Wetenschappelijk Onderzoek- en Datacentrum

Evaluatie Wet Computercriminaliteit III

Een empirisch onderzoek naar de toepassing in de praktijk

Cahier 2025-10

A. van Uden
N. Nijhuis
M. van der Meer

Evaluatie Wet Computercriminaliteit III

Een empirisch onderzoek naar de toepassing in de praktijk

Cahier 2025-10

A. van Uden
N. Nijhuis
M. van der Meer[1]

[1] Deze auteur is alleen inhoudelijk verantwoordelijk voor hoofdstuk 5.

Cahier
De reeks Cahier omvat de rapporten van onderzoek dat door en in opdracht van het Wetenschappelijk Onderzoek- en Datacentrum is verricht. Opname in de reeks betekent niet dat de inhoud van de rapporten het standpunt van de Minister van Justitie en Veiligheid weergeeft.

Inhoud

Begrippenlijst **7**

Samenvatting **11**

1 Inleiding **23**
1.1 Wijzigingen Wetboek van Strafrecht 23
1.1.1 Stelen van gegevens 23
1.1.2 Helen van gegevens 23
1.1.3 Inzet van een lokpuber bij verleiden minderjarigen en grooming 24
1.1.4 Online handelsfraude 24
1.2 Wijzigingen Wetboek van Strafvordering 25
1.2.1 Ontoegankelijkmaking van gegevens 25
1.2.2 Hackbevoegdheid 25
1.3 Centrale vraagstelling 26
1.4 Methoden van onderzoek 27
1.4.1 Documentanalyse 27
1.4.2 Analyse RAC-min 27
1.4.3 Vonnisanalyse 29
1.4.4 Topic-gestuurde interviews 31
1.4.5 Vragenlijst 33
1.4.6 Analyse 34
1.5 Opbouw rapport 35

2 Stelen van gegevens (art. 138c Sr) **36**
2.1 Juridisch kader 36
2.2 Noodzaak en veronderstellingen 36
2.3 Artikel 138c Sr in de praktijk 38
2.3.1 Instroom en afdoening Openbaar Ministerie 38
2.3.2 Vonnissen rechtbank 39
2.3.3 Aard artikel 138c Sr-zaken 39
2.3.4 Voordelen voor de opsporingspraktijk 43
2.3.5 Aandachtspunten 45
2.4 Tot slot 46

3 Helen van gegevens (art. 139g Sr) **48**
3.1 Juridisch kader 48
3.2 Noodzaak en veronderstellingen 49
3.3 Artikel 139g Sr in de praktijk 50
3.3.1 Instroom en afdoening Openbaar Ministerie 50
3.3.2 Vonnissen rechtbank 52
3.3.3 Aard artikel 139g Sr zaken 53
3.3.4 Voordelen voor de opsporingspraktijk 61
3.3.5 Aandachtspunten 63
3.4 Tot slot 70

4 Online handelsfraude (art. 326e Sr) **72**
4.1 Juridisch kader 72
4.2 Noodzaak en veronderstellingen 73

4.3	Artikel 326e Sr in de praktijk	74
4.3.1	LMIO en aangiften bij de politie	74
4.3.2	Instroom en afdoening Openbaar Ministerie	75
4.3.3	Vonnissen rechtbank	77
4.3.4	Aard artikel 326e Sr-zaken	77
4.3.5	Slachtoffers, benadeelden en schade	89
4.3.6	Aanpak van online handelsfraude	90
4.3.7	Voordelen voor de opsporingspraktijk	93
4.3.8	Aandachtspunten	94
4.4	Tot slot	101
5	**De 'lokpuber' in artikel 248e Sr en artikel 248a Sr**	**103**
5.1	Juridisch kader	103
5.1.1	Wet seksuele misdrijven	104
5.2	Noodzaak en veronderstellingen	105
5.3	De lokpuber in de praktijk	106
5.3.1	Zakenanalyse	106
5.3.2	Redenen voor een inzet van de lokpuber	107
5.3.3	Voordelen voor de opsporingspraktijk	109
5.3.4	Aandachtspunten	110
5.4	Tot slot	115
6	**Ontoegankelijkmaking van gegevens (art. 125p Sv)**	**117**
6.1	Juridisch kader	117
6.2	Noodzaak en veronderstellingen	118
6.3	Artikel 125p Sv in de praktijk	120
6.3.1	Notice-and-Takedownprocedure en artikel 125p Sv	121
6.3.2	Aard artikel 125p Sv zaken	122
6.3.3	Voordelen voor de opsporingspraktijk	126
6.3.4	Aandachtspunten	128
6.4	Tot slot	137
7	**Hackbevoegdheid (artt. 126nba, 126zpa en 126uba Sv)**	**140**
7.1	Juridisch kader	140
7.2	Noodzaak en veronderstellingen	143
7.2.1	Technologische ontwikkelingen	143
7.2.2	Bezwaren ten aanzien van andere bevoegdheden	145
7.3	Hackbevoegdheid in de praktijk	146
7.3.1	Aard artikel 126nba Sv zaken	147
7.3.2	Opbrengst hackbevoegdheid	155
7.3.3	Behandeling door de rechtbank	163
7.3.4	Voordelen voor de opsporingspraktijk	167
7.3.5	Aandachtspunten	168
7.4	Sporenaanpak in de beleidsbrief	173
7.4.1	Wijze van binnendringen – steunbevoegdheid	173
7.4.2	Inzet van commerciële middelen	173
7.4.3	Meldplicht onbekende kwetsbaarheden	174
7.4.4	Toezicht door de Inspectie JenV	174
7.4.5	Keuring van technische hulpmiddelen	176
7.5	Tot slot	178

8 Conclusie 181
8.1 Stelen van gegevens (art. 138c Sr) 182
8.2 Helen van gegevens (art. 139g Sr) 182
8.3 Online handelsfraude (art. 326e Sr) 183
8.4 Lokpuber (artt. 248a en 248e Sr) 184
8.5 Ontoegankelijk maken van gegevens (art. 125p Sv) 185
8.6 Hackbevoegdheid (artt. 126nba, 126uba en 126zpa Sv) 186
8.7 Slotbeschouwing 188
8.7.1 Nieuwe ontwikkelingen 188
8.7.2 Beschikbare capaciteit 190
8.7.3 Zaken met een internationale component 190
8.7.4 (Rechtsstatelijke) waarborgen 191

Summary 193

Literatuur 204

Bijlage 1 Samenstelling begeleidingscommissie 208

Bijlage 2 Werkwijze en selectie interviews 209

Bijlage 3 Zoektermen en selectie vonnissen 213

Bijlage 4 Vragenlijst inzet hackbevoegdheid 218

Bijlage 5 Soorten misdrijven hackbevoegdheid 225

Begrippenlijst

In deze lijst staat een opsomming gegeven van de belangrijkste begrippen inclusief een uitleg wat deze begrippen inhouden. Daarbij is niet altijd de juridische definitie gevolgd.

Begrip	**Uitleg**
ATKM:	Autoriteit online Terroristisch en Kinderpornografisch Materiaal
Bitcoin:	Een digitale munt.
Botnet:	Een verzameling van besmette systemen die door actoren centraal bestuurd kan worden. Botnets vormen de infrastructuur voor veel vormen van internetcriminaliteit.
Bug:	Een kleine microfoon die in staat is opgenomen signalen draadloos te verzenden.
Bulletproof hoster:	Een bedrijf dat de mogelijkheid biedt volledig anoniem gebruik te maken van serverruimte en er daarmee van verdacht wordt bewust criminaliteit te faciliteren.
Centrale Toetsingscommissie:	De CTC is een intern adviesorgaan binnen het Openbaar Ministerie dat advies geeft aan het College van Procureurs-Generaal over onder andere de voorgenomen inzet van enkele bijzondere opsporingsbevoegdheden.
Cloud computing:	Het leveren van computerdiensten, zoals servers, opslag, databases, netwerken, software, analyses en meer, via internet (de 'cloud'), in plaats van fysieke hardware.
Combolijsten:	Ook wel bekend als een combinatielijst. Een bestand met een verzameling van gebruikersnamen of e-mailadressen en bijbehorende wachtwoorden.
Cryptocommunicatiedienst:	Een communicatiedienst waarmee gebruikers elkaar heimelijk versleutelde berichten kunnen sturen, buiten het zicht van politie en justitie om.
Cryptovaluta:	Digitale of virtuele valuta binnen een gedecentraliseerd systeem zonder een centrale bank of overheid als tussenpersoon.

Cryptovalutascam:	Een vorm van oplichting, waarbij oplichters misleiding gebruiken om bijvoorbeeld toegang te krijgen tot iemands cryptovaluta tegoeden of proberen frauduleuze cryptovaluta te verkopen.
Cyberpesten:	Online pesten.
Dark web:	Deel van het internet wat niet via zoekmachines gevonden kan worden en enkel via speciale browsers (zoals TOR) bezocht kan worden.
Geautomatiseerd werk:	'Een apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerken' (art. 80sexies Sr). Voorbeelden van geautomatiseerde werken zijn servers, computers, routers, tablets en smartphones.
Gedragscode Notice-and-Take-Down:	Deze gedragscode regelt dat tussenpersonen die in Nederland een openbare telecommunicatiedienst aanbieden op het internet ervoor kunnen zorgen dat 'onmiskenbaar onrechtmatige of strafbare inhoud' kan worden verwijderd.
Infostealer:	Een vorm van malware die persoonlijke gegevens verzamelt voor criminele doeleinden.
IP:	Het internetprotocol dat zorgt voor de adressering van internetverkeer zodat het bij het beoogde doel aankomt.
Keuring en keuringsdienst:	Technische hulpmiddelen moeten (voorafgaand aan de inzet ervan) worden gekeurd. Tijdens de keuring wordt gekeken of een technisch hulpmiddel voldoet aan de in het Besluit gestelde eisen met betrekking tot de betrouwbaarheid, integriteit en herleidbaarheid van gegevens. De Keuringsdienst, onderdeel van de Landelijke eenheid van de Nationale politie, neemt de keuring van technische hulpmiddelen voor haar rekening.
Keylogger:	Een keylogger registreert toetsaanslagen en/of muisbewegingen van een computer.
Kwetsbaarheid:	Een zwakke plek in hard- of software waardoor het voor derden mogelijk kan worden om op een geautomatiseerd werk binnen te komen. Kwetsbaarheden moeten dan wel eerst gebruiksklaar gemaakt zijn. Drie soorten kwetsbaarheden kunnen worden onderscheiden: bekende, bekende onbekende en onbekende onbekende kwetsbaarheden.

Leads:	Digitale lijsten met persoonsgegevens.
Lex specialis:	Latijnse benaming voor bijzondere wetgeving. Een juridisch principe dat regelt dat een bijzondere wet (een lex specialis) voorrang krijgt boven de algemene wetgeving.
Malware:	Samentrekking van kwaadaardige software. Malware is de term die als generieke aanduiding wordt gebruikt voor onder andere virussen, wormen en trojans.
Onbekende kwetsbaarheid:	Een kwetsbaarheid die nog niet wordt verspreid en dus niet bij het grote publiek bekend kan zijn. Ook is er nog geen update voor de kwetsbaarheid beschikbaar, omdat de fabrikant nog niet de tijd heeft gehad (nul dagen) om die te ontwikkelen. Tot het moment van verspreiden is sprake van een zero day. Ook zo'n kwetsbaarheid kan gebruikt worden om een geautomatiseerd werk binnen te dringen.
Paydate:	Een afspraak waarbij geld wordt betaald voor seksuele handelingen.
Payment Service Provider:	Een derde partij die webshops en andere ondernemingen voorziet van digitale betaalmogelijkheden.
Pedojager:	Een burger die zich voordoet als minderjarige op het internet om verdachten van kindermisbruik op te sporen.
Phishing:	Verzamelnaam voor digitale activiteiten die tot doel hebben informatie aan mensen te ontfutselen. Deze informatie kan worden misbruikt voor bijvoorbeeld toegang tot systemen.
Phishing panel:	Een web-tool die cybercriminelen gebruiken om hun phishing-aanvallen te beheren en de gestolen gegevens te volgen.
RAC-min:	Een deelverzameling van het Rapsody Centraal systeem waarin informatie staat over alle zaken die bij het Openbaar Ministerie instromen en over de afhandeling van die zaken door het Openbaar Ministerie en door de rechter in eerste aanleg.
Ransomware:	Gijzelsoftware. Type malware dat systemen of informatie daarop blokkeert en alleen tegen betaling van losgeld weer toegankelijk maakt.

Reseller:	Een communicatiedienstaanbieder die een server huurt van een (meestal grotere) communicatiedienstaanbieder en deze vervolgens doorverhuurt aan klanten, vaak met een kleine winstmarge.
Seed phrases:	Een reeks willekeurige woorden die de benodigde gegevens opslaat om toegang te krijgen tot of cryptovaluta te herstellen.
Sexchatting:	Het online seksueel benaderen van minderjarigen.
Sextortion:	Manier van afpersen waarbij gedreigd wordt met het openbaren van seksueel getint materiaal.
Spoofing:	Een vorm van fraude waarbij iets of iemand een valse identiteit aanneemt door zich voor te doen als iets of iemand anders, bijvoorbeeld door een e-mail te verzenden vanuit een e-mailadres dat niet echt van de verzender is.
Tallon-criterium:	Het criterium dat stelt dat de politie een verdachte niet mag uitlokken om een strafbaar feit te plegen dat buiten het oorspronkelijke opzet van de verdachte valt.
Technisch hulpmiddel:	Een middel, doorgaans software, waarmee Digit data die relevant zijn voor een tactisch onderzoek (denk aan chatberichten, e-mails, geluidsbestanden), ophaalt bij de verdachte en opslaat in de digitale omgeving van Digit.
TOR-browser:	Een speciale browser waarmee anoniem pagina’s op het dark web bezocht kunnen worden.
Versleuteling:	Ook wel encryptie genoemd. Manier van beveiligen van digitale bestanden.
ZSM:	Zorgvuldig Snel en op Maat. Afdoeningsroute binnen het Openbaar Ministerie.

Samenvatting

Op 1 maart 2019 is de Wet Computercriminaliteit III (Wet CCIII) in werking getreden. Met deze Wet zijn zeven nieuwe/aangepaste wettelijke bepalingen geïntroduceerd: vijf strafbaarstellingen en twee (bijzondere) opsporingsbevoegdheden. Bij de strafbaarstellingen gaat het om het stelen van gegevens (art. 138c Sr), het helen van gegevens (art. 139g Sr), online handelsfraude (art. 326e Sr), verleiding van een minderjarige (art. 248a Sr) en *grooming* (art. 248e Sr). De twee nieuwe bevoegdheden zien op de ontoegankelijkmaking van gegevens (art. 125p Sv) en de hackbevoegdheid (artt. 126nba, 126uba en 126zpa Sv). De Wet is een opvolger van de Wet computercriminaliteit I en II en werd nodig geacht omdat daarmee 'het juridisch instrumentarium voor de opsporing en vervolging van computercriminaliteit zou kunnen worden versterkt' (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 2). Eerder verscheen een evaluatierapport (Van Uden & Van den Eeden, 2022) over de wijze waarop één bepaling uit de Wet CCIII, de hackbevoegdheid in de praktijk werd toegepast. Dit rapport bevat een evaluatie van de gehele Wet CCIII, inclusief de hackbevoegdheid. De volgende onderzoekvraag stond centraal:

> In hoeverre worden de doelstellingen zoals geformuleerd in de Wet CCIII in de praktijk gerealiseerd?

Ter beantwoording van deze onderzoeksvraag zijn drie deelvragen geformuleerd.

1 Wat is het doel van de verschillende bepalingen van de Wet CCIII en welke veronderstellingen liggen aan die bepalingen ten grondslag?
2 Hoe wordt in de praktijk uitvoering gegeven aan de verschillende bepalingen van de Wet CCIII?
3 Welke gevolgen (zowel bedoeld als onbedoeld) hebben de verschillende bepalingen van de Wet CCIII voor de opsporingspraktijk?

Om deze onderzoeksvragen te beantwoorden is een combinatie van onderzoeksmethoden gebruikt: documentanalyse, cijfermatige analyse van juridische databestanden (RAC-min), interviews, vonnisanalyse en een vragenlijst. In deze samenvatting wordt een beschrijving gegeven van de belangrijkste bevindingen en conclusies. Per wettelijke bepaling wordt aandacht besteed aan de veronderstelling van de wetgever over de noodzaak en werking van de bepaling. Hieronder worden ook de doelstellingen van de wetgever met de invoering van de wettelijke bepaling begrepen. Verder wordt de aandacht gericht op de uitvoering in de praktijk en de gevolgen voor onder andere de opsporingspraktijk, zowel bedoeld als onbedoeld. Per wettelijke bepaling wordt daarnaast stil gestaan bij de voordelen die de betreffende bepaling de opsporingspraktijk biedt. Ook zal aandacht worden besteed aan aandachtspunten voor diezelfde opsporingspraktijk. Er is gekozen om elke strafbaarstelling apart te bespreken, omdat de nieuwe/aangepaste wettelijke bepalingen diverse thema's beslaan die lang niet altijd nauw met elkaar samenhangen.

Voorafgaand hieraan nog het volgende. In dit onderzoek is een combinatie van onderzoeksmethoden gebruikt. Een combinatie van onderzoeksmethoden komt de validiteit van het onderzoek ten goede. Voor de vonnisanalyse zijn alle vonnissen bekeken, althans voor zover die beschikbaar waren. Op die manier is een zo volledig mogelijk beeld verkregen van de toepassing van vooral de strafbaarstellingen.

Bovendien beschikten wij ook over vonnissen die niet gepubliceerd zijn. Dat is een belangrijke meerwaarde van deze evaluatie.

Wat betreft de afgenomen interviews is voor sommige wettelijke bepalingen met een relatief klein aantal personen gesproken wanneer dat aantal vergeleken wordt met het totaal aantal zaken waarin de wettelijke bepaling voorkwam. Deels was dit een bewuste keuze, omdat we ook andere onderzoeksmethoden gebruikten. Deels is het niet gelukt om meer mensen te spreken, bijvoorbeeld omdat er geen reactie kwam op het interviewverzoek. Tegelijkertijd spraken we onder meer met personen voor wie de thema's waarop de wettelijke bepaling zich richtte hun specialisatie was, denk bijvoorbeeld aan de hackbevoegdheid en het helen en stelen van gegevens. Ondanks de beperkte omvang van het aantal interviews, leveren de resultaten betrouwbare en relevante inzichten op.

Stelen van gegevens (art. 138c Sr)

Artikel 138c Sr regelt dat het strafbaar is om gegevens over te nemen. Een belangrijke veronderstelling van de wetgever was dat gegevens door artikel 138c Sr beter zouden worden beschermd tegen misbruik ervan. In deze evaluatie is duidelijk geworden dat verdachten vervolgd zijn voor het overnemen van gegevens. In dat opzicht zijn gegevens in de praktijk beter beschermd, omdat voor verdachten een risico op vervolging bestaat. Of de nieuwe wettelijke bepaling daadwerkelijk een afschrikwekkende werking heeft, kan op basis van deze evaluatie niet worden gezegd.

In de periode maart 2019-april 2024 zijn 39 zaken ingestroomd bij het Openbaar Ministerie en in 15 zaken heeft de rechter een uitspraak gedaan. In 2 zaken is de zaak afgedaan met een OM-beschikking en in 13 zaken is de verdachte veroordeeld voor het 138c-feit. In bijna alle gevallen ging het om werknemers die in een werksituatie gegevens hadden overgenomen. In de meeste zaken is het overnemen niet het enige feit dat ten laste werd gelegd. Het feit werd bijvoorbeeld ten laste gelegd met misdrijven in de (relationele) levenssfeer. In de 138c Sr-zaken ging het vooral om persoonlijke gegevens (persoonsgegevens en foto's en afbeeldingen). In alle gevallen ging het om computercriminaliteit in brede zin, namelijk traditionele criminaliteit gepleegd met een ICT-middel. Meestal werden persoonlijke gegevens (persoonsgegevens en foto's en afbeeldingen) gestolen. Het is niet altijd duidelijk geworden hoeveel gegevens zijn gestolen. Doorgaans ging het niet om grote aantallen. Een uitzondering hierop vormden de enkele honderden buitenlandse telefoonnummers die waren overgenomen.

Het nieuwe wetsartikel biedt de opsporingspraktijk en soms ook burgers een aantal voordelen. Zo hebben slachtoffers van gestolen gegevens de mogelijkheid om zich te voegen in een strafzaak en kan uitgebreider opsporingsonderzoek worden gedaan. Een andere mogelijkheid, zo blijkt uit de evaluatie, is dat er een juridische omschrijving is gekomen die goed past bij situaties waarin een persoon die rechtmatig toegang heeft tot gegevens deze wederrechtelijk overneemt. Daarbij moet meteen worden opgemerkt dat de rechtspraak zich inmiddels verder heeft ontwikkeld. In de wetsgeschiedenis komt naar voren dat artikel 138ab Sr (computervredebreuk) niet geschikt werd bevonden voor de overname van gegevens in werksituaties. Inmiddels heeft de Hoge Raad meerdere arresten gewezen waaruit blijkt dat ook in werksituaties sprake kan zijn van computervredebreuk waardoor niet altijd gekozen zal worden voor artikel 138c Sr. In die situaties is een belangrijke aanleiding voor artikel 138c Sr dus

niet meer altijd aanwezig. Tegelijkertijd wordt met betrekking tot dit soort zaken ook de vraag gesteld of het begrip computervredebreuk niet te ver wordt opgerekt (zie Berndsen & Visser, 2022, p. 163).

Daarnaast komt een aantal aandachtspunten naar voren. Zo blijkt uit de evaluatie dat afhankelijk van het soort gegevens dat wordt overgenomen, de strafmaat niet in alle situaties passend wordt gevonden. Ook is het niet altijd gemakkelijk om het bestanddeel 'wederrechtelijk' aan te tonen. Tot slot is een aandachtspunt dat het bij artikel 138c Sr moet gaan om het overnemen van gegevens die zijn opgeslagen op een geautomatiseerd werk. Gegevens overgenomen van papier vallen hier niet onder.

Helen van gegevens (art. 139g Sr)

Op basis van artikel 139g Sr is het strafbaar geworden om gegevens te helen. Een belangrijke veronderstelling van de wetgever was dat door de komst van artikel 139g Sr gegevens beter strafrechtelijk zouden worden beschermd tegen misbruik ervan. In deze evaluatie is duidelijk geworden dat verdachten vervolgd zijn voor het helen van gegevens. In dat opzicht zijn gegevens in de praktijk beter beschermd, omdat voor verdachten een risico op vervolging bestaat. Of de nieuwe wettelijke bepaling daadwerkelijk een afschrikwekkende werking heeft, kan op basis van deze evaluatie niet worden gezegd.

