# Hack van de Dam?

Een onderzoek naar aandachtspunten die in een toekomstig verweer met betrekking tot de nieuwe strafbaarstelling van online handelsfraude en/of de nieuwe opsporingsbevoegdheid tot het heimelijk binnendringen in een geautomatiseerd werk kunnen worden toegepast


| | |
|---|---|
| Student: | Angela van der Linden |
| Studentnummer: | 2063642 |
| Opleiding: | Juridisch Hogeschool Avans-Fontys te ’s-Hertogenbosch |
| Eerste afstudeerdocent: | dhr. mr. B. Kratsborn |
| Tweede afstudeerdocent: | mw. mr. S. Adjiembaks |
| Opdrachtgever: | Aarts & Nijenhuis Advocaten te Nijmegen |
| Afstudeermentor: | mw. mr. M. Lamers |
| Afstudeerperiode: | februari 2017 – mei 2017 |
| Plaats en datum: | Nijmegen, 29 mei 2017 |




| | |
|---|---|
| Student: | Angela van der Linden |
| Studentnummer: | 2063642 |
| Opleiding: | Juridisch Hogeschool Avans-Fontys te ’s-Hertogenbosch |
| Eerste afstudeerdocent: | dhr. mr. B. Kratsborn |
| Tweede afstudeerdocent: | mw. mr. S. Adjiembaks |
| Opdrachtgever: | Aarts & Nijenhuis Advocaten te Nijmegen |
| Afstudeermentor: | mw. mr. M. Lamers |
| Afstudeerperiode: | februari 2017 – 29 mei 2017 |
| Plaats en datum: | Nijmegen, 29 mei 2017 |

## Voorwoord

Voor u ligt mijn scriptie ‘Hack van de dam?’. Deze scriptie heb ik geschreven in het kader van mijn afstudeerstage bij Aarts & Nijenhuis Advocaten te Nijmegen. De afgelopen vier maanden, van februari 2017 tot en met mei 2017, heb ik aan mijn scriptie gewerkt in het kader van de afsluiting van mijn studie aan de Juridisch Hogeschool Avans-Fontys. De afgelopen jaren heb ik met veel plezier geleerd over het strafrecht. Aarts & Nijenhuis Advocaten heeft mij de kans geboden op dit rechtsgebied af te studeren. Deze kans heb ik met beide handen aangegrepen. De afgelopen periode heb ik mij verdiept in het wetsvoorstel Computercriminaliteit III. Specifiek heb ik mij gericht op de invoering van de nieuwe strafbaarstelling betreffende online handelsfraude en de invoering van de nieuwe opsporingsbevoegdheid tot het heimelijk binnendringen in een geautomatiseerd werk. Ik was nog niet eerder in aanraking gekomen met het onderwerp computercriminaliteit. De laatste maanden heb ik door mijn scriptie erg veel geleerd over dit onderwerp.

Ik zou graag enkele personen willen bedanken die een bijdrage hebben geleverd aan de totstandkoming van mijn scriptie. Ten eerste wil ik Aarts & Nijenhuis Advocaten bedanken dat ik mijn afstudeerstage bij hen heb mogen volgen. Daarnaast wil ik mijn begeleider mevrouw mr. M.T. Lamers bedanken voor haar feedback, input en adviezen bij het schrijven van mijn scriptie. Tevens wil ik de heer mr. H.J.M. Nijenhuis bedanken voor zijn bijdrage aan de totstandkoming mijn scriptie. Daarnaast wil ik de heer mr. B. Kratsborn bedanken voor zijn tijd, feedback en adviezen betreffende mijn scriptie. Tot slot wil ik de heer mr. Hersmus en de heer mr. Kuijer bedanken voor het afnemen van een interview.

Veel leesplezier toegewenst!

Angela van der Linden

Nijmegen, 29 mei 2017

## INHOUDSOPGAVE

## SAMENVATTING

In 2015 is het wetsvoorstel Computercriminaliteit III ingediend bij de Tweede Kamer. Dit om de toenemende bedreigingen en kwetsbaarheden op het terrein van computercriminaliteit tegen te gaan. Computercriminaliteit is het plegen van strafbare feiten met behulp van dan wel gericht op een geautomatiseerd werk. In dit onderzoeksrapport komen de nieuwe strafbaarstelling van online handelsfraude en de nieuwe opsporingsbevoegdheid tot het heimelijk binnendringen in een geautomatiseerd werk uitgebreid aan bod.

Online handelsfraude is het aanbieden van goederen of diensten door middel van een geautomatiseerd werk met als doel geld te verkrijgen zonder deze goederen of diensten daadwerkelijk aan de koper te leveren. Online handelsfraude is een fenomeen dat de laatste jaren steeds meer voorkomt. Tot op heden wordt online handelsfraude aan de hand van artikel 326 Sr, het artikel van oplichting, berecht en vervolgd. Dit levert bewijstechnisch knelpunten op. De Hoge Raad heeft in zijn arresten namelijk bepaald dat het zich enkel voordoen als bonafide verkoper niet direct het aannemen van een valse hoedanigheid oplevert. Het aannemen van een valse hoedanigheid is een van de oplichtingsmiddelen genoemd in artikel 326 Sr. Om online handelsfraude aan de hand van oplichting te vervolgen, is het noodzakelijk dat dit oplichtingsmiddel wordt bewezen. Nu dit niet in alle gevallen mogelijk is, heeft de wetgever het wenselijk geacht een aparte strafbaarstelling voor online handelsfraude te introduceren. Voor de vervolging van online handelsfraude is niet meer noodzakelijk dat de verkoper een valse hoedanigheid heeft aangenomen. In de toekomst moet alleen worden bewezen dat sprake is van een gewoonte of beroep maken, de verkoper het oogmerk heeft om zonder volledige levering van goederen of diensten geld hiervoor te krijgen en gebruik is gemaakt van een geautomatiseerd werk. In toekomstige procedures is het verstandig voor de advocaat extra aandacht te besteden aan ‘een gewoonte of beroep maken’, ‘het oogmerk’, ‘geautomatiseerd werk’, de strafeis en de verantwoordelijkheid van het slachtoffer.

Het heimelijk binnendringen in een geautomatiseerd werk is als opsporingsbevoegdheid voorgesteld om de technische ontwikkelingen het hoofd te kunnen bieden bij de opsporing naar een strafbaar feit. Deze bevoegdheid mag na de inwerkingtreding van het wetsvoorstel ingezet worden voor strafbare feiten waarop een gevangenisstraf van vier jaren of meer is gesteld of andere misdrijven zoals genoemd in artikel 67 lid 1 Sv. Daarnaast moeten de strafbare feiten ook een ernstige inbreuk op de rechtsorde opleveren. De bevoegdheid mag alleen ingezet worden ten behoeve van de doelen genoemd in artikel 126nba lid 1 Sv. De inzet van de bevoegdheid vindt plaats door middel van een technisch hulpmiddel. Dit technische hulpmiddel moet voldoen aan de eisen genoemd in het Besluit technische hulpmiddelen strafvordering. Indien niet aan deze eisen voldaan is, mag het hulpmiddel niet worden ingezet. Het heimelijk binnendringen in een geautomatiseerd werk is een ingrijpende bevoegdheid die een inbreuk maakt op het privéleven van de verdachte. De controle van de inzet achteraf is beperkt geregeld. Opsporingsambtenaren zijn verplicht een proces-verbaal op te maken van hun handelingen tijdens de opsporing. Het probleem is dat niet alle zaken waar de opsporingsbevoegdheid is toegepast bij de rechter terechtkomen, waardoor niet gecontroleerd kan worden of deze juist is ingezet. In procedures waarin deze bevoegdheid is ingezet wordt aangeraden te controleren of deze is ingezet ten behoeve van de doelen genoemd in artikel 126nba lid 1 Sv, of aan de proportionaliteit en subsidiariteit is voldaan, of het technische hulpmiddel voldoet aan de eisen en of de bevoegdheid is ingezet in een apparaat dat is aan te merken als een geautomatiseerd werk. Mocht dit niet het geval zijn, dan wordt aanbevolen een artikel 359a Sv-verweer te voeren.

## LIJST VAN AFKORTINGEN

| | |
|---|---|
| Bths | Besluit technische hulpmiddelen strafvordering |
| CBS | Centraal Bureau voor Statistiek |
| EHRM | Europese Hof voor de Rechten van de Mens |
| EVRM | Europees Verdrag voor de Rechten van de Mens |
| GW | Grondwet |
| LMIO | Landelijk Meldpunt Internetoplichting |
| LOVS | Landelijk Overleg Vakinhoud Strafrecht |
| Marktplaats | www.marktplaats.nl |
| MvA | memorie van antwoord |
| MvT | memorie van toelichting |
| OM | Openbaar Ministerie |
| OvJ | officier van justitie |
| Sr | Strafrecht |
| Sv | Strafvordering |
| WvSr | Wetboek van Strafrecht |
| WvSv | Wetboek van Strafvordering |

# 1 INLEIDING

In dit hoofdstuk wordt een korte beschrijving gegeven van de afstudeerorganisatie. Verder wordt de probleembeschrijving en aanleiding beschreven aan de hand waarvan het onderzoek tot stand is gekomen. Tevens worden de centrale vraag en de doelstelling beschreven. Daarna wordt het onderzoek verantwoord en afgebakend. Tot slot volgt een leeswijzer van het complete onderzoeksrapport.

## 1.1 DE AFSTUDEERORGANISATIE

Aarts & Nijenhuis Advocaten is een advocatenkantoor gevestigd te Nijmegen. Aarts & Nijenhuis Advocaten is gespecialiseerd in (jeugd)strafrecht, bestuursrecht, letselschade, onrechtmatige daad, huurrecht en sociaal zekerheidsrecht. Het is een sociaal advocatenkantoor dat voornamelijk mensen bijstaat die moeite hebben om financieel rond te komen. Tevens is het een maatschappelijk betrokken kantoor. Aarts & Nijenhuis Advocaten sponsort de Kinder- en jongerenrechtswinkel en daarnaast onderhoudt Aarts & Nijenhuis Advocaten goede contacten met het daklozencentrum NuNN te Nijmegen.

## 1.2 PROBLEEMBESCHRIJVING EN AANLEIDING

In 1993 is de Wet computercriminaliteit in Nederland in werking getreden. Tot deze tijd kende de Nederlandse wetgeving geen wetgeving die gericht was op computercriminaliteit. Zowel formeel- als materieelrechtelijke wetgeving ontbrak.[1] Daarom heeft de minister van Justitie in 1985 een commissie aangewezen om onderzoek te doen naar de mogelijkheid van wetgeving op het gebied van computercriminaliteit.[2] Dit was de Commissie Computercriminaliteit, ook wel bekend als de Commissie-Franken, vernoemd naar haar voorzitter. [3] De Wet computercriminaliteit is tot stand gekomen op basis van de aanbevelingen van de Commissie-Franken in 1987.[4] De technologie op het gebied van computers en andere geautomatiseerde werken veranderde snel. Daarom werd in 1999 een eerste voorstel gedaan om de Wet computercriminaliteit aan te passen.[5] Na het ondertekenen van het Cybercrime-Verdrag is de huidige Wet computercriminaliteit in 2006 in werking getreden.

In 2015 is het wetsvoorstel Computercriminaliteit III bij de Tweede Kamer ingediend. Dit wetsvoorstel heeft als doel het juridische instrumentarium voor de opsporing en vervolging van computercriminaliteit te versterken. Door het toevoegen van nieuwe strafvorderlijke bevoegdheden en strafbepalingen beoogt de wetgever het bestaande instrumentarium uit te breiden. Een voorbeeld hiervan is het creëren van een nieuwe opsporingsbevoegdheid om 'onder voorwaarden een geautomatiseerd werk, dat in gebruik is bij een verdachte, op afstand heimelijk binnen te dringen met het oog op bepaalde doelen op het gebied van de opsporing van ernstige strafbare feiten'.[6] Tevens wordt de bevoegdheid van de officier van justitie (hierna: OvJ) tot het ontoegankelijk maken van gegevens uitgebreid. Daarnaast worden als nieuwe strafbepalingen heling van gegevens en online handelsfraude geïntroduceerd. Tot slot wordt de strafbaarstelling betreffende grooming aangepast en verruimd.[7]

Nu nieuwe strafbaarstellingen met betrekking tot computercriminaliteit geïntroduceerd worden, verwacht het kantoor zaken met betrekking tot computercriminaliteit te gaan behandelen. Gelet

[1] De Vey Mestdagh 2014, p. 211.
[2] www.wodc.nl zoek op: *commissie computercriminaliteit*.
[3] Wiegmans 1991, p. 11.
[4] Koops, *Justitiële verkenningen* 2012, 38(1), p. 12.
[5] www.iusmentis.com zoek op*: computercriminaliteit.*
[6] *Kamerstukken II* 2015/16, 34372, 3, p. 3.
[7] *Kamerstukken II* 2015/16, 34372, 3, p. 3.

op de strafzaken die Aarts & Nijenhuis Advocaten op dit moment behandelt, verwacht het kantoor in de toekomst vooral zaken betreffende online handelsfraude te behandelen. Het probleem is dat Aarts & Nijenhuis Advocaten nog onvoldoende bekend is met de wijzigingen van het wetsvoorstel Computercriminaliteit III. Het gaat om een kennisgat dat het kantoor graag opgevuld ziet worden. Aarts & Nijenhuis Advocaten wil meer informatie over online handelsfraude en het heimelijk binnendringen in een geautomatiseerd werk om in de toekomst de personen die in aanraking komen met computercriminaliteit goed bij te kunnen staan.

In dit onderzoek is gedetailleerd onderzocht wat het wetsvoorstel Computercriminaliteit III inhoudt. Het onderzoek richt zich vooral op online handelsfraude en het heimelijk binnendringen in een geautomatiseerd werk. Dit gebeurt door middel van een literatuur- en jurisprudentieonderzoek en een praktijkonderzoek. Aan de hand van dit onderzoek worden aandachtspunten met betrekking tot de nieuwe regelgeving toegelicht. Deze resultaten kunnen gebruikt worden bij de verdediging van een cliënt in een juridische procedure.

### 1.3 CENTRALE VRAAG

De centrale vraag van het onderzoek luidt als volgt:

*Welke aandachtspunten, die in een mogelijk verweer tegen een vervolging wegens online handelsfraude kunnen worden opgenomen, zijn er naar aanleiding van een onderzoek naar de strafbaarstelling betreffende online handelsfraude en de opsporingsbevoegdheid tot het heimelijk binnendringen van een geautomatiseerd werk met betrekking tot het wetsvoorstel Computercriminaliteit III te formuleren?*

### 1.4 DOELSTELLING

Het doel van dit onderzoek is om op 29 mei 2017 aan mr. Marjolijn Lamers, advocaat bij Aarts & Nijenhuis Advocaten, een onderzoeksrapport te overhandigen waarin advies wordt gegeven over aandachtspunten die naar voren komen naar aanleiding van een onderzoek betreffende de strafbaarstelling van online handelsfraude en de invoering van de opsporingsbevoegdheid tot het heimelijk binnendringen in een geautomatiseerd werk met betrekking tot het wetsvoorstel Computercriminaliteit III, zodat mr. Lamers aan de hand van die aandachtspunten in een strafzaak een gedegen verweer kan opstellen.

### 1.5 ONDERZOEKSSTRATEGIE EN VERANTWOORDING

De onderzoeksstrategie is onderverdeeld in een onderzoek naar het recht en een onderzoek naar de praktijk. Bij het onderzoek naar het recht wordt gebruik gemaakt van een rechtsbronnen- en literatuuronderzoek. Als bronnen zijn rechtsbronnen en literatuur geraadpleegd. Denk hierbij aan de wet, boeken en artikelen uit juridische tijdschriften. De teksten uit deze bronnen zijn geanalyseerd, vergeleken en geïnterpreteerd.[8]
Voor het onderzoek naar de praktijk zijn verschillende uitspraken van rechters (jurisprudentie) en personen geraadpleegd. De jurisprudentie is inhoudelijk geanalyseerd. Naar aanleiding van deze analyse zijn relevante resultaten op papier gezet. Zo is een analyse gedaan naar de invulling van bestanddelen. Daarnaast volgen cijfers over bewezenverklaringen en vrijspraken met betrekking tot vervolging aan de hand van het artikel oplichting. Deze resultaten zijn aangevuld met informatie afkomstig uit afgenomen interviews. De geïnterviewde personen zijn experts op het gebied van computercriminaliteit. Uit deze twee onderdelen is het praktijkdeel van dit onderzoek voortgekomen.

De verantwoording voor de gebruikte bronnen en onderzoeksmethoden is opgenomen in de bijlagen. Daarom wordt voor de verantwoording verwezen naar bijlage 1.

### 1.6 AFBAKENING

[8] Van Schaaijk 2011, p. 79.

Het wetsvoorstel Computercriminaliteit III behelst meer dan alleen het voorstel tot invoering van de nieuwe strafbaarstelling van online handelsfraude en de invoering van de nieuwe opsporingsbevoegdheid tot het heimelijk binnendringen in een geautomatiseerd werk. Helaas kunnen de overige aanpassingen die volgen uit het wetsvoorstel niet gedetailleerd behandeld worden in dit onderzoekrapport. Het onderzoek zou in dat geval te uitgebreid worden. Wel zijn deze aanpassingen kort in hoofdstuk 2 beschreven. Op die manier wordt een duidelijk beeld verkregen van het gehele wetsvoorstel. Daarnaast is besloten om het internationale aspect van computercriminaliteit niet te belichten. In verband met het tijdsbestek van het onderzoek is het niet mogelijk ook deze onderwerpen te behandelen.

### 1.7 LEESWIJZER

Hoofdstuk 2 behandelt het wetsvoorstel Computercriminaliteit III. In dit hoofdstuk wordt beschreven wat de aanleiding en de inhoud van het wetsvoorstel is. Daarnaast wordt aangegeven wat de stand van zaken is met betrekking tot het wetsvoorstel Computercriminaliteit III.

Hoofdstuk 3 behandelt de nieuwe strafbaarstelling van online handelsfraude. Eerst wordt besproken op welke manier online handelsfraude op dit moment vervolgd en bestraft wordt. Tevens is een jurisprudentie-analyse gegeven over deze manier van vervolging. Daarna wordt beschreven wat wijzigt naar aanleiding van de invoering van de nieuwe strafbaarstelling. De resultaten uit deze paragraaf zijn mede afkomstig van een jurisprudentie-analyse. In paragraaf 3.7 worden de afgenomen interviews uitgewerkt. Paragraaf 8 behandeld aandachtspunten die in toekomstige met betrekking tot online handelsfraude gebruikt kunnen worden.

Hoofdstuk 4 ziet op de nieuw voorgestelde opsporingsbevoegdheid tot het heimelijk binnendringen in een geautomatiseerd werk. In dit hoofdstuk wordt de opsporingsbevoegdheid uiteengezet en inhoudelijk behandeld. Daarnaast is door een parketsecretaris van het OM en een raadsheer van het gerechtshof de mening gegeven over de voorgestelde bevoegdheid. Naar aanleiding van de inhoudelijke uiteenzetting van de opsporingsbevoegdheid en de interviews zijn aandachtspunten geformuleerd die gebruikt kunnen worden in toekomstige strafprocedures. Deze procedures hoeven niet in relatie te staan tot computercriminaliteit. De aandachtspunten kunnen in alle procedures worden toegepast waar deze opsporingsbevoegdheid is ingezet.

Tot slot worden in hoofdstuk 5 conclusies en aanbevelingen geformuleerd aan de hand waarvan Aarts & Nijenhuis Advocaten hun juridische procedures, waarin online handelsfraude of het heimelijk binnendringen in een geautomatiseerd werk centraal staat, kunnen aanpassen.

## 2 WETSVOORSTEL COMPUTERCRIMINALITEIT III

In 2013 is een wijziging van het Wetboek van Strafrecht (hierna: WvSr) en het Wetboek van Strafvordering (hierna: WvSv) in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit voorgesteld. Dit wetsvoorstel wordt het wetsvoorstel Computercriminaliteit III genoemd. Dit hoofdstuk is een inleidend hoofdstuk met betrekking tot computercriminaliteit. In paragraaf 1 zijn de aanleiding voor het wetsvoorstel en de aanleiding voor de invoering van de nieuwe strafbaarstelling van online handelsfraude en de invoering van de nieuwe opsporingsbevoegdheid tot het heimelijk binnendringen in een geautomatiseerd werk gegeven. De definitie van computercriminaliteit wordt in paragraaf 2 uitgelegd. Paragraaf 3 behandelt de voorstellen van het wetsvoorstel Computercriminaliteit III die in dit onderzoeksrapport verder niet uitgebreid aan bod komen. De stand van zaken met betrekking tot het wetsvoorstel wordt uiteengezet in paragraaf 4. Tot slot geeft paragraaf 5 een deelconclusie.

### 2.1 AANLEIDING WETSVOORSTEL

In het regeerakkoord 'Bruggen slaan' van het kabinet VVD-PvdA uit 2012 is opgenomen dat de regelgeving met betrekking tot computercriminaliteit aangepast moet worden. Dit in verband met de toenemende bedreigingen en kwetsbaarheden op het terrein van computercriminaliteit. In het regeerakkoord staat opgenomen dat ze deze bedreigingen en kwetsbaarheden het hoofd willen bieden door de opsporing te versterken en het juridisch instrumentarium aan de huidige stand van zaken aan te passen.[9] Daarnaast is tijdens de behandeling van het wetsvoorstel in de Tweede Kamer aangegeven dat computercriminaliteit professionaliseert. Tevens wordt gesteld dat het steeds moeilijker wordt om je eigen gegevens tegen computercriminaliteit te beschermen. De schade die computercriminaliteit aanricht, ligt op dit moment op tien miljard euro per jaar. Verwacht wordt dat dit bedrag alleen maar zal toenemen.[10] Daarom acht de overheid dit wetsvoorstel noodzakelijk.

#### 2.1.1 Aanleiding strafbaarstelling online handelsfraude

De Memorie van Toelichting (hierna: MvT) stelt dat het noodzakelijk is een aparte strafbaarstelling voor online handelsfraude in het leven te roepen. Online handelsfraude zou op dit moment niet op een adequate manier bestraft kunnen worden. Zo heeft de Hoge Raad een lijn in de jurisprudentie ingezet waardoor internetoplichting niet altijd veroordeeld kan worden. Dit knelpunt komt in paragraaf 4 van hoofdstuk 3 aan bod.[11]

Tevens is een toename te zien in het aantal slachtoffers van online handelsfraude.
Het Centraal Bureau voor Statistiek (CBS) stelt elk jaar een Veiligheidsmonitor op. In deze Veiligheidsmonitor wordt sinds 2012 het slachtofferpercentage van computercriminaliteit opgenomen. In 2012 was 2,7% van de Nederlanders slachtoffer van online handelsfraude. In 2016 is dit gestegen naar 3,3%.[12] Uit deze cijfers komt naar voren dat het aantal slachtoffers van online handelsfraude een stijging kent.

Omdat het aantal slachtoffers blijft toenemen en de vervolging van de personen die deze slachtoffers maken op dit moment beperkt succesvol is, heeft de wetgever besloten om een aparte strafbaarstelling te introduceren.

[9] *Regeerakkoord 'Bruggen slaan'* 2012, p. 27.
[10] Kamerstukken II 2016/17, 34372, 34, p. 1.
[11] *Kamerstukken II* 2015/16, 34372, 3, p. 73.
[12] *Veiligheidsmonitor 2016*, p. 39.

### 2.1.2 Aanleiding opsporingsbevoegdheid heimelijk binnendringen

Omdat de bestaande opsporingsbevoegdheden niet afdoende zijn om de knelpunten op het gebied van opsporing van computercriminaliteit tegen te gaan, ziet de wetgever aanleiding tot het invoeren van een nieuwe opsporingsbevoegdheid. Dit is de opsporing tot het heimelijk binnendringen in een geautomatiseerd werk. Deze opsporingsbevoegdheid maakt het mogelijk heimelijk binnen te dringen in een geautomatiseerd werk.[13] De laatste jaren zijn de volgende knelpunten ontstaan met betrekking tot de opsporing van strafbare feiten die verband houden met computercriminaliteit: versleuteling, het gebruik van draadloze netwerken en het gebruik van de Cloud.

