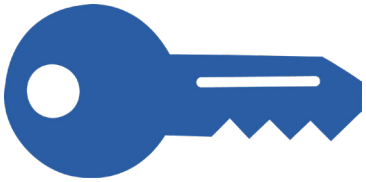

De hackbevoegdheid onder de **Wet Computercriminaliteit III**

Een advies aan Gerbrandy advocaten over het te voeren verweer bij twijfel aan de rechtmatige toepassing van de hackbevoegdheid

Naam: Riëlle Mariska Heemskerk
Studentnummer: s1089128
SVA-Code: HBR-AS17-AS

Gerbrandy Advocaten
Opdrachtgever: dhr. mr. W.A.P. Gerbrandij

Hogeschool Leiden
Afstudeerbegeleider: mevr. mr. D. Westerveld
Onderzoeksdocent: mevr. mr. M. Rietmeijer
Datum: 13-6-2018

Voorwoord

Beste lezer,

Voor u ligt het onderzoeksrapport dat mij hopelijk een grote stap dichterbij het volbrengen van mijn studie brengt. De afgelopen maanden heb ik keihard gewerkt aan dit rapport en ik ben dan ook zeer trots op het product dat u nu in uw handen heeft. Dit eindproduct was echter nooit tot stand gekomen zonder een aantal mensen, die mensen wil ik graag bedanken.

Allereerst mijn opdrachtgever, dhr. mr. W.A.P. Gerbrandij, Ger, bedankt voor de mogelijkheid om dit zeer interessante en actuele onderwerp uit te pluizen. Ik hoop dat dit onderzoeksrapport bruikbaarheid oplevert voor zijn rechtspraktijk en die van zijn kantoorgenoten. Ook ben ik mijn collega's van de Praktizijns-Sociëteit dankbaar voor de ruimte die ik kreeg om dit onderzoek af te ronden.

Daarnaast wil ik mijn onderzoeksdocent, mevr. M. Rietmeijer, en afstudeerbegeleider, mevr. D. Westerveld, bedanken voor hun feedback en hulp bij het opzetten en uitvoeren van dit onderzoek. Door hun kritische blik en oplossingsgerichtheid kon ik steeds een stap verderzetten naar het afronden van dit onderzoek.

Tenslotte wil ik Remko, mijn familie en vrienden bedanken voor hun motiverende woorden.

Ik hoop dat u met genoegen mijn onderzoeksrapport leest!

Riëlle Heemskerk
13 juni 2018

Samenvatting

In december 2015 werd het wetsvoorstel ‘Wet Computercriminaliteit III’ ingediend bij de Tweede Kamer. In dit wetsvoorstel is een nieuwe bevoegdheid opgenomen voor opsporingsambtenaren welke hen de mogelijkheid geeft om op afstand de geautomatiseerde werken, zoals computers, binnen te dringen. Deze bevoegdheid wordt ook wel de hackbevoegdheid genoemd en zal een aanvulling zijn op het juridisch instrumentarium. Deze aanvulling is nodig omdat de opsporingsambtenaren door snelle technologische ontwikkelingen zoals versleuteling van gegevens, draadloze netwerken en cloudcomputingdiensten het opsporingsonderzoek niet op een efficiënte manier uit kunnen voeren.

De hackbevoegdheid, welke zal worden opgenomen in het Wetboek van Strafvordering, is een ingrijpende bevoegdheid voor de privacy van de verdachte. Dit is dan ook de aanleiding voor het feit dat er aan vele voorwaarden moet worden voldaan alvorens de bevoegdheid rechtmatig kan worden toegepast. Er zijn allereerst voorwaarden gesteld aan de inhoud van het bevel van de Officier van Justitie. Voordat dit bevel mag worden uitgevoerd moet hiervoor toestemming zijn van de rechter-commissaris. Daarnaast zijn er eisen gesteld aan het technische hulpmiddel dat zal worden gebruikt om de onderzoekshandelingen uit te voeren, deze moet namelijk aan het Besluit technische hulpmiddelen strafvordering voldoen. Ook mogen niet alle opsporingsambtenaren de bevoegdheid uitvoeren, alleen ambtenaren met specialistische kennis van ICT die geen onderdeel zijn van het tactische team kunnen voor de uitvoering worden aangewezen.

Als aan deze voorwaarden niet wordt voldaan en er wordt wel bewijs gevonden door het toepassen van de bevoegdheid, is er sprake van onrechtmatig verkregen bewijs. Dit kan verschillende gevolgen hebben voor de strafzaak, het bewijs kan namelijk uitgesloten worden, er kan strafvermindering worden toegepast of het vormverzuim wordt alleen geconstateerd. Middels jurisprudentieonderzoek is uitgezocht wanneer de rechter zal oordelen dat sprake is van onrechtmatig verkregen bewijs en wanneer hier welk gevolg aan zal worden verbonden.

Uit het jurisprudentieonderzoek is gebleken dat het goed gemotiveerd aanvoeren van redenen waarom er geen redelijk vermoeden van schuld was ten tijde van het uitvoeren van onderzoekshandelingen en een relatief groot deel van de gevallen leidt tot toekenning van onrechtmatig verkregen bewijs. Hieruit volgt dat vanuit verdedigingsperspectief altijd moet worden gekeken naar de feiten en omstandigheden op basis waarvan de Officier van Justitie het bevel heeft uitgevaardigd.

Ook bleek uit het jurisprudentieonderzoek dat een probleem met de machtiging van de rechter-commissaris kan leiden tot het oordeel dat er sprake is van onrechtmatig verkregen bewijs. In alle gevallen waarin het vermoeden heerst dat door de opsporingsambtenaren onrechtmatig is gehandeld, is het belangrijk aan te tonen hoe ernstig dit vormverzuim was, of er een strafvorderlijk voorschrift of rechtsbeginsel is geschonden en welk nadeel de verdachte hieraan heeft ondervonden. De rechter neemt deze aspecten namelijk mee in de beslissing welk gevolg moet worden gekoppeld aan het vormverzuim.

Tenslotte is uit het onderzoek gebleken dat er nogal wat onduidelijkheid heerst rondom het internationale aspect van de hackbevoegdheid. Gezien het feit dat cyberspace geen duidelijke landsgrenzen kent, kunnen er wrijvingen ontstaan op het gebied van territorialiteit en soevereiniteit. Er wordt door de wetgever voorgesteld dat de hackbevoegdheid buiten de landsgrenzen mag worden ingezet als er sprake is van een geval waarin niet redelijkerwijs valt te zeggen op wiens territorium zich de verdachte of het bewijs bevindt. Hier worden in de literatuur nogal wat vraagtekens bij gezet, gezien de kans op diplomatieke spanningen. In de, in het onderzoek aangehaalde, Tallinn Manual wordt vanuit internationaalrechtelijk perspectief besproken hoe het zit met cyberspace. De wetgever behandelt cyberspace in het wetsvoorstel echter op een manier die vergelijkbaar is met de manier waarop het recht op ‘fysieke ruimte’ van toepassing is. Een uitgebreide analyse van de uiteenlopende denkbeelden over cyberspace valt buiten het bestek van deze scriptie. De Tallinn Manual kan in voorkomende gevallen wel ideeën aandragen die relevant zijn voor de rechtmatigheid van uitvoering van de hackbevoegdheid. Verder onderzoek en de toekomst zullen dus moeten uitwijzen op welke manier er in de
praktijk met cyberspace wordt omgegaan.

Inhoudsopgave

Hoofdstuk 1: Inleiding 8

1.1: Probleemanalyse 9

1.2: Doelstelling, centrale vraag en deelvragen 12

1.3: Onderzoeksmethode 13

1.4: Leeswijzer 15

Hoofdstuk 2: Heimelijk binnendringen in een geautomatiseerd werk 17

2.1: De huidige opsporingsmogelijkheden 19

2.2: De nieuwe bevoegdheid 21

2.2.1: Heimelijk binnendringen 24

2.2.2: Geautomatiseerd werk 26

2.2.3: Internationale toepassing en rechtsmacht 27

2.3: Deelconclusie 30

Hoofdstuk 3: Rechtmatigheid van de hackbevoegdheid 33

3.1: Voorwaarden 35

3.1.1: Het bevel van de Officier van Justitie 36

3.2: Toetsing 39

3.3: Onrechtmatig verkregen bewijs 41

3.4: Deelconclusie 43

Hoofdstuk 4: Onrechtmatig verkregen bewijs in het strafproces 45

4.1: Gronden 48

4.1.1: Verdenking o.g.v. onrechtmatig verkregen informatie 48

4.1.2: Ontbrekende of gebrekkige machtiging van de rechter-commissaris 49

4.1.3: Rechtswaarborgen niet in acht genomen door opsporingsambtenaren 50

4.1.4: Geen redelijk vermoeden van schuld 51

4.2: Straftoemeting 53

4.4: Deelconclusie 56

Hoofdstuk 5: Conclusie 59

Hoofdstuk 6: Aanbevelingen 63

Beroepsproduct 67

Literatuurlijst 71

Bijlage 1: Jurisprudentieanalyse 74

Gebruikte afkortingen:

Sv	=	Wetboek van Strafvordering
Sr	=	Wetboek van Strafrecht
Bths	=	Besluit technische hulpmiddelen strafvordering
MvT	=	Memorie van Toelichting
WODC	=	Wetenschappelijk Onderzoeks- en Documentatie Centrum

Hoofdstuk 1

Inleiding

1.1: Probleemanalyse

In 1993 trad de Wet Computercriminaliteit I in werking in Nederland, dertien jaar later, in 2006, werd deze wet opgevolgd door de Wet Computercriminaliteit II. Snelle technologische ontwikkelingen die de afgelopen decennia hebben plaatsgevonden zorgen echter voor nieuwe uitdagingen op het gebied van de opsporing van computercriminaliteit. Om een oplossing voor deze problemen te bieden werd op 21 december 2015 het wetsvoorstel 'Wet Computercriminaliteit III' (hierna: het wetsvoorstel) voorgelegd bij de Tweede Kamer.[1] Op 20 december 2016 werd het wetsvoorstel door de Tweede Kamer aangenomen waarna het tot op heden bij de Eerste Kamer ligt.[2] Al vroeg blijkt uit de Memorie van Toelichting bij het voorstel dat het beoogde doel het versterken en verbeteren van het juridisch instrumentarium voor opsporing en vervolging van computercriminaliteit is.[3] Het wetsvoorstel geeft daartoe aangewezen opsporingsambtenaren de bevoegdheid om op afstand geautomatiseerde werken van verdachten binnen te dringen. Deze bevoegdheid zal worden aangehaald als 'de hackbevoegdheid'. Deze ingrijpende bevoegdheid kan en zal veel invloed hebben op het onderzoek ter terechtzitting en de bewijsgaring door opsporingsambtenaren.

Advocatenkantoor Gerbrandy is gevestigd aan de Admiraal de Ruijterweg in Amsterdam-West en staat voornamelijk verdachten in strafzaken bij. Bij hen is dan ook de vraag gerezen welke invloed het wetsvoorstel zal hebben op de bewijsgaring in zaken tegen de cliënten die zij bijstaan. Meer specifiek zijn zij benieuwd naar de gronden waarop zij verweer kunnen voeren tegen de manier waarop door de opsporingsambtenaren het bewijs is verzameld. Bij het vormen van verweer zijn zij verder bovengemiddeld benieuwd naar de manier waarop opsporingsambtenaren informatie mogen halen uit geautomatiseerde werken waarbij de gezochte gegevens zich niet op Nederlands grondgebied bevinden.

De hackbevoegdheid onder de Wet Computercriminaliteit III houdt, zoals al kort in de eerste alinea is aangehaald, in dat opsporingsambtenaren op afstand geautomatiseerde werken van verdachten binnen mogen dringen. De bevoegdheid wordt in het voorstel geregeld onder art. 126nba van het Wetboek van Strafvordering. De bevoegdheid kan worden toegepast om

---

[1] Kamerstukken II, 2015/16, 34372, 1, p.1.

[2] Handelingen Tweede Kamer, 2016/17, 34372, nr. 37, item 14.

[3] Kamerstukken II, 2015/16, 34372, 3, p.2.

informatie te verzamelen die kan dienen als bewijs in een strafzaak. Het toepassen van de hackbevoegdheid zorgt voor ernstige privacy inmenging, daarom zijn er strikte waarborgen opgesteld die noodzakelijk zijn voor een rechtmatige toepassing van de bevoegdheid.[4] De vraag die wordt gesteld is dus of deze strikte waarborgen altijd in acht zullen worden genomen en in welke gevallen het niet opvolgen van in de wet opgenomen waarborgen ertoe leidt dat bewijs toch nog wordt meegenomen in het strafproces en in de overweging van de rechter. Een meer specifiek aspect van deze vraag is het jurisdictieprobleem dat de opsporing van computercriminaliteit met zich meebrengt. Er wordt voorgesteld dat de hackbevoegdheid buiten de landsgrenzen mag worden ingezet als er sprake is van een geval waarin niet redelijkerwijs valt te zeggen op wiens territorium zich de verdachte of het bewijs bevindt.[5] Hierbij komen, met het oog op de rechtmatigheid, nog meer toetsingsgronden kijken waar in dit onderzoek naar zal worden gekeken. Onder rechtmatigheid valt in dit onderzoek dus de vraag of aan alle, in de Wet Computercriminaliteit III en bestaande jurisprudentie betreffende onrechtmatig verkregen bewijs, genoemde waarborgen is voldaan bij de (internationale) toepassing van de bevoegdheid.

Het feit is dat het aantal delicten waarbij sprake is van computercriminaliteit of andere computer gerelateerde misdrijven, zoals het verspreiden van kinderpornografie via online forums, steeds vaker voorkomt. Een op de negen Nederlanders was in 2015 slachtoffer van cybercrime.[6] Daarom is het voor een advocatenkantoor dat zich specialiseert in strafrecht goed om zich voor te bereiden op te komen wetgeving. Zeker als die wetgeving een invloed gaat hebben op de manier waarop verdachten zullen worden opgespoord en de manier waarop bewijs wordt vergaard. Zo zullen zij, wanneer de wet eenmaal in werking treedt en de bevoegdheid kan en mag worden toegepast, helder voor ogen hebben welke punten zij aan kunnen voeren als het vermoeden bestaat dat de rechtmatigheid van het toepassen van de bevoegdheid door de opsporingsambtenaren in twijfel moet worden getrokken.

---

[4] Oerlemans, Strafblad 2017/4, p. 356.

[5] Oerlemans, Strafblad, 2017/4, p. 357.