In de periode maart 2019-april 2024 zijn 93 zaken ingestroomd bij het Openbaar Ministerie. In 85 zaken was artikel 139g Sr het enige CCIII-feit in de tenlastelegging en in 8 zaken was sprake van een combinatie van CCIII-feiten, namelijk artikel 139g Sr gecombineerd met artikel 138c Sr of met artikel 326e Sr. In 42 zaken was een eindvonnis beschikbaar. In een ruime meerderheid van die zaken (36) is de verdachte veroordeeld voor het 139g-feit en legde de rechter een straf op. In de meeste zaken waarin artikel 139g Sr ten laste is gelegd draaide het, naast het helen van (vooral) offline en online persoonlijke gegevens, om meerdere feiten. In ruim de helft van de zaken in de vonnisanalyse kwam het artikel samen voor met een vorm van fraude waardoor burgers financieel benadeeld werden. Soms waren het helen van gegevens en de andere feiten direct aan elkaar gerelateerd. Dat wil zeggen dat de geheelde gegevens gebruikt zijn voor het plegen van (een deel van) de andere feiten die in de tenlastelegging zijn opgenomen, bijvoorbeeld geheelde gegevens die gebruikt werden voor fraude. Het aantal gegevens dat geheeld wordt, loopt sterk uiteen, al is niet altijd duidelijk geworden om hoeveel gegevens het ging. Wanneer een 139g-zaak datasets met persoonsgegevens betreft kan het gaan om grote aantallen. Bij andersoortige gegevens, zoals fotomateriaal, zijn die aantallen doorgaans kleiner. Dat laatste zegt overigens niets over de mogelijke impact op het slachtoffer.

Voor de opsporingspraktijk biedt de nieuwe wettelijke bepaling een aantal voordelen. Ten eerste past artikel 139g Sr bij helingsgedragingen die in de praktijk worden gezien. Bovendien maakt dit artikel verbeurdverklaring en ontneming van witgewassen bedragen mogelijk. Ook is artikel 139g Sr behulpzaam bij de aanpak van de gehele keten rondom bankfraudezaken, omdat geheelde gegevens worden gebruikt om bankfraude te plegen. Bovendien maakt artikel 139g Sr het mogelijk een verdenking te creëren in zaken waarin dat vóór de komst van het artikel niet mogelijk was. Hierdoor kunnen opsporingsonderzoeken worden gestart die voorheen niet opgestart konden worden.

De evaluatie van dit artikel heeft ook een aantal aandachtspunten zichtbaar gemaakt. Twee belangrijke worden op deze plek uitgelicht. Het eerste aandachtspunt gaat over de strafmaat van één jaar. Wetstechnisch lijkt dit geen logisch keuze, omdat op het helen van goederen een hogere strafmaat staat. Bovendien laat de praktijk zien dat er grote variatie bestaat wat betreft het aantal gegevens dat gestolen kan worden. Het is de vraag of de strafmaat van één jaar in alle gevallen passend is.

Het tweede aandachtspunt heeft betrekking op het kunnen veroordelen voor het helen van gegevens, als deze gegevens door een eigen misdrijf verkregen zijn (naar analogie van de heler-steler-regel). De jurisprudentie laat zien dat rechters verschillend oordelen over dit punt. Mogelijk wordt in de toekomst nog verder doorgeprocedeerd over de vraag of de heler-steler regel ook van toepassing is wanneer gegevens geheeld worden.

Online handelsfraude (art. 326e Sr)

Op basis van artikel 326e Sr is het strafbaar geworden om online handelsfraude te plegen. Een belangrijke veronderstelling van de wetgever was dat met de komst van artikel 326e Sr online handelsfraude strafrechtelijk vervolgd kon worden, en dan vooral grootschalige vormen van online handelsfraude. Hoewel in een groot aantal zaken, vooral vanwege capaciteitsoverwegingen, besloten is niet tot vervolging over te gaan, zijn op basis van artikel 326e Sr verdachten vervolgd en veroordeeld. In deze zaken was echter nauwelijks sprake van zogenoemde grootschalige online handelsfraude.

In de periode maart 2019-april 2024 zijn 279 zaken ingestroomd bij het Openbaar Ministerie. In 91 zaken heeft de rechter een uitspraak gedaan, waarvan in ruime meerderheid van de zaken de verdachte is vervolgd voor ten minste één 326e Sr-feit. Uit de vonnisanalyse volgt dat in een grote meerderheid van de geanalyseerde vonnissen online handelsfraude samen ten laste is gelegd met andere feiten. Oplichting kwam het vaakst voor, gevolgd door witwassen. In bijna al deze zaken ging het om witwassen van geld verdiend met online handelsfraude.

In de geanalyseerde vonnissen ging het voornamelijk om de frauduleuze verkoop van goederen. Ook kon het gaan om het aanbieden van online diensten. Gemiddeld lag het schadebedrag in de bewezenverklaring rond 2.000 euro per zaak. Het gemiddelde aantal slachtoffers in de bewezenverklaring was vijftien personen per zaak. In bijna alle zaken in de vonnisanalyse is een schadevergoeding geëist. Dat slachtoffers zich konden voegen in een strafzaak was ook een veronderstelling van de wetgever. Een nuancering hierbij is dat het in de vonnisanalyse vooral om zaken ging waarin sprake was van fraude gepleegd middels bestaande online verkoopplatforms en niet om zaken waarin sprake was van tijdelijke websites die ook weer snel de lucht uit gingen. Bij tijdelijke websites is het lastig om een schadevergoeding te vorderen.

Het voorgaande laat zien dat artikel 326e Sr inderdaad gebruikt kan worden om online handelsfraude (succesvol) te vervolgen. Bovendien is artikel 326e Sr een *lex specialis*[2], specifiek toegespitst op online handelsfraude, wat de kwalificatie van online handelsfraude heeft vereenvoudigd. In lijn met de wens van de wetgever om de

[2] *Lex specialis* is de Latijnse benaming voor bijzondere wetgeving. Een juridisch principe dat regelt dat een bijzondere wet (een *lex specialis*) voorrang krijgt boven de algemene wetgeving. De algemene wetgeving in dit geval is artikel 326 Sr (gewone oplichting).

vervolging van online handelsfraude beter mogelijk te maken, is de nieuwe strafbaarstelling duidelijker, makkelijker toepasbaar en makkelijker bewijsbaar in vergelijking met gewone oplichting. Dat kan de vervolging van online handelsfraude vergemakkelijken.

Zoals gezegd wordt het nieuwe wetsartikel nauwelijks benut voor de aanpak van 'grootschalige online handelsfraude'. In de geanalyseerde vonnissen ontbreekt deze grootschaligheid veelal. Slechts in 3 van de 27 geanalyseerde zaken werd gesproken van 'grootschalige online handelsfraude'. Het is in deze evaluatie niet duidelijk geworden hoe het komt dat dit soort zaken slechts sporadisch naar voren kwam tijdens het onderzoek. Een mogelijke verklaring hiervoor is wellicht dat het bij grootschalige vormen van online handelsfraude lastig is om bij de 'echte' dader terecht te komen. Ook omdat dit extra opsporingscapaciteit vraagt die zoals geschreven niet altijd beschikbaar is. Het kan ook zijn dat er nog geen vonnis is gewezen, omdat opsporingsonderzoeken naar dit soort fenomenen meer tijd in beslag nemen en het dus langer duurt voordat een zittingsrechter zich over de zaak buigt. Ook zou het kunnen zijn dat dergelijke vormen van online handelsfraude niet bestaan, of dat deze zich vooral in het buitenland afspelen.

Deze evaluatie heeft ook laten zien dat artikel 326e Sr een tegenstrijdigheid in zich heeft. Enerzijds is het artikel eenvoudiger in vergelijking met het 'gewone' oplichtingsartikel waardoor vervolging van online handelsfraude gemakkelijker is geworden. Anderzijds is de beschikbare opsporingscapaciteit te beperkt om verdachten op basis van dit eenvoudigere artikel te vervolgen. In een groot aantal zaken heeft het Openbaar Ministerie besloten om niet tot vervolging over te gaan, en in het overgrote deel van deze zaken is een rechter, na een artikel 12-procedure, in deze beslissing meegegaan. De beperkte opsporingscapaciteit was hiervoor een belangrijke reden. Er zijn ook wegen buiten het strafrecht om waarmee online handelsfraude aangepakt wordt. Denk hierbij aan een stopgesprek met verdachten.

Naast de beschikbare opsporingscapaciteit en het ontbreken van grootschaligheid is er nog een aandachtspunt ten aanzien van de mogelijkheid tot vervolging op basis van artikel 326e Sr, namelijk de buitenlandcomponent. Wanneer in een online handelsfraudezaak sprake is van een buitenlandcomponent, bijvoorbeeld een buitenlandse leverancier of een buitenlands rekeningnummer, dan is vervolging ingewikkeld, omdat het lastig is om de identiteit van de verdachte te achterhalen. Ook dit is een belangrijke nuancering bij de veronderstelling van de wetgever. Als mogelijke oplossing voor zaken met een buitenlandcomponent wordt een koppeling tussen de verwijzingsportalen van elk Europees land afzonderlijk genoemd.

Lokpuber (artt. 248a en 248e Sr)

De aanpassingen van artikel 248a Sr (verleiding van een minderjarige) en artikel 248e Sr (*grooming*) hebben ervoor gezorgd dat de politie een lokpuber kan inzetten. Een belangrijke veronderstelling van de wetgever was dat minderjarigen beter konden worden beschermd door de artikelen 248a (verleiding minderjarige) en 248e Sr (*grooming*) op een zodanige manier te wijzigen dat de inzet van een lokpuber mogelijk werd. Deze evaluatie heeft laten zien dat het mogelijk is gebleken om een verdachte te veroordelen in een zaak waarin de lokpuber werd ingezet, maar dit is zeer sporadisch gebeurd. Of kinderen inderdaad beter kunnen worden beschermd valt op

basis van deze evaluatie niet te zeggen. Wel is duidelijk geworden dat de lokpuber hiervoor nauwelijks is benut.

In de periode maart 2019-april 2024 is er, voor zover bekend, slechts één zaak geweest waarin een verdachte is vervolgd voor het verleiden van een minderjarige en waarin gebruik is gemaakt van een lokpuber. Dit aantal is zeer klein in verhouding tot het aantal 248a- en 248e-zaken waarin de rechter een vonnis heeft uitgesproken (respectievelijk 92 en 58 zaken) en verdachten vervolgd zijn voor het verleiden van een minderjarige of *grooming*. Naast de zojuist genoemde zaak heeft de politie nog een aantal keer vaker met een lokpuber gewerkt. In deze zaken draaide het om andere artikelen dan de artikelen 248a en 248e Sr of is het niet duidelijk geworden of het deze artikelen betrof. Het is dus mogelijk gebleken om een lokpuber ook voor andere strafbare feiten in te zetten. Tot slot heeft de Landelijke Eenheid nog een pilot gedraaid om in de praktijk te onderzoeken hoe de inzet van de lokpuber vormgegeven zou kunnen worden en wat de mogelijkheden zouden zijn. Deze pilot heeft voor zover bekend niet geleid tot een concrete zaak.

De lokpuber is in de praktijk dus niet vaak ingezet. Belangrijke redenen hiervoor waren de beschikbare capaciteit en het feit dat er al genoeg 'brengzaken' zijn waarin voor andere opsporingswegen gekozen wordt. 'Brengzaken' zijn zaken waarin al een aangifte is gedaan en waarin eventueel al een verdachte bekend is. Hoewel de lokpuber in de praktijk niet vaak is ingezet, zijn er in de interviews verschillende mogelijkheden naar voren gekomen met betrekking tot de inzet van een lokpuber, waaronder een meer proactieve inzet van de lokpuber. In tegenstelling tot een 'brengzaak' hoeft er dan nog geen concrete verdachte op het oog te zijn. Een belangrijke voorwaarde hierbij is dat voldoende capaciteit beschikbaar is voor in elk geval de inzet van de lokpuber.

Sinds de inwerkingtreding van de Wet seksuele misdrijven (Wsm) op 1 juli 2024 bestaan de artikelen 248a en 248e Sr niet meer en zijn deze deels opgegaan in de Wsm. De inzet van de lokpuber blijft mogelijk, namelijk voor het seksueel corrumperen van een minderjarige en *sexchatting*. In dat opzicht kunnen de in dit onderzoek gesignaleerde aandachtspunten, bijvoorbeeld aandacht voor de grens met uitlokking, beperkte beschikbaarheid van capaciteit, het opstellen van een geloofwaardig profiel en bekendheid met de lokpuber binnen opsporingsorganisaties, van nut zijn voor de toepassing van de lokpuber in het kader van de nieuwe wet. De vraag is wel in hoeverre de lokpuber ook in het kader van deze nieuwe Wet benut zal worden. In 2024 was een stijging te zien van meldingen van seksuele delicten in vergelijking met 2023 en zijn 131 meldingen van *sexchatting* gedaan (Politie, 2025). Dat laat zien dat er genoeg 'brengzaken' zijn. In deze evaluatie werd duidelijk dat in die gevallen blijkbaar voor andere opsporingswegen wordt gekozen. Daarom lijkt het niet voor de hand te liggen dat de lokpuber in de toekomst vaker ingezet zal worden. Dit hoeft overigens geen probleem te zijn, zolang opsporingsfunctionarissen op de hoogte zijn dat de mogelijkheid van de lokpuber bestaat en er voldoende menskracht beschikbaar kan worden gesteld wanneer de inzet van de lokpuber noodzakelijk wordt geacht.

Ontoegankelijk maken van gegevens (art. 125p Sv)

Het nieuwe artikel 125p Sv ziet op het ontoegankelijk maken van gegevens. Een belangrijke veronderstelling van de wetgever was dat door de introductie van artikel

125p Sv, een bevoegdheid om via een aanbieder gegevens ontoegankelijk te maken, strafbare feiten sneller beëindigd zouden kunnen worden of zelfs voorkomen. Op die manier zou de samenleving beter worden beschermd. Deze evaluatie heeft laten zien dat gegevens ontoegankelijk zijn gemaakt op basis van artikel 125p Sv. In dat opzicht is het mogelijk gebleken, in lijn met de veronderstelling van de wetgever, strafbare content (tijdelijk) ontoegankelijk te maken. Op basis van deze evaluatie kan niet worden gezegd in hoeverre de samenleving hierdoor beter wordt beschermd. Deze evaluatie heeft ook laten zien dat aanbieders meer dan bereid zijn om op vrijwillige basis gegevens ontoegankelijk te maken. Het precieze aantal zaken waarvoor dit geldt is overigens niet duidelijk geworden. Én zijn er zaken waarin de bevoegdheid nog steeds niet volstaat. Dit zijn belangrijke nuanceringen bij de veronderstelling van de wetgever.

In veertien zaken zijn op basis van artikel 125p Sv gegevens ontoegankelijk gemaakt. Het betrof de ontoegankelijkmaking van filmpjes, malafide en illegale verkoopwebsites, IP-adressen met gehackte gegevens, Telegramgroepen waarin extremistische content werd verspreid en Telegram groepen waarin vervalste geschriften en illegaal vuurwerk werden verkocht. Wat opvalt aan deze gevallen is dat in drie zaken de rechter-commissaris toestemming heeft gegeven voor een toepassing naar analogie van artikel 125p Sv, namelijk een artt. 181 jo 125p Sv-combinatie. In deze zaken heeft de rechter-commissaris geen aanbieder gehoord, omdat de veronderstelling van de officier van justitie en de rechter-commissaris was dat deze niet zou meewerken. In plaats daarvan heeft de politie de opdracht gekregen om gegevens ontoegankelijk te maken.

Zoals gezegd voldoet artikel 125p Sv niet altijd voor de opsporingspraktijk. Een belangrijke reden hiervoor is gelegen in lid vier van artikel 125p Sv: een schriftelijke machtiging van de rechter-commissaris waarbij de aanbieder voorafgaand aan de afgifte daarvan gehoord moet worden. De toets door de rechter-commissaris is geïntroduceerd, omdat artikel 125p Sv een ingrijpende bevoegdheid betreft. Daarnaast moest de toets ervoor zorgen dat gegevens toch relatief snel ontoegankelijk konden worden gemaakt. Deze snelle ontoegankelijkmaking staat in lid 2. In de opsporingspraktijk botsen de toets door de rechter-commissaris en een snelle ontoegankelijkmaking met elkaar. Zowel het proces van afgifte van een schriftelijke machtiging als het horen van de aanbieder nemen (veel) tijd in beslag. Bovendien brengt het horen van een aanbieder nog andere moeilijkheden met zich mee. Snelle ontoegankelijkmaking is dus niet altijd mogelijk, ook een belangrijke nuancering bij de veronderstelling van de wetgever.

Tegelijkertijd is de toets door de rechter-commissaris er niet voor niets. Artikel 125p Sv is een ingrijpende bevoegdheid, omdat de vrijheid van meningsuiting in het geding kan zijn. In veel zaken waarin artikel 125p Sv gebruikt wordt zou het echter doorgaans gaan om onmiskenbaar illegale content, waar geen discussie bestaat over de strafbaarheid ervan, zoals dat bij zogenoemde uitingsdelicten wel het geval kan zijn. Dat neemt niet weg dat er verzoeken kunnen komen die wel degelijk de vrijheid van meningsuiting raken. Een zorgvuldige toetsingsprocedure, een belangrijk onderdeel van de rechtsstaat, blijft om die reden aangewezen. Wel kan gekeken worden of hetgeen nu alleen nog in de memorie van toelichting staat beschreven met betrekking tot het achterwege laten van het horen van de aanbieder ook in de wetstekst zelf opgenomen kan worden.

Tot slot nog drie aandachtspunten met betrekking tot artikel 125p Sv. De eerste betreft het tijdelijke karakter van de ontoegankelijkmaking. In principe volgt definitieve ontoegankelijkmaking pas als een zittingsrechter zich over een zaak gebogen heeft. In deze evaluatie is duidelijk geworden dat de ontoegankelijkmaking van gegevens ook voorkomt in zaken die nooit aan een zittingsrechter zullen worden voorgelegd. Dat betekent dat sprake blijft van een tijdelijke maatregel die in theorie oneindig kan duren. Een tweede aandachtspunt, dat deels samenhangt met hetgeen al besproken is, betreft de ontoegankelijkmaking van gegevens in zaken die een buitenlandcomponent kennen. Voor die zaken geldt dat vaak geen vervolging plaatsvindt, en dus geen einduitspraak wordt gedaan. Bovendien kunnen buitenlandse aanbieders slecht bereikbaar zijn en nemen rechtshulpverzoeken veel tijd in beslag. Mogelijke oplossingsrichtingen die geïnterviewden noemden zijn meer eenduidige wet- en regelgeving over hoe kan worden omgegaan met het verantwoordelijk maken van aanbieders die strafbare inhoud faciliteren, en de mogelijkheid om te werken zonder rechtshulpverzoek, waarbij het inlichten van buitenlandse autoriteiten voldoende zou zijn. Een derde aandachtspunt is de mix van bestuursrechtelijke, civielrechtelijke en strafrechtelijke mogelijkheden die er is om gegevens ontoegankelijk te maken. Deze evaluatie heeft zich vooral gericht op de strafrechtelijke component. Het zou mooi zijn om tot een goed overzicht te komen welke optie voor welke situatie de meest wenselijke is, én dat daarbij nieuwe mogelijkheden worden betrokken die er sinds de inwerkingtreding van de Wet CCIII bijgekomen zijn zoals die van de Autoriteit online Terroristisch en Kinderpornografisch Materiaal.

Hackbevoegdheid (artt. 126nba, 126uba en 126zpa Sv)

In 2022 verscheen zoals gezegd een eerdere WODC-evaluatie over de hackbevoegdheid (Van Uden & Van den Eeden, 2022). De nadruk lag toen op de technische kant van de inzet. In deze evaluatie is vooral gekeken naar de tactische kant van de inzet van de hackbevoegdheid, namelijk op welke wijze de verzamelde gegevens binnen een opsporingsonderzoek worden gebruikt. Tevens is in deze evaluatie gekeken naar de veronderstellingen, inclusief doelstellingen, van de wetgever en in hoeverre die uitgekomen zijn. Tot slot is de aandacht gericht op wat er gedaan is met de kern aandachtspunten die wij in onze eerdere evaluatie formuleerden.

De wetgever heeft de hackbevoegdheid (artt. 126nba, 126uba en 126 zpa Sv) geïntroduceerd om computercriminaliteit en andere vormen van ernstige criminaliteit beter aan te kunnen pakken. Dat was een belangrijke veronderstelling achter de hackbevoegdheid. Vanwege technologische ontwikkelingen zouden reeds bestaande bevoegdheden te weinig opleveren. Bovendien, zo veronderstelde de wetgever, zouden bestaande bevoegdheden praktisch en proportioneel gezien niet altijd de meest aangewezen bevoegdheden zijn. Beide veronderstellingen, weliswaar met een aantal belangrijke nuanceringen, zijn juist gebleken.

In de periode april 2021-april 2024 is in 89 opsporingsonderzoeken een eerste bevel afgegeven om de hackbevoegdheid in te zetten. Bijna alle opsporingsonderzoeken richtten zich op één of meer vormen van traditionele criminaliteit. Een overtreding van de Opiumwet, (poging tot) moord/doodslag en witwassen kwamen het vaakst voor. In tegenstelling tot de naam Wet computercriminaliteit III wellicht doet vermoeden is de hackbevoegdheid slechts sporadisch ingezet voor cybercrime in enge zin.

In de opsporingsonderzoeken waarbinnen ten minste één bevel is afgegeven voor de inzet van de hackbevoegdheid mochten 125 geautomatiseerde werken worden binnengedrongen. Het overgrote deel betrof een inzet op een telefoon, de zogenoemde standaardinzetten. Deze bevindingen liggen in lijn met de eerdere WODC-rapportage (Van Uden & Van den Eeden, 2022).

Er waren verschillende redenen waarom tactische opsporingsteams het noodzakelijk achtten om één of meerdere geautomatiseerde werken binnen te dringen. Allemaal redenen die aansloten bij wat de wetgever had voorzien. Twee redenen sprongen eruit, namelijk de versleuteling van gegevensdragers en de vrees dat een verdachte op de hoogte zou raken van het opsporingsonderzoek. In deze evaluatie is ook duidelijk geworden dat er zaken zijn waarin de keuze wordt gemaakt om de hackbevoegdheid niet te benutten. Een deel hiervan betreft zaken waarvoor de hackbevoegdheid nog (steeds) geen oplossing kan bieden. Bijvoorbeeld opsporingsonderzoeken die zich (deels) in een buitenland afspelen waarmee Nederland geen goede (rechtshulp)relatie heeft. Of zaken waarin er te weinig tijd is voor een inzet van de hackbevoegdheid, bijvoorbeeld omdat het binnendringen in een geautomatiseerd werk niet lukt. Dit is een belangrijke nuancering bij de veronderstelling van de wetgever.

Bij een ruime meerderheid van de inzetten is het gelukt om het geautomatiseerd werk binnen te dringen en gegevens te verzamelen. De verzamelde gegevens betroffen vooral vormen van communicatie die verlopen via communicatie apps. In een derde van de opsporingsonderzoeken zijn de gegevens als sturingsinformatie gebruikt en in een derde van de opsporingsonderzoeken als bewijs. Tussen deze categorieën zit overlap, omdat in negen onderzoeken de verzamelde gegevens én als sturingsinformatie én als bewijs hebben gediend. In 40% van de onderzoeken leidt de inzet van de hackbevoegdheid niet tot een bruikbare opbrengst voor het opsporingsonderzoek. De wijze waarop de hackbevoegdheid een bijdrage levert aan de aanpak van ernstige vormen van criminaliteit en computercriminaliteit kan dus verschillen, wederom een belangrijke nuancering bij de veronderstelling van de wetgever.

