werken en elektronische gegevensdragers ten behoeve van de waarheidsvinding in beslag zijn genomen en nader zijn onderzocht om de op die gegevensdragers en geautomatiseerde werken vastgelegde gegevens ter beschikking te krijgen. Kort wordt stilgestaan bij de relevante internationale verdragen.

De bespreking van het bestaande juridisch kader kan een bijdrage leveren aan het interpreteren en duiden van de kwalitatieve bevindingen. Die bevindingen zelf worden in het volgende hoofdstuk nader gepresenteerd en besproken.

2.2 Verschillende wijzen van het verkrijgen van gegevens ten behoeve van de opsporing

Computergegevens en gegevensbestanden zijn op grond van de huidige wetgeving als zodanig niet in beslag te nemen; zij zijn niet vatbaar voor inbeslagneming. De gegevensdragers zelf, te weten geautomatiseerde werken dan wel elektronische gegevensdragers, zijn dat wel. In het geval men beschikking wil krijgen over op een

bepaalde gegevensdrager opgeslagen gegevens(bestanden) is voor justitie één van de mogelijkheden om het voorwerp waarop de gegevens zijn opgeslagen in beslag te nemen. Indien van die optie gebruik wordt gemaakt, kan aan die voorwerpen op grond van de nog te bespreken jurisprudentie nader onderzoek worden verricht ter verkrijging van de op die voorwerpen vastgelegde gegevens.

Andere wijzen waarop gegevens ten behoeve van de opsporing kunnen worden vergaard, zijn het vorderen van bepaalde relevante gegevens bij een derde – een dergelijke vordering kan niet tot de verdachte worden gericht – en het doorzoeken van een plaats om gegevens die ter plaatse op een gegevensdrager zijn opgeslagen vast te leggen (te kopiëren), in welk geval inbeslagneming van de gegevensdrager achterwege kan blijven.

Op grond van de Wet bevoegdheden vorderen gegevens kan ten aanzien van degene van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot bepaalde opgeslagen of vastgelegde gegevens, een vordering worden gedaan tot het verstrekken van die gegevens. Als uitgangspunt geldt dat, indien met toepassing van de bevoegdheden tot het vorderen van gegevens kan worden volstaan, geen gebruik mag worden gemaakt van de bevoegdheden tot inbeslagneming en de uitlevering ter inbeslagneming.¹⁰

Dit onderzoek richt zich niet op het vorderen van gegevens en deze mogelijkheden worden dan ook verder buiten beschouwing gelaten. Daarbij moet wel worden vastgesteld dat de wetgever in het kader van de regelgeving met betrekking tot het vorderen van gegevens onderscheid heeft aangebracht in het karakter van de te vorderen gegevens. Daarbij wordt een onderscheid gemaakt tussen identificerende gegevens, andere dan identificerende gegevens en gevoelige gegevens.¹¹ Als algemeen uitgangspunt is gehanteerd dat de bevoegdheid tot het vorderen van gegevens is toegekend aan de officier van justitie. Bij het in beslag nemen van voorwerpen, dus ook voorwerpen die gegevens dragen dan wel gegevens kunnen verwerken zoals elektronische gegevensdragers of geautomatiseerde werken, wordt met betrekking tot het onderzoek aan die voorwerpen een dergelijk onderscheid naar de aard van de gegevens (c.q. voorwerpen) in de wet niet gemaakt. In dat geval geldt het uitgangspunt van de officier van justitie als centrale autoriteit niet. In de Wet bevoegdheden vorderen gegevens wordt – anders dan bij de regeling voor de inbeslagneming – dus een onderscheid gemaakt naar de aard van de te vorderen gegevens. Bovendien wordt onderscheid gemaakt tussen gegevens die reeds zijn verwerkt en eerst na het tijdstip van de vordering worden verwerkt.

Het onderhavige onderzoek richt zich, zoals gezegd, in het bijzonder op de inbeslagneming van elektronische gegevensdragers en geautomatiseerde werken. Om de beschikking te

¹⁰ Zie de MvT bij de Wet bevoegdheden vorderen gegevens, *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 12.

¹¹ Hiermee worden gegevens betreffende ras, gezondheid, politieke opvattingen, levensbeschouwelijke overtuigingen en seksuele voorkeuren bedoeld.

krijgen over de, op die voorwerpen vastgelegde, gegevens(bestanden) dient aan het in beslag genomen voorwerp nader onderzoek te worden verricht.

Op de regeling inzake het doorzoeken van een plaats ter vastlegging van gegevens wordt in paragraaf 2.6 nader ingegaan.

2.3 Inbeslagneming van voorwerpen

De inbeslagneming van voorwerpen wordt geregeld in de derde afdeling van de titel ‘Eenige bijzondere dwangmiddelen’ van het Eerste Boek van het Wetboek van Strafvordering.¹²

Er bestaat in de wetgeving een aantal bepalingen dat betrekking heeft op het in beslag nemen van voorwerpen. Daarnaast bestaan bepalingen waarin steunbevoegdheden zijn opgenomen om tot de inbeslagneming van voorwerpen te kunnen komen. De inbeslagneming zelf is in artikel 134 Sv gedefinieerd; onder inbeslagneming wordt verstaan het onder zich nemen of gaan houden van enig voorwerp ten behoeve van strafvordering.

Onder inbeslagneming kan eveneens de situatie vallen waarin een persoon een voorwerp vrijwillig heeft afgestaan en opsporingsambtenaren het voorwerp vervolgens onder zich blijven houden ten behoeve van de strafvordering.

De structuur van de regeling van inbeslagneming in het Wetboek van Strafvordering wordt bepaald door het feit dat aanvankelijk de bevoegdheid tot inbeslagneming voor opsporingsambtenaren alleen bestond bij gelegenheid van de uitoefening van een andere bevoegdheid. Pas later, in 1999, is de huidige algemene bevoegdheid tot inbeslagneming van artikel 96 Sv opgenomen (algemeen in de zin van: los van enige andere bevoegdheid; zie voor de nadere voorwaarden hierna).

De gronden met het oog waarop voorwerpen in beslag mogen worden genomen staan beschreven in artikel 94 Sv.¹³ Alleen voorwerpen waarvan de inbeslagneming een van deze doelen dient, zijn vatbaar voor inbeslagneming.

Artikel 94 lid 1 Sv bepaalt dat voorwerpen, die kunnen dienen om de waarheid aan de dag te brengen of die kunnen dienen om wederrechtelijk verkregen voordeel aan te tonen, vatbaar zijn voor inbeslagneming.

Artikel 94 lid 2 Sv voegt daar de voorwerpen aan toe die verbeurd kunnen worden verklaard dan wel die aan het verkeer kunnen worden onttrokken. De verbeurdverklaring is een

¹² De algemene regels met betrekking tot inbeslagneming van voorwerpen, zoals de regeling voor de gronden voor inbeslagneming, de teruggave van in beslag genomen voorwerpen en de regeling omtrent het bewijs van ontvangst gelden ook bij inbeslagneming op grond van bijzondere wetten, tenzij die wet van de regeling van het Wetboek van Strafvordering afwijkt.

¹³ En overigens ook in artikel 94a Sv, maar dat artikel is binnen het bestek van dit onderzoek niet relevant.

bijkomende straf die beoogt de veroordeelde in zijn vermogen te treffen door hem voorwerpen af te nemen die in een door artikel 33a Sr bepaalde band met een strafbaar feit staan; genoemd artikel 33a Sr bepaalt welke voorwerpen voor verbeurdverklaring vatbaar zijn. De onttrekking aan het verkeer is een maatregel ter bescherming van de samenleving tegen het ongecontroleerde bezit van gevaarzettende voorwerpen. Het opleggen van die maatregel is mogelijk in het geval dat het voorwerp zodanig van aard is dat het ongecontroleerde bezit van dat voorwerp in strijd is met de wet of het algemeen belang.¹⁴

Inbeslagneming van elektronische gegevensdragers of geautomatiseerde werken heeft in de meeste gevallen plaats met het oog op waarheidsvinding. Dat zal de gevallen betreffen waarin wordt vermoed dat op die voorwerpen gegevens zijn opgeslagen die van belang zijn voor het opsporingsonderzoek. Inbeslagneming kan mede plaats hebben of worden voortgezet met het oog op de verbeurdverklaring van de gegevensdrager als voorwerp of de onttrekking aan het verkeer. Bij die laatste maatregel kan het bijvoorbeeld gaan om gegevensdragers waar gegevens(bestanden) op staan die afbeeldingen bevatten van seksuele handelingen van personen, die de leeftijd van achttien jaar nog niet hebben bereikt, of bijvoorbeeld om een grote hoeveelheid creditcardgegevens van derden of andere illegale content.

De bevoegdheid tot inbeslagneming is voor de opsporingsambtenaar (met inbegrip van de (hulp)officier van justitie) geregeld in de artikelen 95 en 96 Sv. De bevoegdheid tot inbeslagneming door de rechter-commissaris is geregeld in artikel 104 Sv. De toepassing van de bevoegdheid tot inbeslagneming door opsporingsambtenaren is nader uitgewerkt in de Aanwijzing inbeslagneming van het College van procureurs-generaal.¹⁵

Teneinde de inbeslagneming mogelijk te maken, bevat het Wetboek van Strafvordering steunbevoegdheden. Dat zijn bevoegdheden die kunnen worden uitgeoefend teneinde de beschikking te krijgen over het in beslag te nemen voorwerp. Steunbevoegdheden zijn: het betreden van een plaats ter inbeslagneming (artikel 96 en 110 Sv), het bevel tot uitlevering van een voorwerp ter inbeslagneming (artikelen 96a, 100, 105 en 114 Sv) en de doorzoeking van een plaats ter inbeslagneming (artikelen 96b, 96c, 97 en 110 Sv). Deze steunbevoegdheden moeten worden onderscheiden van de bevoegdheid een voorwerp in beslag te nemen. De inbeslagneming van bij de uitoefening van steunbevoegdheden aangetroffen en daarvoor vatbare voorwerpen geschiedt op basis van de bevoegdheid tot inbeslagneming (niet op basis van de steunbevoegdheid).

De algemene inbeslagnemingsbevoegdheid (artikel 96 Sv) alsmede de steunbevoegdheden tot het betreden van plaatsen (artikel 96 Sv), het bevel uitlevering (artikel 96a Sv) en het doorzoeken van een vervoermiddel (artikel 96b Sv) kunnen op grond van de genoemde

¹⁴ Artikel 36c Sr.

¹⁵ Aanwijzing inbeslagneming (Artikel 94 Wvsv) (2014A006), laatstelijk gewijzigd per 1 juli 2014, *Stcrt.* 2014, 18598.

bepalingen door iedere opsporingsambtenaar slechts worden toegepast in het geval er sprake is van ontdekking op heterdaad van een strafbaar feit of in geval van een misdrijf als bedoeld in artikel 67 lid 1 Sv.

De officier van justitie is bevoegd ter inbeslagneming plaatsen te doorzoeken, met uitzondering van woningen en kantoren van verschoningsgerechtigden, in geval van ontdekking op heterdaad van een strafbaar feit of in geval van verdenking van een misdrijf als bedoeld in artikel 67 lid 1 Sv (artikel 96c Sv). In geval van spoedeisendheid en wanneer de komst van de rechter-commissaris niet kan worden afgewacht, kan hij met machtiging van de rechter-commissaris ook woningen en kantoren van verschoningsgerechtigden doorzoeken (artikel 97 Sv).

De rechter-commissaris is in geval van verdenking van elk strafbaar feit bevoegd voorwerpen in beslag te nemen (artikel 104 Sv), daartoe de uitlevering te bevelen (artikel 105 Sv) of plaatsen te doorzoeken, met inbegrip van woningen en kantoren van verschoningsgerechtigden (artikel 110 Sv).

Het bovenstaande betreft de regeling in het Wetboek van Strafvordering. Sommige bijzondere wetten geven een ruimere bevoegdheid tot inbeslagneming meestal in die zin dat de bevoegdheden ook door opsporingsambtenaren kunnen worden ingezet bij verdenking van feiten waarvoor geen voorlopige hechtenis op grond van artikel 67 lid 1 Sv is toegelaten. De bevoegdheid van artikel 18 WED bijvoorbeeld bestaat ten aanzien van elk strafbaar feit uit diezelfde WED. Zie ook artikel 9 lid 3 Opiumwet en artikel 52 lid 1 Wet wapens en munitie. Tegelijkertijd geldt dat de toepassing van die bevoegdheden is beperkt tot de gevallen waarin een verdenking bestaat ter zake van strafbare feiten die onder de reikwijdte van de betreffende bijzondere wet vallen.

Naar hun aard komen vrijwel alle voorwerpen voor inbeslagneming in aanmerking, als dat maar een strafvorderlijk doel als bedoeld in artikel 94 Sv kan dienen. Bij de inbeslagneming dient de opsporingsambtenaar dus na te gaan of een grond genoemd in artikel 94 Sv bestaat om over te gaan tot het in beslag nemen van het voorwerp. Indien de inbeslagneming geen strafvorderlijk belang dient, is inbeslagneming niet mogelijk. Opmerking verdient daarbij dat de grond van waarheidsvinding vereist dat het voorwerp redelijkerwijs kan bijdragen aan de opheldering van het betreffende strafbare feit ter zake waarvan verdenking bestaat. Voor de andere gronden van artikel 94 Sv (aantonen van wederrechtelijk voordeel, verbeurdverklaring of onttrekking aan het verkeer van bepaalde voorwerpen) kan de relatie met het strafbare feit indirecter zijn.

[Kennisgeving van inbeslagneming en bewijs van ontvangst](#)

In het geval een opsporingsambtenaar, de officier van justitie of de rechter-commissaris over gaat tot de inbeslagneming van voorwerpen, wordt daarvan ingevolge artikel 94 lid 3

Sv door de opsporingsambtenaar een kennisgeving van inbeslagneming opgemaakt. Daarvan te onderscheiden is het bewijs van ontvangst dat ingevolge hetzelfde artikellid zoveel mogelijk wordt afgegeven en wel aan degene bij wie het voorwerp in beslag is genomen (de beslagene). Zowel de kennisgeving van inbeslagneming als het bewijs van ontvangst dient als uitgangspunt zo spoedig mogelijk te worden opgemaakt. Dit laatste volgt uit de Aanwijzing inbeslagneming (Artikel 94 Wvsv)¹⁶, maar niet rechtstreeks uit de wettekst van artikel 94 lid 3 Sv. Uit artikel 94 lid 3 jo. artikel 116 Sv volgt wel dat de kennisgeving van inbeslagneming zo spoedig mogelijk in handen wordt gesteld van de hulpofficier van justitie, zodat deze kan beoordelen of het beslag dient te worden gehandhaafd of niet. In de hierboven genoemde Aanwijzing worden ook nadere regels gesteld omtrent (de inhoud van) de kennisgeving van inbeslagneming.

Aan de beslagene wordt gevraagd of hij of zij afstand wil doen van de aanspraak op teruggave van de voorwerpen. Dat verzoek blijft achterwege indien duidelijk is dat een voorwerp zich leent voor teruggave aan de beslagene.¹⁷

Uit de verbaliseringsplicht van artikel 152 Sv vloeit voort dat naast de kennisgeving van inbeslagneming ook een proces-verbaal van inbeslagneming wordt opgemaakt. De opsporingsambtenaar wordt geacht een en ander te relateren in een proces-verbaal om zulks in het zaaksdossier op te (doen) nemen.

Het opstellen van een kennisgeving van inbeslagneming moet ook geschieden indien de bewuste inbeslagneming op aanwijzing en onder verantwoordelijkheid van of door de officier van justitie dan wel een rechter-commissaris heeft plaatsgevonden.¹⁸

In de kennisgeving van inbeslagneming kunnen verschillende voorwerpen worden vermeld. Indien meerdere voorwerpen op dezelfde kennisgeving van inbeslagneming worden vermeld is van belang dat die voorwerpen gelijksoortig zijn en dat de afhandeling van het beslag op een gelijksoortige wijze plaatsvindt. Dat laatste hangt samen met de beheersbeslissing die ten aanzien van voorwerpen dient te worden genomen. De kennisgeving van inbeslagneming geeft een beschrijving van de in beslag genomen voorwerpen en geeft de informatie die van belang is voor de te nemen beslissing omtrent het voortduren van beslag weer. De kennisgeving dient onder meer informatie te bevatten over de datum van inbeslagneming, een heldere omschrijving te geven van elk voorwerp en dat voorwerp van een uniek nummer te voorzien zodat elk voorwerp afzonderlijk kan worden geïdentificeerd. De gronden voor de inbeslagneming worden eveneens genoemd en in een categorie geplaatst. De categorie van het beslag is onlosmakelijk verbonden met

¹⁶ Artikel II.2 Aanwijzing inbeslagneming (Artikel 94 Wvsv) (2014A006), laatstelijk gewijzigd per 1 juli 2014, *Stcrt.* 2014, 18598.

¹⁷ Artikel II.2 Aanwijzing inbeslagneming (Artikel 94 Wvsv) (2014A006), laatstelijk gewijzigd per 1 juli 2014, *Stcrt.* 2014, 18598.

¹⁸ Artikel II.2 Aanwijzing inbeslagneming (Artikel 94 Wvsv) (2014A006), laatstelijk gewijzigd per 1 juli 2014, *Stcrt.* 2014, 18598.

het doel van het beslag en dient, ook weer vanwege de beheersbeslissing, te worden vermeld. Tot slot dienen de personalia van de beslagene en eventuele eigenaar of rechthebbende te worden vermeld. Ook dient per voorwerp te worden aangegeven of de rechthebbende of beslagene afstand doet van het voorwerp en of de beslagene heeft verklaard dat het voorwerp aan hem toebehoort. Per beslagene dient in ieder geval een aparte kennisgeving van inbeslagneming op te worden gemaakt.¹⁹

Indien de personalia van de rechthebbende op een later tijdstip bekend worden of alsnog afstand wordt gedaan van de in beslag genomen voorwerpen, dienen de gegevens op de kennisgeving van inbeslagneming gedurende de procedure op een duidelijk kenbare wijze te worden gewijzigd of aangevuld. Dat moet ook gebeuren als een als partij aangemerkte verzameling wordt gesplitst in verschillende verzamelingen voorwerpen of als de (hulp)officier van justitie een beslissing heeft genomen over een van de op de kennisgeving van in beslag genomen genoemde voorwerpen. Degene die de kennisgeving van inbeslagneming in de loop van de procedure wijzigt of aanvult, vermeldt zijn gegevens en het tijdstip daarvan.²⁰

De inbeslagneming van een bepaald voorwerp kan ook met het oog op meer dan één van de in artikel 94 Sv genoemde gronden plaatsvinden. In veel gevallen vormt de waarheidsvinding één van die grondslagen. Indien voorwerpen op grond van ‘bijdrage aan de waarheidsvinding’ in beslag zijn genomen, dienen zij in ieder geval te worden bewaard zolang nog onderzoek aan die voorwerpen moet worden gedaan of niet uitgesloten kan worden dat nog onderzoek aan de voorwerpen moet worden gedaan. Bijvoorbeeld wanneer voorwerpen mogelijk nog op het onderzoek ter terechtzitting als stuk(ken) van overtuiging dienen te worden getoond, of voorwerpen in het kader van een contra-expertise nog nodig kunnen zijn. In die gevallen dient de bewaring derhalve in ieder geval te worden voortgezet, totdat de beslissing in de strafzaak in kracht van gewijsde is gegaan. Dat geldt niet voor voorwerpen die zijn in beslag genomen met het oog op de verbeurdverklaring of onttrekking aan het verkeer. De bewaring van deze voorwerpen kan, in afwachting van een rechterlijke uitspraak, in bepaalde gevallen worden beëindigd door het voorwerp te vervreemden of te vernietigen.²¹

Ten aanzien van de voorwerpen die langer moeten worden bewaard bestaat, voor zover het gaat om gegevensdragers, de mogelijkheid om te volstaan met inbeslagneming van een kopie van de op de gegevensdragers opgeslagen gegevens, waarna de gegevensdrager aan de beslagene kan worden teruggegeven. Hierbij kan worden gedacht aan het maken van

¹⁹ Artikel II.2 Aanwijzing inbeslagneming (Artikel 94 Wvsv) (2014A006), laatstelijk gewijzigd per 1 juli 2014, *Stcrt.* 2014, 18598.

²⁰ Artikel II.2 Aanwijzing inbeslagneming (Artikel 94 Wvsv) (2014A006), laatstelijk gewijzigd per 1 juli 2014, *Stcrt.* 2014, 18598.

²¹ Artikel 117 Sv.

een ‘image’²² van de harde schijf of de inbeslagneming van alleen de harde schijf van een computer waarbij de overige hardware dan weer aan de beslagene kan worden teruggegeven.²³

De kennisgeving van inbeslagneming zelf wordt uiteindelijk op de weergave van de informatie en volledigheid beoordeeld door een hulpofficier van justitie. Hij neemt een beslissing over het handhaven van het beslag en geeft desgewenst een opdracht tot aanpassing of wijziging van de kennisgeving van inbeslagneming.²⁴

Zolang nog geen beslissing is genomen over welke van de in artikel 94 Sv genoemde gronden van toepassing is, en daarmee nog niet duidelijk is op welke wijze het in beslag genomen voorwerp dient te worden bewaard, ligt het beheer tijdelijk in handen van de opsporingsinstantie. Het beheer over het beslag wordt pas overgedragen op het moment dat het aan een bewaarder wordt overhandigd.²⁵ Het Openbaar Ministerie draagt steeds de verantwoordelijkheid over het beslag en de juiste afhandeling daarvan.

Uitstellen van het afgeven van het bewijs van ontvangst

Een aspect dat nader dient te worden besproken in het kader van de inbeslagneming van voorwerpen is de kennisgeving daarvan aan een betrokkene door uitreiking van een bewijs van ontvangst. In beginsel dient dat ‘zoveel mogelijk’ te geschieden. In dit kader moet worden gewezen op het arrest van het Hof Den Bosch in de zaak ‘Maskerbij’.²⁶

In deze zaak, waarin de verdachte werd vervolgd voor de uitvoer van een grote hoeveelheid softdrugs, stelde de verdediging dat het Openbaar Ministerie niet-ontvankelijk in de vervolging moest worden verklaard, vanwege de gehanteerde opsporingsmethoden. Het betrof hier in het bijzonder het bevel van de officier van justitie om een bestelauto en de zich daarin bevindende goederen, heimelijk in beslag te nemen. De heimelijke inbeslagneming hield in dat aan verdachte geen bewijs van ontvangst zou worden afgegeven op grond van artikel 94 lid 3 Sv en/of dat niet anderszins aan hem mededeling zou worden gedaan van de inbeslagneming. Het Hof overwoog in reactie daarop dat het betreden van de bestelauto en het in beslag nemen van de daarin aangetroffen verdovende middelen op rechtmatige wijze plaats had kunnen vinden en op een wettelijke grondslag

²² Een image is een computerbestand waarin een exacte kopie van een opslagmedium, zoals een harde schijf, een cd of een dvd, is opgeslagen. Het bevat alle informatie die nodig is om de structuur en gegevens van het medium opnieuw te construeren, zoals de bestanden, de bestandsstructuur en meta-informatie. Een image verschilt hierin met een gewone back-up waarbij alleen de bestanden worden overgenomen. Het bewaren van de structuur en integriteit van de gegevens is bij een image meer verzekerd.

²³ Artikel IV.2 Aanwijzing inbeslagneming (Artikel 94 Wvsv) (2014A006), laatstelijk gewijzigd per 1 juli 2014, *Stcrt.* 2014, 18598.

²⁴ Artikel II.4 Aanwijzing inbeslagneming (Artikel 94 Wvsv) (2014A006), laatstelijk gewijzigd per 1 juli 2014, *Stcrt.* 2014, 18598.

²⁵ Artikel II.5 Aanwijzing inbeslagneming (Artikel 94 Wvsv) (2014A006), laatstelijk gewijzigd per 1 juli 2014, *Stcrt.* 2014, 18598.

²⁶ Hof Den Bosch 3 april 2014, ECLI:NL:GHSHE:2014:956.

was gestoeld, maar dat geen grondslag bestond voor het op een andere plaats achterlaten van de bestelauto en het achterwege laten van een kennisgeving aan de beslagene.

Concreet werd overwogen dat de gehanteerde zelfstandige bevoegdheden tot inbeslagneming (artikel 96 jo. artikel 94 Sv en artikel 9 Opiumwet) geen grondslag bieden voor het achterwege laten van een kennisgeving aan de verdachte. Het Hof komt dan ook tot het oordeel dat sprake is van een vormverzuim in de zin van artikel 359a Sv, maar volstaat met de enkele constatering hiervan. Dat wordt onderbouwd door te stellen dat de wetgever niet gedacht lijkt te hebben aan de situatie van heimelijke inbeslagneming, ondanks dat volgens artikel 94 lid 3 Sv een bewijs ‘zoveel mogelijk’ hoeft te worden afgegeven. Het Hof voert aan dat deze omschrijving conform de memorie van toelichting²⁷ moet worden gezien tegen de achtergrond van de destijds bestaande capaciteitsproblemen. Ten overvloede merkt het Hof nog op dat indien de wetgever een wens tot het scheppen van een bevoegdheid tot heimelijke inbeslagneming had gehad, die concreet door hem zou zijn verwoord.

In een andere zaak, waarin een aantal verdachten werd vervolgd voor overtredingen van de Wet wapens en munitie heeft de rechtbank Gelderland aansluiting gezocht bij de uitspraak van het Hof Den Bosch in de zaak ‘Maskerbij’. In deze zaak, het BOLA-onderzoek²⁸, werd door verdediging de vraag opgeworpen of “heimelijke inbeslagneming” van telefoons en laptops is toegestaan, waarbij werd gedoeld op de inbeslagneming zonder afgifte van een bewijs van ontvangst ingevolge artikel 94 Sv. De rechtbank Gelderland constateerde, net als het Hof Den Bosch, dat sprake was van een vormverzuim in de zin van artikel 359a Sv, maar oordeelde dat in de gegeven omstandigheden van het geval kon worden volstaan met de constatering daarvan.

2.4 Teruggave van het in beslag genomen voorwerp aan de beslagene

In het voorgaande is geschetst dat aan de inbeslagneming van voorwerpen verschillende, in artikel 94 Sv genoemde, gronden ten grondslag kunnen liggen. Daarbij is geconstateerd dat de grond waarop de inbeslagneming stoelt, van invloed is op het moment waarop moet of kan worden besloten het voorwerp terug te geven. Voorwerpen die in beslag genomen zijn omdat zij vatbaar zijn voor verbeurdverklaring of onttrekking aan het verkeer hoeven in beginsel niet meer te worden teruggegeven aan de beslagene, tenzij gedurende het opsporingsonderzoek duidelijk wordt dat de oplegging van straf of maatregel niet aannemelijk is c.q. deze niet wordt opgelegd. Ook indien de beslagene schriftelijk heeft

²⁷ *Kamerstukken II* 1993/94, 23 692, nr. 3.

²⁸ Rb. Gelderland 8 oktober 2015, ECLI:NL:RBGEL:2015:6215.

verklaard dat het voorwerp hem toebehoort en afstand heeft gedaan van het voorwerp, hoeft het voorwerp niet aan de beslagene te worden teruggegeven.