Elektronische gegevens kunnen tegenwoordig beter versleuteld worden. Hierdoor is het moeilijker om strafbare feiten op te sporen. Het versleutelen van gegevens houdt in dat leesbare data omgevormd worden in onleesbaar materiaal door middel van een wiskundig algoritme.[14] Ook leken op het gebied van versleuteling van gegevens kunnen aan de hand van speciale programma's die op internet worden aangeboden gemakkelijk hun gegevens versleutelen.
Tevens is het gebruik van draadloze netwerken een probleem geworden. Met een router kan een draadloos netwerk worden aangeboden. Zo kan men bijvoorbeeld thuis, maar ook op het werk of een openbare plek zoals een restaurant, café of sportvereniging zijn smartphone of laptop aansluiten op dat draadloze netwerk. Tot op heden is het niet mogelijk om na te gaan welke apparaten gebruik maken van de router. Daarnaast is het niet mogelijk om te achterhalen welke gegevens met welk apparaat worden opgehaald of verzonden.[15] Het probleem daarvan is dat identificatie van de gebruiker van het geautomatiseerde werk vrijwel onmogelijk is. Onderzoek in een geautomatiseerd werk zou kunnen bijdragen aan de identificatie van het geautomatiseerde werk of van de gebruiker.
Tot slot heeft de intrede van de Cloud opsporing van strafbare feiten bemoeilijkt. Bij een Cloud bevindt de opslagplaats zich niet op het geautomatiseerde werk van de persoon, maar op een andere plek. Waar de gegevens precies opgeslagen worden, is niet duidelijk. Een voorbeeld van werken in een Cloud is Dropbox.[16] Indien men gegevens opslaat in de Cloud, dan worden deze gegevens op een server opgeslagen die zich elders in Nederland of in het buitenland bevindt. Bovendien worden de opgeslagen gegevens in de meeste gevallen over meerdere servers verspreid. Daardoor kunnen de gegevens van een gebruiker zich in verschillende landen bevinden. Het is een moeilijke taak om te onderzoeken welke gegevens waar zijn opgeslagen.[17]

## 2.2 COMPUTERCRIMINALITEIT

In Nederland wordt in de wetshistorie en literatuur de definitie computercriminaliteit gehanteerd. De MvT omschrijft computercriminaliteit als volgt:

*"het plegen van strafbare feiten met behulp van dan wel gericht op een geautomatiseerd werk*."[18]

Artikel 80sexies Sr geeft de volgende definitie van een geautomatiseerd werk:

*"Een inrichting die bestemd is om langs elektronische weg gegevens op te slaan, verwerken en over te dragen."*

[13] *Kamerstukken II* 2015/16, 34372, 3, p. 7.
[14] *Kamerstukken II* 2015/16, 34372, 3, p. 7.
[15] *Kamerstukken II* 2015/16, 34372, 3, p. 10.
[16] www.fundaments.nl zoek op: *Werken in de Cloud*.
[17] *Kamerstukken II* 2015/16, 34372, 3, p. 11.
[18] *Kamerstukken II* 2015/16, 34372, 3, p. 7.

Het opslaan, verwerken en overdragen van gegevens zijn cumulatieve voorwaarden. Indien niet aan een van deze voorwaarden wordt voldaan, is geen sprake van een geautomatiseerd werk. Een telefoontoestel waarmee alleen gebeld kan worden, is daarom geen geautomatiseerd werk.[19]

In de literatuur zijn meerdere definities van computercriminaliteit te vinden.[20] Het gaat te ver om al deze definities te behandelen. Daarom wordt voor een duidelijk beeld de definitie gehanteerd die de MvT geeft.

## 2.3 INHOUD WETSVOORSTEL

In deze paragraaf wordt de inhoud van het wetsvoorstel Computercriminaliteit III behandeld. Dit is bedoeld om een goed beeld te krijgen van het gehele wetsvoorstel. Twee onderdelen van het wetsvoorstel worden uitgebreid behandeld: online handelsfraude en het heimelijk binnendringen in een geautomatiseerd werk. Online handelsfraude komt aan bod in hoofdstuk 3. In hoofdstuk 4 wordt ingegaan op het heimelijk binnendringen in een geautomatiseerd werk. De overige onderdelen uit het wetsvoorstel worden in deze paragraaf behandeld.

### 2.3.1 Bevoegdheid OvJ

In artikel 54a Sr staat de bevoegdheid van de OvJ beschreven om gegevens op het internet ontoegankelijk te maken. Dit mag zij alleen doen nadat een schriftelijke machtiging is verleend door de rechter-commissaris. Het nieuwe wetsvoorstel beoogt deze bevoegdheid aan te passen. Het doel van deze wijziging is om de samenleving beter te beschermen tegen strafbare feiten die zich op internet voordoen.[21]

De bedoeling van het wetsvoorstel Computercriminaliteit III is om de combinatie van de vervolgingsuitsluitingsgrond en de bevelsbevoegdheid uit elkaar te halen. Uit de rechtspraak volgt dat deze combinatie vragen oproept en de toepassing van de regeling in de praktijk extra ingewikkeld maakt.[22] Op dit moment staat de regeling in het WvSr. Uit wetssystematisch oogpunt en vanwege de overzichtelijkheid is het wenselijk deze bevoegdheid op te nemen in het WvSv.[23]

### 2.3.2 Heling van gegevens

In het wetsvoorstel Computercriminaliteit III worden twee nieuwe strafrechtelijke bepaling voorgesteld die het wederrechtelijk overnemen en de heling van niet-openbare gegevens strafbaar maakt. Het gaat om twee nieuwe wetsartikelen die worden voorgesteld. Artikel 138c Sr en artikel 139g Sr. Het is de bedoeling dat in artikel 138c Sr het wederrechtelijk met een technisch hulpmiddel overnemen van niet-openbare gegevens door middel van een geautomatiseerd werk strafbaar wordt gesteld. In artikel 139g Sr wordt het voorhanden hebben of bekend maken van niet-openbare gegevens die door een misdrijf zijn verkregen strafbaar gesteld. Op dit moment is het niet mogelijk het wederrechtelijke toe-eigenen van gegevens te bestraffen aan de hand van verduistering of diefstal. Dit komt omdat met de invoering van de het eerste wetsvoorstel Computercriminaliteit is gekozen om gegevens als begrip zijnde afzonderlijk te behandelen en niet gelijk te stellen aan een ‘goed’.[24] Tevens heeft de Hoge Raad in zijn jurisprudentie de gelijkstelling van gegevens aan een goed afgekeurd.[25] Dit geldt ook voor de heling van gegevens. De heling van gegevens kan niet aan de hand van artikel 416 Sr vervolgd worden.

---

[19] Cleiren, Crijns & Verpalen 2016, pagina 875.

[20] Van der Hof, Lodder & Zwenne 2014, p. 213-214.

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

[22] Rb. Assen 22 juli 2008, ECLI:NL:RBASS:2008:BD8451, Hof Leeuwarden 20 april 2009, ECLI:NL:GHLEE:2009:BI1645, Rb. Assen 24 november 2009, ECLI:N:RBASS:2009:BK4226.

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

[24] *Kamerstukken II* 2015/16, 34372, 3, p. 63.

[25] HR 3 december 1996, NJ 1997, 574.

### 2.3.3 Grooming

Het wetsvoorstel Computercriminaliteit III stelt voor om de wetsartikelen met betrekking tot grooming en de verleiding van minderjarigen tot ontucht te verruimen. De huidige regelgeving blijkt niet afdoende om kinderen te beschermen tegen de seksuele benadering van volwassenen via internet. Het is in het belang van een behoorlijke bestrijding van grooming en verleiding van minderjarigen tot ontucht om deze regelgeving aan te passen.[26]
Grooming wordt omschreven als '*het benaderen en verleiden van een kind met als uiteindelijk doel het plegen van seksueel misbruik met dat kind'.*[27]

De wetswijziging van artikel 54a Sr, de invoering van de strafbaarstelling van wederrechtelijke verkrijging en heling van gegevens en de wijziging van de artikelen 248a en 248e Sr, worden in dit onderzoeksrapport verder niet behandeld. In dit onderzoeksrapport staan de regelingen met betrekking tot het heimelijk binnendringen in een geautomatiseerd werk en online handelsfraude centraal.

## 2.4 STAND VAN ZAKEN WETSVOORSTEL

Op 21 december 2015 is het wetsvoorstel ingediend bij de Tweede Kamer. De inhoudelijke behandeling van het wetsvoorstel heeft bijna een jaar later op 13 december 2016 plaatsgevonden. Tijdens deze behandeling is vooral gediscussieerd over het debat met betrekking tot veiligheid en privacy. Voorstanders stellen dat je niet tussen een van deze twee kunt kiezen en dat het wetsvoorstel, dat de veiligheid van burgers moet versterken, ook de privacy van burgers beschermt. Daarentegen zijn de tegenstanders van het wetsvoorstel van mening dat de bevoegdheden, genoemd in het wetsvoorstel, een te grote inbreuk op de privacy maakt. De voorstanders reageren daar weer op door te stellen dat de uitbreiding van de digitale opsporingsmogelijkheden bedoeld is om de burgers te beschermen tegen criminelen die de privegegevens van burgers bekend willen maken of verhandelen. [28] Daarnaast is over de inhoud van het wetsvoorstel gediscussieerd. Op 20 december 2016 heeft de Tweede Kamer gestemd. Zij hebben het wetsvoorstel goedgekeurd. De PvdA, VVD, SGP, ChristenUnie en CDA hebben als partij voor gestemd. Daarnaast hebben de onafhankelijke Kamerleden Van Vliet, Houwers en Monasch voor het wetsvoorstel gestemd.

Na de goedkeuring van het wetsvoorstel door de Tweede Kamer, is het wetsvoorstel ingediend bij de Eerste Kamer. Op dit moment is het wetsvoorstel daar in behandeling. Op 3 april 2017 heeft de Eerste Kamercommissie voor Veiligheid en Justitie het voorlopige verslag uitgebracht. [29] Een behandeling van het wetsvoorstel in de Eerste Kamer is nog niet vastgesteld.

## 2.5 DEELCONCLUSIE

Het wetsvoorstel Computercriminaliteit III is door de wetgever voorgesteld om de toenemende bedreigingen en kwetsbaarheden op het gebied van computercriminaliteit tegen te gaan. De nieuw voorgestelde strafbaarstelling betreffende online handelsfraude wordt ingevoerd vanwege de knelpunten die op dit moment in de jurisprudentie naar voren komen. De versleuteling van gegevens, het gebruik van draadloze netwerken en het gebruik van de Cloud zijn redenen voor de invoering van de nieuwe opsporingsbevoegdheid tot het heimelijk binnendringen in een geautomatiseerd werk.

[26] *Kamerstukken II* 2015/16, 34372, 3, p. 67.
[27] *Kamerstukken II* 2015/16, 34372, 3, p. 68.
[28] *Kamerstukken II* 2015/16, 34372, 26, p. 1.
[29] www.eerstekamer.nl zoek op: *34372*.

# 3 ONLINE HANDELSFRAUDE

Het wetsvoorstel Computercriminaliteit III stelt een nieuwe strafbaarstelling voor. Na inwerkingtreding van het wetsvoorstel Computercriminaliteit III, wordt in het WvSr een nieuw wetsartikel geïntroduceerd dat online handelsfraude strafbaar stelt. In dit hoofdstuk wordt deze strafbaarstelling inhoudelijk behandeld. Tevens wordt bekeken aan de hand van welk wetsartikel online handelsfraude op dit moment vervolgd wordt en wat de aanleiding is voor het opnemen van een aparte strafbaarstelling in het WvSr.
In paragraaf 1 zijn twee voorbeelden gegeven van online handelsfraude. Op die manier wordt een duidelijk beeld gecreëerd wat met online handelsfraude bedoeld wordt. Daarna wordt in paragraaf 2 uitgelegd hoe de overheid en particuliere instanties op dit moment online handelsfraude aanpakken. Omdat online handelsfraude op dit moment wordt berecht aan de hand van oplichting, zal paragraaf 3 het artikel oplichting uiteenzetten. Paragraaf 4 gaat over de knelpunten die naar voren komen door online handelsfraude te berechten aan de hand van oplichting. In paragraaf 5 is een uitgebreide analyse gegeven over de berechting van online handelsfraude aan de hand van oplichting. Deze analyse is tot stand gekomen door meer dan 110 uitspraken en arresten te analyseren. In paragraaf 6 wordt de nieuwe strafbaarstelling van online handelsfraude uiteengezet. De interviews met een parketsecretaris en raadsheer van het gerechtshof zijn in paragraaf 7 uitgewerkt. In paragraaf worden 8 enkele aandachtspunten beschreven die van belang zijn in een procedure betreffende online handelsfraude na invoering van de nieuwe strafbaarstelling. Tot slot is in paragraaf 9 een deelconclusie gegeven.

## 3.1 ONLINE HANDELSFRAUDE

In deze paragraaf wordt uitgelegd wat online handelsfraude inhoudt. Aan de hand van twee voorbeelden wordt online handelsfraude verduidelijkt.

Na inwerkingtreding van het wetsvoorstel Computercriminaliteit III, zal in het WvSr artikel 326d worden opgenomen. Dit artikel luidt als volgt:

*"Hij die een beroep of een gewoonte maakt van het door middel van een geautomatiseerd werk verkopen van goederen of verlenen van diensten tegen betaling met het oogmerk om zonder volledige levering zich of een ander van de betaling van die goederen of diensten te verzekeren, wordt gestraft met een gevangenisstraf van ten hoogste vier jaren of een geldboete van de vijfde categorie."*

In dit artikel wordt online handelsfraude strafbaar gesteld. Online handelsfraude is een strafbaar feit dat wordt gepleegd via het internet. Om een duidelijker beeld te krijgen van online handelsfraude wordt eerst een voorbeeld gegeven. Dit voorbeeld is afkomstig van een rechtszaak bij de rechtbank Rotterdam uit 2016.[30]
Een man heeft een webwinkel opgericht. Op deze webwinkel worden telefoons en tablets aangeboden. Deze artikelen worden op de webwinkel voor een lagere prijs aangeboden dan dat ze eigenlijk waard zijn. Dit verschil in prijs is niet zo groot dat argwaan bij kopers wordt gewekt over de betrouwbaarheid van de verkoper. Door de webwinkel op te richten in de decembermaand, heeft de verdachte geprobeerd zoveel mogelijk kopers bij elkaar te krijgen. Wanneer de kopers een aankoop deden in de webwinkel, werden zij verplicht om eerst het bedrag over te maken naar de rekening van de verdachte. Nadat het aankoopbedrag betaald was, zou het product worden opgestuurd naar de koper. Het product werd echter nooit geleverd. Op deze manier heeft de oprichter van deze webwinkel ongeveer vijfhonderd slachtoffers gemaakt van online handelsfraude.
Dit is een geraffineerde manier van online handelsfraude. Er is nog een veel bekendere manier om online handelsfraude te plegen. In veel gevallen worden goederen op www.marktplaats.nl (hierna: Marktplaats) aangeboden. Marktplaats is een website waarop particulieren nieuwe of

[30] Rb. Rotterdam 30 juni 2016, ECLI:NL:RBROT:2016:4946.

tweedehands goederen kunnen aanbieden met de bedoeling deze aan een andere persoon te verkopen.[31] In sommige gevallen plaatsen mensen advertenties waarin zij een product aanbieden zonder dat zij de bedoeling hebben deze producten te leveren. Zij laten een koper geloven dat het product wordt toegezonden op het moment dat de koper een bepaald bedrag voor het product heeft overgemaakt op de rekening van de verdachte of een derde persoon. In veel gevallen is het moeilijk om na het overmaken van het bedrag contact te krijgen met de verkoper. De verkoper traceren is meestal onmogelijk. Deze vorm van online handelsfraude staat beter bekend als Marktplaatsoplichting.

## 3.2 HUIDIGE AANPAK ONLINE HANDELSFRAUDE

Om internetoplichting adequater te kunnen aanpakken en vervolgen is het Landelijk Meldpunt Internetoplichting (hierna: LMIO) opgericht. Dit hebben de Politie en het Openbaar Ministerie (hierna: OM) in samenwerking met Marktplaats gedaan.[32] Bij het LMIO is een team aangesteld dat gespecialiseerd is in het onderzoek doen naar online handelsfraude. Zo heeft het LMIO ook een eigen OvJ, zoals aangegeven door de heer Hersmus in zijn interview.
Online, op de website www.politie.nl, kunnen slachtoffers aangifte doen van internetoplichting. Deze aangiften komen op een centraal punt binnen, namelijk het LMIO. Daarnaast wordt op deze website uitgelegd wat onder oplichting valt, op welke manier je aangifte kunt doen van online handelsfraude en welke gegevens je daarvoor moet aanleveren. Tevens wordt de mogelijkheid geboden om gebruikersgegevens te controleren en is aangegeven welke voorzorgsmaatregelen genomen kunnen worden om online handelsfraude te voorkomen.

Naast het LMIO geeft Marktplaats op zijn eigen site ook tips tegen internetoplichting. Zo geven zij aan dat het verstandig is de betrouwbaarheid van de verkoper te controleren, verwijzen zij naar websites zoals www.opgelicht.nl en www.opgeletopinternet.nl waar reeds bekende internetoplichters op vermeld staan en bieden zij een test aan met betrekking tot veilig handelen op het internet. Daarnaast verwijst Marktplaats ook expliciet naar het LMIO.

## 3.3 INTERNETOPLICHTING

Op dit moment wordt online handelsfraude berecht aan de hand van oplichting. In de rechtspraak staat online handelsfraude beter bekend als internetoplichting. Volgens de MvT is de berechting van online handelsfraude aan de hand van artikel 326 Sr, het artikel waarin oplichting strafbaar is gesteld, beperkt succesvol.[33] In paragraaf 3.4 wordt aandacht besteed aan deze beperkingen. Artikel 326 lid 1 Sr luidt als volgt:

"*Hij die, met het oogmerk om zich of een ander wederrechtelijk te bevoordelen, hetzij door het aannemen van een valse naam of van een valse hoedanigheid, hetzij door listige kunstgrepen, hetzij door een samenweefsel van verdichtsels, iemand beweegt tot de afgifte van enig goed, tot het verlenen van een dienst, tot het ter beschikking stellen van gegevens, tot het aangaan van een schuld of het teniet doen van een inschuld, wordt, als schuldig aan oplichting, gestraft met een gevangenisstraf van ten hoogste vier jaren of een geldboete van de vijfde categorie*".

Om een goed begrip van het artikel oplichting te krijgen, worden de belangrijkste bestanddelen toegelicht.

### 3.3.1 Oplichtingsmiddelen

Het aannemen van een valse naam of een valse hoedanigheid, het aanwenden van listige kunstgrepen en het gebruik van een samenweefsel van verdichtsels staan bekend als de oplichtingsmiddelen. Oplichting kan pas bewezen worden indien één of meer van deze oplichtingsmiddelen is toegepast om een persoon op te lichten. De Hoge Raad heeft in 2016

[31] www.marktplaats.nl zoek op: *Over Marktplaats.*
[32] www.opgelicht.avrotros.nl zoek op: *Internetoplichting.*
[33] *Kamerstukken II* 2015/16, 34372, 3, p. 73.

een arrest gewezen waarin hij deze oplichtingsmiddelen uitlegt.[34] Het arrest is bedoeld als hulpmiddel bij de beantwoording van vragen over het gebruik van oplichtingsmiddelen in concrete gevallen. De oplichtingsmiddelen zullen los van elkaar toegelicht worden.

*3.3.1.1 Het aannemen van een valse naam of een valse hoedanigheid*
Dit oplichtingsmiddel wordt het meeste gebruikt bij internetoplichting. Wanneer internetoplichting bewezen kan worden, is altijd sprake van dit oplichtingsmiddel. De Hoge Raad legt het oplichtingsmiddel als volgt uit:

*"Het gaat er in de kern om dat het handelen van de verdachte ertoe kan leiden dat bij de ander een onjuiste voorstelling van zaken in het leven wordt geroepen met betrekking tot de 'persoon van de verdachte, hetzij wat betreft diens naam, hetzij wat betreft diens hoedanigheid, waarbij die onjuiste voorstelling van zaken in het leven wordt geroepen teneinde daar misbruik van te maken'."*[35]

Van een valse hoedanigheid kan sprake zijn indien een persoon zich voordoet als bonafide verkoper door bijvoorbeeld een valse naam aan te nemen of valse contactgegevens te gebruiken. Vaak wordt dit ook in combinatie gedaan.[36] Het enkele voordoen als een bonafide verkoper levert niet per direct een valse hoedanigheid op.[37] Hiermee wordt bedoeld dat een persoon zich valselijk voordoet als betrouwbaar verkoper of koper, maar wel zijn eigen contactgegevens en naam gebruikt. In dat geval kan niet gesproken worden van een valse hoedanigheid. Met andere woorden moet een persoon een bepaalde beeldvorming creëren bij een ander, waardoor die ander besluit zaken te doen met die persoon. Een oplichter probeert door het aannemen van een valse naam of valse hoedanigheid vertrouwen te creëren bij personen.

*3.3.1.2 Het aanwenden van listige kunstgrepen*
De Hoge Raad heeft de volgende omschrijving van listige kunstgrepen gegeven:

"*Bedrieglijke handelingen, geschikt om leugenachtige voorwendsels en valse voorstellingen ingang te doen vinden en daaraan kracht bij te zetten."*[38]

Een voorbeeld van een listige kunstgreep is gebruik maken van briefpapier van KPN om daarmee een bank met een valse betaalopdracht te bewegen tot overboeking van een geldbedrag.[39]

*3.3.1.3 Het gebruiken van samenweefsel van verdichtsels*
Bij samenweefsel van verdichtsels kan gedacht worden aan leugens. De Hoge Raad verwoordt het als volgt:

*"Gesproken en/of geschreven uitingen die bij de ander een op meer dan een enkele leugenachtige mededeling gebaseerde onjuiste voorstelling van zaken in het leven kunnen roepen."*[40]

In de meeste gevallen moet sprake zijn van meerdere leugens die elkaar versterken waardoor een beeld van vertrouwen wordt geschetst. Toch kan een enkele leugen ook worden

[34] HR 20 december 2016, ECLI:NL:HR:2016:2889.
[35] HR 20 december 2016, ECLI:NL:HR:2016:2889.
[36] HR 11 november 2014, ECLI:NL:HR:2014:3144.
[37] HR 11 november 2014, ECLI:NL:HR:2014:3144.
HR 9 december 2014, ECLI:NL:HR:2014:3546.
[38] HR 1 november 1920, *NJ* 1920, p. 1215.
[39] HR 20 december 2016, ECLI:NL:HR:2016:2889.
[40] HR 20 december 2016, ECLI:NL:HR:2016:2889.

gekwalificeerd tot een samenweefsel van verdichtsels, indien sprake is van een leugenachtige mededeling van voldoende gewicht in combinatie met bijvoorbeeld een vertrouwensrelatie met de oplichter die reeds bestaat.[41]

### 3.3.2 Schuldverband

Naast oplichtingsmiddelen moet sprake zijn van een schuldverband om (internet)oplichting te kunnen bewijzen. Zo moet het oogmerk gericht zijn op de wederrechtelijke bevoordeling. Het oogmerk veronderstelt opzet op de gedraging waarmee wordt bedrogen. De gedraging wordt verricht aan de hand van één of meer van de oplichtingsmiddelen.[42] Wederrechtelijke bevoordeling houdt in dat een persoon onrechtmatig is bevooroordeeld. Dus een persoon moet bijvoorbeeld geld hebben verkregen terwijl hij daar geen recht op had. Bij internetoplichting verkrijgt de verkoper (de oplichter) geld door een goed aan te bieden, maar niet te leveren na betaling. Op dat moment heeft de verkoper onrechtmatig geld verkregen.

### 3.3.3 Causaliteit

De causaliteit komt tot uitdrukking in de woorden 'iemand bewegen tot'. Er moet sprake zijn van een causaal verband tussen het gebruiken van een oplichtingsmiddel en het resultaat dat is behaald door de inzet van deze oplichtingsmiddelen. De Hoge Raad stelt dat sprake is van een causaal verband:

*"Indien voldoende aannemelijk is dat het slachtoffer mede onder invloed van de door het desbetreffende oplichtingsmiddel in het leven geroepen onjuiste voorstelling van zaken is overgegaan tot de afgifte van enig goed, tot het verlenen van een dienst, tot het ter beschikking stellen van gegevens, tot het aangaan van een schuld of tot het teniet doen van een inschuld."*[43]

Aan de hand van feiten en omstandigheden van het geval kan de rechter oordelen of sprake is van een causaal verband. De Hoge Raad geeft in zijn overzichtsarrest enkele algemene omstandigheden die hieraan kunnen bijdragen: in hoeverre het slachtoffer zelf een idee had moeten krijgen van de oplichting. Dus had het slachtoffer gemakkelijk onderzoek kunnen doen naar de betrouwbaarheid van de persoon waarmee hij of zij handelde. Wanneer op een gemakkelijke manier achterhaald kon worden dat oplichting reëel was, dan kan nooit sprake zijn van oplichting. Bij internetoplichting is dit het geval indien de verkoper op verschillende sites bekend stond als oplichter.[44]

De Hoge Raad heeft hier laatst enkele extra maatstaven voor gegeven. De Hoge Raad stelt dat indien het gebruikelijk is om op vertrouwen een rechtsbetrekking aan te gaan, dat het slachtoffer minder grondig onderzoek hoeft te doen naar de persoon van de verdachte. Onder andere de betrouwbaarheid van de verdachte. Op het moment dat de verdachte zichzelf voordoet als bonafide verkoper of bonafide koper in een situatie waarin op goed vertrouwen gehandeld wordt, dan zal de verdachte al snel als schuldige aangewezen worden.[45]

### 3.3.4 Beoogde doel

Tot slot moet de oplichting gericht zijn op de afgifte van een goed, het verlenen van een dienst, het ter beschikking stellen van gegevens, het aangaan van een schuld of het teniet doen van een inschuld. Indien hier geen sprake van is, kan oplichting niet bewezen worden.