[6] CBS 2017, p. 32.

In de praktijk komt het erop neer dat de volgende onderzoeksvraag zal moeten worden beantwoord: ‘Welk advies kan worden gegeven over het te voeren verweer wanneer sprake is van toepassing van de, in de Wet Computercriminaliteit III vastgelegde, hackbevoegdheid ter verkrijging van grensoverschrijdende gegevens door opsporingsambtenaren?’ Hiertoe zal een advies worden opgesteld in de vorm van een compact adviesrapport met voorwaarden waaraan de toepassing van de hackbevoegdheid moet voldoen alvorens het bewijs in de strafzaak mag worden gebruikt. Er zal dan worden gekeken naar de processuele toepassing van de bevoegdheid alsmede of de bevoegdheid rechtmatig is toegepast en meer specifiek of de bevoegdheid op internationaal gebied op de juiste manier is toegepast.

1.2: Doelstelling, centrale vraag en deelvragen

Het doel van dit onderzoek is het vormen van een advies over het te voeren verweer in gevallen waarin de nieuwe hackbevoegdheid voor opsporingsambtenaren is toegepast door het uitvoeren van literatuuronderzoek naar de wijze waarop bewijs dat middels deze bevoegdheid is vergaard mag worden meegenomen in het onderzoek ter terechtzitting.

De (voorlopige) centrale vraag die tijdens het uitvoeren van het onderzoek in acht zal worden genomen is:

- Welk advies kan op basis van wetsanalyse en literatuur- en jurisprudentieonderzoek aan Gerbrandy advocaten worden gegeven over het te voeren verweer wanneer sprake is van toepassing van de in de Wet Computercriminaliteit III vastgelegde hackbevoegdheid ter verkrijging van gegevens door opsporingsambtenaren?

De deelvragen waarmee naar het antwoord op de centrale vraag zal worden toegewerkt zijn:

- Wat houdt de hackbevoegdheid zoals deze onder de Wet Computercriminaliteit III in het leven geroepen is in?
- Welke eisen worden er gesteld aan de toepassing van de bevoegdheid op nationaal en internationaal gebied?
- Op welke manier wordt de toepassing van de bevoegdheid op nationaal en internationaal gebied gecontroleerd?
- Wat zijn de overwegingen van de rechter om onrechtmatig verkregen bewijs wel of niet mee te nemen in het strafproces blijkens jurisprudentie- en literatuuronderzoek?
- Welke punten van verweer zijn eraan te dragen op het gebied van het wel of niet aannemen van het bewijs verkregen middels de hackbevoegdheid in het strafproces?

1.3: Onderzoeksmethode

Deelvraag	Onderzoeksmethode
Wat houdt de hackbevoegdheid zoals deze onder de Wet Computercriminaliteit III in het leven geroepen is in?	Ter beantwoording van deze deelvraag zal met name een wetsanalyse worden toegepast, in de Memorie van Toelichting en het Voorlopig Verslag wordt uitgebreid toegelicht hoe de wetgever deze vraag beantwoordt. Daarnaast zal een link worden gelegd naar verschillende bronnen door middel van literatuuronderzoek ter verdere onderbouwing en beantwoording van deze deelvraag.
Welke eisen worden er gesteld aan de toepassing van de bevoegdheid op nationaal en internationaal gebied?	Ook deze deelvraag zal worden beantwoord door zowel een wetsanalyse als literatuuronderzoek uit te voeren. De eisen worden in de Memorie van Toelichting toegelicht en met name tijdschriftartikelen zullen waarschijnlijk verdere uitleg en toelichting bieden.
Op welke manier wordt de toepassing van de bevoegdheid op nationaal en internationaal gebied gecontroleerd?	Deze deelvraag zal, net als de voorgaande twee deelvragen, worden beantwoord middels resultaten uit het uitvoeren van wetsanalyse en literatuuronderzoek. Ook bij de beantwoording van deze deelvraag speelt de Memorie van Toelichting een rol. Er zullen een aantal interessante boeken worden geraadpleegd om uit te zoeken op welke manier de hackbevoegdheid op internationaal gebied kan en mag worden toegepast.

Wat zijn de overwegingen van de rechter om onrechtmatig verkregen bewijs wel of niet mee te nemen in het strafproces blijkens jurisprudentie- en literatuuronderzoek?	Zoals blijkt uit de vraagstelling zal ter beantwoording van deze vraag jurisprudentie- en literatuuronderzoek worden uitgevoerd. Er zullen uitspraken worden geraadpleegd waarin onrechtmatig verkregen bewijs wel of niet in de zaak is meegenomen en er wordt met name gekeken naar de motivering van de rechter om te besluiten een bewijsstuk wel of niet mee te nemen in zijn overwegingen. De uitspraken die voor het jurisprudentieonderzoek zijn gebruikt komen uit 2014 of zijn recenter gedaan. De uitspraken komen van rechtbanken uit het hele land en er wordt in alle uitspraken door de verdediging een beroep gedaan op onrechtmatig verkregen bewijs. De lijst met onderzochte uitspraken is te vinden in de literatuurlijst.
Welke punten van verweer zijn er aan te dragen op het gebied van het wel of niet aannemen van bewijs verkregen middels de hackbevoegdheid in het strafproces?	Het antwoord op deze deelvraag zal gevormd worden op basis van de resultaten uit jurisprudentieonderzoek en literatuuronderzoek. Zo worden punten gevormd waarop verweer kan worden gevoerd in een zaak waarin de hackbevoegdheid is toegepast.

1.4: Leeswijzer

In hoofdstuk 2 van dit onderzoek zal worden toegelicht welke opsporingsbevoegdheden er nu worden toegepast om gegevens te achterhalen en wat de voorgestelde opsporingsbevoegdheid inhoudt. Er zal worden ingegaan op de verschillende aspecten rondom deze nieuwe hackbevoegdheid, waaronder de internationale kant van de bevoegdheid. Dit hoofdstuk geeft eveneens antwoord op de eerste deelvraag.

Vervolgens zal in hoofdstuk 3 uiteen worden gezet welke eisen er worden gesteld aan de toepassing van de nieuwe hackbevoegdheid. Aan deze eisen moet worden voldaan alvorens er sprake kan zijn van een rechtmatige toepassing van de hackbevoegdheid. Hiermee zullen de tweede en de derde deelvraag worden beantwoord. Ook wordt in hoofdstuk 3 gekeken naar het begrip ‘onrechtmatig verkregen bewijs’ en wat dat inhoudt.

Tenslotte wordt er in hoofdstuk 4 gekeken naar rechtspraak waarin een beroep is gedaan op onrechtmatig verkregen bewijs. Er worden 20 uitspraken van rechtbanken geanalyseerd om te kijken in welke gevallen de rechter een beroep op onrechtmatig verkregen bewijs honoreert en wat de gevolgen zijn voor de straftoemeting. Middels de analyse van de uitspraken zal er een antwoord worden gevonden op de laatste twee deelvragen. Ook wordt de koppeling naar de praktijk gemaakt door te kijken naar manieren waarop verweer kan worden gevoerd in geval van twijfel aan de rechtmatigheid van de toepassing van de hackbevoegdheid.

Hoofdstuk 2

Heimelijk binnendringen in een geautomatiseerd werk

In dit hoofdstuk zal de nieuwe opsporingsbevoegdheid worden besproken die mogelijkheid biedt tot het heimelijk binnendringen in een geautomatiseerd werk. Hiertoe zal eerst worden besproken welke bevoegdheden er reeds die het verkrijgen van gegevens door opsporingsambtenaren mogelijk maken. Daarna zal worden ingegaan op de nieuwe bevoegdheid en er zal aan het einde van het hoofdstuk een korte deelconclusie worden gegeven waarin wordt samengevat wat de nieuwe bevoegdheid inhoudt.

2.1: De huidige opsporingsmogelijkheden

In deze paragraaf zal worden ingegaan op een dwangmiddel dat nu in het Wetboek van Strafvordering (hierna: Sv) is opgenomen en waarmee gegevens uit een geautomatiseerd werk kunnen worden vastgelegd door middel van plaats doorzoeking. Dit middel is opgenomen in artt. 125i Sv – 125o Sv. Dit middel biedt de politie een wettelijke basis om een huis binnen te gaan en ter plekke de aangetroffen geautomatiseerde werken, zoals laptops, te doorzoeken. Indien er gegevens op het geautomatiseerde werk worden aangetroffen die nodig zijn voor de waarheidsvinding, dan mogen deze gegevens worden vastgelegd.

De huidige bevoegdheid biedt dus de mogelijkheid om een plaats te doorzoeken ten behoeve van het vastleggen van gegevens, maar wat valt er eigenlijk onder het begrip 'gegevens'? De definitie van het begrip 'gegevens' is vastgelegd in de Memorie van Toelichting bij het artikel en luidt als volgt: 'informatie die is vastgelegd of opgeslagen op een gegevensdrager, hetzij op schrift, hetzij in elektronische vorm''. [7] De gegevens zullen zijn opgeslagen op een geautomatiseerd werk, hiervan is ook een definitie gevormd, namelijk in art. 80sexies Sr: 'een inrichting die bestemd is om langs de elektronische weg gegevens op te slaan en te verwerken'.

Inhoudelijk verleent het dwangmiddel tot vastlegging van gegevens uit een geautomatiseerd werk door middel van doorzoeking van een plaats, aan de rechter-commissaris, de Officier van Justitie, de Hulpofficier van Justitie en de opsporingsambtenaar de bevoegdheid om een plaats te doorzoeken. De doorzoeking kan, blijkens de Memorie van Toelichting, onderzoek naar gegevens, inzage in de gegevens of het maken van een kopie van de gegevens ter vastlegging als doel of gevolg hebben.[8]

Er is een aantal voorwaarden gesteld aan het uitoefenen van het besproken dwangmiddel. Allereerst mag slechts tot doorzoeking ter vastlegging van gegevens worden overgegaan als andere, minder vergaande bevoegdheden, niet effectief zijn gebleken.[9] Dit heet ook wel het subsidiariteitsbeginsel. Aan welke voorwaarden verder moet worden voldaan hangt af van de

---

[7] Kamerstukken II 2003/04, 29441, 3, p. 7

[8] Kamerstukken II 2003/04, 29441, 3, p. 11

[9] Kamerstukken II 2003/04, 29441, 3, p. 12

functionaris die van de bevoegdheid gebruik wil maken. De rechter-commissaris kan bijvoorbeeld op vordering van de officier van justitie overgaan tot doorzoeking van elke plaats. Voor de officier van justitie en de hulpofficier en opsporingsambtenaren gelden, afhankelijk van de te doorzoeken plaats, andere voorwaarden welke zijn opgenomen in artt. 96 en 97 Sv. Deze voorwaarden zijn voor dit onderzoek niet relevant.

Door de technologische ontwikkelingen die de laatste jaren hebben plaatsgevonden, ondervinden opsporingsambtenaren moeilijkheden om het opsporingsonderzoek op een efficiënte manier uit te voeren. De bestaande opsporingsbevoegdheden zijn niet afdoende om een oplossing te bieden voor de problemen en knelpunten op het gebied van de bestrijding van computercriminaliteit en andere zware misdrijven.

Daarom wordt in het wetsvoorstel 'Wet Computercriminaliteit III' de bevoegdheid tot onderzoek in een geautomatiseerd werk voorgesteld. Dit wetsvoorstel vindt zijn aanleiding in het regeerakkoord 'Bruggen Slaan' uit 2012. De toenmalige coalitie, die gevormd werd door de VVD en PvdA, nam in dit regeerakkoord op dat in verband met de toenemende bedreigingen en kwetsbaarheden op het gebied van computercriminaliteit, de wet- en regelgeving rondom dit onderwerp zou moeten worden aangepast.[10] Dit leidde tot het wetsvoorstel onder de naam 'Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit' dat op 21 december 2015 werd ingediend bij de Tweede Kamer en ook wel 'Wet Computercriminaliteit III' wordt genoemd.[11] Het wetsvoorstel omvat meerdere voorgestelde onderwerpen en wetswijzigingen maar alleen op de voorgestelde bevoegdheid tot het heimelijk binnendringen van geautomatiseerde werken zal in dit onderzoek worden ingegaan.

[10] Rutte & Samsom 2012, p. 27.

[11] Kamerstukken II 2015/16, 34372, 1, p. 1.

2.2: De nieuwe bevoegdheid

De nieuwe hackbevoegdheid is, blijkens de Memorie van Toelichting, noodzakelijk omdat de bestaande wettelijke bevoegdheden tekort schieten in de bestrijding van computercriminaliteit. Het doel van de bevoegdheid is dan ook het versterken van het juridische instrumentarium voor het effectief opsporen en vervolgen van computercriminaliteit.[12] Gesteld wordt dat de bevoegdheid zal voorzien in een leemte in de bestaande wettelijke bevoegdheden. In de Memorie van Toelichting wordt een aantal technologische ontwikkelingen opgesomd die deze leemte op dit gebied veroorzaken:

1. Versleuteling van elektronische gegevens: Leesbare data wordt omgevormd in onleesbaar materiaal door middel van wiskundige algoritmes.[13] Ook mensen die niet zozeer thuis zijn in het schrijven of gebruiken van zulke algoritmes kunnen door middel van op internet aangeboden versleutelingsprogramma's hun data 'verstoppen' achter de wiskundige algoritmes.
2. Gebruik van draadloze netwerken: De gebruiker maakt gebruik van verschillende openbare internet hotspots waardoor de communicatie niet goed af te tappen is.[14] Zo maken mensen bijvoorbeeld in restaurants, hotels of bij sportverenigingen gebruik van een router. Het is tot op heden ook nog niet mogelijk om na te gaan welke apparaten gebruik hebben gemaakt van de router. Ook is het niet mogelijk om erachter te komen welke gegevens er zijn verzonden of ontvangen via het netwerk.
3. Cloudcomputingdiensten: Een Cloud is een opslagplaats waarin gegevens worden opgeslagen en die zich niet op het geautomatiseerde werk van een persoon bevindt. Twee voorbeelden hiervan zijn Dropbox en Google Drive. Het is onduidelijk waar de gegevens precies worden opgeslagen, ook of de server zich in het buitenland of in Nederland bevindt is niet bekend. Het is in dit kader bovendien moeilijk om te onderzoeken welke gegevens waar zijn opgeslagen, omdat de gegevens ook kunnen worden verspreid over meerdere servers.[15]

---

[12] Kamerstukken II 2015/16, 34372, 3, p. 2

[13] Kamerstukken II 2015/16, 34372, 3, p. 7.