Uit het bepaalde in artikel 116 lid 1 Sv volgt, dat indien geen strafvorderlijk belang meer wordt gediend met het voortduren van het beslag, dat beslag wordt beëindigd en de officier van justitie of de hulpofficier van justitie het voorwerp doet teruggeven aan de beslagene. Uit lid 2 van die bepaling volgt dat indien de beslagene schriftelijk afstand heeft gedaan van het voorwerp en het redelijkerwijs aannemelijk is dat een ander dan de beslagene als rechthebbende heeft te gelden, dit voorwerp wordt teruggegeven aan degene die redelijkerwijs als rechthebbende kan worden beschouwd. Indien teruggave aan diegene nog niet mogelijk is, kan worden gelast dat het voorwerp ten behoeve van de rechthebbende in bewaring zal blijven. Het is ook mogelijk dat met het voorwerp, in het geval het daadwerkelijk aan de beslagene toebehoort, op een zelfde wijze wordt gehandeld als met voorwerpen die vatbaar zijn voor verbeurdverklaring of onttrekking aan het verkeer.²⁹ Het Openbaar Ministerie heeft overigens ook de mogelijkheid om bij het afdoen van de zaak door middel van een beleidssepot, strafbeschikking of transactie daaraan de voorwaarde te verbinden dat de verdachte afstand doet van het voorwerp of een voorwerp uitlevert. Die mogelijkheid is echter wel beperkt tot de gevallen dat een voorwerp kan worden verbeurd verklaard, kan worden onttrokken aan het verkeer of toebehoort aan een ander. Voorts kan de officier van justitie bij strafbeschikking ook in beslag genomen voorwerpen onttrekken aan het verkeer.³⁰ Ten slotte kan de rechter de onttrekking aan het verkeer bij afzonderlijke beschikking op vordering van het Openbaar Ministerie uitspreken conform artikel 36b lid 1 sub 4 jo. artikel 552f Sv.

Vernietigen of verwijderen van (een gedeelte van) de op een in beslag genomen elektronische gegevensdrager of geautomatiseerd werk opgeslagen gegevens

Het Wetboek van Strafvordering en de Aanwijzing inbeslagneming (Artikel 94 Wvsv) bevatten geen regeling omtrent het ontoegankelijk maken, het vernietigen of verwijderen van gegevens op in beslag genomen voorwerpen. Wel kunnen de voorwerpen die in beslag zijn genomen, zoals eerder vermeld, vatbaar zijn voor verbeurdverklaring dan wel onttrekking aan het verkeer (ook als zij in eerste instantie op andere grond in beslag zijn genomen).

Dat betekent dat ten aanzien van het voorafgaand aan de teruggave van de gegevensdrager (al dan niet gedeeltelijk) vernietigen, verwijderen of ontoegankelijk maken van de daarop aanwezige gegevens(bestanden) geen expliciete regeling bestaat.

²⁹ Artikel 116 lid 2 Sv.

³⁰ Artikel 257a lid 2 sub c Sv.

Dat ligt anders in het geval de gegevens tijdens een doorzoeking van een plaats ter vastlegging van gegevens in een geautomatiseerd werk, zijn aangetroffen.³¹ In artikel 125o Sv is een bepaling opgenomen die het mogelijk maakt om bepaalde gegevens met betrekking waartoe of met behulp waarvan het strafbare feit is gepleegd ontoegankelijk te maken indien dit noodzakelijk is ter beëindiging van een strafbaar feit of ter voorkoming van nieuwe strafbare feiten.³² Het betreft dan maatregelen die worden genomen om te voorkomen dat onbevoegden van de gegevens(bestanden) kennis kunnen nemen. Het ontoegankelijk maken van gegevens kan volgens de memorie van toelichting softwarematig geschieden: het deleten of verwijderen van bestanden, waarbij de opsporingsinstantie een kopie van de gegevens(bestanden) onder zich neemt of hardwarematig: door de gegevensdrager zelf onbruikbaar te maken. Daarbij dient de methode die de minste inbreuk maakt te worden gehanteerd.³³ Uiteindelijk bepaalt de rechter of dergelijke gegevens definitief worden vernietigd of dat ze weer ter beschikking van de beheerder van het geautomatiseerde werk worden gesteld.³⁴ De officier van justitie kan overigens in een eerder stadium, te weten zodra het belang van de strafvordering zich daar niet meer tegen verzet, de ontoegankelijkmaking ongedaan maken. De beslissing ontoegankelijk gemaakte gegevens definitief te vernietigen kan ook bij afzonderlijke rechterlijke beschikking op vordering van de officier van justitie worden genomen.³⁵

2.5 Onderzoek aan in beslag genomen voorwerpen

In het bovenstaande is ingegaan op de gronden voor de inbeslagneming van voorwerpen en aan het voortduren van het beslag. Naast de verbeurdverklaring, het aantonen van het wederrechtelijk voordeel en de onttrekking aan het verkeer van voorwerpen wordt de waarheidsvinding in artikel 94 Sv als grond genoemd. Daarbij kan worden gedacht aan het wapen waarmee een moord is begaan, maar ook aan stoffen waarvan het vermoeden bestaat dat het een middel, als bedoeld in de Opiumwet betreft. In geval van de inbeslagneming van een stof dient vanzelfsprekend nader te worden onderzocht of die stof daadwerkelijk een middel als bedoeld in de Opiumwet betreft. Ook zal er behoefte zijn het vuurwapen nader te onderzoeken. De wet geeft omtrent het nader onderzoek aan dergelijke in beslag genomen voorwerpen geen verdere regels.

De wet geeft omtrent de inbeslagneming van elektronische gegevensdragers en geautomatiseerde werken eveneens geen nadere regels of dergelijk onderzoek aan in beslag genomen voorwerpen al dan niet mag worden uitgevoerd. Die bevoegdheid wordt verondersteld onderdeel uit te maken van de bevoegdheid tot inbeslagneming van het

³¹ Zoals eerder vermeld wordt later op die regeling ingegaan.

³² Artikel 125o lid 1 Sv.

³³ *Kamerstukken II* 1998/99, 26 671, nr. 3, p. 21.

³⁴ Artikel 354 lid 2 Sv.

³⁵ Artikel 552fa lid 1 Sv.

voorwerp ten behoeve van de waarheidsvinding. Aan het nader onderzoek aan in beslag genomen elektronische gegevensdragers en geautomatiseerde werken is in recente jurisprudentie bijzondere aandacht besteed. Dit zal in paragraaf 2.10 nader uiteen worden gezet.

Het professioneel verschoningsrecht bij inbeslagneming

Bij onderzoek aan in beslag genomen gegevensdragers (geautomatiseerde werken of elektronische gegevensdragers) kan het voorkomen dat daarop gegevens zijn opgeslagen die onder het verschoningsrecht van een professioneel verschoningsgerechtigde als bedoeld in artikel 218 Sv vallen. Dat ligt voor de hand wanneer de gegevensdragers in beslag worden genomen onder professioneel verschoningsgerechtigden. Dergelijke gegevens kunnen zich echter ook bevinden op een elektronische gegevensdrager of geautomatiseerd werk die bij een ander dan de verschoningsgerechtigde, bijvoorbeeld de verdachte, in beslag wordt genomen.

Met betrekking tot de inbeslagneming van de voorwerpen onder een professioneel verschoningsgerechtigde is artikel 98 Sv van belang. In die bepaling worden nadere regels gesteld met betrekking tot de inbeslagneming en doorzoeking bij een professioneel verschoningsgerechtigde. De rechter-commissaris is degene die bevoegd is bij discussie over de vraag of een voorwerp wel of niet onder de reikwijdte van het verschoningsrecht valt te beslissen.³⁶

Die bepaling betreft brieven of andere geschriften tot welke de geheimhoudingsplicht van de professioneel verschoningsgerechtigde zich uitstrekt. Een en ander is nader uitgewerkt in lagere regelgeving. Daar wordt vrij uitvoerig ingegaan op de voorbereiding, uitvoering, beslissingen en eventuele toetsing achteraf inzake de inbeslagneming bij advocaten.³⁷ Uit de jurisprudentie volgt dat de bepaling van artikel 98 Sv zich ook uitstrekt tot elektronisch vastgelegde 'brieven en geschriften'.³⁸

In dit kader kan gewezen worden op een arrest van de Hoge Raad van 20 februari 2007.³⁹ In die zaak werd geklaagd over het oordeel van de rechtbank dat de inbeslagneming door de FIOD-ECD van computers redelijkerwijs kon bijdragen aan de waarheidsvinding van

³⁶ Artikel 98 lid 1 Sv.

³⁷ Aanwijzing toepassing opsporingsbevoegdheden en dwangmiddelen tegen advocaten, (2011A003), laatstelijk gewijzigd per 1 april 2011, *Stcr.* 2011, 4981.

³⁸ Recent heeft de Hoge Raad een uitspraak gedaan waaruit blijkt dat correspondentie tussen anderen dan de verschoningsgerechtigde en degene die zich tot hem heeft gewend, geen brief of een geschrift is in de zin van artikel 98 lid 1 Sv. Indien van die correspondentie een afschrift wordt toegezonden aan de notaris kan niet gezegd worden dat reeds daarom de inhoud daarvan kan worden aangemerkt als wetenschap die aan de notaris in het kader van zijn juridische dienstverlening is toevertrouwd. De in beslag genomen e-mailwisseling, waarin de notaris in de cc staat, valt in beginsel niet onder het verschoningsrecht van de notaris. Zie HR 26 januari 2016, ECLI:NL:HR:2016:110.

³⁹ HR 20 februari 2007, ECLI:NL:HR:2007:AZ3564, *NJ* 2008, 113, m.nt. T.M. Schalken onder *NJ* 2008, 115.

het strafbare feit waarvan de klager werd verdacht. De klacht betoogde blijkens het oordeel van de rechtbank, dat het in beslag nemen van de computers zonder toestemming van de klager in strijd was met artikel 98 Sv. De verdediging onderbouwde die klacht met het standpunt dat niet de hele computer in beslag genomen had mogen worden, maar dat de klager de gelegenheid had moeten worden geboden per gegevens(bestand) aan te geven of dit onder zijn verschoningsrecht viel.⁴⁰

De Hoge Raad overwoog bij de beoordeling dat bij professioneel verschoningsgerechtigden, ook zonder hun toestemming, brieven of geschriften die voorwerp van het strafbare feit uitmaken of tot het begaan daarvan hebben gediend in beslag mogen worden genomen, aangezien die geen object zijn van de aan die personen toekomende bevoegdheid tot verschoning.⁴¹ De Hoge Raad oordeelde vervolgens dat, gelet daarop, de opvatting dat artikel 98 Sv meebrengt dat computers met daarin opgeslagen gegevens(bestanden), ook indien zij voorwerp uitmaken van het strafbare feit dan wel tot het begaan daarvan hebben gediend, slechts in beslag mogen worden genomen met toestemming van de professioneel verschoningsgerechtigde onjuist is.⁴²

Ten aanzien van het per gegevens(bestand) op het geautomatiseerd werk aanwijzen of dat onder het professioneel verschoningsrecht valt, overwoog de Hoge Raad in een eerder arrest dat in het kader van de waarheidsvinding onderzoek mag worden gedaan aan in beslag genomen voorwerpen teneinde gegevens voor het strafrechtelijk onderzoek ter beschikking te krijgen en dat in computers opgeslagen gegevens daarvan niet uitgezonderd zijn.⁴³ Hierbij wordt door de Hoge Raad opgemerkt dat bij een dergelijk onderzoek, op grond van het (in paragraaf 2.6.2 te bespreken) bepaalde in artikel 125l Sv, het verschoningsrecht dient te worden gerespecteerd.⁴⁴ Ter aanvulling overweegt de Hoge Raad daarbij dat de opvatting dat bij een dergelijk onderzoek behoudens toestemming van de verschoningsgerechtigde niet mag worden gezocht naar gegevens die voorwerp van het strafbare feit uitmaken of tot het begaan daarvan hebben gediend als onjuiste uitleg van artikel 125l Sv moet worden beschouwd, aangezien dat geen gegevens betreft waartoe de plicht tot geheimhouding zich uitstrekt.⁴⁵

Tot slot overweegt de Hoge Raad dat er geen reden hoeft te zijn het onderzoek op voorhand te beperken tot bestanden die volgens de betrokkene niet onder het

⁴⁰ HR 20 februari 2007, ECLI:NL:HR:2007:AZ3564, r.o. 4.2.1, *NJ* 2008, 113, m.nt. T.M. Schalken onder *NJ* 2008, 115.

⁴¹ Zoals eerder overwogen in een uitspraak van HR 29 maart 1994, ECLI:NL:HR:1994:AD2076, *NJ* 1994, 537, m.nt. T.M. Schalken onder *NJ* 1994, 577.

⁴² HR 20 februari 2007, ECLI:NL:HR:2007:AZ3564, r.o. 4.2.4, *NJ* 2008, 113, m.nt. T.M. Schalken onder *NJ* 2008, 115.

⁴³ HR 29 maart 1994, ECLI:NL:HR:1994:AD2076, *NJ* 1994, 537, m.nt. T.M. Schalken onder *NJ* 1994, 577.

⁴⁴ HR 20 februari 2007, ECLI:NL:HR:2007:AZ3564, r.o. 4.2.6, *NJ* 2008, 113, m.nt. T.M. Schalken onder *NJ* 2008, 115.

⁴⁵ Onder verwijzing naar HR 29 maart 1994, ECLI:NL:1994:AD2076, *NJ* 1994, 537, m.nt. T.M. Schalken onder *NJ* 1994, 577.

verschoningsrecht vallen. De Hoge Raad noemt dat onderdeel van de rechtbank in casu niet onbegrijpelijk. Dat laatste vloeit volgens de Hoge Raad voort uit het feit dat computerbestanden zich naar hun aard niet eenvoudig lenen voor afzonderlijk onderzoek. Van belang werd wel geacht dat voldoende gewaarborgd is dat de in beslag genomen computers worden onderzocht op een wijze waarbij het verschoningsrecht van de klager niet in het gedrang komt, dat wil zeggen op een wijze zoals in artikel 125l Sv genormeerd wordt.⁴⁶

2.6 Doorzoeken van plaatsen ter vastlegging van gegevens

Naast de inbeslagneming van gegevensdragers en geautomatiseerde werken kunnen ook gegevens worden verkregen door tijdens een doorzoeking van een plaats die gegevens vast te leggen die in een op de te doorzoeken plaats aanwezige gegevensdragers zijn vastgelegd of opgeslagen. Dat vastleggen van gegevens vindt plaats op grond van de bepalingen met betrekking tot de ‘doorzoeking van een plaats ter vastlegging van gegevens’ in de zevende afdeling van Titel IV van het eerste boek van het Wetboek van Strafvordering, artikelen 125i tot en met 125o.

Op grond van het bepaalde in artikel 125i Sv kunnen, onder dezelfde voorwaarden als bedoeld in de artikelen 96b, 96c, lid 1 tot en met lid 3, artikel 97, lid 1 tot en met lid 4, en artikel 110, lid 1 en lid 2, Sv, plaatsen worden doorzocht ter vastlegging van gegevens en kunnen gegevens die op deze plaats op een gegevensdrager zijn vastgelegd of opgeslagen, ‘in het belang van het onderzoek’ worden vastgelegd. De gegevens kunnen vervolgens worden onderzocht.

De normering van de doorzoeking van een plaats ter vastlegging van gegevens sluit aan bij de normering van de doorzoeking ter inbeslagneming van voorwerpen.⁴⁷ Die normering maakt onderscheid naar de aard van de locatie (de woning, etc.) waar de doorzoeking wordt uitgevoerd. Het onderscheid naar de aard van de gegevens (identificerende gegevens, andere dan identificerende gegevens en gevoelige gegevens), zoals de wet dat kent met betrekking tot de bevoegdheden tot het vorderen van gegevens, wordt in het kader van de doorzoeking van een plaats ter vastlegging van gegevens niet gemaakt. Dat laatste vindt voornamelijk zijn oorzaak in het feit dat het bij de doorzoeking van te voren lastig is vast te stellen op welke gegevens de met opsporing belaste instantie of de rechter-commissaris zullen stuiten. Dit geldt ook bij het in beslag nemen van een voorwerp met het oog op het vergaren van de daarop opgeslagen gegevens.

De bevoegdheid tot het doorzoeken ter vastleggen van gegevens dient pas te worden toegepast als andere minder ingrijpende bevoegdheden, zoals het vorderen van gegevens

⁴⁶ HR 20 februari 2007, ECLI:NL:HR:2007:AZ3564, r.o. 4.2.8, NJ 2008, 113, m.nt. T.M. Schalken onder NJ 2008, 115.

⁴⁷ *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 12.

of het bevelen van de uitlevering van een voorwerp ter inbeslagneming, niet het gewenste effect kunnen bereiken.⁴⁸ Nadere uitvoeringsregels met betrekking tot de toepassing van de bepalingen die de doorzoeking ter vastlegging van gegevens reguleren, zijn niet opgesteld.

Netwerkzoeking

De bevoegdheid tot doorzoeking van een plaats ter vastlegging van gegevens kan worden uitgebreid van de op die plaats aanwezige geautomatiseerde werken tot elders aanwezige geautomatiseerde werken, zo vloeit uit lid 1 van artikel 125j Sv voort. De reikwijdte van het onderzoek in elders aanwezige geautomatiseerde werken is overigens beperkt: enkel geautomatiseerde werken waartoe de personen die plegen te werken of te verblijven aanwezig op de plaats waar de doorzoeking plaatsvindt met toestemming van de rechthebbende tot dat geautomatiseerde werk, toegang toe hebben, mogen worden benaderd. Dat volgt uit lid 2 van artikel 125j Sv. Met ‘toestemming’ wordt bedoeld de toestemming om bepaalde gegevens in een elders geautomatiseerd werk te benaderen door personen die werken of verblijven op de plaats die wordt doorzocht.

Dat betekent, anders gezegd, dat indien bij een doorzoeking, een geautomatiseerd werk wordt onderzocht ter vastlegging van gegevens, eveneens gegevens mogen worden vastgelegd, die zich op een elders aanwezig geautomatiseerd werk (binnen het netwerk) bevinden, maar dat die vastlegging van gegevens beperkt is tot die gegevens die vanaf het eerstgenoemde geautomatiseerd werk, dat wordt onderzocht, rechtmatig kunnen worden bereikt.

Bij een netwerkzoeking die wordt uitgevoerd op grondslag van artikel 125j Sv, kan het voorkomen dat in een geautomatiseerd werk van een ander gegevens worden vastgelegd. Een vraag die met een dergelijke doorzoeking wordt opgeroepen is of van het enkele onderzoek melding dient te worden gemaakt aan die derde. In ieder geval dient mededeling te worden gedaan indien gegevens daadwerkelijk zijn vastgelegd of in het geval deze ontoegankelijk zijn gemaakt.⁴⁹

Grensoverschrijdend onderzoek

Uit bovenstaande komt naar voren dat gegevens kunnen worden vastgelegd in het kader van de bevoegdheid tot doorzoeking van plaats ter vastlegging van gegevens. Daarbij verdienen nog enkele aspecten die aan de inzet van deze bevoegdheden verbonden kunnen zijn, nadere aandacht.

⁴⁸ *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 12.

⁴⁹ Zo volgt uit artikel 125m lid 1 Sv.

Dat betreft de mogelijkheid dat bij netwerkzoeking, zoals bedoeld in de bepaling van artikel 125j Sv, gegevens worden vastgelegd die zich niet op het Nederlands grondgebied bevinden. Dat laatste zou mee kunnen brengen dat daarmee de soevereiniteit van de staat, waar dat ‘elders aanwezige geautomatiseerde werk’ zich bevindt, wordt geschonden. Met het opslaan van gegevens in netwerken (zoals de cloud) is bovendien niet zonder meer duidelijk in welk land de desbetreffende gegevens feitelijk zijn opgeslagen. Bij opslag van gegevensbestanden in de cloud zijn bestanden vaak in deeltjes opgeknipt en verspreid over verschillende servers opgeslagen. Dat brengt mee dat het antwoord op de vraag in welk land de gegevens liggen opgeslagen niet altijd eenvoudig te beantwoorden is.⁵⁰

Uit de wetsgeschiedenis blijkt dat in beginsel geen onderzoek mag worden verricht in een computersysteem dat zich kennelijk in het buitenland bevindt. De persoon die het onderzoek verricht moet zich afvragen of het geautomatiseerde werk waarin hij tijdens een netwerkzoeking onderzoek doet als hij daartoe het geautomatiseerde werk betreedt en eventueel daarop aanwezige gegevens vastlegt, binnen zijn bevoegdheid valt.⁵¹ Dat is anders indien op grond van een verdrag dergelijke grensoverschrijdende handelingen zijn toegelaten.⁵² Een voorbeeld van zo’n verdrag vormt het Cybercrimeverdrag.⁵³

Voor een grensoverschrijdende onderzoekshandeling is een grondslag te vinden in artikel 32b van dat Cybercrimeverdrag. In dat artikel wordt bepaald dat de grensoverschrijdende toegang tot data in ieder geval is toegestaan indien het gaat om publiekelijk toegankelijke data (open bronnen) of wanneer toestemming is verkregen van de persoon die gerechtigd is de desbetreffende gegevens te verstrekken.

Notificatieplicht

Op grond van artikel 125m Sv dient, indien een doorzoeking van een plaats ter vastlegging van gegevens leidt tot het vastleggen of ontoegankelijk maken van gegevens, hiervan zo spoedig mogelijk schriftelijk mededeling te worden gedaan aan de betrokkenen. Dit wordt ook wel de notificatieplicht genoemd. Conform artikel 125m lid 1 Sv kan deze mededeling achterwege blijven voor zover uitreiking daarvan redelijkerwijs niet mogelijk is. Dit brengt dus een zekere inspanningsverplichting voor de autoriteiten met zich. Er bestaat daarnaast een wettelijke mogelijkheid tot uitstel van deze notificatie (artikel 125m lid 2 Sv). Hiervoor heeft de wetgever concrete waarborgen gegeven in lid 2. Zo is deze bevoegdheid enkel toegekend aan de officier van justitie (of de rechter-commissaris als die doorzocht heeft) en alleen zolang het belang van het onderzoek zich tegen mededeling aan de betrokkene

⁵⁰ B.J. Koops e.a., *Misdaad en opsporing in de wolken, Knelpunten en kansen van cloud computing voor de Nederlandse opsporing*, Tilburg: TILT 2012, p. 57.

⁵¹ *Kamerstukken II 1989/90*, 21 551, nr. 3, p. 11.

⁵² *Kamerstukken II 1989/90*, 21 551, nr. 3, p. 12.

⁵³ Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronisch netwerken, Boedapest 23 november 2001, *Trb*, 2002, 18.

verzet. Lid 4 schrijft voorts voor dat mededeling aan een betrokkene achterwege kan blijven, indien de betrokkene de verdachte is en hij van de vastlegging of het ontoegankelijk maken van de gegevens op de hoogte komt door opneming in de processtukken.

2.6.1 Ontsleutelingsbevel

Uit het bepaalde in artikel 125k Sv volgt dat aan degene die daarvoor (vermoedelijk) de benodigde kennis heeft bevel mag worden gegeven toegang te verschaffen tot een geautomatiseerd werk, een deel daarvan of daarop aanwezige versleutelde gegevens, om het onderzoek daaraan mogelijk te maken. Dit bevel tot ontsleuteling kan worden gegeven bij een doorzoeking ter vastlegging van gegevens (toepassing van artikel 125i en 125j Sv).

Dat kan door het bevel te geven toegang te verschaffen tot het geautomatiseerde werk. Dat houdt onder meer het verstrekken van het wachtwoord door een medewerker van de ICT-ondersteuning in. Aan het bevel kan ook worden voldaan door het ter beschikking stellen van informatie met betrekking tot de wijze van versleuteling van bepaalde in het geautomatiseerde werk aangetroffen versleutelde gegevens(bestanden), zo valt uit het bepaalde in artikel 125k Sv af te leiden. Bij dat laatste kan worden gedacht aan decrypteren van gegevens(bestanden) die door middel van een encryptieprogramma versleuteld zijn. Het ontsleutelingsbevel wordt niet gegeven aan de verdachte. De verschoningsgerechtigde hoeft niet aan het bevel te voldoen: artikel 125k lid 3 Sv.

2.6.2 Gegevens waarover het professioneel verschoningsrecht zich uitstrekt

De hierboven reeds aangestipte regeling van doorzoeking van plaatsen ter vastlegging van op geautomatiseerde werken of elektronische gegevensdragers opgeslagen gegevens kent nadere regels met betrekking tot de geheimhouders. Die regeling is neergelegd in artikel 125l Sv. Daaruit volgt dat in beginsel geen onderzoek wordt gedaan naar gegevens, die zijn ingevoerd door of vanwege professioneel verschoningsgerechtigden voor zover hun plicht tot geheimhouding zich daarover uitstrekt. Dat wordt anders in het geval zij toestemming hebben gegeven tot een dergelijk onderzoek.⁵⁴

2.6.3 Gegevens bij de aanbieder van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst

In artikel 125la Sv is in het kader van de doorzoeking van een plaats ter vastlegging van gegevens bepaald dat indien bij een dergelijke doorzoeking bij een aanbieder van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst gegevens worden aangetroffen welke niet voor deze bestemd zijn of afkomstig zijn, de officier van

⁵⁴ Artikel 125l Sv.

justitie slechts kan bepalen dat van deze gegevens wordt kennisgenomen en dat deze worden vastgelegd in het geval zij klaarblijkelijk van de verdachte afkomstig zijn, voor hem bestemd zijn, op hem betrekking hebben of tot het begaan van het strafbare feit hebben gediend. Bovendien heeft de officier van justitie voor het geven van deze beslissing een voorafgaande, schriftelijke machtiging van de rechter-commissaris nodig.

Dat brengt mee dat opsporingsinstanties in het geval een doorzoeking van een plaats ter vastlegging van gegevens bij de aanbieder van een communicatiedienst plaatsvindt, alleen die gegevens zullen mogen vastleggen die klaarblijkelijk van de verdachte afkomstig zijn, voor hem bestemd zijn, op hem betrekking hebben of tot het begaan van het strafbare feit hebben gediend. Zonder voorafgaande machtiging van de rechter-commissaris is het kennisnemen, maar ook het vastleggen van dergelijke gegevens niet toegelaten.

Dat kennisneming of vastlegging van gegevens die zijn opgeslagen bij de aanbieder van een communicatiedienst en die niet voor deze zijn bestemd of van deze afkomstig zijn van extra waarborgen zijn voorzien blijkt ook uit het feit dat een machtiging van de rechter-commissaris is vereist voor het vorderen van dergelijke gegevens bij de aanbieder (artikel 126ng lid 2 en lid 4 Sv).⁵⁵

Voor de situatie dat bij de aanbieder van een communicatiedienst gegevensdragers of geautomatiseerde werken zijn in beslag genomen waarop gegevens zijn opgeslagen die niet voor deze bestemd of van deze afkomstig zijn, heeft de wetgever geen bijzondere bepalingen in de wet opgenomen.

2.6.4 Bewaren en vernietigen van gegevens die tijdens een doorzoeking van een plaats ter vastlegging van gegevens zijn vergaard

In het geval de gegevens zijn verkregen in het kader van een doorzoeking van een plaats ter vastlegging van gegevens dienen de vastgelegde gegevens op grond van artikel 125n Sv te worden vernietigd, zodra duidelijk wordt dat zij van geen betekenis zijn voor het onderzoek.

De vernietiging kan achterwege blijven met het oog op andere doeleinden. Indien onder de vastgelegde gegevens, gegevens worden aangetroffen die van belang kunnen zijn voor een ander strafrechtelijk onderzoek dan kan de vernietiging op grond van dezelfde wetsbepaling achterwege blijven en kunnen die gegevens voor een ander strafrechtelijk onderzoek worden gebruikt. In dat geval hoeven de gegevens pas te worden vernietigd na afronding van dat andere onderzoek.⁵⁶ Daarnaast kan de officier van justitie bepalen dat

⁵⁵ Die extra waarborgen houden verband met het feit dat, net zoals bij de briefpost, ook bij e-mail geldt dat die niet zomaar bij het bedrijf dat voor de overbrenging zorg draagt kan worden opgehaald (vgl. artikel 100 Sv). G.J.M. Corstens & M.J. Borgers, *Het Nederlands strafprocesrecht*, Deventer: Wolters Kluwer 2014, p. 574.