In net iets minder dan een derde van de zaken heeft een zittingsrechter zich inhoudelijk gebogen over de zaak waarin de hackbevoegdheid is ingezet. In ruim een derde van de zaken zal een zittingsrechter dat nog gaan doen. Opvallend aan de zaken die tot nu toe behandeld zijn door een zittingsrechter is dat de inzet van de hackbevoegdheid maar in een zeer klein aantal zaken besproken is. In de betreffende zaken besteedde een advocaat in het verweer aandacht aan de hackbevoegdheid. Deze bevinding is van belang in het licht van de aangekondigde verandering ten aanzien van de keuring van technische hulpmiddelen. De politie gebruikt een technisch hulpmiddel om gegevens te verzamelen. De keuring moet waarborgen dat de gegevens die verzameld zijn met de hackbevoegdheid betrouwbaar zijn. Eerder was het de bedoeling dat alleen gewerkt zou worden met vooraf goedgekeurde technische hulpmiddelen. In onze eerdere evaluatie lieten wij zien dat dat niet realistisch is gebleken, onder andere omdat vooral gewerkt werd met commerciële middelen waarvan de officier van justitie had besloten dat de aard ervan zich verzette tegen een keuring. De toenmalig Minister van Justitie en Veiligheid heeft, mede naar aanleiding van deze bevinding, de keuze gemaakt dat alle technische hulpmiddelen ter keuring aangeboden moeten worden en dat gewerkt mag worden met technische hulpmiddelen die niet (volledig) goedgekeurd zijn. De inzet van een vooraf goedgekeurd middel is zodoende niet langer het uitgangspunt. Indien gewerkt wordt met een middel dat

vooraf niet (volledig) goedgekeurd is, dan is het aan de officier van justitie om tactische waarborgen in te stellen en aan de zittingsrechter om het bewijs te wegen en daar een oordeel over te vellen. Een dergelijke wijziging, die overigens op dit moment nog niet is doorgevoerd, betekent dat er géén technische hulpmiddelen meer worden benut die niet door een keuringsinstantie bekeken zijn. Dat is op zichzelf een goede ontwikkeling, omdat inzichtelijk zal zijn waar eventueel nog risico's zitten ten aanzien van de betrouwbaarheid van de gegevens die verzameld worden met het ingezette technisch hulpmiddel. Een belangrijk aandachtspunt hierbij is dat deze evaluatie heeft laten zien dat de inzet van de hackbevoegdheid nog nauwelijks besproken is tijdens de behandeling van de zaak door een zittingsrechter. Dat betekent dat een zittingsrechter zich over dit specifieke onderwerp niet structureel buigt en dat de inzet van de bevoegdheid slechts beperkt getoetst wordt. Gezien de ingrijpendheid van de bevoegdheid is dat een belangrijke beperking.

Tot slot nog twee belangrijke aandachtspunten, één met betrekking tot de keuring en één met betrekking tot de inzet van commerciële middelen. Zoals gezegd heeft de toenmalig Minister van Justitie en Veiligheid in december 2023 in een brief aangekondigd dat de wijze waarop met technische hulpmiddelen zal worden omgegaan, gewijzigd zal worden. In haar brief kondigde zij aan dat alle betrokken partijen hierover met elkaar in overleg zouden gaan. Dat lag in lijn met een belangrijk aandachtspunt dat in de eerdere WODC-evaluatie beschreven werd. Daarin werd geconstateerd dat dit gesprek belangrijk was, omdat het een gedeeld belang is van alle betrokkenen om betrouwbare gegevens te verzamelen. Deze evaluatie heeft laten zien dat dit gesprek tot nu toe zeer moeizaam op gang gekomen is. Het voortzetten van het moeizaam op gang gekomen overleg blijft om die reden een aandachtspunt.

Het tweede aandachtspunt ziet op het gebruik van commerciële middelen. Bij het overgrote deel van de inzetten werd gebruikgemaakt van een commercieel middel, zowel om binnen te dringen als om gegevens te verzamelen. Dit past bij de verwachting die de toenmalig Minister van Justitie en Veiligheid in haar beleidsbrief uitspreekt dat commerciële producten 'relatief vaak' zullen worden ingezet. Wel roept dit de vraag op of het gebruik van commerciële middelen net zoals in de wetsgeschiedenis, meer specifiek het Besluit (Besluit onderzoek geautomatiseerd werk, p. 15) beschreven staat, een uiterst middel moet worden genoemd. De term uiterst middel wekt de suggestie dat het gebruik ervan een uitzondering is. Deze evaluatie heeft wederom laten zien dat het gebruik ervan eerder de regel is.

Tot besluit

Met de komst van de Wet CCIII is het juridisch instrumentarium versterkt voor de opsporing en vervolging van computercriminaliteit. Dit was ook wat de wetgever beoogde met de introductie van de nieuwe wet. Bij computercriminaliteit gaat het om computercriminaliteit in zeer brede zin, zo blijkt uit deze evaluatie. Dat betekent dat deels sprake is van meer traditionele vormen van criminaliteit waarbij ICT slechts een middel is om een strafbaar feit te plegen.

De versterking van het juridisch instrumentarium heeft vorm gekregen middels vijf nieuwe of aangepaste strafbaarstellingen in het Wetboek van Strafrecht en twee nieuwe bevoegdheden in het Wetboek van Strafvordering. Het grootste deel van de nieuwe strafbaarstellingen heeft ervoor gezorgd dat verdachten vervolgd kunnen worden voor feiten waarbij dat vóór de introductie van de wet minder goed mogelijk

was. Denk aan het helen en stelen van gegevens en online handelsfraude. Voor de aangepaste strafbaarstellingen artikelen 248a Sr (verleiding van een minderjarige) en 248e Sr (*grooming*) is dit veel minder het geval. In dat opzicht is er wel een juridisch instrument ('lokpuber') bijgekomen, maar wordt dit in de opsporingspraktijk nauwelijks benut.

Net als een groot deel van de strafbaarstellingen worden de twee nieuwe opsporingsbevoegdheden, de ontoegankelijkmaking van gegevens en de hackbevoegdheid, in de praktijk gebruikt. Beide bevoegdheden hebben ervoor gezorgd dat opsporingshandelingen kunnen worden verricht die voorheen niet (hackbevoegdheid) of in mindere mate (ontoegankelijkmaking) mogelijk waren. Deze handelingen leveren, al dan niet indirect, een bijdrage aan de aanpak van computercriminaliteit en andere ernstige vormen van criminaliteit. Er doen zich echter ook situaties voor waarin deze twee nieuwe bevoegdheden niet de gewenste bijdrage kunnen leveren binnen een opsporingsonderzoek, vooral bij de ontoegankelijkmaking van gegevens.

In deze evaluatie zijn tot slot vier aspecten naar voren gekomen die meerdere wettelijke bepalingen uit de Wet CCIII raken: 1) nieuwe ontwikkelingen; 2) beschikbare capaciteit; 3) zaken met een internationale component; en 4) (rechtsstatelijke) waarborgen bij de inzet van bijzondere opsporingsbevoegdheden.

Ten eerste nieuwe ontwikkelingen. Voor artikel 138c Sr geldt dat een deel van de noodzaak voor dit artikel verdwenen is. Nieuwe jurisprudentie volgend kan, vooral in sommige werksituaties, ook het artikel computervredebreuk (art. 138ab Sr) gebruikt worden. Wat betreft artikel 139g Sr is van belang dat uit recente cijfers van Europol (2025) blijkt dat de illegale handel in gegevens is toegenomen. Dat heeft de impact veranderd die het helen van gegevens kan hebben. Om die reden zou het goed zijn dat de wetgever de strafmaat van artikel 139g Sr heroverweegt. Met betrekking tot de hackbevoegdheid wordt het steeds ingewikkelder om versleuteling te doorbreken. In dat kader is het voor de wetgever van belang om na te denken hoe met deze ontwikkeling om te gaan, en daarbij rekening te houden met én de bescherming van grondrechten zoals de persoonlijke levenssfeer van burgers én met de effectiviteit van de opsporing.

Ten tweede de beschikbare capaciteit. De beschikbare opsporingscapaciteit is een belangrijk aandachtspunt bij de toepassing van een aantal wettelijke bepalingen uit de Wet CCIII. Vooral bij de lokpuber, online handelsfraude en de hackbevoegdheid werd dit onderwerp als reden genoemd voor het mogelijk beperktere gebruik van de betreffende bepaling. De oplossing hiervoor is niet eenvoudig: er zullen bijvoorbeeld altijd keuze moeten worden gemaakt. Bovendien kan de vraag worden gesteld of strafrecht altijd de oplossing is. Daarom is het goed om te kijken waar een bredere aanpak, dat wil zeggen breder dan het strafrecht, (verdere) invulling kan krijgen. Daarbij is het van belang dat dat soort initiatieven goed geëvalueerd wordt.

Ten derde zaken die een internationale component bevatten. Een internationale component in een zaak zorgt ervoor dat een deel van de wettelijke bepalingen in de opsporingspraktijk niet optimaal benut kan worden. Daarom zou het goed zijn de aandacht te richten op gezamenlijke Europese en internationale initiatieven over hoe bijvoorbeeld kan worden omgegaan met het verantwoordelijk maken van aanbieders die strafbare inhoud faciliteren. Wat betreft online handelsfraude zou gekeken kunnen worden in hoeverre het mogelijk is om een koppeling te realiseren tussen de

verwijzingsportalen van elk Europees land afzonderlijk waardoor het gemakkelijker is om de mogelijke identiteit van een buitenlandse rekeninghouder te achterhalen.

Ten vierde de (rechtsstatelijke) waarborgen bij de inzet van bijzondere opsporingsbevoegdheden. In de praktijk is een spanningsveld zichtbaar tussen enerzijds de efficiency en effectiviteit van een inzet en anderzijds de rechtsstatelijkheid. Vanwege de ingrijpendheid van de bevoegdheden is het van belang dat stevige toetsingsvoorwaarden blijven bestaan. Wat betreft de ontoegankelijkmaking van gegevens kan wel gekeken worden of bepaalde voorwaarden anders ingevuld kunnen worden. Met betrekking tot de hackbevoegdheid heeft de toenmalig Minister van Justitie en Veiligheid al de keuze gemaakt dat te gaan doen, namelijk ten aanzien van de keuring van technische hulpmiddelen. Daarbij gaat deze minister ervan uit dat een zittingsrechter het bewijs, verzameld met de hackbevoegdheid, toetst. Tot nu toe heeft een zittingsrechter zich zeer sporadisch inhoudelijk over de inzet van de hackbevoegdheid gebogen. Dat betekent dat geen recht worden gedaan aan een belangrijke rechtsstatelijke waarborg waarvan wel verondersteld wordt dat die in de praktijk aanwezig is.

1 Inleiding

Op 1 maart 2019 is de Wet computercriminaliteit III (hierna Wet CCIII) in werking getreden. Deze nieuwe wet moet het 'juridisch instrumentarium voor de opsporing en vervolging van computercriminaliteit'[3] versterken (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 2). Een belangrijk doel van deze wet, zo blijkt uit de memorie van toelichting, is een betere bescherming van de samenleving tegen criminaliteit en tegen enkele gedragingen die nog niet strafbaar gesteld zijn (*Kamerstukken II* 2015/16, 34 372, nr. 3). De Wet CCIII bevat zowel wijzigingen in het Wetboek van Strafrecht als wijzigingen van het Wetboek van Strafvordering.

1.1 Wijzigingen Wetboek van Strafrecht

1.1.1 Stelen van gegevens

Op basis van artikel 138c Sr is het strafbaar geworden om niet-openbare gegevens die middels een geautomatiseerd werk zijn opgeslagen wederrechtelijk met een technisch hulpmiddel over te nemen. Dit nieuwe artikel moet een betere bescherming bieden in gevallen waarin gegevens gekopieerd worden. Door het kopiëren heeft de rechthebbende immers geen volledige invloed meer op wat er met de gekopieerde gegevens gebeurt. Daardoor kan hij/zij benadeeld worden (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 61). De wetgever achtte dit artikel noodzakelijk, omdat bestaande strafbaarstellingen in haar ogen niet in alle gevallen voldeden. Zo is het voor het nieuwe artikel niet vereist dat de gegevens middels computervredebreuk (art. 138ab Sr) zijn verkregen. Het ontbreken van dat vereiste is relevant wanneer een verdachte rechtmatige toegang heeft tot niet-openbare gegevens van een computer en de gegevens wederrechtelijk[4] overneemt. Bijvoorbeeld een werknemer van een bedrijf die gegevens kopieert voor eigen gebruik zonder dat hij/zij daartoe gerechtigd is. In dit geval is geen sprake van verduistering, omdat de rechthebbende de beschikkingsmacht over de gekopieerde gegevens behoudt (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 64).

1.1.2 Helen van gegevens

In artikel 139g Sr is geregeld dat het strafbaar is om niet-openbare gegevens voor handen te hebben of bekend te maken die door een misdrijf zijn verkregen, ook wel het 'helen van gegevens' (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 61-62). Helen heeft betrekking op situaties waarin niet aangetoond kan worden dat degene die de gegevens bekend maakt, ook degene is die de gegevens heeft overgenomen, al dan niet nadat die persoon een geautomatiseerd werk is binnengedrongen (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 61-62). Op die manier zijn personen strafbaar die gegevens, ontvreemd uit de computer van anderen, bekend maken aan een ander, op het internet plaatsen of verkopen. Het is daarbij niet nodig dat deze persoon weet dat

[3] Computercriminaliteit wordt gedefinieerd als 'het plegen van strafbare feiten met behulp van, dan wel gericht op een geautomatiseerd werk' (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 7).

[4] In de memorie van toelichting wordt toegelicht wat onder wederrechtelijk wordt verstaan, althans in welke situaties de wederrechtelijkheid ontbreekt. Van wederrechtelijk is bijvoorbeeld sprake als gegevens niet met toestemming van de rechthebbende zijn overgenomen en wanneer niet op rechtmatige wijze uitvoering wordt gegeven aan de wettelijke bevoegdheid tot het overnemen van gegevens (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 63).

gegevens door een misdrijf zijn verkregen. Een redelijk vermoeden dat dit het geval was, volstaat (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 65). De wetgever achtte de toevoeging van artikel 139g Sr noodzakelijk, omdat het vóór de introductie van dat artikel niet altijd mogelijk was heling van gegevens strafrechtelijk te vervolgen (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 62). In de memorie van toelichting wordt een voorbeeld genoemd van een casus waarbij ontvreemde gegevens door waren gegeven aan een derde. Deze derde publiceerde de gegevens op het internet, ook al moest deze persoon hebben geweten dat deze gegevens door een misdrijf waren verkregen. Vervolging op basis van heling van een goed was niet mogelijk, omdat het in deze casus om gekopieerde gegevens ging en niet om een goed (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 62).

1.1.3 Inzet van een lokpuber bij verleiden minderjarigen en grooming

Om kinderen beter te beschermen tegen benadering voor seksuele doeleinden heeft de wetgever twee wettelijke bepalingen gewijzigd.[5] Het eerste artikel (art. 248a Sr) betreft het verleiden van een minderjarige en het tweede artikel (art. 248e Sr) heeft betrekking op *grooming*.[6] Beide artikelen zijn gewijzigd omdat het verleiden van een minderjarige en *grooming* alleen strafbaar waren als het slachtoffer daadwerkelijk minderjarig was. Het potentiële slachtoffer mocht dus niet een meerderjarige zijn die zich voordeed als minderjarige (bijvoorbeeld een politieagent, ook wel lokpuber genoemd). De doorgevoerde wijzigingen betekenen dat beide strafbaarstellingen ook gelden wanneer een verdachte iemand benadert die doet alsof hij/zij de leeftijd van zestien jaar (*grooming*) of achttien jaar (verleiding van een minderjarige tot ontucht) nog niet heeft bereikt (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 69). De wetgever achtte deze wijzigingen noodzakelijk, omdat voorheen de inzet van een lokpuber niet kon bijdragen aan bewijs in zaken betreffende *grooming* of verleiding van een minderjarigen (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 69). Met een wijziging van beide strafbaarstellingen moet de inzet van een lokpuber wel mogelijk worden. Bovendien kan tot een bewezenverklaring worden gekomen als een ouder, broer of zus zich voordoet als een minderjarige, bijvoorbeeld omdat diegene de chat van zijn kind, broertje of zusje heeft overgenomen (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 69-70).

1.1.4 Online handelsfraude

Om internetoplichting het hoofd te bieden is artikel 326e toegevoegd aan het Wetboek van Strafrecht. Middels dat artikel wordt het strafbaar om, via het internet, goederen of diensten aan te bieden zonder dat de aanbieder de intentie heeft de goederen of diensten te leveren. Kopers worden in dat geval benadeeld (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 4). Het gaat hierbij om zowel nieuwe als tweedehands producten (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 72-73). De wetgever achtte de toevoeging van deze strafbaarstelling noodzakelijk, omdat de aanpak en vervolging van online handelsfraude niet altijd mogelijk is gebleken, zo wordt in de memorie van toelichting beargumenteerd (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 73). Grote marktpartijen nemen bijvoorbeeld maatregelen om malafide aanbieders te weren, maar deze maatregelen zijn niet toereikend. Het komt voor dat aanbieders werken met zeer tijdelijke websites waardoor de aanbieder niet meer aangesproken kan

[5] Met de inwerkingtreding van de Wet Seksuele misdrijven op 1 juli 2024 zijn deze twee bepalingen inmiddels achterhaald.

[6] De politie omschrijft *grooming* als 'digitaal kinderlokken'. Van *grooming* is sprake als een volwassenen via ICT contact legt met een kind (jonger dan 16 jaar) met de intentie om elkaar te ontmoeten om kinderpornografisch materiaal te vervaardigen of seksueel misbruik te plegen (Politie, z.d.).

worden en geen schadevergoeding meer kan worden geëist. De politie heeft meer mogelijkheden om zicht te krijgen op online handelsfraude. Toch acht de wetgever ook deze niet afdoende, omdat het lastig zou zijn om online handelsfraude op grond van oplichting (art. 326 Sr) te vervolgen. De jurisprudentie is hier niet eenduidig over en in de memorie van toelichting worden diverse voorbeelden gegeven waaruit dat zou blijken (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 73). De wetgever constateert uiteindelijk dat 'beperkt strafrechtelijk kan worden opgetreden tegen aanbieders die zich bij herhaling schuldig maken aan het verkopen of aanbieden zonder te leveren'. Daarom moet het Openbaar Ministerie middels artikel 326e Sr in staat worden gesteld om op te treden tegen 'grootschalige handelsfraude'. Strafrechtelijke vervolging dient echter wel te worden gezien als laatste redmiddel. Private als publieke partijen zijn zelf ook verantwoordelijk voor de bestrijding van online handelsfraude (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 75).

Naast bovengenoemde strafbaarstellingen zijn met de inwerkingtreding van de Wet CCIII twee bevoegdheden toegevoegd aan het Wetboek van Strafvordering.

1.2 Wijzigingen Wetboek van Strafvordering

1.2.1 Ontoegankelijkmaking van gegevens

Artikel 125p Sv regelt dat gegevens op basis van een bevel van de officier van justitie ontoegankelijk kunnen worden gemaakt. Er bestonden al mogelijkheden om gegevens ontoegankelijk te maken, maar deze voldeden volgens de wetgever niet meer. Allereerst hebben aanbieders van telecommunicatiediensten een 'Gedragscode *Notice-and-Take-Down*' (hierna Gedragscode) ondertekend. Deze Gedragscode regelt dat tussenpersonen die in Nederland een openbare telecommunicatiedienst aanbieden op het internet ervoor kunnen zorgen dat 'onmiskenbaar onrechtmatige of strafbare inhoud' kan worden verwijderd (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 57). Echter, niet alle aanbieders van een communicatiedienst hebben de gedragscode ondertekend, denk bijvoorbeeld aan *hosting providers* en beheerders van een website. Met de nieuwe bevoegdheid wordt het mogelijk om ook in die gevallen strafbare feiten te beëindigen en te voorkomen (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 57). Daarnaast kan het voorkomen dat een aanbieder (die de gedragscode wel ondertekend heeft) meent dat geen sprake is van strafbare inhoud. Op dat moment kan overgegaan worden tot het doen van aangifte of het betrekken van de rechter. Vóór de introductie van de nieuwe bevoegdheid was het op basis van artikel 54a Sr mogelijk om gegevens ontoegankelijk te maken. Ook deze mogelijkheid schiet volgens de wetgever tekort. Vanuit 'wetsystematisch oogpunt' en vanwege 'overzichtelijkheid en duidelijkheid voor de praktijk' moest ontoegankelijkmaking opgenomen worden in het Wetboek van Strafvordering (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 57).

1.2.2 Hackbevoegdheid

De tweede bevoegdheid die is toegevoegd aan het Wetboek van Strafvordering is de hackbevoegdheid. Deze bevoegdheid, neergelegd in de artikelen 126nba, 126uba, 126zpa Sv, regelt dat opsporingsambtenaren die daarvoor zijn aangewezen, 'onder voorwaarden een geautomatiseerd werk, dat bij een verdachte in gebruik is, op afstand heimelijk [kunnen] binnendringen met het oog op bepaalde doelen op het gebied van de opsporing van ernstige strafbare feiten' (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 3).

De nieuwe bevoegdheid is een zogenoemde 'paraplubevoegdheid'. Dit betekent dat na het binnendringen verschillende andere opsporingsbevoegdheden kunnen worden benut (Oerlemans, 2017, p. 355). Volgens de wetgever is deze hackbevoegdheid noodzakelijk omdat bestaande opsporingsbevoegdheden in toenemende mate tekortschieten om 'aan de wezenlijke problemen en gebleken knelpunten op het gebied van de bestrijding van computercriminaliteit tegemoet te komen' (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 7). Een belangrijke reden voor dat tekortschieten zijn diverse technologische ontwikkelingen, waaronder de versleuteling van gegevens(-dragers) (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 7-13).

1.3 Centrale vraagstelling

De gehele Wet CCIII moest na vijf jaar worden geëvalueerd. Eerder verscheen al een evaluatierapport over één van de bepalingen uit de wet, namelijk over de uitvoering van de hackbevoegdheid (Van Uden & Van den Eeden, 2022). In dat onderzoek is vooral gekeken naar de technische kant van de inzet van de hackbevoegdheid en niet naar wat de hackbevoegdheid in een opsporingsonderzoek opleverde. In deze evaluatie wordt daar wel naar gekeken. Bovendien is het doel van deze evaluatie breder, namelijk het evalueren van de gehele Wet CCIII. Daarbij zal de aandacht zich richten op het doel en de veronderstelde werking van de wet, de uitvoering van de wet in de praktijk en de vraag of de beoogde doelstellingen van de nieuwe wet behaald (kunnen) worden.