---

[41] HR 20 december 2016, ECLI:NL:HR:2016:2889.
[42] Cleiren, Crijns & Verpalen 2016, p. 1791.
[43] HR 20 december 2016, ECLI:NL:HR:2016:2889.
[44] HR 20 december 2016, ECLI:NL:HR:2016:2889.
[45] HR 18 april 2017, ECLI:NL:HR:2017:718.

### 3.4 KNELPUNTEN BERECHTING INTERNETOPLICHTING

In de MvT wordt aangegeven dat knelpunten bestaan met betrekking tot de vervolging van online handelsfraude aan de hand van oplichting. Volgens de MvT is de jurisprudentie niet eenduidig op dit punt. [46] Zo heeft het gerechtshof Arnhem-Leeuwarden in 2013 geoordeeld dat het niet leveren van een goed aan een koper voldoende is om een valse hoedanigheid aan te nemen. Het gerechtshof vindt dit aan te merken als het aannemen van een valse hoedanigheid, omdat in strijd is gehandeld met het goed vertrouwen dat in het maatschappelijk verkeer gebruikelijk is.[47] In dat geval zou het bewijzen van online handelsfraude aan de hand van oplichting geen probleem zijn. In alle geanalyseerde uitspraken met betrekking tot online handelsfraude, worden goederen niet geleverd. De Hoge Raad heeft anders geoordeeld dan het gerechtshof Arnhem-Leeuwarden. De Hoge Raad is van mening dat het niet leveren van een goed niet zonder meer aangemerkt kan worden als het aannemen van een valse hoedanigheid.

#### 3.4.1 Arresten Hoge Raad

In 2014 heeft de Hoge Raad als volgt geoordeeld:

*"Het Hof heeft met juistheid geoordeeld dat de enkele omstandigheid dat iemand zich in strijd met de waarheid voordoet als bonafide verkoper die in staat en voornemens is de bij hem gekochte en aan hem vooruitbetaalde goederen te leveren, niet oplevert het aannemen van een valse hoedanigheid als bedoeld in artikel 326 Sr."*[48]

Bonafide betekent te goeder trouw. Met andere woorden is het zich enkel voordoen als een betrouwbare verkoper onvoldoende om als het aannemen van een valse hoedanigheid aan te merken. Om het aannemen van een valse hoedanigheid te kunnen bewijzen, zijn bijkomende omstandigheden nodig. In deze zaak die de Hoge Raad behandelde, heeft het gerechtshof geoordeeld dat verdachte meer heeft gedaan dan alleen zichzelf uitgeven als bonafide verkoper. Verdachte heeft tevens gebruik gemaakt foutieve namen en verschillende e-mailadressen. Dit heeft hij gedaan zodat kopers moeilijk in contact kunnen komen met hem. Het gerechtshof acht het aannemen van een valse hoedanigheid bewezen. De Hoge Raad is het met het gerechtshof eens dat deze omstandigheden afdoende zijn om te kunnen spreken van het aannemen van een valse hoedanigheid.

Later dat jaar heeft de Hoge Raad wederom geoordeeld dat het zich voordoen als bonafide verkoper niet kan worden aangemerkt als het aannemen van een valse hoedanigheid.[49] In deze zaak heeft verdachte een webwinkel opgericht. De verdachte heeft zijn bedrijf ingeschreven bij de Kamer van Koophandel. Daarnaast heeft de verdachte zijn eigen naam en contactgegevens gebruikt bij de verkoop van de goederen die op internet door hem zijn aangeboden. Het gerechtshof heeft geoordeeld dat het handelen van verdachte in civielrechtelijke zin aangemerkt kan worden als wanprestatie. Een wanprestatie betekent niet dat dit strafrechtelijk gezien direct oplichting oplevert. Die aanname mag en kan niet gemaakt worden.[50]

### 3.5 ANALYSE JURISPRUDENTIE INTERNETOPLICHTING

Naar aanleiding van bovengenoemde knelpunten is een jurisprudentieonderzoek verricht om te controleren of deze knelpunten in de jurisprudentie waar te nemen zijn. In totaal zijn 108 zaken geanalyseerd. Dit zijn uitspraken van de rechtbank, arresten van het gerechtshof en arresten van de Hoge Raad. Door middel van deze analyse wordt geprobeerd een beeld te geven van de berechting en vervolging van online handelsfraude op dit moment aan de hand

[46] *Kamerstukken II* 2015/16, 34372, 3, p. 73.
[47] Hof Arnhem-Leeuwarden 21 juni 2013, ECLI:NL:GHARL:2013:4498.
[48] HR 11 november 2014, ECLI:NL:HR:2014:3144.
[49] HR 9 december 2014, ECLI:NL:HR:2014:3546.
[50] Hof Amsterdam 2 mei 2012, ECLI:NL:GHAMS:2012:982.

van cijfers. In alle zaken is bekeken of oplichting bewezen kon worden. Indien oplichting bewezen kon worden, is gekeken naar het aantal slachtoffers van onlinehandelsfraude in de betreffende zaak. Deze cijfers zullen aan de hand van afbeeldingen toegelicht worden.

Daarnaast zijn 52 zaken uitgebreider geanalyseerd. In deze zaken is ook gekeken of de verdachte alleen veroordeeld is voor oplichting of voor meerdere delicten. Tot slot zijn in deze zaken de straffen die aan verdachte zijn opgelegd, ingeval van een bewezenverklaring, geïnventariseerd.

### 3.5.1 Bewezenverklaringen

In totaal zijn van de rechtbank en het gerechtshof samen 99 zaken geanalyseerd. Van deze 99 zaken zijn dertien verdachten vrijgesproken. In de overige 86 zaken is oplichting bewezenverklaard.
De rechtbank heeft in de afgelopen jaren 77 zaken behandeld met betrekking tot online handelsfraude. Zeven zaken hebben geleid tot een vrijspraak. In de overige 70 zaken is oplichting wel bewezenverklaard.




Het gerechtshof heeft aanzienlijk minder zaken behandeld. In totaal zijn 22 zaken aan bod gekomen bij het gerechtshof. In zestien zaken is het gerechtshof tot een bewezenverklaring gekomen. De overige zes zaken hebben tot een vrijspraak geleid.

Uit deze analyse kan geconcludeerd worden dat het veroordelen van online handelsfraude aan de hand van oplichting, in tegenstelling tot wat in de MvT wordt beweerd, vrij succesvol is. Slechts in 13% van de behandelde zaken volgde een vrijspraak. Bij de rechtbank volgt zelfs maar in 9% van de zaken een vrijspraak. Wel is een groot verschil te zien met zaken bij het gerechtshof. Bij het gerechtshof volgt in 27% van de zaken een vrijspraak. In hoger beroep gaan als verdachte zijnde, blijkt succesvol te zijn.

Tot slot is geanalyseerd in welke gevallen een vrijspraak volgde. Dus wat was de motivering van de rechtbank of het gerechtshof, indien een verdachte werd vrijgesproken. In de meeste gevallen werd vrijgesproken, omdat de verdachte juiste contactgegevens had gebruikt. In die gevallen kon niet bewezen worden dat de verdachte gebruik had gemaakt van een van de oplichtingsmiddelen. Deze vrijspraken komen overeen met de lijn in de jurisprudentie die de Hoge Raad in 2014 heeft uitgezet. In een van de zaken is een verdachte vrijgesproken, omdat de rechtbank van mening was dat de verdachte niet wist dat zijn bankrekening voor oplichting werd gebruikt. Dit heeft het gerechtshof later bevestigd.[51] Tevens kon in een van de zaken het oorzakelijk verband tussen het aanwenden van het oplichtingsmiddel (de valse naam) en het afgeven van geld niet bewezen worden. Het bewijzen van dit verband is noodzakelijk om van oplichting te kunnen spreken.

[51] Rb. Assen 23 april 2010, ECLI:NL:RBASS:2010:BM2269,
Hof Leeuwarden 29 oktober 2010, ECLI:NL:GHLEE:2010:BO2524.

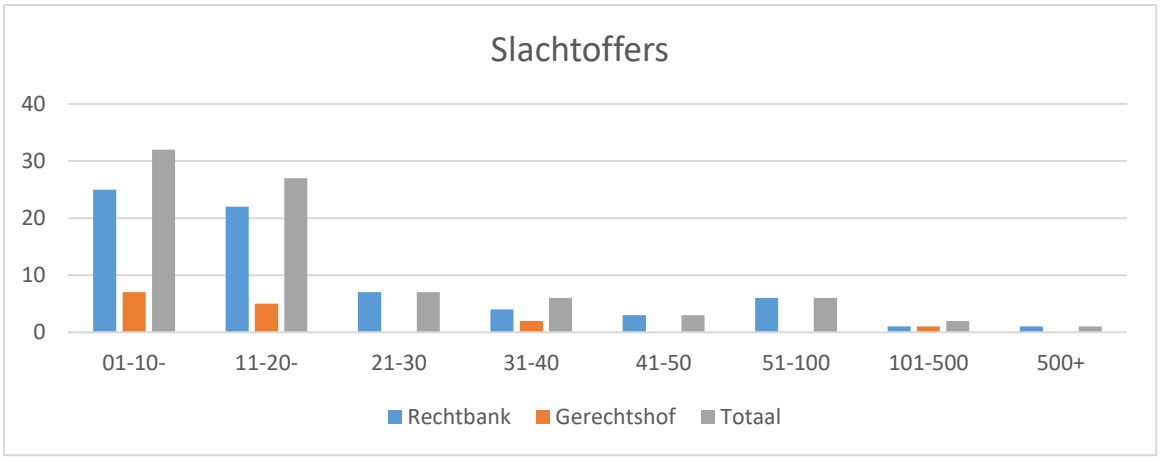
### 3.5.2 Aantal slachtoffers

In 86 zaken is oplichting bewezen. In deze zaken zijn slachtoffers gemaakt. In twee zaken zijn geen concrete cijfers gegeven met betrekking tot het precieze aantal slachtoffers. Daarom worden deze twee zaken niet meegenomen in de statistieken.[52] Opmerking verdient dat het totale aantal slachtoffers vaak moeilijk te bepalen is. Niet iedereen doet aangifte en in sommige gevallen kan oplichting niet bewezen worden. Daarom ligt het daadwerkelijk aantal slachtoffers vele malen hoger dan hier weergegeven.

Het aantal slachtoffers is in verschillende categorieën ingedeeld. De volgende categorieën worden gehanteerd: 1-10, 11-20, 21-30, 31-40, 41-50, 51-100, 101-500 en 500+. Tevens zal, net als bij de cijfers van de bewezenverklaring, een onderverdeling worden gemaakt in rechtbank en gerechtshof. Daarnaast worden ook de cijfers van de rechtbank en het gerechtshof samen weergegeven.

Hieronder is de grafiek weergegeven. Op de horizontale lijn staan bovengenoemde categorieën. Dit zijn het aantal slachtoffers in een bepaalde zaak. Dus stel dat in een zaak 35 slachtoffers zijn gevallen, dan komt deze zaak in de categorie 31-40 te staan. Met de verticale lijn wordt weergegeven hoeveel zaken in de betreffende categorie vallen. In de categorie 1-10 vallen 25 zaken die bij de rechtbank behandeld zijn. Voor concrete aantal slachtoffers in een bepaalde zaak wordt verwezen naar bijlage 2 en 3. In deze bijlagen zijn alle zaken in een tabel opgenomen. In deze tabel staat om welke zaak het gaat, een vrijspraak of bewezenverklaring is gevolgd en het precieze aantal slachtoffers.

Aan de hand van de cijfers kan opgemerkt worden dat in de meeste zaken 1-10 slachtoffers gemaakt worden door de verdachte. Ook in de categorie 11-20 vallen veel zaken. De andere categorieën behelzen beduidend minder zaken. Toch is wel opvallend dat in bepaalde zaken extreem veel slachtoffers vallen, met als meest opmerkelijke een zaak waarin meer dan 500 slachtoffers zijn gevallen. Geconcludeerd kan worden dat online handelsfraude bij uitstek zaken zijn waarin meerdere slachtoffers gemaakt worden.




Verder in deze paragraaf wordt aandacht besteed aan de inhoudelijke analyse van 52 zaken. In deze zaken is ook gekeken naar de opgelegde straf en de delicten waarvoor de verdachte is veroordeeld. In de meeste gevallen is een verdachte voor een combinatie van delicten veroordeeld en niet alleen voor oplichting. Niet alle 52 zaken komen hier apart aan bod. Daarom wordt verwezen naar bijlage 2, waar al deze gegevens per zaak zijn opgenomen in een tabel.

[52] Rb. Groningen 23 februari 2006, ECLI:NL:RBGRO:2006:AV2491,
Hof Amsterdam 06 oktober 2016, ECLI:NL:GHAMS:2016:4390.

### 3.5.3 Opgelegde straf

Bij de rechtbank wordt in 27 van de 42 geanalyseerde zaken een onvoorwaardelijke gevangenisstraf opgelegd. Opmerking verdient hierbij dat in zeventien van deze zaken de verdachte niet enkel voor oplichting is veroordeeld. In vijftien zaken is een voorwaardelijke gevangenisstraf, een taakstraf of een combinatie van een voorwaardelijke gevangenisstraf en taakstraf opgelegd. In een zaak waarin de verdachte 206 mensen heeft opgelicht, is door de rechtbank een gevangenisstraf van 36 maanden, waarvan 12 maanden voorwaardelijk, opgelegd.[53] Dit is de hoogste straf die door de rechtbank is opgelegd.
Het gerechtshof heeft in zaken waarin oplichting bewezen is verklaard een onvoorwaardelijke of voorwaardelijke gevangenisstraf opgelegd. Indien een voorwaardelijke gevangenisstraf is opgelegd, heeft het gerechtshof daarnaast ook een taakstraf opgelegd.

Het OM heeft richtlijnen voor de strafvordering van internetoplichting op internet gepubliceerd. Deze richtlijn is als een tabel opgenomen in bijlage 5. Daarom wordt voor deze richtlijnen verwezen naar deze bijlage.

Uit deze gegevens kan de conclusie getrokken worden dat online handelsfraude vrij zwaar wordt bestraft. Uit artikel 326 Sr volgt natuurlijk dat maximaal een gevangenisstraf van vier jaren opgelegd kan worden. Dit is in geen van de gevallen gedaan. Toch wordt in de overgrote meerderheid van de zaken wel een onvoorwaardelijke gevangenisstraf opgelegd. Hiermee wordt een duidelijk signaal afgegeven dat online handelsfraude als een serieus delict wordt gezien.

### 3.5.4 Veroordeelde delicten

In 21 van de 52 geanalyseerde zaken is de verdachte niet alleen voor oplichting veroordeeld. In de meeste gevallen wordt oplichting in combinatie met witwassen en valsheid in geschrifte gepleegd. In een van de zaken heeft de verdachte oplichting gepleegd met een andere identiteit. De verdachte is in die zaak veroordeeld voor oplichting en identiteitsfraude.[54] In de andere zaken staan de delicten los van de oplichting. Hier gaat het bijvoorbeeld om diefstal, bedreiging met geweld of vernieling. In bijlage 2 staat een precieze beschrijving gegeven van de delicten waarvoor een verdachte in een zaak is veroordeeld.
Wat daarnaast opvalt is dat in veel zaken de verdachte zijn veroordeeld voor het medeplegen van oplichting.

In de volgende paragraaf komt de nieuwe strafbaarstelling aan bod. Er wordt bekeken wat anders is ten opzichte van het wetsartikel oplichting. Daarnaast wordt bekeken of de nieuwe strafbaarstelling voordelen oplevert of juist aandachtspunten met zich mee brengt.

## 3.6 NIEUWE STRAFBAARSTELLING

Zoals eerder beschreven wordt met het invoeren van het wetsvoorstel Computercriminaliteit III de nieuwe strafbaarstelling voor online handelsfraude geïntroduceerd. De MvT stelt dat de mogelijkheid om strafrechtelijk op te treden tegen malafide verkopers of aanbieders die zich met herhaling schuldig maken aan online handelsfraude niet goed mogelijk is.[55] Vooral het stukje met herhaling valt op in die zin. Hiermee willen ze de nieuwe strafbaarstelling ongeveer hetzelfde maken als flessentrekkerij uit artikel 326a Sr. Flessentrekkerij is het herhaaldelijk kopen van goederen of diensten zonder deze goederen of diensten te betalen.[56] Met het instellen van de nieuwe strafbaarstelling wordt gepoogd om het OM in staat te stellen om vormen van grootschalige handelsfraude te vervolgen.[57] Met handelsfraude wordt waarschijnlijk online handelsfraude bedoeld. Het is niet duidelijk wat wordt verstaan onder

[53] Rb. Zeeland-West-Brabant 16 oktober 2014, ECLI:NL:RBZWB:2014:7103.
[54] Rb. Midden-Nederland 24 februari 2017, ECLI:NL:RBMNE:2017:904.
[55] *Kamerstukken II* 2015/16, 34372, 3, p. 75.
[56] Cleiren, Crijns & Verpalen 2016, p. 1795.
[57] *Kamerstukken II* 2015/16, 34372, 3, p. 75.

grootschalig. Hier wordt verder niet op ingegaan. Het is natuurlijk de vraag of het plegen van online handelsfraude bij bijvoorbeeld twee personen onder grootschalige handelsfraude gecategoriseerd kan worden. De nieuwe strafbaarstelling zal in het WvSr worden opgenomen onder artikel 326d Sr:

*"Hij die een beroep op gewoonte maakt van het door middel van een geautomatiseerd werk verkopen van goederen of verlenen van diensten tegen betaling met het oogmerk om zonder volledige levering zich of een ander van de betaling van die goederen of diensten te verzekeren, wordt gestraft met gevangenisstraf van ten hoogste vier jaren of geldboete van de vijfde categorie."*[58]

De tekst uit artikel 326d Sr verschilt op veel punten van de tekst uit artikel 326 Sr. Zo wordt niet meer gesproken over de oplichtingsmiddelen van het aannemen van een valse naam of hoedanigheid, een samenweefsel van verdichtsels en listige kunstgrepen. Met andere woorden hoeft voor online handelsfraude in de toekomst niet bewezen te worden dat gebruik is gemaakt van een oplichtingsmiddel. Tevens is in artikel 326d Sr bepaald dat sprake moet zijn van een beroep of een gewoonte. Dit was voor oplichting niet noodzakelijk. De maximale straf die kan worden opgelegd is wel hetzelfde als de maximale straf die voor oplichting geldt.

### 3.6.1 Bestanddelen

De belangrijkste bestanddelen die uit artikel 326d Sr gehaald kunnen worden, zijn de volgende: 'beroep of gewoonte maken', 'door middel van een geautomatiseerd werk verkopen', 'goederen of diensten', 'oogmerk', 'zonder volledige levering' en 'verzekeren van betaling van die goederen of diensten'.
De bestanddelen 'beroep of gewoonte maken', 'door middel van een geautomatiseerd werk verkopen' en 'het oogmerk' zullen apart behandeld worden. De overige bestanddelen zijn vanzelfsprekend en hebben geen uitleg nodig.

#### *3.6.1.1 Flessentrekkerij*

Voordat de bestanddelen inhoudelijk behandeld worden, is het van belang het artikel van flessentrekkerij aan te stippen. Flessentrekkerij is opgenomen in artikel 326a Sr en toont veel gelijkenis met de nieuw voorgestelde strafbaarstelling van online handelsfraude. Omdat flessentrekkerij net als de strafbaarstelling van online handelsfraude de bestanddelen 'beroep of gewoonte maken' en 'oogmerk' kent, wordt daarom Tekst & Commentaar en jurisprudentie met betrekking tot flessentrekkerij geraadpleegd. Op die manier kan een goed beeld verkregen worden voor de invulling van deze bestanddelen. Wat de rechter in de toekomst voor invulling gaat geven aan de bestanddelen uit het artikel van onlinehandelsfraude is niet zeker.

#### *3.6.1.2 Beroep of gewoonte maken*

In de MvT wordt niet uitgelegd wat onder 'een beroep of gewoonte maken' wordt verstaan. Daarom zal informatie met betrekking tot flessentrekkerij geraadpleegd worden. Voor het bewijzen van flessentrekkerij is namelijk nodig dat sprake is van 'een beroep of een gewoonte'. In de Memorie van Antwoord (hierna: MvA) met betrekking tot het artikel van flessentrekkerij wordt bepaald dat 'een gewoonte maakt' een meervoud van handelingen vereist. Tussen deze meervoud van handelingen moet een verband bestaan.[59] Meer specifiek wordt met 'gewoonte' een pluraliteit van feiten bedoeld. Deze feiten volgen elkaar niet toevallig op, maar vertonen wat betreft de feiten een onderling een verband. Daarnaast kan het verband ook afgeleid worden uit de psychische gerichtheid van de dader. Hij of zij moet steeds de neiging hebben om online handelsfraude te plegen.[60] Bij 'een beroep' hoeft niet sprake te zijn van meer dan één handeling. 'Een beroep' kan ook volgen uit de verklaring dat iemand een beroep

[58] *Kamerstukken II* 2015/16, 34372, 2, p. 3.
[59] Cleiren, Crijns & Verpalen 2016, p. 1796.
[60] Cleiren, Crijns & Verpalen 2016, p. 1495-1497.

uitoefent.[61] De Hoge Raad heeft bepaald dat bij een bewezenverklaring niet gekozen hoeft te worden tussen beroep of gewoonte maken, omdat dit niet belangrijk is voor een strafrechtelijke betekenis van de bewezenverklaring.[62]

Om een beeld te krijgen wanneer sprake is van 'een gewoonte', zijn uitspraken van de rechtbank en arresten van het gerechtshof betreffende flessentrekkerij geanalyseerd. Dit zijn allemaal uitspraken of arresten uit de jaren 2013 tot en met 2016. Bij de betreffende uitspraken/arresten is gekeken naar het aantal slachtoffers dat is gemaakt, de verdediging die gevoerd is en of een vrijspraak of bewezenverklaring is gevolgd. Op die manier is geprobeerd te analyseren of een sprake moet zijn van een bepaald aantal slachtoffers voordat gesproken kan worden van een 'gewoonte maken'.
Uit de analyse volgt dat al snel gesproken kan worden van een gewoonte. De rechtbank heeft in twee gevallen een verdachte veroordeeld voor flessentrekkerij in een zaak waarin twee slachtoffers waren gemaakt. In een van de zaken is geen nadere motivering gegeven waarom de rechtbank het maken van twee slachtoffers als 'een beroep of gewoonte' ziet.[63] In de andere zaak stelde de rechtbank dat de Hoge Raad heeft bepaald dat het bestanddeel een beroep of gewoonte maken bewezen kan worden indien sprake is van een meervoud van handelingen waartussen een verband bestaat. Dit verband is aanwezig in het geval dat de verdachte bij verschillende slachtoffers op eenzelfde manier te werk is gegaan.[64] Het gerechtshof heeft in een van de arresten bepaald dat de verdachte veroordeeld wordt voor flessentrekkerij bij twee personen, nu uit de justitiële documentatie van verdachte blijkt dat hij vaker op eenzelfde manier tewerk is gegaan. Daarom stelt het gerechtshof dat in deze zaak sprake is van een van pluraliteit van handelingen gevormde en voortgezette gewoonte.[65] Het is de vraag of de verdachte ook veroordeeld zou zijn als uit zijn justitiële documentatie bleek dat hij niet eerder voor flessentrekkerij was veroordeeld. In dat geval zou namelijk geen sprake zijn van een door de pluraliteit van handeling gevormde en voortgezette gewoonte. Uit de analyse blijkt verder dat drie of vier gevallen van flessentrekkerij voldoende is om te spreken van een gewoonte. De rechtbank Amsterdam heeft wel een verdachte vrijgesproken die verdacht werd van flessentrekkerij. De rechtbank stelde dat geen sprake is van een beroep of gewoonte omdat het feit in een te kort tijdsbestek heeft plaatsgevonden. De flessentrekkerij zou hebben plaatsgevonden op een vlucht van Amsterdam naar Ibiza.[66] Voor de volledige analyse wordt verwezen naar bijlage 4.