⁵⁶ Artikel 125n lid 3 en lid 4 Sv.

gegevens niet worden vernietigd, maar worden verwerkt⁵⁷ met het oog op het verkrijgen van inzicht in de betrokkenheid van personen bij misdrijven en handelingen als bedoeld in lid 1, onderdelen a en b, van artikel 10 van de Wet politiegegevens (hierna: Wpg).

2.7 Wet bescherming persoonsgegevens en Wet politiegegevens

In zijn algemeenheid geldt dat op de verwerking van persoonsgegevens de Wet bescherming persoonsgegevens (hierna: Wbp) van toepassing is. De Wbp is echter niet van toepassing op de verwerking van persoonsgegevens ten behoeve van de uitvoering van de politietaak, bedoeld in de artikelen 3 en 4, lid 1, van de Politiewet 2012.⁵⁸ Deze uitzondering op de werkingssfeer van de Wbp is opgenomen in artikel 2 lid 2 onder c. van die wet. De verwerking van persoonsgegevens die zijn vergaard in het kader van de politietaak vallen onder het regime van de Wpg. Met betrekking tot politiegegevens geldt dat zij slechts worden verwerkt voor zover dit noodzakelijk is voor de bij of krachtens de Wpg opgesomde doeleinden (artikel 3 lid 1 Wpg). De bepalingen in artikelen 8, 9 en 10 Wpg werken die doeleinden concreter uit. Het betreft dan de verwerking van gegevens met het oog op de uitvoering van de dagelijkse politietaak (artikel 8 Wpg), verwerking van gegevens in het kader van een onderzoek met het oog op de handhaving van de rechtsorde in een bepaald geval (artikel 9 Wpg) en de verwerking van gegevens met het oog op het verkrijgen van inzicht in de betrokkenheid van personen bij het plegen of beramen van misdrijven die door hun omvang of ernst of hun samenhang met andere misdrijven een ernstig gevaar voor de rechtsorde opleveren of bij handelingen die, gezien hun aard of frequentie of het georganiseerde verband waarin zij worden gepleegd, een ernstige schending van de openbare orde vormen (artikel 10 Wpg). Andere gronden voor verwerking kent de Wpg niet.

De Wpg en de daarop gebaseerde lagere regelgeving bevatten tevens regels over bewaartermijnen⁵⁹ en het ter beschikking stellen van politiegegevens.⁶⁰ De vergaarde gegevens worden vernietigd zodra zij niet langer noodzakelijk zijn voor de uitvoering van de dagelijkse politietaak,⁶¹ de gegevens niet langer noodzakelijk zijn voor het doel van het

⁵⁷ Met verwerken in de Wet Politiegegevens wordt elke handeling of elk geheel van handelingen met betrekking tot politiegegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, vergelijken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van politiegegevens, zie artikel 1, onder c. Wpg.

⁵⁸ De politietaak omvat volgens artikel 3 Politiewet 2012 het in ondergeschiktheid aan het bevoegd gezag en in overeenstemming met de geldende rechtsregels zorgen voor de daadwerkelijk handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven. Artikel 4 lid 1 Politiewet 2012 draagt een aantal daar genoemde politietaken op aan de Koninklijke marechaussee.

⁵⁹ Artikel 14 Wpg.

⁶⁰ Artikel 15 Wpg.

⁶¹ Artikel 8 lid 6 Wpg.

onderzoek⁶² of de gegevens niet langer noodzakelijk zijn voor het doel van de verwerking.⁶³ In beginsel worden de verwijderde politiegegevens gedurende een termijn van vijf jaar bewaard ten behoeve van de verwerking met het oog op de afhandeling van klachten en de verantwoording van verrichtingen en vervolgens, na die vijf jaar, vernietigd.⁶⁴ In bijzondere gevallen kunnen de op grond van lid 3 en lid 4 van artikel 14 Wpg verwijderde gegevens opnieuw gebruikt worden of kan van vernietiging worden afgezien.⁶⁵ De verantwoordelijke stelt de gegevens ter beschikking aan de opsporingsambtenaren die zijn geautoriseerd voor de verwerking van politiegegevens voor zover zij deze behoeven voor de uitvoering van hun taak.⁶⁶

2.8 Het Europees Verdrag voor de Rechten van de Mens

Inbeslagneming van voorwerpen en onderzoek aan in beslag genomen elektronische gegevensdragers en geautomatiseerde werken ten behoeve van de opsporing en vervolging van strafbare feiten raakt, zoals zoveel opsporingsmethoden, ook aan de bescherming van het recht op privéleven. Er kan sprake zijn van een inbreuk op dat recht van de gebruiker van het voorwerp of van derden, bijvoorbeeld degene op wie bepaalde gegevens betrekking hebben. Zodanige inbreuk kan door een wettelijke bevoegdheid zijn gelegitimeerd.

De voornaamste in het geding zijnde verdragsbepaling is die van artikel 8 EVRM.⁶⁷ Dit is een breed en veelomvattend mensenrecht, waarvan hier de relevante aspecten verkend worden.

Artikel 8 lid 1 EVRM bepaalt dat een ieder het recht heeft op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie. Volgens lid 2 is inmenging in de uitoefening van dit recht niet toegelaten, anders dan voor zover bij wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede

⁶² Artikel 9 lid 4 Wpg.

⁶³ Artikel 10 lid 6 Wpg.

⁶⁴ Artikel 14 lid 1 Wpg.

⁶⁵ Zie ten aanzien van de bewaartermijnen en naleving daarvan de privacy-audit die de Auditdienst Rijk (ADR) heeft uitgevoerd. *Kamerstukken II*, 2015/16, 33 842, nr. 3 en bijlage en J. Smits e.a., *Glazen privacy. Knelpuntenonderzoek uitvoering Wet politiegegevens (Wpg)*, Deventer/Groningen: Arena Consulting/Pro Facto (WODC) 2013. Zie *Kamerstukken II* 2005/06, 30327, nr. 3, p. 3. Zie ook J.B.J. van der Leij, 'De staat van onze informatieve privacy binnen het domein van opsporing, vervolging en berechting van strafbare feiten', *Strafblad* 2014/42, afl. 4, p. 271-277.

⁶⁶ Artikel 15 lid 1 Wpg.

⁶⁷ Artikel 8 EVRM luidt:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

zeden of voor de bescherming van de rechten en vrijheden van anderen. Het tweede lid stelt daarmee verschillende eisen waaraan de – in de woorden van artikel 8 lid 2 – ‘inmenging van enig openbaar gezag in de uitoefening van dit recht’ (van artikel 8 lid 1) moet voldoen. Het artikellid benoemt de gevallen waarin een inmenging in het privéleven is toegelaten en schrijft de waarborgen voor waaraan de inmenging moet voldoen. Met deze eisen beschermt artikel 8 lid 2 de burger tegen willekeurige inmenging door de overheid in het privéleven.

Artikel 8 lid 1 EVRM spreekt van privéleven, familie- en gezinsleven, woning en correspondentie. De laatste vier belangen worden gezien als uitwerking van privéleven (dat ook nog meer kan omvatten). ‘Correspondentie’ kan ook volgens het EHRM worden opgevat als ‘communicatie’.⁶⁸

Het begrip ‘privéleven’ vormt een zeer complex begrip. Een eenduidige definitie van wat het beschermde rechtsgoed omvat, is niet eenvoudig te geven. Het EHRM heeft in de jaren negentig reeds overwogen dat het onmogelijk en waarschijnlijk zelfs ongewenst is om het begrip ‘privacy’ uitputtend te definiëren.⁶⁹ Of het privéleven door bepaald overheidsoptreden wordt geraakt, moet van geval tot geval worden bekeken.

Het verkrijgen van gegevens door onder meer het in beslag nemen van gegevensdrager en geautomatiseerde werken en het daarbij behorende onderzoek naar gegevens teneinde die beschikbaar te krijgen dan wel het doorzoeken van plaatsen ter vastlegging van gegevens, betekent normaliter een inbreuk op het recht van artikel 8 lid 1 EVRM. Dat geldt ook voor het verkrijgen van gegevens uit handen van derden.⁷⁰ Deze handelingen brengen het optreden van de overheid binnen de reikwijdte van artikel 8 lid 1 EVRM.

Een inbreuk op artikel 8 lid 1 EVRM levert als gezegd geen schending van het EVRM op als deze inbreuk door artikel 8 lid 2 wordt gelegitimeerd. De voorwaarden voor legitieme inmenging in het recht moeten terughoudend worden uitgelegd. Elke inbreuk op het recht op privéleven dient ‘in accordance with the law’ te zijn (in *Trb.* 1951, 154 vertaald als ‘bij de wet voorzien’). De overheid mengt zich als uitgangspunt niet in het persoonlijke leven van de individuele burgers, tenzij daarvoor goede redenen bestaan en de inmenging op grond van de wettelijk bevoegdheid met voldoende waarborgen omkleed plaatsheeft.⁷¹ Het Hof oordeelt van geval tot geval of voor een eventuele inbreuk op het recht op eerbiediging van het recht op privéleven voldoende legitimering bestaat. Bij de beoordeling of aan de verschillende, hierna te bespreken voorwaarden van artikel 8 lid 2 EVRM is voldaan, toetst

⁶⁸ Zie o.a. EHRM 24 april 1990, 11801/85 (*Kruslin/Frankrijk*), par. 26. Zie ook EHRM 6 september 1978, 5029/71 (*Klass & anderen/Duitsland*), par. 41: “Although telephone conversations are not expressly mentioned in paragraph 1 of Article 8 (art. 8-1), the Court considers, as did the Commission, that such conversations are covered by the notions of “private life” and “correspondence” referred to by this provision.”

⁶⁹ EHRM 16 december 1992, *Publ. ECHR, Series A, vol. 251-B (Niemiets/Duitsland)*, par. 29.

⁷⁰ J.B.J. van der Leij, *Privacyrecht en slachtoffers*, Den Haag: Boom 2015, p. 51.

⁷¹ B.J. Koops & A.H. Vedder, *Opsporing versus Privacy*, Den Haag: SDU-uitgevers 2015, p. 22.

het EHRM ook of aan genoemde voorwaarden in samenhang en onderling verband is voldaan.

Artikel 8 lid 2 EVRM stelt drie belangrijke voorwaarden. Dat betreft de voorwaarde van een wettelijke basis ('in accordance with the law'), de voorwaarde van een 'legitimate aim' en de voorwaarde dat de inbreuk 'necessary in a democratic society' is.

In accordance with the law

Volgens het Europese Hof stelt de voorwaarde van 'in accordance with the law' vier nadere eisen.⁷²

De belangrijke waarborg dat de inbreuk 'in accordance with the law' moet zijn, betekent volgens het EHRM in de eerste plaats dat de inbreuk een basis moet hebben in het nationale recht. Dat kan volgens het EHRM zowel geschreven als ongeschreven recht betreffen. Het geschreven recht is niet beperkt tot recht afkomstig van de nationale overheid, maar kan ook van lagere wetgevers komen. Wetten in formele zin, materiele zin, algemene maatregelen van bestuur en gepubliceerde beleidsregels van het Openbaar Ministerie⁷³ zijn hieronder te scharen, mits voor de burger voldoende kenbaar.⁷⁴ Het EHRM toetst dit slechts marginaal; het is vooral aan de nationale autoriteiten om nationaal recht toe te passen.⁷⁵

Vervolgens hecht het EHRM in het bijzonder aan de 'toegankelijkheid' (*accessibility*) van de bepaling, die de inbreuk op dat recht legitimeert,⁷⁶ en de 'voorzienbaarheid' (*foreseeability*)⁷⁷ van de inbreuk. De burger moet de mogelijkheid hebben de toepasselijke regelgeving te kennen; hij moet er kennis van kunnen hebben. Bovendien moet de burger kunnen voorzien wat de consequenties voor hem zijn. Hij moet kunnen voorzien onder welke omstandigheden door de overheid een inbreuk kan worden gemaakt op zijn recht op bescherming van zijn privéleven. In het kader van die laatste eis moet de regelgeving ('law') met voldoende precisie zijn geformuleerd. Met name die eis van precisie staat in het licht

⁷² Zie bijvoorbeeld de hierna te bespreken zaak EHRM 30 september 2014, 8429/05 (*Prezhdarovi/Bulgarije*), par. 43: "The Court notes that the expression "in accordance with the law", within the meaning of Article 8 § 2 requires firstly that the impugned measure should have some basis in domestic law. Second, the domestic law must be accessible to the person concerned. Third, the person affected must be able, if need be with appropriate legal advice, to foresee the consequences of the domestic law for him, and fourth, the domestic law must be compatible with the rule of law."

⁷³ Voor deze laatste categorie moet voldaan zijn aan de eisen die de Hoge Raad stelt aan artikel 79 Wet RO. Zie: HR 19 juni 1990, ECLI:NL:HR:1990:ZC8556, NJ 1991, 119 m.nt. Th.W. van Veen en M. Scheltema en recent HR 26 april 2011, ECLI:NL:HR:2011:BO4015, NJ 2012, 63 m.nt. B.F. Keulen.

⁷⁴ G.J.M. Corstens & M.J. Borgers, *Het Nederlands strafprocesrecht*, Deventer: Wolters Kluwer 2014, p. 316.

⁷⁵ J.B.J. van der Leij, *Privacyrecht en slachtoffers*, Den Haag: Boom 2015, p. 60.

⁷⁶ Zie hiervoor EHRM 29 april 2003, 39042/97 (*Kuznetsov/Oekraïne*), EHRM 1 juli 2008, 58243/00 (*Liberty/het Verenigd Koninkrijk*), maar ook EHRM 15 mei 2012, 49458/06 (*Colon/Nederland*).

⁷⁷ Zie daarvoor onder meer EHRM 24 april 1990, 11801/85 (*Kruslin/Frankrijk*), EHRM 2 augustus 1984, 8691/79 (*Malone/het Verenigd Koninkrijk*), EHRM 29 juni 2006, 54934/00 (*Weber & Saravia/Duitsland*) en EHRM 25 maart 1998, 13/1997/797/1000 (*Kopp/Zwitserland*).

van de strekking van artikel 8 EVRM: de bescherming tegen willekeurige inbreuk op het recht op privéleven. In de eisen die het EHRM aan die ‘precisie’ stelt (er zijn geen algemene regels of nadere eisen) laat het Hof ruimte voor ‘changing circumstances’. Voorts is van belang dat de eisen van precisie verschillen, al naar gelang de aard van de inbreuk. Aan de regels met betrekking tot het afluisteren van telefoons lijken de hoogste eisen van precisie te worden gesteld.

Legitimate aim

Zoals hiervoor gezegd geldt naast de eis van ‘in accordance with the law’ de eis van ‘legitimate aim’ en ‘necessary in a democratic society’. De in artikel 8 lid 2 genoemde doelen die een inbreuk kunnen rechtvaardigen zijn zo algemeen (zoals het voorkomen van strafbare feiten en het beschermen van de rechten en vrijheden van anderen), dat bij strafvorderlijke wetgeving niet snel sprake zal zijn van een niet door artikel 8 lid 2 EVRM gerechtvaardigde inbreuk op het recht van artikel 8 lid 1 EVRM.

Necessary in a democratic society

De eis van ‘necessary in a democratic society’ raakt aan de proportionaliteit van de (in de wet (*law*) geregelde inbreuk. Bij deze afweging van belangen laat het EHRM een – enigszins naar aard van de materie in reikwijdte verschillende – ‘margin of appreciation’ aan de lidstaten.⁷⁸

Het Hof toetst of meer algemeen sprake is van een dringende maatschappelijke behoefte (*pressing social need*) aan de regeling en of die regeling gelet op de na te streven doelen proportioneel is.⁷⁹ Onder dit criterium wordt ook getoetst of de toepassing van een bevoegdheid in concreto proportioneel was. Het Hof laat aan de lidstaten een zekere ‘margin of appreciation’, die evenwel kleiner is als er kernonderdeel van het bestaan of de identiteit van het individu op het spel staan. Bij de afweging is ook van belang of er vooraf of achteraf procedurele waarborgen bestaan die er mede voor zorgen dat geen sprake is van een willekeurige inbreuk op het privéleven of misbruik van bevoegdheid. Het Hof toetst of van een effectieve waarborg sprake is.⁸⁰

In het kader van dit onderzoek kan nog worden gewezen op de uitspraak van het EHRM in de zaak *Prezhdarovi* tegen Bulgarije.⁸¹ In deze zaak vond op bevel van de officier van justitie een doorzoeking van een bedrijfspand plaats waarbij een aantal computers in beslag genomen werd. De beslagene had verschillende malen verzocht om teruggave van de computers, onder andere omdat zich daarop persoonlijke gegevens bevonden. Het Hof

⁷⁸ EHRM 15 mei 2012, 49458/06 (*Colon/Nederland*), par. 86 en 87.

⁷⁹ J.B.J. van der Leij, *Privacyrecht en slachtoffers*, Den Haag: Boom 2015, p. 65.

⁸⁰ Zie de hierna te bespreken beslissing, EHRM 30 september 2014, 8429/05 (*Prezhdarovi/Bulgarije*), par. 49.

⁸¹ EHRM 30 september 2014, 8429/05 (*Prezhdarovi/Bulgarije*).

stelt vast dat geen rechterlijke toetsing voorafgaand aan de doorzoeking en inbeslagneming van de computers heeft plaatsgevonden (geen ‘prior judicial warrant’) en benadrukt dat dit gemis dan kan worden gecompenseerd door adequate rechterlijke toetsing achteraf om schending van artikel 8 te voorkomen. Die toetsing achteraf dient te zijn voorzien van voldoende waarborgen zodat het recht op bescherming van privéleven niet wordt geschonden.⁸² Het Hof stelt vooraf vast dat het nationale recht geen bepalingen bevat over de reikwijdte van de rechterlijke toetsing en baseert zijn oordeel dus op de motivering die de nationale rechter naar aanleiding van het verzoek om teruggave van de computers heeft gegeven. Daarbij merkt het Hof nog op dat de reikwijdte van een doorzoeking en daaropvolgende inbeslagneming een relevante factor is bij de beoordeling of de maatregel in overeenstemming is met artikel 8 EVRM. Het Hof komt tot het oordeel dat die rechterlijke toetsing achteraf onvoldoende was. Het Hof overwoog hieromtrent dat in beginsel het onder zich houden van gegevensdragers gedurende een strafrechtelijk onderzoek met het oog op de waarheidsvinding als bevoegdheid is toegelaten.⁸³ Echter, het feit dat bij de rechterlijke toetsing achteraf geen onderscheid is gemaakt tussen gegevens die voor het onderzoek van belang zijn en niet-relevante gegevens en motivering omtrent de relevantie van de in beslag genomen gegevens voor het onderzoek ontbrak, in samenhang met het feit dat de rechter niet is ingegaan op de klacht dat op de computers persoonlijke gegevens stonden, bracht met zich mee dat de rechterlijke toetsing formalistisch was. De omstandigheid dat voor de doorzoeking en inbeslagneming geen rechterlijke toets vooraf nodig was en een betekenisvolle rechterlijke toets achteraf ontbrak, bracht het Hof tot de vaststelling dat in het onderhavige geval sprake was van schending van artikel 8 EVRM.⁸⁴

Mocht sprake zijn van een schending van artikel 8 EVRM, dan levert het gebruik van daarmee verkregen bewijsmateriaal in een strafzaak volgens het EHRM niet zonder meer een schending op van artikel 6 EVRM, inzake de bescherming van het recht op een eerlijk proces⁸⁵

⁸² EHRM 30 september 2014, 8429/05 (*Prezhdarovi/Bulgarije*), par 45-47.

⁸³ EHRM 30 september 2014, 8429/05 (*Prezhdarovi/Bulgarije*), par. 49: “While the Court accepts that, as a matter of principle, the retention of the computers for the duration of the criminal proceedings pursues the legitimate aim of securing physical evidence in an ongoing criminal investigation.”

⁸⁴ EHRM 30 september 2014, 8429/05 (*Prezhdarovi/Bulgarije*), par. 50: “In conclusion, the Court finds that the lack of clear rules regarding the scope of the judicial review in such a situation, combined with the lack of any meaningful review of the lawfulness of and the justification for the measure, rendered the *post factum* judicial review ineffective for the purposes of the protection of the applicants’ rights as guaranteed by Article 8 of the Convention.”

⁸⁵ EHRM 1 juni 2010, 22978/05 (*Gäfgen/Duitsland*), par. 165. Zie ook par. 137 uit de ‘Guide On Article 6’: “As to the examination of the nature of the Convention violation found, the question whether the use as evidence of information obtained in violation of Article 8 rendered a trial as a whole unfair contrary to Article 6 has to be determined with regard to all the circumstances of the case, and in particular to the question of respect for the applicant’s defence rights and the quality and importance of the evidence in question”. (http://www.echr.coe.int/Documents/Guide_Art_6_criminal_ENG.pdf) Ook de Hoge Raad verwijst in HR 7 juli 2009, ECLI:NL:HR:2009:BH8889, NJ 2009, 399 naar deze opvatting van het EHRM.

Uit het bovenstaande komt als voornaamste aandachtspunt de vraag naar voren of het Nederlandse recht op het punt van onderzoek aan in beslag genomen voorwerpen voldoet aan de eisen die het EHRM aan het nationale recht stelt bij de beoordeling of sprake is van een beperking van het privéleven ‘in accordance with the law’.

Deze vraag is recent in een aantal beslissingen van Nederlandse rechters aan de orde geweest. Die jurisprudentie wordt hierna in paragraaf 2.10 nader besproken.

2.9 Grondwettelijke bescherming

Sinds 1983 is de bescherming van de persoonlijke levenssfeer als grondrecht opgenomen in artikel 10 van de Grondwet.⁸⁶ De bescherming die het grondwetsartikel biedt, is net zo min absoluut als de bescherming geboden door artikel 8 EVRM. Beperkingen op dit recht zijn mogelijk. De bepaling spreekt in dat kader in artikel 10 lid 1 Grondwet over ‘behoudens bij of krachtens de wet’ te stellen beperkingen. Er is met andere woorden een formeel-wettelijke grondslag vereist om een inbreuk te maken op het grondrecht, maar de beperking zelf hoeft volgens artikel 10 lid 1 Grondwet⁸⁷ niet in een wet formele zin te staan; delegatie van de beperkingsbevoegdheid is geoorloofd.

In artikel 10 lid 2 Grondwet is bepaald dat de wet regels stelt ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens. Met persoonsgegevens worden gegevens bedoeld die zijn te herleiden tot te identificeren of identificeerbare natuurlijke personen.⁸⁸ In artikel 10 lid 3 Grondwet is bepaald dat bij wet regels worden gesteld inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens. In het kader van dit onderzoek zijn de in paragraaf 2.7 genoemde, Wbp en de Wpg als belangrijkste wetten aan te merken die hieraan uitvoering geven.

Voor de problematiek die in dit onderzoek centraal staat kan worden gezegd dat artikel 10 Grondwet geen nadere beoordelingscriteria oplevert die niet ook reeds op basis van het

⁸⁶ Artikel 10 Grondwet, luidt:

1. Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer.
2. De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens.
3. De wet stelt regels inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens.

Het artikel spreekt van ‘de persoonlijke levenssfeer’. Artikel 8 lid 1 EVRM spreekt van ‘privéleven’. Beide begrippen verschillen inhoudelijk niet.

⁸⁷ Op grond van artikel 1 Sv ligt dat anders.

⁸⁸ Artikel 1 onder a. Wbp.

EVRM-recht hiervoor zijn beschreven. Hooguit is het zo dat het wetsbegrip in de Nederlandse Grondwet beperkter is: het omvat niet jurisprudentie of ongeschreven recht.

Wel is het zo dat zeer geringe inbreuken zonder specifieke, afzonderlijke wettelijke legitimering toelaatbaar worden geacht in de zin van ‘bij of krachtens de wet bepaald’, op basis van wettelijke bepalingen met een algemene, taakstellende inhoud, zoals artikel 3 Politiewet 2012 of artikel 141 Sv. Daarin kan onder omstandigheden een rechtvaardiging worden gevonden voor geringe inbreuken op de persoonlijke levenssfeer, zoals de niet-stelselmatige observatie van een persoon. Voor zover daarbij (geringe) inbreuken worden gemaakt op de persoonlijke levenssfeer zijn zij ‘bij of krachtens de wet bepaald’ in de zin van artikel 10 lid 1 Grondwet.⁸⁹

2.10 Recente ontwikkelingen in verband met nader onderzoek aan in beslag genomen elektronische gegevensdragers of geautomatiseerde werken

Dat de wet geen nadere regels stelt voor het onderzoek naar de op de in beslag genomen voorwerpen aanwezige gegevens, betekent niet per definitie, dat daarmee kan worden gezegd dat de inbreuk door het onderzoek aan die voorwerpen om de gegevens ter beschikking te krijgen, niet voldoende genormeerd is, maar er worden in onder meer de rechtspraak wel vraagtekens bij geplaatst. Zoals in de inleiding reeds is vermeld, is in de lagere rechtspraak op dit punt verschillende uitleg gegeven aan de reikwijdte van de bevoegdheden tot inbeslagneming van voorwerpen.

In dat kader kan in chronologische volgorde in eerste plaats worden verwezen naar een arrest van het Hof Arnhem-Leeuwarden.⁹⁰ In deze zaak heeft de verdediging aangevoerd dat het door de politie verrichte onderzoek aan een smartphone een vormverzuim in de zin van artikel 359a Sv oplevert. Volgens de verdediging moest dat verzuim leiden tot bewijsuitsluiting dan wel strafvermindering. De verdediging voert daartoe aan dat de werkwijze van de politie, te weten: de inbeslagneming van een smartphone in het kader van de waarheidsvinding, weliswaar conform de wettelijke bepalingen was toegelaten, maar dat deze wettelijke bepalingen niet meer op de feitelijke maatschappelijke situatie zijn toegespitst. In die actuele maatschappelijke situatie is volgens de verdediging een smartphone aan te merken als een bron van opslag van gegevens die betrekking hebben op het gehele persoonlijke leven van de gebruiker daarvan. Daaruit volgt volgens de verdediging dat de opsporing met betrekking tot de smartphone van de verdachte handelingen heeft verricht, die een inbreuk op de rechten van verdachte op eerbiediging

⁸⁹ J.S. Nan, *Vormverzuimen in het voorbereidend onderzoek*, Praktijckahiers Strafrecht deel 9, Den Haag: Sdu uitgevers 2015, p. 6 en 7.

⁹⁰ Hof Arnhem-Leeuwarden 22 april 2015, ECLI:NL:GHARL:2015:2954, www.sr-updates.nl, SR 2015-0215, m.nt. P.C. Verloop.

van zijn privéleven en correspondentie met zich brengen. De verdediging betoogt dat voor een rechtvaardiging van deze inbreuk weliswaar een basis in artikel 94 Sv kan worden gevonden, maar dat deze bevoegdheid geen nadere basis biedt voor het verrichten van onderzoek aan de in beslag genomen smartphone. Hierdoor schiet, zo stelt de verdediging, de Nederlandse regelgeving tekort in het bieden van een redelijke begrenzing van de onderzoeksbevoegdheid van de politie, met name tot hetgeen noodzakelijk en proportioneel is. Op die manier is feitelijk sprake is van een onbegrensde onderzoeksbevoegdheid van de politie, hetgeen strijdig is met het bepaalde in artikel 8 EVRM. Bovendien is volgens de verdediging sprake van strijdigheid met die bepaling omdat een voorafgaande rechterlijke machtiging of rechterlijk bevel tot onderzoek aan de smartphone ontbrak en het door de politie verrichte onderzoek aan de smartphone niet noodzakelijk noch proportioneel was, gelet op de aard van de verdenking, de concrete omstandigheden van het geval en het voorhanden zijnde bewijsmateriaal.