In dit rapport staat de volgende onderzoeksvraag centraal:

> In hoeverre worden de doelstellingen zoals geformuleerd in de Wet CCIII in de praktijk gerealiseerd?

Om deze onderzoeksvraag te beantwoorden zijn drie deelvragen geformuleerd.

1 Wat is het doel van de verschillende bepalingen van de Wet CCIII en welke veronderstellingen liggen aan die bepalingen ten grondslag?
2 Hoe wordt in de praktijk uitvoering gegeven aan de verschillende bepalingen van de Wet CCIII?
3 Welke gevolgen (zowel bedoeld als onbedoeld) hebben de verschillende bepalingen van de Wet CCIII voor de opsporingspraktijk?

Het doel van de eerste deelvraag is om inzicht te krijgen in het doel/de doelen die behaald dienen te worden met de verschillende bepalingen van de Wet CCIII en de wijze waarop de wetgever verwacht deze doelen te kunnen behalen. Op die manier wordt inzichtelijk welke veronderstellingen ten grondslag liggen aan de wet. Inzicht in die veronderstellingen is nodig om in kaart te brengen in hoeverre de door de wetgever geformuleerde veronderstellingen (al dan niet impliciet) in de praktijk daadwerkelijk gerealiseerd worden. Het doel van de tweede deelvraag is om in kaart te brengen hoe de verschillende bepalingen van de Wet CCIII in de (opsporings)praktijk worden benut. Daarbij wordt onder andere aandacht besteed naar de voordelen voor de opsporingspraktijk en de aandachtspunten. Met de derde deelvraag wordt inzichtelijk gemaakt wat, in meer algemene zin, de gevolgen zijn, zowel bedoeld als onbedoeld, van de verschillende bepalingen binnen de Wet CCIII.

1.4 Methoden van onderzoek

In dit evaluatieonderzoek is een combinatie van kwantitatieve maar vooral kwalitatieve onderzoeksmethoden gebruikt. Dat komt de validiteit van het onderzoek ten goede (Maesschalck, 2010; Braster, 2000). Het gebruik van verschillende onderzoeksmethoden zorgt ervoor dat een onderwerp vanuit meerdere kanten begrepen kan worden waardoor een completer beeld van de werkelijkheid verkregen wordt. In dit onderzoek gebruikten we de volgende onderzoeksmethoden:
1) documentanalyse, 2) cijfermatige analyse van juridische databestanden (RAC-min), 3) interviews (zowel algemeen als verdiepend), 4) vonnisanalyse en 5) een vragenlijst. Deze onderzoeksmethoden zijn deels parallel en deels na elkaar toegepast. Een deel van de documentanalyse is bijvoorbeeld gebruikt om de topiclijsten voor de interviews en de vonnisanalyse op te stellen. Een ander deel van de documentanalyse vond gedurende het proces van dataverzameling plaats. Verder vormden de uitkomsten van de algemene interviews een belangrijke bron voor de verdiepende interviews. Parallel aan dit alles werd op een aantal momenten in de tijd een cijfermatige analyse uitgevoerd.

1.4.1 Documentanalyse

Om een goed beeld te krijgen van de inhoud van de wet en de wetsgeschiedenis zijn diverse documenten bestudeerd. Een groot deel hiervan betrof parlementaire stukken zoals de wetstekst zelf (inclusief de verschillende versies die er zijn geweest gedurende het wetgevingstraject), de memorie van toelichting, de inbreng van deskundigen gedurende de verschillende consultatierondes en de (schriftelijke en mondelinge) debatten die zijn gevoerd in de Eerste en Tweede Kamer. Een groot deel van deze documenten was reeds geraadpleegd en geanalyseerd in het kader van de eerdere evaluatie (Van Uden & Van den Eeden, 2022, p. 26-27). Deze analyse is aangevuld met betrekking tot de andere wettelijke bepalingen uit de Wet CCIII. Op basis van de volledige analyse is een eerste beeld verkregen van de inhoud van de wet en konden (impliciete) veronderstellingen achterhaald worden die aan de wet ten grondslag liggen (deelvraag 1).

Naast documenten gerelateerd aan het wetgevingstraject zijn (interne) documenten geraadpleegd van betrokken (uitvoerings)partijen, zoals de politie, het Openbaar Ministerie en de Inspectie Justitie en Veiligheid (hierna Inspectie JenV). Het ging daarbij bijvoorbeeld om beschrijvingen van werkprocessen en handleidingen hoe in bepaalde gevallen dient te worden gehandeld. Deze documenten zijn niet gevonden op basis van een systematische zoekanalyse. In plaats daarvan zijn deze verkregen via interviews of via door ons geraadpleegde documenten waarin werd verwezen naar documenten die voor ons relevant waren. Op basis van deze documenten werd een eerste beeld verkregen van de uitvoering in de praktijk (deelvraag 2).

1.4.2 Analyse RAC-min

Om het aantal keer vast te stellen dat de nieuwe strafbaarstellingen zijn gebruikt (deelvraag 2), zijn over de periode maart 2019-april 2024, cijfers uit RAC-min opgevraagd bij de afdeling Informatievoorziening & Datamanagement van het WODC. In RAC-min staat informatie over alle zaken die bij het Openbaar Ministerie instromen en over de afhandeling van die zaken door het Openbaar Ministerie en door de rechter in eerste aanleg. Per zaak is uitgebreide informatie beschikbaar over de aard van de gepleegde feiten, de verschillende afdoeningen in de zaak door het Openbaar

Ministerie, het vonnis van de rechter en de opgelegde sancties. Het doel van RAC-min is om te voorzien in een landelijke informatiebehoefte en om wetenschappelijk onderzoek op het gebied van vervolging en berechting mogelijk te maken. RAC-min is een deelverzameling van het Rapsody systeem. Rapsody is gebaseerd op de registratiesystemen COMPAS en GPS. Deze registratiesystemen gebruikt het Openbaar Ministerie en de rechterlijke macht om strafzaken, afgedaan in eerste aanleg, te registreren. COMPAS staat voor Communicatiesysteem Openbaar Ministerie-Parket AdminiStratie en dit is een case-managementsysteem dat de processtappen van proces-verbaal en dagvaarding tot vonnis ondersteunt en het mogelijk maakt deze te registreren. Sinds 2008 is het Openbaar Ministerie begonnen met de invoer van GPS (Geïntegreerd Processysteem Strafrecht) met als doel de kwaliteit, flexibiliteit en snelheid in de strafrechtketen te bevorderen. GPS en COMPAS zijn 'levende' systemen wat inhoudt dat sprake is van continue registratie van nieuwe informatie, maar ook zijn aanpassingen aan reeds ingevoerde informatie mogelijk. In Rapsody worden gegevens uit COMPAS en GPS opgenomen die voor beleidsinformatie van belang worden geacht. Rapsody is een decentraal systeem met afzonderlijke databases in elk van de arrondissementen. In Rapsody Centraal (RAC) worden de lokale gegevens samengebracht' (Verweij & Tollenaar, 2020, p. 12).

De afdeling Informatievoorziening & Datamanagement van het WODC heeft een Excel-overzicht verstrekt met daarin door ons gevraagde gegevens met betrekking tot afdoeningen door het Openbaar Ministerie en een Excel-overzicht over de rechterlijke afdoening in eerste aanleg. In de OM-Excel waren onder andere de volgende kenmerken opgenomen: versleuteld parketnummer OM, soort strafbaarstelling, wel of geen hoger beroep, vonnisomschrijving[7], aantal feiten dat in de zaak voorkomt, aantal CCIII-feiten dat in de betreffende zaak voorkomt, aantal sepots en sepotgronden van de CCIII-feiten. In het Excel-bestand over de rechterlijke macht stonden onder andere de volgende kenmerken: versleuteld parketnummer OM, soort strafbaarstelling, wel of geen hoger beroep, vonnisomschrijving, aantal feiten dat in de zaak voorkomt, aantal CCIII-feiten dat in de betreffende zaak voorkomt en het aantal feiten, zowel CCIII-feiten als andere feiten die vrijgesproken zijn.

De cijferoverzichten zijn als volgt samengesteld. Allereerst is een selectie gemaakt van de strafbaarstellingen in de Wet CCIII (artt. 138c Sr, 139g Sr, 248a Sr, 248e Sr en 326e Sr). Op basis daarvan kon worden vastgesteld in welke zaken de betreffende CCIII-feiten voorkwamen. De selectie had betrekking op de periode maart 2019-april 2024, waarbij de pleegdatum in elk geval lag na 1 maart 2019 (de dag waarop de Wet CCIII in werking trad). Verder is geselecteerd op basis van de afdoeningsdatum door het Openbaar Ministerie. Deze moest ook in de betreffende periode liggen, uiterlijk april 2024. In zaken waarin meerdere feiten voorkwamen (zowel CCIII-feiten als andere feiten), is per feit gecontroleerd of de betreffende CCIII-feiten daadwerkelijk zijn gedagvaard of geseponeerd. Deze stap was nodig om te bepalen of het CCIII-feit deel uitmaakte van de tenlastelegging, en dus potentieel door een rechter was beoordeeld. Er is vervolgens vastgesteld of de betreffende CCIII-feiten beoordeeld zijn door een rechter, en zo ja, of dit heeft geleid tot een veroordeling of vrijspraak ten aanzien van het CCIII-feit/ de CCIII-feiten. Ook hier is een specifieke tijdsperiode gehanteerd, namelijk op basis van de afdoeningsdatum van de zaak door de rechter (tot en met april 2024). Dit betreft de datum van het eindvonnis. De pleegdatum was ook hier vanaf 1 maart 2019.

[7] Dit geldt voor de zaken waarover een zittingsrechter zich gebogen heeft.

Op basis van de cijferoverzichten uit RAC-min konden we inzicht krijgen in het aantal opsporingsonderzoeken (hierna zaken) waarin de betreffende strafbaarstellingen voorkwamen en de wijze waarop het Openbaar Ministerie deze zaken had afgedaan (sepot, strafbeschikking, dagvaarding en administratieve beëindiging). Ook was op basis van deze cijferoverzichten duidelijk wat voor een sepot was opgelegd. Verder werd op basis van deze cijferoverzichten duidelijk hoe een zittingsrechter in eerste aanleg de zaak had afgedaan (strafoplegging, ter terechtzitting gevoegd, schuldigverklaring zonder oplegging van straf, ontslag van alle rechtsvervolging of vrijspraak). De cijferoverzichten uit RAC-min zijn ook gebruikt voor het selecteren van vonnissen voor de vonnisanalyse en voor het selecteren van zaken voor de zaaksinterviews. Dit geldt alleen voor de 138c-, 139g- en 326e-zaken.

In RAC-min stonden helaas geen gegevens over de inzet van de lokpuber, het nieuwe element in de artikelen 248a en 248e Sr. Om die reden hebben we via contacten met het Openbaar Ministerie en de politie en via het e-archief/rechtspraak.nl zicht proberen te krijgen op het aantal zaken waarin een lokpuber was ingezet. RAC-min biedt ook geen overzicht over het aantal keer dat de nieuwe bevoegdheden zijn ingezet. Het aantal keer dat de hackbevoegdheid is ingezet (en het soort zaken) hebben we opgevraagd bij het specialistisch team van de politie dat zich bezighoudt met de hackbevoegdheid (Digit-politie). Via contacten bij het Openbaar Ministerie, onder andere de BOB-coördinatoren, en bij de rechtspraak en via het e-archief/rechtspraak.nl, waar helaas maar een selectie van zaken te vinden was, hebben we geprobeerd een zo volledig mogelijk overzicht te krijgen van het aantal keer dat artikel 125p Sv was gebruikt.

1.4.3 Vonnisanalyse

Selectie vonnissen

Om zicht te krijgen op de wijze waarop de strafbaarstelling in de praktijk (deelvraag 2 en 3) is benut, hebben we voor alle wettelijke bepalingen een vonnisanalyse uitgevoerd. Dat betekent dat we alle beschikbare vonnissen hebben geanalyseerd waarin één of meer wettelijke bepalingen voorkwamen. Om deze vonnissen tot onze beschikking te krijgen zijn we op verschillende manieren te werk gegaan. Voor de artikelen 138c en 139g Sr (overnemen en helen van gegevens) hebben we gebruikgemaakt van RAC-min. Via RAC-min hadden we van alle zaken die de rechter in eerste aanleg behandeld had een versleuteld parketnummer tot onze beschikking. Deze parketnummers zijn over twee periodes aangeleverd, namelijk periode 1 maart 2019 tot 1 juli 2023 en periode 1 juli 2023 tot 1 april 2024. Vervolgens zijn deze parketnummers ontsleuteld en hebben we de ontsleutelde parketnummers gebruikt om de vonnissen op te zoeken op rechtspraak.nl en in het e-archief. Op rechtspraak.nl wordt een deel van de vonnissen gepseudonimiseerd gepubliceerd. In het Besluit selectiecriteria uitsprakendatabank Rechtspraak.nl, vernieuwd in 2024, zijn criteria vastgelegd op basis waarvan besloten wordt of een vonnis gepubliceerd wordt. De gepubliceerde vonnissen zijn voor iedereen toegankelijk. In het e-archief staan meer vonnissen dan op rechtspraak.nl, maar niet alle vonnissen. Vonnissen in het e-archief zijn niet gepseudonomiseerd. In het e-archief worden in principe alle vonnissen opgenomen die uitgesproken zijn door de meervoudige kamer (drie rechters). In de praktijk gebeurt dat niet altijd. Om toegang te krijgen tot het e-archief hebben wij een toestemmingstraject bij de Raad voor de Rechtspraak (RvdR) doorlopen. Via een door de RvdR verstrekte laptop hadden wij toegang tot de vonnissen.

Niet alle parketnummers, die wij op basis van RAC-min hadden verkregen, waren terug te vinden op rechtspraak.nl of in het e-archief. In dat geval hebben we onze contactpersoon bij de Raad voor de Rechtspraak gevraagd of wij het vonnis alsnog konden ontvangen. In 57 gevallen is dat niet gelukt, omdat de betreffende rechtbank de gevraagde vonnissen uiteindelijk niet verstrekte (er bestaat geen verplichting). In een aantal gevallen (9) hebben we wel vonnissen ontvangen. Dat betekent dat wij ons in dit onderzoek kunnen baseren op niet voor iedereen toegankelijke vonnissen, een belangrijke meerwaarde van dit evaluatieonderzoek. Een belangrijke reden waarom een deel van deze vonnissen niet gepubliceerd is, is dat het een vonnis betrof van een kinder- of politierechter. Deze worden doorgaans niet gepubliceerd.

Ook voor online handelsfraude hebben wij een groot deel van de vonnissen via bovenstaande weg verkregen. Omdat deze cijfers echter pas later beschikbaar waren hebben we op 6 mei 2024 zelf een zoekslag uitgevoerd op rechtspraak.nl en in het e-archief (zie bijlage 3 voor de uitgevoerde zoekslag). Een groot deel van de zaken kwam overeen met zaken die we uiteindelijk ook via RAC-min vonden. Een klein deel week af. Dat had onder andere te maken met het feit dat op rechtspraak.nl en in het e-archief ook vonnissen te vinden zijn die een uitspraak in hoger beroep betreffen. Deze staan niet in het RAC-min-systeem. Verder werd tijdens het onderzoek duidelijk dat het Openbaar Ministerie regelmatig besluit geen vervolging in te stellen in een online handelsfraude-zaak en dat burgers hiertegen in beroep gaan. Daarom zijn in de vonnisanalyse ook beschikkingen meegenomen die zien op een artikel 12-procedure. In deze procedure vragen burgers de rechter om te beslissen dat het Openbaar Ministerie alsnog vervolging in moeten stellen bij een zaak waarin het Openbaar Ministerie in een eerder fase heeft besloten dat niet te doen.

Voor de overige wettelijke bepalingen is een andere werkwijze gehanteerd om vonnissen te selecteren. Op basis van RAC-min konden weliswaar 271 zaken gevonden worden waarin artikelen 248a en/of 248e Sr (verleiden van minderjarigen en *grooming*) waren gebruikt, maar binnen deze grote hoeveelheid zaken was het niet mogelijk om de zaken eruit de filteren waarin een lokpuber was ingezet. Om die reden hebben we via ons netwerk en via rechtspraak.nl en het e-archief een beeld proberen te krijgen van de lokpuberzaken (zie wederom bijlage 3 voor de uitgevoerde zoekslag).

Ook voor de bevoegdheden hebben we een of meerdere zoekopdrachten uitgevoerd in het e-archief (zie bijlage 3). In tabel 1.1 staat per wettelijke bepaling het aantal geanalyseerde vonnissen weergegeven. In bijlage 3 staat ook het aantal vonnissen dat uiteindelijk niet geanalyseerd is, inclusief de reden waarom die vonnissen niet in de analyse zijn meegenomen.

Tabel 1.1 Aantal geanalyseerde vonnissen

Wettelijke bepaling	Aantal vonnissen
Strafbaarstellingen	
Artikel 138c Sr	11
Artikel 139g Sr	44
Artikel 326e Sr ➢ Vonnissen ➢ Beklagzaken	195 28 167
Artikelen 248a/248e Sr	11
Totaal	**261**
Bevoegdheden	
Artikel 125p Sv	4
Artikelen 126nba, 126uba en 126zpa Sv	10
Totaal	**14**

Uitvoering vonnisanalyse
Voorafgaand aan het uitvoeren van de vonnisanalyse zijn topiclijsten opgesteld met daarin de verschillende onderwerpen waaraan we tijdens de vonnisanalyse aandacht wilden schenken. Voor een deel kwamen de topiclijsten voor de verschillende wettelijke bepalingen overeen, maar er is bij elke wettelijke bepaling ook steeds gekeken of aanvullende topics nodig waren. Soms zijn gedurende de analyse nog topics toegevoegd. Per wettelijke bepaling zijn alle topics in een document gezet, met daarbij een instructie hoe deze topics gedurende de vonnisanalyse moesten worden gescoord. De topics zelf zijn uiteindelijk overgenomen in een Excel-bestand zodat de relevante tekstpassages uit de vonnissen per zaak overzichtelijk konden worden weergegeven. Op die manier kregen we voor alle vonnissen een goed beeld wat daarin naar voren kwam met betrekking tot de topics waarin wij geïnteresseerd waren. De ingevulde topiclijsten zijn uiteindelijk per topic verder geanalyseerd. Dat leidde soms tot een cijfermatig overzicht, bijvoorbeeld met betrekking tot de vraag in hoeveel zaken een strafbaarstelling alleen of samen met andere feiten in een zaak voorkwam. In andere gevallen is gekeken naar overeenkomsten en verschillen tussen de verschillende zaken met betrekking tot een bepaald topic, bijvoorbeeld wat een rechtbank overwoog ten aanzien van het artikel waarin wij geïnteresseerd waren.

1.4.4 Topic-gestuurde interviews

Algemene interviews
De vierde onderzoekmethode die gedurende dit onderzoek werd gebruikt is het topicgestuurde interview (Hutjes & Van Buuren, 1992). Deze interviews waren vooral bedoeld om zicht te krijgen op de uitvoering in de praktijk (deelvraag 2) en mogelijke gevolgen voor vooral de opsporingspraktijk, zowel bedoeld als onbedoeld (deelvraag 3). Twee soorten interviews vonden plaats: algemene en verdiepende interviews. De algemene interviews waren vooral bedoeld om een eerste beeld te krijgen hoe in de praktijk werd omgegaan met de wettelijke bepalingen uit de Wet CCIII. Tevens boden deze algemene interviews de mogelijkheid om onderwerpen te selecteren die in de verdiepende fase extra aandacht moesten krijgen. De algemene interviews werden gehouden met zowel medewerkers van de politie als met medewerkers van het

Openbaar Ministerie. Sommige van hen benaderden we omdat zij werkzaam zijn bij een landelijk programma dat zich bezighoudt met een thema gerelateerd aan één van de wettelijke bepalingen. Anderen geïnterviewden werden ons via contacten aangedragen, de zogenoemde sneeuwbalmethode. Omdat sommige bepalingen nauw met elkaar samenhangen, hebben we de algemene interviews georganiseerd rondom de volgende thema's: omgang met gegevens (artt. 138c en 139g Sr), zeden (artt. 248a en 248e Sr), fraude (art. 326e Sr), ontoegankelijkmaking (art. 125p Sv) en hackbevoegdheid (art. 126nba Sv). Bijna alle algemene interviews vonden plaats in de periode juni-augustus 2023. Een uitzondering hierop was een interview over artikel 125p Sv dat werd gehouden in maart 2024. De algemene interviews vonden plaats met zeven personen werkzaam bij de politie en met twaalf personen werkzaam bij het Openbaar Ministerie (officieren van justitie, onderzoeksjuristen en parketsecretarissen).

In het kader van het evalueren van de hackbevoegdheid hebben we wat betreft de technische kant van de inzet vijf overkoepelende 'update-interviews' gehouden. Deze waren vooral bedoeld om zicht te krijgen op de uitvoering in de praktijk, vooral of zich, sinds het verschijnen van de eerdere evaluatie, belangrijke veranderingen hadden voorgedaan met betrekking tot de belangrijkste aandachtspunten die wij in een eerdere evaluatie formuleerden (deelvraag 2). Er werd gesproken met personen werkzaam bij Digit-politie, bij Digit-OM, bij de Keuringsdienst van de politie, bij de Inspectie en bij het ministerie van Justitie en Veiligheid. Deze interviews vonden plaats in de periode november 2024 en augustus 2025. In tabel 1.2 staat per wettelijke bepaling het aantal afgenomen interviews weergegeven. De gemiddelde duur van een interview, berekend op basis van hele minuten, was 64 minuten.[8]

Tabel 1.2 Algemene interviews

Wettelijke bepaling	Aantal interviews	Aantal personen
Artikel 138c/139g Sr – stelen en helen van gegevens	3	5
Artikel 248a/248e Sr - lokpuber	3	6
Artikel 326e Sr – online handelsfraude	3	3
Artikel 125p Sv – ontoegankelijkmaking	3	5
Artikel 126nba Sv - hackbevoegdheid	5	7
Totaal	**17**	**26**

Verdiepende interviews

De verdiepende interviews hadden tot doel om concreter zicht te krijgen op wat de verschillende bepalingen in de uitvoeringspraktijk betekenen en wat de ervaringen zijn van de betrokken actoren. Daartoe zijn 34 zaaksinterviews uitgevoerd met medewerkers van het Openbaar Ministerie officieren van justitie, parketsecretarissen en onderzoeksjuristen. Tijdens die interviews werd vooral stilgestaan bij de ervaringen met de concrete zaak, maar werd ook gesproken over meer algemene ervaringen, zowel wat betreft zaken als wat betreft andere wettelijke bepalingen uit de Wet CCIII dan waar het interview in eerste instantie betrekking op had. In bijlage 2 wordt onder ander ingegaan op de wijze waarop de geïnterviewden zijn geselecteerd, hoe de gebruikte topiclijsten eruitzagen en op welke wijze verslaglegging van de interviews heeft plaatsgevonden.

[8] Eén interview is niet helemaal volledig uitgewerkt, omdat de geluidsopname per ongeluk al vernietigd was.