#### *3.6.1.3 Door middel van een geautomatiseerd werk verkopen*

Het is van belang te weten wat onder een geautomatiseerd werk wordt verstaan. In het wetsvoorstel Computercriminaliteit III is een nieuwe beschrijving van het geautomatiseerd werk opgenomen in artikel 80sexies Sr. Aangezien beide bepalingen in het WvSr worden opgenomen na inwerkingtreding van het wetsvoorstel, wordt daarom de nieuwe beschrijving van geautomatiseerde werken gehanteerd. Deze is als volgt:

*"Onder geautomatiseerd werk wordt verstaan een apparaat of groep van onderling verbonden samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerken."*[67]

Hieronder vallen natuurlijk vaste computers of laptops, maar een smartphone en tablet kan ook aangemerkt worden als een geautomatiseerd werk. Met andere woorden is het aanbieden van goederen en diensten via een krant en deze niet leveren, niet aan te merken als online

[61] Cleiren, Crijns & Verpalen 2016, p. 1796.
[62] HR 6 januari 1998, *NJ* 1998, 423.
[63] Rb. Noord-Nederland 3 maart 2015, ECLI:NL:RBNNE:2015:897.
[64] Rb. Limburg 7 juli 2015, ECLI:NL:RBLIM:2015:6353.
[65] Hof 's-Hertogenbosch 18 februari 2013, ECLI:NL:GHSHE:2013:BZ2652.
[66] Rb. Amsterdam 1 september 2014, ECLI:NL:RBAMS:2014:5735.
[67] *Kamerstukken II* 2015/16, 34372, 2, p. 2.

handelsfraude. Simpelweg omdat een krant niet aan te merken is als een geautomatiseerd werk. Over grensgevallen is nog geen duidelijkheid. Dit komt omdat de nieuw voorgestelde bepaling met betrekking tot geautomatiseerde werken verschillend is van de oude definitie betreffende geautomatiseerd werk die is opgenomen in het WvSr. Voor de definitie van geautomatiseerde werken die nu geldt, wordt verwezen naar paragraaf 2.2.

#### *3.6.1.4 Oogmerk*

Het oogmerk moet gericht zijn op het verkrijgen van geld voor goederen of diensten zonder dat die goederen of diensten geleverd worden.
De Hoge Raad heeft bij flessentrekkerij bepaald dat het oogmerk op niet- of niet-volledige betaling niet reeds aanwezig hoeft te zijn op het moment van de aankoop. Het niet-betalen en het vaststellen dat verdachte op verschillende tijdstippen goederen heeft gekocht, is voldoende om het oogmerk uit af te leiden. Het betalen van goederen op het moment dat een strafoplegging dreigt, zorgt er niet voor dat het oogmerk verdwijnt.[68] Waarschijnlijk gaat deze bepaling ook voor het artikel van online handelsfraude gelden. In dat geval hoeft het oogmerk om niet te leveren niet aanwezig te zijn op het moment dat het goed verkocht wordt. Door het wel leveren van een goed of dienst op het moment dat een straf dreigt, wordt de straf niet voorkomen.

Uit de jurisprudentie-analyse komt naar voren dat de meeste advocaten verweer voeren op het ontbreken van het oogmerk. De advocaat geeft in dat geval aan dat de verdachte het verschuldigde bedrag nog wilde betalen. In de meeste gevallen heeft de rechtbank of het gerechtshof dit verweer verworpen. In één zaak is de rechtbank meegegaan met het verweer van de raadsvrouw. De raadsvrouw voerde aan dat het oogmerk ontbrak, aangezien de verdachte in dienst van medeverdachte handelde. Verdachte wist niet dat medeverdachte nimmer de bedoeling heeft gehad om te betalen voor de goederen. De rechtbank stelt dat uit de bewijsmiddelen niet blijkt dat verdachte wist dat het de bedoeling was om niet te betalen voor de goederen. Daarom ontbreekt bij de verdacht het oogmerk op het niet betalen van de bestelde goederen.[69]

### 3.7 INTERVIEWS

In deze paragraaf wordt de mening, met betrekking tot online handelsfraude, van twee experts op het gebied van computercriminaliteit gegeven. Eerst komt de mening van de heer mr. Hersmus[70] aan bod. Daarna zal de mening van de heer mr. Kuijer[71] behandeld worden.

#### 3.7.1 Interview de heer mr. Hersmus[72]

De heer Hersmus stelt voorop dat oplichting in het WvSr terecht is gekomen op het moment dat er nog geen computers bestonden. Mensen konden op dat moment ook nog niet op afstand met elkaar handel drijven, daar had de wetgever niet in voorzien. Oplichting is nooit specifiek voor Marktplaatsfraude geschreven. Dat is een probleem. Daarnaast mag het volgens de heer Hersmus niet zo zijn dat elke civielrechtelijke wanprestatie in het strafrecht getrokken wordt. Dat gevaar is op dit moment wel aanwezig. Bij Marktplaatsfraude is vooral het probleem dat slachtoffers niet de mogelijkheid hebben om de tegenpartij civielrechtelijk aan te spreken, omdat je niet weet wie de tegenpartij is. In de meeste gevallen zijn geen bruikbare gegevens. In het geval dat er wel gegevens zijn, is de kans groot dat niet op een contactverzoek gereageerd wordt. Op dat moment wordt aangifte gedaan in de hoop op die manier het geld terug te krijgen.

---

[68] Cleiren, Crijns & Verpalen 2016, p. 1796.
[69] Rb. Noord-Nederland 16 februari 2017, ECLI:NL:RBNNE:2017:565.
[70] De heer Hersmus is parket-secretaris bij het OM in 's-Hertogenbosch. De heer Hersmus heeft als portefeuille cybercrime.
[71] De heer Kuijer is raadsheer bij het gerechtshof te 's-Gravenhage. Tevens is de heer Kuijer lid van het Kenniscentrum Cybercriminaliteit van het gerechtshof 's-Gravenhage.
[72] Het volledige interview met de heer Hersmus is bijgevoegd in bijlage 6.

De nieuwe strafbaarstelling is volgens de heer Hersmus het tegenovergestelde van flessentrekkerij. Hij vindt het goed dat een aparte strafbaarstelling wordt geïntroduceerd. Volgens hem wordt bewijstechnisch een gat gedicht met de invoering van online handelsfraude. Het is namelijk lastig om online handelsfraude te vervolgen aan de hand van oplichting. Vooral indien een persoon online handelsfraude pleegt met zijn eigen contactgegevens. In dat geval kan deze persoon niet voor oplichting vervolgd worden, omdat geen gebruik is gemaakt van een oplichtingsmiddel. Ook al doet de verdachte dit bijvoorbeeld dertig keer. De nieuwe strafbaarstelling zal deze personen wel kunnen bestraffen.

Tevens stelt de heer Hersmus dat het strafrechtelijk onderzoek naar online handelsfraude aan de hand van de nieuwe strafbaarstelling wellicht sneller kan gaan. Indien bewezen kan worden dat een persoon tien advertenties op Marktplaats heeft geplaatst, van die tien advertenties dat meerdere mensen geld hebben aangeboden en de verdachte dit geld heeft aangenomen, dan kan de verdachte aan de hand van de nieuwe strafbaarstelling al veroordeeld worden. Simpelweg omdat de verdachte meerdere biedingen op een advertentie accepteert. De verdachte kan die goederen nooit aan iedereen leveren. Bewijstechnisch is dat makkelijker dan bewijzen dat sprake is van een van de oplichtingsmiddelen.

Concluderend vindt de heer Hersmus de invoering van de nieuwe strafbaarstelling een positieve ontwikkeling. Vooral met betrekking tot het bewijstechnisch aspect.

### 3.7.2 Interview de heer mr. Kuijer[73]

De heer Kuijer duidt online handelsfraude aan als Marktplaatsfraude. Hij geeft aan dat Marktplaatsfraude een delict is dat de laatste vijf jaar in opkomst is. Daarvoor bestond Marktplaatsfraude ook, maar werd er geen werk van gemaakt. Door middel van het instellen van het LMIO is de politie dit centraal gaan aanpakken, waardoor meer zaken vervolgd kunnen worden.

De heer Kuijer heeft zelf ook zaken met betrekking tot online handelsfraude berecht.[74] Hij geeft aan dat in de jurisprudentie twee scholen waar te nemen zijn. De eerste school is vooral formalistisch. Zij vinden dat van oplichting gesproken kan worden, indien je door middel van oplichtingsmiddelen bewogen wordt tot een handeling die je normaal gesproken niet zou hebben gedaan. Alleen op een knop drukken omdat iemand iets te koop aanbiedt, geldt niet als ‘bewogen tot’. Zij vinden dat je in dat geval zelf beter moet opletten. De tweede school, waar de heer Kuijer zelf bij hoort, is van mening dat de hele internetontwikkeling als een zelfstandig iets gezien moet worden. Deze school kijkt veel meer naar het totale plaatje. Het gebruiken van valse btw-nummers of het voordoen als een bonafide bedrijf met een vals keurmerk wordt in dat geval ook als oplichtingsmiddel gezien. Oplichting kan dan gewoon bewezen worden. Volgens de heer Kuijer is het gerechtshof in ’s-Hertogenbosch hier mede leidend in geweest.
De heer Kuijer neemt zelf waar dat de laatste school de afgelopen twee/tweeëneenhalf jaar aan de winnende hand is. Er wordt minder formalistisch gekeken en meer naar de feiten en omstandigheden. De heer Kuijer is van mening dat de wetgever wat dat betreft wel een beetje ‘mosterd na de maaltijd’ is. Tegenwoordig worden zowel de oplichtingsmiddelen als het ‘bewegen tot’ ruimer uitgelegd door de rechtspraak dan vijf jaar geleden. Wat betreft de bewezenverklaring is het op dat punt minder prangend om een nieuwe strafbaarstelling in te voeren. De wetgever gaat online handelsfraude nu gewoon generiek strafbaar stellen, zonder dat ingewikkelde discussies ontstaan welke oplichtingsmiddelen zijn gebruikt en waaruit blijkt dat iemand heeft ‘bewogen tot’. Die nieuwe wet zal het bewijzen van online handelsfraude voor een deel makkelijker maken. Dat de wetgever nu een nieuwe strafbaarstelling wil invoeren

[73] Het volledige interview met de heer Kuijer is bijgevoegd in bijlage 7.
[74] Hof Den Haag 16 april 2014, ECLI:NL:GHDHA:2014:1640; Hof Den Haag 16 april 2014, ECLI:NL:GHDHA:2014:1647; Hof Den Haag 17 november 2015, ECLI:NL:GHDHA:2015:3256.

die een beetje ‘mosterd na de maaltijd is’, betekent niet dat de heer Kuijper de nieuwe strafbaarstelling overbodig vindt. Hij stelt dat de Hoge Raad voor hetzelfde geld kan besluiten dat de verantwoordelijkheid bij de kopers ligt en dat zij zelf beter moeten opletten. In dat geval zou online handelsfraude niet goed aan de hand van oplichting bewezen kunnen worden.

Volgens de heer Kuijer is het verschil tussen de twee strafbaarstellingen (nieuwe strafbaarstelling en oplichting) dat bij oplichting iemand ‘bewogen tot’ moest worden en bij de nieuwe strafbaarstelling dat een verdachte heel vaak iets aangeboden en niet geleverd heeft. Dat is een ander perspectief op de zaak en brengt een andere eis voor de bewijsvoering met zich mee. Met de nieuwe strafbaarstelling kunnen de zaken wellicht wat sneller door het systeem gaan.

Het probleem met betrekking tot de huidige strafbaarstelling is de feitelijke bewijsvoering. Het is vaak niet moeilijk om de gegevens terug te geleiden tot een plek, een IP-adres of een server. In het strafrecht gaat het alleen niet om apparaten of gegevens. Het gaat om personen. Het opsporen van de persoon die de advertentie heeft geplaatst is vaak moeilijk. Daarnaast is de persoon die het geld op de rekening gestort krijgt en collecteert, vaak niet dezelfde persoon als degene die de advertentie heeft geplaatst. Dat zijn vaak losse samenwerkingsverbanden. Dat probleem blijft, ook na invoering van de nieuwe strafbaarstelling. Het wordt ook steeds lastiger om de identiteit van een persoon te ontdekken, omdat de verdachten beter worden in het verbergen van hun identiteit.

De heer Kuijper is van mening dat Marktplaats en de consumenten zelf ook een bijdrage kunnen leveren om online handelsfraude tegen te gaan of te voorkomen. Marktplaats kan bijvoorbeeld algoritmes gebruiken waarmee oplichters makkelijker opgespoord kunnen worden. Er zijn technieken, algoritmes waarmee gescreend kan worden wie wat aanbiedt en waarmee bijgehouden kan worden welke personen, IP-adressen of device nummers al vaker naar boven zijn gekomen. Op die manier kan Marktplaats zelf achterhalen wie oplichters zijn en deze data verstrekken aan het OM. Consumenten zelf zouden beter op kunnen letten of een aangeboden goed of dienst te mooi is om waar te zijn. In dat geval is het niet verstandig om tot een aankoop over te gaan. In sommige gevallen helpt opletten niet. Soms zijn oplichters erg doortrapt en creëren ze nepsites die veel lijken op echte sites. Als mensen daarin trappen, dan is dit volstrekt begrijpelijk.

Tevens ziet de heer Kuijper de geringe affiniteit van de rechters met het onderwerp als een probleem. De heer Kuijper is onderdeel van het Kenniscentrum Cybercrime. Zij proberen, mede op het gebied van online handelsfraude, jurisprudentie en de gedachte te verzamelen, informatie uit de wetsgeschiedenis te duiden en vergelijkingsmateriaal uit andere oplichtingsvelden te verzamelen om op deze manier rechters hierover te informeren. Rechters worden ook geïnformeerd aan de hand van voorlichtingen.

De nieuwe strafbaarstelling heeft volgens de heer Kuijper zeker zijn voordelen. Wanneer veel mensen aangifte doen dat zij een goed hebben betaald dat nooit geleverd is, dan heeft de verdachte al een bewijsvermoeden tegen. Als de verdachte op dat moment geen uitleg geeft, dan mag de rechter daaruit de conclusie trekken dat dit opzettelijk voortdurend is gedaan. Wat wel kan is dat de verdachte op zo’n moment zegt dat hij wel wilde leveren, maar dat de leverancier in gebreke bleef. Op dat moment is de vraag aanwezig of iemand opzet heeft op het niet leveren van goederen. Dat moet dan nog bewezen worden.

Toch blijven er volgens de heer Kuijper problemen bestaan die aan de hand van voorlichting en het invoeren van een nieuwe strafbaarstelling niet kunnen worden opgelost. Omdat steeds meer losse samenwerkingsverbanden bestaan, wordt het lastiger om medeplegen of medeplichtigheid van online handelsfraude te bewijzen. Vooral als iemand een advertentie plaatst voor een ander zonder dat deze persoon wist dat deze advertentie voor online handelsfraude is bedoeld. Dit geldt ook indien een persoon het geld ophaalt van de voldane

trasactie, maar zich niet bewust is van het feit dat dit geld afkomstig is van online handelsfraude. De heer Kuijper stelt dat de samenleving steeds horizontaler wordt en dat de verticale juridische begrippen zoals medeplegen en medeplichtigheid daar niet veel tegen kunnen doen. Tevens blijft de bewijsvoering, zoals eerder vermeldt, met betrekking tot de verdachte een probleem. Vooral het verband maken tussen de handelingen die zijn gepleegd en de betreffende verdachte is problematisch. Deze handelingen moeten gekoppeld kunnen worden aan de verdachte. Lukt dit niet, dan zal online handelsfraude nooit bewezen kunnen worden. Vaak zijn er een heleboel omstandigheden die een persoon verdacht maakt, maar het harde bewijs is niet gemakkelijk te leveren.

Concluderend kan gesteld worden dat de heer Kuijper positief tegen de nieuwe strafbaarstelling aankijkt, maar dat deze nieuwe strafbaarstelling een aantal grote problemen niet kan oplossen. Onder andere het koppelen van de persoon van de verdachte aan de handelingen die zijn gepleegd en de losse samenwerkingsverbanden blijven een probleem.

## 3.8 AANDACHTSPUNTEN

In deze paragraaf worden de aandachtpunten gegeven die van belang zijn in toekomstige procedures

### 3.8.1 *Beroep of gewoonte maken*

#### *3.8.1.1 Aantal gemaakte slachtoffers*

Uit de MvA met betrekking tot het artikel van flessentrekkerij volgt dat ‘een gewoonte maken’ een meervoud van handelingen vereist. Meer specifiek moet sprake zijn van een pluraliteit van handelingen. Tussen deze handelingen moet een onderling verband bestaan. Daarentegen hoeft bij ‘een beroep’ niet sprake te zijn van meerdere handelingen, maar kan het feit dat iemand verklaart dat hij een beroep beoefent voldoende zijn om te kunnen spreken van ‘een beroep’. Bij de opbouw van een verweer met betrekking tot ‘een gewoonte maken’ is het daarom van belang aan te geven dat sprake moet zijn van een pluraliteit van handelingen waartussen een onderling verband bestaat. Indien een verdachte twee slachtoffers maakt, is het de vraag of dit is aan te merken als een pluraliteit van handelingen. Daarnaast moet blijken dat tussen de handelingen een onderling verband bestaat. Uit de jurisprudentie-analyse betreffende flessentrekkerij volgt dat de rechtbank en het gerechtshof al snel aannemen dat voldaan is aan ‘een beroep of gewoonte maken’. Dit hebben zij onder meer gedaan in zaken waarin een verdachte zich twee keer schuldig heeft gemaakt aan het bestellen en ontvangen van goederen, maar de rekening van deze goederen nimmer hebben betaald.
Aan de hand van de jurisprudentie-analyse kan gesteld worden dat verweren waarin wordt aangevoerd dat niet gesproken kan worden van ‘een gewoonte of beroep maken’ omdat geen sprake is van herhaaldelijke handelingen, dit tot nu toe niet succesvol is gebleken. Dit betekent echter niet dat een verweer voeren op dit punt geen zin heeft. In het geval dat sprake is van twee of drie slachtoffers zou het een discutabel punt kunnen zijn of sprake is van ‘een beroep of gewoonte maken’. Daarnaast is nog niet duidelijkheid hoe de rechter gaat oordelen in zaken met betrekking tot online handelsfraude. Daarom is het verstandig hierop een verweer te voeren.

#### *3.8.1.2 Tijdsbestek*

Wellicht is het mogelijk om het volgende punt aan te stippen in een verdediging. De rechtbank heeft een verdachte vrijgesproken van flessentrekkerij, omdat geen sprake is van een gewoonte nu het feit ziet op een kort tijdsbestek. Dit tijdsbestek is een vlucht van Amsterdam naar Ibiza geweest. Een vlucht van Amsterdam naar Ibiza duurt ongeveer twee uur en een kwartier.[75] De verdachte heeft in het vliegtuig meerdere drankjes genuttigd zonder te betalen.[76]
In een rechtszaak met betrekking tot online handelsfraude zou aangevoerd kunnen worden dat geen sprake is van een gewoonte maken indien de verdachte bijvoorbeeld in een kort

[75] www.royalibiza.nl zoek op: *reistijd Ibiza*.
[76] Rb. Amsterdam 1 september 2014, ECLI:NL:RBAMS:2014:5735

tijdsbestek zich schuldig heeft gemaakt aan het verkopen van een goed en het niet leveren van dat goed. Stel dat de verdachte in een aantal uren meerdere goederen heeft verkocht, zou in dat geval ook sprake kunnen zijn van een kort tijdsbestek. Het is de vraag of de rechter op dat moment van mening is dat voldaan is 'een gewoonte of beroep maken'.

### *3.8.2 Oogmerk*

Zoals in paragraaf 3.6.1.4 beschreven staat, moet het oogmerk gericht zijn op het verkrijgen van geld voor goederen of diensten zonder deze goederen of diensten te leveren aan de koper. Met betrekking tot flessentrekkerij heeft de Hoge Raad bepaald dat het oogmerk op niet- of niet-volledige betaling niet reeds aanwezig hoeft te zijn op het moment van de aankoop van de goederen. Uit de jurisprudentie-analyse betreffende flessentrekkerij heeft de rechtbank dit jaar een verdachte vrijgesproken van flessentrekkerij, omdat deze verdachte niet het oogmerk heeft gehad op het niet betalen van gekochte goederen. Deze verdachte werkte in dienst van medeverdachte. De medeverdachte had daarentegen wel het oogmerk op het niet betalen van goederen.[77] Uit de jurisprudentie-analyse met betrekking tot internetoplichting is gebleken dat een samenwerking tussen personen steeds vaker voorkomt. Zo zijn er meerdere zaken waarin een persoon alleen het geld dat verkregen wordt door internetoplichting uit de pinautomaat gaat halen. Het is de vraag of bij deze personen altijd sprake is van een oogmerk gericht op het verkrijgen van geld zonder de bestelde goederen of diensten te leveren. De advocaat kan in dat geval het verweer voeren dat bij de verdachte het oogmerk ontbreekt, omdat de verdachte niet wist dat het geld verkregen is door middel van het plegen van online handelsfraude.

In meerdere zaken betreffende flessentrekkerij is verweer gevoerd op 'het oogmerk' of 'een gewoonte of beroep maken'. Deze verweren zijn in de meeste situaties niet succesvol gebleken. Het feit dat deze verweren niet gegrond zijn verklaard, betekent niet automatisch dat het niet zinvol is op deze punten verweer te voeren. In de toekomst gaat het namelijk over een nieuwe strafbaarstelling waar nog geen jurisprudentie voor is. Het berechten van online handelsfraude aan de hand van oplichting is wezenlijk anders dan het berechten van online handelsfraude aan de hand van de nieuwe strafbaarstelling. Als advocaat zijnde is het natuurlijk altijd belangrijk goed naar de feiten en omstandigheden van de betreffende zaak te kijken. Aan de hand daarvan kan een goed opgebouwd en onderbouwd verweer opgesteld worden. Vooral in de zaken waarin weinig slachtoffers zijn gemaakt, bijvoorbeeld twee of drie, is het belangrijk om te controleren of gesproken kan worden van een pluraliteit van handelingen met een onderling verband. Verweren betreffende 'het oogmerk' zijn succesvoller gebleken. Dit blijkt uit de jurisprudentie-analyse betreffende vrijspraken voor flessentrekkerij. In bijlage 4 staat precies in welke zaak een vrijspraak is gevolgd en wat voor een verweer is gevoerd.

### 3.8.3 *Geautomatiseerd werk*

Online handelsfraude kan alleen bewezen worden als de goederen of diensten verkocht zijn door middel van een geautomatiseerd werk. In elke zaak moet dus gecontroleerd worden of dit het geval is geweest.
Op dit moment worden onder andere computers, laptops, netwerken van aan elkaar verbonden computers, geautomatiseerde inrichtingen voor telecommunicatie en een harde schijf als geautomatiseerd werk aangemerkt als een geautomatiseerd werk.[78] De MvT bij het wetsvoorstel Computercriminaliteit, het eerste wetsvoorstel, geeft aan dat werken die alleen gegevens opslaan of werken die functioneren zonder interactie met hun omgeving niet aangemerkt kunnen worden als een geautomatiseerd werk. Hieronder valt onder andere een elektronisch klokje.[79] Daarnaast is in de MvT bij het wetsvoorstel Computercriminaliteit II

[77] Rb. Noord-Nederland 16 februari 2017, ECLI:NL:RBNNE:2017:565.
[78] *Kamerstukken II* 1989/90, 21551, 3, p. 6.
*Kamerstukken II* 1998/99, 26671, 3, p. 33.
[79] *Kamerstukken II* 1989/90, 21551, 3, p. 6.

bepaald dat een eenvoudig telefoontoestel en bepaalde zend- en ontvanginrichtingen geen geautomatiseerde werken zijn.[80] Uit het huidige artikel 80sexies volgt namelijk dat een inrichting gegevens moet opslaan, verwerken en overdragen. Indien de inrichting alleen gegevens opslaat of gegevens overdraagt, kan niet gesproken worden van een geautomatiseerd werk.[81]
Nu de definitie van een geautomatiseerd werk na inwerkingtreding van het nieuwe wetsvoorstel zal wijzigen, is niet duidelijk wat precies onder een geautomatiseerd werk valt. Zijn de inrichtingen die hierboven zijn genoemd nu wel als een geautomatiseerd werk aan te merken? Het is de vraag of een eenvoudig telefoontoestel computergegevens verwerkt. Daarnaast is het de vraag of een eenvoudig telefoontoestel onderling verbonden is met andere samenhangende apparaten.
Als advocaat zijnde is het dus van belang dit aan te stippen in een verweer. In het geval dat getwijfeld wordt over de vraag of het apparaat is aan te merken als een geautomatiseerd werk, kan een advocaat dit in zijn of haar verweer aanvoeren. Zo kan bijvoorbeeld gesteld worden dat een eenvoudige telefoon geen geautomatiseerd werk is en dit bestanddeel daarom niet bewezen moet worden. De advocaat kan in dat geval pleiten voor een vrijspraak. Omdat de definitie van geautomatiseerd werk na inwerkingtreding gaat wijzigen, moet deze definitie nog uitgekristalliseerd worden in de jurisprudentie.