Het Hof Arnhem-Leeuwarden onderschrijft in zijn arrest het standpunt van de verdediging in die zin dat de verdachte ten aanzien van de inhoud van zijn smartphone een beroep op bescherming op artikel 8 EVRM (en artikel 10 Grondwet) toekomt. Het Hof oordeelt dat de inbeslagneming, het onderzoek aan de smartphone en het lichten van gegevens van die smartphone door de politie op grond van artikel 94 Sv een inbreuk vormen op de bescherming van de persoonlijke levenssfeer. Het Hof overweegt daarbij dat de bevoegdheid van de politie tot het maken van een inbreuk op dit recht voldoende kenbaar en voorzienbaar dient te zijn omschreven in de wet. Zulks omdat naar de mening van het Hof via een smartphone niet slechts toegang wordt verkregen tot de verkeersgegevens, maar ook tot de inhoud van communicatie en privé-informatie van de gebruiker van de smartphone, zonder dat enige vorm van voorafgaande beoordeling van de subsidiariteit en/of proportionaliteit van de bevoegdheid plaatsvindt.

Gelet daarop oordeelt het Hof dat sprake is van een zodanig ingrijpende bevoegdheid dat, mede gelet op artikel 1 Sv, de algemene bevoegdheidsomschrijving van artikel 94 Sv heden ten dage niet meer kan worden aangemerkt als een wettelijk voorschrift dat als voldoende kenbaar en voorzienbaar kan worden aangemerkt bij de uitoefening van de verleende bevoegdheid en dus de toets van artikel 8 lid 2 EVRM niet (meer) kan doorstaan.

Het Hof oordeelt daarom dat het onderzoek door de politie aan de smartphone van de verdachte een schending van diens recht op privéleven oplevert en de verdachte in zijn belangen is getroffen, aangezien de uitwerking van gegevens uit die smartphone (in casu een WhatsApp-gesprek) aan het strafdossier was toegevoegd.

Dat het Hof Arnhem-Leeuwarden het verweer van de verdediging gegrond acht, maakt voor de uitkomst van de strafzaak uiteindelijk geen verschil aangezien het concrete onderzoeksresultaat geen onderdeel vormde van de bewijsconstructie van de tenlastegelegde gedraging. Desalniettemin acht het Hof dat de inbeslagneming, het

onderzoek aan de smartphone en het lichten van gegevens van die smartphone door de politie op grond van artikel 94 Sv een inbreuk vormen op de door artikel 8 EVRM verleende bescherming van de persoonlijke levenssfeer.

Het inhoudelijke oordeel over de reikwijdte van de bevoegdheid wordt gevolgd door de Rechtbank Noord-Holland in een vonnis van 4 juni 2015.⁹¹ In deze zaak wordt op het politiebureau zonder toestemming van de verdachte de inhoud van zijn smartphone bekeken, op grond van artikel 94 Sv. De rechtbank neemt de overwegingen van het Hof Arnhem-Leeuwarden over en is van oordeel dat het onderzoek door de politie aan de smartphone van de verdachte een schending van zijn recht op privéleven oplevert. De rechtbank volstaat, overigens in deze zaak, gelet op de factoren genoemd in artikel 359a lid 2 Sv, met constatering van het vormverzuim.

Andere beslissingen van lagere rechters bevatten echter een ander oordeel. Zo overweegt de rechtbank Limburg in een recent vonnis dat het verweer van de verdediging dat het door de verbalisant verrichte onderzoek aan de telefoon van verdachte onrechtmatig is vanwege schending van artikel 8 EVRM (en artikel 10 Grondwet), niet slaagt. De rechtbank overweegt daartoe dat de verdachte voorafgaand aan zijn verhoor door de politie overleg heeft gehad met zijn raadsman, vervolgens heeft hij in het verhoor vrijwillig de pincode van zijn telefoon kenbaar gemaakt. Zulks nadat hem door de verhorende verbalisanten was meegedeeld dat zijn telefoon in beslag genomen was en onderzocht zou worden en hem gevraagd was of hij wilde meewerken en zijn pincode wilde geven.

De rechtbank gaat er, gelet op de daarna gegeven pincode, vanuit dat verdachte met het onderzoek aan zijn telefoon heeft ingestemd. Daarom kan niet worden gezegd dat dit onderzoek ‘onrechtmatig’ is. De rechtbank merkt daarbij nog op dat het belang van de verdachte dat het gepleegde feit niet wordt ontdekt, niet kan worden aangemerkt als een rechtens te respecteren belang. De resultaten van het verrichte onderzoek kunnen derhalve als bewijs worden gebezigd.⁹² Opgemerkt moet worden dat in deze zaak het onderzoek aan het in beslag genomen voorwerp leunt op de instemming daarmee van de zijde van de verdachte. Als die toestemming voldoende vrijwillig is (informed consent) is naar vaste rechtspraak geen, door een wettelijke bepaling gelegitimeerde overheidsbevoegdheid noodzakelijk.⁹³

Daarnaast heeft de rechtbank Rotterdam in een mensensmokkelzaak ten aanzien van een verweer omtrent de wijze van verkrijging van sms’jes op een in beslag genomen en onderzochte smartphone, overwogen dat voorwerpen, die kunnen dienen om de waarheid aan de dag te brengen ingevolge het bepaalde in artikel 94 Sv in beslag kunnen worden genomen en dat artikel 96 Sv opsporingsambtenaren de bevoegdheid toekent om, in

⁹¹ Rb. Noord-Holland 4 juni 2015, ECLI:NL:RBNHO:2015:4660.

⁹² Rb. Limburg (zittingsplaats Maastricht) 5 juni 2015, parketnr. 03/659119-14.

⁹³ J.S. Nan, *Vormverzuimen in het voorbereidend onderzoek*, Praktijckahiers Strafrecht deel 9, Den Haag: Sdu uitgevers 2015, par. 2.7.

omschreven gevallen, daarvoor vatbare voorwerpen in beslag te nemen. De rechtbank overweegt dat uit die bepalingen niet kan worden afgeleid op welke wijze en onder welke voorwaarden het onderzoek aan in beslag genomen voorwerpen dient te worden uitgevoerd. De rechtbank overweegt vervolgens dat in zoverre dan ook een expliciete wettelijke basis ontbreekt voor het onderzoek naar de sms berichten en overige gegevens (zoals foto's en een contactlijst) in de in beslag genomen (smart)telefoon. De Rotterdamse rechtbank stelt dat daarmee echter niet is gezegd dat een belangrijk strafvorderlijk voorschrift met dergelijk onderzoek is geschonden en oordeelt dat, gelet op het doel en de reikwijdte van de genoemde bepalingen en de toepassing en invulling die daaraan sinds jaar en dag in de opsporings- en rechtspraak wordt gegeven, niet zonder meer kan worden gezegd dat dergelijk onderzoek strijd oplevert met enig wettelijk voorschrift of (verdragsrechtelijk) rechtsbeginsel.⁹⁴

Ook de rechtbank Oost-Brabant wees een vonnis waarin de verdediging met verwijzing naar bovengenoemd arrest van het Hof Arnhem-Leeuwarden een verweer voerde met betrekking tot schending van artikel 8 EVRM. De rechtbank overweegt dat alle voorwerpen die kunnen dienen om de waarheid aan de dag te brengen, op grond van artikel 134 jo. 94 Sv vatbaar zijn voor inbeslagneming en, met verwijzing naar de jurisprudentie van de Hoge Raad⁹⁵, dat voor de waarheidsvinding onderzoek mag worden gedaan aan en in het in beslag genomen voorwerp teneinde gegevens voor het strafrechtelijk onderzoek ter beschikking te krijgen. De rechtbank ziet geen aanknopingspunten om ten aanzien van de inhoud van een smartphone en laptop anders te oordelen. Met betrekking tot de inbreuk op artikel 8 EVRM ziet de rechtbank Oost-Brabant in weersprek van het beroep op het arrest van het Hof Arnhem-Leeuwarden door de verdediging, in artikel 94 Sv in samenhang met de uitleg daarvan door de Hoge Raad een voldoende duidelijke en voorzienbare wettelijke grondslag voor inbeslagneming en het daaropvolgende onderzoek in de smartphone en laptop van de verdachte.⁹⁶

Tevens kan worden gewezen op de uitspraak van de rechtbank Limburg van 28 oktober 2015.⁹⁷ Het standpunt van de verdediging is dat de gegevens opgeslagen in een smartphone onrechtmatig waren verkregen. De verdediging verwijst hierbij uiteraard naar de hiervoor besproken uitspraak van het gerechtshof Arnhem-Leeuwarden. De verdediging stelt zich op het standpunt dat de inhoud van een smartphone heden ten dage niet kan worden vergeleken met de inhoud van een computer in 2007. De rechtbank oordeelt dat voor de waarheidsvinding onderzoek mag worden gedaan in het in beslag genomen voorwerp teneinde gegevens voor het strafrechtelijk onderzoek ter beschikking te krijgen. De

⁹⁴ Rb. Rotterdam 4 juni 2015, ECLI:NL:RBROT:2015:4085.

⁹⁵ Het gaat om HR 20 februari 2007, ECLI:NL:HR:2007:AZ3564, NJ 2008, 113 m.nt. T.M. Schalken onder NJ 2008, 115 en HR 29 maart 1994, ECLI:NL:HR:1994:AD2076, NJ 1994, 537, m.nt. T.M. Schalken onder NJ 1994, 577.

⁹⁶ Rb. Oost-Brabant 5 juni 2015, ECLI:NL:RBOBR:2015:3228.

⁹⁷ Rb. Limburg 28 oktober 2015, ECLI:NL:RBLIM:2015:9128.

rechtbank gaat niet mee in het verweer van de verdediging dat hierbij onderscheid moet worden gemaakt tussen gegevens afkomstig van een computer of van een smartphone. De bepaling van artikel 94 Sv vormt een voldoende duidelijke en voorzienbare wettelijke grondslag, waardoor de inbreuk op artikel 8 EVRM gelegitimeerd is. Het betoog van de verdediging dat een voorafgaande rechterlijke machtiging is vereist voor het onderzoek naar de inhoud van een smartphone, zoals bij het openen van een in beslag genomen poststuk, heeft de rechtbank niet gevolgd.

In het arrest van het Hof Amsterdam van 17 september 2015⁹⁸ werd, het verweer gevoerd dat het onderzoek aan een smartphone een inbreuk op het bij artikel 8 EVRM gewaarborgde recht zou opleveren omdat niet slechts verkeersgegevens maar ook de inhoud van communicatie en privé-informatie van de gebruiker van de smartphone was verkregen. Het Hof Amsterdam verwierp het verweer met de overweging dat voor de waarheidsvinding onderzoek mag worden gedaan aan in beslag genomen voorwerpen teneinde gegevens voor het strafrechtelijk onderzoek ter beschikking te krijgen en dat in computers opgeslagen gegevens daarop geen uitzondering vormen.⁹⁹ Het Hof ziet geen reden ten aanzien van een smartphone anders te oordelen en overweegt nog eens expliciet dat artikel 94 Sv een voldoende duidelijke grondslag vormt voor de inbeslagneming en het daarop volgende onderzoek.

Tot slot dient nog worden gewezen op een ander arrest van het Hof Amsterdam,¹⁰⁰ en wel van 13 november 2015.¹⁰¹ Ook in dit arrest had de verdediging, onder verwijzing naar het arrest van het Hof Arnhem-Leeuwarden, aangevoerd dat onderzoek aan een in beslag genomen smartphone op grond van artikel 8 EVRM onrechtmatig is geweest omdat naast toegang tot verkeersgegevens ook de inhoud van communicatie en privé-informatie van de gebruiker van de smartphone is verkregen. De verdediging voert daartoe dat artikel 94 Sv een onvoldoende wettelijke grondslag biedt voor het ophalen van de gegevens die op de smartphone zijn opgeslagen. Daarom zou het ophalen van die opgeslagen gegevens een inbreuk vormen op het bij artikel 8 EVRM gewaarborgde recht op privéleven. De verdediging betoogde dat er sprake is van een ernstig vormverzuim als bedoeld in artikel 359a Sv, waaraan het gevolg moet worden verbonden dat al het bewijs dat door het uitlezen van de gegevens van de smartphone is verkregen, in het bijzonder de WhatsApp-berichten, van het bewijs moet worden uitgesloten.

Het Hof verwierpt ook hier het verweer en overweegt daartoe dat artikel 94 Sv bepaalt dat alle voorwerpen die aan de waarheidsvinding dienstbaar kunnen zijn vatbaar zijn voor inbeslagneming. Teneinde de waarheid aan het licht te brengen mag aan in beslag genomen

⁹⁸ Hof Amsterdam 17 september 2015, ECLI:NL:GHAMS:2015:4348.

⁹⁹ Met verwijzing naar het eerder genoemde HR 29 maart 1994, ECLI:NL:HR:1994:AD2076, *NJ* 1994, 537, m.nt. T.M. Schalken onder *NJ* 1994, 577.

¹⁰⁰ Met een andere samenstelling dan de samenstelling bij het eerder genoemde arrest van 17 september 2015, ECLI:NL:GHAMS:2015:4348.

¹⁰¹ Hof Amsterdam 13 november 2015, ECLI:NL:GHAMS:2015:5007.

voorwerpen onderzoek worden gedaan met het oog op het ter beschikking krijgen van gegevens voor het strafrechtelijk onderzoek. Gegevens die in computers zijn opgeslagen zijn daarvan niet uitgezonderd. Het Hof ziet dan ook geen reden om anders te oordelen ten aanzien van de gegevens die zijn opgeslagen in een smartphone. De smartphone van verdachte is volgens het Hof, in het kader van de waarheidsvinding, rechtmatig in beslag genomen en artikel 94 Sv vormt een voldoende duidelijk en voorzienbare wettelijke grondslag voor de inbeslagneming en het daaropvolgende onderzoek in de smartphone.

Het Hof oordeelde daarom dat er geen sprake is van een vormverzuim, zodat de WhatsApp-berichten kunnen dienen tot het bewijs.

Uit bovenstaande kan worden afgeleid dat de lagere rechtspraak over de inbeslagneming van en met name over het daarop volgende nader onderzoek aan elektronische gegevensdragers en geautomatiseerde werken verdeeld is. Dat geldt zowel op het niveau van de rechtbanken als op dat van de gerechtshoven.

3. Uitwerking en analyse van het onderzoek

3.1 Inleiding

In het voorgaande hoofdstuk is het juridisch kader van de inbeslagneming en het onderzoek aan in beslag genomen elektronische gegevensdragers en geautomatiseerde werken geschetst. Uit de in paragraaf 2.10 besproken lagere rechtspraak is naar voren gekomen dat de uitleg van die bepalingen voor zover dat betrekking heeft op het in beslag nemen van voorwerpen teneinde nader onderzoek te verrichten om de daarop vastgelegde gegevens ter beschikking te krijgen met het oog op de waarheidsvinding, niet eenduidig is.

Het onderhavige onderzoek dient om inzage te verwerven in de wijze waarop in de praktijk wordt omgegaan met de inbeslagneming van voorwerpen, voor zover die inbeslagneming betrekking heeft op nader onderzoek van de op de voorwerpen vastgelegde gegevens. In dit hoofdstuk wordt verslag gedaan van het praktijkonderzoek.

Diverse uit de interviews naar voren komende bevindingen worden per onderzoeksvraag geschetst. Hierbij is, om de anonimiteit van de respondenten te verzekeren, ervoor gekozen om bij de citaten enkel te verwijzen naar de functie van de betreffende respondent. Er worden drie functies onderscheiden: de officier van justitie, de opsporingsambtenaar (in alle rangen, zowel bij de politie als bij de Koninklijke marechaussee) en de opsporingsambtenaar werkzaam bij een bijzondere opsporingsdienst (waarbij in dit onderzoek wordt gedoeld op de respondenten van de FIOD).

In het onderhavige hoofdstuk wordt zowel bij de kwantitatieve als de kwalitatieve onderzoeksbevindingen stilgestaan. De bevindingen uit het onderzoek schetsen een concreet beeld van de wijze waarop in de praktijk wordt omgegaan met voorwerpen waarop op enigerlei wijze gegevens zijn vastgelegd en het nader onderzoek aan die voorwerpen. Het onderzoek naar die gegevens en de vastlegging en verwerking daarvan zijn in de interviews meegenomen. Ook is in de interviews gesproken over de betekenis van de aard van de verschillende gegevens(bestanden).

3.2 Kwantitatieve onderzoeksvragen

Met het oog op het verkrijgen van inzicht in de cijfers over onderzoeken aan in beslag genomen voorwerpen, teneinde de beschikking te krijgen over de daarop vastgelegde gegevens, is een aantal vragen aan de respondenten voorgelegd. Daarnaast zijn uit verschillende regio's cijfers verkregen die een beeld kunnen geven over de omvang van de toepassing van de inbeslagnemingsbevoegdheid. In het navolgende worden de resultaten voor de verschillende onderzoeksvragen per paragraaf behandeld.

3.2.1 Cijfers over de praktijk van inbeslagneming

A) Zijn er cijfers bekend over hoe vaak een opsporingsambtenaar een mobiele telefoon, laptop, computer, usb-stick etc. in beslag neemt (i) op grond van een zelfstandige inbeslagnemingsbevoegdheid (zoals artikelen 95, 96, 96a en 96b Sv) en (ii) tijdens een doorzoeking van een plaats door de officier van justitie (artikel 96c Sv) of door de rechter-commissaris (artikel 110 Sv)? Zo ja, wat zeggen deze cijfers?

Bij het BMI is gevraagd naar het aantal malen dat de bevoegdheid tot inbeslagneming is toegepast op telefoons en computers en hoeveel telefoons en computers daarbij in beslag zijn genomen. De cijfers van de jaren 2012, 2013 en 2014 zijn door het BMI aangeleverd op basis van het Basisvoorziening Handhaving systeem (BVH). Deze cijfers zijn weergegeven per eenheid binnen de politie. In de cijfers is onderscheid gemaakt in het aantal activiteiten en de hoeveelheid goederen. Met het aantal activiteiten wordt het aantal opsporingshandelingen bedoeld. Hierbij kan zowel worden gedacht aan de zelfstandige inbeslagnemingsbevoegdheden als inbeslagneming tijdens de doorzoeking van plaatsen ter inbeslagneming, hieromtrent wordt in de cijfers geen onderscheid gemaakt. Bij een enkele opsporingshandeling kan meer dan één voorwerp (telefoons of computers) in beslag zijn genomen.

Deze zoekvraag leverde de volgende kruistabellen op.

Tabel 1: Aantal malen dat de bevoegdheid tot inbeslagneming is toegepast op telefoons en aantal telefoons dat daarbij in beslag is genomen naar regio en jaar

In beslag genomen telefoons	2012		2013		2014	
	Aantal activiteiten	Goed hoeveelheid	Aantal activiteiten	Goed hoeveelheid	Aantal activiteiten	Goed hoeveelheid
Eenheid Amsterdam	3.091	4.657	3.333	5.475	3.206	5.302
Eenheid Den Haag	2.443	3.954	3.085	4.579	3.042	4.247
Eenheid Limburg	1.644	2.763	1.595	2.355	1.619	2.346
Eenheid Midden-Nederland	2.354	3.868	2.765	4.185	2.897	4.472
Eenheid Noord-Holland	1.652	2.441	1.955	2.687	1.857	2.796
Eenheid Noord-Nederland	1.155	1.710	1.356	2.019	1.488	2.291
Eenheid Oost-Brabant	1.428	2.203	1.672	2.807	1.721	2.646
Eenheid Oost-Nederland	2.408	3.663	2.812	3.942	3.089	4.251
Eenheid Rotterdam	3.247	5.143	3.921	6.572	3.844	6.012
Eenheid Zeeland-West-Brabant	1.853	2.829	1.812	2.689	1.912	2.858
Landelijke Eenheid	233	344	273	392	215	341
Totaal	21.508	33.575	24.579	37.702	24.890	37.562

Bron: BMI uit Basisvoorziening Handhaving systeem

In beslag genomen telefoons

In het jaar 2012 zijn in totaal 21.508 ‘activiteiten’ verricht (met ‘activiteiten’ wordt hier bedoeld het aantal malen dat de bevoegdheid tot inbeslagneming op telefoons is toegepast). Bij deze 21.508 ‘activiteiten’ zijn 33.575 telefoons in beslag genomen. In 2013 is sprake van een toename naar 24.579 ‘activiteiten’, daarbij zijn 37.702 telefoons in beslag genomen. In 2014 is een (zeer) lichte afname in het aantal in beslag genomen telefoons zichtbaar. Hoewel er ten opzichte van 2013 meer ‘activiteiten’ hebben plaatsgevonden (24.890) zijn er daarbij iets minder telefoons in beslag genomen (37.562).

Tabel 2: Aantal malen dat de bevoegdheid tot inbeslagneming is toegepast op computers en aantal computers dat daarbij in beslag is genomen naar regio en jaar

In beslag genomen computers	2012		2013		2014	
	Aantal activiteiten	Goed hoeveelheid	Aantal activiteiten	Goed hoeveelheid	Aantal activiteiten	Goed hoeveelheid
Eenheid Amsterdam	606	865	691	1.035	596	932
Eenheid Den Haag	539	837	609	894	559	899
Eenheid Limburg	329	498	318	479	502	765
Eenheid Midden-Nederland	588	1.005	584	1.118	576	997
Eenheid Noord-Holland	329	493	297	442	334	534
Eenheid Noord-Nederland	430	673	444	803	467	789
Eenheid Oost-Brabant	375	1.262	364	609	346	593
Eenheid Oost-Nederland	670	5.318	712	1.211	641	982
Eenheid Rotterdam	552	946	775	1.393	665	1.034
Eenheid Zeeland-West-Brabant	529	842	518	815	403	771
Landelijke Eenheid	50	60	79	87	44	53
Totaal	4.997	12.799	5.391	8.886	5.133	8.349

Bron: BMI uit Basisvoorziening Handhaving systeem

In beslag genomen computers

In vergelijking met het aantal in beslag genomen telefoons, zijn aanzienlijk minder computers in beslag genomen. In 2012 zijn in totaal 4.997 ‘activiteiten’ (aantal malen dat de bevoegdheid tot inbeslagneming op computers is toegepast) verricht, waarbij 12.799 computers in beslag zijn genomen. Een opvallend groot gedeelte van de in beslag genomen computers (5.318) is in de eenheid Oost-Nederland in beslag genomen. Het totale aantal gevallen van inbeslagneming van computers is in de daarop volgende jaren aanzienlijk afgenomen. Hoewel in 2013 het aantal ‘activiteiten’ ten opzichte van 2012 is toegenomen (5.391), is een sterke daling van het aantal in beslag genomen computers (8.886) te

constateren. In 2014 daalde het aantal ‘activiteiten’ verder naar 5.133 en daalde het aantal in beslag genomen computers ook verder naar 8.349.

Ten aanzien van de hierboven opgenomen aantallen in beslag genomen telefoons en computers dient een belangrijk voorbehoud te worden gemaakt. De cijfers geven niet noodzakelijkerwijs de hoeveelheid daadwerkelijk uitgelezen¹⁰² gegevensdragers en geautomatiseerde werken weer, omdat niet één op één kan worden gezegd dat alle in beslag genomen voorwerpen, die gegevens kunnen dragen of verwerken, ook daadwerkelijk worden of zijn onderzocht. Daarnaast blijkt dat bij de politie ook andere systemen worden gehanteerd waarin inbeslagneming geregistreerd wordt. Dit leidt er toe dat concrete aantallen niet te bepalen zijn. Bij de registratie van de in beslag genomen voorwerpen in de kennisgeving van inbeslagneming worden gelijksoortige voorwerpen niet altijd op dezelfde wijze aangeduid. Uit de opgemaakte kennisgevingen van inbeslagneming kunnen de exacte cijfers dan ook niet op eenvoudige wijze geaggregeerd worden. In diverse categorieën binnen het BVH-systeem kunnen diverse goederen anders worden aangeduid. Zo zou een telefoon bijvoorbeeld kunnen worden opgenomen onder de term ‘GSM’, ‘Mobiele telefoon’, ‘Telefoon’ en ‘Smartphone’. Er zijn nog diverse andere termen denkbaar. Ditzelfde geldt voor de computer (waar ook de tablets en e-readers onder vallen).

Regio Haaglanden

Aparte cijfers zijn verkregen vanuit de regio Haaglanden. Deze cijfers zijn afkomstig uit een eigen intern gehanteerd registratiesysteem, waarbij over de betrouwbaarheid door de onderzoekers geen uitspraken gedaan kunnen worden.¹⁰³

In de regio Haaglanden zijn in het jaar 2013 in totaal 4273 in beslag genomen elektronische gegevensdragers en geautomatiseerde werken geregistreerd. Dit betreft enkel de cijfers van het team Digitale Opsporing. Van die ruim vierduizend in beslag genomen elektronische gegevensdragers en geautomatiseerde werken, waren een kleine tweeduizend (1925) een mobiele telefoon dan wel een tablet. De overige aantallen werden verspreid over maar liefst 25 andere categorieën elektronische gegevensdragers en geautomatiseerde werken, geregistreerd. In het jaar 2014 is een lichte afname waarneembaar in de geregistreerde in beslag genomen voorwerpen. In dat jaar werden door het team Digitale Opsporing in totaal 3902 in beslag genomen elektronische gegevensdragers en geautomatiseerde werken geregistreerd. Het aandeel mobiele telefoons en tablets bedroeg 1766 daarvan.

¹⁰² Met ‘uitlezen’ wordt in dit verband voornamelijk bedoeld op het maken van een image.

¹⁰³ De betreffende cijfers zijn door middel van een Excelbestand aangeleverd.

Respondenten

In de interviews met de respondenten zijn ook vragen gesteld over de aantallen in beslag genomen elektronische gegevensdragers en geautomatiseerde werken. Indien concrete aantallen bij de respondenten niet bekend waren, werd gevraagd hoeveel voorwerpen de respondenten in de eigen praktijk in beslag hebben genomen. Ten aanzien van de vragen over de kwantitatieve gegevens op het gebied van aantallen in beslag genomen elektronische gegevensdragers of geautomatiseerde werken moet worden opgemerkt dat hierop wisselende antwoorden werden gegeven. Diverse respondenten gaven daarbij aan moeite te hebben met het maken van een inschatting van aantallen. Bovendien bleek uit de antwoorden dat voor velen veelal onbekend was in hoeverre registratie van de aantallen in beslag genomen voorwerpen plaatsvond.

Qua inschatting van de aantallen kan wel worden gezegd dat het aanzienlijke aantallen betreft. Met name de opsporingsambtenaren werkzaam op locaties met meer digitale expertise in grootschalige onderzoeken schatten de aantallen in beslag genomen voorwerpen hoog in. In de grootschalige onderzoeken wordt veelal gewerkt met afzonderlijke teams bij de eenheden, die zich uitsluitend bezighouden met het (technische) onderzoek aan elektronische gegevensdragers en geautomatiseerde werken.

Dit beeld wordt door alle respondenten bevestigd. Uit de beantwoording van de vragen is niet te achterhalen of de inbeslagneming op grond van een zelfstandige inbeslagnemingsbevoegdheid van een opsporingsambtenaar is gehanteerd, of dat inbeslagneming plaats had in het kader van een doorzoeking van plaatsen door of onder leiding van de officier van justitie of rechter-commissaris.

Zoals gezegd, door de meeste respondenten wordt aangegeven dat het maken van een inschatting lastig is. Een van de respondenten schatte dat in de regio Amsterdam-Amstelland in de afgelopen drie jaar in totaal ongeveer 35.000 elektronische gegevensdragers en geautomatiseerde werken in beslag zijn genomen. Dit betrof slechts een gissing, waarbij wel moet worden vermeld dat deze gissing was gebaseerd op een intern registratiesysteem, maar niet kon worden onderbouwd met concrete cijfers of cijferbestanden.