Ook is gesproken met vijf advocaten. Met drie advocaten[9] spraken wij over meerdere wettelijke bepalingen uit de Wet CCIII, en met twee advocaten hielden wij een interview over een concrete zaak. In beide gevallen betrof dit een 326e-zaak. Hoewel we graag meer advocaten hadden willen spreken, is dat niet gelukt. Een aantal van hen heeft geen gehoor gegeven aan een interviewverzoek. Ook een herhaald verzoek aan twee beroepsverenigingen (de Nederlandse Vereniging van Jonge StrafrechtAdvocaten en de Nederlandse Vereniging van StrafrechtAdvocaten) heeft geen reacties opgeleverd.

In tabel 1.3 staat per wettelijke bepaling het aantal interviews weergegeven. Daarin is ook het aantal advocaten meegenomen waarmee gesproken is. De gemiddelde duur van een interview, berekend op basis van hele minuten, was 59 minuten.

Tabel 1.3 Verdiepende (zaaks)interviews

Wettelijke bepaling	Aantal interviews[a]	Aantal personen
Artikel 138c Sr – overnemen gegevens	5[b]	5
Artikel 139g Sr – helen gegevens	5	6
Artikel 326e Sr – online handelsfraude	6	6
Artikel 248a/248e Sr – lokpuber	4	4
Artikel 125p Sv – ontoegankelijkmaking	6[c]	9
Artikel 126nba Sv – hackbevoegdheid	13	15
Totaal	**39**	**45[d]**

a Voor zowel online handelsfraude als het helen van gegevens zijn meer personen benaderd dan we uiteindelijk gesproken hebben.

b Eén interview betrof geen mondeling interview. In plaats daarvan heeft een onderzoeksjurist een aantal vragen via e-mail beantwoord.

c In sommige interviews zijn meerdere zaken besproken. Verder is bij twee personen twee keer een interview afgenomen. Dit is geteld als één interview, beide zijn ook één keer meegeteld bij het aantal personen, omdat de interviews over één wettelijke bepaling gingen.

d Eén persoon is twee keer geïnterviewd, beide keren voor een andere wettelijke bepaling uit de Wet CCIII. Deze persoon is bij beide wettelijke bepalingen één keer meegeteld.

1.4.5 Vragenlijst

De vijfde onderzoeksmethode die we hebben gebruikt is het afnemen van een vragenlijst over de hackbevoegdheid. Deze onderzoeksmethode is alleen toegepast voor het evalueren van de hackbevoegdheid. Deze vragenlijst was bedoeld om de tweede en derde deelvraag inzake de hackbevoegdheid te kunnen beantwoorden. De vragenlijst bestond uit negentien, vooral gesloten vragen. De volgende onderwerpen kwamen in de vragenlijst aan bod (zie bijlage 4 voor de volledige vragenlijst):

- algemeen (het aantal opsporingsonderzoeken, het aantal bevelen dat in één onderzoek is afgegeven en de misdrijven waarnaar onderzoek werd gedaan);
- doel en noodzaak inzet hackbevoegdheid;
- binnendringen;
- verzamelen van gegevens;

[9] Eén interview is opgenomen bij artikel 125p Sv, één interview bij artikel 126nba Sv en één interview bij artikel 139g Sr.

- opbrengst binnen het opsporingsonderzoek;
- afronding (inhoudelijke behandeling zittingsrechter).

In de introductie van de vragenlijst is aangegeven dat het invullen van de vragenlijst vrijwillig was en dat de e-mails met de ingevulde vragenlijst in PDF na afronding van het onderzoek vernietigd zouden worden. Gedurende de onderzoeksperiode is aan elke toegestuurde vragenlijst een nummer toegekend, waardoor tijdens het onderzoek achterhaald kon worden wie de vragenlijst had ingevuld. Dit in verband met het versturen van reminders en het stellen van aanvullende vragen. De ingevulde vragenlijst zelf, waarop geen persoonsgegevens te vinden zijn van degene die hem ingevuld heeft, blijft wel bewaard na afloop van het onderzoek.

De vragenlijst is in december 2024 via e-mail verstuurd naar alle officieren van justitie die in de periode maart 2019-april 2024 in één of meerdere onderzoeken de hackbevoegdheid hadden ingezet. Het ging om 107 officieren van justitie. In januari 2025 zijn twee reminders verstuurd naar degenen die nog geen vragenlijst hadden ingevuld. Verder is naar enkele officieren van justitie een persoonlijke reminder gestuurd, omdat één van de onderzoekers hen eerder gesproken had. Uiteindelijk hebben 68 officieren van justitie een vragenlijst teruggestuurd (responspercentage 63,5%). Twee ingevulde vragenlijsten zijn verder niet meegenomen in de analyse: één vragenlijst betrof een vragenlijst die al door een collega officier van justitie was ingevuld en een andere vragenlijst was niet ingevuld, omdat alle onderzoeken waaraan deze officier van justitie had meegewerkt een buitenlandcomponent bevatte.

De ingevulde vragenlijsten in PDF zijn omgezet naar één Excel-bestand. Vervolgens is dit Excel-bestand klaargemaakt voor het kunnen doen van beschrijvende analyses (alle stappen zijn bijgehouden in een logboek). In sommige vragenlijsten bleken niet alle vragen ingevuld of spraken antwoorden elkaar tegen. Bij een aantal vragenlijsten, vooral de vragenlijsten ingevuld door officieren van justitie waarmee ook zaaksinterviews zijn gehouden, is aan de betreffende officier van justitie gevraagd welk antwoord juist was. Die antwoorden hebben de onderzoekers zelf aan het Excel-bestand toegevoegd. In sommige gevallen hebben onderzoekers antwoorden gecorrigeerd of aangepast op basis van andere informatie in de vragenlijst of in het geval invoerfouten werden vastgesteld. Dat gebeurde alleen als het juiste antwoord met behulp van andere gegevens antwoorden te achterhalen was. Een voorbeeld hiervan is een respondent die een open antwoord had gegeven, naar niet de optie ‘anders’ had aangevinkt. Een ander voorbeeld is wanneer bij een open antwoord precies het antwoord stond dat bij een gesloten vraag ingevuld had kunnen worden. In dat geval is het open antwoord verwijderd en een gesloten antwoord aangevinkt. Op basis van het Excel-bestand zijn beschrijvende figuren en tabellen gemaakt die in hoofdstuk 7 zijn opgenomen.

1.4.6 Analyse

De analyse van het verzamelde (empirisch) materiaal heeft in twee delen plaatsgevonden. Het eerste deel van de analyse betrof de analyse van de wetsgeschiedenis met betrekking tot alle wettelijke bepalingen van de Wet CCIII behalve de hackbevoegdheid. Dat laatste was al gebeurd in het kader van de eerdere evaluatie. Ook heeft in deze fase, na de analyse van de wetsgeschiedenis, een eerste analyseslag plaatsgevonden van de algemene interviews. Dit gebeurde vooral handmatig en de uitkomsten vormden belangrijke input voor de verdere invulling van de evaluatie.

Het tweede deel van de analyse betrof het empirisch materiaal dat verzameld is in de verdiepende fase. Per wettelijke bepaling heeft een aparte analyse plaatsgevonden. Het analysewerk is over drie onderzoekers verdeeld. Elk van hen namen één of meerdere wettelijke bepalingen voor hun rekening. De wijze waarop de vonnissen, de RAC-min cijfers en de ingevulde vragenlijsten zijn geanalyseerd is eerder in het hoofdstuk al aan de orde gekomen. Voor het analyseren van de interviews en een deel van de vonnisanalyse is gebruikgemaakt van het analyseprogramma MAXQDA. Op basis van de onderzoeksvragen is een aantal codes aangemaakt. Vervolgens zijn gedurende het analyseproces open codes toegevoegd. Voorbeelden hiervan zijn de codes 'aandachtspunten', 'aard zaken', 'aanpak online handelsfraude' en 'ontoegankelijkmaking in de praktijk' die nader gespecificeerd zijn door middel van subcodes. Vooral in het begin van het analyseproces vond overleg plaats tussen de onderzoekers over de toegekende codes. Na deze eerste analyseslag heeft handmatig een volgende analyseslag plaatsgevonden waarbij verschillende codes weer werden samengevoegd. Zo zijn verschillende subcodes rondom bijvoorbeeld capaciteit en buitenland, weer teruggebracht tot de respectievelijke overkoepelende thema's 'capaciteit' en 'buitenland'. Deze thema's zijn vervolgens gebruikt voor het schrijven van het rapport.

1.5 Opbouw rapport

Dit rapport is als volgt opgebouwd. De hoofdstukken 2 tot en met 7 gaan elk over één of twee nieuwe wettelijke bepalingen uit de Wet computercriminaliteit III. Hoofdstuk 2 en 3 richten zich op respectievelijk het stelen en helen van gegevens, hoofdstuk 4 gaat over online handelsfraude en hoofdstuk 5 over de inzet van de lokpuber. Daarna richt de aandacht zich op de nieuwe bevoegdheden: de ontoegankelijkmaking van gegevens (hoofdstuk 6) en de hackbevoegdheid (hoofdstuk 7). Het rapport besluit met hoofdstuk 8 waarin antwoord wordt gegeven op de hoofdvraag en waarin een aantal overkoepelde thema's worden besproken die meerdere wettelijke bepalingen uit de Wet CCIII raken.

2 Stelen van gegevens (art. 138c Sr)

In dit hoofdstuk wordt ingegaan op het stelen van gegevens (art. 138c Sr). Allereerst wordt het juridisch kader van dit wetsartikel uiteengezet (paragraaf 2.1). Vervolgens wordt de noodzaak voor het nieuwe wetsartikel (volgens de wetgever) besproken, alsmede de veronderstellingen die aan het nieuwe wetsartikel ten grondslag liggen. Daarmee wordt ook meteen ingegaan op de doelstelling van de wetgever (paragraaf 2.2). Daarna wordt ingegaan op de wijze waarop artikel 138c Sr in de praktijk gebruikt is (paragraaf 2.3). Er wordt aandacht besteed aan de aard van de 138c-zaken (paragraaf 2.3.3). Daarna richt de aandacht zich op de belangrijkste voordelen voor de opsporingspraktijk en de aandachtspunten van het nieuwe artikel (paragraaf 2.3.4 en 2.3.5). Het hoofdstuk besluit met een paragraaf waarin de veronderstellingen van de wetgever gelegd worden naast het wijze waarop artikel 138c Sr in de praktijk benut is (paragraaf 2.4).

2.1 Juridisch kader

Artikel 138c Sr, waarin het overnemen van gegevens strafbaar wordt gesteld, luidde ten tijde van de inwerkingtreding van de Wet CCIII als volgt:

> Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt gestraft degene die opzettelijk en wederrechtelijk niet-openbare gegevens die zijn opgeslagen door middel van een geautomatiseerd werk, voor zichzelf of voor een ander overneemt.

Op 1 mei 2021 zijn, vanwege de implementatie van de Europese richtlijn 2019/713/EU van het Europees parlement en de Raad van 17 april 2019 betreffende de bestrijding van fraude met en vervalsing van niet contante betaalmiddelen en ter vervanging van het Kaderbesluit 2001/413/JBZ van de Raad, lid 2 en 3 aan het wetsartikel toegevoegd. Het artikel luidt sindsdien als volgt:

1 Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt gestraft degene die opzettelijk en wederrechtelijk niet-openbare gegevens die zijn opgeslagen door middel van een geautomatiseerd werk, voor zichzelf of voor een ander overneemt of doorgeeft.
2 Indien de gegevens een niet-contant betaalinstrument betreffen, wordt de schuldige gestraft met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie.
3 Indien het feit wordt gepleegd met het oogmerk om zich of een ander wederrechtelijk te bevoordelen, wordt de schuldige gestraft met gevangenisstraf van ten hoogste drie jaren of geldboete van de vierde categorie.

2.2 Noodzaak en veronderstellingen

In de memorie van toelichting staat beschreven dat ontwikkelingen van informatie en communicatietechnologie het steeds gemakkelijker maken om gegevens uit een computer over te nemen en die op het internet te plaatsen. Vertrouwelijke gegevens kunnen op die manier snel verspreid worden en het is lastig om die gegevens volledig

te verwijderen van het internet. Daarom achtte de wetgever 'verdere strafrechtelijke bescherming van gegevens' nodig. Dat werd vooral belangrijk gevonden omdat de persoonlijke levenssfeer moest worden beschermd van degene van wie de gegevens zijn. Strafrechtelijke bescherming werd ook nodig geacht in gevallen dat een verdachte gegevens in zijn bezit heeft die door een misdrijf zijn verkregen, bijvoorbeeld bankgegevens die middels *phishing* zijn verkregen (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 62).

In de eerste Wet computercriminaliteit is onderscheid gemaakt tussen de begrippen goed en gegevens. In het Wetboek van Strafrecht zijn bepalingen opgenomen die betrekking hebben op gegevens. In lijn daarmee heeft de wetgever besloten artikelen 138c en 139g Sr (zie hoofdstuk 3) in de Vijfde Titel van het Tweede Boek van het Wetboek van Strafrecht op te nemen (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 63) in plaats van het overnemen en helen van gegevens strafbaar te stellen als diefstal, verduistering en heling (artt. 310, 321, 416 en 417bis Sr) (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 65). In het Tweede Boek waren al een aantal artikelen strafbaar gesteld die verband houden met de nieuwe wetsartikelen.[10] De wetgever achtte het echter wenselijk, vanwege ontwikkelingen op het terrein van informatie- en communicatietechnologie, de strafrechtelijke bescherming van gegevens te versterken door het wederrechtelijk overnemen van gegevens in zijn algemeenheid strafbaar te stellen (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 64). Die toevoeging werd ook nodig geacht omdat artikel 138ab Sr (computervredebreuk) niet in alle gevallen bruikbaar is, namelijk wanneer gegevens niet door computervredebreuk zijn verkregen, bijvoorbeeld wanneer rechtmatig toegang kan worden verkregen tot niet openbare-gegevens, maar deze wel wederrechtelijk worden overgenomen. Denk hierbij aan een werknemer die vanuit zijn of haar functie toegang heeft tot bepaalde gegevens, deze gegevens kopieert om die vervolgens voor anderen of voor zichzelf te gebruiken (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 64).

Op basis van het voorgaande kan de volgende veronderstelling geformuleerd worden:

> Ontwikkelingen op het gebied van ICT maken het steeds gemakkelijker om gegevens uit een computer over te nemen en op het internet te plaatsten. Dat leidt er (ook) toe dat gegevens gemakkelijker gestolen kunnen worden. Vóór inwerkingtreding van de Wet CCIII konden stelers en helers van gegevens niet goed worden vervolgd, omdat bestaande wettelijke regelingen niet voldeden. Daardoor konden gegevens minder goed strafrechtelijk worden beschermd. Het nieuwe wetsartikel stelen van gegevens (art. 138c Sr) leidt ertoe dat gegevens beter dan voorheen tegen het overnemen ervan kunnen worden beschermd. Door deze nieuwe strafbaarstelling wordt het mogelijk personen te vervolgen die, voor zichzelf of voor een ander, wederrechtelijk niet-openbare gegevens kopiëren waar zij op rechtmatige wijze toegang toe hadden. Dit leidt ertoe dat voortaan degene die wederrechtelijk gegevens overneemt vervolgd kan worden. Hierdoor zijn gegevens beter strafrechtelijk beschermd.

[10] Het wederrechtelijk overnemen van gegevens sluit hier bij aan. Het gaat om de volgende artikelen: het wederrechtelijk aftappen en opnemen van gegevens die zijn opgeslagen middels een geautomatiseerd werk (art. 139c Sr), het overnemen van gegevens uit een geautomatiseerd werk door iemand die daarin wederrechtelijk is binnengedrongen (art. 138ab lid 2 Sr) en het wederrechtelijk overnemen van gegevens door een aanbieder van een telecommunicatienetwerk- of dienst (art. 273d Sr).

2.3 Artikel 138c Sr in de praktijk

2.3.1 Instroom en afdoening Openbaar Ministerie

In tabel 2.1 wordt een overzicht gegeven van de wijze waarop het Openbaar Ministerie 138c-zaken heeft afgehandeld. Deze gegevens zijn gebaseerd op cijfers uit RAC-min. Daarin staat informatie over de instroom van zaken bij het Openbaar Ministerie en over de afhandeling van die zaken door het Openbaar Ministerie en door de rechter in eerste aanleg (Verweij & Tollenaar, 2022, p. 12).

Tabel 2.1 Afdoening Openbaar Ministerie artikel 138c Sr

Afdoening Openbaar Ministerie	Aantal
Dagvaarding	23
➢ Geen sepot	22
➢ Sepot 138c-feit	1
OM-strafbeschikking	2
Sepots	14
➢ Onvoorwaardelijk	13
➢ Voorwaardelijk	1
Totaal	**39**

Tabel 2.1 laat zien dat in de periode maart 2019-april 2024 het Openbaar Ministerie 39 zaken heeft behandeld waarin artikel 138c Sr ten minste één keer voorkwam. Het betreft hierbij zaken met een pleegdatum van het gepleegde strafbare feit in de periode 1 maart 2019 tot en met 30 april 2024. In net iets meer dan de helft van de zaken (22) heeft de verdachte een dagvaarding ontvangen voor het 138c-feit en in twee zaken ontving de verdachte een OM-strafbeschikking. Verder zijn 14 zaken geseponeerd zonder dat een dagvaarding is uitgereikt. Het ging hierbij zowel om voorwaardelijke (1) als onvoorwaardelijke (13) sepots.

Er zijn verschillende redenen voor het seponeren van een 138c-feit. Deze staan in tabel 2.2 weergegeven:

Tabel 2.2 Sepotgronden artikel 138c Sr*

Sepotgronden	Aantal
Dagvaarding	1
➢ Onvoldoende bewijs	1
Onvoorwaardelijk sepots	13
➢ Onvoldoende bewijs	6
➢ Beperkte kring[a]	1
➢ Ander dan strafrechtelijk ingrijpen prevaleert	1
➢ Door feit of gevolg getroffen[b]	1
➢ Feit dubbel ingeboekt	1
➢ Maatschappelijk belangenconflict	1
➢ Ten onrechte als verdachte aangemerkt	2
Voorwaardelijk sepots	1
➢ Door feit of gevolg getroffen	1

* In deze tabel staat het aantal unieke sepotgronden weergegeven. Het kan voorkomen dat in één zaak een CCIII-feit meerdere keren voorkomt, en ook meerdere keren geseponeerd wordt.

a Sepotcode 73: Het feit heeft zich in zo beperkte kring afgespeeld – gezin, buren, e.d. – dat, in verband met de mate van ernst van het feit, onvoldoende gemeenschapsbelang aanwezig lijkt om een strafvervolging te rechtvaardigen.

b Sepotcode 52: Door eigen letsel; door letsel of verlies van naasten; in zijn maatschappelijke positie of in de verhouding tot zijn naaste omgeving; door ernstige financiële schade, rechtstreeks uit het feit voortvloeiend of door verplichte schadevergoeding; door een reactie van de overheid op het gepleegde feit, welke reactie voldoende representatief, te zwaar of minder juist blijkt te zijn geweest, bijv. inverzekeringstelling, hard politieoptreden of onjuiste formaliteiten.

2.3.2 Vonnissen rechtbank

In de periode maart 2019-april 2024 zijn 15 zaken ingestroomd bij de rechtbank waarbij ook een eindvonnis voor de onderzoekers beschikbaar was. In tabel 2.3 is te zien op welke wijze de rechter deze zaken heeft afgedaan. In een groot deel van de zaken (12) legde de rechter een straf op voor ten minste 1 138c Sr-feit.

Tabel 2.3 Gerechtelijke afdoening artikel 138c Sr

Afdoening*	Aantal
Schuldigverklaring zonder oplegging van straf of maatregel	1
Strafoplegging	12
Vrijspraak	2
Totaal	**15**

* Hierin is één zaak meegenomen die ter terechtzitting gevoegd was.

2.3.3 Aard artikel 138c Sr-zaken

Voor de vonnisanalyse hebben wij 14 zaken nader bestudeerd. Het ging daarbij om 9 vonnissen in eerste aanleg, 1 vonnis van een politie- of kinderrechter en 1 vonnis in

hoger beroep. Daarnaast namen wij zaaksinterviews af. Van alle zaken die tijdens de zaaksinterviews aan bod kwamen hadden wij niet altijd het vonnis tot onze beschikking, omdat doorgaans niet elk vonnis wordt gepubliceerd. Uit de vonnisanalyse en de interviews blijkt dat in een klein aantal zaken (vier) het stelen van gegevens het enige feit was dat in de tenlastelegging stond opgenomen. In al deze zaken werden de gegevens gestolen in een werksituatie. In de eerste zaak (ECLI:NL:RBROT:2022:8560) verstrekte de verdachte gegevens uit de Basisregistratie Personen (BRP) aan een collega. Deze collega werkte bij dezelfde organisatie als de verdachte, maar kon zelf niet over de gegevens beschikken. Het ging hier om een organisatie die voor verschillende bedrijven de administratie verzorgt. De verstrekker van de gegevens had de gegevens niet mogen verstrekken, omdat de collega in een ander team én voor een ander bedrijf werkte. In de tweede zaak (ECLI:NL:RBOVE:2023:2524) betrof het stelen van gegevens het overnemen en doorgeven van toetsvragen. Deze stonden opgeslagen in het toetsopslagsysteem van een hogeschool. De verdachte had vanuit zijn functie rechtmatig toegang tot dit systeem, maar gebruikte deze toegang om wederrechtelijk gegevens over te nemen, namelijk op verzoek van twee studenten die de verdachte hiervoor betaalden. De derde zaak (ECLI:NL:RBGEL:2023:4766), waarin artikel 138c Sr het enige artikel in de tenlastelegging was, draaide om een werknemer die in de tandartsenpraktijk waar hij werkte, vertrouwelijke en persoonlijke informatie had overgenomen. Het betrof verslagen van functioneringsgesprekken, arbeidsovereenkomsten en een kopie van een paspoort. In de vierde en laatste zaak, zo blijkt uit een mailwisseling met een betrokkene vanuit het Openbaar Ministerie, draaide het om een werknemer die een filmpje had gemaakt van de klantgegevens van één persoon. Met dit filmpje, dat de verdachte plaatste op het socialemediakanaal Telegram, wilde de verdachte laten zien dat dergelijke contactgegevens bij hem te koop waren. De verdachte is hiervoor uiteindelijk vrijgesproken, omdat niet bewezen kon worden dat het de verdachte was die het filmpje had gemaakt.

In de andere zaken ging het stelen van gegevens samen met andere bepalingen uit het Wetboek van Strafrecht. Op basis van de vonnisanalyse en de interviews kan een aantal categorieën zaken onderscheiden worden waarin het stelen van gegevens samen voorkomt met andere bepalingen uit het Wetboek van Strafrecht, namelijk afpersing/afdreiging, vervalsing van geschriften, drugshandel en misdrijven die een inbreuk maken op de (relationele) levenssfeer. Ook deze zaken hebben betrekking op de werksituatie. Een uitzondering hierop zijn de casussen waarin het stelen van gegevens samenging met misdrijven die zich afspelen in de persoonlijke (relationele) levenssfeer.