[14] Kamerstukken II 2015/16, 34372, 3, p. 10.

[15] Kamerstukken II 2015/16, 34372, 3, p. 11.

Onder de Wet Computercriminaliteit III wordt de volgende bevoegdheid voorgesteld: ‘Daartoe aangewezen opsporingsambtenaren zijn bevoegd om onder strikte voorwaarden een geautomatiseerd werk dat in gebruik is bij een verdachte, op afstand heimelijk binnen te dringen en onderzoek te doen met het oog op de vaststelling van bepaalde kenmerken van het geautomatiseerde werk of de gebruiker, zoals de identiteit en de locatie, en de vastlegging daarvan, de vastlegging van gegevens die in het geautomatiseerde werk zijn of worden opgeslagen, de ontoegankelijkmaking van gegevens, het opnemen van communicatie of van vertrouwelijke communicatie en de stelselmatige observatie.’[16] Deze bevoegdheid wordt in het kort: ‘onderzoek in een geautomatiseerd werk’ genoemd en zal in het vervolg van dit onderzoek aangehaald worden als de hackbevoegdheid.

De bevoegdheid mag, anders dan de naam van het wetsvoorstel waarin het is opgenomen doet vermoeden, worden gebruikt ten aanzien van misdrijven waarop op grond van art. 67 lid 1 Sv voorlopige hechtenis is toegestaan. Het gaat dus niet alleen om misdrijven die betrekking hebben op computercriminaliteit, zoals computervredebreuk. Wel zal voor de volledigheid worden uitgelegd hoe het begrip computercriminaliteit in de Memorie van Toelichting wordt beschreven. Daar wordt namelijk de volgende definitie gehanteerd: ‘het plegen van strafbare feiten met behulp van dan wel gericht op een geautomatiseerd werk.’[17] Wat een geautomatiseerd werk is, zal in paragraaf 2.2.2 van dit onderzoeksrapport worden uitgelegd.

Uiteindelijk zal de bevoegdheid worden opgenomen in art. 126 nba Sv, dit artikel zal vallen onder Titel IVA van het Wetboek van Strafvordering Waarom het artikel onder die titel wordt gevoegd wordt uitgelegd onder hoofdstuk 2.2.1. Het artikel zal als volgt luiden:

[16] Kamerstukken II 2015/16, 34372, 3, p. 6.

[17] Kamerstukken II 2015/16, 34372, 3, p. 7.

1.
In geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, dat gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert, kan de officier van justitie, indien het onderzoek dit dringend vordert, bevelen dat een daartoe aangewezen opsporingsambtenaar binnendringt in een geautomatiseerd werk dat bij de verdachte in gebruik is en, al dan niet met een technisch hulpmiddel, onderzoek doet met het oog op:
a.
de vaststelling van bepaalde kenmerken van het geautomatiseerde werk of de gebruiker, zoals de identiteit of locatie, en de vastlegging daarvan;
b.
de uitvoering van een bevel als bedoeld in de artikelen 126l of 126m;
c.
de uitvoering van een bevel als bedoeld in artikel 126g, waarbij de officier van justitie kan bepalen dat ter uitvoering van het bevel een technisch hulpmiddel op een persoon wordt bevestigd;
en, ingeval van een misdrijf, waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaren of meer is gesteld, dan wel een misdrijf dat bij algemene maatregel van bestuur is aangewezen;
d.
de vastlegging van gegevens die in het geautomatiseerde werk zijn verwerkt, of die eerst na het tijdstip van afgifte van het bevel worden verwerkt, voor zover redelijkerwijs nodig om de waarheid aan de dag te brengen;
e.
de ontoegankelijkmaking van gegevens, bedoeld in artikel 126cc, vijfde lid.
Artikel 11.7a van de Telecommunicatiewet is niet van toepassing op handelingen ter uitvoering van een bevel als bedoeld in de eerste volzin.

2.2.1: Heimelijk binnendringen

De bevoegdheid gaat om het 'heimelijk binnendringen' van een geautomatiseerd werk. Maar wat houdt 'heimelijk binnendringen' eigenlijk in? Heimelijk houdt in dat de bevoegdheid wordt uitgeoefend zonder dat de verdachte daar kennis van heeft. De bevoegdheid zal worden opgenomen in Titel IVA van het Wetboek van Strafvordering. In die titel zijn de 'Bijzondere bevoegdheden tot opsporing' opgenomen. Voorbeelden hiervan zijn stelselmatige observatie en infiltratie, dit zijn de bevoegdheden waarvoor strenge waarborgen gelden. Dat zal dus ook het geval zijn met de toekomstige bevoegdheid, op de voorwaarden en waarborgen die aan het toepassen van de bevoegdheid zullen worden gekoppeld zal later in dit onderzoek worden ingegaan.

Zoals genoemd wordt de bevoegdheid dus toegepast zonder dat de verdachte daar weet van heeft. De betrokkene, wie doorgaans dezelfde persoon als de verdachte is, wordt uiteindelijk wel ingelicht, dit gebeurt pas wanneer het belang van het onderzoek dit toelaat, zo blijkt uit de Memorie van Toelichting.[18] De mededeling kan worden uitgesteld vanwege de heimelijkheid van het uitvoeren van de bevoegdheid. Als het belang van het onderzoek het toelaat zal de verdachte alsnog worden geïnformeerd over de, op hem gerichte, uitoefening van de bevoegdheid. Het onderzoek is afgelopen wanneer het doel ervan is bereikt of wanneer het bevel is verlopen. Dit vloeit voort uit de notificatieplicht die is vastgelegd in art. 126bb Sv.

[18] Kamerstukken II 2015/16, 34372, 3, p. 39.

Het kan ook gebeuren dat het vastleggen van de gegevens betrekking heeft op gegevens van iemand anders, bijvoorbeeld als een werk door meerdere personen wordt gebruikt. In zo'n geval moet ook de verantwoordelijke voor die gegevens in kennis worden gesteld, dit gebeurt op hetzelfde moment als wanneer het gaat om een verdachte. Namelijk wanneer het doel van de bevoegdheid is bereikt of wanneer het bevel is verlopen. De kennisgeving geschiedt schriftelijk. Er hoeft geen uitgebreide lijst van de vastgelegde gegevens worden meegestuurd maar er moet wel worden aangeduid wat voor soort gegevens er zijn vastgelegd.[19] Het beschrijven van de aard van de gegevens heeft als doel dat de betrokkene hiermee zelf kan beoordelen of hij naar zijn mening is geschonden in zijn rechten.[20]

Nadat het geautomatiseerde werk heimelijk is binnengedrongen kunnen nog andere opsporingsbevoegdheden worden ingezet. Voorbeelden van bevoegdheden die dan kunnen worden ingezet zijn:

- het uitvoeren van (stelselmatige) observatie;
- het ontoegankelijk maken van gegevens;
- en het vastleggen van gegevens.[21]

[19] Kamerstukken II 2015/16, 34372, 3, p. 40.

[20] Kamerstukken II 2007/08, 30517, 3, p. 52.

[21] Oerlemans, Strafblad 2017/ 4, p. 355.

2.2.2: Geautomatiseerd werk

De volgende zinssnede uit de voorgestelde bevoegdheid die onder de loep zal worden genomen is de term ‘geautomatiseerd werk’. In welke soorten werken mag worden binnengedrongen en zijn er bijvoorbeeld ook specifieke uitzonderingen? Deze vraag zal in deze paragraaf worden beantwoord. De definitie van een geautomatiseerd werk is vastgelegd in art. 80sexies Sr: ‘Een inrichting die bestemd is om langs de elektronische weg gegevens op te slaan, verwerken en over te dragen.’

Als het wetsvoorstel uiteindelijk wordt aangenomen zal de inhoud van dit artikel veranderen en zal het begrip ‘geautomatiseerd werk’ een nieuwe definitie krijgen. De voorgestelde definitie luidt als volgt ‘Onder geautomatiseerd werk wordt verstaan een apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerken.’[22] In de praktijk worden hieronder onder andere apparaten gezien die onder de noemer ‘computer’ vallen zoals PC’s, mobiele telefoons en servers.[23]

Omdat de genoemde definitie verder geen grenzen stelt en een vrij brede term is, zijn er nog veel meer objecten die hieronder vallen en waar je in eerste instantie niet meteen aan denkt. Voorbeelden hiervan zijn ‘slimme’ apparaten zoals lampen, meters en auto’s, maar ook pacemakers.[24] Voormalig Staatssecretaris Dijkhoff heeft echter aangegeven dat het niet voor de hand ligt om daadwerkelijk auto’s of pacemakers te hacken voor opsporingsonderzoek. De veiligheidsrisico’s voor de betreffende personen zijn hiervoor te groot.[25] Het feit dat de risico’s te groot zijn zorgt ervoor dat de inzet van de bevoegdheid de proportionaliteitstoets niet zal doorstaan. Ook gegevensdragers die verbonden zijn met geautomatiseerde werken, zoals USB-sticks, vallen onder de reikwijdte van de bevoegdheid.[26] Er is dus meer mogelijk dan dat er volgens de verwachtingen zal gebeuren, het uitoefenen van de hackbevoegdheid zal zich op bepaalde werken meer richten dan op andere geautomatiseerde werken.

---

[22] Kamerstukken II 2015/16, 34372, 3, p. 85.

[23] Woude, van der 2018.

[24] Oerlemans, Strafblad 2017/ 4, p. 356.

[25] Kamerstukken II 2015/16, 34372, 6, p. 32.

[26] Kamerstukken II 2015/16, 34372, 6, p. 98.

2.2.3: Internationale toepassing en rechtsmacht

Het verspreiden van gegevens via het internet kent geen landsgrenzen zoals we die wel kennen zodra we een fysiek dossier met informatie daadwerkelijk van het ene naar het andere land willen verplaatsen. Dit stelt politie en justitie voor een uitdaging, het is namelijk vaak niet te achterhalen op welke fysieke locatie gegevens zijn opgeslagen. De rechtsmacht over een bepaald territoriaal gebied is de onderscheiden in twee 'onderdelen': uitvoerende rechtsmacht en wetgevende rechtsmacht. Tussen deze twee begrippen onderling is samenhang te vinden, het land met de uitvoerende rechtsmacht wordt namelijk verondersteld ook wetgevende rechtsmacht te hebben. Dat houdt in dat waar de Nederlandse wet van toepassing is, daar handhavingshandelingen worden verricht met het oog op opsporing en vervolging in Nederland.[27] De grondslagen die van toepassing zijn op deze begrippen zijn het territorialiteitsbeginsel en het nationaliteitsbeginsel. Het territorialiteitsbeginsel is opgenomen in art. 2 Sr: de Nederlandse strafwet is van toepassing op eenieder die zich in Nederland schuldig maakt aan het plegen van een strafbaar feit. Het nationaliteitsbeginsel stelt dat de Nederlandse strafwet van toepassing is op Nederlanders die zich buiten Nederland aan het plegen van strafbare feiten schuldig maken.

Naast territorialiteit en nationaliteit is het begrip soevereiniteit van toepassing, dit begrip hangt enigszins samen met territorialiteit. Het is van belang dat Nederland, zodra het opsporingsonderzoek een internationaal aspect krijgt of dreigt te krijgen, de soevereiniteit van de andere staat respecteert.[28] Een definitie voor soevereiniteit die door Schmitt en Vihul gehanteerd wordt is dat soevereiniteit staat voor onafhankelijkheid. Het gaat dan om onafhankelijkheid om binnen een bepaald gedeelte van de aarde te bepalen hoe alles gaat zonder dat een andere staat zich daarin mengt.[29] De link tussen soevereiniteit en territorialiteit ligt dus in het feit dat een staat binnen zijn territorium de soevereiniteit heeft om haar eigen regels te bepalen en te handhaven.

---

[27] Kamerstukken II 2015/16, 34372, 3, p. 43.

[28] Kamerstukken II 2015/16, 34372, 3, p. 44.

[29] Schmitt & Vihul 2017, p. 11.

Nederlandse opsporingsambtenaren mogen zonder expliciete toestemming van de betreffende staat geen opsporingshandelingen op het grondgebied van die staat verrichten. Daarom moet er bij maatregelen zoals huiszoekingen die Nederland zou willen uitvoeren in dat land een rechtshulpverzoek worden ingediend.[30] De staat op wiens grondgebied de dader zich bevindt wordt dan verzocht om ten behoeve van het opsporingsonderzoek bepaalde handelingen te verrichten. De vraag is echter hoe aan internationale vraagstukken invulling zal worden gegevens als het gaat om de hackbevoegdheid. Wat moet er gebeuren als blijkt dat de gegevens zich op ander grondgebied bevinden of als de locatie van de gebruiker of de gegevens niet bekend is? In hoeverre mag de bevoegdheid zonder overleg met het betreffende land internationaal worden uitgeoefend?

De Raad van Europa stelde in 2001 het zogenoemde Cybercrimeverdrag op, de volledige Nederlandse benaming hiervan luidt 'Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken'. In art. 22 van dit Cybercrimeverdrag is een regeling opgenomen die betrekking heeft op de grensoverschrijdende toegang tot computergegevens, namelijk dat de landen die zich aangesloten hebben bij het verdrag overleg dienen te voeren als er sprake is van overlappende rechtsmacht. Omdat de uitvoering hiervan onduidelijk bleef is er in opdracht van het WODC onderzoek gedaan naar de rechtmatigheid van grensoverschrijdende toegang tot gegevens.[31] Uit dit onderzoek blijkt dat het internationale recht toch echt verankerd ligt in de opvattingen over territorialiteit en grondgebied, cyberspace is hierin een vreemde eend in de bijt. Ook uit het boek van Schmitt en Vihul blijkt dat cyberspace in internationaalrechtelijk perspectief niet op dezelfde manier kan worden gezien als fysieke ruimte.[32] De onderzoekers van het WODC beargumenteren dat zij vinden dat er een alternatieve manier van omgang tussen staten mogelijk moet zijn als het gaat over cyberspace en de cloud. Ook uit de uitspraken die andere specialisten op het gebied van cybercrime doen blijkt dat jurisdictie een uitdaging blijft, gesteld wordt bijvoorbeeld dat het uitvoeren van de bevoegdheid op ander grondgebied kan leiden tot diplomatieke spanningen. [33]

---

[30] Dorst, van 2015

[31] Koops & Goodwin 2014

[32] Schmitt & Vihul 2017

[33] Koops & Goodwin 2014, p. 12.