### 3.8.4 *Onderzoek doen slachtoffer*

Het is de vraag in hoeverre het slachtoffer zelf onderzoek moet doen naar de betrouwbaarheid van de verkoper. In een arrest uit 2017 heeft de Hoge Raad hier enkele maatstaven voor gegeven. De raadsman heeft in het cassatiemiddel aangevoerd dat de slachtoffers de in het maatschappelijk verkeer geldende voorzichtigheid niet in acht hebben genomen. De slachtoffers zouden namelijk meer onderzoek naar de betrouwbaarheid van verdachte hebben moeten doen door bijvoorbeeld legitimatie te vragen.
De verdachte heeft zich in deze zaak uitgegeven als medewerker van verschillende bedrijven. In werkelijkheid was de verdachte helemaal geen medewerker van deze bedrijven. De verdachte heeft gereedschap besteld bij winkels gespecialiseerd in bouwmaterialen. Tussen de winkels en de bedrijven, waarbij de verdachte zich voordeed als een medewerker, bestond een vertrouwensrelatie. Daarom werden de goederen vaak op rekening gekocht en meegegeven aan de verdachte en werd niet om verdere legitimatie gevraagd. De Hoge Raad oordeelt dat als het gebruikelijk is om op vertrouwen een rechtsbetrekking aan te gaan, dat het slachtoffer minder grondig onderzoek hoeft te doen naar de persoon van de verdachte. Omdat tussen de winkels en de bedrijven een vertrouwensrelatie bestond, waren deze slachtoffers (de winkels) daarom niet verplicht om onderzoek te doen naar de betrouwbaarheid van de verdachte. De Hoge Raad heeft het cassatiemiddel daarom ongegrond verklaard.[82]
Op het moment dat de verdachte zich voordoet als bonafide verkoper of bonafide koper in een situatie waar op goed vertrouwen gehandeld wordt, dan zal de verdachte al snel als schuldige aangewezen worden.

In het geval dat goederen of diensten gekocht worden via Marktplaats of een andere verkoopsite, is het gebruikelijk om van te voren geld te betalen voor een goed of dienst, voordat dit goed of deze dienst geleverd wordt. In de rechtspraak is gesteld dat het online handelen op basis van wederzijds vertrouwen wordt gedaan. Voor kopers zijn verschillende manieren beschikbaar om onderzoek te doen naar de betrouwbaarheid van de verkoper. Ook al wordt gehandeld via het internet, dan nog kan de betrouwbaarheid van de verkoper getest worden. Zo kan bijvoorbeeld om een foto van het identiteitsbewijs gevraagd worden. Op die manier kan achterhaald worden of niet onder een valse naam gehandeld wordt. Daarnaast zijn op verschillende sites de namen vermeld van personen die bekend staan als internetoplichters. Tevens kan de koper de Bank Krediet Registratie (BKR) van de verkoper kunnen opvragen.

[80] *Kamerstukken II* 1998/99, 26671, 3, p. 44.
[81] *Kamerstukken II* 1998/99, 26671, 3, p. 44.
[82] HR 18 april 2017, ECLI:NL:HR:2017:718.

Indien goederen besteld worden bij een webwinkel kan gekeken worden of de webwinkel aan een keurmerk voldoet. Met andere woorden zijn er vele mogelijkheden om de betrouwbaarheid van een verkoper te controleren. Daarom ligt een deel van de verantwoordelijkheid bij het slachtoffer. De heer Kuijer heeft dit in zijn interview ook aangegeven. Volgens hem moeten kopers beseffen dat als een product ver onder de reële waarde wordt aangeboden, de kans groter is dat je wordt opgelicht. Een advocaat zou in zijn of haar verweer kunnen aanvoeren dat online handelen risico's met zich meebrengt. De koper is vaak niet bekend met de verkoper. Daarom ligt bij het slachtoffer een verantwoordelijkheid om onderzoek te doen naar de persoon van verkoper, vooral omdat dit gemakkelijk gedaan kan worden. In een verweer kan de advocaat in dat geval vragen om een strafvermindering.

### 3.8.5 *Strafbepaling*

Uit de jurisprudentie-analyse met betrekking tot internetoplichting volgt dat in de meeste gevallen een onvoorwaardelijke gevangenisstraf, voorwaardelijke gevangenisstraf of een taakstraf opgelegd wordt. De hoogste straf die hierbij is opgelegd (enkel voor het feit internetoplichting), is 36 maanden gevangenisstraf, waarvan 12 maanden voorwaardelijk. De persoon in deze zaak heeft 206 mensen opgelicht. Het Landelijke Overleg Vakinhoud Strafrecht (hierna te noemen: LOVS) heeft een handreiking gepubliceerd waarin oriëntatiepunten staan voor de straftoemeting. In deze handreiking zijn geen oriëntatiepunten gegeven voor de straftoemeting van meerderjarigen met betrekking tot oplichting. Dit is wel gedaan bij de straftoemeting van minderjarigen. Als oriëntatiepunt is daarvoor het volgende bepaald: voor een schade onder de € 150,- is een taakstraf van 25 uur aan te raden of een boete ad € 125,-. Voor schade die boven de € 150,- uitkomt, is een taakstraf vanaf veertig uur of een boete vanaf € 200,- aan te raden. Stel dat de advocaat een minderjarige verdachte bijstaat die € 70,- euro schade heeft aangericht met online handelsfraude, dan is het aan te raden om te controleren of de strafeis niet meer is dan een taakstraf van 25 uur of dat de boete niet hoger is dan € 125,-.[83]

Voor volwassenen zijn dus geen oriëntatiepunten gegeven in de handreiking van het LOVS. Daarentegen heeft het OM wel een richtlijn voor strafvordering oplichting gegeven.[84] Het OM heeft een aparte tabel waarin richtlijnen zijn gegeven voor internetoplichting. In dat geval moet sprake zijn van internetoplichting die door een verdachte gepleegd is. Voor de duidelijkheid is deze tabel opgenomen in bijlage 5. Deze tabel is ingedeeld in de categorieën first offender, één keer recidive en meermalen recidive. Daarnaast worden richtlijnen gegeven voor één slachtoffer, twee tot vier slachtoffers en een reeks aan slachtoffers. De precieze richtlijnen worden hier niet genoemd. Daarvoor wordt verwezen naar bijlage 5. Wel wordt benoemd dat medeplegen, net als de mate van professionaliteit, aangemerkt kunnen worden als een strafverzwarende omstandigheid.
Het controleren van de strafeis is daarom een aandachtspunt. Vooral nu richtlijnen zijn gegeven door het OM. Stel dat de strafeis de richtlijnen ver te boven gaat, dan is het verstandig dit aan te stippen in een verweer. Stel dat een first offender drie slachtoffers heeft gemaakt en de strafeis is een gevangenisstraf van drie maanden, dan gaat dit de richtlijn ver te boven. Als advocaat kan dan aangevoerd worden dat de strafeis totaal niet overeenkomt met de richtlijnen. In dat geval kan gevraagd worden dat, indien de rechter de verdachte schuldig verklaard van het tenlastegelegde, een straf wordt opgelegd in overeenstemming met de richtlijnen.

## 3.9 DEELCONCLUSIE

Uit de analyse naar de nieuwe strafbaarstelling van online handelsfraude volgt dat de vervolging en berechting van dit delict in de toekomst op veel punten veranderd ten opzichte van de vervolging en berechting op dit moment. Zo hoeft online handelsfraude in de toekomst niet meer bewezen te worden aan de hand van oplichting. Daarom hoeft ook niet meer

[83] Oriëntatiepunten voor straftoemeting en LOVS-afspraken 2017, p. 34.
[84] www.om.nl zoek op: *richtlijn voor strafvordering oplichting*

bewezen te worden dat gebruik is gemaakt van oplichtingsmiddelen. Hiermee is het grootste knelpunt voor de huidige vervolging en berechting van online handelsfraude opgelost. Wel moet in de toekomst bewezen worden dat bij de verdachte sprake is van een ‘gewoonte of beroep maken’ van online handelsfraude. Daarnaast is het van belang dat de verdachte het oogmerk heeft gehad op het verkrijgen van geld voor goederen of diensten zonder de bedoeling deze volledig te leveren. Tevens moeten deze goederen en diensten zijn verkocht door middel van een geautomatiseerd werk. Denk hierbij aan een advertentie die op Marktplaats is geplaatst. Na inwerkingtreding van het wetsvoorstel Computercriminaliteit III zal de definitie van een geautomatiseerd wijzigen. Daarom is op dit moment niet precies duidelijk wat hieronder verstaan wordt.
De Hoge Raad heeft bepaald dat het slachtoffer ook enkele verantwoordelijkheden draagt met betrekking tot de betrouwbaarheid van de verkoper. Op het moment dat een rechtsbetrekking wordt aangegaan op basis van vertrouwen, dan hoeft het slachtoffer minder onderzoek te doen naar de betrouwbaarheid van de verkoper.
Tot slot kan aan de hand van de analyse naar de huidige strafoplegging bij online handelsfraude en de ‘richtlijn voor strafvordering internetoplichting’ van het OM een conclusie getrokken worden. Online handelsfraude wordt vrij zwaar gestraft. De kans dat een gevangenisstraf opgelegd wordt is groot. Zelfs een verdachte die voor de eerste maal in aanraking komt met online handelsfraude en die meerdere slachtoffer heeft gemaakt, zal in principe een gevangenisstraf te wachten staan. Indien geen gevangenisstraf geëist wordt, dan zal een taakstraf geëist worden.

# 4 HEIMELIJK BINNENDRINGEN IN EEN GEAUTOMATISEERD WERK

Dit hoofdstuk besteedt aandacht aan de nieuw voorgestelde opsporingsbevoegdheid tot het heimelijk binnendringen in een geautomatiseerd werk. In dit hoofdstuk wordt de inhoud van de voorgestelde bevoegdheid behandeld. Daarnaast wordt de mening van twee experts op het gebied van computercriminaliteit gegeven met betrekking tot de voorgestelde bevoegdheid. Tot slot komen aandachtspunten aan bod die gebruikt kunnen worden in toekomstige procedures.
Paragraaf 1 gaat over de opsporingsbevoegdheden die op dit moment worden ingezet ten behoeve van de opsporing van computercriminaliteit. Paragraaf 2 besteedt aandacht aan de juridische voorwaarden voor de inzet van de nieuwe opsporingsbevoegdheid. In paragraaf 3 komen de doelen ten behoeve waarvan de opsporingsbevoegdheid mag worden ingezet aan bod. In paragraaf 4 wordt behandeld hoe de nieuwe opsporingsbevoegdheid in zijn werk gaat. Paragraaf 5 gaat over de toetsing van de bevoegdheid. De voorgestelde opsporingsbevoegdheid maakt een inbreuk op grondrechten. Dit wordt in paragraaf 6 behandeld. Het praktijkdeel van dit hoofdstuk komt in paragraaf 7 aan bod. In deze paragraaf wordt de mening van twee experts op het gebied van computercriminaliteit met betrekking tot de voorgestelde opsporingsbevoegdheid gegeven. In paragraaf 8 komen de aandachtspunten aan bod die in de toekomst van belang zijn in procedures waarin de opsporingsbevoegdheid is toegepast. Tot slot wordt in paragraaf 9 een deelconclusie gegeven.

## 4.1 HUIDIGE OPSPORINGSMOGELIJKHEDEN

In Titel IV van het WvSv staan de bijzondere dwangmiddelen. Een dwangmiddel wordt omschreven als:

"*Het krachtens de wet optreden met een strafvorderlijk doel, waardoor inbreuk op fundamentele rechten en vrijheden van personen gemaakt wordt, tegen of ongeacht de wil van de betrokkenen".*[85]

Het is daarom verplicht om dwangmiddelen op te nemen in een wet in formele zin. Bij de totstandkoming van een wet in formele zin worden de belangen van burgers voldoende meegewogen. De rechtsbescherming wordt geboden door grenzen te stellen aan de betreffende regeling.[86]

### 4.1.1 Doorzoeking van een plaats ter vastlegging van gegevens (artikel 125i)

In deze paragraaf komt de doorzoeking van een plaats ter vastlegging van gegevens aan bod. Omdat een goed begrip van gegevens nodig is, wordt eerst uitgelegd wat onder gegevens verstaan wordt. Daarna komt artikel 125i Sv inhoudelijk aan bod.

#### *4.1.1.1 Gegevens*

In artikel 125i Sv is de opsporingsbevoegdheid tot het doorzoeken in een plaats ter vastlegging van gegevens geregeld. Voor een goed begrip van deze opsporingsbevoegdheid wordt eerst beschreven wat onder het begrip 'gegevens' wordt verstaan. In artikel 80quinquies Sr staat de definitie van het begrip 'gegevens':

"*Iedere weergave van feiten, begrippen of instructies, op een overeengekomen wijze, geschikt voor overdracht, interpretatie of verwerking door personen of geautomatiseerde werken*".

Gegevens zijn onder andere bestanden die zijn opgeslagen in geautomatiseerde werken. Bovendien kunnen ook programma's waarmee geautomatiseerde werken worden bestuurd als gegevens worden aangemerkt. Gegevens hoeven zich niet persé te bevinden in een

[85] Cleiren, Crijns & Verpalen 2015, p. 317.
[86] Cleiren, Crijns & Verpalen 2015, p. 317.

geautomatiseerd werk. De wetgever heeft bepaald dat gegevens niet hetzelfde zijn als een goed.[87] De Hoge Raad heeft in 2012 bepaald dat:

"*De enkele omstandigheid dat een object ook eigenschappen heeft van gegevens in de zin van artikel 80quinquies Sr brengt niet mee dat dit object reeds daarom niet meer als goed in de zin van artikel 310 Sr kan worden aangemerkt*."[88]

Dit onderscheid is bijvoorbeeld van belang wanneer sprake is van diefstal. Zo valt diefstal van gegevens niet onder artikel 310 Sr. Bij diefstal moet namelijk sprake zijn van een goed. Tevens zijn gegevens niet hetzelfde als voorwerpen. Daarom is een aparte wettelijke bepaling opgenomen in het WvSv om gegevens te doorzoeken en vast te leggen.

#### *4.1.1.2 artikel 125i Sv*

Artikel 125i Sv geeft de bevoegdheid tot het doorzoeken van een plaats ter vastlegging van gegevens. Deze bevoegdheid houdt in dat een plaats, bijvoorbeeld een huis van een verdachte, wordt onderzocht. Indien een geautomatiseerd werk wordt aangetroffen in dat huis, dan mag op grond van artikel 125i Sv in dit geautomatiseerde werk gezocht worden naar gegevens. Als de gegevens van belang zijn voor het onderzoek, mogen de gegevens worden vastgelegd. Dit kan bijvoorbeeld door het kopiëren van de betreffende gegevens.

De hoedanigheid van de functionaris is van belang bij de inzet van deze bevoegdheid. Zo heeft de rechter-commissaris meer bevoegdheden dan een (hulp)OvJ. De rechter-commissaris mag op grond van artikel 110 lid 1 en 2 Sv elke plaats doorzoeken. Net als een rechter-commissaris mag een (hulp)OvJ een woning en een kantoor van een geheimhouder doorzoeken. Hieraan zijn wel enkele voorwaarden verbonden. Zo moet het gaan om een ontdekking op heterdaad of een verdenking van een misdrijf waarop voorlopige hechtenis is toegelaten. Tevens moet niet gewacht kunnen worden op het optreden van de rechter-commissaris. Indien een (hulp)OvJ een woning of kantoor doorzoekt, moet een machtiging van de rechter-commissaris aanwezig zijn voor de doorzoeking. De opsporingsambtenaar is alleen bevoegd tot het doorzoeken van een vervoermiddel. In dat geval moet wederom sprake zijn van ontdekking op heterdaad. Wel mag de bevoegdheid ingezet worden bij elk strafbaar feit. De opsporingsambtenaar heeft geen toestemming nodig om deze bevoegdheid uit te oefenen.[89]

### 4.1.2 Netwerkzoeking

Een andere opsporingsbevoegdheid die op dit moment mag worden toegepast, is de netwerkzoeking. Deze bevoegdheid is opgenomen in artikel 125j Sv. Met deze bevoegdheid kan vanaf een geautomatiseerd werk naar gegevens worden gezocht op een ander geautomatiseerd werk dat is aangesloten op hetzelfde netwerk.[90] Deze bevoegdheid lijkt veel op de bevoegdheid uit artikel 125i Sv. Het verschil is dat deze bevoegdheid ziet op onderzoek doen naar gegevens in een elders geautomatiseerd werk vanaf de plaats waar de doorzoeking plaatsvindt.[91] Voordeel hiervan is dat meerdere geautomatiseerde werken tegelijkertijd onderzocht kunnen worden. De netwerkzoeking is bedoeld ter vastlegging van gegevens die van belang zijn voor het onderzoek.

Artikel 125j Sv is een op zichzelf staande bevoegdheid die alleen toegepast kan worden in combinatie met een van de doorzoekingsbevoegdheden uit artikel 96b Sv, artikel 96c Sv, artikel 97 Sv en artikel 110 Sv.[92] Artikel 96b Sv ziet op de doorzoeking van een voertuig. Artikel 96c Sv geeft de bevoegdheid tot doorzoeking van plaatsen anders dan een woning. Een

[87] Cleiren, Crijns & Verpalen 2016, p. 874.
[88] HR 31 januari 2012, ECLI:NL:HR:2012:BQ9251.
[89] Cleiren, Crijns & Verpalen 2015, p. 540-542.
[90] Conings & Oerlemans, *Computerrecht* 2013, nr. 1, p. 23-32.
[91] Cleiren, Crijns & Verpalen 2015, p. 543.
[92] Cleiren, Crijns & Verpalen 2015, p. 543-545.

woning of kantoor kan doorzocht worden op grond van artikel 97 Sv. Artikel 110 Sv geeft de mogelijkheid tot doorzoeking van een woning of kantoor van een persoon met de bevoegdheid tot verschoning. Het feit dat netwerkdoorzoeking alleen gecombineerd kan worden met een van de doorzoekingsbevoegdheden, brengt met zich mee dat elke keer andere voorwaarden zullen gelden voor de netwerkzoeking. In het geval dat artikel 125j Sv wordt gecombineerd met artikel 96c Sv, dan zullen de voorwaarden uit artikel 96c Sv ook gelden voor de netwerkzoeking.

Aan de inzet van de bevoegdheid uit artikel 125j Sv zijn enkele beperkingen verbonden. Zo volgt uit lid 2 dat een netwerkzoeking op een elders geautomatiseerd werk pas mag plaatsvinden indien de personen die op de plek van doorzoeking wonen, werken of verblijven daartoe toegang hebben. Tevens mag alleen doorzoeking plaatsvinden ingeval een vermoeden bestaat dat de gegevens relevant zijn voor het verdere onderzoek.[93]

### 4.2 JURIDISCHE VOORWAARDEN VOOR DE INZET VAN DE TOEKOMSTIGE BEVOEGDHEID

De voorgestelde bevoegdheid tot het heimelijk binnendringen in een geautomatiseerd werk is een ingrijpende bevoegdheid. Daarom zijn aan de inzet van deze bevoegdheid voorwaarden verbonden. In deze paragraaf wordt beschreven welke voorwaarden gelden voor de inzet van de bevoegdheid.

Om te beginnen moet sprake zijn van een misdrijf waarop voorlopige hechtenis is toegelaten. Het gaat dan om strafbare feiten waarop een gevangenisstraf van vier jaren of meer is gesteld of andere misdrijven die genoemd zijn artikel 67 lid 1 Sv. Tevens moeten de strafbare feiten een ernstige inbreuk op de rechtsorde opleveren.[94] Een moord of ernstig financieel misdrijf levert een ernstige inbreuk op de rechtsorde op. Daarnaast kan een minder ernstig misdrijf een ernstige inbreuk op de rechtsorde maken, indien zij in combinatie met andere misdrijven worden gepleegd. Denk hierbij aan valsheid in geschrifte in combinatie met omkoping van ambtenaren om op die manier een vergunning te verkrijgen. Een precieze lijn kan niet getrokken worden. Aan de hand van feiten en omstandigheden moet bepaald worden of het misdrijf een ernstige inbreuk op de rechtsorde oplevert.[95] De opsporingsbevoegdheid geldt niet alleen voor strafbare feiten met betrekking tot computercriminaliteit. De opsporingsbevoegdheid kan ingezet worden voor alle misdrijven als omschreven in artikel 67 lid 1 Sv.[96]

Voor enkele onderzoekshandelingen gelden strengere voorwaarden. Zo moet bij het vastleggen/veiligstellen en het ontoegankelijk maken van gegevens sprake zijn van een verdenking van een misdrijf waarop een gevangenisstraf van acht jaar of meer is gesteld of een misdrijf dat bij algemene maatregel van bestuur is aangewezen.[97]

Voordat de bevoegdheid tot het heimelijk binnendringen in een geautomatiseerd werk door de OvJ kan worden ingezet in een opsporingsonderzoek, dient de OvJ toestemming te vragen aan de rechter-commissaris. Een bevel tot onderzoek in een geautomatiseerd werk kan pas gegeven worden na een voorafgaande schriftelijke machtiging van de rechter-commissaris.[98]

De rechter-commissaris zal controleren of sprake is van een ‘dringend onderzoeksbelang’. De inzet van de bevoegdheid moet in dat geval voldoen aan de eisen van proportionaliteit en subsidiariteit. Bij proportionaliteit moet het belang dat gediend wordt met de bevoegdheid in

[93] Conings & Oerlemans, *Computerrecht* 2013, nr. 1, p. 23-32.
[94] *Kamerstukken II* 2015/16, 34372, 3, p. 28.
[95] Rb. Dordrecht 3 juli 2008, ECLI:NL:RBDOR:2008:BD6243.
[96] *Kamerstukken II* 2015/16, 34372, 3, p. 15.
[97] *Kamerstukken II* 2015/16, 34372, 3, p. 18.
[98] *Kamerstukken II* 2015/16, 34372, 3, p. 38.

verhouding staan tot de omvang van de beperking van de grondrechten van burgers.[99] Er is voldaan aan de subsidiariteit indien de gegevens niet op een minder ingrijpende manier verkregen kunnen worden.[100] Pas wanneer aan deze vereisten is voldaan, zal de rechter-commissaris toestemming geven voor de inzet van de bevoegdheid.[101] Op deze proportionaliteit, subsidiariteit en de beperking van grondrechten wordt in paragraaf 4.6 dieper ingegaan.

Deze voorwaarden zijn noodzakelijk aangezien sprake is van een ingrijpende bevoegdheid met een heimelijk karakter. De ingrijpendheid van deze opsporingsbevoegdheid wordt gelijkgesteld aan opsporingsbevoegdheden zoals infiltratie, direct afluisteren en het aftappen van communicatie. Voor deze opsporingsbevoegdheden gelden namelijk dezelfde vereisten.[102]

### 4.2.1 Bevel tot onderzoek in een geautomatiseerd werk

Aan de hand van het bevel dat de OvJ opstelt, toetst de rechter of is voldaan aan de eisen van proportionaliteit en subsidiariteit. In het bevel moet worden opgenomen om wat voor misdrijf het gaat. Daarnaast worden de feiten en omstandigheden opgenomen die hebben geleid tot een verdenking. Tevens moet het apparaat waarin de OvJ onderzoek wil doen, duidelijk beschreven worden. Verder moet worden beschreven met behulp van welk technisch middel het geautomatiseerde werk onderzocht gaat worden. Op die manier kan de rechter-commissaris controleren of dit middel aan de eisen genoemd in het Besluit technische hulpmiddelen trafvordering (hierna: Bths) voldoet. Tot slot moet worden aangegeven voor welke tijdsduur de bevoegdheid wordt ingezet en moet aangegeven worden welk onderdeel van het geautomatiseerde werk onderzocht gaat worden.[103]

### 4.2.2 Procedurele eisen aan het onderzoek in een geautomatiseerd werk

De bevoegdheid mag alleen uitgevoerd worden door bepaalde opsporingsambtenaren. Zij zijn gespecialiseerd op het gebied van informatie en communicatietechnologie. Daarnaast mogen deze opsporingsambtenaren geen onderdeel zijn van het opsporingsteam dat het tactische onderzoek verricht. Tijdens het tactische onderzoek wordt informatie verzameld over het strafbare feit en de persoon van de verdachte. Zo wordt onder andere onderzocht wat de motief is voor het begaan van het strafbare feit. Tevens wordt onderzocht wat precies is gebeurd.[104] Deze regeling bevordert het voorkomen van tunnelvisie.[105]

Daarnaast worden ook eisen gesteld aan het technische hulpmiddel waarmee in een geautomatiseerd werk onderzoek wordt gedaan. Het technische hulpmiddel wordt ingezet ter vervanging van de eigen directe waarneming van de opsporingsambtenaar.[106] Het technisch hulpmiddel moet voldoen aan de regeling als genoemd in artikel 126ee Sv. In lid 1 van dit artikel staat vermeld dat regels worden gesteld bij algemene maatregel van bestuur. Deze algemene maatregel van bestuur is het Bths.[107]

Tot slot dienen de gegevens betreffende het onderzoek in het geautomatiseerde werk bijgehouden te worden in een proces-verbaal. Controle ten aanzien van welke handelingen wel of niet met behulp van een technisch hulpmiddel in het geautomatiseerde werk hebben

[99] *Kamerstukken II* 2015/16, 34372, 3, p. 53.
[100] *Kamerstukken II* 2015/16, 34372, 3, p. 54.
[101] *Kamerstukken II* 2015/16, 34372, 3, p. 30.
[102] *Kamerstukken II* 2015/16, 34372, 3, p. 28.
[103] *Kamerstukken II* 2015/16, 34372, 3, 30.
[104] www.politie.nl zoek op: *tactische recherche.*
[105] *Kamerstukken II* 2015/16, 34372, 3, p. 31.
[106] Cleiren, Crijns & Verpalen 2015, p. 791-794.
[107] Cleiren, Crijns & Verpalen 2015, p. 791-794.

plaatsgevonden, moet te allen tijde mogelijk zijn.[108] Dit kan bijgehouden worden door middel van het opmaken van een proces-verbaal. Deze processen-verbaal dienen opgenomen te worden in een dossier. Op die manier kunnen advocaten en rechters controleren of de handelingen juist hebben plaatsgevonden.