Concreet kan worden vastgesteld dat in de praktijk van de inbeslagneming van en het daaropvolgende onderzoek dat wordt gedaan aan elektronische gegevensdragers en geautomatiseerde werken, het om aanzienlijke aantallen gaat. Hoewel dit onderscheid niet kan worden afgeleid uit het BVH systeem, blijkt uit de interviews dat het merendeel hiervan tijdens de doorzoeking ter inbeslagneming, onder leiding van de officier van justitie of de rechter-commissaris in beslag genomen wordt en niet op grond van een zelfstandige inbeslagnemingsbevoegdheid van de opsporingsambtenaar.

B) Zijn er cijfers bekend over hoe vaak een opsporingsambtenaar onderzoek verricht aan een smartphone, computer etc. zonder dat deze in beslag wordt genomen?

Over deze situatie zijn geen cijfers voorhanden. De beantwoording van de vragen door de respondenten hieromtrent kan wel tot een zekere beantwoording van de onderzoeksvraag leiden. Uit de bevindingen afkomstig uit de interviews volgt, dat het voorkomt dat een opsporingsambtenaar ter plaatse in een geautomatiseerd werk kijkt met het doel om van de daarop opgeslagen gegevens kennis te nemen, zonder dat de gegevensdrager formeel ten behoeve van de waarheidsvinding in beslag wordt genomen. In deze situatie vindt geen enkele vorm van registratie en notificatie plaats; zowel de kennisgeving van inbeslagneming als het bewijs van ontvangst worden hier niet opgemaakt of afgegeven. Het komt ook voor dat onderzoek wordt verricht aan een geautomatiseerd werk en dat daarop opgeslagen gegevens worden gekopieerd, zonder dat dit formeel in beslag is genomen. In dit geval ontbreekt dan ook de afgifte van een bewijs van ontvangst aan de verdachte. Het voornaamste voorbeeld dat door de respondenten daarvan werd gegeven is onderzoek verricht aan bij de insluitingsfouillering afgegeven of afgenomen gegevensdragers. Deze situatie wordt in paragraaf 3.3.7 nader toegelicht.

Tot slot blijkt uit de antwoorden van de respondenten dat in beginsel de hier bedoelde handelingen niet worden geregistreerd, waardoor cijfers over het aantal onderzoeken dat wordt verricht aan een elektronische gegevensdrager of geautomatiseerd werk zonder dat een kennisgeving van inbeslagneming en bewijs van ontvangst is opgemaakt, niet bekend zijn. Het blijkt ook lastig voor de respondenten om hier een concrete inschatting van te maken. Dat is begrijpelijk, omdat het voornamelijk situaties betreft die buiten het werkveld van de opsporingsambtenaren met digitale expertise plaatsvindt. In sommige gevallen wordt een en ander wel opgenomen als ambtshandeling in een proces-verbaal. Omdat dit niet in alle gevallen zo blijkt te zijn, kunnen hieruit geen concrete cijfers worden gedestilleerd en kan derhalve geen representatief beeld gevormd worden.

C) Zijn er cijfers bekend over hoe vaak bestanden van een smartphone, computer etc. worden gewist voordat deze wordt teruggegeven aan de beslagene?

Over de frequentie van de toepassing van het wissen van bestanden van elektronische gegevensdragers of geautomatiseerde werken lijken geen cijfers geregistreerd te worden. In het geval van een rechterlijk oordeel tot verbeurdverklaring of onttrekking aan het verkeer zal het hele voorwerp, inclusief de bestanden worden, vernietigd. Desondanks is uit de interviews af te leiden dat het (al dan niet gedeeltelijk) wissen van gegevens vóór teruggave in sommige gevallen voorkomt. De gevallen waarin dat voorkomt worden in paragraaf 3.3.8 nader toegelicht.

3.3 Kwalitatieve onderzoeksvragen

Om meer inzicht te verkrijgen in de werkwijze met betrekking tot het nadere onderzoek aan in beslag genomen voorwerpen, teneinde beschikking te krijgen over de daarop vastgelegde gegevens, zijn de respondenten in de interviews verschillende vragen gesteld. In het navolgende worden de resultaten van de onderzoeksvragen per paragraaf behandeld.

3.3.1 Autoriteit en gronden

1. Wie beslist dat aan de in beslag genomen gegevensdrager of in het in beslag genomen geautomatiseerde werk onderzoek mag worden gedaan en dat de daarop of daarin opgeslagen gegevens mogen worden vastgelegd?

Afhankelijk van de wettelijke grondslag is de autoriteit die beslist over het in beslag nemen van elektronische gegevensdragers en geautomatiseerde werken de rechter-commissaris, de officier van justitie of de (andere) opsporingsambtenaar. Uit de reacties van enkele digitaal rechercheurs kan worden afgeleid dat in sommige gevallen op verzoek van de rechter-commissaris de digitaal rechercheurs het onderzoeksteam vanuit hun expertise aanvullend adviseren over een te maken selectie van de in beslag te nemen elektronische gegevensdragers en geautomatiseerde werken.

Uit de beantwoording van de vragen in de interviews – die op diverse onderwerpen verder strekken dan datgene wat strikt uit de onderzoeksvragen voortvloeit – volgt dat elektronische gegevensdragers en geautomatiseerde werken in de meeste gevallen in beslag worden genomen met als doel het doen van onderzoek daaraan (in het kader van de waarheidsvinding). Er vindt daarbij dan ook geen aparte toets meer plaats omtrent de vraag in hoeverre aan het in beslag genomen voorwerp onderzoek mag worden gedaan. Dat hangt samen met het feit dat die toets reeds in een eerdere fase, bij het daadwerkelijk in beslag nemen en meenemen van het voorwerp, gemaakt wordt nu het uitgangspunt is dat het betreffende voorwerp ook nader zal worden onderzocht. In samenspraak met de betreffende officier van justitie en het onderzoeksteam kan wel worden bepaald dat uiteindelijk niet alle in beslag genomen elektronische gegevensdragers en geautomatiseerde werken daadwerkelijk worden onderzocht. De beslissing om bepaalde gegevensdragers niet nader te onderzoeken wordt voornamelijk ingegeven door praktische overwegingen. Hiermee wordt bedoeld op de situatie waarbij – om uiteenlopende redenen – vele elektronische gegevensdragers of geautomatiseerde werken in beslag zijn genomen, maar waarbij de beslissing tot daadwerkelijk onderzoeken en uitlezen daarvan nog gemaakt moet worden.

Opsporingsambtenaar als bevoegde autoriteit

Als aan de wettelijke voorwaarden is voldaan kan de bevoegdheid tot inbeslagneming door elke opsporingsambtenaar ook buiten een doorzoeking worden uitgeoefend. De situatie waarin de opsporingsambtenaar zelfstandig overgaat tot inbeslagneming van een elektronische gegevensdrager of geautomatiseerd werk, doet zich in de praktijk weinig voor, zo blijkt uit de reacties van de respondenten. De achterliggende redenen om een voorwerp niet in beslag te nemen verschillen van karakter. Die verschillen zijn mede te verklaren door gebrek aan digitale expertise. Daarnaast liggen praktische redenen (bijvoorbeeld een afweging tussen de te verrichten administratieve inspanningen en het belang van de bijdrage aan de waarheidsvinding) aan het niet in beslag nemen van een voorwerp ten grondslag.

Uit de antwoorden van de respondenten is gebleken dat het merendeel van de inbeslagneming van elektronische gegevensdragers en geautomatiseerde werken plaatsvindt in het kader van de doorzoeking van plaatsen en niet is gegrond op de zelfstandige bevoegdheid van de opsporingsambtenaar.

In geval van zelfstandige uitoefening van de bevoegdheid tot inbeslagneming door de opsporingsambtenaar, ligt de bevoegdheid tot het doen van nader onderzoek aan dat voorwerp teneinde beschikking te krijgen over de gegevens ook bij hem. Uit de interviews is gebleken dat in het geval van toepassing van de zelfstandige bevoegdheid van de opsporingsambtenaar tot inbeslagneming soms wordt gekozen om een beperkte hoeveelheid informatie te kopiëren. Dit betekent dus dat in die gevallen niet altijd een volledige kopie (image) van de gegevens(bestanden) op de gegevensdrager wordt gemaakt.

Doelen inbeslagneming

In de interviews is gevraagd naar de achterliggende doelen van het in beslag nemen van elektronische gegevensdragers en geautomatiseerde werken als criterium bij de beslissing tot inbeslagneming en bij de beslissing over de selectie en omvang van de in beslag te nemen voorwerpen. In het algemeen wordt de waarheidsvinding als het achterliggende doel van de inbeslagneming genoemd. In sommige gevallen, ondanks dat het niet expliciet een zelfstandige grond voor inbeslagneming betreft zoals in artikel 94 Sv bedoeld, wordt door de respondenten ook het voorkomen van voortzetting van strafbare feiten of het begaan van andere strafbare feiten (bijvoorbeeld in het geval van kinderporno, terroristische misdrijven, etc.) als doel van de inbeslagneming genoemd.

Selectie van de inbeslagneming

Uit de verdere bevraging blijkt, dat de beslissing over de omvang van het beslag gedurende de doorzoeking wordt gemaakt. Die beslissing is onlosmakelijk verbonden met het doel van de inbeslagneming. Uit de reacties van de respondenten volgt, dat de praktijk om gedurende een doorzoeking alle of vele aangetroffen elektronische gegevensdragers en geautomatiseerde werken in beslag te nemen, een kentering naar het slechts in beslag nemen van een beperkt aantal daarvan, lijkt te kennen. Dat kan mede worden verklaard door de toename in het gebruik van elektronische gegevensdragers en geautomatiseerde werken. In de huidige praktijk wordt in de meeste gevallen in de voorbereiding en voornamelijk ter plaatse een bewuste afweging gemaakt omtrent de in beslag te nemen gegevensdragers. Dit geldt in het bijzonder voor de opsporingsdiensten met digitale expertise die in grote onderzoeken met elektronische gegevensdragers of geautomatiseerde werken te maken hebben. Desondanks komt het voor dat bij zwaardere zaken veiligheidshalve toch grote hoeveelheden of alle aangetroffen elektronische gegevensdragers en geautomatiseerde werken in beslag worden genomen in het kader van de waarheidsvinding c.q. het zeker stellen van het verkrijgen van alle relevante informatie. Zoals reeds opgemerkt kan het voorkomen dat uiteindelijk niet alle in beslag genomen voorwerpen onderzocht worden. Onderstaande citaten illustreren de afweging bij de selectie van de in beslag te nemen voorwerpen.

“Afhankelijk van de zaak. Een zaak waarin je ad hoc bezig bent en tegen iets aanloopt en direct reageert, daar is mede vanwege de tijd niet van te voren al over nagedacht. Bij grotere zaken is er van te voren over nagedacht. Ik denk dat in te weinig zaken er echt goed van te voren over nagedacht wordt. Zowel politie als OM realiseren soms te weinig wat voor vracht aan gegevens wordt binnengehaald bij inbeslagname. Deze bewustwording begint wel steeds meer te komen. Er wordt vaak wel een selectie gemaakt (even over nagedacht worden of iets echt nodig is voor het onderzoek), afweging om waar te kunnen maken om alles wat wordt meegenomen ook voorwerp van onderzoek te maken). Ook afhankelijk van waar je naar op zoek bent.”¹⁰⁴

“Alle afwegingen, moeten we echt iets in beslag nemen, worden per individuele casus heel bewust gemaakt. Proportionaliteit, subsidiariteit en belangenafweging. Heeft ook met capaciteit te maken.”¹⁰⁵

Uit de interviewbevindingen kan worden geconstateerd dat de afweging omtrent de in beslag te nemen voorwerpen sterk afhankelijk is van de verdenking en de omvang van het onderzoek, maar anderzijds ook van de bij de inbeslagneming betrokken autoriteit. Zo worden in een onderzoek naar (virtuele) kinderporno in beginsel alle gegevensdragers zonder uitzondering in beslag genomen. Dat is anders in geval voorwerpen worden in beslag genomen op grond van een verdenking van een meer eenvoudig delict of delicten van een andere aard. Afhankelijk van de omstandigheden en de betrokken autoriteit wordt

¹⁰⁴ Citaat afkomstig van een officier van justitie.

¹⁰⁵ Citaat afkomstig van een opsporingsambtenaar werkzaam bij een bijzondere opsporingsdienst.

een toename van de invloed van de beginselen van proportionaliteit en subsidiariteit in die afweging merkbaar.

Kennisgeving van inbeslagneming en verstrekken bewijs van ontvangst

In de interviews is ook aandacht besteed aan de verslaglegging van de inbeslagneming. Zoals in hoofdstuk 2 omschreven, is de kennisgeving van inbeslagneming bedoeld voor de hulpofficier van justitie ter beoordeling of het beslag gehandhaafd mag worden. Het bewijs van ontvangst dient als uitgangspunt zo veel mogelijk te worden afgegeven en is bedoeld voor de beslagene. De respondenten geven vrijwel zonder uitzondering aan dat indien wordt overgegaan tot inbeslagneming, een kennisgeving van inbeslagneming wordt opgemaakt. Door de respondenten wordt gezegd dat hierop uitzonderingen bestaan. Bij de bevraging is het de onderzoekers opgevallen dat door de respondenten in de regel bij de beantwoording van de vragen geen onderscheid tussen kennisgeving van inbeslagneming en bewijs van ontvangst wordt gemaakt. Ook bij verdere navraag lijkt dat onderscheid niet te worden gemaakt. Het lijkt er in veel gevallen op dat respondenten bewijs van ontvangst bedoelen, terwijl ze daarbij veelal de term kennisgeving van inbeslagneming gebruiken. Indien verslaglegging wordt uitgesteld, wordt bijvoorbeeld gesproken over het uitstellen van het opstellen van de kennisgeving van de inbeslagneming tot een later tijdstip. Ook wordt in bepaalde gevallen, indien het voorwerp wordt teruggegeven, gesproken over het achterwege laten van kennisgeving aan de beslagene. Dat achterwege laten geschiedt dan in de veronderstelling dat de beslagene op de hoogte is van het feit dat onderzoek heeft plaatsgevonden dan wel in de veronderstelling dat hem op later tijdstip daarvan mededeling wordt gedaan. In die gevallen vindt het verstrekken van het bewijs van ontvangst bij de verstrekking van het dossier aan de verdediging dan wel bij dagvaarding plaats. Er lijkt derhalve in de praktijk sprake van een spraak-en begripsverwarring. Onderstaand citaat illustreert die verwarring. De opmerkingen van de respondenten bevestigen de indruk van de onderzoekers dat met de term kennisgeving van inbeslagneming ook het bewijs van ontvangst aan de beslagene wordt bedoeld.

“Er kunnen redenen zijn om de kvi uit te stellen (soms pragmatisch ingegeven). Administratieve handeling vergt ook tijd. Kan ook in heimelijkheid in beslag worden genomen, vanwege afbreuk onderzoek dan pas later een kvi. Bij heimelijkheid wordt het item vaak alweer teruggegeven voordat de verdachte door heeft dat het in beslag is genomen.”¹⁰⁶

Uit het onderzoek komt voorts naar voren dat in sommige regio's een kennisgeving van inbeslagneming noodzakelijk is voor het onderzoek naar de op de in beslag genomen gegevensdrager opgeslagen gegevens. In die regio's wordt namelijk bij het opmaken van de

¹⁰⁶ Citaat afkomstig van een officier van justitie.

kennisgeving van inbeslagneming een (bestands)nummer gegenereerd waaronder de vergaarde gegevens opgeslagen worden. Zonder dat (bestands)nummer is het gecompliceerd om de gegevens op de juiste wijze op te slaan en te verwerken of onderzoeken. Zonder een dergelijk (bestands)nummer worden die gegevens van beperkte waarde voor de opsporing.

Niet alle respondenten konden antwoord geven op de vragen over de kennisgeving van inbeslagneming. Daaraan lagen verschillende oorzaken ten grondslag. Enerzijds hing dat samen met het feit dat de kennisgeving van inbeslagneming buiten het bereik van het werkveld van een aantal respondenten leek plaats te vinden, anderzijds leken de respondenten geen duidelijk onderscheid te maken tussen de kennisgeving van inbeslagneming en het bewijs van ontvangst aan de beslagene. In onderstaand citaat wordt met de term bewijs van afgifte het wettelijk voorgeschreven bewijs van ontvangst bedoeld.

“Het wordt soms vergeten om een apart formulier bewijs van afgifte op te maken, volgens de wet dient er wel altijd bij inbeslagneming een bewijs van afgifte aan beslagene af te worden gegeven.”¹⁰⁷

Ten aanzien van het moment van kennisgeving aan de verdachte door middel van het verstrekken van een bewijs van ontvangst bestaat discussie. Uit de antwoorden van de respondenten is ook geen eenduidig beleid te destilleren. Dit hangt niet samen met de functie van de betreffende respondent. Een onderdeel van die discussie richt zich op heimelijke inbeslagneming en het uitstellen van de verstrekking van een bewijs van ontvangst. In de huidige praktijk komt het voor dat de verstrekking van het bewijs van ontvangst wordt uitgesteld tot aan het moment van verstrekking van de processtukken aan de verdediging. Uit de antwoorden van de respondenten volgt dat hieraan zowel inhoudelijke als administratieve redenen ten grondslag lagen. Tot dat moment heeft de beslagene geen weet van het feit dat een hem toebehorende gegevensdrager in beslag genomen is geweest, is onderzocht en dat de daarop opgeslagen gegevens mogelijk zijn gekopieerd en verwerkt ten behoeve van de opsporing. Onderstaand citaat illustreert een toelichting op de heimelijke inbeslagneming..

“Het heimelijke zit meer in het onderzoek dan in het resultaat van het onderzoek.”¹⁰⁸

Aard van de gegevens

In het geval van inbeslagneming van elektronische gegevensdragers en geautomatiseerde werken wordt geen onderscheid gemaakt naar de aard van de daarop opgeslagen gegevens,

¹⁰⁷ Citaat afkomstig van een opsporingsambtenaar.

¹⁰⁸ Citaat afkomstig van een officier van justitie.

zoals blijkt uit de antwoorden van alle respondenten.¹⁰⁹ De aard van de op de in beslag te nemen voorwerpen aanwezige gegevens heeft geen invloed op de autoriteit die de beslissing omtrent de inbeslagneming van de voorwerpen en het onderzoek daarin neemt. Zo wordt geen onderscheid gemaakt naar de eventuele aanwezigheid van niet voor het publiek bestemde communicatie en andere gegevens, hetgeen wordt bevestigd door de respondenten.

Eén punt werd nog nader benoemd. Ten aanzien van de gevoelige gegevens kan het zijn dat na het kopiëren van gegevens alles gezien kan worden door het betreffende tactisch onderzoeksteam. Het kan dus zo zijn dat ook kennis wordt genomen van gevoelige gegevens, die niet per definitie relevant zijn voor het onderzoek. Immers, met een image wordt de volledige informatie aanwezig op de betreffende gegevensdrager of het geautomatiseerde werk vastgelegd. Meer problematisch lijkt dit voor zover dat betrekking heeft op handelen op grond van die informatie. In de interviews is door een tweetal digitaal rechercheurs genoemd dat dit gevoelig kan liggen. Het kan in sommige gevallen niet wenselijk zijn om dezelfde opsporingsambtenaar een verdachte te laten horen, indien hij ook de gehele inhoud van een smartphone of computer heeft gezien. Dit kan veel persoonlijke informatie bevatten, die niet per definitie relevant is in het betreffende strafrechtelijk onderzoek, maar optioneel wel kan werken als een machtsmiddel.

Gegevens die eerst na de inbeslagneming worden gegenereerd

Uit de interviews is gebleken dat in sommige gevallen het in beslag genomen geautomatiseerde werk nog aan staat en in verbinding staat met internet nadat het is in beslag genomen. In dat geval kan het voorkomen dat nieuwe gegevens, zoals bijvoorbeeld nieuwe WhatsApp-berichten op het geautomatiseerde werk worden ontvangen. Door de respondenten wordt op verschillende wijze omgesprongen met gegevens die eerst op een later tijdstip dan het moment van inbeslagneming worden verkregen. Hierover lijkt geen beleid te bestaan dat algemeen bekend is, of in alle gevallen consequent gevolgd wordt. Opsporingsambtenaren die veelvuldig te maken hebben met onderzoek naar gegevens, zetten de telefoon in 'vliegtuigmodus' zodat de verbinding met internet wordt verbroken. Dat wordt in de regel gedaan om te voorkomen dat de op de telefoon aanwezige gegevens op afstand worden beïnvloed dan wel gewijzigd of verwijderd. Het in 'vliegtuigmodus' zetten van de telefoon heeft als neveneffect dat geen gegevens meer ontvangen kunnen worden. Dat is van belang vanwege de forensische bewijswaarde van de verkregen gegevens.

Uit de interviews is gebleken dat in zeldzame gevallen de vliegtuigmodus niet is ingeschakeld en toch nieuwe gegevens gegenereerd worden. Die informatie kan bovendien

¹⁰⁹ Dat ligt anders indien het gegevens betreft waarover het professioneel verschoningsrecht zich uitstrekt, zie nader in paragraaf 3.3.4.

relevant zijn voor het onderzoek. De officier van justitie moet dan beslissen in hoeverre de nieuwe informatie nog wordt toegevoegd aan het onderzoek. In het segment van hoogwaardig onderzoek aan elektronische gegevensdragers en geautomatiseerde werken wordt naast de ‘vliegtuigmodus’ bovendien gebruik gemaakt van zogeheten ‘Faraday-dozen’, waardoor beïnvloeding van de gegevens op deze gegevensdragers van buitenaf onmogelijk wordt gemaakt.¹¹⁰ Onderstaand citaat illustreert het dilemma van de praktijk. Gevraagd werd naar de omgang met gegevens die pas na het moment van de inbeslagneming van het geautomatiseerde werk worden ontvangen en opgeslagen.

“Dat is heel listig. Onze wetgever leek er van uit te gaan dat het in beslag genomen goed statisch is. Dat is allang niet meer zo. Landelijk Parket heeft een stuk gemaakt waarin zij de lijn hebben uitgezet dat het vanaf het moment van inbeslagname stopt. Maar je kan je afvragen wat de grondslag is om dat te doen. De wetgever heeft het niet verboden (niet onmogelijk gemaakt), de HR zegt: aan een in beslag genomen goed mag je onderzoek doen. Maar mag dat dan alleen op het statische van het goed? De setting is nu alleen voorstelbaar op conservatoire grond in beginsel. Deze variant is heel lastig. Telefoon in beslag genomen en er staat een tap op, laat de tap dan nog een week doorlopen. De toestemming van de RC is er dan in ieder geval. Het beleid is alleen van het Landelijk Parket en daar zijn van te voren eigenlijk te weinig gesprekken over gevoerd. Die discussie loopt nog. En dus lijkt dit nu niet geheel nageleefd te worden. Zolang daar van de wetgever of HR geen uitsluitsel over is, wordt eigen beleid gehanteerd.”¹¹¹

3.3.2 Kopiëren van gegevens

2. Worden gegevens gekopieerd voor verder onderzoek? Zo ja, alle gegevens (‘image’ maken) of alleen een deel daarvan? In geval van een deel, waarom een/dat deel en niet alle gegevens?

Uit de interviews komt omtrent het kopiëren van gegevens ten behoeve van nader onderzoek een wisselend beeld naar voren. In de situatie waarbij gegevensdragers worden aangedragen bij opsporingsambtenaren werkzaam op de zijde van het spectrum van hoogwaardig technisch forensisch onderzoek, wordt voornamelijk een volledige kopie (image) gemaakt. Bij hen wordt zelden tot nooit slechts een gedeelte van de gegevens vastgelegd. Uit de antwoorden van opsporingsambtenaren die minder met gegevensonderzoek werken, zonder grote digitale expertise, blijkt dat zij minder moeite hebben met het vastleggen van beperkte hoeveelheden geselecteerde gegevens(bestanden).

Er kan worden gewerkt met twee methoden, ofwel een volledige image, of een selectie van de te kopiëren gegevens. In de meeste gevallen wordt een volledige image gemaakt. Dat wordt voornamelijk gedaan met het oog op de validiteit van de gegevens. Door het maken

¹¹⁰ Met de doos van Faraday wordt bedoeld op de ‘kooi van Faraday’, genoemd naar M. Faraday. Dit is de benaming voor een kooivormige constructie van elektrisch geleidend materiaal, zoals koper of ijzer, die ervoor zorgt dat statische elektrische velden niet tot binnen de kooi kunnen doordringen.

¹¹¹ Citaat afkomstig van een officier van justitie.

van een exacte kopie van de op de gegevensdrager opgeslagen gegevens kan contra-expertise plaatsvinden en kunnen rechter en verdediging zo nodig de betrouwbaarheid en volledigheid van de gegevens toetsen. In het geval van grote onderzoeken, voornamelijk bij hightech criminaliteit, gaat het om een aanzienlijke hoeveelheid aan gegevens die gekopieerd worden. Ten aanzien van het maken van de image is de respondenten geen specifieke wet- en regelgeving bekend.

De opsporingsambtenaren die niet werkzaam zijn in de grote onderzoeken waarbij met vele digitale gegevens wordt gewerkt hanteren, zoals gezegd, een andere aanpak. Het gaat bij de geselecteerde gegevens veelal om specifieke gegevens, van veel kleinere omvang.

Ont sleuteling

Uit de reacties van de respondenten die deze vraag hebben beantwoord blijkt dat ruim de helft daarvan¹¹² te kennen geeft dat het regelmatig voorkomt dat het niet mogelijk is om aan het in beslag genomen geautomatiseerde werk onderzoek te verrichten. Het komt voor dat gegevens niet kunnen worden gebruikt in het onderzoek, omdat deze niet toegankelijk zijn. Dat kan samenhangen met de encryptie van die gegevens of een blokkering van de toegang tot die gegevens of de gegevensdragers. Hier zijn twee situaties mogelijk. Enerzijds betreft dat de situatie dat het geautomatiseerde werk is vergrendeld (met bijvoorbeeld een wachtwoord of een code). Daarnaast bestaat de situatie dat het geautomatiseerd werk wel toegankelijk is, maar de gegevens(bestanden) zijn versleuteld. Het huidige artikel 125k Sv voorziet in de mogelijkheid van een bevel tot ontsleuteling in het geval van een doorzoeking ter vastlegging van gegevens. Dit bevel mag niet aan de verdachte gegeven worden. De respondenten is de vraag voorgelegd in hoeverre een wettelijke regeling, die de mogelijkheid zou bieden een bevel tot ontsleuteling te geven (zoals thans geregeld in artikel 125k Sv voor de doorzoeking ter vastlegging van gegevens), ook buiten de situatie van de doorzoeking gewenst zou zijn.

Uit het onderzoek ontstaat het beeld dat de huidige praktijk er in berust dat het in sommige gevallen simpelweg niet mogelijk is om nader onderzoek aan de betreffende elektronische gegevensdrager of het geautomatiseerde werk te verrichten. Het idee voor een nadere regeling van toegang tot gegevens op in beslag genomen gegevensdragers door middel van een bevel tot ontsleuteling, wordt niet unaniem door de respondenten gedragen. Enkele respondenten benadrukken dat in de afweging van de mogelijkheid tot het doen van onderzoek in het kader van de waarheidsvinding, de bescherming van de persoonlijke levenssfeer in voldoende mate moet worden meegewogen. Enkele andere digitaal rechters gaven te kennen dat de balans niet altijd evenwichtig is, omdat met de huidige wet- en regelgeving en technologische ontwikkelingen, afgewogen tegen de bescherming

¹¹² 13 van de 22 respondenten.

van de persoonlijke levenssfeer van verdachte, het soms lastig is om goed onderzoek uit te kunnen voeren, wat niet in alle gevallen wenselijk is voor de respondenten.