Uiteindelijk wordt een conclusie getrokken in de Memorie van Toelichting. Die luidt dat het van essentieel belang is dat de onderzoeksbevoegdheden ook moeten kunnen worden gebruikt als de situatie zich voordoet dat er toegang wordt verkregen tot geautomatiseerde werken die zich in het buitenland bevinden. Zodra de Officier van Justitie een machtiging van de rechter-commissaris heeft ontvangen om de bevoegdheid uit te voeren, wordt ervan uitgegaan dat de regels betreffende internationale samenwerking worden gerespecteerd.[34] Hieruit volgt dat wordt gesteld dat, zodra de locatie van de gegevens wel bekend is, er een rechtshulpverzoek dient te worden ingesteld. Als de locatie niet bekend is wordt er gesteld dat er in het kader van het zelfstandig bestrijden van computercriminaliteit alsnog uitvoering mag worden gegeven aan de bevoegdheid, ook als de kans bestaat dat er handelingen worden verricht die betrekking hebben op gegevens die buiten ons grondgebied zijn opgeslagen.

Uit de literatuur blijkt, zoals ook op basis van het onderzoek door het WODC[35] en het boek van Schmitt en Vihul[36] is aangehaald, dat er nogal wat vraagtekens zijn bij de manier waarop in de Memorie van Toelichting het internationale aspect van de hackbevoegdheid wordt behandeld. De assumptie uit de MvT heeft namelijk geen basis in het internationale recht.[37] Gesteld wordt dat door extraterritoriale opsporingshandelingen een bewuste soevereiniteitsschending wordt gepleegd en dat Nederland zich hiermee boven alle andere staten stelt. Hiermee vormt Nederland een gevaar voor haar eigen positie in het internationale bestel. Ook kan het zo zijn dat de handeling die ter uitvoering van de hackbevoegdheid is verricht een strafbare handeling is in het betreffende land, er kan door het land uiteindelijk een strafvorderlijk onderzoek worden ingesteld naar de opsporingsambtenaar die het onderzoek in het geautomatiseerde werk uitvoerde.[38] De manier waarop in de Memorie van Toelichting met de internationale aspecten van de hackbevoegdheid wordt omgegaan zorgt nog voor een hoop vragen waarop in de toekomst een antwoord zal moeten worden gevonden.

---

[34] Kamerstukken II 2015/16, 34372, 3, p. 102.

[35] Koops & Goodwin 2014

[36] Schmitt & Vihul 2017

[37] Zoetekouw, TvI 2017/1, p. 31.

[38] Zoetekouw, TvI 2017/1, p. 33.

2.3: Deelconclusie

Middels de bevoegdheid tot het heimelijk binnendringen van een geautomatiseerd werk, mag door daartoe aangewezen opsporingsambtenaren op afstand toegang worden gezocht tot geautomatiseerde werken zoals laptops, telefoons en usb-sticks. Omdat deze bevoegdheid een flinke inbreuk maakt op de persoonlijke levenssfeer zijn er strenge voorwaarden opgesteld die in hoofdstuk drie onder de loep zullen worden genomen. Het internationale aspect van de bevoegdheid zorgt voor vraagtekens, deze worden in de Memorie van Toelichting beantwoord met de stelling dat, indien de locatie in het buitenland bekend is, er een rechtshulpverzoek wordt ingediend. Als er geen bekende locatie is zal uitvoering worden gegeven aan de bevoegdheid ter voortzetting van het opsporingsonderzoek, ondanks dat het risico bestaat dat de gegevens zich buiten ons grondgebied bevinden en dit kan leiden tot diplomatieke spanningen.

Hoofdstuk 3

Rechtmatigheid van de hackbevoegdheid

In dit hoofdstuk zal worden uitgelegd en toegelicht aan welke voorwaarden moet worden voldaan alvorens de hackbevoegdheid rechtmatig kan worden toegepast. Zoals uit hoofdstuk 2 is gebleken is de hackbevoegdheid een behoorlijk ingrijpende bevoegdheid, dit is dan ook de reden waarom er veel waarborgen in het wetsvoorstel zijn opgenomen die moeten zorgen voor rechtmatige toepassing. Daarnaast zal worden uitgelegd op welke manier men het voor zicht ziet om toetsen of de bevoegdheid rechtmatig wordt toegepast. Tenslotte wordt uitgelegd wat onrechtmatig verkregen bewijs is en welke gevolgen dit kan hebben voor het strafproces.

3.1: Voorwaarden

Allereerst mag de hackbevoegdheid alleen worden ingezet als dit gebeurt met het oog op een bepaalde, te verrichten onderzoekshandeling. Er is een lijst van handelingen opgesteld die hieronder vallen, deze zijn tevens opgenomen in lid 1 sub a van art. 126nba Sv:

1. Vaststellen van bepaalde kenmerken van het geautomatiseerde werk of de gebruiker, zoals de identiteit of locatie, en de vastlegging daarvan.
2. De vastlegging van gegevens die in het geautomatiseerd zijn of worden opgeslagen.
3. De ontoegankelijkmaking van gegevens.
4. De uitvoering van een bevel tot het aftappen en opnemen van communicatie of opnemen van vertrouwelijke communicatie.
5. De uitvoering van een bevel tot stelselmatige observatie.

Daarnaast mag de bevoegdheid slechts worden toegepast als het gaat om het opsporingsonderzoek in geval van verdenking van het plegen van strafbare feiten die een ernstige inbreuk leveren op de rechtsorde.[39] Dit zijn de strafbare feiten die vallen onder art. 67 Sv, namelijk de feiten waarbij voorlopige hechtenis is toegestaan. Voorlopige hechtenis houdt in dat de verdachte, met toestemming van de rechter-commissaris, in afwachting van het strafproces wordt vastgehouden.[40] Uit deze voorwaarde blijkt eveneens de indringendheid van de bevoegdheid, het mag niet zomaar worden ingezet, deze voorwaarde geldt ook voor andere bijzondere opsporingsbevoegdheden zoals infiltratie, het aftappen van communicatie en afluisteren.[41]

Er is echter een uitzondering op de voorwaarde betreffende de voorlopige hechtenis, deze heeft te maken met de eerdergenoemde onderzoekshandelingen. Als het gaat om het toepassen van de hackbevoegdheid met het oog op het veiligstellen of ontoegankelijk maken van gegevens (onderzoekshandelingen 2 en 3) moet er sprake zijn van verdenking van een misdrijf waarop een gevangenisstraf van meer dan acht jaar staat of een misdrijf dat bij

[39] Kamerstukken II 2015/16, 34372, 3, p. 19-25.

[40] ‘Voorlopige Hechtenis’, Openbaar Ministerie

[41] Kamerstukken II 2015/16, 34372, 3, p. 28.

algemene maatregel van bestuur is aangewezen.[42] De hoofdregel is dus dat de hackbevoegdheid mag worden toegepast als sprake is van verdenking van een misdrijf waarbij voorlopige hechtenis is toegelaten.

3.1.1: Het bevel van de Officier van Justitie

Om te voorkomen dat de overheid de grondrechten van de burger schendt door willekeurig in diens privéleven te mengen, moet een Officier van Justitie eerst schriftelijk gemachtigd worden door de rechter-commissaris. Pas na machtiging door de rechter-commissaris mag de Officier van Justitie een bevel tot onderzoek in een geautomatiseerd werk doen. Omdat het uitvoeren van de bevoegdheid ervoor kan zorgen dat er vertrouwelijke informatie van de burger wordt gevonden en dit inbreuk maakt op het recht op eerbiediging van privé familie- en gezinsleven[43] moet de rechter-commissaris bij de vordering van de Officier van Justitie controleren of het bevel voldoet aan de wettelijke eisen die hiervoor gelden.[44] De wettelijke eisen zijn terug te vinden in de volgende alinea. De rechter-commissaris toetst aan de hand van het door de Officier van Justitie opgestelde bevel de proportionaliteit en subsidiariteit, er moet worden kunnen geconcludeerd dat er geen andere, minder ingrijpende, manier was geweest om de gewenste gegevens te verkrijgen.

Een Officier van Justitie kan, met machtiging van een rechter-commissaris, een bevel tot onderzoek in een geautomatiseerd werk doen. Dit bevel stelt hij op nadat hij op basis van informatie van de politie de afweging maakt of, in zijn optiek, de bevoegdheid dient te worden toegepast.[45] Naast het voorleggen van het bevel aan de rechter-commissaris legt de Officier van Justitie het voornemen ook voor bij de Centrale Toetsingscommissie.[46] Aan het bevel kleven een aantal inhoudelijke eisen die in de MvT redelijk nauwkeurig omschreven zijn. Deze eisen dienen ertoe om de rechter-commissaris in staat te stellen om een conclusie te

[42] Kamerstukken II 2015/16, 34372, 3, p. 29.

[43] Art. 8 EVRM en art. 13 Grondwet

[44] Kamerstukken II 2015/16, 34372, 3, p. 29.

[45] Kamerstukken II 2015/16, 34372, 3, p. 33.

[46] Kamerstukken II 2015/16, 34372, 3, p. 33.

trekken betreffende de subsidiariteit en proportionaliteit van het bevel.[47] Het volgende moet door de Officier van Justitie in het bevel worden opgenomen:

- Misdrijf
    - Aard en ernst van het misdrijf
    - Feiten en omstandigheden die ten grondslag liggen aan de verdenking
- Personalia van de verdachte
- Feiten en omstandigheden waaruit blijkt dat aan de voorwaarden voor de hackbevoegdheid is voldaan
    - Gegevens kunnen niet op een andere wijze worden verkregen
    - Ernstig misdrijf met inbreuk op de rechtsorde
    - Dringendheid van de bevoegdheid
- Gegevens betreffende het geautomatiseerde werk
    - Bijvoorbeeld: IP-adres
    - Indien aan de orde: vermelden dat de gegevens zich niet in Nederland bevinden of de locatie onbekend is
    - Feiten en omstandigheden die aannemelijk maken dat het geautomatiseerde werk in gebruik is bij de verdachte
- Aangeven welk technisch hulpmiddel zal worden gebruikt ter uitvoering van de bevoegdheid
    - Aard en functionaliteit van het hulpmiddel
- Specificering van de doelen
- Tijdstip waarop de bevoegdheid wordt toegepast en voor welke duur
- Ten aanzien van welk deel van het geautomatiseerde werk uitvoering aan het bevel wordt gegevens
    - Aard van het geautomatiseerde werk
    - Aard van de gegevens
- In het geval van een bevel tot stelstelmatige observatie moet dit voornemen worden opgenomen.[48]

[47] Kamerstukken II 2015/16, 34372, 3, p. 30.

[48] Kamerstukken II 2015/16, 34372, 3, p. 101-102.

Naast inhoudelijke eisen gelden er procedurele eisen bij de uitvoering van de bevoegdheid. De opsporingsambtenaren die de bevoegdheid uitvoeren moeten deskundige ambtenaren zijn die door de korpschef zijn aangewezen en die beschikken over specialistische kennis op het gebied van informatie- en communicatietechnologie.[49] Daarnaast mogen de opsporingsambtenaren, die in dit geval deel uitmaken van het technische team, geen onderdeel zijn van het tactische team. Het technische team voert de onderzoekshandelingen uit, het tactische team voert het operationele onderzoek uit.[50] De reden hiervoor is dat deze scheiding het risico op tunnelzicht vermindert en dat het technische team niet beïnvloed wordt bij het maken van keuzes betreffende de haalbaarheid en de manier waarop de onderzoekshandelingen worden uitgevoerd.[51]

Ook worden er eisen gesteld aan de software met behulp waarvan de onderzoekshandelingen worden verricht, deze eisen zullen worden uitgewerkt in het, met technische hulpmiddelen aan te vullen, 'Besluit technische hulpmiddelen strafvordering' en vloeien voort uit art. 126ee Sv.[52] Op dit besluit zal later in dit hoofdstuk nog worden ingegaan. Het technische hulpmiddel wordt overigens na afsluiting van het onderzoek in het geautomatiseerde werk weer verwijderd. Het onderzoek is afgelopen wanneer het doel is bereikt of wanneer de tijdsduur van het bevel is verlopen. De derde en laatste procedurele eis waaraan moet worden voldaan is dat de wijze van binnentreden in het geautomatiseerde werk dient te worden 'gelogd' zodat naderhand kan worden nagegaan welke handelingen zijn verricht. De manier waarop dit dient te gebeuren zal eveneens worden opgenomen in het 'Besluit technische hulpmiddelen strafvordering'.[53]

---

[49] Kamerstukken II 2015/16, 34372, 3, p. 30.

[50] Kamerstukken II 2015/16, 34372, 3, p. 14.

[51] Kamerstukken II 2015/16, 34372, 3, p. 31.

[52] Kamerstukken II 2015/16, 34372, 3, p. 31.

[53] Kamerstukken II 2015/16, 34372, 3, p. 31.

3.2: Toetsing

Gezien de verregaande manier waarop de bevoegdheid impact heeft op de persoonlijke levenssfeer van de verdachte, is het belangrijk dat er ook kan worden getoetst of er aan de gestelde voorwaarden wordt voldaan. Indien er niet aan de voorwaarden wordt voldaan is middels de bevoegdheid verkregen bewijs onrechtmatig verkregen, wat gevolgen kan hebben voor het strafproces. Hoe ver deze gevolgen strekken zal later in dit onderzoek worden behandeld.

De eerste manier waarop kan worden gekeken naar de toepassing van de bevoegdheid is door het voornemen voor te leggen aan de Centrale Toetsingscommissie. Voordat de bevoegdheid daadwerkelijk wordt toegepast zal het voornemen om de bevoegdheid in te zetten worden voorgelegd aan de Centrale Toetsingscommissie (hierna: de Commissie). Dit is een intern adviesorgaan dat bestaat uit leden van het Openbaar Ministerie en van de Politie. De inzet van de bevoegdheid wordt door de Commissie getoetst aan de relevante wet- en regelgeving, jurisprudentie, subsidiariteit, proportionaliteit en de afbreukrisico's.[54] Op basis van deze toets wordt door de Commissie een advies gevormd, welke wordt voorgelegd aan het College van procureurs-generaal.[55] Het doel van deze adviesprocedure is dat er een landelijk beleid wordt ontwikkeld over de proportionaliteit en subsidiariteit in gevallen waarin bijzondere opsporingsbevoegdheden (gewenst te) worden toegepast.[56]

Vervolgens moet er worden gekeken of het technische hulpmiddel dat gebruikt wordt wel voldoet aan de eisen die worden gesteld in het Besluit technische hulpmiddelen strafvordering (hierna: Bths). De grondslag voor deze eisen ligt in art. 126ee Sv.[57] Er zijn drie voorwaarden waaraan technische hulpmiddelen moeten voldoen:

1. De waarneming moet betrouwbaar zijn.
2. De waarneming moet voor derden te toetsen zijn.
3. De waarneming mag niet te manipuleren zijn.[58]

---

[54] Kamerstukken II 2015/16, 34372, 3, p. 37.