Indien de opsporingsbevoegdheid wordt toegepast ten behoeve van ontoegankelijkmaking van gegevens, het aftappen van communicatie of de stelselmatige observatie, dan gelden de bepalingen over de inzet van deze opsporingsbevoegdheden ook.[109]

### 4.3 INHOUD VAN DE NIEUWE OPSPORINGSBEVOEGDHEID

In deze paragraaf wordt beschreven ten aanzien van welke doelen de opsporingsbevoegdheid ingezet mag worden.

#### 4.3.1 Vaststelling en vastlegging van gegevens

In de eerste plaats kan de opsporingsbevoegdheid ingezet worden tot vaststelling en vastlegging van bepaalde kenmerken van het geautomatiseerde werk of tot vaststelling en vastlegging van de gebruiker. In het geval dat de opsporingsbevoegdheid voor dit doel gebruikt wordt, is dit ter voorbereiding van het inzetten van andere opsporingsbevoegdheden of om te bepalen in welke richting het opsporingsonderzoek uit moet gaan. Op deze manier kan bijvoorbeeld de identiteit of locatie van een geautomatiseerd werk of een gebruiker worden vastgesteld. Met vastlegging wordt gedoeld op het overnemen van gegevens. De gegevens worden in dat geval gekopieerd.[110]

#### 4.3.2 Vastlegging van gegevens die in het geautomatiseerde werk zijn opgeslagen

Bovendien wordt de bevoegdheid gebruikt om gegevens vast te leggen die in het geautomatiseerde werk zijn opgeslagen. Het verschil met het vorige doel is dat deze vastlegging verder gaat dan alleen ter identificatie of locatiebepaling.
Volgens de MvT brengt de term ‘opgeslagen’ tot uitdrukking dat de gegevens in het geautomatiseerde werk aanwezig zijn. Het gaat in dat geval om gegevens die opgeslagen zijn of worden opgeslagen.[111]
Het toepassen van de opsporingsbevoegdheid in deze situatie is bedoeld voor waarheidsvinding van ernstige strafbare feiten. Alleen de gegevens die noodzakelijk zijn voor waarheidsvinding worden vastgelegd. Gegevens die niet van belang zijn voor waarheidsvinding worden dus ook niet vastgelegd.[112]

#### 4.3.3 Ontoegankelijkmaking van gegevens

Daarnaast wordt de opsporingsbevoegdheid gebruikt voor het ontoegankelijk maken van gegevens. Dit mag alleen bij gegevens waarmee of met behulp waarvan een ernstig delict is gepleegd. Het ontoegankelijk maken van gegevens is alleen toegestaan voor zover hiermee het strafbare feit beëindigd kan worden of nieuwe strafbare feiten voorkomen kunnen worden. Door middel van het ontoegankelijk maken van gegevens wordt voorkomen dat de beheerder van het geautomatiseerd werk of derden gebruik kunnen maken van de gegevens. Tevens wordt voorkomen dat de gegevens verder verspreid worden.[113]

#### 4.3.4 De uitvoering van een bevel tot aftappen en opnemen van communicatie

Tevens wordt de opsporingsbevoegdheid gebruikt voor het heimelijk aftappen of opnemen van communicatie en het opnemen van vertrouwelijke communicatie. De opsporingsbevoegdheid tot onderzoek in een geautomatiseerd werk wordt in dat geval gecombineerd met de

[108] *Kamerstukken II* 2015/16, 34372, 3, p. 31.
[109] *Kamerstukken II* 2015/16, 34372, 3, p. 31.
[110] *Kamerstukken II* 2015/16, 34372, 3, p. 19.
[111] *Kamerstukken II* 2015/16, 34372, 3, p. 20.
[112] *Kamerstukken II* 2015/16, 34372, 3, p. 21.
[113] *Kamerstukken II* 2015/16, 34372, 3, p. 21.

opsporingsbevoegdheid van het aftappen van communicatie. Het aftappen van communicatie is geregeld in de artikelen 126l, 126m, 126s, 126t en 126zg Sv. De nieuw voorgestelde opsporingsbevoegdheid moet in dit geval gecombineerd worden met reeds bestaande opsporingsbevoegdheden. Communicatie mag niet afgetapt worden zonder een bevel op grond van artikel 126l, 126m, 126s, 126t of 126zg Sv.

Volgens de MvT betreft communicatie de uitwisseling van informatie in de vorm van een gesprek of een bericht. Deze communicatie wordt uitgewisseld door middel van e-mail of SMS.[114] Als communicatie tussen twee personen wordt uitgewisseld, dan kan deze communicatie afgetapt of opgenomen worden indien dit in het belang van de opsporing van een strafbaar feit is.

#### 4.3.5 De uitvoering van een bevel tot stelselmatige observatie

De laatste situatie waarin de voorgestelde opsporingsbevoegdheid mag worden toegepast, is voor het stelselmatig observeren van personen. Deze situatie is vooral van belang bij mobiele apparaten. Denk hierbij aan een smartphone, tablet of laptop. Indien een verdachte wordt geobserveerd, dan kunnen ze aan de hand van de locatie van het mobiele apparaat in de meeste gevallen observeren waar de verdachte zich bevindt. De kans is groot dat de bezitter van het mobiele apparaat deze bij zich draagt.[115] Op die manier kan de locatie van de verdachte bijgehouden worden.

De bevoegdheid tot het heimelijk binnendringen in een geautomatiseerd werk wordt in dit geval ingezet om stelstelmatige observatie van een verdachte mogelijk en gemakkelijker te maken.[116]

De stelselmatige observatie houdt in dat een persoon langere tijd in de gaten wordt gehouden. De observatie kan verdeeld worden in dynamische observatie en statische observatie. Dynamische observatie is het stelselmatig volgen van een persoon. Statische observatie is het stelselmatig waarnemen van de aanwezigheid of het gedrag van de persoon.[117] Opsporing is stelselmatig als min of meer een volledig beeld kan worden verkregen van het leven van een burger.[118] Indien sprake is van een ingrijpende vorm van observatie die een verdergaande inbreuk maken op de persoonlijke levenssfeer, dan kan pas gesproken worden van stelselmatige observatie.[119] Iemand één keer observeren valt niet aan te merken als stelselmatige observatie.

De bevoegdheid tot onderzoek in een geautomatiseerd werk mag dus plaatsvinden voor de vaststelling en vastlegging van gegevens, de vastlegging van gegevens die in een geautomatiseerd werk zijn opgeslagen, de ontoegankelijkmaking van gegevens, de uitvoering van een bevel tot het aftappen of opnemen van gegevens en de uitvoering van een bevel tot stelselmatige observatie.
Het is niet zo dat de bovengenoemde situaties altijd apart worden toegepast. De onderzoekshandelingen kunnen ook gecombineerd worden. Zo kan het zijn dat het vastleggen van gegevens wordt gecombineerd met het ontoegankelijk maken van gegevens.[120]

[114] *Kamerstukken II* 2015/16, 34372, 3, p. 23.
[115] *Kamerstukken II* 2015/16, 34372, 3, p. 25.
[116] *Kamerstukken II* 2015/16, 34372, 3, p. 25.
[117] Cleiren, Crijns & Verpalen 2015, p. 588-590.
[118] Buruma, *NJCM-Bulletin* 2000, p. 649-658.
[119] Aanwijzing opsporingsbevoegdheden, *Stcrt.* 2011, 3240, p. 3.
[120] *Kamerstukken II* 2015/16, 34372, 3, p. 24.

## 4.4 WERKWIJZE NIEUWE OPSPORINGSBEVOEGDHEID

In deze paragraaf wordt aandacht besteed aan de manier waarop de inzet van de voorgestelde opsporingsbevoegdheid in zijn werk gaat. De bevoegdheid wordt namelijk in verschillende fasen ingezet. Deze fasen zullen in deze paragraaf uitgewerkt worden.

### 4.4.1 Verkennende fase

De verkennende fase gaat vooraf aan de fase waarin de bevoegdheid daadwerkelijk wordt ingezet. Zo wordt in deze fase het geautomatiseerde werk of de gebruiker daarvan geïdentificeerd om zeker te weten dat de bevoegdheid ten aanzien van de juiste persoon wordt toegepast. Daarnaast wordt onderzoek gedaan zodat toegang kan worden verkregen tot het geautomatiseerde werk en worden de risico's beoordeeld. Het beoordelen van de risico's is mogelijk door het geautomatiseerde werk goed in kaart te brengen. Zo wordt bekeken welke programma's op het geautomatiseerde werk zijn geïnstalleerd, welke bestandsmappen aanwezig zijn, of dat het geautomatiseerde werk wordt gebruikt door meerdere gebruikers, hoe het beheer van het geautomatiseerde werk verloopt en welke besturingsprogramma's van toepassing zijn.[121]

### 4.4.2 Het onderzoek in een geautomatiseerd werk

Nadat onderzoek is gedaan in de verkennende fase naar het geautomatiseerde werk en de gebruiker van het geautomatiseerde werk en een zorgvuldige belangenafweging heeft plaatsgevonden, kan de OvJ bepalen dat onderzoek in het betreffende geautomatiseerde werk wordt gestart. Dit is alleen mogelijk indien de rechter-commissaris toestemming heeft gegeven voor het onderzoek in het geautomatiseerde werk.
Het onderzoek in het geautomatiseerde werk vindt plaats met behulp van een technisch hulpmiddel. Dit technische hulpmiddel is dan een softwareapplicatie. Aan de hand van de installatie van deze softwareapplicatie kunnen geluidsfragmenten worden opgenomen, screenshots worden gemaakt, toetsaanslagen worden vastgelegd of bestandsmappen worden doorzocht.[122]

### 4.4.3 De afsluiting van het onderzoek in een geautomatiseerd werk

Bij de afsluiting van het onderzoek in een geautomatiseerd werk, wordt het technische hulpmiddel weer verwijderd. Het onderzoek in een geautomatiseerd werk stopt wanneer het doel van het onderzoek is bereikt of wanneer de duur van het bevel is verlopen.
In de gevallen waarin gebruik is gemaakt van een technisch hulpmiddel, wordt dit technische hulpmiddel na beëindiging van het gebruik van de bevoegdheid verwijderd. Niet in alle gevallen wordt het technische hulpmiddel verwijderd. In dat geval moet sprake zijn van aanzienlijke risico's die schade aan het systeem van het geautomatiseerde werk kunnen brengen.
Bij de afsluiting van het onderzoek in een geautomatiseerd werk is het de bedoeling dat het geautomatiseerde werk zoveel mogelijk wordt hersteld in de staat waarin het geautomatiseerde werk verkeerde voordat de bevoegdheid werd toegepast.[123]

## 4.5 TOETSING VAN DE BEVOEGDHEID

De bevoegdheid tot het heimelijk binnendringen in een geautomatiseerd werk wordt in Titel IVA geplaatst. Het heimelijk binnendringen in een geautomatiseerd werk kan daarmee gekwalificeerd worden als een bijzondere bevoegdheid. Het is van belang dat toetsing en controle op de bevoegdheid mogelijk is. Uit de MvT volgen enkele manieren waarop de bevoegdheid getoetst gaat worden.

### 4.5.1 Besluit technische hulpmiddelen strafvordering

In het Bths worden onder andere eisen gesteld aan de technische hulpmiddelen. Daarnaast is in het Bths bepaald dat logging van gegevens noodzakelijk is. Logging is het vastleggen van

[121] *Kamerstukken II* 2015/16, 34372, 3, p. 32.
[122] *Kamerstukken II* 2015/16, 34372, 3, p. 35.
[123] *Kamerstukken II* 2015/16, 34372, 3, p. 36.

gegevens. Een van de problemen die logging oplost, is het voorkomen van misbruik door gebruikers van informatiesystemen.[124] Door middel van logging wordt getracht de authenticiteit en integriteit van de gegevens te waarborgen. Daarnaast kan de uitvoering van de bevoegdheid worden gecontroleerd.[125]

Aan technische hulpmiddelen worden drie voorwaarden gesteld. Ten eerste moet de waarneming betrouwbaar zijn. Daarnaast moet de waarneming voor derden te toetsen zijn. Tot slot moet de waarneming niet te manipuleren zijn. Dit is van belang voor de betrouwbaarheid van het bewijs. De resultaten die worden verkregen door het technische hulpmiddel kunnen namelijk als bewijsmateriaal gebruikt worden.[126] Aan deze technische hulpmiddelen zijn kwaliteitseisen verbonden die in het Bths vermeldt staan.

Alleen technische hulpmiddelen die voldoen aan de beschrijving genoemd in artikel 126ee Sv worden aangemerkt als technisch hulpmiddel. Indien een technisch hulpmiddel geen registratiefunctie bevat, dus alleen signalen detecteert, dan wordt niet gesproken van een technisch hulpmiddel in de zin van artikel 126ee Sv. Een voorbeeld van zo'n hulpmiddel is een verrekijker.[127]

De waarnemingen die worden vastgelegd door het technisch hulpmiddel moeten aan technische en procedurele eisen voldoen. Uit artikel 10 Bths volgt de technische eis. De datum en tijd waarop de gegevens worden geregistreerd, moeten automatisch en doorlopend op de gegevensdrager worden vastgelegd.

Het Bths stelt in artikel 18 lid 1 dat in principe alleen gekeurde technische hulpmiddelen mogen worden ingezet in het geval dat een bijzondere opsporingsbevoegdheid wordt toegepast. Alleen in het geval van een dringend onderzoeksbelang mag een technisch hulpmiddel worden ingezet dat niet gekeurd is. Uit artikel 22 lid 1 Bths volgt dat het technisch hulpmiddel wordt gekeurd door de keuringsdienst van het Korps landelijke politiediensten.

### 4.5.2 Opmaken van een proces-verbaal door een opsporingsambtenaar

Op grond van artikel 152 Sv is iedere opsporingsambtenaar verplicht een proces-verbaal op te maken van de werkzaamheden die deze opsporingsambtenaar heeft verricht. Dit wordt de verbaliseringsplicht genoemd. Uit artikel 152 Sv volgt verder dat dit proces-verbaal ten spoedigste moet worden opgesteld. Het hangt van de feiten en omstandigheden af of een proces-verbaal ten spoedigste is opgesteld.[128]
Een proces-verbaal hoeft alleen opgemaakt te worden voor werkzaamheden die zijn verricht in het opsporingsonderzoek. Voor werkzaamheden die zijn verricht voorafgaande aan het opsporingsonderzoek geldt geen verbaliseringsplicht. Toch heeft de Hoge Raad wel bepaald dat ook voor deze werkzaamheden enige vorm van verslaglegging moet plaatsvinden.[129]
Aan de hand van de processen-verbaal die worden opgesteld in het opsporingsonderzoek, kan naderhand gecontroleerd worden of de opsporingsbevoegdheid op een juiste manier is toegepast.

### 4.5.3 Notificatieplicht (artikel 126bb Sv)

Uit artikel 126bb Sv volgt de notificatieplicht. Deze notificatieplicht houdt in dat wanneer de overheid een inbreuk maakt op de persoonlijke levenssfeer van een burger, deze burger daarvan naderhand op de hoogte moet worden gesteld. De mededeling vindt plaats zodra het belang van het onderzoek dat toelaat. De mededeling moet uiterlijk gebeuren na de betekening

[124] www.noraonline.nl zoek op: *Patroon voor logging*.
[125] *Kamerstukken II* 2015/16, 34372, 3, p. 39.
[126] Cleiren, Crijns & Verpalen 2013, p. 646-649.
[127] Cleiren, Crijns & Verpalen 2013, p. 646-649.
[128] Cleiren, Crijns & Verpalen 2015, p. 952.
[129] HR 5 oktober 2010, ECLI:NL:HR:2010:BL5629, m.nt. T.M. Schalken.

van de dagvaarding aan verdachte.[130] In de meeste gevallen is de mededeling bedoeld voor de verdachte. In sommige gevallen kan echter ook een inbreuk worden gemaakt op de persoonlijke levenssfeer van een derde. Mocht dit het geval zijn, dan geldt de notificatieplicht ook ten aanzien van deze derde.

## 4.6 BESCHERMING VAN GRONDRECHTEN

Omdat het onderzoek in een geautomatiseerd werk een ernstige aantasting op het recht op eerbiediging van de persoonlijke levenssfeer maakt, zal hier een aparte paragraaf aan besteed worden.[131]

Uit de MvT komt naar voren dat het recht om niet lastiggevallen te worden door de overheid onderdeel is van het recht op eerbiediging van de persoonlijke levenssfeer.[132] Uit de Grondwet volgt dat een beperking op dit grondrecht alleen mogelijk is, indien deze beperking voortvloeit uit de wet.[133] Volgens het Europese Verdrag voor de Rechten van de Mens (hierna: EVRM) is een beperking alleen mogelijk indien dit in de wet is opgenomen en de beperking in een democratische samenleving noodzakelijk is in het belang van de openbare veiligheid, de nationale veiligheid, het welzijn van het land, het voorkomen van wanordelijkheden, het voorkomen van strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.[134] De noodzaak van een inbreuk op de eerbiediging van de persoonlijke levenssfeer wordt mede bepaald door de proportionaliteit en subsidiariteit. Dit heeft het Europese Hof voor de rechten van de mens (hierna te noemen: EHRM) in haar rechtspraak bepaald.[135] In deze rechtspraak is mede bepaald dat de wettelijke regeling die een beperking mogelijk maakt voldoende precies is geformuleerd en waarborgen kan bieden tegen een willekeurige inmenging in het privéleven. Tevens moet de wettelijke regeling waarborgen bieden tegen misbruik van de bevoegdheid.

### 4.6.1 Proportionaliteit

Zoals in paragraaf 4.2 staat beschreven, houdt de proportionaliteit in dat het belang dat wordt gediend door de bevoegdheid, in verhouding moet staan tot de omvang van de beperking van de persoonlijke levenssfeer.[136] Het beginsel van proportionaliteit wordt verder ingevuld aan de hand van vijf eisen waaraan voldaan moet worden, voordat een inbreuk gemaakt mag worden op de persoonlijke levenssfeer:

1. Het onderzoek in een geautomatiseerd werk moet een aanvulling vormen op de bestaande wettelijke bevoegdheden;

Indien de opsporing succesvol kan zijn met andere, minder ingrijpende opsporingsbevoegdheden, mag de opsporingsbevoegdheid tot onderzoek in een geautomatiseerd werk niet ingezet worden. Het is van belang dat sprake is van een dringend opsporingsbelang.

2. De inzet van onderzoek in een geautomatiseerd werk mag alleen plaatsvinden in de in artikel 126nba lid 1 Sv omschreven doelen;

Artikel 126nba Sv is het artikel waarin de opsporingsbevoegdheid tot onderzoek in een geautomatiseerd werk wordt opgenomen. In lid 1 zijn de volgende doelen opgenomen aan de hand waarvan de bevoegdheid ingezet mag worden. Deze doelen zijn in paragraaf 4.3 aan bod gekomen.

---

[130] Cleiren, Crijns & Verpalen 2015, p. 783.
[131] *Kamerstukken II* 2015/16, 34372, 3, p. 51.
Oerlemans, *DD* 2011, afl. 8/62, p. 898.
[132] *Kamerstukken II* 2015/16, 34372, 3, p. 52.
[133] Artikel 10 lid 1 GW.
[134] Artikel 8 lid 2 EVRM.
[135] *Kamerstukken II* 2015/16, 34372, 3, p. 52.
[136] *Kamerstukken II* 2015/16, 34372, 3, p. 53.

3. De rechter-commissaris moet van tevoren toetsen of de opsporingsbevoegdheid mag worden ingezet;

De uitleg met betrekking tot de toetsing door de rechter-commissaris is opgenomen in paragraaf 4.4.

4. De bevoegdheid mag maar beperkt worden toegepast;

Hiermee wordt bedoeld dat, indien dit mogelijk is, de bevoegdheid wordt toegepast in een zo beperkt mogelijk deel van het geautomatiseerde werk.[137] Op deze manier kan voorkomen worden dat gegevens die niet noodzakelijk zijn voor de opsporing ook worden onderzocht. Dit beschermt de persoonlijke levenssfeer van de burger.

5. De bevoegdheid mag niet oneindig worden uitgevoerd.

De bevoegdheid mag niet langer toegepast worden dan voor vier weken. Wel kan deze periode telkens met vier weken verlengd worden.[138]

Pas als aan al deze eisen is voldaan, kan geconcludeerd worden dat de inzet van de bevoegdheid tot het heimelijk binnendringen in een geautomatiseerd werk in een strafzaak proportioneel is. Naast proportioneel moet de inzet van de bevoegdheid ook aan de subsidiariteit voldoen.

### 4.6.2 Subsidiariteit

De MvT verwoordt het beginsel van subsidiariteit als volgt:

*"Het beoogde doel kan niet worden bereikt met een andere maatregel die minder ingrijpend is voor de persoonlijke levenssfeer."*[139]

Bij elke zaak zal bekeken moeten worden of een andere opsporingsbevoegdheid mogelijk is die een minder grote inbreuk maakt op de eerbiediging van de persoonlijke levenssfeer. Indien dat het geval is, mag de bevoegdheid tot onderzoek in een geautomatiseerd werk niet ingezet worden.

## 4.7 INTERVIEWS

In deze paragraaf wordt de mening van twee experts op het gebied van computercriminaliteit met betrekking tot de nieuwe opsporingsbevoegdheid gegeven. Ten eerste komt de mening van de heer Mr. Hersmus[140] aan bod. Daarna zal de mening van de heer Mr. Kuijer[141] behandeld worden.

### 4.7.1 De heer Mr. Hersmus[142]

De heer Hersmus vindt de nieuwe opsporingsbevoegdheid een positieve ontwikkeling in het strafrecht. Zoals ook in de MvT is beschreven, erkent de heer Hersmus dat het versleutelen van gegevens en het opslaan van gegevens in de Cloud een probleem vormen in de opsporing van computercriminaliteit, maar ook criminaliteit in zijn algemeenheid. Als voorbeeld noemt de heer Hersmus Skype. Je kunt met Skype internetbellen, maar dit is dan wel versleuteld. De nieuwe opsporingsbevoegdheid kan dit probleem oplossen doordat de versleuteling wordt omzeild. Op dat moment wordt een programma gecreëerd dat ervoor zorgt dat alle gegevens die via Skype worden verzonden, ook naar het IP-adres van de politie wordt verstuurd. In dat geval worden gegevens niet naderhand en versleuteld ontvangen, maar worden de gegevens direct onderschept. Je kunt dan horen waar de mensen over praten via Skype. Dit geldt niet

[137] *Kamerstukken II* 2015/16, 34372, 3, p. 53-54.

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

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

[140] De heer Hersmus is parket-secretaris bij het OM in 's-Hertogenbosch. De heer Hersmus heeft als portefeuille cybercrime.

[141] De heer Kuijer is raadsheer bij het gerechtshof te 's-Gravenhage. Tevens is de heer Kuijer lid van het Kenniscentrum Cybercriminaliteit van het gerechtshof 's-Gravenhage.

[142] Het interview van de heer Hersmus is bijgevoegd als bijlage 6.

alleen voor Skype, maar geldt heel breed, omdat zoveel gegevens versleuteld worden. Men kan tegenwoordig gemakkelijk programma's downloaden die zorgen dat gegevens versleuteld zijn. De huidige opsporingsbevoegdheden zijn hier niet tegen opgewassen. De technologie gaat harder dan dat de wetgeving kan bijhouden. De heer Hersmus is tevens van mening dat de technische mogelijkheden van opsporing groter zijn dan dat daar juridisch in is voorzien door de wetgever. De inzet van deze technische mogelijkheden is niet toegestaan in de wet. De nieuwe opsporingsbevoegdheid is een middel om de technologische ontwikkelingen bij te halen.
De heer Hersmus stelt dat de Cloud het bemoeilijkt om te achterhalen waar bepaalde gegevens zich precies bevinden. De heer Hersmus verwoordt het als volgt:

"*Het moeilijke aan een Cloud is van waar is die informatie nou precies. Het kan zijn dat het op een server op een computer in Nederland staat. Het kan ook zijn dat het een server in Ierland of de Verenigde Staten is. Het kan ook zijn dat het op meerdere computers tegelijk staat, het kan ook dat het in land A op een computer staat die weer door een bedrijf van land B gehuurd wordt. En dat maakt het soms heel lastig. Want wil je dan bij die gegevens, dan zal je over het algemeen een rechtshulpverzoek sturen naar het land wat gaat over die gegevens.*"

Het probleem is dus vooral dat moeilijk te achterhalen is in welk land en op welke server de gegevens opgeslagen staan. Met deze nieuwe opsporingsbevoegdheid kan je inbreken in bijvoorbeeld een smartphone van de verdachte en daar een programma op zetten. Op het moment dat hij dan een document bekijkt dat staat opgeslagen in een Cloud, dan bekijkt de verdachte dat in Nederland. Indien de gegevens dan door middel van dat programma naar de politie wordt gestuurd, is het niet nodig om uit te zoeken waar de gegevens zijn opgeslagen. Tevens zijn op dit moment vaak rechtshulpverzoeken nodig om gegevens te verkrijgen van een bepaalde persoon of bepaalde communicatie. Dit zorgt voor grote vertragingen in de opsporing naar strafbare feiten. Zoals zojuist uitgelegd kan door middel van het inzetten van de nieuwe opsporingsbevoegdheid het aantal rechtshulpverzoeken verminderd worden met betrekking tot computercriminaliteit.