Combinatie met afpersing en dreiging
In één zaak, waarin twee zaken met elkaar gecombineerd werden, (ECLI:NL:RBAMS:2021:5168) maakte een werknemer van een afhaalrestaurant foto’s van het computersysteem waarin bestelgegevens van klanten stonden. Vervolgens gebruikte de verdachte deze gegevens om klanten dreigende teksten te sturen om hen te dwingen geld over te maken naar zijn rekening. In dat opzicht was er een directe relatie tussen de gestolen gegevens en het andere misdrijf.

Combinatie met vervalsing van geschriften
In twee zaken draaide het om een vader (ECLI:NL:RBNNE:2021:394) en zoon (ECLI:NL:RBNNE:2021:395) die eindexamenfraude pleegden. De vader was werkzaam op de school waar zijn zoon eindexamen moest doen. Op illegale wijze namen beiden centrale examens van een cd-rom over. Na het eindexamen paste de zoon voor een

aantal vakken de eerder door hem ingevulde formulieren aan. Het overnemen van de examens was in deze zaken het tenlastegelegde 138c-feit. Beide verdachten zijn hiervoor echter (deels) vrijgesproken, omdat een deel van de overname is gebeurd door het maken van kopieën van papier naar papier: die examens waren niet opgeslagen middels een computer of andere gegevensdrager. Overname van gegevens van een geautomatiseerd werk is echter wel nodig om het feit wettig en overtuigend te bewijzen zo blijkt uit beide vonnissen. Een deel van de overname vond plaats door een kopie te maken van een cd-rom, wat in het vonnis wel aangemerkt is als geautomatiseerd werk. Deze verdachten zijn ook veroordeeld voor het medeplegen van valsheid in geschrifte (art. 225 Sr) en diefstal in vereniging (art. 311 Sr). Beide feiten waren direct gerelateerd aan het 138c-feit.

Combinatie met drugshandel
In één van de zaken hield de verdachte zich, samen met anderen, bezig met voorbereidingshandelingen voor de invoer van en de handel in cocaïne (ECLI:NL:RBNHO:2023:7896). Ook nam de verdachte niet-openbare gegevens over uit het KLM-systeem waarin vlucht-, transfer- en cargogegevens opgeslagen worden, het 138c-feit. Deze gegevens lijken te zijn gebruikt voor de voorbereidingshandelingen, omdat in de bewezenverklaring onder andere staat beschreven dat de verdachte chatgesprekken voerde met anderen waarbij de verdachte informatie en foto's uit het systeem van KLM deelde.

Combinatie met misdrijven (relationele) levenssfeer
In vier zaken kwam het stelen van gegevens samen voor met misdrijven die inbreuk maken op de relationele levenssfeer van het slachtoffer. In twee van deze zaken waren de verdachte en het slachtoffer voormalig liefdespartners. In de eerste zaak (niet-openbaar vonnis) ging het om bedreiging en mishandeling van een ex-partner. Daarnaast had de verdachte een lijst met honderden buitenlandse telefoonnummers, afkomstig uit één land, in zijn bezit die hij had verkregen via het socialemediakanaal Telegram. Deze had hij verkregen nadat hij expliciet om telefoonnummers van vrouwen had gevraagd. In de tenlastelegging was de lijst met telefoonnummers het 138c-feit, dat overigens subsidiair ten laste was gelegd. Primair was dat het helen van gegevens. De verdachte is voor het primaire feit veroordeeld. De gevonden telefoonnummers lijken verder niet gerelateerd te zijn aan de andere feiten. Een directe link tussen het stelen van gegevens en de andere feiten is wel aanwezig in de tweede zaak. In deze casus (niet-openbaar vonnis) nam de verdachte twee naaktfoto's van zijn ex-partner voor zichzelf over, terwijl hij daartoe niet gerechtigd was – het 138c-feit dat subsidiair ten laste was gelegd.[11] Aan deze verdachte was ook smaad ten laste gelegd, maar daar is de verdachte voor vrijgesproken, omdat het slachtoffer niet tijdig aangifte had gedaan. Tussen de naaktfoto's en smaad bestond een directe link. In de derde zaak is de precieze relatie tussen de verdachte en het slachtoffer onbekend gebleven. In deze zaak maakte de verdachte zich schuldig aan *stalking* en inbraak in de woning van het slachtoffer, zo blijkt uit een interview met een medewerker van het Openbaar Ministerie. Daarnaast kopieerde hij video- en beeldmateriaal van de computer van het slachtoffer – het 138c-feit. Het is onduidelijk of dit materiaal is gebruikt voor de *stalking*. Wel was er een directe relatie met de inbraak. In de vierde zaak (ECLI:NL:RBNNE:2021:3628), waarin geen sprake was van een (voormalig) liefdesrelatie, maakte de verdachte zich gedurende een lange periode telkens opnieuw schuldig aan het belagen van het slachtoffer door op verschillende manieren contact met haar te zoeken. Daarnaast maakte de verdachte zich schuldig aan de heling van een telefoon. Verder zijn bij de verdachte zogenoemde

[11] Primair was computervredebreuk (art. 138ab Sr) ten laste gelegd. De verdachte is daarvoor vrijgesproken.

'combolijsten' aangetroffen, lijsten met gebruikersnamen en/of e-mailadressen en wachtwoorden die de verdachte zelf zou hebben overgenomen – het 138c-feit. Deze lijsten lijken in deze zaak verder niet gerelateerd te zijn aan de andere feiten.

Eén van de geïnterviewden werkzaam bij het Openbaar Ministerie merkt op dat artikel 138c Sr ook heel geschikt zou kunnen zijn voor het vervolgen van diefstal, gepleegd door medewerkers van de GGD, van persoonsgegevens van mensen die bij de GGD een coronatest hebben laten doen. Een dergelijke zaak is niet teruggevonden in de vonnisanalyse. Een mogelijke verklaring hiervoor is dat in zo'n zaak niet het stelen van gegevens (primair) ten laste is gelegd, maar computervredebreuk (art. 138ab Sr) (zoals bijvoorbeeld in deze zaken is gebeurd: ECLI:NL:RBMNE:2022:55; ECLI:NL:RBMNE:2022:3538; ECLI:NL:RBMNE:2021:4434). Een andere verklaring zou kunnen zijn dat er nog geen uitspraak is in een dergelijke zaak waarin artikel 138c Sr primair ten laste was gelegd.

Hoofdpunten

- In een meerderheid van de zaken werd artikel 138c Sr samen met andere feiten tenlastegelegd. De volgende categorieën zaken zijn onderscheiden: combinatie met afpersing en afdreiging, combinatie met valsheid in geschrifte, combinatie met drugshandel en combinatie met misdrijven in de (relationele) levenssfeer.
- Het grootste deel van de zaken speelde zich af in een werkcontext.
- Als sprake is van een combinatie van feiten in de tenlastelegging, dan werden in de meerderheid van de zaken de gestolen gegevens gebruikt voor het plegen van de andere feiten.

Soort en hoeveelheid gegevens

In het grootste deel van de zaken werden persoonlijke gegevens gestolen. Daarbij ging het om (offline) persoonsgegevens. Voorbeelden hiervan zijn gegevens van dertien klanten die bij een afhaalrestaurant hun eten hadden besteld en gegevens van één klant van een energiemaatschappij. Naast klantgegevens werden persoonsgegevens uit de BRP, honderden buitenlandse telefoonnummers en een kopie van een paspoort gestolen. In die laatste zaak was ook sprake van de diefstal van verslagen van functioneringsgesprekken en arbeidsovereenkomsten. Naast offline persoonsgegevens, draaide het in één zaak om (online) persoonsgegevens. Daarbij ging het om zogenoemde 'combolijsten', e-mailadressen en/of gebruikersnamen en wachtwoorden. Een ander soort persoonlijk gegeven betreft afbeeldingen[12]. Het ging daarbij om foto's en video-opnames, al dan niet met een seksuele lading (niet-openbaar vonnis en interview). Naast persoonlijke gegevens draaide het in vier zaken om toetsgegevens van een onderwijsinstelling. In twee zaken betroffen de gegevens eindexamens en antwoordmodellen van acht middelbare schoolvakken (ECLI:NL:RBNNE:2021:394; ECLI:NL:RBNNE:2021:395). In twee andere zaken draaide het om toetsen die op een hogeschool afgenomen werden (ECLI:NL:RBOVE:2023:2524; ECLI:NL:RBOVE:2023:2917).

De omvang van het aantal gestolen gegevens varieert. Uit het voorgaande werd deels al duidelijk dat het niet gaat om lijsten met honderden gegevens. Een uitzondering hierop vormen de honderden buitenlandse telefoonnummers. In sommige gevallen is niet duidelijk geworden om hoeveel gegevens het ging, bijvoorbeeld bij de persoonsgegevens afkomstig uit de BRP en bij de toetsen die gestolen werden op een hogeschool. Een medewerker van het Openbaar Ministerie merkt op dat een klein

[12] Afbeeldingen van persoonsgegevens, zoals foto's van bestelbonnen met klantgegevens van een afhaalrestaurant horen niet binnen deze categorie.

aantal gegevens geen reden hoeft te zijn om niet over te gaan tot vervolging. Deze medewerker was betrokken bij een zaak waarbij de verdachte klantgegevens van één klant op het socialemediakanaal Telegram plaatsten. Op die manier liet hij zien dat mensen bij hem klantgegevens konden kopen. Hoewel het overnemen van klantgegevens van één klant 'een relatief kleine inbreuk' betrof, vond het Openbaar Ministerie het van belang om toch tot vervolging over te gaan, onder andere vanwege de 'potentiële inbreuk' die het zou hebben als alle persoonsgegevens overgenomen zouden zijn.

Hoofdpunten

- In de 138c-zaken draait het om verschillende soorten gegevens die worden gestolen.
- In het grootste deel van de zaken werden persoonlijke gegevens gestolen, zowel online als offline.
- De omvang van het aantal gestolen gegevens is niet altijd duidelijk geworden. In de zaken waarin dit wel bekend was, bleef het aantal beperkt.

2.3.4 Voordelen voor de opsporingspraktijk

Uit de interviews komt naar voren dat artikel 138c Sr op verschillende manieren van nut kan zijn voor de opsporingspraktijk. Ten eerste past het artikel in een aantal zaken goed bij de handelingen die een verdachte verricht heeft, vooral in een werksituatie. Doorgaans heeft de verdachte in dat soort situaties legitiem toegang tot de gegevens[13] waardoor vervolging lastig is/kan zijn. Eén van de geïnterviewden, werkzaam bij het Openbaar Ministerie en betrokken bij de zaak rondom examendiefstal, merkt op dat er waarschijnlijk geen alternatief was geweest voor artikel 138c Sr, omdat bij diefstal van gegevens geen sprake is van 'gewone' diefstal[14]:

> Interviewer: Stel de artikelen waren er niet geweest. Hoe was zo'n zaak dan aangevlogen? Heb je daar enig idee van?
>
> Geïnterviewde: Dat is een goeie vraag. Dan wordt die lastig. Want in dit geval waren de toetsen digitaal ontvreemd. Dus gaat diefstal in principe niet op. (…). Het origineel is er nog gewoon. (…) Volgens mij heb je dan weinig grond om, om iets ten laste te leggen. (…) Dan had je moeten gaan kijken van, goh had je iets met (…) oplichting of valsheid in geschrifte ofzo [kunnen doen]. Witwassen ergens. (…). Dan wordt het echt puzzelen. (…). Dan moet je gaan knutselen om zoiets in elkaar te zetten.

Vervolging kan ook lastig zijn omdat in de eindexamen-zaak geen sprake hoeft te zijn van computervredebreuk (art. 138ab Sr), er kon immers legitiem toegang worden verkregen. Een andere geïnterviewde, werkzaam bij het Openbaar Ministerie, legt uit dat het in een werksituatie voor het onderscheid tussen de artikelen 138c Sr en 138ab Sr belangrijk is om goed te kijken naar het moment waarop de gegevens zijn overgenomen. Als iemand gedurende zijn werkdag besluit om gegevens over te

[13] Er kunnen overigens ook situaties zijn waarbij iemand legitiem toegang had, zonder dat sprake is van een werksituatie. Eén van de geïnterviewden, een officier van justitie, geeft aan dat het bijvoorbeeld kan gaan om iemand die met toestemming inloggegevens heeft van een socialemedia-account en daaruit gegevens overneemt.

[14] De Hoge Raad wees op 10 juni 2017 al naar een arrest waarin de Raad dezelfde redenering volgt. Uit de feiten in deze zaak kon niet worden afgeleid dat de 'fotografische opnames van gestolen eindexamenopgaven' en 'een gegevensdrager met daarop opgeslagen afbeeldingen van eindexamenopgaven' waren gestolen. Daardoor konden de foto's en de gegevensdrager niet aangemerkt worden als door diefstal verkregen goederen zoals bedoeld in artikel 416 Sr (ECLI:NL:HR:2017:2573).

nemen, dan kun je volgens hem niet spreken van computervredebreuk. De situatie wordt in zijn ogen anders wanneer de werknemer op een dag dat hij ziek is, inlogt en dan gegevens voor hemzelf overneemt. Dan zou sprake kunnen zijn van computervredebreuk, met artikel 138c Sr 'als vangnet'. Volgens deze geïnterviewde vult artikel 138c Sr een leemte, namelijk waar 'computervredebreuk niet te bewijzen is of op veel verweer zou kunnen stuiten'. Volgens twee andere geïnterviewden, beide werkzaam als officier van justitie én die artikel 138c Sr nauwelijks gebruiken in hun praktijk, is in werksituaties juist wel snel sprake van computervredebreuk. Computervredebreuk is in die zin 'breed gedefinieerd,' zo geeft één van hen aan. Dat komt vooral door het feit dat werknemers slechts voor bepaalde doelen gegevens op hun werk mogen raadplegen. Zodra gegevens geraadpleegd worden voor een ander doel, is volgens hen sprake van computervredebreuk. Hoewel dit laatste als valide grond kan worden gezien voor computervredebreuk – de Hoge Raad heeft met betrekking tot dit thema inmiddels meerdere arresten gewezen[15] – kan terughoudendheid bestaan om computervredebreuk in dit soort situaties ten laste te leggen.[16] Een medewerker van het Openbaar Ministerie die zich heeft gebogen over een zaak waarin een medewerker een filmpje plaatste van contactgegevens van één klant mailt hierover:

> Nu deze verdachte in principe geen betrokkenheid had met de klant waarvan de gegevens werden aangeboden zou er wellicht te betogen zijn geweest dat artikel 138ab [Sr] ook van toepassing was. Die kwalificatie had echter veel meer toelichting gevergd en tevens een diepere kennis van cybercrimejurisprudentie bij de rechter.

Deze medewerker geeft aan dat het in deze zaak, 'naast een voor de hand liggende keuze, een veiligere keuze' was om voor artikel 138c Sr te kiezen. Er is, zo merkt een andere geïnterviewde, werkzaam als officier van justitie, 'soms twijfel waar wederrechtelijkheid begint, en waar wederrechtelijkheid ophoudt'. Wat betreft één van de geïnterviewde advocaten zou artikel 138ab Sr niet meer moeten worden gebruikt in een tenlastelegging, wanneer artikel 138c Sr volstaat.

Ook als er wel alternatieven zijn voor artikel 138c Sr, kan het stelen van gegevens nog steeds het best passende artikel zijn. Dat geldt bijvoorbeeld voor de zaak waarin de verdachte klantgegevens stal uit het restaurant waar hij werkzaam was. In deze zaak is de verdachte ook vervolgd voor afpersing. Dat artikel had volgens de zojuist aangehaalde officier van justitie ook als enige strafbaarstelling in de zaak gebruikt kunnen worden. Er was echter ook een verdenking tegen het restaurant, en men wilde graag weten waar die gegevens precies vandaan kwamen. Daar bood artikel 138c Sr uitkomst voor.

Een tweede manier waarop artikel 138c Sr van nut kan zijn voor de opsporingspraktijk is dat gemakkelijker een (uitgebreider) opsporingsonderzoek kan worden uitgevoerd. Aangegeven wordt dat artikel 138c Sr als basis kan dienen voor een opsporingsonderzoek en een vangnetartikel kan zijn, zeker in gevallen waarin sprake lijkt te zijn van meerdere strafbare feiten. De zojuist al aangehaalde geïnterviewde vertelt dat in een zaak sprake kan zijn van gegevens die zijn overgenomen. Op dat moment hoeft nog niet duidelijk te zijn hoe dat precies is gebeurd. Is dat bijvoorbeeld

[15] ECLI:NL:HR: 2021:1691; ECLI:NL:HR:2025:201.

[16] Berndsen en Visser (2022, p. 163) menen dat de Hoge Raad het begrip computervredebreuk te ver opgerekt heeft. Onder andere omdat hierdoor niet alleen het binnendringen van het systeem een belangrijk kenmerk is van computervredebreuk, maar de informatie die wordt opgezocht. Zij opperen artikel 138c Sr als één van de alternatieven.

middels de eerder beschreven computervredebreuk gebeurd? En wie heeft de gegevens precies overgenomen? In dat geval is het 'goed' dat dit artikel in het Wetboek van Strafrecht is opgenomen, aldus deze geïnterviewde. Dat geldt overigens ook voor situaties waarin zwaardere delicten uiteindelijk niet te bewijzen blijken te zijn. Een veroordeling voor artikel 138c Sr zorgt er dan toch voor dat aan de verdachte duidelijk wordt gemaakt dat hij 'niet wegkomt met gedrag dat strafbaar is'. Bovendien, zo legt dezelfde geïnterviewde uit, zorgt een veroordeling ervoor dat de staat geen vergoeding aan de verdachte hoeft te betalen, omdat het andere feit niet te bewijzen viel. Verder kunnen, en dit komt vooral doordat artikel 138c Sr aangemerkt is als feit waarvoor voorlopige hechtenis kan worden opgelegd (art. 67, lid 1b Sv), extra (opsporings)handelingen worden verricht, bijvoorbeeld het ophalen van IP-adressen en een aanhouding buiten heterdaad. Dat laatste kan nodig zijn wanneer nader onderzoek moet plaatsvinden naar een mogelijke verspreiding van gevoelige organisatiegegevens.

Een derde manier heeft betrekking op de periode nadat een opsporingsonderzoek is afgerond. Zo hebben slachtoffers van gegevensdiefstal de mogelijkheid om zich te voegen in een strafzaak, bijvoorbeeld om schadevergoeding te eisen. Daarnaast, en dit geldt voor situaties waarin het feit bewezen wordt verklaard, kunnen overgenomen gegevens, die bijvoorbeeld op een USB-stick zijn gezet, onttrokken worden aan het verkeer (art. 36c Sr).

Hoofdpunten

- Artikel 138c Sr kan op verschillende manieren van nut zijn voor de opsporingspraktijk. 1) Het artikel past goed bij handelingen die een verdachte verricht heeft en die in sommige opsporingsonderzoeken naar voren komen; 2) Het artikel kan een leemte vullen dat artikel 138ab Sr (computervredebreuk) achterlaat; 3) Er kan (uitgebreider) opsporingsonderzoek worden gedaan; 4) Slachtoffers kunnen zich voegen en overgenomen gegevens kunnen worden onttrokken aan het verkeer.

2.3.5 Aandachtspunten

Op basis van de interviews is ook een aantal aandachtspunten onderscheiden. Een eerste aandachtspunt, zo merken enkele geïnterviewden op, is dat de strafmaat aan de lage kant is. Volgens één van de geïnterviewden, werkzaam bij het Openbaar Ministerie, is dat problematisch, omdat het bij het stelen van gegevens kan gaan om bedrijfsgegevens. Afhankelijk van de aard van die gegevens kan dit leiden tot een schadepost van 'honderden miljoenen'. Deze geïnterviewde is verbaasd dat de strafmaat voor het stelen van gegevens niet hetzelfde is als die voor diefstal en verduistering van goederen. Dit verschil leidt ertoe dat een werknemer die een USB-stick steelt met daarop bedrijfsgegevens maximaal drie jaar gevangenisstraf kan krijgen, terwijl een werknemer die zijn eigen USB-stick meeneemt en daarop gegevens opslaat maximaal één jaar gevangenisstraf kan krijgen. Om die reden doet deze geïnterviewde de suggestie om in de wettelijke bepaling een verzwaring op te nemen, namelijk wederrechtelijke bevoordeling gepleegd uit hoofde van persoonlijke dienstbetrekking, vergelijkbaar met 'normale' verduistering uit dienstbetrekking. Op die manier komt er meer eenheid qua strafmaat. Niet alle geïnterviewden zien de strafmaat overigens als problematisch, bijvoorbeeld in de zaak waar persoonsgegevens uit het BRP werden gestolen. Volgens de geïnterviewde voldeed de strafmaat in deze zaak, omdat de gevolgen van de diefstal 'redelijk beperkt zijn gebleven'. Bovendien was de verdachte door deze zaak zijn baan kwijtgeraakt.

Het tweede aandachtspunt is dat het lastig kan zijn om de wederrechtelijkheid te bewijzen. Aangetoond moet worden dat het niet toegestaan was om gegevens over te nemen. Iemand kan bijvoorbeeld zeggen dat hij de gegevens overnam om thuis te kunnen werken. In één van de zaken (ECLI:NL:RBROT:2022:8560) was het verweer van de advocaat dat degene die de gegevens overnam dat deed omdat hij ervan uit ging dat een andere collega die nodig had voor zijn werk. Binnen deze organisatie zou het een gebruikelijke werkwijze zijn dat aan niet-geautoriseerde collega's gegevens mochten worden verstrekt, omdat een beperkt aantal licenties beschikbaar was om in die systemen te kijken. De rechtbank ging hier niet in mee. Zij overwoog dat de verdachte er niet van uit mocht gaan dat de gevraagde gegevens voor werk gebruikt zouden worden. Daarnaast kon de verdachte niet worden verontschuldigd, ondanks dat hij handelde volgens een wijze die gebruikelijk was op de werkvloer. Dat laatste is wel meegenomen bij de uiteindelijke strafoplegging, namelijk schuldigverklaring zonder oplegging van straf of maatregel.

Een laatste aandachtpunt is de definitie van een geautomatiseerd werk. In het artikel is geregeld dat het moet gaan om de overname van gegevens die zijn opgeslagen op een geautomatiseerd werk. In één van de zaken is de verdachte slechts gedeeltelijk veroordeeld voor het overnemen van gegevens, omdat een deel van de gegevens, eindexamenopgaves, van papier naar papier werden gekopieerd, hetgeen geen geautomatiseerd werk is. De verdachten zijn wel veroordeeld voor de gekopieerde examens vanaf een CD-rom (ECLI:NL:RBNNE:2021:394; ECLI:NL:RBNNE:2021:395).

Hoofdpunten

- Er is een aantal aandachtspunten onderscheiden met betrekking tot artikel 138c Sr: 1) Afhankelijk van het soort gegevens dat gestolen wordt, kan de strafmaat aan de lage kant zijn; 2) Het is niet altijd gemakkelijk om het bestanddeel 'wederrechtelijk' aan te tonen; 3) Artikel 138c Sr ziet op gegevens die overgenomen zijn uit een geautomatiseerd werk.