[55] Kamerstukken II 2015/16, 34372, 3, p. 38.

[56] Kamerstukken II 2015/16, 34372, 3, p. 37.

[57] Kamerstukken II 2015/16, 34372, 3, p. 109.

[58] Blom 2017

Alleen hulpmiddelen die voldoen aan de beschrijving uit art. 126ee Sv kunnen worden aangemerkt als technisch hulpmiddel. Tenzij er een dringend onderzoeksbelang is dat rechtvaardigt dat een niet-goedgekeurd hulpmiddel mag worden ingezet, moet er ter uitvoering van de bijzondere opsporingsbevoegdheden altijd gebruik worden gemaakt van een goedgekeurd technisch hulpmiddel.[59]

Een andere vorm van registratie van het uitvoeren van de opsporingsbevoegdheid is het proces-verbaal dat door de opsporingsambtenaar moet worden opgesteld en het logboek van de technisch opsporingsambtenaar. De verplichting tot het opstellen van een proces-verbaal is opgenomen in art. 152 Sv. In het proces-verbaal moet worden opgenomen welke werkzaamheden de opsporingsambtenaar verricht in het opsporingsonderzoek. Deze vorm van verslaggeving zorgt ervoor dat naderhand kan worden gecontroleerd of de opsporingsbevoegdheid op de juiste manier is toegepast. Aan de hand van dit proces-verbaal kan dus getoetst worden wat de werkwijze van de opsporingsambtenaar is geweest, dit maakt deze werkwijze ook controleerbaar.

[59] Art. 18 lid 1 Bths

3.3: Onrechtmatig verkregen bewijs

‘Wettig en overtuigend bewezen’ is wat de rechter moet oordelen voor een bewezenverklaring. De rechter mag alleen oordelen dat de verdachte het ten laste gelegde feit heeft begaan als:

- het bewijs ter terechtzitting tot de rechter is gekomen;
- het bewijsmiddel ‘wettig’ is;
- het bewijsmiddel de rechter heeft overtuigd.[60]

Als bij het controleren van de toepassing bevoegdheid blijkt dat er een fout is gemaakt in het navolgen van de gestelde voorwaarden, dit wordt ook wel een vormverzuim genoemd, is er sprake van onrechtmatig verkregen bewijs. Een voorbeeld van onrechtmatig verkregen bewijs in het geval van de nieuwe hackbevoegdheid is als de Officier van Justitie geen machtiging van de rechter-commissaris heeft ontvangen en desondanks toch uitvoering aan het bevel geeft. Uit art. 359a Sv kan worden opgemaakt dat onrechtmatig verkregen bewijs verschillende consequenties kan hebben. Onrechtmatig verkregen bewijs botst daarnaast ook met het EVRM, namelijk met het recht op een eerlijk proces. Het gebruiken van onrechtmatig bewijs doet inbreuk aan het recht op een eerlijk proces. Dit is ook de reden waarom onrechtmatig bewijs tot bewijsuitsluiting en uiteindelijk vrijspraak kan leiden, omdat burgers beschermd dienen te worden tegen willekeurig en/of onrechtmatig handelen van de overheid.

De gevolgen kunnen bewijsuitsluiting, strafvermindering en constatering zijn. Als bewijsuitsluiting het gevolg is, wordt het bewijs dat op onrechtmatige wijze is verkregen niet meer meegenomen in het strafproces. Dit zal tot gevolg hebben dat de verdachte, wegens gebrek aan bewijsmiddelen, wordt vrijgesproken. Een minder ingrijpend gevolg is strafvermindering, de rechter is dan van mening van de onrechtmatigheid en het nadeel dat de verdachte hiervan heeft ondervonden kunnen worden gecompenseerd met een vermindering van de strafmaat. Het laatste gevolg wat mogelijk is, is constatering. Dit is het geval wanneer er wel sprake is van een vormverzuim maar dit verzuim niet ingrijpend was voor de verdachte of geen inbreuk maakte op diens rechten. De rechter is dan van mening dat dit niet hoeft te worden gecompenseerd in de straf.

---

[60] Verbaan 2013, p. 284.

Welke consequentie van toepassing zal zijn en hoeveel invloed dit uiteindelijk heeft op de strafmaat is afhankelijk zijn de ernst van het verzuim. Onrechtmatig verkregen bewijs kan ertoe leiden dat het bewijs volledig wordt uitgesloten, dit kan tot gevolg hebben dat de rechter niet tot het oordeel kan komen dat er ‘wettig en overtuigend’ bewijs is en de verdachte wordt vrijgesproken. Middels het jurisprudentieonderzoek dat ook onderdeel is van dit onderzoek zal worden gekeken naar de gevolgen van onrechtmatig verkregen bewijs voor de straftoemeting.

3.4: Deelconclusie

Al met al zijn er nogal wat voorwaarden waaraan voldaan moet worden voorafgaand aan en tijdens het uitvoeren van de hackbevoegdheid. Er is onder andere een voorwaarde aan het delict waarvan iemand verdacht moet worden, de hackbevoegdheid moet daarnaast met een bepaald doel worden ingezet. Met name aan het bevel van de Officier van Justitie kleeft een flinke lijst met eisen en voordat hij iets met dit bevel mag doen, kijkt er eerst nog een rechter-commissaris naar. Ook mogen slechts daartoe bevoegde opsporingsambtenaren het bevel uitvoeren en mogen zij dit alleen middels een goedgekeurd technisch hulpmiddel doen. Al deze voorwaarden dienen ertoe dat de bevoegdheid rechtmatig wordt uitgeoefend.

Voorafgaand aan het bevel stelt de Centrale Toetsingscommissie een advies op. Mocht de rechtmatige toepassing van de bevoegdheid naderhand in twijfel worden getrokken, dan kan op een aantal manieren de rechtmatigheid worden getoetst. Zo kan worden getoetst of het technische hulpmiddel voldoet aan het Bths en kan naderhand aan de hand van het proces-verbaal nog worden gekeken hoe de opsporingsambtenaar het bevel heeft uitgevoerd.

De voorwaarden kunnen aan de hand van de manieren van toetsing worden getoetst. Blijkt er na toetsing sprake is van onrechtmatige toepassing van de hackbevoegdheid? Dan is er sprake van vormverzuim en is het bewijs op onrechtmatige wijze verkregen. Onrechtmatig verkregen bewijs kan, blijkens art. 359a Sv, verschillende gevolgen hebben voor de straftoemeting. Het ene gevolg is groter dan het andere en is afhankelijk van de ernst van het verzuim wat het gevolg is dat de rechter aan het vormverzuim verbindt. Hier zal in het volgende hoofdstuk van dit rapport jurisprudentieonderzoek naar worden gedaan.

Hoofdstuk 4

Onrechtmatig verkregen bewijs in het strafproces

Vanuit verdedigingsperspectief is het belangrijk om te kijken naar de rechtspraak, wanneer oordeelt de rechter dat er sprake is van onrechtmatig verkregen bewijs? Omdat het gaat om een wetsvoorstel en een nieuw in te voeren bevoegdheid, klinkt het vreemd om jurisprudentieonderzoek uit te voeren. Het doen van jurisprudentieonderzoek dient er in dit geval echter toe om te kijken in welke gevallen de rechter een verdedigingsverzoek tot beoordeling van onrechtmatig verkregen bewijs toekent. Daarnaast wordt er gekeken wat het gevolg is wanneer de rechter iets beoordeelt als onrechtmatig verkregen bewijs, wordt dit bewijs dan per definitie uitgesloten of zijn er ook andere gevolgen mogelijk?

Voor de jurisprudentieanalyse zijn 20 uitspraken geselecteerd die redelijk recent zijn gedaan, niet ouder dan vier jaar (begin 2014), en die gedaan zijn door rechtbanken. In deze uitspraken is sprake van een verdedigingsargument waarin wordt gesteld dat het bewijs ter ondersteuning van de verdenking op onrechtmatige wijze is verkregen. Er is geen selectie gemaakt op het gebied van door welke rechter de uitspraak is gedaan.

In Tabel 1 is te zien wat de kwantitatieve resultaten van het onderzoek zijn, ook is in de tabel te zien hoe vaak er sprake was van onrechtmatig verkregen bewijs, welke gronden er werden aangevoerd en hoe vaak het bewijs volledig werd uitgesloten. Voor het uitgebreide overzicht van de onderzoeksresultaten verwijs ik u door naar Bijlage 1.

Topic	**Aantal keer voorgekomen**
Onrechtmatig verkregen bewijs	
- **Verweer verworpen (geen onrechtmatig verkregen bewijs)**	7
- **Verweer gehonoreerd**	13
Grond	
- **Verdenking o.g.v. onrechtmatig verkregen informatie**	2
- **Ontbrekende of gebrekkige machtiging van de rechter-commissaris**	4
- **Rechtswaarborgen niet in acht genomen door opsporingsambtenaren/verbalisanten**	5
- **Geen redelijk vermoeden van schuld**	9
Gevolg voor de straftoemeting in geval van onrechtmatig verkregen bewijs	
- **Alleen constatering, geen gevolg voor de straftoemeting**	3
- **Strafvermindering**	1
- **Bewijsuitsluiting**	9

Tabel 1: Jurisprudentieanalyse Onrechtmatig verkregen bewijs

4.1: Gronden

Uit de twintig onderzochte uitspraken komt naar voren dat er vier verschillende gronden zijn die door de verdediging worden aangevoerd en op grond waarvan zij van mening zijn dat het bewijs ter ondersteuning van de verdenking onrechtmatig verkregen is. De gronden die werden aangevoerd zijn op te maken uit tabel 1 en zullen één voor één worden uitgewerkt. Zo wordt duidelijk of en op welke manier verweer kan worden gevoerd als sprake is van het aanvoeren van een van de genoemde gronden.

4.1.1: Verdenking o.g.v. onrechtmatig verkregen informatie

In beide gevallen waarin deze grond werd aangedragen is de rechter niet meegegaan in het verweer. In de eerste uitspraak waarin n.a.v. een kinderporno-onderzoek informatie verkregen uit Zwitserland, stelde de verdediging dat de verkrijging van dit materiaal werd niet nader onderzocht was door de Nederlandse autoriteiten.[61] De rechter oordeelde dat er sprake was van een interstatelijk vertrouwensbeginsel. Daarmee mag er vanuit worden gegaan dat het bewijsmateriaal in overeenstemming met de geldende regelgeving werd verkregen, tenzij er aanknopingspunten bestaan om aan dit vertrouwen te twijfelen. Ook in de zaak Spookburgeractie begreep de rechter het besluit dat door de opsporingsambtenaren werd genomen. Zij gaven aan dat in ‘de combinatie van (betrouwbare en rechtmatig bijeen verzamelde) indicatoren’ voldoende aanleiding bestond om aan de slag te gaan en een zich voortzettend onderzoek te doen. In beide gevallen ging de rechter dus mee in het oordeel van de Nederlandse autoriteiten/opsporingsambtenaren. Omdat er slechts twee zaken onderzocht zijn waarin deze grond door de verdediging werd aangedragen kan er geen goed gefundeerd advies voor worden gegeven betreffende het te voeren verweer. Slechts als er een sterk te onderbouwen vermoeden is dat de verdenking gebaseerd is op onrechtmatig verkregen informatie is het een mogelijkheid om op basis hiervan verweer te construeren. In beide uitspraken was de rechter begripvol voor de denkwijze van de Nederlandse autoriteiten.

[61] Rb. Noord-Nederland, 27-07-2017, ECLI:NL:RBNNE:2017:2882

4.1.2: Ontbrekende of gebrekkige machtiging van de rechter-commissaris

Vier keer werd er een beroep gedaan op een gebrekkige of ontbrekende machtiging van de rechter-commissaris. Driemaal ging de rechter mee in dit beroep, van die driemaal werd het bewijs twee keer volledig uitgesloten en een keer constateerde de rechtbank het verzuim en verbond hier verder geen gevolgen aan.

De enige zaak waarin de rechter niet meeging met het verweer was er toestemming voor doorzoeking van een loods en niet voor de doorzoeking een woning.[62] De verdediging stelde dat hier ook toestemming voor had moeten zijn, echter is de woning niet doorzocht en concludeerde de rechter dat er dus ook geen probleem was met de machtiging.

In de gevallen waarin het bewijs werd uitgesloten had de rechter-commissaris überhaupt geen toestemming gegeven voor de uitvoering van de opsporingsbevoegdheid, dit bracht in beide gevallen ook een schending van art. 8 EVRM met zich mee.[63] [64] Deze schending weegt de rechter zeer zwaar mee in de straftoemeting en dit zorgde er dan ook voor dat de rechter geen ander gevolg passend vond dan bewijsuitsluiting.

In het geval waarin het vormverzuim alleen werd geconstateerd maar er geen gevolgen aan werden verbonden hadden de opsporingsambtenaren wel toestemming voor doorzoeking van een telefoon maar niet voor de doorzoeking van een computer.[65] Desondanks is de computer onderzocht, echter werd hierbij nauwelijks nieuwe informatie gevonden ten opzichte van de doorzoeking in de telefoon. Er was dus wel sprake van schending van het privéleven van de verdachte maar dit werd gerechtvaardigd door de machtiging voor het doorzoeken van de telefoon.

---

[62] Rb. Oost-Brabant 12-04-2016, ECLI:NL:RBOBR:2016:1720

[63] Rb. Zeeland-West-Brabant 17-10-2017, ECLI:NL:RBZWB:2017:6692

[64] Rb. Den Haag 12-102-17, ECLI:NL:RBDHA:2017:11688

[65] Rb. Amsterdam 16-05-2018, ECLI:NL:RBAMS:2018:3297

Een beroep op een probleem met de machtiging van de rechter-commissaris kan dus zeker relevant zijn en gehonoreerd worden door de rechter. Hierbij is het ook belangrijk om te kijken naar waar de rechter-commissaris een machtiging voor heeft gegeven en wat er uiteindelijk daadwerkelijk is gebeurd. Ook moet duidelijk worden aangetoond op welke manier de belangen van de verdachte zijn geschonden.