Verder is de heer Hersmus van mening dat de nieuwe opsporingsbevoegdheid genoeg waarborgen biedt die de persoonlijke levenssfeer van burgers beschermt. Dit vloeit voort uit het feit dat een machtiging van de rechter-commissaris nodig is om deze bevoegdheid in te kunnen zetten. Daarnaast verwacht de heer Hersmus dat de bevoegdheid in het begin zeer terughoudend toegepast gaat worden.

Geconcludeerd kan worden dat de heer Hersmus zeer positief is over de nieuw voorgestelde opsporingsbevoegdheid. Volgens hem is de opsporingsbevoegdheid hard nodig om de technologische ontwikkelingen het hoofd te bieden.

### 4.7.2 De heer mr. Kuijer[143]

De heer Kuijer stelt dat de nieuw voorgestelde opsporingsbevoegdheid een positieve bijdrage kan leveren aan de opsporing van computercriminaliteit, maar ook andere delicten. Volgens de heer Kuijer is het met de nieuw voorgestelde opsporingsbevoegdheid gemakkelijker om een bepaalde persoon, vaak de verdachte, te identificeren. Dit komt doordat je met onderzoek in een geautomatiseerd werk ook stromende data kan opvangen. Met de huidige opsporingsbevoegdheden is dit niet mogelijk. De heer Kuijer geeft aan dat mensen vaak meer van hun identiteit prijsgeven in stromende data. Vaak wordt dan meer duidelijk over de geografische locaties, maar ook mailberichten waar identiteiten aan gekoppeld kan worden.

Tevens stelt de heer Kuijer dat de oude systematiek, waarbij een rechtshulpverzoek werd gedaan, volstrekt onwerkzaam is gebleken. Dit komt vooral door de tijd dat een rechtshulpverzoek in beslag neemt. Op het moment dat zo'n rechtshulpverzoek goedgekeurd

[143] Het interview van de heer Kuijer is bijgevoegd als bijlage 7.

werd, was de verdachte vaak verdwenen. Om goed op te kunnen treden tegen computercriminaliteit is volgens de heer Kuijer de nieuw voorgestelde opsporingsbevoegdheid onmisbaar.

De drempel die geldt voor het inzetten van de bevoegdheid vindt de heer Kuijer vrij hoog gelegd. De heer Kuijer uit wel zorgen over de controle van de inzet van de bevoegdheid achteraf. Volgens hem blijft dat een zwak punt. Een rechter-commissaris moet voor het inzetten van de bevoegdheid een machtiging geven. Het probleem is alleen dat de rechter-commissaris aan het begin van het onderzoek weinig weet. Dit geldt ook voor de politie. Er valt nog niet veel te beoordelen volgens de heer Kuijer. Toch is de kans wel groot dat een machtiging wordt gegeven voor de inzet van de bevoegdheid. Dat zou niet erg zijn als de controle achteraf heel goed is, maar dat is in veel gevallen een probleem. Bij het zwaardere segment van computercriminaliteit is opvallend dat er wel strafbare feiten zijn, maar vaak weinig verdachten en nog minder strafzaken. Zonder een verdachte kan de controle achteraf op zitting niet plaatsvinden. De heer Kuijer verwoordt het als volgt:

"*Dus je creëert eigenlijk een heel veld van inzet van bevoegdheden die eigenlijk achteraf nooit meer worden gecontroleerd of dat eigenlijk wel klopt, of dat wel goed is uitgevoerd, of dat wel binnen de kaders is gebleven."*

De heer Kuijer geeft ook aan dat het lastig is om dit probleem op te lossen. Hij stelt dat als er niet afdoende controle is, de bevoegdheid breder wordt ingezet dan waarvoor hij bedoeld is. De verdachte gaat in de meeste gevallen ook niet klagen, omdat hij zich dan bekend maakt. De neiging om de bevoegdheid in dat geval breed in te zetten, zal heel groot zijn. De heer Kuijer verwacht dat dit binnen vijf tot tien jaar uit de klauwen is gelopen. De heer Kuijer ziet in de controle vooraf een lacune, maar de toetsing van de inzet achteraf is eigenlijk nog minder inconsistent.

In het geval dat een zaak wel voor de rechter komt, is de heer Kuijer van mening dat wel op een juiste manier gecontroleerd kan worden of de opsporingsbevoegdheid op een goede manier is ingezet. Als advocaat zijnde is het verstandig om dit punt aan te stippen in een verweer. Bijvoorbeeld welke middelen ze hebben ingezet, of een technisch hulpmiddel wel op lijst X staat, of iets wel gekeurd is, etc. Indien een raadsman of –vrouw dit opwerpt, dan moeten de feiten vastgesteld worden. Als rechter zijnde wordt in dat geval gekeken of binnen de kaders is gebleven. In extreme gevallen, waarin niet binnen de kaders is gebleven, kan dit leiden tot een beslissing over de ontvankelijkheid, over de toelaatbaarheid van het bewijs of over strafvermindering. Met betrekking tot de voorgesteld opsporingsbevoegdheid benadrukt de heer Kuijer nogmaals dat het drempelniveau van de bevoegdheid niet slecht is. De machtiging van de rechter-commissaris werpt een hobbel op tegen al te lichtvaardige inzet, maar van de materiële toetsing door de rechter-commissaris moet niet teveel voorgesteld worden. Vooral de toetsing achteraf is het zwakke punt in de regeling.

## 4.8 AANDACHTSPUNTEN

In de laatste paragraaf van dit hoofdstuk worden aandachtspunten beschreven met betrekking tot de nieuw voorgestelde opsporingsbevoegdheid tot het heimelijk binnendringen in een geautomatiseerd werk. In voorgaande paragrafen is aandacht besteed aan de inhoud van de bevoegdheid en is de mening betreffende de bevoegdheid door praktijkexperts gegeven. Aan de hand van deze informatie wordt aangegeven welke aandachtspunten van belang zijn. Als advocaat kan op die manier in een (straf)procedure rekening gehouden worden met deze aandachtspunten. In deze paragraaf komen twee aandachtspunten aan bod: algemene vereisten en geautomatiseerd werk.

### 4.8.1 *Algemene vereisten*

Voor de inzet van de bevoegdheid gelden enkele algemene vereisten. Deze worden onderverdeeld in: doelen uit artikel 126nba lid 1 Sv ten behoeve waarvan de bevoegdheid mag

worden ingezet, naleving van proportionaliteit en subsidiariteit en inzet van een hulpmiddel als genoemd in het Bths.

Uit artikel 126nba lid 1 Sv volgt dat de bevoegdheid alleen ingezet mag worden voor een van de volgende doelen: de vaststelling van bepaalde kenmerken van het geautomatiseerde werk of de gebruiker, zoals de identiteit van de locatie, en de vastlegging daarvan, de uitvoering van een bevel tot opnemen van vertrouwelijke communicatie met een technisch hulpmiddel, de uitvoering van een bevel tot stelselmatige observatie, de vastlegging van gegevens die in het geautomatiseerde werk zijn verwerkt of de ontoegankelijkmaking van gegevens.

Daarnaast gelden de eisen van proportionaliteit en subsidiariteit voor de inzet van de bevoegdheid. De inzet van de bevoegdheid kan namelijk leiden tot een inbreuk op grondrechten, zoals het recht op een eerbiediging van de persoonlijke levenssfeer. Met betrekking tot de eis van proportionaliteit is het belangrijk dat het belang dat gediend wordt met de inzet van de bevoegdheid in verhouding staat tot de omvang van de beperking van de grondrechten van burgers.[144] Aan de eis van subsidiariteit is voldaan indien de gegevens niet op een minder ingrijpende manier verkregen kunnen worden.[145]
Een advocaat kan in een verweer bijvoorbeeld aanvoeren dat een andere opsporingsbevoegdheid ingezet had kunnen worden die minder aangrijpend is. Bijvoorbeeld de bevoegdheid tot doorzoeking in van een plaats ter vastlegging van gegevens. Daarnaast kan aangevoerd worden dat het grondrecht van de verdachte teveel beperkt is en dat dit niet in verhouding staat tot het te dienen doel van de inzet van de bevoegdheid. Wellicht lijkt dit een vanzelfsprekend aandachtspunt, maar op het moment dat getwijfeld wordt of de inzet van de bevoegdheid aan de eisen van proportionaliteit of subsidiariteit voldoet, is het verstandig dit aan te voeren in een verweer.

Tot slot geldt als vereiste dat het hulpmiddel dat wordt ingezet om de bevoegdheid uit te voeren, moet voldoen aan de eisen als benoemd in het Bths. In paragraaf 4.5.1 is aangegeven aan wat voor eisen een technisch hulpmiddel moet voldoen. In het geval dat het hulpmiddel niet aan de vereisten voldoet zoals genoemd in het Bths, mag dit hulpmiddel niet gebruikt worden. Voor de behandeling van de zaak door de rechter, dient de advocaat informatie te verkrijgen over de gebruikte hulpmiddelen. Pas op dat moment kan de advocaat controleren of het hulpmiddel voldoet aan de eisen. Indien de advocaat van mening is dat het hulpmiddel niet voldoet aan de eisen zoals genoemd in het Bths, kan hij of zij dit aanvoeren in een verweer. Dit kan bijvoorbeeld door te stellen dat de inzet van het hulpmiddel onrechtmatig is, omdat het niet aan de vereisten voldoet genoemd in het Bths.

Deze vereisten lijken wellicht overbodig om te noemen, maar het is wel degelijk belangrijk om als advocaat aandacht te besteden aan deze punten. Op het moment dat aan een van deze vereisten niet is voldaan, zou de bevoegdheid niet ingezet mogen worden. Dit geldt niet in het geval dat het verkeerde hulpmiddel is ingezet. De bevoegdheid had dan wel ingezet mogen worden, maar de bevoegdheid is dan op een foute manier ingezet. Ook dit kan grote gevolgen hebben voor de uitkomst van de procedure.

Zo kan een advocaat in zijn of haar verweer pleiten dat een van de consequenties genoemd in artikel 359a Sv dienen te volgen. Dit kan indien vormen onherstelbaar zijn verzuimd in het voorbereidend onderzoek. In het geval dat de bevoegdheid is ingezet ten behoeve van een doel dat niet is benoemd in artikel 126nba lid 1 Sv, dan is sprake van een vormverzuim. Dit is ook het geval indien niet aan de proportionaliteit of subsidiariteit is voldaan. De inzet van een hulpmiddel dat niet aan de vereiste voldoet genoemd in het Bths kan ook aangemerkt worden als een vormverzuim. Artikel 359a Sv geeft de volgende consequenties die verbonden kunnen

[144] *Kamerstukken II* 2015/16, 34372, 3, p. 53.
[145] *Kamerstukken II* 2015/16, 34372, 3, p. 54.

worden aan het vormverzuim: strafvermindering, bewijsuitsluiting en niet-ontvankelijkheid van het OM.

Het OM zal niet-ontvankelijkheid alleen in zeer uitzonderlijke gevallen toepassen. In dat geval moet '*een ernstige inbreuk zijn gemaakt op beginselen van een behoorlijke procesorde waardoor doelbewust of met grove veronachtzaming van de belangen van de verdachte aan diens recht op een eerlijke behandeling van zijn zaak is tekortgedaan'*.[146]

Bewijsuitsluiting komt aan de orde indien '*een belangrijk (strafvorderlijk) voorschrift of rechtsbeginsel in aanzienlijke mate is geschonden'*. [147] De Hoge Raad heeft criteria geformuleerd in welk geval bewijsuitsluiting toegepast kan worden. Ten eerste moet dus sprake zijn van het in aanzienlijke mate schenden van een voorschrift of rechtsbeginsel. Daarnaast moet sprake zijn van een van de volgende gevallen: schending van het recht op een eerlijk proces, een ander belangrijk strafvorderlijk voorschrift of rechtsbeginsel is geschonden en bewijsuitsluiting is het enige middel om vergelijkbare vormverzuimen te voorkomen of indien sprake is van een zeer uitzonderlijke situatie waaruit blijkt dat vormverzuimen structureel naar voren komen, waarbij de verantwoordelijke autoriteiten onvoldoende inspanningen hebben getoond om overtredingen van het desbetreffende voorschrift te voorkomen.[148]

Strafvermindering zal plaatsvinden indien '*de verdachte daadwerkelijk nadeel ondervonden heeft, dit nadeel veroorzaakt is door het verzuim, het nadeel geschikt is voor compensatie door middel van strafvermindering en strafvermindering ook in het licht van het belang van het geschonden voorschrift en de ernst van het verzuim gerechtvaardigd is'*.[149]

Ten aanzien van schending of het niet toepassen van een van de vereisten met betrekking tot het onderzoek in een geautomatiseerd werk, is het verstandig als advocaat zijnde een verweer te voeren waarin wordt gepleit tot bewijsuitsluiting of strafvermindering. De bevoegdheid tot onderzoek in een geautomatiseerd werk is een zeer ingrijpende bevoegdheid die op de juiste manier moet worden ingezet. De advocaat kan primair in zijn of haar verweer stellen dat sprake is van een aanzienlijke schending van een voorschrift of rechtsbeginsel. Daarnaast kan gesteld worden dat bewijsuitsluiting de enige manier is om vergelijkbare vormverzuimen te voorkomen. In dat geval kan gepleit worden dat het bewijs dat door het verzuim is vergaard, uitgesloten dient te worden. Subsidiair kan de advocaat pleiten voor een strafvermindering nu de verdachte nadeel heeft ondervonden dat is veroorzaakt door het verzuim.
De advocaat moet in zijn of haar verweer alle vereisten voor een artikel 359a Sv-verweer toepassen. Zo moet dus ook aangegeven worden dat sprake is van een onherstelbaar vormverzuim, dat geen sprake is van een vrijheidsbenemend dwangmiddel en dan de verdachte zelf wordt getroffen door het vormverzuim.[150]

### 4.8.2 *Geautomatiseerd werk*

Omdat in een geautomatiseerd heimelijk wordt binnengedrongen, is het van belang om zeker te zijn dat het onderzoek heeft plaatsgevonden in een geautomatiseerd werk. Omdat de definitie van een geautomatiseerd werk zal wijzigen na invoering van het wetsvoorstel Computercriminaliteit III, is op dit moment niet duidelijk wat allemaal onder een geautomatiseerd werk verstaan wordt. Daarom wordt dit als aandachtpunt aangemerkt. Voor de verdere uitwerking van dit aandachtspunt, wordt verwezen naar paragraaf 3.8.3. In deze paragraaf wordt dit aandachtspunt uitgebreid behandeld.

[146] HR 30 maart 2004, ECLI:NL:HR:2004:AM2533.
[147] HR 30 maart 2004, ECLI:NL:HR:2004:AM2533.
[148] HR 19 februari 2013, ECLI:NL:HR:2013:BY5321.
[149] HR 30 maart 2004, ECLI:NL:HR:2004:AM2533.
[150] HR 30 maart 2004, ECLI:NL:HR:2004:AM2533.

## 4.9 DEELCONCLUSIE

Onderzoek in een geautomatiseerd werk is een ingrijpende opsporingsbevoegdheid die mogelijkerwijs een inbreuk kan maken op de grondrechten van burgers. Onder andere op het recht op eerbiediging van de persoonlijke levenssfeer. De wetgever heeft daarom meerdere eisen gesteld waaraan de inzet van de bevoegdheid moet voldoen. Daarnaast heeft de wetgever in de MvT uitgebreid beschreven hoe de opsporingsbevoegdheid te werk gaat. Aan de hand van een analyse naar de eisen en de inhoud van de inzet van de nieuwe bevoegdheid, zijn enkele aspecten naar voren gekomen die aan te merken zijn als aandachtspunten. Zo is de inzet van de bevoegdheid beperkt aan bepaalde doelen. Deze doelen zijn beschreven in artikel 126nba lid 1 Sv. In dit artikel zal de bevoegdheid tot het heimelijk binnendringen in een geautomatiseerd werk worden opgenomen. Indien geen sprake is van een van deze doelen, dan mag de bevoegdheid dus niet ingezet worden. Daarnaast spelen de proportionaliteits- en subsidiariteitseis een rol. Deze eisen gelden, omdat de opsporingsbevoegdheid een inbreuk maakt op de persoonlijke levenssfeer van de verdachte.

De nieuw voorgestelde opsporingsbevoegdheid kan alleen ingezet worden met behulp van een technisch hulpmiddel. Dit technisch hulpmiddel moet aan de eisen voldoen die het Bths daaraan stelt. Indien niet aan deze eisen voldaan wordt, mag dat betreffende hulpmiddel niet ingezet worden. Stel dat achteraf blijkt dat een hulpmiddel is ingezet dat niet aan de eisen voldoet, dan is sprake van een vormverzuim.

Het technisch hulpmiddel mag alleen maar ingezet worden in een apparaat dat te kwalificeren valt als een geautomatiseerd werk. Stel dat een apparaat niet als geautomatiseerd werk aan te merken valt, dan mag de opsporingsbevoegdheid tot het heimelijk binnendringen niet ingezet worden. In dat geval moet een andere opsporingsbevoegdheid worden ingezet. Indien deze bevoegdheid toch is ingezet in zo'n apparaat, dan is sprake van een vormverzuim.

# 5 CONCLUSIES & AANBEVELINGEN

In de vorige hoofdstukken is het wetsvoorstel Computercriminaliteit III behandeld, met in het bijzonder de bepaling betreffende online handelsfraude en het heimelijk binnendringen in een geautomatiseerd werk. Aan de hand van dat onderzoek kunnen een aantal conclusies getrokken worden. Tevens is het mogelijk een aantal aanbevelingen te doen. Daarmee kan de centrale vraag van het onderzoeksrapport worden beantwoord. Voor de duidelijkheid wordt de centrale vraag hier herhaald: *welke aandachtspunten, die in een mogelijk verweer tegen een vervolging wegens online handelsfraude kunnen worden opgenomen, zijn er naar aanleiding van een onderzoek naar de strafbaarstelling betreffende online handelsfraude en de opsporingsbevoegdheid tot het heimelijk binnendringen van een geautomatiseerd werk met betrekking tot het wetsvoorstel Computercriminaliteit III te formuleren?*

## 5.1 CONCLUSIES

In deze paragraaf worden de conclusies gepresenteerd. Omwille van de duidelijkheid worden de conclusies per hoofdstuk gegeven. Nadat de conclusies zijn getrokken, worden in de volgende paragraaf de aanbevelingen beschreven.

### 5.1.1 Wetsvoorstel Computercriminaliteit III

Het wetsvoorstel Computercriminaliteit III is noodzakelijk gebleken vanwege de technische ontwikkelingen waarmee de maatschappij, maar ook de criminaliteit in aanraking komt. Zonder de aanpassingen die het wetsvoorstel voorstelt, zou niet adequaat genoeg opgekomen kunnen worden tegen computercriminaliteit.

### 5.1.2 Online handelsfraude

Online handelsfraude wordt op dit moment berecht en vervolgd aan de hand van oplichting uit artikel 326 Sr. Uit de jurisprudentie van de Hoge Raad blijkt dat het bewijzen van sommige bestanddelen problematisch kan zijn. Dit geldt voor het bewijzen van het gebruik van oplichtingsmiddelen. Zo levert het zich voordoen als bonafide verkoper niet direct het aannemen van een valse naam of valse hoedanigheid op. In zaken waarin de verdachte met zijn eigen naam of eigen contactgegevens goederen te koop aanbiedt, levert dit een bewijsprobleem op. Vooral op bewijstechnisch aspect zou de nieuwe strafbaarstelling een oplossing moeten bieden. Na inwerkingtreding van de nieuwe strafbaarstelling zullen procedures betreffende online handelsfraude aanzienlijk veranderen. Het invoeren van de nieuwe strafbaarstelling lost het zojuist genoemde bewijsprobleem op. In de toekomst hoeft niet meer bewezen te worden dat een oplichtingsmiddel is gebruikt om goederen aan personen te verkopen. In de toekomst moeten de volgende bestanddelen bewezen worden: ‘een gewoonte of beroep maken’, ‘goederen of diensten’, ‘door middel van een geautomatiseerd werk verkopen’, ‘oogmerk’, ‘zonder volledige levering’ en ‘verzekeren van betaling van die goederen of diensten’. Aan de hand van een jurisprudentie-analyse naar het bestanddeel ‘een gewoonte of beroep maken’, is gebleken dat al snel gesproken kan worden van een gewoonte. Daarnaast is uit de jurisprudentie-analyse gebleken dat het oogmerk niet aanwezig hoeft te zijn op het moment dat de koop plaatsvindt. Uit het feit dat een verdachte zijn goederen niet levert, kan afgeleid worden dat het oogmerk aanwezig is. Deze analyse is gemaakt aan de hand van jurisprudentie met betrekking tot het strafbare feit flessentrekkerij. Het is natuurlijk niet zeker dat de rechter deze lijn doorzet in de afhandeling van zaken van online handelsfraude op het moment dat de nieuwe strafbaarstelling gaat gelden. Tevens is het bestanddeel ‘door middel van een geautomatiseerd werk’ een aandachtspunt. Omdat na de inwerkingtreding van het wetsvoorstel een nieuwe definitie voor geautomatiseerde werken gaat gelden in de wet, zal daarom nog duidelijk moeten worden wat onder een geautomatiseerd werk wordt verstaan. Deze drie bestanddelen zullen na inwerkingtreding van de strafbaarstelling uitgekristalliseerd worden in de jurisprudentie. Daarom zijn deze drie bestanddelen op dit moment aan te merken als een aandachtspunt in de procedure. In een procedure betreffende online handelsfraude is het ook van belang te letten op de strafeis. Tot

slot kan de verantwoordelijk van het slachtoffer om onderzoek te doen naar de betrouwbaarheid van de verkoper worden aangemerkt als aandachtspunt.

### 5.1.3 Heimelijk binnendringen in een geautomatiseerd werk

Het heimelijk binnendringen in een geautomatiseerd werk is als opsporingsbevoegdheid voorgesteld om knelpunten met betrekking tot de opsporing van computercriminaliteit het hoofd te bieden.
Aan het inzetten van de nieuw voorgestelde bevoegdheid zijn enkele juridische voorwaarden verbonden. Zo moet sprake zijn van een misdrijf waarvoor voorlopige hechtenis is toegelaten. In dat geval moet een straf opgelegd kunnen worden van vier jaren of meer, of het strafbare feit moet in artikel 67 lid 1 Sv genoemd zijn. Daarnaast moet het feit een ernstige inbreuk op de rechtsorde opleveren. Indien aan deze eisen is voldaan, geeft de rechter-commissaris toestemming voor de inzet van de bevoegdheid. Het is van belang te benadrukken dat de opsporingsbevoegdheid niet alleen ingezet kan worden voor de opsporing van computercriminaliteit. De bevoegdheid kan ook worden ingezet voor de opsporing van traditionele strafbare feiten.
Het nieuw voorgestelde artikel 126nba Sv geeft in lid 1 aan ten behoeve van welke doelen de opsporingsinzet mag worden ingezet. Dit mag voor de volgende doeleinden: de vaststelling en vastlegging van gegevens, vastlegging van gegevens die in een geautomatiseerd werk zijn opgeslagen, ontoegankelijkmaking van gegevens, de uitvoering van een bevel tot het aftappen en opnemen van communicatie en de uitvoering van een bevel tot stelselmatige observatie. Indien geen sprake is van deze doelen, dan mag de opsporingsbevoegdheid niet ingezet worden.
Het toepassen van de bevoegdheid maakt een inbreuk op de persoonlijke levenssfeer. Hiertegenover stelt de MvT dat deze inbreuk rechtvaardig is, omdat de bevoegdheid aan de eis van proportionaliteit en subsidiariteit voldoet. Toch kan dit niet zomaar geconcludeerd worden. Niet alle zaken zijn hetzelfde en niet in alle zaken zal voldaan zijn aan de eis van proportionaliteit en subsidiariteit.
In een geautomatiseerd werk kan alleen heimelijk binnengedrongen worden door middel van een technisch hulpmiddel. Dit technische hulpmiddel moet aan een aantal eisen voldoen. Ten eerste moet de waarneming van het technisch hulpmiddel betrouwbaar zijn. Daarnaast moet de waarneming voor derden te toetsen zijn. Tot slot moet de waarneming niet te manipuleren zijn. Daarnaast zijn aan de technische hulpmiddelen zijn kwaliteitseisen verbonden die in het Bths vermeldt staan. Indien niet aan deze eisen voldaan wordt, is de inzet van de bevoegdheid niet rechtmatig.
Gebleken is dat er twee aandachtspunten te geven zijn. Het eerste aandachtspunt is de controle van de inzet van de bevoegdheid achteraf is. Zo moet gecontroleerd worden of aan de volgende eisen is voldaan: de bevoegdheid is ingezet ten behoeve van een van de doelen genoemd in artikel 126nba lid 1 Sv, de inzet van de bevoegdheid voldoet aan de proportionaliteit en subsidiariteit en het hulpmiddel dat is gebruikt om de bevoegdheid uit te voeren voldoet aan de eisen genoemd in het Bths. Ten tweede is het controleren of de bevoegdheid is ingezet in een geautomatiseerd werk een aandachtspunt.