2.4 Tot slot

De wetgever heeft artikel 138c Sr geïntroduceerd om gegevens beter te kunnen beschermen. Vóór de introductie was dat ingewikkelder, omdat de beschikbare artikelen niet altijd van toepassing waren op het wederrechtelijk overnemen van opgeslagen gegevens. Om iemand te kunnen vervolgen voor computervredebreuk (art. 138ab Sr) moest bijvoorbeeld de beveiliging zijn doorbroken. Wanneer iemand echter in een werksituatie gegevens overneemt uit een omgeving waartoe hij rechtmatig toegang heeft, kon geen vervolging plaatsvinden, zo was de redenering. Dit onderzoek heeft laten zien dat, sinds de inwerkingtreding van de Wet CCIII, verdachten vervolgd zijn voor het stelen van gegevens. 39 zaken zijn ingestroomd bij het Openbaar Ministerie en in 15 zaken heeft de rechter een uitspraak gedaan. In 2 zaken is de zaak afgedaan met een OM-beschikking en in 13 zaken is de verdachte veroordeeld voor ten minste één 138c Sr-feit. In dat opzicht zijn gegevens in de praktijk beter beschermd, omdat voor verdachten een risico op vervolging bestaat. Of de nieuwe wettelijke bepaling daadwerkelijk een afschrikwekkende werking heeft, kan op basis van deze evaluatie niet worden gezegd.

Artikel 138c Sr wordt vooral toegepast in zaken die zich in een werksituatie afspelen. Meestal was het overnemen van gegevens niet het enige ten laste gelegde feit. Wanneer sprake was van een combinatie van feiten, dan waren in de meerderheid van

de zaken de gestolen gegevens gebruikt voor het plegen van (een deel van) de andere feiten in de tenlastelegging. Meestal stalen de verdachten persoonlijke gegevens (persoonsgegevens en foto's en afbeeldingen). Het is niet altijd duidelijk geworden hoeveel gegevens gestolen waren. Doorgaans ging het niet om grote aantallen (honderden gegevens). Een belangrijke wijze waarop dit artikel van nut is voor de opsporingspraktijk, zo blijkt uit de evaluatie, is dat er nu een juridische omschrijving is die goed past bij situaties waarin een persoon, die rechtmatig toegang tot gegevens heeft, deze wederrechtelijk overneemt. Bovendien maakt de strafbaarstelling het gemakkelijker om in een aantal situaties (uitgebreider) opsporingsonderzoek te doen. Voorheen was dat niet het geval. Daarbij moet worden opgemerkt dat de rechtspraak zich inmiddels verder heeft ontwikkeld. In de wetsgeschiedenis komt zoals gezegd naar voren dat artikel 138ab Sr (computervredebreuk) niet geschikt werd bevonden voor de overname van gegevens in werksituaties. Inmiddels heeft de Hoge Raad een aantal arresten gewezen waaruit blijkt dat ook in werksituaties sprake kan zijn van computervredebreuk. Daardoor hoeft niet altijd gekozen te worden voor artikel 138c Sr. In die situaties lijkt het artikel dus niet meer altijd nodig te zijn. Tegelijkertijd wordt de vraag gesteld of in die situaties het begrip computervredebreuk niet te ver wordt opgerekt, onder andere omdat het binnendringen van het systeem niet langer een belangrijk kenmerk zou zijn van computervredebreuk. In plaats daarvan zou het gaan om de informatie die wordt opgezocht.

3 Helen van gegevens (art. 139g Sr)

In dit hoofdstuk richt de aandacht zich op het helen van gegevens, artikel 139g Sr. Allereerst wordt het juridisch kader uiteengezet (paragraaf 3.1). Vervolgens komt de noodzaak (volgens de wetgever) van deze nieuwe wettelijke bepaling aan bod en worden de veronderstellingen beschreven die aan de bepaling ten grondslag liggen. Daarbij wordt meteen ook de doelstelling geschetst (paragraaf 3.2). Daarna komt de uitvoering in de praktijk aan de orde (paragraaf 3.3). In dit gedeelte over de praktijk zal eerst een cijfermatig overzicht worden gegeven van de wijze waarop het Openbaar Ministerie 139g-zaken heeft afgehandeld (paragraaf 3.3.1). Daarna volgt een cijfermatig overzicht met betrekking tot de afhandeling door de rechtbank (paragraaf 3.3.2). Vervolgens zal op basis van de vonnisanalyse en interviews dieper worden ingegaan de inhoud van de 139g-zaken (paragraaf 3.3.3) en de voordelen die dit artikel heeft voor de opsporingspraktijk (paragraaf 3.3.4). Ook zal worden ingegaan op de aandachtspunten van het nieuwe wetsartikel (paragraaf 3.3.5). Het hoofdstuk sluit af met een paragraaf waarin de doelstelling/veronderstelling en de praktijk met elkaar vergeleken worden (paragraaf 3.4).

3.1 Juridisch kader

Het aangepaste artikel 139g Sr, waarin het helen van gegevens strafbaar wordt gesteld, is als volgt opgenomen in het Wetboek van Strafrecht:

1 Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt gestraft degene die niet-openbare gegevens:
   a verwerft of voorhanden heeft, terwijl hij ten tijde van de verwerving of het voorhanden krijgen van deze gegevens wist of redelijkerwijs had moeten vermoeden dat deze door misdrijf zijn verkregen;
   b ter beschikking van een ander stelt, aan een ander bekend maakt of uit winstbejag voorhanden heeft of gebruikt, terwijl hij weet of redelijkerwijs moet vermoeden dat het door misdrijf verkregen gegevens betreft.
2 Niet strafbaar is degene die te goeder trouw heeft kunnen aannemen dat het algemeen belang het verwerven, voorhanden hebben, ter beschikkingstellen, bekendmaken of gebruik van de gegevens, bedoeld in het eerste lid, vereiste.

De tekst voor inwerkingtreding van de wet was als volgt:

> Met gevangenisstraf van ten hoogste zes maanden of geldboete van de vierde categorie wordt gestraft hij die een afbeelding, als bedoeld in het vorige artikel, onder 2°, openbaar maakt.

Net zoals artikel 138c Sr moet artikel 139g Sr ervoor zorgen dat de strafrechtelijke bescherming van gegevens, die middels een geautomatiseerd werk zijn opgeslagen, verder wordt verbeterd. Door de aanpassing van artikel 139g Sr wordt degene die gekopieerde of gestolen gegevens in handen heeft of bekend maakt strafrechtelijk aansprakelijk, zo staat in de memorie van toelichting beschreven. Het moet daarbij gaan om niet-openbare gegevens. Dat zijn gegevens die 'niet voor het publiek beschikbaar zijn' (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 61). In een brief van de Minister van Justitie en Veiligheid van 26 juni 2009 werd al aangekondigd dat er een

strafbaarstelling zou komen van het helen van gegevens. Destijds was het plan de heling van gegevens onder de reikwijdte van artikel 416 Sr (heling van een goed) onder te brengen (*Kamerstukken II* 2009/09, 28684 nr. 232, P. 4). In de memorie van toelichting bij de Wet CCIII wordt duidelijk dat uiteindelijk voor een apart artikel gekozen is, onder andere om het onderscheid duidelijk te maken ten aanzien van het verschil tussen goederen (waarop artikel 416 Sr ziet) en gegevens *Kamerstukken II* 2015/16, 34 372, nr. 3, p. 65). Verder blijkt uit de memorie van toelichting dat de strafbaarstelling van de heling van gegevens van belang is in die gevallen waarin niet kan worden aangetoond dat degene die de gegevens bekend maakt, ook degene is die de gegevens zelf heeft overgenomen, al dan niet na het binnendringen van een geautomatiseerd werk (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 61).

Op het helen van gegevens is een strafmaximum van één jaar gesteld. De strafbedreiging van één jaar ligt in lijn met gevallen waarin sprake is van beeldmateriaal dat middels een misdrijf verkregen is. De maximale gevangenisstraf komt daarmee overeen met het wederrechtelijk overnemen of aftappen van gegevens die via telecommunicatie of een geautomatiseerd werk worden verwerkt of overgedragen (art. 139c Sr). In de memorie van toelichting wordt toegelicht dat dit strafmaximum in lijn ligt met schuldheling (art. 417bis Sr[17]) (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 89).

3.2 Noodzaak en veronderstellingen

Omdat de aanleiding voor artikel 139g Sr voor een deel hetzelfde is als voor artikel 138c Sr, kan op basis van het voorgaande en het vorige hoofdstuk de volgende veronderstelling worden geformuleerd:

Ontwikkelingen op het gebied van ICT maken het steeds gemakkelijker om gegevens uit een geautomatiseerd werk over te nemen en op het internet te plaatsten. Dat leidt er (ook) toe dat gegevens gemakkelijker geheeld kunnen worden. Vóór inwerkingtreding van de Wet CCIII konden helers van gegevens niet goed worden vervolgd, omdat bestaande wettelijke regelingen niet voldeden. Door het vernieuwde wetsartikel 139g Sr (helen van gegevens) worden personen strafbaar die gegevens, ontvreemd uit een geautomatiseerd werk van een ander, bekend maken aan een ander, verkopen of op het internet plaatsen. Helers van gegevens kunnen daardoor worden vervolgd. Hierdoor kunnen gegevens, beter dan voorheen, strafrechtelijk worden beschermd.

[17] Artikel 417bis Sr luidt als volgt:
1 Als schuldig aan schuldheling wordt gestraft met gevangenisstraf van ten hoogste een jaar of geldboete van de vijfde categorie:
   a hij die een goed verwerft, voorhanden heeft of overdraagt, dan wel een persoonlijk recht op of zakelijk recht ten aanzien van een goed vestigt of overdraagt, terwijl hij ten tijde van de verwerving of het voorhanden krijgen van het goed dan wel het vestigen van het recht redelijkerwijs had moeten vermoeden dat het een door misdrijf verkregen goed betrof;
   b hij die uit winstbejag een goed voorhanden heeft of overdraagt dan wel een persoonlijk recht op of zakelijk recht ten aanzien van een goed overdraagt, terwijl hij redelijkerwijs moet vermoeden dat het een door misdrijf verkregen goed betreft.
2 Met dezelfde straf wordt gestraft hij die uit de opbrengst van enig goed voordeel trekt, terwijl hij redelijkerwijs moet vermoeden dat het een door misdrijf verkregen goed betreft.

3.3 Artikel 139g Sr in de praktijk

3.3.1 Instroom en afdoening Openbaar Ministerie

In tabel 3.1 wordt een overzicht gegeven van de wijze waarop het Openbaar Ministerie 139g-zaken heeft afgehandeld. Deze gegevens zijn gebaseerd op cijfers uit RAC-min. Daarin staat informatie over de instroom van zaken bij het Openbaar Ministerie en over de afhandeling van die zaken door het Openbaar Ministerie en door de rechter in eerste aanleg (Verweij & Tollenaar, 2022, p. 12).

Tabel 3.1 Afdoening Openbaar Ministerie artikel 139g Sr

Afdoening Openbaar Ministerie	Aantal
Administratief beëindigd	1
Dagvaarding	62
➢ Geen sepot	58
➢ Sepot 139g-feit	4
OM-strafbeschikking	2
Sepots	18
➢ Onvoorwaardelijk	16
➢ Voorwaardelijk	2
Afdoening onbekend	2
Totaal	**85**

Tabel 3.1 laat zien dat het Openbaar Ministerie, in de periode maart 2019-april 2024, 85 zaken heeft behandeld waarin artikel 139g Sr ten minste één keer voorkwam. Het betreft zaken met een pleegdatum van het gepleegde strafbare feit in de periode 1 maart 2019 tot en met 30 april 2024. In ruim twee derde van deze zaken (62) ontving de verdachte een dagvaarding. In 4 van die zaken is het 139g-feit geseponeerd. Verder zijn 18 zaken geseponeerd zonder dat een dagvaarding is uitgereikt. Het gaat hierbij om zowel voorwaardelijke (16) als onvoorwaardelijke (2) sepots. Tot slot is 1 zaak administratief beëindigd en is in 2 zaken een strafbeschikking opgelegd. Bij 2 zaken is het proces van afdoening nog niet bekend: de zaken zijn nog in behandeling bij het Openbaar Ministerie.

Er zijn verschillende redenen voor het seponeren van een 139g-feit. Deze staan in tabel 3.2 opgenomen.

Tabel 3.2 Sepotgronden artikel 139g Sr*

Sepotgronden	Aantal
Dagvaarding	4
➢ Feit dubbel ingeboekt	4
Onvoorwaardelijk sepot	16
➢ Onvoldoende bewijs	6
➢ Feit dubbel ingeboekt	1
➢ Door feit of gevolg getroffen[a]	1
➢ Oud feit	3
➢ Gering aandeel in feit	1
➢ Niet ontvankelijk	2
➢ Recente bestraffing	1
➢ Ten onrechte als verdachte aangemerkt	1
Voorwaardelijk sepot	2
➢ Gewijzigde omstandigheden	1
➢ Door feit of gevolg getroffen	1

* In deze tabel staat het aantal unieke sepotgronden weergegeven. Het kan voorkomen dat in 1 zaak een CCIII-feit meerdere keren voorkomt, en meerdere keren geseponeerd wordt.

e Sepotcode 52: Door eigen letsel; door letsel of verlies van naasten; in zijn maatschappelijke positie of in de verhouding tot zijn naaste omgeving; door ernstige financiële schade, rechtstreeks uit het feit voortvloeiend of door verplichte schadevergoeding; door een reactie van de overheid op het gepleegde feit, welke reactie voldoende representatief, te zwaar of minder juist blijkt te zijn geweest, bijv. inverzekeringstelling, hard politieoptreden of onjuiste formaliteiten.

In acht zaken komt artikel 139g Sr samen voor met een ander CCIII-feit: in vier zaken gecombineerd met artikel 138c Sr en in vier zaken gecombineerd met artikel 326e Sr (online handelsfraude – zie hoofdstuk 4). In tabel 3.3 en tabel 3.4 staat meer gedetailleerd weergeven hoe het Openbaar Ministerie de zaken heeft afgedaan.

Tabel 3.3 OM-afdoening artikelen 139g & 138c Sr*

OM-afdoening	Aantal
Dagvaarding	3
Gedeeltelijk sepot	3
➢ Sepot 138c-feit – feit dubbel ingeboekt	1
➢ Sepot 138c-feit – onvoldoende bewijs	1
➢ Sepot 139g-feit – onvoldoende bewijs	1
Sepots	1
Voorwaardelijk sepot	1[a]
➢ Sepot 138c-feit – feit dubbel ingeboekt	1
➢ Sepot 139g-feit – gering aandeel in feit	1
Totaal	**4**

* In deze tabel staat het aantal unieke sepotgronden weergegeven. Het kan voorkomen dat in 1 zaak een CCIII-feit meerdere keren voorkomt, en meerdere keren geseponeerd wordt.

a Het betreft hier één zaak, waarin twee CCIII-feiten op de tenlastelegging stonden. Beide feiten zijn geseponeerd, met elk een andere sepotgrond.

Tabel 3.4 OM-afdoening artikelen 139g & 326e Sr

OM-afdoening	Aantal
Dagvaarding	
Geen sepot	4
Totaal	**4**

3.3.2 Vonnissen rechtbank

In de periode maart 2019-april 2024 zijn 42 139g-zaken ingestroomd bij de rechtbank waarbij ook een eindvonnis voor de onderzoekers beschikbaar was. In tabel 3.5 en tabel 3.6 is te zien op welke wijze de rechter deze heeft afgedaan, zowel de 139g-zaken als de artikel 139g Sr gecombineerd met 326e-zaken. In het grootste deel van de zaken heeft de rechter een straf opgelegd.

Tabel 3.5 Gerechtelijke afdoening artikel 139g Sr

Afdoening*	Aantal
Strafoplegging	32
Vrijspraak	7
Totaal	**39**

* Hierin zijn twee zaken meegenomen die ter terechtzitting gevoegd waren.

Tabel 3.6 Gerechtelijke afdoening artikelen 139g & 326e Sr

Afdoening	Aantal
Gedeeltelijke vrijspraak	
➢ Vrijspraak artikel 139g Sr	1
➢ Vrijspraak artikel 326e Sr	2
Totaal	**3**

3.3.3 Aard artikel 139g Sr zaken

In het vervolg van dit hoofdstuk wordt dieper ingegaan op het soort zaken waarin artikel 139g Sr voorkomt. Dit gebeurt op basis van de vonnisanalyse en interviews, zowel de algemene interviews als de zaaksinterviews. 44 vonnissen zijn nader bestudeerd. Het ging om 31 vonnissen in eerste aanleg van de meervoudige kamer, 2 vonnissen in hoger beroep en 6 vonnissen van een politie- of kinderrechter. 2 vonnissen hadden betrekking op dezelfde zaak: 1 vonnis betrof de uitspraak in eerste aanleg en 1 vonnis de uitspraak in hoger beroep. Van 1 zaak was alleen de tenlastelegging bekend. Een officier van justitie heeft deze aan ons beschikbaar gesteld.

Zowel uit de interviews als de vonnisanalyse komt naar voren dat het helen van gegevens slechts in een paar gevallen het enige feit was dat in een zaak voorkwam. Het betreft drie uitspraken waarin het draaide om toetsfraude. In deze zaken (ECLI:NL:RBOVE:2023:2526; ECLI:NL:RBOVE:2023:2523; ECLI:RBOVE:2023:2525) hadden de verdachten toetsen van een hogeschool in hun bezit en werden deze toetsen doorverkocht aan studenten die deze toetsen nog moesten maken. Ook is er een zaak, zo blijkt uit de interviews, waarin artikel 139g Sr het startpunt was voor het opsporingsonderzoek. Deze zaak bestond uit allemaal subzaken waarin per verdachte nader onderzoek is gedaan. Soms leverde dat uiteindelijk meerdere feiten op. Soms bleef het bij artikel 139g Sr. Voor de overige zaken geldt dat er altijd meerdere feiten ten laste zijn gelegd.

Op basis van de vonnisanalyse en de interviews is een aantal categorieën zaken worden onderscheiden waarmee het helen van gegevens samen voorkomt. Deze categorieën zijn overigens niet in alle gevallen even scherp van elkaar te scheiden, maar vanwege analytische redenen wordt dat op deze plek toch gedaan. De volgende categorieën worden nader besproken: combinatie met fraude, diefstal cryptovaluta, financieel nadeel bedrijven en misdrijven binnen de relationele sfeer. Daarna volgen zaken waarin artikel 139g Sr gecombineerd wordt met drugshandel, uitbuiting en mensenhandel en computervredebreuk en *phishing*.

Combinatie met fraude

In een groot deel van de onderzochte vonnissen (16) gaat het om zaken waarin (individuele) burgers financieel nadeel ondervonden door een vorm van bankfraude. Ten eerste twee zogenoemde vriend-in-nood fraudezaken (ECLI:NL:RBROT:2022:8395; ECLI:NL:RBZWB:2023:5123). In die zaken deed de verdachte zich voor als een bekende van het slachtoffer die in financiële nood verkeerde met het doel geld te ontvangen van het slachtoffer. Een voorbeeld hiervan is een casus waarin de verdachte samen met een medeverdachte de aangeefster benaderde en zich voordeed als haar kind. Dat 'kind' vroeg een aantal openstaande rekeningen te betalen. In deze zaak werd ook een foto aangetroffen met een lijst

persoonsgegevens – het 139g-feit. Omdat verder geen onderzoek is gedaan naar deze gegevens, is de verdachte voor dit feit vrijgesproken.

Ten tweede is in vijf zaken sprake van bankhelpdeskfraude (ECLI:NL:RBMNE:2022:677; ECLI:NL:RBDHA:2024:4472; drie niet-openbare vonnissen[18]). In die zaken werden slachtoffers benaderd door een persoon die zich voordeed als bankmedewerker, bijvoorbeeld nadat zij een e-mail hadden ontvangen met daarin het bericht dat een derde gemachtigd was om geld van zijn/haar rekening af te schrijven. In alle vijf zaken had het helen van gegevens betrekking op het bezit van zogenoemde *leads*. Dat zijn lijsten met persoonsgegevens. Deze lijsten met persoonsgegevens werden gebruikt voor fraude. In één van de zaken is de verdachte hier niet voor veroordeeld, omdat niet bewezen kon worden dat de lijsten afkomstig waren uit een misdrijf (ECLI:NL:RBMNE:2022:677). Ook in een andere zaak is de verdachte vrijgesproken van het voorhanden hebben van niet-openbare gegevens en bankfraude (computervredebreuk, oplichting en diefstal). De geheelde gegevens werden gebruikt voor bankfraude, maar dat de verdachte de enige gebruiker was van de laptop waarop de gegevens waren aangetroffen kon niet worden bewezen. Wel is de verdachte veroordeeld voor witwassen en voor deelname aan een criminele organisatie die bankfraude pleegde (niet-openbaar vonnis).

Inbraak in accounts om te kunnen internetbankieren is een derde vorm van bankfraude (ECLI:NL:RBMNE:2023:6180; ECLI:NL:RBMNE:2023:6179; ECLI:NL:RBAMS:2022:6219; niet-openbare tenlastelegging) die samen voorkwam met het helen van gegevens. Twee uitspraken betreffen eenzelfde zaak waarin twee verdachten zijn vervolgd. In beide gevallen werden accountgegevens achterhaald via *phishing* om deze vervolgens te gebruiken om geld te stelen en om een nieuwe pinpas aan te vragen. In de zaak van één van deze verdachten (ECLI:NL:RBMNE:2023:6180) had artikel 139g Sr betrekking op het via het socialemediakanaal Telegram aanschaffen van zogenoemde *splits*[19], lijsten met e-mailadressen en wachtwoorden. In de zaak van de andere verdachte ging het om marktplaatsaccounts en lijsten met e-mailadressen en wachtwoorden (ECLI:NL:RBMNE:2023:6179). Die laatste lijken te zijn gebruikt om *phishing*links te versturen. In de derde zaak (ECLI:NL:RBAMS:2022:6219) hield de verdachte zich onder andere bezig met het versturen van valse betaalherinneringen van de ANWB. Deze werden benut om gegevens te achterhalen waarmee vervolgens kon worden binnengedrongen op de servers van financiële dienstverleners. Artikel 139g Sr had in deze zaak betrekking op het bezitten van afbeeldingen van 80 paspoorten, waarvan de verdachte overigens is vrijgesproken.[20] Op basis van het vonnis wordt niet duidelijk wat de precieze relatie was met de andere feiten. Ook in de vierde zaak (niet-openbare tenlastelegging) lijkt geen link te zijn tussen de geheelde gegevens (e-mailadressen en wachtwoorden) en het ander gepleegde feit, namelijk diefstal van geld middels een internetbankieraccount.