Ten overvloede wordt nog opgemerkt dat met de meeste respondenten tevens is gesproken over de wens tot het geven van een ontsleutelingsbevel aan de verdachte. De respondenten waren zich ervan bewust dat dit een lastige en tevens ethische discussie is.¹¹³ De wens tot een dergelijke regeling wordt ook in deze kwestie niet unaniem geuit. Enkele officieren van justitie en digitaal rechercheurs verwezen naar de beperkingen die het nemo teneturbeginsel in deze situatie met zich brengt.

3.3.3 Bewaring van gekopieerde gegevens

3. Wat wordt gedaan met de gekopieerde gegevens? Hoe en hoe lang worden ze bewaard?

In de vorige paragraaf is uiteengezet op welke wijze de respondenten omgaan met het opslaan van gegevens door middel van kopieën. Die kopieën worden in de bedrijfssystemen, oftewel de interne systemen, van de opsporingsdiensten vastgelegd. Hiermee wordt bedoeld op interne opslagcapaciteit binnen de regionale politie. Uit de reacties op de vraag op welke wijze met de bewaring van dergelijke gegevens wordt omgesprongen, blijkt dat voor de verwerking van de gegevens onderscheid gemaakt dient te worden tussen de bewaring en verwerking gedurende het onderzoek, en de bewaring en vernietiging na afronding van het onderzoek.

Bewaring van en toegang tot vastgelegde gegevens gedurende het onderzoek

Uit de reacties blijkt dat veel respondenten niet bekend zijn met landelijke regelgeving omtrent de wijze van bewaring en het verlenen van toegang tot de gekopieerde gegevens. De praktijk blijkt dan ook per regio te verschillen. Het blijkt niet altijd duidelijk waar gegevens worden bewaard en welke personen toegang hebben tot die gegevens. In elk geval maken de opsporingsdiensten belast met grootschalige digitale onderzoeken een selectie bij het verlenen van toegang tot de gekopieerde gegevens en hanteren een exclusief toegangsbeleid. Een toegangsbeleid is minder bekend bij opsporingsambtenaren die gegevens bewaren die zijn ontleend aan een gegevensdrager met toepassing van een zelfstandige inbeslagnemingsbevoegdheid is in beslag genomen. Uit de interviews is gebleken dat in geval van een groot onderzoek met veel vastgelegde gegevens veelal een bewuste keuze wordt gemaakt welke ambtenaren toegang krijgen tot de betreffende gegevens. Dit wordt voornamelijk bevestigd door de officieren van justitie en enkele digitaal rechercheurs. In de praktijk blijken problemen te bestaan met de opslagcapaciteit

¹¹³ Ter illustratie wordt verwezen naar het onderzoek van B.J. Koops, *Het decryptiebevel en het nemo tenetur beginsel. Nopen ontwikkelingen sinds 2000 tot invoering van een ontsleutelplicht voor verdachten?*, Tilburg: Universiteit van Tilburg 2012.

door de grote hoeveelheden data die opgeslagen moeten worden. Die problemen ontstaan doordat interne opslag servers vol raken. Ook ten aanzien van de bescherming van gegevens(bestanden) en de controle hierop worden problemen ervaren, mede vanwege de onduidelijkheid over het verlenen van toegang tot de vastgelegde gegevens. Het beleid hieromtrent vertoont sterke verschillen per regio.

Bewaring van vastgelegde gegevens na afronding van het onderzoek

Het bestaan van beleid over de duur van de bewaring van gegevens is niet bij alle respondenten (zowel digitaal rechercheurs als wijkagenten) bekend. Sommigen verwijzen in dat kader naar de Wpg, maar zijn niet op de hoogte van de exacte inhoud van die regelgeving.¹¹⁴ Er lijkt een spanningsveld te ontstaan tussen het recht op bescherming van de persoonlijke levenssfeer van de betrokkenen en het mogelijk in een later stadium nog kunnen beschikken over de op image vastgelegde gegevens. Hierbij kan gedacht worden aan de situatie dat een beslissing in een strafzaak die nog niet onherroepelijk is geworden, maar ook aan verzoeken tot herziening, zowel ten voordele als ten nadele van de gewezen verdachte. Dat doet bij de respondenten de vraag rijzen hoe lang gegevens bewaard mogen blijven. Dit geldt te meer met het oog op de steeds langer wordende verjaringstermijnen.

Een van de respondenten, een digitaal rechercheur gaf aan dat bij de politie eenheid Amsterdam-Amstelland sinds drie jaar een zeker systeem wordt gehanteerd met betrekking tot de opslag van data. Na afronding van de strafzaak tegen de verdachte kunnen de rechten om de gegevens te raadplegen, worden ingetrokken. De gegevens worden dan offline gehaald, hetgeen meebrengt dat niemand meer toegang tot die gegevens heeft. Bij dringende noodzaak kunnen de gegevens, in het geval er een vraag naar of omtrent die gegevens ontstaat, weer worden teruggeplaatst. Dat gebeurt pas na een zorgvuldige toets, mede door de officier van justitie. Na terugplaatsing zijn de gegevens bijvoorbeeld voor een bepaald tactisch team weer te raadplegen.

Het gebruiken van dergelijke systemen, gericht op het bewaring van en het eventueel ontoegankelijk maken van, gegevens, wordt ook in de eenheid Haaglanden als praktijk gehanteerd.

De indruk is ontstaan dat er geen centraal orgaan of centrale instantie, noch eenduidig beleid of regie is, die bepaalt op welke wijze en op welk moment gegevens vernietigd moeten worden dan wel ontoegankelijk moeten worden gemaakt. Dit kan betekenen dat eenmaal uit gegevensdragers vergaarde gegevens voor lange duur bewaard blijven. Dat kan ook gebeuren indien de vergaarde gegevens geen relevantie voor een concreet

¹¹⁴ Dit sluit ten aanzien van de bewaring van gegevens aan bij een van de conclusies van de privacy-audit die de Auditdienst Rijk (ADR) heeft verricht naar de naleving van de Wpg door de politie. De conclusie ten aanzien van dit onderdeel was dat de naleving van de bewaartermijnen onvoldoende op orde is.

opsporingsonderzoek hebben. Diverse respondenten, met name digitaal rechercheurs, geven te kennen dat behoefte bestaat aan het hanteren en uitvoeren van een centraal beleid. Tevens vinden die respondenten dat het Openbaar Ministerie de beslissing tot vernietigen van gegevens zou moeten nemen.

Hoewel veel respondenten melden dat over de toepassing van de regelgeving rondom de bewaring veel onduidelijkheid bestaat, werd door sommigen juist gesteld dat door hun opsporingsdienst de kaders van de Wpg werden gevolgd. Bij die respondenten bestond geen discussie hieromtrent. Dat laatste geldt ook in relatie tot de beslissingen omtrent het vernietigen van gegevens. In het bijzonder geldt dat geen onduidelijkheid bestaat voor de bijzondere opsporingsdiensten. Kanttekening daarbij is wel dat controle op de daadwerkelijke vernietiging niet in alle gevallen door de respondenten kon worden bevestigd. Ook bij die respondenten leefde de vraag in hoeverre de kaders van de Wpg daadwerkelijk werden nageleefd, omdat zij niet wisten of de vernietiging daadwerkelijk plaats vond.

3.3.4 Gegevens waarover het professioneel verschoningsrecht zich uitstrekt

4. Wat wordt er gedaan als opsporingsinstanties gegevens van een geheimhouder (professioneel verschoningsgerechtigde) tegenkomen?

Bij de vergaring van gegevens die zijn opgeslagen op een elektronische gegevensdrager of in een geautomatiseerd werk kan informatie van een geheimhouder voorbij komen. Dat doet zich voor als gegevens(bestanden) van verschoningsgerechtigden afkomstig zijn of de gegevensdragers bij de verschoningsgerechtigde zelf in beslag worden genomen.¹¹⁵ In dit laatste geval werd in de interviews door twee officieren van justitie genoemd dat in het geval inbeslagneming bij de geheimhouder zelf plaatsvindt, dit in nauw overleg met de rechter-commissaris gebeurt en dat ook een vertegenwoordiger van de betreffende beroepsgroep betrokken is. De respondenten noemden voor de inbeslagneming bij de advocaat de deken van de Orde van Advocaten.

Daar waar het gaat om het onderzoek aan gegevensdragers die bij derden (en dus niet bij een professioneel verschoningsgerechtigde zelf zijn in beslag genomen) kan het gaan om communicatie tussen de verdachte en diens raadsman, maar bijvoorbeeld ook verklaringen van artsen of communicatie met een geestelijke. Uit de antwoorden van de respondenten volgt dat er programma's bestaan om eventuele informatie afkomstig van verschoningsgerechtigden te filteren, zoals het systeem 'Xiraf' en het systeem 'Hansken'. Ondanks het bestaan van mogelijkheden tot filtering, blijken deze filters bij toepassing in de praktijk lastig om mee te werken. De praktijk lijkt op twee problemen te stuiten. Het eerste probleem is dat bij het maken van een gehele kopie (image) ook gegevens die onder

¹¹⁵ Met inachtneming van artikel 98 Sv.

de reikwijdte van het verschoningsrecht vallen worden vastgelegd. Filtering kan pas nadien plaatsvinden. Het andere probleem is dat de filtering (nog) niet op zodanige effectieve wijze werkt dat uit de betrokken gegevens wel al, maar ook alleen het materiaal dat onder het verschoningsrecht valt wordt uitgefilterd. Het blijkt ingewikkeld de filters precies zo te maken dat zij noch te breed, noch te smal filteren.¹¹⁶ Kortom, het vastleggen van gegevens waarover het verschoningsrecht zich uitstrekt is onvermijdelijk bij het maken van een forensische kopie (image) en de bestaande systemen om geheimhoudersinformatie te filteren zijn nog te grofmazig, waardoor er teveel of te weinig uitgefilterd wordt.

Volgens respondenten worden de gegevens van of met betrekking tot een geheimhouder dus wel in de forensische kopie (image) vastgelegd. Dit blijkt onvermijdelijk wanneer een forensische kopie van een elektronische gegevensdrager of geautomatiseerd werk wordt gemaakt. Tegelijk wordt in de interviews aangegeven dat er vervolgens een grote verantwoordelijkheid rust op het betreffende onderzoeksteam bij het verwerken van die gegevens. Die moeten immers erop toezien dat de betreffende gegevens die informatie over of van een verschoningsgerechtigde bevatten, niet worden gebruikt in het onderzoek. Uit de interviews is niet gebleken of dit in de praktijk altijd plaatsvindt.

Bij de bijzondere opsporingsdiensten wordt een afwijkend systeem gehanteerd ten aanzien van het omgaan met gegevens afkomstig van verschoningsgerechtigden. Onderstaand citaat illustreert dit systeem.

“Je hebt een image gemaakt van de totale harde schijf. Dat wordt geïndexeerd door forensische tools. Bij zoekslagen kan daar informatie van verschoningsgerechtigden tussen zitten. De rechercheur moet stoppen met kennisneming van de inhoud van dat materiaal, hij draagt het over aan een medewerker geheimhouding en dat is iemand die niet direct bij het onderzoek betrokken is. Als hij die globale beoordeling maakt dan gaat het via het OM naar de RC toe, die het oordeel maakt of het onder het verschoningsrecht valt. Dan moet die informatie ontoegankelijk gemaakt worden. Beschikking van de RC, de digitale rechercheur (die staat ook buiten het onderzoek), die zorgt dan dat het bestand uit de werkkopie verwijderd wordt, en indexeert het geheel opnieuw. De werkkopie wordt aangepast, niet de originele image zelf. Die is honderd procent ook vanwege gedoe met de advocaat. Hier is beleid over, de instructie geheimhouders van het OM.”¹¹⁷

Praktische problemen lijken voornamelijk te liggen in de eventuele vertraging van onderzoek die het gevolg is van het eerst ontoegankelijk maken van dergelijke informatie. Daarnaast speelt het probleem dat men niet in de originele forensische kopie data wil wijzigen omdat daarmee de validiteit van de gemaakte kopie wordt aangetast. Sommige

¹¹⁶ Bij gegevens opgeslagen op voorwerpen afkomstig van verschoningsgerechtigden is de verwachting reëel dat door filtering vrijwel alle gegevens worden uitgesloten.

¹¹⁷ Citaat afkomstig van een opsporingsambtenaar werkzaam bij een bijzondere opsporingsdienst.

officiëren van justitie geven aan de Instructie vernietiging geïntercepteerde gesprekken met geheimhouders van het Openbaar Ministerie als leidraad te hanteren.¹¹⁸

3.3.5 Gegevens die elders zijn opgeslagen in de cloud of in een netwerk

5. Wordt er ook gekeken naar gegevens die via de in beslag genomen smartphone, computer of tablet toegankelijk zijn en zijn opgeslagen in de cloud (denk aan Gmail, Dropbox, Picasa etc.)? Zo ja, worden deze gegevens ook gekopieerd/vastgelegd?

Bij de inbeslagneming van elektronische gegevensdragers en geautomatiseerde werken wordt veelal uitgegaan van de informatie direct afkomstig van de gegevensdrager of het geautomatiseerde werk zelf. In de huidige digitale wereld blijkt steeds meer informatie ook daarbuiten gedeeld, opgeslagen en verwerkt te worden, waarbij gesproken wordt van begrippen als 'cloud' en 'netwerk'.

Uit de bevindingen afkomstig uit de interviews met de respondenten blijkt, dat in de praktijk nog relatief weinig gebruik wordt gemaakt van het vergaren van gegevens die zijn opgeslagen in de cloud of als gegevens(bestand) elders in een netwerk. Door diverse respondenten, waaronder de bijzondere opsporingsdiensten en enkele officieren van justitie, werd aangegeven dat er nog relatief weinig ervaring is op dit gebied.

Een genoemde, mogelijke verklaring hiervoor is dat in de praktijk problemen met het territorialiteitsbeginsel worden ervaren. Gegevens die zich op buitenlands grondgebied bevinden zijn moeilijker te bemachtigen vanwege het feit dat in dergelijke gevallen meestal een rechtshulpverzoek is vereist. Zodra blijkt dat informatie zich in de cloud bevindt, kan het voorkomen dat de betreffende servers, en dus de daarop opgeslagen informatie zich in het buitenland bevindt. Veelal wordt er dan ook in de praktijk vanuit gegaan dat zodra gegevens zijn opgeslagen in de cloud, deze zich in het buitenland bevinden.

De problemen met soevereiniteit en territorialiteit vormen een belangrijk discussiepunt binnen de uitvoering in de huidige praktijk. Hierbij is een verschil waar te nemen tussen de bijzondere en reguliere opsporingsdiensten. Enkele digitaal rechercheurs gaven te kennen dat in het geval onbekend was waar de betreffende data zou staan, de informatie ook zonder rechtshulpverzoek zou mogen worden verkregen. Dit is dan wel altijd in overleg met de rechter-commissaris. De bijzondere opsporingsdiensten lijken zich strikter te houden aan de grenzen van het soevereiniteitsbeginsel. Vele respondenten lieten weten behoefte te hebben aan praktische oplossingen op dit punt.¹¹⁹

¹¹⁸ Deze instructie is gebaseerd op artikel 126aa lid 2 Sv.

¹¹⁹ Zie nader over dit onderwerp B.J. Koops e.a., *Misdaad en opsporing in de wolken, Knelpunten en kansen van cloud computing voor de Nederlandse opsporing*, Tilburg: Universiteit van Tilburg 2012.

3.3.6 Teruggave van elektronische gegevensdragers en geautomatiseerde werken na afronding van het onderzoek

6. Wat gebeurt er met de gegevensdrager / het geautomatiseerde werk indien het onderzoek daaraan is afgerond (teruggeven aan beslagene, deponeren bij Domeinen Roerende Zaken, anders)? Indien beslag wordt voortgezet, op welke grond?

Uit de bevindingen afkomstig uit de interviews blijkt dat in de meeste gevallen de betreffende gegevensdrager of het geautomatiseerde werk, indien de beslagene daarvan geen afstand heeft gedaan, wordt teruggegeven aan de beslagene, nadat de rechter daartoe heeft beslist. Dit betreft dus het voorwerp (de gegevensdrager) zelf met inbegrip van de daarop opgeslagen gegevens. Dit is uiteraard anders wanneer de rechter beslist tot verbeurdverklaring of onttrekking aan het verkeer van het voorwerp.

Uitzonderingen op de regel van teruggave aan de beslagene doen zich voornamelijk voor in het geval dat de gegevensdrager of het geautomatiseerde werk ‘illegale content’ bevat en het voorwerp niet verbeurd verklaard of onttrokken aan het verkeer wordt. Ook in dat geval wordt de gegevensdrager of het geautomatiseerde werk zelf niet teruggegeven aan de beslagene, hetgeen door enkele officieren van justitie in de interviews werd bevestigd. Het is in overleg met de officier van justitie soms wel mogelijk om bij wijze van uitzondering bepaalde privébestanden apart te retourneren aan de verdachte, op diens verzoek. Dit voorbeeld werd door diverse respondenten gegeven.

“In principe wordt alles teruggegeven. Tenzij kinderporno. Vroeger kreeg ik nog weleens het verzoek om kinderporno ertussen uit te halen en de rest terug te geven, ik heb het een keer uitgerekend en dat kost ongeveer 2000 euro voor een harde schijf van 89 euro. Wat we wel vaak doen, mocht zoonlief bezig met zijn scriptie en die gegevens staan er op, die scriptie halen we er dan af op verzoek van de officier. Wij hebben nooit rechtstreeks contact met degene van wie de voorwerpen zijn.”¹²⁰

Ten aanzien van de informatievoorziening aan de verdachte in het geval de gegevensdrager of het geautomatiseerde werk niet wordt teruggegeven, volgden wisselende antwoorden. Hierbij kan zowel gedacht worden aan de situatie dat de gegevensdrager vanwege illegale content niet wordt teruggegeven, maar ook in het geval van destructief onderzoek, waarna het voorwerp niet meer te gebruiken is. Over enige vorm van kennisgeving hiervan werd door respondenten niet eenduidig geantwoord.

In sommige gevallen wordt volstaan met het geven van een nieuwe, lege versie (een nieuwe harde schijf), of kan een schadevergoeding worden vastgesteld ter compensatie. De

¹²⁰ Citaat afkomstig van een opsporingsambtenaar.

respondenten in dit onderzoek hebben weinig ervaring met het al dan niet toekennen van schadecompensatie, omdat, zo stellen ze, dit buiten hun werkveld ligt.

3.3.7 Onderzoek aan geautomatiseerde werken zonder formele inbeslagneming

7. Komt het voor dat door een opsporingsambtenaar onderzoek wordt verricht aan een smartphone, computer etc. zonder dat deze in beslag wordt genomen? Zo ja, wordt van dergelijk onderzoek proces-verbaal gemaakt? Worden bij dergelijk onderzoek door de opsporingsambtenaar ook gegevens vastgelegd (gekopieerd) ten behoeve van de opsporing?

Uit de bevindingen volgt dat het voorkomt dat een opsporingsambtenaar ter plaatse in een geautomatiseerd werk kijkt om van de daarop opgeslagen gegevens kennis te nemen, zonder dat wordt overgegaan tot het daadwerkelijk onder zich nemen of gaan houden van dat voorwerp ten behoeve van de strafvordering. Dit doet zich voornamelijk voor in de situatie dat een betrokkene vrijwillig een mobiele telefoon toont met als doel dat de opsporingsambtenaar kennis kan nemen van de daarop zichtbare gegevens (zoals een sms'je met een bedreiging of een filmpje van een situatie). Uit de reacties van de respondenten – in het bijzonder de opsporingsambtenaren die minder bij grootschalige gegevensverwerking betrokken zijn – blijkt dat dit regelmatig voorkomt. Ook enkele officieren van justitie en digitaal rechercheurs konden dit op basis van hun ervaring bevestigen.

Ook kan het voorkomen dat de opsporingsambtenaar kennis neemt van gegevens op een geautomatiseerd werk zonder dat sprake is van vrijwillige afgifte daarvan. In sommige gevallen wordt zelfs geen proces-verbaal opgemaakt van de bekeken gegevens, ook niet wanneer naar aanleiding daarvan verdere actie wordt ondernomen. Als voorbeeld is genoemd het bekijken van beelden alvorens de afweging te maken de gegevensdrager of het geautomatiseerde werk al dan niet in beslag te nemen.

Ondanks dat er geen kennisgeving van inbeslagneming opgemaakt wordt, aangezien de gegevensdrager niet in beslag is genomen, worden de uitkomsten van het onderzoek aan die gegevensdrager in sommige gevallen wel geregistreerd in een proces-verbaal.

Het verrichten van onderzoek aan een elektronische gegevensdrager of geautomatiseerd werk, zonder dat het voorwerp uiteindelijk in beslag wordt genomen, komt ook voor tijdens doorzoekingen. Indien de bekeken gegevens gebruikt worden voor het onderzoek, wordt dit in de meeste gevallen wel opgenomen in proces-verbaal, zo blijkt uit de antwoorden van respondenten. Deze situatie werd voornamelijk geschetst door enkele officieren van justitie en digitaal rechercheurs. Het komt ook voor dat het ter plaatse bekijken van gegevens op een gegevensdrager plaats heeft met het oog op het uitsluiten

van voorwerpen van inbeslagneming. Het bekijken dient dan om zeker te stellen dat het voorwerp niet in beslag hoeft te worden genomen.

Uit de gehouden interviews volgt dat er ook andere situaties zijn waarin een opsporingsambtenaar in een geautomatiseerd werk kijkt zonder dat het betreffende voorwerp formeel in beslag genomen is. Deze situatie doet zich voornamelijk voor bij de toepassing van de insluitingsfouillering. Diverse respondenten (voornamelijk digitaal rechercheurs) lieten weten dat het voorkomt dat, indien een telefoon niet vergrendeld is, de bij de insluitingsfouillering afgegeven telefoon wordt bekeken. Dat beperkte zich in sommige gevallen tot het enkel bekijken van de gegevens(bestanden) op de telefoon, maar in bepaalde gevallen waarin dit noodzakelijk werd geacht, werd ook een forensische kopie gemaakt. Uit de interviews is niet gebleken in hoeverre hierbij toestemming van de officier van justitie werd gevraagd. Enige digitaal rechercheurs spraken het vermoeden uit dat dit laatste niet het geval zou zijn. Diverse digitaal rechercheurs uitten hun onvrede over deze bestaande praktijk. Die onvrede stelde, zo is vastgesteld, met name op de validiteit van de op deze wijze vastgelegde en bekeken gegevens. Die validiteit van de aangetroffen gegevens(bestanden) is namelijk groter indien die op een image van de gegevensdrager staan en wanneer niet eerst handelingen door de opsporingsambtenaar zijn verricht aan het geautomatiseerde werk die mogelijk tot wijziging van de gegevens hebben geleid. Laatstgenoemde bezwaren over validiteit van gegevens leven overigens veel sterker bij digitale rechercheurs dan bij de rechercheurs die minder met gegevensverwerking bezig zijn.

Er bestaat in de praktijk onduidelijkheid over de vraag in hoeverre het wettelijk is toegestaan om tijdens de inverzekeringstelling van de verdachte in zijn in het kader van de insluitingsfouillering afgegeven telefoon te kijken. Onder meer die onduidelijkheid zet bij de digitale rechercheurs aan tot terughoudendheid ten aanzien van de toepassing hiervan. Dat laatste leeft wederom minder bij de andere hierboven genoemde groep van opsporingsambtenaren.

3.3.8 Het wissen van bestanden alvorens de gegevensdrager wordt teruggegeven

8. Komt het voor dat bestanden van een smartphone, computer etc. worden gewist voordat deze worden teruggegeven aan de beslagene? Als bestanden worden gewist, wie beslist daarover? Worden alle bestanden gewist of alleen de in de ogen van de opsporingsambtenaar ‘ illegale content’? Wordt de verdachte daarvan in kennis gesteld?

Voorafgaand wordt opgemerkt dat diverse aspecten ten aanzien van de bewaring en teruggave tevens bij andere onderzoeksvragen aan de orde zijn gekomen (paragraaf 3.3.6). In deze paragraaf wordt de focus gelegd op het wissen van gegevens(bestanden) op gegevensdragers, voordat deze wordt teruggegeven aan de beslagene.

Onder de respondenten bestaat discussie over het al dan niet gedeeltelijk of geheel wissen van gegevens alvorens de gegevensdrager wordt teruggegeven aan de beslagene. Meer in het bijzonder wanneer dat een (gedeeltelijk) illegale content betreft.¹²¹ Het lijkt in de praktijk lastig uitvoerbaar om gegevens gedeeltelijk te wissen en de oorspronkelijke gegevensdrager zonder illegale content terug te geven aan de beslagene. Het wissen neemt veel tijd in beslag en het is onvoldoende duidelijk of beelden definitief verwijderd zijn. Sommige officieren van justitie menen dat illegale content teruggeven een strafbaar feit oplevert. Over teruggave van voorwerpen met daarop illegale content blijkt verschil in interpretatie te bestaan tussen verschillende regio's. De opsporingsambtenaren die met grotere regelmaat betrokken zijn bij de digitale opsporing zijn minder geneigd tot teruggave van voorwerpen met illegale content. Andere opsporingsambtenaren gaan lichtvoetiger om met de beslissing tot teruggave van dergelijke voorwerpen. Op de vraag wat er gebeurt met de gegevens op de gegevensdrager dan wel het geautomatiseerde werk indien het onderzoek daaraan is afgerond, werd door een van de respondenten als volgt gereageerd.

“Afhankelijk van het doel. In het merendeel van de gevallen zal het item terug gaan. Als het gaat om strafbare gegevens die erop staan gaat het item niet terug maar moet het verbeurd worden verklaard. Als een rechtbank beslist dat een item terug moet waarvan is vastgesteld dat er kinderporno op staat, maar er geen veroordeling is, dan heb je een hele lastige situatie. Het teruggeven levert in principe een strafbaar feit op. Praktische beslissing (zonder expliciete wettelijke grondslag), is of de gegevensdrager in het geheel ‘wipen’, of een deel daarvan (maar dat is lastig, want ook daar kunnen bestanden op staan waar nare dingen op staan). Dit is een hele lastige situatie. Er kunnen weleens beelden zijn van een doorzoeking (camera in huis), maar er is niet echt een grondslag om die beelden weg te kunnen halen. Eventueel vanwege tactische overwegingen, afscherming van de methodieken, maar ook dan is er niet echt een wettelijke grondslag om te vernijderen. Vooral bij de politie bestaat hier veel onrust over.”¹²²

Een ander aspect dat bij de vragen naar het wissen van gegevens voorafgaand aan de eventuele teruggave van een gegevensdrager veelvuldig wordt genoemd, betreft de gegevens geregistreerd door een particuliere beveiligingscamera. De mogelijkheid dat daarop beelden van de doorzoeking zijn geregistreerd, waarbij de betrokken opsporingsambtenaren herkenbaar in beeld zijn gebracht wordt regelmatig aangehaald. Dit kan bijvoorbeeld problemen opleveren voor de veiligheid van die opsporingsambtenaren. Bij de opsporingsinstanties leeft de vraag in hoeverre die beelden verwijderd mogen worden. Ondanks de onduidelijkheid lijkt de bestaande praktijk dat die beelden als uitgangspunt worden gewist. Het wissen van gegevens kan als een ambtshandeling worden opgevat waarover in beginsel in een proces-verbaal dient te worden gerelateerd. Dit blijkt echter niet in alle gevallen te gebeuren.

¹²¹ Door de respondenten wordt veelal kinderporno als voorbeeld gegeven. Wellicht kan ook worden gedacht aan grote onverklaarbare hoeveelheden creditcardgegevens of malware (digitale inbrekersgereedschap).

¹²² Citaat afkomstig van een officier van justitie.

Het ontbreken van een concrete wettelijke regeling over het wissen van bestanden wordt in de opsporing als problematisch ervaren.