## 5.2 AANBEVELINGEN

Er wordt aanbevolen om in strafrechtelijke procedures met betrekking tot online handelsfraude extra aandacht te besteden aan de bestanddelen ‘een gewoonte of beroep maken’, ‘het oogmerk’ en of ‘gebruik is gemaakt van een geautomatiseerd werk’. Dit wordt aanbevolen, omdat met betrekking nog niet helemaal duidelijk is hoe de rechter in hier in de toekomst over gaat oordelen. Daarnaast wordt aanbevolen om in toekomstige procedures te controleren of de strafeis van het OM niet ver boven de richtlijnen van de strafvordering voor internetoplichting uit komen. In de meeste gevallen wordt een taakstraf of gevangenisstraf geëist. De precieze richtlijnen voor de strafvordering staan vermeld in bijlage 5. Tot slot speelt de verantwoordelijkheid van het slachtoffer om onderzoek te doen ook een rol in de procedure. Het is de vraag in hoeverre het slachtoffer zelf verantwoordelijk is om onderzoek te doen naar de betrouwbaarheid van het aanbod.

In het geval dat de verdachte enkele slachtoffers heeft gemaakt, kan in een verweer aangestipt worden dat geen sprake is van het maken van een gewoonte of beroep. Het is namelijk maar de vraag of bij een klein aantal slachtoffers, bijvoorbeeld twee of drie, het maken van een gewoonte of beroep bewezen kan worden. Dit geldt ook indien de verdachte in een kort tijdsbestek van bijvoorbeeld een uur of twee uren een goed meerdere malen heeft verkocht. In dat geval kan in een verweer aangevoerd worden dat geen sprake is van een gewoonte maken, omdat in een kort tijdsbestek nooit sprake is van een gewoonte maken. Met betrekking tot het oogmerk zou in een verweer beargumenteerd kunnen worden dan nimmer sprake is geweest van het oogmerk om niet te leveren, maar dat nog geleverd wilde worden. In het geval dat de verdachte al honderd keer geld heeft ontvangen voor een goed en dat goed niet geleverd heeft, zal dit verweer hoogstwaarschijnlijk verworpen worden. Dit verweer kan wellicht wel succesvol zijn in zaken waar sprake is van een gering aantal slachtoffers. Daarnaast is het van belang om te controleren of gebruik gemaakt is van een geautomatiseerd werk bij de verkoop van de goederen of diensten. Indien een inrichting voor de inwerkingtreding van de nieuwe definitie niet kon worden aangemerkt als geautomatiseerd werk, is het verstandig in een verweer te stellen dat geen sprake is van gebruikmaking van een geautomatiseerd werk. In dat geval moet de rechter hierover oordelen en zal verder uitgekristalliseerd worden wat onder een geautomatiseerd werk verstaan wordt. Verder wordt aanbevolen te kijken naar de rol van het slachtoffer. In hoeverre heeft het slachtoffer zelf een onderzoeksplicht? In een verweer kan aangevoerd worden dat het slachtoffer zelf verantwoordelijkheid had onderzoek te doen naar de betrouwbaarheid. Zo kan aangegeven worden dat het slachtoffer naar een identiteitsbewijs had kunnen vragen om te controleren dat de naam van de verkoper overeenkwam met de daadwerkelijke persoon die het goed aanbood. Tevens kan in een verweer aangegeven worden dat het slachtoffer op internetsites had kunnen controleren of de verkoper bekend stond als oplichter. In al deze gevallen wordt aanbevolen een vrijspraak te bepleiten. Indien de strafeis niet overeenkomt met de richtlijnen strafvordering voor internetoplichting wordt aanbevolen in een verweer aan te voeren dat de strafeis niet overeenkomt met de richtlijnen en dat verzocht wordt bij een eventuele strafoplegging hier rekening mee te houden.

### 5.2.1 Heimelijk binnendringen in een geautomatiseerd werk

Zoals eerder aangestipt, mag de opsporingsbevoegdheid tot het heimelijk binnendringen in een geautomatiseerd werk ook ingezet worden voor de opsporing van strafbare feiten die geen verband houden met computercriminaliteit. Het kan in dat geval gaan om bijvoorbeeld moord of diefstal. Daarnaast is de opsporingsbevoegdheid bij uitstek ook geschikt voor de opsporing van computercriminaliteit, zoals online handelsfraude.
Met betrekking tot procedures waarin het heimelijk binnendringen in een geautomatiseerd werk is ingezet, wordt aanbevolen om in een verweer enkele punten met betrekking tot de eisen voor de inzet van de opsporingsbevoegdheid aan te stippen. Op die manier wordt de inzet van de bevoegdheid achteraf gecontroleerd. In het geval dat het hulpmiddel dat gebruikt is voor de inzet van de bevoegdheid niet voldoet aan de eisen die gesteld zijn, wordt aanbevolen dit aan te voeren in het verweer. Op het moment dat de beginselen van proportionaliteit en subsidiariteit niet nageleefd zijn, kan in een verweer aangegeven worden dat met de inzet van de bevoegdheid het OM zich niet aan de beginselen van de proportionaliteit en subsidiariteit gehouden heeft. Daarnaast is het een aanbeveling om te controleren of de opsporingsbevoegdheid is ingezet ten behoeve van een van de doelen zoals genoemd in artikel 126nba lid 1 Sv. Als dit niet het geval is, dan mag de opsporingsbevoegdheid niet ingezet worden. Indien naderhand blijkt dat sprake is van een vormverzuim in het voorbereidend onderzoek zoals hierboven genoemd, wordt aan de advocaat aanbevolen in het verweer een verzoek te doen tot primair bewijsuitsluiting van het bewijs dat is verkregen door middel van het vormverzuim en subsidiair strafvermindering aan de hand van artikel 359a Sv. Tot slot wordt ook hier aanbevolen te controleren of de bevoegdheid is ingezet in een geautomatiseerd werk. Indien de bevoegdheid is ingezet in een andere inrichting die niet aangemerkt kan worden als een geautomatiseerd werk, wordt aanbevolen ook hier een artikel 359a Sv-verweer te voeren.

## LITERATUUR- EN BRONNENLIJST


Boeken

**Cleiren, Crijns & Verpalen 2016**
C.P.M. Cleiren, J.H. Crijns & M.J.M. Verpalen, *Tekst en Commentaar – Strafrecht*, Deventer: Wolters Kluwer 2016.

**Cleiren, Crijns & Verpalen 2015**
C.P.M. Cleiren, J.H. Crijns & M.J.M. Verpalen, *Tekst en Commentaar – Strafvordering*, Deventer: Wolters Kluwer 2015.

**Cleiren, Crijns & Verpalen 2013**
C.P.M. Cleiren, J.H. Crijns & M.J.M. Verpalen, *Tekst en Commentaar – Strafvordering*, Deventer: Wolters Kluwer 2013.

**Groenhuijsen 1991**
M.S. Groenhuijsen, *Het wetsvoorstel computercriminaliteit bezien vanuit het gezichtspunt van een behoorlijk wetgevingsbeleid op strafrechtelijk gebied*, in F.P.E. Wiegmans (Ed.), *Commentaren op het wetsvoorstel computercriminaliteit*, Maastricht: Cipher Management 1991.

**Van der Hof, Lodder & Zwenne 2014**
S. van der Hof, A.R. Lodder & G.J. Zwenne, *Recht en computer*, Deventer: Kluwer 2014.

**Van Schaaijk 2011**
G.A.F.M. van Schaaijk, *Praktijkgericht juridisch onderzoek*, Den Haag: Boom Juridische uitgevers 2011.

**De Vey Mestdagh 2014**
C.N.J. de Vey Mestdagh, *Inleiding IT-recht*, Groningen: Stichting Recht & ICT 2014.

Tijdschriftartikelen:

**Buruma, *NJCM-Bulletin* 2000, p. 649-658.**
Y. Buruma, 'Stelselmatig – een sleutelbegrip in de Wet Bijzondere Opsporingsbevoegdheden', *NJCM-Bulletin* 2000, p. 649-658.

**Conings & Oerlemans, *Computerrecht* 2013, p. 23-32.**
C. Conings & J.J. Oerlemans, 'Van een netwerkzoeking naar online doorzoeking: grenzeloos of grensverleggend?', *Computerrecht* 2013, nr. 1, p 23-32.

**Koops, *Justitiële verkenning* 2012, p. 9-24**
E.J. Koops, 'De dynamiek van cybercrimewetging in Europa en Nederland', *Justitiële verkenningen: Documentatieblad van het Ministerie van Justitie* 2012, 38(1), p. 9-24.

**Oerlemans, *DD* 2011/62, p. 888-908.**
J.J. Oerlemans, 'Hacken als opsporingsbevoegdheid', *DD* 2011, alf. 8/62, p. 888-908.

Documenten:

**Oriëntatiepunten voor straftoemeting en LOVS-afspraken 2017**
De rechtspraak, *Oriëntatiepunten voor straftoemeting en LOVS-afspraken*, 2017.

**Regeerakkoord ‘Bruggen slaan’ 2012**
*Regeerakkoord ‘Bruggen slaan’ van de VVD – PvdA*, 2012.

**Veiligheidsmonitor 2016**
CBS & Ministerie van Veiligheid en Justitie, *Veiligheidsmonitor*, 2016.

Elektrische bronnen:
www.eerstekamer.nl
www.fundaments.nl
www.iusmentis.com
www.marktplaats.nl
www.noraonline.nl
www.om.nl
www.opgelicht.avrotros.nl
www.politie.nl
www.royalibiza.nl
www.wodc.nl

## JURISPRUDENTIELIJST


Hoge Raad
HR 1 november 1920, NJ 1920
HR 3 december 1996, NJ 1997, 574
HR 19 januari 1998, NJ 1998, 423
HR 30 maart 2004, ECLI:N:HR:2004:AM2533
HR 5 oktober 2010, ECLI:NL:HR:2010:BL5329
HR 31 januari 2012, ECLI:NL:HR:2012:BQ9251
HR 19 februari 2013, ECLI:NL:HR:2013:BY5321
HR 11 november 2014, ECLI:NL:HR:2014:3144
HR 9 december 2014, ECLI:NL:HR:2014:3546
HR 26 mei 2015, ECLI:NL:HR:2015:1336
HR 12 april 2016, ECLI:NL:HR:2016:618
HR 12 april 2016, ECLI:NL:HR:2016:621
HR 20 december 2016, ECLI:NL:HR:2016:2889
HR 10 januari 2017, ECLI:NL:HR:2017:20
HR 18 april 2017, ECLI:NL:HR:2017:718

Gerechtshof
Hof Amsterdam 28 juni 2006 ECLI:NL:GHAMS:2006:AY0307
Hof 's-Hertogenbosch 16 januari 2007 ECLI:NL:GHSHE:2007:BA2770
Hof Leeuwarden 20 april 2009 ECLI:NL:GHLEE:2009:BI1645
Hof Leeuwarden 3 september 2009 ECLI:NL:GHLEE:2009:BJ6902
Hof Leeuwarden 29 oktober 2010 ECLI:NL:GHLEE:2010:BO2524
Hof Leeuwarden 1 maart 2011 ECLI:NL:GHLEE:2011:BP6255
Hof Leeuwarden 5 juli 2011 ECLI:NL:GHLEE:2011:BR0614
Hof Leeuwarden 12 augustus 2011 ECLI:NL:GHLEE:2011:BR5593
Hof Leeuwarden 5 september 2011 ECLI:NL:GHLEE:2011:BT1911
Hof Leeuwarden 30 september 2011 ECLI:NL:GHLEE:2011:BT6410
Hof 's-Gravenhage 20 april 2012 ECLI:NL:GHSGR:2012:BW5086
Hof Amsterdam 2 mei 2012 ECLI:NL:GHAMS:2012:982
Hof Arnhem 11 juli 2012 ECLI:NL:GHARN:2012:BX4194
Hof 's-Hertogenbosch 7 februari 2013 ECLI:NL:GHSHE:2013:BZ2702
Hof 's-Hertogenbosch 18 februari 2013 ECLI:NL:GHSHE:2013:BZ2652
Hof Amsterdam 27 maart 2013 ECLI:NL:GHAMS:2013:BZ5771
Hof Arnhem-Leeuwarden 7 juni 2013 ECLI:NL:GHARL:2013:4093
Hof Arnhem-Leeuwarden 21 juni 2013 ECLI:NL:GHARL:2013:4498
Hof 's-Hertogenbosch 11 juli 2013 ECLI:NL:GHSHE:2013:3013
Hof 's-Hertogenbosch 23 januari 2014 ECLI:NL:GHSHE:2014:121
Hof 's-Hertogenbosch 2 april 2014 ECLI:NL:GHSHE:2014:1007
Hof Den Haag 16 april 2014 ECLI:NL:GHDHA:2014:1640
Hof Den Haag 16 april 2014 ECLI:NL:GHDHA:2014:1647
Hof Arnhem-Leeuwarden 9 september 2014 ECLI:NL:GHARL:2014:7098
Hof Den Haag 4 februari 2015 ECLI:NL:GHDHA:2015:1440
Hof Den Haag 17 november 2015 ECLI:NL:GHDHA:2015:3256
Hof Arnhem-Leeuwarden 4 maart 2016 ECLI:NL:GHARL:2016:1647
Hof Amsterdam 23 maart 2016 ECLI:NL:GHAMS:2016:1214
Hof Den Haag 21 april 2016 ECLI:NL:GHDHA:2016:1102
Hof Arnhem-Leeuwarden 3 oktober 2016 ECLI:NL:GHARL:2016:7861
Hof Amsterdam 6 oktober 2016 ECLI:NL:GHAMS:2016:4390

Rechtbank
Rb. 's-Gravenhage 4 maart 2005 ECLI:NL:RBSGR:2005:AS8906

Rb. Dordrecht 16 februari 2006 ECLI:NL:RBDOR:2006:AV1905
Rb. Groningen 23 februari 2006 ECLI:NL:RBGRO:2006:AV2491
Rb. 's-Gravenhage 7 april 2006 ECLI:NL:RBSGR:2006:AV9196
Rb. Maastricht 16 augustus 2006 ECLI:NL:RBMAA:2006:AY8467
Rb. 's-Gravenhage 4 oktober 2006 ECLI:NL:RBSGR:2006:AY9483
Rb. Alkmaar 7 november 2006 ECLI:NL:RBALK:2006:AZ1790

Rb. Dordrecht 7 februari 2007 ECLI:NL:RBDOR:2007:AZ9390
Rb. Groningen 26 maart 2007 ECLI:NL:RBGRO:2007:BA1487

Rb. Breda 1 april 2008 ECLI:NL:RBBRE:2008:BC8213
Rb. Breda 1 april 2008 ECLI:NL:RBBRE:2008:BC8241
Rb. Middelburg 23 april 2008 ECLI:NL:RBMID:2008:BD0409
Rb. Dordrecht 3 juli 2008 ECLI:NL:RBDOR:2008:BD6243
Rb. Assen 22 juli 2008 ECLI:NL:RBASS:2008:BD8451
Rb. Arnhem 5 september 2008 ECLI:NL:RBARN:2008:BE9908
Rb. Groningen 3 november 2008 ECLI:NL:RBGRO:2008:BG3284
Rb. Almelo 30 december 2008 ECLI:NL:RBALM:2008:BG8562

Rb. Maastricht 2 februari 2009 ECLI:NL:RBMAA:2009:BK1160
Rb. Maastricht 6 april 2009 ECLI:NL:RBMAA:2009:BI4842
Rb. Roermond 8 april 2009 ECLI:NL:RBROE:2009:BI2037
Rb. 's-Hertogenbosch 23 april 2009 ECLI:NL:RBSHE:2009:BI1886
Rb. 's-Gravenhage 8 juni 2009 ECLI:NL:RBSGR:2009:BI7328
Rb. Zutphen 26 juni 2009 ECLI:NL:RBZUT:2009:BJ0009
Rb. Zutphen 3 juli 2009 ECLI:NL:RBZUT:2009:BJ1414
Rb. Almelo 18 augustus 2009 ECLI:NL:RBALM:2009:BJ6223
Rb. Haarlem 15 september 2009 ECLI:NL:RBHAA:2009:BL7294
Rb. Dordrecht 17 september 2009 ECLI:NL:RBDOR:2009:BJ8215
Rb. Assen 29 november 2009 ECLI:NL:RBASS:2009:BK4226
Rb. Amsterdam 30 november 2009 ECLI:NL:RBAMS:2009:BK4742
Rb. Zutphen 1 december 2009 ECLI:NL:RBZUT:2009:BK4976
Rb. Maastricht 8 december 2009 ECLI:NL:RBMAA:2009:BK6187
Rb. Zwolle-Lelystad 17 december 2009 ECLI:NL:RBZLY:2009:BL0027

Rb. 's-Gravenhage 29 januari 2010 ECLI:NL:RBSGR:2010:BL1143
Rb. Arnhem 25 februari 2010 ECLI:NL:RBARN:2010:BL5523
Rb. Haarlem 13 maart 2010 ECLI:NL:RBHAA:2010:BL8051
Rb. Assen 23 april 2010 ECLI:NL:RBASS:2010:BM2269
Rb. Arnhem 4 mei 2010 ECLI:NL:RBARN:2010:BM3281
Rb. Arnhem 2 juni 2010 ECLI:NL:RBARN:2010:BM6703
Rb. Zutphen 23 juni 2010 ECLI:NL:RBZUT:2010:BM8948
Rb. Zutphen 23 juni 2010 ECLI:NL:RBZUT:2010:BM8951
Rb. Leeuwarden 23 juli 2010 ECLI:NL:RBLEE:2010:BN2401
Rb. Breda 12 oktober 2010 ECLI:NL:RBBRE:2010:BO0111
Rb. Haarlem 29 oktober 2010 ECLI:NL:RBHAA:2010:BO8294

Rb. Breda 25 maart 2011 ECLI:NL:RBBRE:2011:BP9283
Rb. Zwolle-Lelystad 14 april 2011 ECLI:NL:RBZLY:2011:BR1716
Rb. Zwolle-Lelystad 14 april 2011 ECLI:NL:RBZLY:2011:BR1736
Rb. Assen 19 april 2011 ECLI:NL:RBASS:2011:BQ4020
Rb. Maastricht 11 mei 2011 ECLI:NL:RBMAA:2011:BQ4797
Rb. Alkmaar 26 mei 2011 ECLI:NL:RBALK:2011:BR4481
Rb. Zutphen 18 oktober 2011 ECLI:NL:RBZUT:2011:BT8503

Rb. Zwolle-Lelystad 7 november 2011 ECLI:NL:RBZLY:2011:BU5753
Rb. Utrecht 17 november 2011 ECLI:NL:RBUTR:2011:BV1498
Rb. Utrecht 17 november 2011 ECLI:NL:RBUTR:2011:BV1510
Rb. Utrecht 17 november 2011 ECLI:NL:RBUTR:2011:BV1594

Rb. Breda 29 februari 2012 ECLI:NLRBBRE:2012:BV7195
Rb. Assen 20 maart 2012 ECLI:NL:RBASS:2012:BV9321
Rb. Gelderland 7 augustus 2012 ECLI:NL:RBGEL:2012:BX3786

Rb. Oost-Nederland 19 februari 2013 ECLI:NL:RBONE:2013:BZ1862
Rb. Noord-Nederland 25 februari 2013 ECLI:NL:RBNNE:2013:2415
Rb. Midden-Nederland 25 maart 2013 ECLI:NL:RBMNE:2013:CA1872
Rb. Midden-Nederland 25 maart 2013 ECLI:NL:RBMNE:2013:CA1885
Rb. Overijssel 2 april 2013 ECLI:NL:RBOVE:2013:BZ6029
Rb. Noord-Holland 29 april 2013 ECLI:NL:RBNHO:2013:BZ9266
Rb. Gelderland 28 mei 2013 ECLI:NL:RBGEL:2013:BZ9709
Rb. Overijssel 17 juni 2013 ECLI:NL:RBOVE:2013:CA3835
Rb. Den Haag 3 juli 2013 ECLI:NL:RBDHA:2013:8128
Rb. Zeeland-West-Brabant 8 november 2013 ECLI:NL:RBZWB:2013:8025
Rb. Amsterdam 22 november 2013 ECLI:NL:RBAMS:2013:7777
Rb. Noord-Holland 2 december 2013 ECLI:NL:RBNHO:2013:11557
Rb. Den Haag 20 december 2013 ECLI:NL:RBDHA:2013:19224
Rb. Gelderland 24 december 2013 ECLI:NL:RBGEL:2013:6182

Rb. Den Haag 22 april 2014 ECLI:NL:RBDHA:2014:2641
Rb. Overijssel 2 mei 2014 ECLI:NL:RBOVE:2014:2378
Rb. Den Haag 20 juni 2014 ECLI:NL:RBDHA:2014:7979
Rb. Amsterdam 1 september 2014 ECLI:NL:RBAMS:2014:5735
Rb. Den Haag 26 september 2014 ECLI:NL:RBDHA:2014:11793
Rb. Zeeland-West-Brabant 16 oktober 2014 ECLI:NL:RBZWB:2014:7103

Rb. Overijssel 18 februari 2015 ECLI:NL:RBOVE:2015:845
Rb. Noord-Nederland 26 februari 2015 ECLI:NL:RBNNE:2015:3023
Rb. Noord-Nederland 3 maart 2015 ECLI:NL:RBNNE:2015:897
Rb. Noord-Holland 16 maart 2015 ECLI:NL:RBNHO:2015:2180
Rb. Den Haag 30 maart 2015 ECLI:NL:RBDHA:2015:3710
Rb. Limburg 29 april 2015 ECLI:NL:RBLIM:2015:3669
Rb. Midden-Nederland 1 mei 2015 ECLI:NL:RBMNE:2015:3908
Rb. Overijssel 3 juni 2015 ECLI:NL:RBOVE:2015:2677
Rb. Gelderland 17 juni 2015 ECLI:NL:RBGEL:2015:3966
Rb. Gelderland 17 juni 2015 ECLI:NL:RBGEL:2015:3967
Rb. Limburg 7 juli 2015 ECLI:NL:RBLIM:2015:6353
Rb. Limburg 27 juli 2015 ECLI:NL:RBLIM:2015:6360
Rb. Midden-Nederland 4 augustus 2015 ECLI:NL:RBMNE:2015:5831
Rb. Noord-Nederland 2 oktober 2015 ECLI:NL:RBNNE:2015:4656
Rb. Den Haag 16 november 2015 ECLI:NL:RBDHA:2015:13050
Rb. Den Haag 16 november 2015 ECLI:NL:RBDHA:2015:13065
Rb. Noord-Nederland 26 november 2015 ECLI:NL:RBNNE:2015:6400
Rb. Noord-Nederland 26 november 2015 ECLI:NL:RBNNE:2015:6401
Rb. Den Haag 18 december 2015 ECLI:NL:RBDHA:2015:15159

Rb. Overijssel 26 januari 2016 ECLI:NL:RBOVE:2016:213
Rb. Den Haag 11 februari 2016 ECLI:NL:RBDHA:2016:1388
Rb. Noord-Nederland 26 februari 2016 ECLI:NL:RBNNE:2016:825
Rb. Oost-Brabant 29 april 2016 ECLI:NL:RBOBR:2016:1811

Rb. Noord-Nederland 19 april 2016 ECLI:NL:RBNNE:2016:2104
Rb. Rotterdam 30 juni 2016 ECLI:NL:RBROT:2016:4946
Rb. Gelderland 1 augustus 2016 ECLI:NL:RBGEL:2016:4531
Rb. Overijssel 13 september 2016 ECLI:NL:RBOVE:2016:3429
Rb. Midden-Nederland 1 november 2016 ECLI:NL:RBMNE:2016:5781
Rb. Gelderland 18 november 2016 ECLI:NL:RBGEL:2016:6275
Rb. Oost-Brabant 7 december 2016 ECLI:NL:RBOBR:2016:6767

Rb. Noord-Nederland 16 februari 2017 ECLI:NL:RBNNE:2017:565
Rb. Midden-Nederland 24 februari 2017 ECLI:NL:RBMNE:2017:904
Rb. Noord-Nederland 15 maart 2017 ECLI:NL:RBNNE:2017:909
Rb. Noord-Nederland 15 maart 2017 ECLI:NL:RBNNE:2017:917