4.1.3: Rechtswaarborgen niet in acht genomen door opsporingsambtenaren

Er zijn vijf uitspraken onderzocht waarin sprake was van een verweer dat gefundeerd was op de grond dat de opsporingsambtenaren de rechtswaarborgen niet in acht hadden genomen. In drie van deze uitspraken ging de rechter niet mee in dit verweer, tweemaal was hij het eens met de verdediging. Van die twee zaken werd het bewijs één keer uitgesloten en volstond de rechter één keer met een zuivere constatering. Hierbij werden er uiteindelijk geen gevolgen aan het vormverzuim verbonden. In de gevallen waarin er geen sprake was van onrechtmatig verkregen bewijs lag dit deels in het handelen van de verdachte zelf. De verdachte gaf zelf toestemming of heeft nagelaten te reageren op een cautie die door de verbalisanten werd gegeven. Dit deed de rechtbank in deze gevallen besluiten dat de verbalisanten binnen hun bevoegdheden hebben gehandeld en het bewijs dus op een rechtmatige wijze werd verkregen.

De gevallen waarin wel werd geconstateerd dat er sprake was van onrechtmatig verkregen bewijs hebben de opsporingsambtenaren daadwerkelijk op een verkeerde manier gehandeld door de verdachte niet te wijzen op zijn rechten of door zonder wettelijke basis onderzoekshandelingen te verrichten. In deze gevallen oordeelde de rechter dat er inderdaad sprake was van onrechtmatig verkregen bewijs, echter nam hij hierin in één geval ook de ernst van het delict mee.[66] Het gevaarzettende karakter van het delict zorgde ervoor dat het vormverzuim niet als disproportioneel werd gezien en de rechtbank het verzuim daarom alleen constateerde. Bewijsuitsluiting was alleen het gevolg in een zaak waarin de minderjarige verdachte niet op zijn rechten werd gewezen, dit werd door de rechtbank zeer ernstig gevonden.[67]

[66] Rb. Oost-Brabant 25-04-2017, ECLI:NL:RBOBR:2017:2288

[67] Rb. Rotterdam 13-01-2017, ECLI:NL:RBROT:2017:1010

Een beroep op het niet (op de juiste wijze) in acht nemen van de rechtswaarborgen door de opsporingsambtenaren is dus twee keer toegewezen en heeft slechts in een van de vijf gevallen daadwerkelijk bewijsuitsluiting tot gevolg gehad. Het is dus in eerste instantie niet aan te raden om vanuit verdedigingsperspectief op deze grond een verweer te construeren. Dit omdat ook in dit geval, net zoals beschreven onder 4.1.1, de rechter in veel gevallen de opsporingsambtenaren volgt in hun manier van denken en in de manier waarop zij invulling aan hun bevoegdheden hebben gegeven.

4.1.4: Geen redelijk vermoeden van schuld

De laatste grond waarop zal worden ingegaan, en eveneens de meest aangevoerde grond, is het ontbreken van een redelijk vermoeden van schuld. Van de twintig geanalyseerde uitspraken werd in negen gevallen door de verdediging een verweer gevoerd dat gebaseerd werd op deze grond. Opmerkelijk is dat in acht van deze negen geanalyseerde uitspraken de rechter het honoreerde verweer en er inderdaad werd geoordeeld dat er sprake was van onrechtmatig verkregen bewijs. Veelal, namelijk in zes van de negen gevallen, ontbrak het aan de feiten en omstandigheden die ten grondslag lagen aan de verdenking. Zo kan louter ambtshalve kennis niet zorgen voor een redelijk vermoeden van schuld, ook moet worden gekeken naar het moment waarop de verdenking aanwezig moet zijn. Oude antecedenten zijn namelijk niet voldoende voor een redelijk vermoeden.

Verder leidde het oordeel dat er sprake was van onrechtmatig verkregen bewijs in zes van de negen gevallen tot bewijsuitsluiting, een maal tot strafvermindering en een maal tot constatering. In de gevallen waarin het vormverzuim geen bewijsuitsluiting tot gevolg had was de schending niet ernstig genoeg en ontbrak er daarmee ook een aanzienlijk nadeel voor de verdachte. Het is dus belangrijk om aan te tonen dat de verdachte nadeel heeft ondervonden aan het vormverzuim, als dit bewezen wordt geacht is de kans groter dat de rechter bewijsuitsluiting zal toepassen en de verdachte wordt vrijgesproken van hetgeen hem ten laste is gelegd.

Al met al is het dus zeer belangrijk om te kijken naar de feiten en omstandigheden die ten grondslag hebben gelegen aan de verdenking en hierbij de vraag te stellen: ‘Waren deze feiten en omstandigheden voldoende voor een redelijk vermoeden van schuld?’ Als deze vraag met ‘Nee’ wordt beantwoord dan is het zeer raadzaam om hierop een verweer te baseren, zoals uit de jurisprudentieanalyse blijkt gaat de rechter hier relatief vaak in mee en zal het bewijs als onrechtmatig verkregen worden beschouwd. Ook hier is, met het oog op de straftoemeting, het belangrijk om in het verweer mee te nemen wat de impact voor de verdachte is geweest, hoe ernstig was het verzuim en welk nadeel heeft hij hiervan ondervonden. Deze aspecten neemt de rechter zwaar mee in de straftoemeting, hoe de rechter hierin te werk gaat zal in de volgende paragraaf aan de orde komen.

4.2: Straftoemeting

Zoals uit het voorgaande is gebleken en ook eerder is toegelicht kan onrechtmatig bewijs verschillende gevolgen hebben voor de straftoemeting. Zodra is geconstateerd dat sprake is van onrechtmatig verkregen bewijs moet op grond van art. 359a Sv besloten worden welke consequenties dit heeft. Alleen als er een dusdanig grote inbreuk is gemaakt op de belangen van de verdachte door het schenden van een rechtsbeginsel mag bewijsuitsluiting het gevolg zijn, anders kan er worden gekozen voort strafvermindering of constatering. Het hangt er dus vanaf in welke mate welke beginselen of voorschriften ten aanzien van de verdachte zijn geschonden en welk nadeel hij hiervan heeft ondervonden.

Zoals uit Tabel 1 op te maken valt werd er in negen van de dertien gevallen besloten om het bewijs volledig uit te sluiten. In drie van de dertien gevallen werd slechts geconstateerd dat er sprake was van onrechtmatig verkregen bewijs, maar werden hier geen gevolgen aan verbonden. In één van de dertien gevallen leidde het feit dat het bewijs onrechtmatig was verkregen tot strafvermindering. Het kan dus zo zijn dat er inderdaad sprake is van onrechtmatig verkregen bewijs maar dat de rechtbank van mening is dat dit geen reden mag zijn om de straftoemeting hierop aan te passen. De gevolgen voor de straftoemeting worden gebaseerd op een aantal vragen die door de rechtbank worden beantwoord. Deze vragen komen in meerdere uitspraken die in het jurisprudentieonderzoek werden meegenomen aan bod maar in uitspraak no. 15 is uit de motivering van de rechter duidelijk op te maken hoe het beantwoorden van deze vragen leidt tot een bepaald gevolg voor de straftoemeting.[68] De vragen zullen worden benoemd en aan de hand van de argumentatie die in de genoemde zaak is gebruikt zal worden uitgelegd op welke manier de vraag beantwoord kan worden en uiteindelijk waarom bepaalde antwoorden tot een conclusie leiden.

[68] Rb. Amsterdam 03-09-2015, ECLI:NL:RBAMS:2015:5746

De essentie van de zaak die besproken zal worden zal kort worden geschetst: verdachte is gefouilleerd zonder dat er een redelijk vermoeden van schuld was. Op grond van de Politiewet mag er alleen gefouilleerd worden als er onmiddellijk gevaar dreigt en het fouilleren noodzakelijk is om dit gevaar af te weten. Dit was niet het geval, er bestond redelijkerwijs geen aanleiding om te fouilleren, ook niet op basis van Sv omdat er geen verdenking was. Het besluit om alsnog te fouilleren is onrechtmatig genomen en zorgt voor een onherstelbaar vormverzuim. Wat is hiervan het gevolg?

Vraag	Mogelijke beantwoording
Welk belang dient het geschonden voorschrift?	Er is inbreuk gemaakt op de persoonlijke levenssfeer van de verdachte: art. 8 EVRM. Het belang van een juist toepassing van dit voorschrift is zeer groot gezien de strikte waarborgen die de wetgever in het leven heeft geroepen om een dergelijke inbreuk op de privacy te voorkomen.
Wat is de ernst van het verzuim?	De wettelijke waarborgen zijn omzeild/niet in acht genomen, er is daarom sprake van een bijzonder ernstig verzuim.
Welk nadeel wordt veroorzaakt door het verzuim?	De verdachte heeft nadeel ondervonden in de zin van publieke vernedering die de stigmatisering van fouilleren in het openbaar vormt. Daarnaast is er, zoals genoemd, inbreuk gemaakt op zijn privacy/persoonlijke levenssfeer.

Als het zo is dat de vragen beantwoorden op bovenstaande manier worden beantwoord, is er geen ander gevolg voor de straftoemeting passelijk dan bewijsuitsluiting. Uit de leidende uitspraak ‘De onbevoegde hulpofficier’ blijkt dat bewijsuitsluiting alleen passend is als een belangrijk (strafvorderlijk) voorschrift of rechtsbeginsel in aanzienlijke mate is geschonden.[69]

[69] HR 19-02-2013, ECLI:NL:HR:2013:BY5321

Om de vraag te beantwoorden wanneer welke consequentie van toepassing zal zijn zullen dus de drie vragen leidend zijn en zal sprake moeten zijn van schending van een belangrijk strafvorderlijk voorschrift of beginsel. Als er sprake is van een schending van de privacy van de verdachte en de verdachte hierbij nadeel heeft ondervonden lijkt de trend dat bewijsuitsluiting het gevolg zal zijn. Is het zo dat er sprake is van een vormverzuim waarbij op een geringe manier inbreuk is gemaakt op de rechten van de verdachte en de verdachte hier dan ook beperkt nadeel van heeft ondervonden? Dan zal de rechter voor strafvermindering kiezen. Zodra er sprake is van een vormverzuim dat, bijvoorbeeld door de aard van het delict, te rechtvaardigen is of waarbij geen inbreuk is gemaakt op de rechten van de verdachte en hij hiervan geen nadeel heeft ondervonden zal de rechtbank het vormverzuim slechts constateren. Een constatering van het vormverzuim heeft het geen gevolgen voor de straftoemeting.

4.4: Deelconclusie

Het jurisprudentieonderzoek heeft aangetoond dat de verdediging haar verweer in zaken waarin een beroep wordt gedaan op onrechtmatig verkregen bewijs vaak baseert op de gronden ‘geen redelijk vermoeden van schuld’ of ‘gebrekkige of ontbrekende machtiging van de rechter-commissaris’. Naast dat deze standpunten het vaakst terug te zien zijn Ook is te zien dat de artt. 6 en 8 EVRM vaak terugkomen en dat, indien de belangen van de verdachte op deze gronden zijn geschaad, de trend lijkt dat bewijsuitsluiting de enige passende consequentie voor de straftoemeting is. Het is dan ook belangrijk om een schending van deze rechten duidelijk toe te lichten in het verweer.

De rechter baseert het besluit om onrechtmatig verkregen bewijs wel of niet mee te nemen in het strafproces dus voornamelijk op de vraag in welke mate de verdachte in zijn belangen is geschonden door de onrechtmatigheid. De meest belangrijke pijlers die worden gehanteerd om te bepalen wat de gevolgen zijn van het onrechtmatig verkregen bewijs zijn de drie vragen die de rechtbank zichzelf stelt. Om uiteindelijk de knoop door te hakken of bewijsuitsluiting passend is wordt vraag die voortvloeit uit het ‘Onbevoegde hulpofficier’-arrest beantwoord: Is er een belangrijk (strafvorderlijk) voorschrift of rechtsbeginsel in aanzienlijke mate geschonden?

Hoofdstuk 5

Conclusie

In de loop van dit rapport is toegewerkt naar een antwoord op de centrale vraag die aan het begin van het onderzoek werd gesteld. Er is gezocht naar een advies dat aan Gerbrandy advocaten kan worden gegeven indien er twijfel is aan de rechtmatigheid van de toepassing van de hackbevoegdheid. Het advies dat is gevormd uit zicht vooral in het nalopen van alle voorwaarden die gelden voor de toepassing van de hackbevoegdheid.

Zodra er aan de hand van de voorwaarden blijkt dat de opsporingsambtenaren de regels niet hebben nageleefd dient dit in het verweer te worden opgenomen. De twee gronden, waarover uit het jurisprudentieonderzoek is gebleken dat deze door de rechter het meest worden gehonoreerd, zijn ‘Geen redelijk vermoeden van schuld’ en ‘Ontbrekende of gebrekkige machtiging van de rechter-commissaris’. Dit zijn gronden die ook in het kader van de hackbevoegdheid zeer relevant zijn. Er dient dus altijd te worden gekeken naar de feiten en omstandigheden die ten grondslag liggen aan de verdenking en naar de machtiging van de rechter-commissaris. Is in het bevel van de Officier van Justitie meegenomen hoe het geautomatiseerde werk wordt benoemd, met welk hulmiddel wordt gewerkt? Hebben de opsporingsambtenaren het onderzoek wel gedaan binnen de marges en tijdsduur waar ze toestemming voor hadden en hadden ze wel toestemming voor alle feitelijke handelingen die zij hebben verricht? Dit zijn de belangrijkste punten waar door de verdediging naar moeten worden gekeken voordat het verweer wordt opgesteld.

Met het oog op de gevolgen van onrechtmatig verkregen bewijs voor de straftoemeting, die voortvloeien uit art. 359a Sv, moeten nog een aantal dingen duidelijk worden uitgewerkt in het verweer. Hierbij is het zeer belangrijk om aan te tonen dat de belangen van de verdachte middels het vormverzuim zijn geschaad, hoe ernstig dit is geweest en welk nadeel de verdachte hiervan heeft ondervonden. Duidelijk gemaakt moet worden dat er een belangrijk strafvorderlijk voorschrift of beginsel is geschonden, goede voorbeelden hiervan zijn artt. 6 en 8 EVRM. Het gevolg van onrechtmatig verkregen bewijs zal dan zijn: bewijsuitsluiting, strafvermindering of constatering. Het hangt van de ernst van de inbreuk op de rechten van de verdachte af welk gevolg de rechter zal verbinden aan het onrechtmatig verkregen bewijs. Mogelijk is het arrest ‘Onbevoegde hulpofficier’ op een gewijzigde manier toe te passen naar de kennisvereisten die aan de politiehacker worden gesteld.