4. Conclusies en observaties

4.1 Inleiding

In dit onderdeel worden de voornaamste bevindingen en conclusies van het onderzoek bijeen gebracht. Daartoe worden eerst de voornaamste conclusies per onderzoeksvraag geformuleerd, uitgesplitst in de kwantitatieve onderzoeksvragen en de kwalitatieve onderzoeksvragen. Daarna volgen nog enkele overkoepelende conclusies die op verschillende deelvragen of op het gehele onderzoek betrekking hebben.

4.2 Kwantitatieve onderzoeksvragen: cijfers over inbeslagneming, onderzoek en het wissen van gegevens

A) Zijn er cijfers bekend over hoe vaak een opsporingsambtenaar een mobiele telefoon, laptop, computer, usb-stick etc. in beslag neemt (i) op grond van een zelfstandige inbeslagnemingsbevoegdheid (zoals artikelen 95, 96, 96a en 96b Sv) en (ii) tijdens een doorzoeking van een plaats door de officier van justitie (artikel 96c Sv) of door de rechter-commissaris (artikel 110 Sv)? Zo ja, wat zeggen deze cijfers?

Geconcludeerd wordt, dat op basis van de bestaande cijfers over de inbeslagneming van en het daaropvolgende nadere onderzoek dat wordt gedaan aan elektronische gegevensdragers en geautomatiseerde werken, aanzienlijke aantallen elektronische gegevensdragers en geautomatiseerde werken door de opsporingsambtenaren in beslag worden genomen. Dit kan onderbouwd worden met cijfers, hoewel die wel genuanceerd moeten worden, zoals is toegelicht in paragraaf 3.2.1. In deze cijfers wordt geen onderscheid gemaakt tussen de grond voor inbeslagneming en de betreffende autoriteit onder wiens verantwoordelijkheid of door wie de voorwerpen zijn in beslag genomen.

De hoeveelheid voorwerpen die kunnen worden aangemerkt als elektronische gegevensdrager of geautomatiseerd werk, is bij de opsporingsambtenaren niet goed bekend. Gelet op de antwoorden van de respondenten komt die situatie in de dagelijkse praktijk zeer regelmatig voor. Uit de antwoorden van de respondenten kan voorts worden afgeleid dat het merendeel van deze voorwerpen tijdens de doorzoeking ter inbeslagneming, onder leiding van de officier van justitie of de rechter-commissaris wordt in beslag genomen en niet op grond van een zelfstandige inbeslagnemingsbevoegdheid van de opsporingsambtenaar.

B) Zijn er cijfers bekend over hoe vaak een opsporingsambtenaar onderzoek verricht aan een smartphone, computer etc. zonder dat deze in beslag wordt genomen?

Concrete cijfers lijken bij de opsporingsdiensten niet bekend. Dat hangt samen met het feit dat onderzoeken aan gegevensdragers zonder dat deze in beslag zijn genomen niet worden geregistreerd. Uit de interviews is evenwel naar voren gekomen dat het voorkomt dat opsporingsambtenaren ter plaatse in een geautomatiseerd werk kijken om van de daarop opgeslagen gegevens kennis te nemen, zonder dat het voorwerp formeel ten behoeve van de waarheidsvinding in beslag wordt genomen.

C) Zijn er cijfers bekend over hoe vaak bestanden van een smartphone, computer etc. worden gewist voordat deze wordt teruggegeven aan de beslagene?

Cijfers met betrekking tot het wissen van bestanden van elektronische gegevensdragers of geautomatiseerde werken zijn niet bekend aangezien registratie van dergelijke handelingen niet blijkt plaats te hebben.

4.3 Kwalitatieve onderzoeksvragen: inbeslagneming, onderzoek en gegevensverwerking door opsporingsinstanties

1. Wie beslist dat aan de in beslag genomen gegevensdrager of in het in beslag genomen geautomatiseerde werk onderzoek mag worden gedaan en dat de daarop of daarin opgeslagen gegevens mogen worden vastgelegd?

De inbeslagneming van elektronische gegevensdragers en geautomatiseerde werken vindt in de regel plaats met als doel het doen van onderzoek daaraan in het kader van de waarheidsvinding. Degene die beslist een gegevensdrager in beslag te nemen, beslist daarmee tevens tot het doen van onderzoek daaraan. Aanvullende of nadere toetsen omtrent welke gegevens in de voorwerpen nader (mogen) worden onderzocht, vinden niet plaats. Dat laatste geldt ook voor de omvang van het aantal in beslag te nemen voorwerpen. Het moment waarop dergelijke afwegingen worden gemaakt, is in de regel het moment van inbeslagneming. Die afweging wordt mede gestuurd door de vooraf vastgestelde onderzoeksvraag. Het achterwege laten van nader onderzoek aan de gegevensdrager is in de meeste gevallen het resultaat van praktische overwegingen. Het komt voor dat slechts een beperkte hoeveelheid informatie wordt bekeken om het voorwerp vervolgens onmiddellijk weer terug te geven aan de betrokkene.

De autoriteit die beslist over de omvang van de in beslag te nemen voorwerpen en het verrichten van onderzoek daaraan is degene onder wiens gezag een doorzoeking of inbeslagneming plaatsvindt. In veruit de meeste gevallen is dit de officier van justitie of de rechter-commissaris. De autoriteiten worden daarbij in bepaalde gevallen geadviseerd door opsporingsambtenaren van de digitale recherche. De aard van de op de in beslag te nemen voorwerpen aanwezige gegevens heeft geen invloed op het al dan niet overgaan tot

inbeslagneming. Dat is uiteraard anders in het geval er sprake is van inbeslagneming bij een verschoningsgerechtigde. In de huidige praktijk wordt in de meeste gevallen in de voorbereiding en voornamelijk ter plaatse een bewuste afweging gemaakt omtrent de in beslag te nemen gegevensdragers. Als uitgangspunt wordt ervan uitgegaan dat alle op de voorwerpen aanwezige gegevens mogen worden onderzocht. Ten aanzien van de gegevens die nog gedurende het onderzoek worden gegenereerd (dus na het moment van inbeslagneming) kan het in zeldzame gevallen voorkomen dat die alsnog, met toestemming van de officier van justitie, worden gebruikt in het onderzoek. Met de kanttekening dat bij hoogwaardig technisch forensisch onderzoek veelal wordt voorkomen dat nog gegevens worden gegenereerd of dat gegevens op de gegevensdrager van buitenaf worden beïnvloed. Omtrent de aard van de gegevens en de wijze waarop daarmee dient te worden omgegaan, lijkt geen breed gedragen beleid te bestaan.

Geconstateerd kan worden dat de afweging omtrent de in beslag te nemen voorwerpen sterk afhankelijk is van enerzijds de verdenking van het strafbare feit en de omvang van het onderzoek, maar anderzijds ook van de bij de inbeslagneming betrokken autoriteit. Bij de doorzoeking ter inbeslagneming, onder leiding van een officier van justitie of rechter-commissaris, lijken - afhankelijk van de omstandigheden - in die afweging de beginselen van proportionaliteit en subsidiariteit meer te worden betrokken.

Als uitgangspunt wordt een kennisgeving van inbeslagneming opgemaakt. In de praktijk blijkt, in verband met bedrijfsprocesssystemen, een kennisgeving van inbeslagneming veelal nodig te zijn om de gegevens die zijn opgeslagen op een in beslag genomen gegevensdrager op juiste wijze in de systemen te kunnen verwerken. Uit de reacties van de respondenten blijkt het onderscheid tussen de terminologie van de kennisgeving van inbeslagneming ten behoeve van het Openbaar Ministerie en het bewijs van ontvangst voor de beslagene beperkt bekend te zijn. De respondenten stellen dat het voorkomt dat een uitzondering op de kennisgeving van inbeslagneming wordt gemaakt, waarbij dan op een later tijdstip alsnog kennis wordt gegeven. Met uitstel van kennisgeving lijkt door de respondenten bedoeld te worden op het uitstellen van het verstrekken van het bewijs van ontvangst. Indien het voorwerp wordt teruggegeven, blijft kennisgeving van inbeslagneming (ook hier wordt dan waarschijnlijk bedoeld op bewijs van ontvangst) ook achterwege op grond van de veronderstelling dat de betrokkene op de hoogte moet zijn van het feit dat onderzoek heeft plaatsgevonden dan wel dat hem dat op later tijdstip wordt meegedeeld. Er lijken twee verschillende redenen te zijn voor deze handelswijze. Aan de ene kant lijken respondenten vermindering van administratieve lasten aan te voeren, immers beslagene is reeds op de hoogte van de inbeslagneming. Aan de andere kant geven respondenten aan dat er onderzoeksbelangen zijn die het uitstel van het informeren van beslagene rechtvaardigen. In de praktijk leeft de vraag sterk in hoeverre dit uitstel een wettelijke grondslag heeft, en of in die gevallen dat uitstel voor komt sprake is van heimelijke inbeslagneming.

2. Worden gegevens gekopieerd voor verder onderzoek? Zo ja, alle gegevens ('image' maken) of alleen een deel daarvan? In geval van een deel, waarom een/dat deel en niet alle gegevens?

Het onderzoek levert een wisselend beeld op, voor zover dat het kopiëren van gegevens voor nader onderzoek betreft. In de situatie waarbij gegevensdragers worden aangedragen bij opsporingsambtenaren werkzaam in de sfeer van het hoogwaardig technisch forensisch onderzoek, wordt vrijwel uitsluitend een volledige kopie (image) van de op die gegevensdragers aanwezige gegevens gemaakt. De opsporingsambtenaren die minder met grootschalige gegevensverwerking werken blijken vaker te volstaan met het vastleggen van beperkte hoeveelheden gegevens(bestanden).

Ten aanzien van de image van gegevensdragers geldt dat in de meeste gevallen een image wordt gemaakt van alle gegevens op de gegevensdrager en niet van gedeelten daarvan. Die keuze om alle gegevens op de image vast te leggen, is ingegeven met het oog op de mogelijkheid voor de verdediging om contra-expertise te laten uitvoeren en de mogelijkheid om de betrouwbaarheid van de gekopieerde gegevens aan te tonen.

Het niet maken van een image van alle gegevens kan samenhangen met de encryptie van die gegevens of een blokkering van de toegang tot die gegevens of de gegevensdrager. Hier zijn twee situaties denkbaar. Ten eerste de situatie dat het geautomatiseerde werk is vergrendeld (met bijvoorbeeld een wachtwoord of een code). Ten tweede bestaat de situatie dat het geautomatiseerd werk wel toegankelijk is, maar dat de gegevens(bestanden) versleuteld zijn. Het benutten van vergaarde gegevens is door het gebruik van encryptie niet altijd mogelijk.

Op grond van artikel 125k Sv kan aan personen (met uitzondering van de verdachte) een bevel tot ontsluiting van gegevens(dragers) worden gegeven tijdens een doorzoeking van een plaats ter vastlegging van gegevens. Dat ontsleutelingsbevel kan op grond van het genoemde artikel niet gegeven worden voor de ontsluiting van in beslag genomen gegevensdragers. De vraag is gesteld in hoeverre het wenselijk zou zijn om een ontsleutelingsbevel ook mogelijk te maken in het geval van in beslag genomen gegevensdragers. Bij respondenten bleek aan het scheppen van dergelijke mogelijkheid geen unaniem gevoelde behoefte te bestaan. Voor zover de mogelijkheid ter sprake kwam een dergelijk bevel ook tot de verdachte te richten, werd hierbij ook verwezen naar de beperkingen die het nemo teneturbeginsel in deze situatie met zich brengt.

3. Wat wordt gedaan met de gekopieerde gegevens? Hoe en hoe lang worden ze bewaard?

Kopieën van gegevens worden in de bedrijfssystemen van de opsporingsdiensten vastgelegd. De vraag wie toegang tot die gegevens heeft, is niet landelijk maar regionaal

geregeld. Het regionale gehanteerde beleid daaromtrent is niet eenduidig. Bij de meer op digitaal rechercheren gefocuste diensten wordt veelal een bewuste afweging gemaakt welke opsporingsambtenaren toegang dienen te krijgen tot de gegevens(bestanden). Rechercheurs die niet bij een concreet opsporingsonderzoek betrokken zijn, hebben dan geen toegang tot de gegevens(bestanden).

Van het beleid omtrent de bewaring en vernietiging na afronding van het onderzoek zijn niet alle respondenten op de hoogte. Sommigen verwijzen naar de Wpg, maar kennen de inhoud van die regelgeving niet. De indruk bestaat dat de wijze waarop en het moment waarop gegevens vernietigd moeten worden dan wel ontoegankelijk moeten worden gemaakt, geen centrale regie kent. Dat beeld wordt bevestigd in de recent uitgevoerde Wpg-audit van de Auditdienst.¹²³

Zoals in hoofdstuk 2 is opgemerkt, is de Wpg van toepassing op gegevens die in het kader van de uitvoering van de politietaak als omschreven in artikelen 3 en 4 Politiewet 2012, zijn vastgelegd. Dat betreft ook gegevens vastgelegd in het kader van nader onderzoek aan een in beslag genomen elektronische gegevensdrager of geautomatiseerd werk. In de Wpg wordt in artikel 3 bepaald met welke doeleinden de gegevens mogen worden verwerkt. De Wpg stelt ook regels omtrent de bewaartermijnen en de vernietiging van die gegevens. Het Wetboek van Strafvordering kent dergelijke bepalingen niet, behoudens aanvullende regels voor gegevens die tijdens een doorzoeking van een plaats ter vastlegging van gegevens zijn vastgelegd. Zo is in artikel 125n Sv onder andere bepaald dat gegevens die tijdens een doorzoeking van een plaats ter vastlegging van gegevens, zijn vastgelegd en niet van betekenis zijn voor het opsporingsonderzoek moeten worden vernietigd.

4. Wat wordt er gedaan als opsporingsinstanties gegevens van een geheimhouder (professioneel verschoningsgerechtigde) tegenkomen?

Zoals beschreven in hoofdstuk 2 worden onder ‘brieven en geschriften’ in artikel 98 Sv ook elektronisch vastgelegde brieven en geschriften verstaan. Dit betekent dat bij het in beslag nemen van elektronische gegevensdragers en geautomatiseerde werken, het verschoningsrecht geëerbiedigd moet worden. Door de praktijk worden op dit gebied problemen ondervonden. Verschillende respondenten geven aan dat bestaande wet- en regelgeving hen onvoldoende duidelijkheid verschaft op welke wijze met dat verschoningsrecht moet worden omgegaan.

¹²³ Zie de privacy-audit die de Auditdienst Rijk (ADR) heeft uitgevoerd naar de naleving van de Wpg door de politie. De conclusie ten aanzien van dit onderdeel was dat de naleving van de bewaartermijnen onvoldoende op orde is. Zie *Kamerstukken II*, 2015/16, 33 842, nr. 3 en bijlage.

Ten behoeve van het onderzoek aan in beslag genomen voorwerpen waarop elektronische gegevens(bestanden) zijn vastgelegd bestaan programma's om gegevens waarover het professioneel verschoningsrecht zich uitstrekt te filteren. In de praktijk levert het filteren van gegevens, in het bijzonder waar het gaat om het onderzoek aan gegevensdragers die bij derden (en dus niet bij een professioneel verschoningsgerechtigde zelf zijn in beslag genomen) een lastige situatie op, omdat door het filteren een grote hoeveelheid gegevens(bestanden) wordt uitgesloten voor het onderzoek. In het geval geen gebruik wordt gemaakt van de mogelijkheid tot filteren, zijn alle gegevens(bestanden) te raadplegen en rust er een grote verantwoordelijkheid op het onderzoeksteam om die gegevens vervolgens niet te benutten. Dat brengt mee dat op dit moment in de praktijk de gegevens afkomstig van geheimhouders weliswaar worden vastgelegd, maar dat de resultaten daarvan vervolgens terzijde worden gelegd. Uit de interviews blijkt dat bepaalde bijzondere opsporingsdiensten een afwijkend systeem ten aanzien van het omgaan met gegevens afkomstig van geheimhouders hanteren, waarbij die gegevens voor de tactische opsporingsbeambten niet te raadplegen zijn. Zij werken met een systeem van twee kopieën, de image en een werkkopie waar de betreffende gegevens uit gehaald worden. Door de overige respondenten is het gebruik van dit systeem niet benoemd. In de praktijk wordt met name de vertraging van het onderzoek die het ontoegankelijk maken van dergelijke informatie veroorzaakt, als problematisch beschouwd. Die vertraging wordt veroorzaakt doordat per afzonderlijk gegevens(bestand) moet worden beoordeeld of dit al dan niet onder de reikwijdte van het verschoningsrecht valt.

5. Wordt er ook gekeken naar gegevens die via de in beslag genomen smartphone, computer of tablet toegankelijk zijn en zijn opgeslagen in de cloud (denk aan Gmail, Dropbox, Picasa etc.)? Zo ja, worden deze gegevens ook gekopieerd/vastgelegd?

De huidige wet kent geen bevoegdheid om via een in beslag genomen geautomatiseerd werk gegevens te vergaren die elders (in de cloud) zijn opgeslagen. Ook ontbreken beleidsregels ten aanzien van dergelijk onderzoek. Een dergelijke bevoegdheid bestaat wel indien tijdens een doorzoeking van een plaats ter vastlegging van gegevens elders opgeslagen gegevens rechtmatig kunnen worden benaderd (de netwerkzoeking, bedoeld in artikel 125j Sv). In dat geval moet het via het netwerk verbonden elders aanwezige geautomatiseerde werk wel rechtmatig toegankelijk zijn.

Zoals hierboven is vermeld, wordt bij de inbeslagneming van elektronische gegevensdragers en geautomatiseerde werken als uitgangspunt gehanteerd dat onderzoek mag worden gedaan aan alle gegevens. Het vergaren van gegevens die zijn opgeslagen in de cloud dan wel in een netwerk vindt sporadisch plaats. Dat hangt onder meer samen met vragen die leven omtrent schendingen van de soevereiniteit van andere landen. De bijzondere opsporingsdiensten hanteren met betrekking tot de mogelijke schending van

soevereiniteit van andere landen een zeer strikt beleid. Dat beleid hanteert het uitgangspunt dat bij twijfel omtrent schendingen van soevereiniteit van andere landen gegevens niet worden vastgelegd.

Het is wenselijk de praktijk duidelijkheid te verschaffen over de grenzen en mogelijkheden van grensoverschrijdend onderzoek in verband met de door de opsporingsdiensten ervaren problemen met de territoriale grenzen.

6. Wat gebeurt er met de gegevensdrager / het geautomatiseerde werk indien het onderzoek daaraan is afgerond (teruggeven aan beslagene, deponeren bij Domeinen Roerende Zaken, anders)? Indien beslag wordt voortgezet, op welke grond?

Bij teruggave van de gegevensdrager, met inbegrip van de daarop opgeslagen gegevens wordt in eerste instantie geleund op het oordeel van de rechter. Indien de rechter beslist tot teruggave van het voorwerp, wordt het voorwerp teruggegeven aan de beslagene.

In bepaalde gevallen waarin geen sprake is van verbeurdverklaring of onttrekking aan het verkeer van de gegevensdrager, wordt een meer praktische oplossing gevonden indien het onwenselijk is alle op de gegevensdrager opgeslagen gegevens te retourneren (bijvoorbeeld in het geval van illegale content). Deze praktische oplossing kan eruit bestaan dat het voorwerp wordt teruggegeven uitgerust met een nieuwe harde schijf of dat een schadevergoeding ter compensatie van het niet teruggeven van het voorwerp, wordt uitbetaald. Omtrent de hoogte van een eventuele schadevergoeding kunnen de respondenten geen uitspraken doen.

Ten aanzien van de informatievoorziening aan de verdachte in het geval de gegevensdrager of het geautomatiseerde werk niet wordt teruggegeven buiten de situatie van de verbeurdverklaring om, volgden wisselende antwoorden. Hierbij kan zowel gedacht worden aan de situatie dat de gegevensdrager vanwege illegale content niet wordt teruggegeven, maar ook in het geval van destructief onderzoek, waarna het voorwerp niet meer te gebruiken is. De respondenten verklaarden gevraagd naar de kennisgeving hieromtrent niet eenduidig.

7. Komt het voor dat door een opsporingsambtenaar onderzoek wordt verricht aan een smartphone, computer etc. zonder dat deze in beslag wordt genomen? Zo ja, wordt van dergelijk onderzoek proces-verbaal opgemaakt? Worden bij dergelijk onderzoek door de opsporingsambtenaar ook gegevens vastgelegd (gekopieerd) ten behoeve van de opsporing?

Het komt voor dat opsporingsambtenaren onderzoek verrichten aan een smartphone, computer etc. zonder dat deze formeel ten behoeve van de waarheidsvinding in beslag wordt genomen. Meer specifiek gaat dit om de categorie geautomatiseerde werken. Dit betreft voornamelijk situaties waarin betrokkenen vrijwillig gegevens(bestanden) tonen met als doel dat de opsporingsambtenaar kennis kan nemen van de daarop zichtbare gegevens (te denken valt aan een sms'je met een bedreiging of een filmpje van een situatie). Het komt ook voor dat de opsporingsambtenaar kennisneemt van de gegevens op het geautomatiseerde werk, zonder dat sprake is van een vrijwillige afgifte. De respondenten merkten op dat in dergelijke situaties over het resultaat van het onderzoek aan die gegevensdrager in het algemeen wordt gerelateerd in een proces-verbaal. Onderzoek aan een elektronische gegevensdrager of een geautomatiseerd werk komt ook voor tijdens doorzoekingen. Dat onderzoek heeft in sommige gevallen tot doel bepaalde voorwerpen uit te sluiten van inbeslagneming. Daarover wordt in proces-verbaal melding gedaan. Dit kan worden beschouwd als een goede ontwikkeling vanwege de meer doordrongen belangenafweging en het zoveel mogelijk beperken van de inbreuk op de persoonlijke levenssfeer door alleen bij noodzakelijkheid tot inbeslagneming over te gaan. Dat laat de vraag open in hoeverre dit past binnen de kaders van de huidige wet- en regelgeving.

Ook tijdens de insluitingsfouillering komt het voor dat onderzoek zonder formele inbeslagneming plaats vindt. Het komt voor dat, indien de telefoon niet vergrendeld is, gedurende de insluitingsfouillering in de telefoon wordt gekeken. In sommige gevallen beperkte dit zich tot het enkele kijken, in bepaalde gevallen werd ook een forensische kopie gemaakt.

Met name bij de met digitale opsporing belaste rechercheurs bestaat onvrede over die praktijk. Bezorgdheid over de validiteit van de op die wijze vastgelegde gegevens ligt hieraan ten grondslag. Bij de opsporingsambtenaren blijkt geen duidelijk beeld te bestaan over de wettelijke bevoegdheden en de gevallen waarin gegevensdragers mogen worden onderzocht.

8. Komt het voor dat bestanden van een smartphone, computer etc. worden gewist voordat deze worden teruggegeven aan de beslagene? Als bestanden worden gewist, wie beslist daarover? Worden alle bestanden gewist of alleen de in de ogen van de opsporingsambtenaar ‘ illegale content’? Wordt de verdachte daarvan in kennis gesteld?

In het geval ‘illegale content’ op de gegevensdrager wordt aangetroffen, wordt de gegevensdragers als uitgangspunt niet meer teruggegeven, hoewel daar per regio verschillen in beleid in blijken te bestaan. In uitzonderlijke gevallen wordt een gegevensdragers wel teruggegeven na vernietiging van de bewuste gegevens(bestanden). In de regel wordt echter in bijzondere gevallen waarin de beslagene om teruggave van een specifiek

gegevens(bestand) dat op de gegevensdrager staat heeft verzocht, dat bestand van de gegevensdrager gekopieerd en afzonderlijk teruggegeven aan de beslagene. Hierbij kan worden gedacht aan gegevens(bestanden) die niet in relatie staan tot het strafbare feit en die van bijzondere waarde zijn voor de beslagene.

Een ander aspect dat bij de vragen naar het wissen van gegevens voorafgaand aan de eventuele teruggave van een gegevensdrager veelvuldig wordt genoemd, betreft de gegevens geregistreerd door een particuliere beveiligingscamera. De mogelijkheid dat op een beveiligingscamera beelden van de doorzoeking zijn geregistreerd, waarbij de betrokken opsporingsambtenaren herkenbaar in beeld zijn gebracht, wordt regelmatig genoemd. Hierdoor kunnen problemen ontstaan ten aanzien van de veiligheid van de opsporingsambtenaren. Bij de opsporingsinstanties leeft de vraag in hoeverre die beelden verwijderd mogen worden. Het wissen van gegevens kan als een ambtshandeling worden opgevat waarover in beginsel in proces-verbaal dient te worden gerelateerd. Dit gebeurt echter niet in alle gevallen.

Zoals gezegd kent de wet geen regeling voor het wissen van bestanden die zijn aangetroffen op een in beslag genomen elektronische gegevensdrager of geautomatiseerd werk. De wet kent daarentegen wel een regeling voor het wissen van gegevens die zijn aangetroffen in een geautomatiseerd werk tijdens een doorzoeking van een plaats ter vastlegging van gegevens. Het betreft de bevoegdheid tot het (tijdelijk) ontoegankelijk maken van bepaalde gegevens met betrekking tot welke of met behulp waarvan het strafbare feit is gepleegd. Een dergelijke ontoegankelijkmaking kan plaatsvinden indien dit noodzakelijk is ter beëindiging van een strafbaar feit of ter voorkoming van nieuwe strafbare feiten. Indien dergelijke gegevens ontoegankelijk zijn gemaakt, dan dient de rechter vervolgens te beslissen of die gegevens definitief mogen worden vernietigd. Buiten deze situaties om bestaat in de praktijk onduidelijkheid over de bevoegdheid tot het wissen van gegevens. Het ontbreken van een concrete wettelijke regeling daaromtrent wordt in de opsporing als problematisch ervaren en zou ten grondslag kunnen liggen aan het niet registreren van het, al dan niet gedeeltelijk, wissen van bestanden van een elektronische gegevensdrager of geautomatiseerd werk.

4.4 Algemene conclusie

Het totaalbeeld dat uit het onderzoek ontstaat, is dat op het kwantitatieve vlak weinig cijfermateriaal beschikbaar is om gegronde conclusies uit te kunnen afleiden. Ten aanzien van de aantallen in beslag genomen elektronische gegevensdragers en geautomatiseerde werken kan worden geconcludeerd dat uit het cijfermateriaal dat, per regio, ter beschikking van de onderzoekers is gesteld gesproken kan worden van aanzienlijke hoeveelheden in beslag genomen gegevensdragers. In die aantallen wordt geen onderscheid gemaakt tussen

de grond voor de inbeslagneming of de bevoegde autoriteit onder wiens verantwoordelijkheid of door wie het voorwerp in beslag is genomen.

Geconstateerd is dat binnen de verscheidene functies binnen de politie op andere wijze wordt omgegaan met inbeslagneming en het onderzoek aan het voorwerp dat in beslag genomen is. Uit de bevindingen van het onderzoek ontstaat het beeld van een spectrum met twee uitersten voor zover dat betrekking heeft op het onderzoek aan elektronische gegevensdragers en geautomatiseerde werken door de opsporingsautoriteiten. Enerzijds betreft dat het hoogwaardig technisch forensisch onderzoek aan vele elektronische gegevensdragers en geautomatiseerde werken met vele gegevens zoals dat onder meer door digitaal rechercheurs en het NFI wordt uitgevoerd. Anderzijds, een meer door de praktijk op het dagelijkse niveau van de opsporing ingegeven vorm van onderzoek. Bij dit laatste aspect van het spectrum blijkt weinig tot geen aandacht te worden besteed aan de validiteit van de vergaring en verwerking van de bewuste gegevens. De gegevens die daar worden vergaard zijn aanzienlijk beperkter van omvang.