In het onderzoek is eveneens gekeken naar het internationale aspect en het vertrouwensbeginsel in het kader van de hackbevoegdheid. De wetgever stelt in de Memorie van Toelichting dat internationale toepassing van de hackbevoegdheid zonder voorafgaand rechtshulpverzoek is toegestaan in gevallen waarin niet duidelijk is waar/op welk grondgebied de gegevens zich bevinden. Is wel duidelijk op welk grondgebied de gegevens zich bevinden? Dan zal er een rechtshulpverzoek moeten worden ingediend bij het betreffende land. De conclusie die hieromtrent in de MvT wordt getrokken, wordt in de literatuur echter in twijfel getrokken. Zo wordt gesteld dat deze denkwijze geen basis heeft in het internationale recht en benaderen het onderzoek van het WODC en de Tallinn manual cyberspace op een andere manier. Het analyseren van deze uiteenlopende benaderingen vallen buiten deze scriptie. De toekomst zal moeten uitwijzen hoe deze problemen op internationaalrechtelijk gebied zich in de praktijk zullen manifesteren.

Hoofdstuk 6

Aanbevelingen

In de loop van het onderzoek is gebleken dat er aan nogal wat voorwaarden voldaan moet worden alvorens er sprake is van een rechtmatige toepassing van de nieuwe hackbevoegdheid. Aan de hand van de resultaten die uit dit onderzoek zijn voortgekomen kan een tweetal aanbevelingen worden gevormd.

Allereerst de aanbeveling die ziet op het verweer in zaken waarin door opsporingsambtenaren de hackbevoegdheid is toegepast. Gezien het ingrijpende karakter van de hackbevoegdheid zijn er veel voorwaarden gesteld aan de toepassing van de hackbevoegdheid. Voor de verdediging is het raadzaam om alle genoemde voorwaarden langs te lopen en te controleren of er conform deze voorwaarden is gehandeld. Met name is het belangrijk om twee vragen te stellen:

1. Was er op het moment dat het bevel van de Officier van Justitie werd uitgevaardigd sprake van een redelijk vermoeden van schuld betreffende de cliënt?
2. Was er een machtiging van de rechter-commissaris of was er sprake van noodzakelijkheid waardoor het gerechtvaardigd was om zonder machtiging de bevoegdheid uit te voeren?
    i. In het geval er een machtiging was: Is er gehandeld binnen de grenzen van de hetgeen waar de rechter-commissaris toestemming voor heeft gegeven?

Als een van de bovenstaande vragen met ‘Nee’ wordt beantwoord of er aan een andere voorwaarde niet is voldaan dient dit te worden opgenomen in het verweer. Er moet worden onderbouwd dat er sprake is van een vormverzuim en aan de hand daarvan moet worden aangetoond in hoeverre er inbreuk is gemaakt op de rechten van de cliënt en welk nadeel de cliënt hiervan heeft ondervonden. Is er inbreuk gemaakt op de persoonlijke levenssfeer? Dan zal de rechter het bewijs vermoedelijk uitsluiten, als het gaat om een minder ingrijpend vormverzuim zal de rechter tot andere gevolgen komen.

De tweede aanbeveling heeft betrekking op het internationale aspect van de hackbevoegdheid. Door de wetgever wordt dit afgedaan door te stellen dat, wanneer de locatie van de gegevens(drager) bekend is en in het buitenland is, er een rechtshulpverzoek zal worden gedaan. Als de locatie niet bekend is wordt de hackbevoegdheid uitgevoerd, ondanks dat het risico bestaat dat de gegevens(drager) zich op ander grondgebied begint en dit door territorialiteit en soevereiniteit tot diplomatieke spanningen kan leiden. In het boek 'Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations' wordt vanuit internationaalrechtelijk perspectief beschreven hoe met cyberspace moet worden omgegaan. De wetgever bekijkt dit aspect echter vanuit een heel ander perspectief. Het valt buiten het bestek van deze scriptie om deze denkbeelden te analyseren. Het is daarom aanbevolen dat hier nader onderzoek naar wordt gedaan en dat er wordt gekeken naar de wijze waarop de opvattingen van de wetgever uitwerking zullen hebben in de praktijk.

Beroepsproduct

Advies ‘Rechtmatigheid van de Hackbevoegdheid’ – Gerbrandy Advocaten

Zodra de Wet Computercriminaliteit III in werking treedt mogen opsporingsambtenaren op afstand de geautomatiseerde werken binnentreden. Deze nieuwe bevoegdheid wordt heimelijk uitgevoerd, dat betekent dat de gebruiker van het geautomatiseerde werk geen weet heeft van wat er op afstand met zijn apparaat gebeurt. In deze adviesnotitie zal kort worden toegelicht wat de bevoegdheid inhoudt, welke voorwaarden er van toepassing zijn en op welke manier verweer kan worden gevoerd bij twijfel aan de rechtmatige toepassing van de bevoegdheid.

1. De hackbevoegdheid

De nieuwe bevoegdheid, die zal worden opgenomen onder art. 126nba Sv, biedt daartoe aangewezen opsporingsambtenaren de mogelijkheid om op afstand geautomatiseerde werken binnen te dringen. De definitie van een geautomatiseerd werk is vastgelegd in art. 80sexies Sr en luidt: ‘Een inrichting die bestemd is om langs de elektronische weg gegevens op te slaan, verwerken en over te dragen.’ Het toepassen van de hackbevoegdheid zal een van de volgende onderzoekshandelingen als doel hebben:

- ☐ Vaststellen van kenmerken van het geautomatiseerde werk,
- ☐ Vastleggen van gegevens die in het geautomatiseerde werk zijn opgeslagen,
- ☐ Ontoegankelijk maken van gegevens,
- ☐ Uitvoeren van een bevel tot aftappen en opnemen van (vertrouwelijke) communicatie, of
- ☐ Uitvoering van een bevel tot stelselmatige observatie.

2. De voorwaarden

Omdat de hackbevoegdheid nogal ingrijpend kan zijn voor de gebruiker, moet er aan vele voorwaarden worden voldaan alvorens sprake kan zijn van rechtmatige toepassing van de hackbevoegdheid. Deze voorwaarden zijn opgenomen in de Memorie van Toelichting en zullen hieronder worden opgesomd:

- ☐ Onderzoekshandeling als doel,
- ☐ Strafbaar feit waarbij voorlopige hechtenis is toegestaan,
- ☐ Officier van Justitie moet gemachtigd zijn door de rechter-commissaris,

- ☐ Het bevel van de Officier van Justitie moet informatie bevatten omtrent:
    - ☐ Het misdrijf,
    - ☐ De personalia van de verdachte
    - ☐ Feiten en omstandigheden waaruit blijkt dat aan de voorwaarden voor de hackbevoegdheid is voldaan,
    - ☐ Gegevens betreffende het geautomatiseerde werk,
    - ☐ Indien bekend: locatie van de gegevens,
    - ☐ Feiten en omstandigheden waaruit blijkt dat het werk in gebruik is bij de verdachte,
    - ☐ Het technische hulpmiddel dat zal worden gebruikt,
    - ☐ Tijdstip en duur van de toepassing,
    - ☐ Indien van toepassing: voornemen tot stelselmatige observatie.
- ☐ Uitgevoerd door opsporingsambtenaren met specialistische kennis op het gebied van ICT en die geen onderdeel zijn van het tactische team,
- ☐ Het technische hulpmiddel moet aan de eisen uit het 'Besluit technische hulpmiddelen strafvordering' voldoen (betrouwbaar, door derden te toetsen, niet te manipuleren).

3. Het verweer

Zodra er sprake is van twijfel aan de rechtmatigheid van de toepassing van de hackbevoegdheid, dient dit te worden opgenomen in het verweer. Hierbij is het belangrijk om de hele lijst met voorwaarden langs te lopen en te checken bij welke voorwaarde(n) het probleem ligt. Met het oog op het aanvoeren van het argument dat er sprake is van onrechtmatig verkregen bewijs moeten er een aantal dingen in het verweer worden opgenomen.

- ☐ Op welke manier is het vormverzuim begaan?
- ☐ Is er sprake van een geschonden strafvorderlijk voorschrift of rechtsbeginsel?
    - ☐ Welk belang dient het geschonden voorschrift?
    - ☐ Wat is de ernst van het verzuim?
    - ☐ Welk nadeel heeft de verdachte hiervan ondervonden?

Als het probleem ligt in de voorwaarde dat er geen redelijk vermoeden van schuld was of in het feit dat er zonder of niet conform de machtiging van de rechter-commissaris is gehandeld dient dit duidelijk te worden gemaakt in het verweerschrift. Deze twee gronden kent de rechter het meest toe en relatief vaak met de meest ingrijpende consequentie, is uit het jurisprudentieonderzoek gebleken. Daarnaast is het raadzaam om, indien hier sprake van is, te beargumenteren dat de verdachte is geschonden in zijn recht op privéleven (art. 8 EVRM). Deze factoren neemt de rechter mee in de overweging om mee te gaan in het standpunt betreffende onrechtmatig verkregen bewijs en de gevolgen hiervoor voor de straftoemeting (bewijsuitsluiting, strafvermindering of constatering).

Literatuurlijst

Boeken, rapporten en commentaren:

Blom 2017

T. Blom, 'Technische hulpmiddelen', in: C.P.M. Cleiren, J.H. Crijns & M.J.M. Verpalen (red), *Tekst & Commentaar: Strafvordering*, Deventer: Kluwer 2017.

CBS 2017

CBS, Cybersecuritymonitor 2017: een eerste verkenning van dreigingen, incidenten en maatregelen, Den Haag 2017.

Dorst, van 2015

A.J.A. van Dorst, 'Internationale rechtshulp', in: Y. Buruma, *Handboek Strafzaken,* Deventer: Kluwer.

Koops & Goodwin 2014

B.J. Koops & M. Goodwin, Cyberspace, the cloud en and cross-border criminal investigation, Den Haag: WODC 2014.

Rutte & Samsom 2012

M. Rutte & D.M. Samsom, Bruggen Slaan: Regeerakkoord VVD – PvdA, 2012.

Schmitt & Vihul 2017

M.N. Schmitt & L. Vihul, Tallinn manual 2.0 on the International Law applicable to Cyber Operations, Cambridge: Cambridge University Press 2017.

Verbaan 2013

J.H.J. Verbaan, *Straf(proces)recht begrepen*, Den Haag: Boom Juridische Uitgevers 2013

Woude, van der 2018

M.A.H. van der Woude, 'Art. 80sexies Sr', in: C.P.M. Cleiren, J.H. Crijns & M.J.M. Verpalen (red), *Tekst & Commentaar: Strafrecht*, Deventer: Kluwer 2018.

Artikelen uit vaktijdschriften:

Oerlemans, Strafblad 2017/4, p. 350-359

J.J. Oerlemans, 'De Wet Computercriminaliteit III: Meer handhaving op internet', *Strafblad* 2017, afl. 4, p. 350-359.

Zoetekouw, Tvl 2017/ 1, p. 30-33.

M. Zoetekouw, 'Internationaalrechtelijke aspecten van het wetsvoorstel Computercriminaliteit III', *Tijdschrift voor Internetrecht* 2017, afl. 1, p. 30-33.

Parlementaire stukken:

- Kamerstukken II, 2015/16, 34372, 1.
- Handelingen Tweede Kamer, 2016/17, 34372, nr. 37, item 14.
- Kamerstukken II, 2015/16, 34372, 3.
- Kamerstukken II 2003/04, 29441, 3.
- Kamerstukken II 2007/08, 30517, 3.

Wetten en besluiten:

- Besluit technische hulpmiddelen strafvordering
- Wetboek van strafrecht
- Wetboek van strafvordering
- Wet Computercriminaliteit III
- Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden

Internetbronnen:

- 'Voorlopige Hechtenis', *Openbaar Ministerie*, www.om.nl (zoek op Voorlopige Hechtenis)

Jurisprudentie:

Hoge Raad:

- Hoge Raad, 19-02-2013, ECLI:NL:HR:2013:BY5321

Rechtbanken:

- Rb. Limburg 28-01-2014, ECLI:NL:RBLIM:2014:755
- Rb. Amsterdam, 03-09-2015, ECLI:NL:RBAMS:2015:5746
- Rb. Midden-Nederland, 26-01-2016, ECLI:NL:RBMNE:2016:589
- Rb. Den Haag, 11-02-2016, ECLI:NL:RBDHA:2016:1390
- Rb. Oost-Brabant, 12-04-2016, ECLI:RBOBR:2016:1720
- Rb. Limburg 23-09-2016, ECLI:NL:RBLIM:2016:8324
- Rb. Amsterdam, 15-12-2016, ECLI:NL:RBAMS:2016:8313
- Rb. Rotterdam 13-01-2017, ECLI:NL:RBROT:2017:1010
- Rb. Noord-Nederland 31-01-2017, ECLI:NL:RBNNE:2017:463
- Rb. Gelderland, 05-04-2017, ECLI:NL:RBGEL:2017:1894
- Rb. Oost-Brabant 25-04-2017, ECLI:NL:RBOBR:2017:2288
- Rb. Noord-Holland, 20-07-2017, ECLI:RBNHO:2017:6175
- Rb. Noord-Nederland 27-07-2017, ECLI:NL:RBNNE:2017:2882
- Rb. Amsterdam 08-08-2017, ECLI:NL:RBAMS:2017:5704
- Rb. Den-Haag, 12-10-2017, ECLI:NL:RBDHA:2017:11688
- Rb. Zeeland-West-Brabant 17-10-2017, ECLI:NL:RBZWB:2017:6692
- Rb. Amsterdam 29-12-2017, ECLI:NL:RBAMS:2017:9861
- Rb. Oost-Brabant, 23-02-2018, ECLI:NL:RBOBR:2018:830
- Rb. Limburg, 27-02-2018, ECLI:NL:RBLIM:2018:2212
- Rb Amsterdam 16-05-2018, ECLI:NL:RBAMS:2018:3

Bijlage 1: Jurisprudentieanalyse

1. Rb. Noord-Nederland 27 juli 2017, ECLI:NL:RBNNE:2017:2882
2. Rb. Zeeland-West-Brabant 17-10-2017, ECLI:NL:RBZWB:2017:6692
3. Rb. Den-Haag, 12-10-2017, ECLI:NL:RBDHA:2017:11688
4. Rb. Amsterdam 08-08-2017, ECLI:NL:RBAMS:2017:5704
5. Rb. Amsterdam 29-12-2017, ECLI:NL:RBAMS:2017:9861
6. Rb. Noord-Holland, 20-07-2017, ECLI:RBNHO:2017:6175
7. Rb. Gelderland, 05-04-2017, ECLI:NL:RBGEL:2017:1894
8. Rb. Limburg, 27-02-2018, ECLI:NL:RBLIM:2018:2212
9. Rb. Oost-Brabant, 23-02-2018, ECLI:NL:RBOBR:2018:830
10. Rb. Midden-Nederland, 26-01-2016, ECLI:NL:RBMNE:2016:589
11. Rb. Amsterdam, 15-12-2016, ECLI:NL:RBAMS:2016:8313
12. Rb. Limburg 23-09-2016, ECLI:NL:RBLIM:2016:8324
13. Rb. Oost-Brabant, 12-04-2016, ECLI:NL:RBOBR:2016:1720
14. Rb. Den Haag, 11-02-2016, ECLI:NL:RBDHA:2016:1390
15. Rb. Amsterdam, 03-09-2015, ECLI:NL:RBAMS:2015:5746
16. Rb Amsterdam 16-05-2018, ECLI:NL:RBAMS:2018:3297
17. Rb. Rotterdam 13-01-2017, ECLI:NL:RBROT:2017:1010
18. Rb. Noord-Nederland 31-01-2017, ECLI:NL:RBNNE:2017:463
19. Rb. Limburg 28-01-2014, ECLI:NL:RBLIM:2014:755
20. Rb. Oost-Brabant 25-04-2017, ECLI:NL:RBOBR:2017:2288

No.	Standpunt verdediging	Argument rechter	Gevolgen voor de straftoemeting
1	Verdenking op grond van onrechtmatig verkregen informatie	Nederlandse autoriteiten mogen erop vertrouwen dat informatie van buitenlandse autoriteiten betrouwbaar is	Geen bewijsuitsluiting
2	Rechter-commissaris was niet aanwezig en heeft geen toestemming gegeven	Geen dringende noodzakelijkheid om de bevoegdheid zonder toestemming van de rechter-commissaris uit te voeren. Gelet op het geschonden belang en de ernst van het verzuim, is de rechtbank van oordeel dat niet kan worden volstaan met de enkele constatering dat sprake is van een onherstelbaar vormverzuim. Naar het oordeel van de rechtbank is sprake van een ernstige inbreuk op een grondrecht van de verdachte waarbij het belang om toekomstige vergelijkbare vormverzuimen te voorkomen noopt tot bewijsuitsluiting.	In ernstige mate is inbreuk gemaakt op het belang van verdachte, te weten de persoonlijke levenssfeer en het huisrecht in het bijzonder, welk belang door de strafvorderlijke voorschriften gewaarborgd wordt: **bewijsuitsluiting**.
3	Rechter-commissaris heeft geen toestemming gegeven	Geen toestemming om tot uitvoering van de bevoegdheid over te gaan, daardoor vergaande inbreuk op grondrechten. Zonder voorafgaande toetsing door de rechter-commissaris, maar ook zonder toezicht op de uitvoering daarvan door de rechter-commissaris of door een (hulp)officier van justitie en zonder dat de gang van zaken tijdens de	Er is niet alleen een vergaande inbreuk gemaakt op de persoonlijke levenssfeer van verdachte, maar is eveneens het recht van verdachte op een eerlijk proces in de zin van artikel 6 van het Europees Verdrag tot bescherming van de Rechten van de Mens en de fundamentele vrijheden (EVRM) geschonden. Gelet op de hierboven genoemde belangen die de geschonden

		doorzoeking is vastgelegd in een op ambtseed of ambtsbelofte opgemaakt proces-verbaal, zodat dit niet door de rechtbank valt te toetsen.	voorschriften dienen, de ernst van het verzuim en de omstandigheden waaronder het verzuim is begaan, en het nadeel dat daardoor is veroorzaakt, is de rechtbank van oordeel dat het bewijsmateriaal dat door de onrechtmatige doorzoeking is verkregen moet worden **uitgesloten van het bewijs**.
4	Verdenking op grond van onrechtmatig vekregen informatie	Omstandigheden en combinatie van indicatoren zorgen ervoor dat het niet onrechtmatig is	Geen bewijsuitsluiting
5	Geen redelijk vermoeden van schuld	Aanhouding onrechtmatig omdat er geen redelijk vermoeden van schuld was, echter niet ingrijpend, geen inbreuk op grondrechten en geen concreet nadeel voor verdachte.	De schendingen zijn niet dusdanig ingrijpend en leveren niet in die mate een inbreuk op ten aanzien van de grondrechten van verdachte, dat bewijsuitsluiting moet volgen. Verder is niet gesteld dat verdachte enig concreet nadeel heeft ondervonden als gevolg van de vormverzuimen. De rechtbank zal daarom **niet overgaan tot strafvermindering.**
6	Geen redelijk vermoeden van schuld	Op het moment van de machtiging al voldoende vermoeden voor een rechtmatige machtiging	Geen bewijsuitsluiting
7	Geen redelijk vermoeden van schuld	Oudere antecedenten dragen niet bij aan het redelijk vermoeden, dwangmiddel onrechtmatig toegepast. Het belang dat het strafbare feit dat iemand heeft gepleegd onontdekt blijft is geen belang dat door de	Bewijsuitsluiting kan echter slechts aan de orde komen indien het bewijsmateriaal door het verzuim is verkregen en door de onrechtmatige bewijsgaring een belangrijk (strafvorderlijk) voorschrift of rechtsbeginsel in

		strafvorderlijke voorschriften moet worden gerespecteerd.	aanzienlijke mate is geschonden. Daar is in deze zaak geen sprake van. Het betreft hier een doorzoeking van de kofferbak van een huurauto. Voorts volgt uit de jurisprudentie van de Hoge Raad dat het belang dat een strafbaar feit onontdekt blijft niet een rechtens te respecteren belang is. Aldus is geen plaats voor bewijsuitsluiting. Wel dient het vormverzuim naar het oordeel van de rechtbank te worden gecompenseerd door **vermindering van de hoogte van de straf**.
8	Geen redelijk vermoeden van schuld	Anonieme melding en resultaten van een netmeting niet voldoende voor verdenking, r-c had geen machtiging mogen verlenen: onherstelbaar vormverzuim in het voorbereidend onderzoek	Het geschonden voorschrift betreft een belangrijk strafvorderlijk voorschrift; eerst in geval van een redelijk vermoeden van overtreding van de Opiumwet op een bepaalde plaats zijn opsporingsambtenaren bevoegd tot binnentreden. Binnentreden betreft een vergaande bevoegdheid, zeker in geval van betreden van woningen. Binnentreden van een woning tegen de wil van de bewoner vereist dan ook een schriftelijke machtiging. Het huisrecht gelet op het voorgaande is geschonden. Gelet op de ernst van deze schending van verdachtes privacy acht de rechtbank **bewijsuitsluiting** in dit geval op zijn plaats. De aard en ernst van de verdenkingen tegen verdachte die zijn opgekomen naar aanleiding van het

			onrechtmatig verkregen bewijs, nopen niet tot een andere uitkomst van de belangenafweging.
9	Rechtswaarborgen niet in acht genomen door opsporingsambtenaren	Opsporingsambtenaren hebben geen ongeoorloofde druk uitgeoefend	Geen bewijsuitsluiting
10	Geen redelijk vermoeden van schuld	Onvoldoende bevindingen om te stellen dat er sprake was van een redelijk vermoeden van schuld aan een strafbaar feit. Het belang van de aanwezigheid van een redelijk vermoeden van schuld alvorens een (bedrijfs-) pand te mogen doorzoeken, is gelegen in het belangrijke rechtsstatelijke principe dat willekeurig politieoptreden dient te worden voorkomen.	Zonder voldoende gegronde basis voor een verdenking mochten de politieambtenaren niet een dergelijke vergaande inbreuk maken op het recht van verdachte op privacy. De rechtbank kwalificeert de inbreuk die het verzuim heeft gemaakt op voornoemd belang als ernstig. Verdachte heeft voorts persoonlijk nadeel ondervonden van het verzuim. Hij heeft immers moeten dulden dat opsporingsambtenaren - onbevoegdelijk - het door hem gehuurde pand binnen zijn gegaan en hebben doorzocht. De rechtbank komt daarom tot het oordeel dat het resultaat dat door dit verzuim is verkregen, te weten de in de inleiding genoemde aangetroffen goederen, **niet mag bijdragen aan het bewijs**.
11	Rechtswaarborgen niet in acht genomen door opsporingsambtenaren	Opsporingsambtenaren hebben de rechtswaarborgen in acht genomen en niet onrechtmatig gehandeld	Geen bewijsuitsluiting

12	Geen redelijk vermoeden van schuld	Bijna een jaar nadat het delict plaatsvond, op dat moment geen redelijk vermoeden van schuld/verdenking.	De rechtbank is dan ook van oordeel dat de telefoontaps vanaf 3 april 2012 niet rechtmatig zijn, met als gevolg dat in dezen geen andere sanctie geboden is dan het bewijsmateriaal wat op basis van de telefoontaps is verkregen **uit te sluiten van het bewijs**.
13	Geen machtiging van de rechter-commissaris	Het woongedeelte is niet daadwerkelijk binnengetreden dus daar hoefde geen machtiging voor te zijn	Geen bewijsuitsluiting
14	Rechtswaarborgen niet in acht genomen door opsporingsambtenaren	Het feit dat de verdachte geen reactie gaf op de gegeven cautie zorgt niet voor onrechtmatigheid	Geen bewijsuitsluiting
15	Geen redelijk vermoeden van schuld	Er bestond redelijkerwijs geen aanleiding om dwangmiddel uit te oefenen.	De rechtbank is van oordeel dat de fouilleringsbevoegdheid een inbreuk maakt op de persoonlijke levenssfeer van verdachte, zoals bedoeld in artikel 8 van het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden. Het belang van een juiste toepassing van deze bevoegdheid is groot, gezien de strikte waarborgen die de wetgever in het leven heeft geroepen om een dergelijke inbreuk op de privacy te rechtvaardigen. De rechtbank acht **bewijsuitsluiting** noodzakelijk in het licht van de rechtsstatelijke waarborgen die fundamentele strafvorderlijke beginselen

			bieden, alsmede opdat inbreuken als de onderhavige in de toekomst zoveel mogelijk worden voorkomen.
16	Geen toestemming van de rechter-commissaris	Rechter-commissaris gaf alleen toestemming voor het doorzoeken van de smartphone, niet voor de computer. Kwam weinig nieuws aan het licht wat niet uit de smartphone kwam.	De rechtbank is van oordeel dat met de doorzoeking van de computer van verdachte sprake is van een beperkte schending van het privéleven van de verdachte. Met de doorzoeking van de telefoon van verdachte, waarvoor wel toestemming was verleend door de rechter-commissaris, was al een grotendeels volledig beeld verkregen van het digitale leven van verdachte. Niet is aannemelijk geworden dat met de doorzoeking van de computer van verdachte nieuwe gegevens bekend zijn geworden waaruit iets over zijn privéleven kan worden afgeleid. Verdachte heeft daardoor naar mag worden aangenomen beperkt nadeel ondervonden aan het onrechtmatig doorzoeken van zijn computer. **Alleen constatering, geen gevolgen.**
17	Rechtswaarborgen niet in acht genomen door opsporingsambtenaren	Er was voldoende vermoeden van schuld, verdachte is ten onrechte als getuige gehoord en niet gewezen op zijn rechten	Nu de verdachte niet de gelegenheid is geboden om voorafgaand aan het verhoor een advocaat te raadplegen (strafvorderlijk voorschrift), dient de op 28 januari 2016 afgelegde verklaring van de verdachte op grond van de hiervoor aangehaalde rechtspraak van de Hoge Raad **uitgesloten te worden van het bewijs.**

18	Geen redelijk vermoeden van schuld	Rapport is niet onderzocht en dat had wel moeten gebeuren, niet voldoende basis voor verdenking en daarom bevoegdheden onrechtmatig toegepast	Hoewel de vraag of opsporingsfunctionarissen een 'redelijk vermoeden' mochten koesteren door de rechter slechts marginaal kan worden getoetst, kan naar het oordeel van de rechtbank hetgeen in de onderhavige zaak ten grondslag heeft gelegen aan de inzet van de bijzondere opsporingsbevoegdheid als bedoeld in artikel 126n Sv, die toets niet doorstaan. Dit leidt ertoe dat al hetgeen naar aanleiding hiervan is verkregen van het **bewijs dient te worden uitgesloten**.
19	Geen redelijk vermoeden van schuld	Omstandigheden zijn, zonder de ambtshalve kennis van verbalisanten, niet voldoende voor verdenking. Omdat er onvoldoende grond was voor de aanhouding van verdachte, is de rechtbank van oordeel dat er tevens onvoldoende “redelijk vermoeden” in de zin van de Opiumwet bestond om de auto te doorzoeken.	De gevonden verdovende middelen zijn onrechtmatig verkregen bewijs en zullen van het **bewijs worden uitgesloten.**
20	Rechtswaarborgen niet in acht genomen door opsporingsambtenaren	Opsporingsambtenaren hebben zonder wettelijke onderzoek in telefoon verricht. Was voor de opsporingsambtenaren niet duidelijk dat die basis ontbrak. Bij de beoordeling van de ernst van het verzuim betrekt de rechtbank voorts dat het geautomatiseerde onderzoek aan de telefoon van	Voor wat betreft de ernst van het verzuim en het nadeel dat daardoor wordt veroorzaakt, betrekt de rechtbank in haar overweging dat het handelen van de opsporingsambtenaren op het moment in kwestie niet verwijtbaar is geweest. De hiervoor beschreven weging en waardering van de in aanmerking te nemen

		verdachte plaatsvond tegen de achtergrond van de redelijke verdenking dat verdachte op grote schaal handelde in professioneel vuurwerk (gevaarzettend karakter).	beoordelingsfactoren brengt de rechtbank tot de slotsom dat weliswaar sprake is van een onherstelbaar vormverzuim in de zin van artikel 359a van het Wetboek van Strafvordering, maar niet van een dermate ernst en gewicht dat daaraan de consequentie van bewijsuitsluiting dient te worden verbonden. De rechtbank zal, gelet op het vorenstaande, in deze zaak volstaan met de **constatering dat een vormverzuim is begaan.**