Uit de interviews komt naar voren dat er relatief weinig tot geen intern beleid is geformuleerd ten aanzien van het onderzoek aan in beslag genomen elektronische gegevensdragers en geautomatiseerde werken. Daar waar wel beleid bestaat, wordt dat niet in alle gevallen voldoende nageleefd of heeft het beleid onvoldoende draagvlak. Daardoor ontbreekt een uniforme werkwijze als het gaat om de verwerking van, de toegang tot, de bewaring van en de ontsluiting van gegevens, maar ook als het gaat om gegevens die zich elders in een netwerk bevinden, dan wel op de zogenoemde cloud zijn opgeslagen. Ook wordt verschillend omgegaan met gegevens die eerst worden gegenereerd na inbeslagneming en met gegevens die (mogelijk) onder het verschoningsrecht vallen. Voorts geldt dit ten aanzien van het wissen van gegevens alvorens een gegevensdrager aan de beslagene wordt teruggegeven. De nu in de opsporingspraktijk gehanteerde werkwijze lijkt te zijn ingegeven door ervaringen in de praktijk waarbij zowel per regio als naar de aard van het aan de gegevensdragers uit te voeren onderzoek, verschillen zijn waar te nemen. Er zijn verschillen waarneembaar tussen de beantwoording van respondenten aan de hand van functie.

Uit hoofdstuk 2 is gebleken dat het Wetboek van Strafvordering nauwelijks specifieke regels kent ten aanzien van onderzoek aan in beslag genomen elektronische gegevensdragers of geautomatiseerde werken. Dit in tegenstelling tot het onderzoek aan gegevensdragers en geautomatiseerde werken tijdens een doorzoeking van een plaats ter vastlegging van gegevens, waarvoor de wet wel specifieke bepalingen bevat. Voorts lijkt in de lagere rechtspraak verschillend te worden geoordeeld over de vraag of de bepalingen inzake de inbeslagneming van voorwerpen, waaronder artikel 94 Sv, mede in het licht van het bepaalde in artikel 8 EVRM, een voldoende voorzienbare grondslag vormen voor het door een opsporingsambtenaar vergaren van gegevens die zijn opgeslagen op een in beslag genomen smartphone.

Een meer definitieve beantwoording van die vraag kan door de Hoge Raad worden gegeven, maar dat laat onverlet dat in dat geval een uitleg wordt gegeven aan een bepaling die in 1926 door de wetgever in het Wetboek van Strafvordering is opgenomen. Bovendien geldt in dat geval dat de uitleg over de reikwijdte van een bevoegdheid, zoals die in de wet is opgenomen, niet door de wetgever zelf nader wordt geduid, maar dat het aan de rechtspraak wordt overgelaten. Dat draagt, zo kan in ieder geval worden gezegd, bij aan een zwakkere democratische legitimering van de uitleg van de reikwijdte van een strafvorderlijke bevoegdheid, gelet op de technische voortschrijding. Waar procedurele voorzieningen nodig worden geacht, zal zulks de rechtsvormende taak van de Hoge Raad gemakkelijk te buiten gaan. Het lijkt in die zin dan ook wenselijk te noemen dat de wetgever zelfstandig een standpunt inneemt omtrent de reikwijdte van de bevoegdheid tot inbeslagneming en eventueel een nadere wettelijke regeling opstelt.

Dat laatste is van belang nu vanuit het Ministerie van Veiligheid en Justitie wordt gewerkt aan een modernisering van het Wetboek van Strafvordering. Die modernisering, die onderdeel uitmaakt van het programma Versterking Prestaties Strafrechtsketen (VPS), omvat eveneens de regelingen omtrent de dwangmiddelen.

Tegen die achtergrond en de hierboven geschetste uiteenlopende rechterlijke oordelen met betrekking tot de reikwijdte van de bevoegdheden tot inbeslagneming is het voor de praktijk van groot belang om een eenduidige werkwijze voorgeschreven te krijgen. Dit is in de huidige wet- en regelgeving op sommige gebieden onvoldoende duidelijk en blijkt in de praktijk vragen op te roepen.

Op basis van het onderzoek kan als algemene aanbeveling gelden dat ten aanzien van een aantal juridische en praktische aandachtspunten verheldering van geldende regelgeving gewenst is. Daar waar zulks aan de orde is, kan die verheldering op verschillende wijzen worden gerealiseerd. Dit hoeft niet in alle gevallen te gebeuren door wijziging van de bestaande wetgeving op het niveau van het Wetboek van Strafvordering. Ook het hanteren van een meer eenduidig beleid waaruit de praktijk handvatten voor de dagelijkse uitvoering kan ontleen, kan al voor de gewenste opheldering zorgen.

Samenvatting

In dit rapport wordt verslag gedaan van een inventariserend onderzoek naar een onderdeel van de huidige opsporingspraktijk omtrent de inbeslagneming. Het gaat daarbij vooral om het onderzoek dat na de inbeslagneming wordt gedaan aan elektronische gegevensdragers en geautomatiseerde werken door opsporingsambtenaren. Het rapport staat in het teken van een eventuele nadere normering van dergelijk onderzoek in het kader van de modernisering van het Wetboek van Strafvordering. De centrale vraagstelling van het onderzoek is: “Wat is er bekend over de inbeslagneming van en het daaropvolgende onderzoek dat wordt gedaan aan elektronische gegevensdragers en in geautomatiseerde werken door opsporingsambtenaren?”

Uit deze algemene vraagstelling vloeit een aantal kwantitatieve en kwalitatieve onderzoeksvragen voort die bij het inzichtelijk maken van de inbeslagnemingspraktijk als algemene leidraad zijn genomen.

In hoofdstuk 2 is het juridisch kader van de inbeslagneming van voorwerpen en het onderzoek aan in beslag genomen elektronische gegevensdragers en geautomatiseerde werken geschetst. Hieruit blijkt dat het Wetboek van Strafvordering nauwelijks specifieke regels kent ten aanzien van onderzoek aan in beslag genomen elektronische gegevensdragers of geautomatiseerde werken. Dit in tegenstelling tot het onderzoek aan gegevensdragers en geautomatiseerde werken tijdens een doorzoeking van een plaats ter vastlegging van gegevens, waarvoor de wet wel specifieke bepalingen bevat. Uit de besproken rechtspraak blijkt dat in lagere rechtspraak verschillend wordt geoordeeld over de vraag of de bepalingen inzake de inbeslagneming van voorwerpen, waaronder artikel 94 Sv, mede in het licht van het bepaalde in artikel 8 EVRM en tegen de achtergrond van technologische ontwikkelingen, nog een voldoende voorzienbare grondslag vormen voor het door een opsporingsambtenaar vergaren van gegevens die zijn vastgelegd op een in beslag genomen smartphone. De uitleg van die bepalingen voor zover die betrekking heeft op het in beslag nemen van voorwerpen teneinde nader onderzoek te verrichten om de daarop vastgelegde gegevens ter beschikking te krijgen met het oog op de waarheidsvinding, is niet eensluidend. Tot op heden is geen specifieke regelgeving op dit (deel)gebied voorhanden.

Ten aanzien van de kwantitatieve onderzoeksvragen komt naar voren dat op basis van de bestaande cijfers over de inbeslagneming van en het daaropvolgend onderzoek aan elektronische gegevensdragers en geautomatiseerde werken, aanzienlijke aantallen gegevensdragers door de opsporingsambtenaren in beslag worden genomen. Bij die cijfers wordt geen onderscheid gemaakt tussen de grond voor inbeslagneming en de betreffende autoriteit onder wiens verantwoordelijkheid of door wie de voorwerpen zijn in beslag genomen. Hoewel de situatie wel voorkomt, zijn geen concrete cijfers bekend ten aanzien

van het door een opsporingsambtenaar ter plaatse in een geautomatiseerd werk kijken om van de daarop opgeslagen gegevens kennis te nemen, zonder dat het voorwerp formeel in beslag wordt genomen. Met betrekking tot het wissen van bestanden van elektronische gegevensdragers of geautomatiseerde werken zijn ook geen cijfers bekend aangezien registratie daarvan achterwege blijft.

Ten aanzien van de kwalitatieve onderzoeksvragen wordt geconcludeerd dat in de meeste gevallen in de voorbereiding en voornamelijk ter plaatse een afweging wordt gemaakt omtrent de in beslag te nemen gegevensdragers. Deze afweging wordt in de meeste gevallen, gelet op het feit dat in de meeste gevallen de inbeslagneming plaatsvindt tijdens een doorzoeking van een plaats door de officier van justitie of de rechter-commissaris gemaakt. De uitkomst van die afweging is sterk afhankelijk van de verdenking van het strafbare feit en de omvang van het onderzoek, maar ook van de bij de inbeslagneming betrokken autoriteiten. Als uitgangspunt wordt ervan uitgegaan dat alle op de voorwerpen aanwezige gegevens mogen worden onderzocht, met uitzondering van de gegevens die onder het verschoningsrecht vallen.

Gegevens worden geheel of deels gekopieerd voor verder onderzoek, tenzij de gegevens versleuteld zijn of de toegang tot die gegevens geblokkeerd is. De kopieën worden in bedrijfssystemen vastgelegd. Het beleid omtrent toegang tot die bedrijfssystemen verschilt regionaal. Er lijkt geen centrale regie te bestaan met betrekking tot de wijze waarop en het moment waarop gegevens vernietigd moeten worden dan wel ontoegankelijk moeten worden gemaakt. De Wpg stelt regels omtrent de bewaartermijnen en de vernietiging van die gegevens, maar de inhoud daarvan is niet breed bekend in de praktijk. Het Wetboek van Strafvordering bevat geen bepalingen daaromtrent.

In de praktijk worden problemen ondervonden op het gebied van de inbeslagneming van elektronische gegevensdragers en geautomatiseerde werken voor zover gegevens binnen de reikwijdte van het verschoningsrecht vallen. De bestaande wet- en regelgeving lijkt daarover onvoldoende duidelijkheid te verschaffen aan de praktijk. Het filteren van gegevens waarover het professioneel verschoningsrecht zich uitstrekt, levert (nog) geen goed werkbaar resultaat voor het opsporingsonderzoek op.

Ten aanzien van het vergaren van gegevens die elders (in de cloud) zijn opgeslagen bevat de huidige wet geen specifieke bevoegdheid; ook beleidsregels ontbreken. Het vergaren van dergelijke gegevens vindt sporadisch plaats. Problemen hangen samen met vragen omtrent schendingen van de soevereiniteit van andere landen en de afwezigheid van een voldoende duidelijke wettelijke regeling op dit punt. Het uitgangspunt van beleid is, dat bij twijfel omtrent schendingen van soevereiniteit gegevens niet worden vastgelegd. Het is wenselijk de praktijk in dat kader duidelijkheid te verschaffen over de grenzen en mogelijkheden van grensoverschrijdend onderzoek.

Het komt voor dat opsporingsambtenaren onderzoek verrichten aan, voornamelijk, geautomatiseerde werken die niet formeel in beslag genomen zijn. Bij de opsporingsambtenaren blijkt geen duidelijk beeld te bestaan over de wettelijke bevoegdheden en de gevallen waarin gegevensdragers mogen worden onderzocht.

In het geval ‘illegale content’ op de gegevensdrager wordt aangetroffen, wordt de gegevensdrager als uitgangspunt niet meer teruggegeven. Het beleid hierover blijkt regionaal verschillend te zijn. De mogelijkheid dat op een beveiligingscamera beelden van de doorzoeking zijn geregistreerd, waarbij de betrokken opsporingsambtenaren herkenbaar in beeld zijn gebracht, wordt regelmatig genoemd als te wissen ‘content’. Bij de opsporingsinstanties leeft de vraag in hoeverre die beelden verwijderd mogen worden en wie daartoe bevoegd is. Het ontbreken van een concrete regeling daaromtrent wordt in de opsporing als problematisch ervaren en zou ten grondslag kunnen liggen aan het niet registreren van het, al dan niet gedeeltelijk, wissen van bestanden van een elektronische gegevensdrager of geautomatiseerd werk.

Met de beantwoording van de kwantitatieve en kwalitatieve onderzoeksvragen in het achterhoofd is de centrale vraagstelling van het onderzoek beantwoord met de volgende algemene conclusies.

Het totaalbeeld dat uit het onderzoek ontstaat, is dat op het kwantitatieve vlak weinig cijfermateriaal beschikbaar is om al te sterke conclusies te kunnen trekken, behalve dat er sprake is van aanzienlijk aantallen in beslag genomen gegevensdragers. Uit de interviews komt naar voren dat relatief weinig tot geen intern beleid is geformuleerd ten aanzien van het onderzoek aan in beslag genomen elektronische gegevensdragers en geautomatiseerde werken. Daar waar wel beleid bestaat, wordt dat niet in alle gevallen voldoende nageleefd of heeft het beleid onvoldoende draagvlak.

Een meer definitieve beantwoording van de vraag of de bepalingen inzake de inbeslagneming van voorwerpen, waaronder artikel 94 Sv mede in het licht van het bepaalde in artikel 8 EVRM, een voldoende voorzienbare grondslag vormen voor het door een opsporingsambtenaar vergaren van gegevens die zijn opgeslagen op een in beslag genomen smartphone, zal door de Hoge Raad (moeten) worden gegeven. In dat geval wordt de uitleg over de reikwijdte van een bevoegdheid, zoals die in de wet is opgenomen, die niet door de wetgever zelf nader wordt gedefinieerd, aan de rechtspraak overgelaten. Dat zou kunnen bijdragen aan een zwakkere democratische legitimering van de uitleg van de reikwijdte van een strafvorderlijke bevoegdheid, gelet op de technische voortschrijding. Waar procedurele voorzieningen nodig worden geacht, zal zulks de rechtsvormende taak van de Hoge Raad gemakkelijk te buiten gaan. Het lijkt wenselijk dat de wetgever zelfstandig een standpunt inneemt omtrent de reikwijdte van de bevoegdheid en desgewenst een nadere wettelijke regeling initieert.

Het is voor de praktijk van groot belang om op voormelde punten een (meer) eenduidige werkwijze voorgeschreven te krijgen. Op een aantal in het onderzoek gesignaleerde punten is de huidige wet- en regelgeving onvoldoende duidelijk en blijkt zij in de praktijk vragen op te roepen. Waar verheldering van regelgeving gewenst is, is van belang dat die verheldering op verschillende wijzen kan worden gerealiseerd. Wijziging van het Wetboek van Strafvordering zal niet op alle punten noodzakelijk zijn. Ook het hanteren van een meer eenduidig beleid waaraan de praktijk handvatten voor de dagelijkse uitvoering kan ontnemen, kan daar betekenisvol in zijn.

Summary

This report gives an account of research carried out in order to compile an inventory of part of current investigation practices relating to the confiscation of certain items. This mainly concerns investigations carried out by investigating officers on electronic data carriers and computerised works after such confiscation. The report focuses on possible further standardisation of such research in connection with modernising the Code of Criminal Procedure. The main question posed in this research is: “What do we know about the confiscation of electronic data carriers and computerised works and the subsequent police investigations carried out on them?”

This general question gives rise to various quantitative and qualitative research questions which have been taken as a general guideline when clarifying confiscation practices.

Section 2 outlines the legal framework for the confiscation of items and the subsequent police investigation of electronic data carriers and computerised works. This makes it clear that the Code of Criminal Procedure contains very few specific regulations relating to the investigating of confiscated electronic data carriers or computerised works, as opposed to investigations carried out on data carriers and computerised works during an on-site search carried out in order to establish data: the law does contain specific provisions in respect of the latter. From the legal precedents discussed, it emerges that the lower courts differ in their opinions on whether the provisions governing the confiscation of items, including Article 94 of the Code of Criminal Procedure, still constitute a sufficiently foreseeable basis to enable investigating officers to compile information stored on a confiscated smart phone, partly in view of the provisions in Article 8 of the European Convention on Human Rights while also taking technological developments into account. The interpretation of these provisions, insofar as they relate to the confiscation of items for the purpose of carrying out additional investigations to gain access to the data they contain in the interests of establishing the truth, is not unanimous. There is still no specific legislation relating to this particular field to date.

With respect to the quantitative research questions, it has emerged that on the basis of existing figures for the confiscation and subsequent investigation of electronic data carriers and computerised works, investigating officers do confiscate a great many data carriers. These figures do not distinguish between the grounds for confiscation and the relevant authority by which or under whose responsibility the items are confiscated. Although such situations do occur, no specific figures exist in respect of the on-site inspection of computerised works by investigating officers in order to take cognisance of the data contained therein without formally confiscating the item in question. Moreover, no figures

relating to the deleting of files on electronic data carriers or computerised works are available either because these figures are not registered.

With respect to the qualitative research questions, the report concludes that in most cases, the decision whether data carriers are to be confiscated is made during preparations and particularly while in situ. In most cases the decision to confiscate these data carriers is made by the Public Prosecutor or the examining judge in view of the fact that items are generally confiscated while the premises are being searched. The outcome of this decision strongly depends on suspicion of the offence and the scope of the inquiry, and also on the authorities involved in such confiscation. The main principle here is that an assumption is made that all data present on the relevant items may be investigated, except for any data that comes under the professional right of non-disclosure.

All or part of the data is copied for further investigation unless such data is encrypted or access to it has been blocked. The copies are recorded in business systems, and policy relating to access to such business systems varies from region to region. Apparently there is no central management in existence with respect to the way in which data must be destroyed or made inaccessible, or when this should be done. Although the Police Data Act does contain regulations on statutory retention periods for such data and on its destruction, their content is not widely known in practice. The Code of Criminal Procedure does not contain any stipulations in this respect.

In practice, certain problems occur in respect of the confiscation of electronic data carriers and computerised works insofar as the relevant data comes within the scope of the professional right of non-disclosure. The existing legislation and regulations apparently do not provide sufficient clarity on these points in practice. The filtering of data that comes under the professional right of non-disclosure has not resulted in any practicable methods for criminal investigations to date.

With respect to the compiling of data that has been stored elsewhere (in the cloud), current legislation does not provide any specific powers, and no policy regulations are in existence either. Such data is only compiled sporadically. The relevant problems relate to issues concerning violations of other nations' sovereignty and the absence of sufficiently clear legal provisions on this point. Policy is based on the main principle that no data should be recorded in the event of doubts relating to violations of national sovereignty. It is advisable to ensure clarity with respect to the limits and options of cross-border investigations.

Investigating officers occasionally carry out investigations on (mainly) computerised works that have not been formally confiscated. Apparently these investigating officers do not have a clear idea of their legal powers and the circumstances under which data carriers may be investigated.

In the event that investigating officers find ‘illegal content’ on a data carrier, the general principle is that this data carrier is not restored to its owner. Policy in this respect varies from region to region. The possibility that security cameras register images of the relevant search in which investigating officers can clearly be identified is often cited as ‘content to be deleted’. The investigation departments themselves are in some doubt regarding the extent to which such images may be deleted, and if so, who has the authority to delete them. The lack of any specific regulations in this connection is regarded as a problem by the criminal investigation departments, and this might be the reason why the deleting of all or part of files on electronic data carriers or computerised works is not registered.

While bearing the answering of the quantitative and qualitative research questions in mind, the report answers the main question relating to the research with the following general conclusions.

The overall picture that emerges from the research is that insufficient figures are available in a quantitative sense to enable any definite conclusions to be drawn, apart from the fact that large numbers of data carriers have been confiscated. The interviews show that no internal policy - or relatively little - has been formulated with respect to investigations into confiscated electronic data carriers and computerised works. In cases where such policy does exist, this is not always complied with to a sufficient extent, or it does not enjoy sufficient support.

It is up to the Dutch Supreme Court to provide a more definite answer to the question of whether the provisions relating to the confiscation of items (including Article 94 of the Code of Criminal Procedure partly in conjunction with the stipulations in Article 8 of the European Convention on Human Rights) constitute a sufficiently foreseeable basis for investigating officers to compile data stored on a confiscated smart phone. In such an event, the explanation of the scope of certain powers as stated in the law, which is not specified further in the relevant legislation, will be left to the judiciary. This might contribute to the weakening of a democratic legitimisation of the explanation of the scope of powers relating to criminal procedure in view of technological developments. In cases where procedural facilities are deemed necessary, this will easily exceed the Supreme Court’s law-formative duties. It seems desirable for the legislator to adopt an independent viewpoint on the scope of the relevant powers, and to initiate further statutory regulations if desired.

In practice, it is of great importance that a more unambiguous working method is prescribed for the points stated in the foregoing. The present legislation and regulations are insufficiently clear with respect to a number of points identified in the research, and it has emerged that they give rise to questions in practice. In cases where clarification of legislation and regulations is required, it is important that this clarification can be achieved in various ways. Amendments to the Code of Criminal Procedure will not be necessary

with respect to all the points. Moreover, maintaining a more unambiguous policy that can provide guidelines for everyday implementation in practice could be a significant factor here.

Literatuurlijst

Literatuur

G.J.M. Corstens & M.J. Borgers, *Het Nederlands strafprocesrecht*, Deventer: Wolters Kluwer 2014.

B.J. Koops, *Het decryptiebevel en het nemo tenetur beginsel. Nopen ontwikkelingen sinds 2000 tot invoering van een ontsleutelplicht voor verdachten?*, Tilburg: Universiteit van Tilburg 2012.

B.J. Koops e.a., *Misdaad en opsporing in de wolken, Knelpunten en kansen van cloud computing voor de Nederlandse opsporing*, Tilburg: TILT 2012.

B.J. Koops & A.H. Vedder, *Opsporing versus Privacy*, Den Haag: Sdu-uitgevers 2015.

J.B.J. van der Leij, 'De staat van onze informationele privacy binnen het domein van opsporing, vervolging en berechting van strafbare feiten', *Strafblad* 2014/42, afl. 4, p. 271-277.

J.B.J. van der Leij, *Privacyrecht en slachtoffers, Een studie naar de grondslagen en juridische kaders van privacy van slachtoffers*, Den Haag: Boom (WODC) 2015.

J.S. Nan, *Vormverzuimen in het voorbereidend onderzoek*, Praktijkcahiers Strafrecht deel 9, Den Haag: Sdu uitgevers 2015.

J. Smits e.a., *Glazen privacy. Knelpuntenonderzoek uitvoering Wet politiegegevens (Wpg)*, Deventer/Groningen: Arena Consulting/Pro Facto (WODC) 2013.

Regelgeving en parlementaire stukken

Aanwijzing inbeslagneming (Artikel 94 Wvsv) (2014A006), laatstelijk gewijzigd per 1 juli 2014, *Stcrt.* 2014, 18598.

Aanwijzing toepassing opsporingsbevoegdheden en dwangmiddelen tegen advocaten, (2011A003), laatstelijk gewijzigd per 1 april 2011, *Stcrt.* 2011, 4981.

Kamerstukken II 2015/16, 33 842, nr. 3 en bijlage.

Kamerstukken II 2015/16, 29 279, nr. 278.

Kamerstukken II 2005/06, 30 327, nr. 3.

Kamerstukken II 2003/04, 29 441, nr. 3.

Kamerstukken II 1998/99, 26 671, nr. 3.

Kamerstukken II 1993/94, 23 692, nr. 3.

Kamerstukken II 1989/90, 21 551, nr. 3.

Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronisch netwerken, Boedapest 23 november 2001, *Trb.* 2002, 18.

Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden, Rome 4 november 1950, *Trb.* 1951, 154.

Council of Europe/European court of Human Rights, ‘*Guide On Article 6*’ 2014 (http://www.echr.coe.int/Documents/Guide_Art_6_criminal_ENG.pdf)

Lijst met aangehaalde zaken

Nederlandse jurisprudentie

HR 26 januari 2016, ECLI:NL:HR:2016:110.

HR 26 april 2011, ECLI:NL:HR:2011:BO4015, *NJ* 2012, 63 m.nt. B.F. Keulen.

HR 7 juli 2009, ECLI:NL:HR:2009:BH8889, *NJ* 2009, 399.

HR 20 februari 2007, ECLI:NL:HR:2007:AZ3564, *NJ* 2008, 113, m.nt. T.M. Schalken onder *NJ* 2008, 115.

HR 8 mei 2001, ECLI:NL:HR:2001:AB1517, *NJ* 2001, 479.

HR 29 maart 1994, ECLI:NL:HR:1994:AD2076, *NJ* 1994, 537, m.nt. T.M. Schalken onder *NJ* 1994, 577.

HR 19 juni 1990, ECLI:NL:HR:1990:ZC8556, *NJ* 1991, 119 m.nt. Th.W. van Veen en M. Scheltema.

Hof Amsterdam, 13 november 2015, ECLI:NL:GHAMS:2015:5007.

Hof Amsterdam, 17 september 2015, ECLI:NL:GHAMS:2015:4348.

Hof Arnhem-Leeuwarden 22 april 2015, www.sr-updates.nl, SR 2015-0215, m.nt. P.C. Verloop, ECLI:NL:GHARL:2015:2954.

Hof Den Bosch, 3 april 2014, ECLI:NL:GHSHE:2014:956.

Rechtbank Limburg 28 oktober 2015, ECLI:NL:RBLIM:2015:9128.

Rechtbank Gelderland 8 oktober 2015, ECLI:NL:RBGEL:2015:6215.

Rechtbank Limburg (zittingsplaats Maastricht) 5 juni 2015, parketnr. 03/659119-14.

Rechtbank Oost-Brabant 5 juni 2015, ECLI:NL:RBOBR:2015:3228.

Rechtbank Rotterdam 4 juni 2015, ECLI:NL:RBROT:2015:4085.

Rechtbank Noord-Holland 4 juni 2015, ECLI:NL:RBNHO:2015:4660.

Europees Hof voor de Rechten van de Mens

EHRM 30 september 2014, 8429/05 (*Prezhdarovi/Bulgarije*).

EHRM 15 mei 2012, 49458/06 (*Colon/Nederland*).

EHRM 1 juni 2010, 22978/05 (*Gäffen/Duitsland*). EHRM 1 juli 2008, 58243/00 (*Liberty/bet Verenigd Koninkrijk*).

EHRM 29 juni 2006, 11901/02 (*Panteleyenko/Oekraïne*).

EHRM 29 juni 2006, 54934/00 (*Weber & Saravia/Duitsland*).

EHRM 17 juli 2003, 25337/94 (*Craxi/Italië*).

EHRM 29 april 2003, 39042/97 (*Kuznetsov/Oekraïne*).

EHRM 25 maart 1998, 13/1997/797/1000 (*Kopp/Zwitserland*).

EHRM 16 december 1992, *Publ. ECHR, Series A*, vol. 251-B (*Niemietz/Duitsland*).

EHRM 24 april 1990, 11801/85 (*Kruslin/Frankrijk*).

EHRM 2 augustus 1984, 8691/79 (*Malone/bet Verenigd Koninkrijk*).

EHRM 6 september 1978, 5029/71 (*Klass & anderen/Duitsland*).

Bijlage: de begeleidingscommissie

Voorzitter:

Prof.mr. J.H. Crijns, hoogleraar straf- en strafprocesrecht aan de Universiteit Leiden

Leden:

Drs. W.M.E.H. Beijers, universitair docent en coördinator van de opleiding Criminologie, Vrije Universiteit Amsterdam

Mw. drs. N.G. de Boer, senior project-/programmamanager Project- Programma- en AdviesCentrum, Ministerie van Veiligheid en Justitie

Mw. mr. A.M.C. Boerwinkel, raadadviseur Directie Wetgeving en Juridische Zaken, Ministerie van Veiligheid en Justitie

Mw. mr. drs. M. Hallers, medewerker afdeling Directoraat-Generaal Politie, Ministerie van Veiligheid en Justitie

Mw. mr. A.M. van Hoorn, senior onderzoeker, Wetenschappelijk Bureau van het Openbaar Ministerie

Mr. dr. J.B.J. van der Leij, Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC)

Dhr. E. Tamminga, directie adviseur en technical consultant, Nederlands Forensisch Instituut

Mr. M. Zoetekouw, Jurist Cybercrime & Digitale Technologie, Politie - Landelijke Eenheid - Dienst Landelijke Operationele Samenwerking; Ph.D. Researcher 'Jurisdiction on het Internet', UNI JURIS research group, Universiteit Utrecht