De hiervoor besproken vormen van fraude kwamen ook samen voor. In één zaak (ECLI:NL:RBDHA:2021:14871) ging het om een combinatie van vriend-in-nood fraude en bankhelpdeskfraude en in een andere zaak (ECLI:NL:RBMNE:2022:655) kwamen bankhelpdeskfraude en inbraak in internetbankieraccounts samen voor. In die tweede

[18] Hoewel in één van deze zaken sprake was van vrijspraak in deze zaak met betrekking tot bankhelpdeskfraude, wordt deze zaak hier toch besproken, omdat de verdachte wel is veroordeeld voor deelname aan een criminele organisatie die bankhelpdeskfraude pleegde.

[19] Een andere benaming hiervoor zijn de in het vorige hoofdstuk genoemde 'combolijsten' en de in dit hoofdstuk genoemde '*leads*'.

[20] Hij bleek uiteindelijk 'slechts' twee afbeeldingen van identiteitskaarten in zijn bezit te hebben waarvan het vermoeden bestond dat die niet rechtmatig verkregen waren.

zaak werd de inbraak in het account overigens niet bewezen verklaard. Daarnaast is ook deze verdachte vrijgesproken van het 139g-feit, omdat niet kon worden bewezen dat de gegevens door een misdrijf waren verkregen. Wel is vast komen te staan dat deze gegevens zijn gebruikt voor oplichting. In weer een andere zaak (niet openbaar vonnis) ging het om vriend-in-nood fraude en inbraak in internetbankieraccounts. De verdachte in deze zaak had ook NAW-gegevens (naam, adres, woonplaats) en/of telefoonnummers van een groot aantal personen in zijn bezit, het 139g-feit. In het vonnis wordt dit feit niet expliciet gekoppeld aan de andere feiten, hoewel het voor de hand ligt dat deze gegevens voor de fraude zijn gebruikt.

De laatste drie vormen van fraude waarmee het helen van gegevens samen voorkwam zijn marktplaatsfraude, webwinkelfraude en eindexamenfraude. In één van de zaken (ECLI:NL:RBZWB:2021:6062) ging het helen van gegevens samen met oplichting via Marktplaats. De verdachte hield zich onder andere bezig met marktplaatsoplichting en gewoontewitwassen. Daarnaast maakte de verdachte zich schuldig aan computervredebreuk. Via een *phishing*mail achterhaalde de verdachte inloggegevens en wachtwoorden van een aantal gebruikers van het verkoopplatform om deze vervolgens te misbruiken. Op basis van het vonnis lijken deze gegevens te zijn gebruikt voor het oplichten van slachtoffers. Het bezit van deze gegevens was in de tenlastelegging het 139g-feit. De verdachte is hier uiteindelijk voor vrijgesproken, omdat hij zelf degene was die de gegevens door een misdrijf verkreeg. In een andere zaak (ECLI:NL:RBDHA:2023:14140) schafte de verdachte via *Genesis Market*[21] verschillende bots aan. Dat zijn pakketjes met onder andere inloggegevens zoals gebruikersnamen en wachtwoorden. De verdachte gebruikte deze vervolgens om bij verschillende webshops, via accounts van anderen, luxegoederen te bestellen. Deze liet de verdachte bij zichzelf afleveren. Het bezit van bots was in deze zaak het 139g-feit en dit feit is direct gerelateerd aan de andere feiten, omdat de gegevens gebruikt zijn om bestellingen te doen.

Combinatie met diefstal cryptovaluta

Naast bankfraude kwam het helen van gegevens samen voor met diefstal van cryptovaluta. Dat gebeurde in één zaak (ECLI:NL:RBAMS:2023:3748) waarin de verdachte *phishing* websites, *phishing*mails en een grote hoeveelheid *seed phrases*[22] in bezit had waarmee *phishing* kon worden gepleegd en waarmee een groot bedrag aan cryptovaluta gestolen werd. Ook had deze verdachte cryptovaluta witgewassen. Naast deze feiten had de verdachte een groot aantal datasets met privacygevoelige persoonsgegevens in zijn bezit, het 139g-feit, die hij op een illegale online handelsplaats te koop aanbood. Deze gegevens zijn niet gebruikt voor het plegen van de andere feiten, zo blijkt uit één van de interviews.

Combinatie met financieel nadeel organisaties

In drie zaken ging het helen van gegevens samen met feiten waarbij niet burgers, maar bedrijven financieel zijn benadeeld. In de eerste casus (ECLI:NL:GHDHA:2024:226) betaalde de verdachte met Bijenkorf-cadeaukaarten. Het bezit van de cadeaukaarten is het 139g-feit. In de tweede casus (ECLI:NL:RBAMS:2023:6967) zijn meerdere bedrijven gehackt en dreigde de verdachte vertrouwelijke informatie van deze bedrijven openbaar te maken. Bij deze verdachte werd ook software aangetroffen waarmee *phishing* activiteiten konden worden uitgevoerd. Tevens zijn gestolen databases gevonden met daarin gegevens

[21] *Genesis market* is een internationaal illegaal handelsplatform (Spinner, 2023).
[22] Een *seed phrase* is een reeks willekeurige woorden die de benodigde gegevens opslaat om toegang te krijgen tot of cryptovaluta te herstellen (Coinbase, z.d.).

van miljoenen mensen. De gegevens die de verdachte stal, zijn gebruikt voor andere feiten in de tenlastelegging. Met betrekking tot een aantal databases werd deze verdachte voor het 139g-feit ontslagen van rechtsvervolging, omdat hij deze zelf door een misdrijf had verkregen. De derde zaak draaide om examenfraude (ECLI:NL:RBNNE:2021:395). Deze zaak is reeds besproken in het vorige hoofdstuk. In deze zaak had de zoon kopieën van eindexamens in zijn bezit die hij had gekregen met behulp van zijn vader die als conciërge werkte op de school van zijn zoon. Het bezit van deze examens, die zijn gekopieerd van papier naar papier, was het 139g-feit. De zoon is voor dit feit vrijgesproken, omdat de gegevens niet overgenomen waren uit een geautomatiseerd werk.[23] De zoon is, zoals eerder besproken, wel veroordeeld voor de andere feiten. Namelijk voor het overnemen van eindexamens van een cd-rom en het aanpassen van examenantwoorden.

Combinatie met misdrijven binnen relationele sfeer

In vier zaken kwam het helen van gegevens samen voor met feiten die zich hebben afgespeeld in de (voormalig) relationele sfeer. In de eerste zaak (niet-openbaar vonnis), die ook besproken is in het vorige hoofdstuk, ging het om bedreiging en mishandeling van een ex-partner. Daarnaast had de verdachte een lijst met honderden buitenlandse telefoonnummers, afkomstig uit één land, in zijn bezit die hij verkreeg via Telegram. Deze had hij in bezit gekregen nadat hij expliciet om telefoonnummers van vrouwen had gevraagd. In de tweede zaak (niet openbaar vonnis) maakte de verdachte wederrechtelijk een filmpje van het slachtoffer waarin te zien was dat zij hem oraal bevredigde. Dat filmpje stuurde de verdachte vervolgens naar meerdere personen, het 139g-feit in deze zaak. In de derde zaak (niet openbaar vonnis) verschafte de verdachte zichzelf, zonder toestemming, toegang tot het huis van zijn ex. Daarna logde hij met haar wachtwoord in op haar laptop en nam berichten van een online socialemediaplatform over door er foto's van te maken. Vervolgens stuurde hij deze foto's naar meerdere personen door. Ook in deze zaak is het verspreiden van, in dit geval het beeldmateriaal, het 139g-feit. Datzelfde gold voor de vierde zaak (ECLI:NL:RBNHO:2022:921 / ECLI:NL:GHAMS:2024:1320), waarin het draaide om beeldmateriaal waarop te zien is hoe de aangeefster wordt verkracht door de verdachte en een medeverdachte. De verdachte heeft hier video-opnames van gemaakt en verspreid. In de laatste drie casussen is er een directe relatie tussen het helen van gegevens en de andere feiten. Bij de eerste zaak lijkt die relatie er niet te zijn.

Combinatie met drugshandel, uitbuiting en mensenhandel

Het helen van gegevens kwam ook voor in een zaak waarin het draaide om drugshandel (ECLI:NL:RBMNE:2023:5582). De betreffende verdachte hield zich voor een langere periode bezig met het medeplegen van grootschalige harddrugshandel en de export van harddrugs. Tevens was hij betrokken bij het voorbereiden en bevorderen hiervan. Ook handelde de verdachte in verboden vuurwapens en gestolen politie-informatie, het 139g-feit. Op basis van het vonnis is niet duidelijk in hoeverre de gestolen politie-informatie (het 139g-feit) gerelateerd was aan de andere feiten. In een andere zaak (ECLI:NL:RBAMS:2022:5158) kwam het helen van gegevens samen voor met onder andere mensenhandel. De verdachte in deze casus maakte zich onder andere schuldig aan de afpersing en/of chantage van zeven slachtoffers, criminele uitbuiting en het voordeel trekken uit de uitbuiting van één van zijn minderjarige slachtoffers. Ook benaderde hij slachtoffers met het bericht dat hij compromitterende

[23] Hier lijkt de rechter een redenering te volgen gebaseerd op artikel 138c Sr. Voor artikel 138c Sr is het nodig dat sprake is van overname van een geautomatiseerd werk. Dat daar ook bij artikel 139g Sr sprake van moet zijn, volgt niet uit de wetstekst en de wetsgeschiedenis.

foto's van hen zou verspreiden. Het 139g-feit, waar overigens vrijspraak voor volgde, betrof enkele foto's die de verdachte in bezit had.

Combinatie met computervredebreuk en phishing
Tot slot kwam helen van gegeven samen voor met computervredebreuk (of voorbereiding hiervan) en *phishing* (zes vonnissen over vijf zaken). Beide feiten kwamen overigens ook voor in eerder geschetste zaken. In één van de zaken (ECLI:NL:RBAMS:2023:3358) brak de verdachte met een zelfgeschreven script in op accounts waarvoor hij geen toestemming had. Om dat te kunnen doen, brak hij in bij de servers van een bedrijf. Daarnaast downloadde de verdachte lijsten met inlognamen en wachtwoorden die hij van een bekende had gekregen, het 139g-feit. De verdachte wist dat deze gegevens van een misdrijf afkomstig waren. Beide feiten lijken niet aan elkaar gerelateerd te zijn. Ook in twee andere uitspraken (zelfde zaak, maar twee verdachten), kwam het helen van gegevens samen voor met computervredebreuk (twee niet-openbare vonnissen). Het betrof verdachten die zichzelf in een werkomgeving toegang verschaften tot klantgegevens en deze gegevens naar anderen doorstuurden en te koop aanboden. In dat opzicht waren het helen van gegevens en computervredebreuk direct gerelateerd aan elkaar. In de laatste zaak (niet-openbaar vonnis) handelde de verdachte in persoonlijke financiële gegevens waarvan hij wist dat deze werden gebruikt voor oplichting. Daarnaast werd deze persoon verdacht van het bezitten van een technisch hulpmiddel waarmee onder andere computervredebreuk kon worden gepleegd. Van dat laatste is hij echter vrijgesproken. In deze zaak zijn de verschillende feiten direct aan elkaar gerelateerd. De geheelde gegevens konden worden gebruikt voor oplichting en mogelijk ook voor het technisch hulpmiddel.

Naast computervredebreuk waren er twee zaken waarin het draaide om *phishing*. In één van deze casussen (ECLI:NL:RBNNE:2023:1302) vervaardigde en verspreidde de verdachte *phishing panels*. Daarnaast bezat de verdachte persoons- en accountgegevens en bood deze aan via socialemediakanaal Telegram, het 139g-feit. In het vonnis is niet duidelijk geworden in hoeverre beide feiten aan elkaar gerelateerd waren. Dat geldt ook voor de tweede casus (ECLI:NL:RBZWB:2022:4532), waarin de verdachte creditcardgegevens in zijn bezit had (het 139g-feit). Daarnaast zijn bij de verdachte softwareprogramma's zoals *Sendblaster* en *Ultramailer* aangetroffen waarmee een groot aantal e-mails tegelijkertijd verstuurd kan worden. Ook had de verdachte voorbeeld *phishing* e-mails in zijn bezit.

Twee geïnterviewden, werkzaam bij het Openbaar Ministerie en die de aanpak van (grootschalige) datahandel als hun specialisme hebben, maken op basis van hun ervaringen een driedeling wat betreft het soort zaken waarin artikel 139g Sr een rol speelt, namelijk dataveredeling, georganiseerde criminaliteit en ethisch hacken. Vooral de eerste twee soorten komen terug in de vonnisanalyse. Bij dataveredeling gaat het om zaken waarin iemand de gegevens hackt, deze met elkaar combineert en ze vervolgens verkoopt (zogenoemde 'l*eads*handel') of gebruikt voor afpersing. De zaken met ECLI-nummers ECLI:NL:RBAMS:2023:3748 en ECLI:NL:RBAMS:2023:6967 zijn hier voorbeelden van. Bij georganiseerde criminaliteit kopen verdachten, bijvoorbeeld op Telegram, gegevens om allerlei vormen van criminaliteit te plegen. Deze verdachten zijn zelf niet in staat om deze lijsten te verwerven via het hacken. Zij hebben de gegevens nodig om 'hun businessmodel uit te voeren', aldus één van de geïnterviewden. Het plegen van bankfraude in georganiseerd verband is hier een voorbeeld van. Overigens komt in een ander interview naar voren dat het ook individuen kunnen zijn die voor zichtzelf gegevens aankopen, zonder dat hier een

georganiseerd verband achter zit. Tot slot onderscheiden deze twee geïnterviewden ethische hackers. Daarbij doelen zij op zaken waarin bijvoorbeeld een journalist beschikt over een database met gegevens die ooit gehackt is en er een aangifte komt van een persoon die op zo'n lijst staat. In de vonnisanalyse kwam een dergelijke zaak niet voor.

Hoofdpunten

- In de meeste zaken kwam het helen van gegevens samen voor met andere strafbare feiten. Er zijn verschillende categorieën zaken onderscheiden waarmee artikel 139g Sr samen voorkwam: combinatie met fraude, met diefstal cryptovaluta en met financieel nadeel organisaties. Daarnaast kwam artikel 139g Sr samen voor met misdrijven binnen relationele sfeer, met drugshandel, uitbuiting en mensenhandel en met computervredebreuk en *phishing.*
- In sommige gevallen bestond een directe relatie tussen het helen van gegevens en de andere strafbare feiten in de tenlastelegging. Bijvoorbeeld wanneer betaald werd met een valse cadeaukaart (helen van gegevens en witwassen) of wanneer leads (lijst met persoonsgegevens) werden gebruikt voor bankfraude of *phishing*activiteiten. In andere gevallen is die relatie niet duidelijk geworden of bestond er geen relatie.

Soort en hoeveelheid gegevens

Soort gegevens

Uit de interviews en de vonnisanalyse komt naar voren dat verschillende soorten gegevens zijn geheeld. In een meerderheid van de zaken ging het om persoonlijke gegevens. Daarbij ging het ten eerste om offline persoonsgegevens, zowel gewoon als bijzonder. Denk daarbij aan: naam, adres, telefoonnummer, geboortedatum en/of rekeningnummer of een foto van een identiteitsbewijs.[24] In bijna alle gevallen kwamen deze persoonsgegevens voor in zaken waarin individuele burgers financieel werden benadeeld door één van de eerder beschreven vormen van bankfraude. Een uitzondering hierop vormt een zaak die draaide om drugshandel waarin de verdachte beschikte over gestolen politiegegevens. Een andere uitzondering is de casus waarin het draaide om diefstal van cryptovaluta. In deze casus beschikte de verdachte naast persoonsgegevens over medische gegevens.

Ten tweede was er een aantal zaken waarin het draaide om online (identificerende) persoonsgegevens. Meestal betrof het een combinatie van gebruikersnamen en/of wachtwoorden.[25] Ook in deze zaken betrof het individuele burgers die financieel zijn benadeeld, doorgaans door bankfraude en in een enkel geval door het plaatsen van een valse bestelling bij een webshop. Daarnaast was in één zaak sprake van computervredebreuk. In twee andere zaken was sprake van een combinatie van offline en online persoonsgegevens, namelijk persoons- en/of accountgegevens van verschillende (online) winkels (ECLI:NL:RBNNE:2023:1302) en persoonsgegevens zoals rekeningnummer en e-mailadressen (niet-openbaar vonnis). Het soort persoonsgegevens wordt niet altijd gespecificeerd ('niet-openbare gegevens van

[24] ECLI:NL:RBROT:2022:8395; ECLI:NL:RBDHA:2021:14871; ECLI:NL:RBMNE:2022:677; ECLI:NL:RBAMS:2023:3748; ECLI:NL:RBDHA:2024:4472; niet-openbaar vonnis; ECLI:NL:RBMNE:2023:5582; ECLI:NL:RBAMS:2022:6219; niet openbaar vonnis; ECLI:NL:RBMNE:2022:655; niet openbaar vonnis.

[25] ECLI:NL:RBDHA:2023:14140; ECLI:NL:RBZWB:2021:6062; ECLI:NL:RBMNE:2023:6180; ECLI:NL:RBMNE:2023:6179; niet openbaar vonnis; ECLI:NL:RBAMS:2023:3358.

mogelijke klanten van ondernemingen' (niet openbare vonnissen) en 'negen Excel lijsten met niet-openbare persoonsgegevens' (niet openbaar vonnis[26]).[27]

Ten derde ging het bij persoonlijke gegevens om creditcardgegevens. Het betrof hier een *phishing* zaak (ECLI:NL:RBZWB:2022:4532) waarin gesproken werd over een 'groot aantal creditcardgegevens' en een zaak waarin een grote hoeveelheid creditcardgegevens en/of bankgegevens en de daarbij behorende CVC-gegevens is aangetroffen (niet-openbaar vonnis[28]). Daarnaast kwamen creditcardgegevens naar voren in een bankfraude zaak (ECLI:NL:RBZWB:2023:5123) waarin een Britse creditcard met CVC-nummer voorkwam die overigens uit eigen misdrijf was verkregen. Om die reden volgde vrijspraak voor heling van gegevens. In het vonnis wordt ook gesproken over 'gegevens op telefoons en laptops'. Deze gegevens zijn verder niet nader gespecificeerd.

Ten vierde zijn (intieme) foto's of video's voorbeelden van persoonlijke gegevens die voorbij zijn gekomen in de vonnisanalyse.[29] Het ging daarbij om filmpjes waarop seksuele handelingen te zien zijn en om foto's van berichten op een socialemediaplatform die te zien waren op een laptop. De eerste twee zaken deden zich voor in de relationele sfeer. Er is ook een zaak die draaide om uitbuiting en mensenhandel (ECLI:NL:RBAMS:2022:5158) waarin foto's en informatie op een telefoon een rol speelden. Het betrof in deze casus een foto van het slachtoffer en informatie over een bedrag op een jongerenrekening.

Naast persoonlijke gegevens kunnen 139g-gegevens ook toetsen zijn van een hogeschool (ECLI:NL:RBOVE:2023:2526; ECLI:RBOVE:2023:2525; ECLI:NL:RBOVE:2023:2523) en middelbare school (ECLI:NL:RBNNE:2021:395) alsmede digitale cadeaukaarten van de Bijenkorf (ECLI:NL:GHDHA:2024:226).

Hoeveelheid gegevens
Uit de vonnisanalyse en de interviews kwam een grote variatie naar voren wat betreft de hoeveelheid geheelde gegevens. In de vonnissen werd lang niet altijd duidelijk gemaakt om hoeveel gegevens het precies ging, bijvoorbeeld wanneer gesproken werd over leads, splits, negen Excel-lijsten met niet-openbare persoonsgegevens of een groot aantal gegevens of datasets. Daaruit kwamen geen concrete aantallen gegevens naar voren die een verdachte in zijn bezit had. Soms was het aantal wel nader gespecificeerd, bijvoorbeeld persoonsgegevens van ten minste 17 personen, 700 euro aan digitale kaarten, honderden buitenlandse mobiele telefoonnummers, of een filmpje waarin iemand seksuele handelingen verrichtte.

Tijdens de interviews is duidelijk geworden dat het bij het helen van gegevens om hele grote aantallen kan gaan, zeker wanneer het gaat om datasets met persoonsgegevens. Zo vertelt één van de geïnterviewden over een zaak waarin de verdachte beschikte over een database met daarin van alle Nederlandse autobezitters het kenteken, het e-mailadres, het woonadres en het telefoonnummer.

---

[26] Een andere zaak (niet openbaar vonnis) is verwant met deze zaak. Daarin werden de gegevens wel nader gespecificeerd, namelijk: lange lijst met namen, telefoonnummers, geboortedata en bankrekeningnummer, ook wel leads genoemd.

[27] Dit geldt ook voor een zaak die draait om de afpersing en afdreiging van bedrijven (ECLI:NL:RBAMS:2023:6967). Daarin wordt gesproken over 'datasets van bedrijven' die niet nader gespecificeerd worden.

[28] In deze zaak (niet-openbaar vonnis) zijn ook NAW-gegevens, en andere persoonlijke gegevens van andere personen dan verdachte zelf aangetroffen.

[29] Twee niet-openbare vonnissen; ECLI:NL:RBNHO:2022:921; ECLI:NL:GHAMS:2024:1320; ECLI:NL:RBAMS:2022:5158.

Wanneer het andersoortige gegevens betreft, is het aantal doorgaans kleiner.

Hoofdpunten

- In de 139g-zaken draaide het om verschillende soorten gegevens die geheeld werden.
- In het merendeel van de zaken draaide het om offline dan wel online persoonsgegevens die in veel gevallen gebruikt zijn voor fraude.
- De hoeveelheid geheelde gegevens werd lang niet altijd gespecificeerd. Het kan gaan om zeer grote aantallen.

Artikel 139g Sr ten laste gelegd

Uit de interviews komt naar voren dat het helen van gegevens voorkomt in relatief eenvoudige opsporingsonderzoeken onder leiding van een officier van justitie van het arrondissementsparket, maar ook in de meer complexe opsporingsonderzoeken die geleid worden door het Landelijk Parket dat gespecialiseerd is in de aanpak van datadiefstal en -handel.

In een groot deel van de zaken is artikel 139g Sr zoals gezegd niet het enige artikel dat ten laste werd gelegd. De wijze waarop artikel 139g Sr binnen een opsporingsonderzoek wordt gebruikt, verschilt, zo blijkt uit de interviews. Soms is artikel 139g Sr het startpunt voor een onderzoek. Bijvoorbeeld bij een onderzoek waarbij een buitenlandse autoriteit Nederland op de hoogte bracht dat een Nederlander over een grote hoeveelheid (buitenlandse) persoonsgegevens beschikte. Gedurende het opsporingsonderzoek bleek dat de verdachte veel meer op zijn kerfstok had, en uiteindelijk werd artikel 139g Sr het 'kleinere feit' in de tenlastelegging. Het helen van gegevens kan ook bijvangst zijn. In twee van de bestudeerde zaken bleek de verdachte bij een doorzoeking van zijn gegevensdragers te beschikken over geheelde gegevens, terwijl het bezit van die geheelde gegevens niet het onderzoeksonderwerp was waarop het opsporingsonderzoek zich oorspronkelijk richtte. Eén van die zaken betreft een zaak waarin een bedrijf aangifte deed, omdat haar gegevens waren gehackt. Bij het doorzoeken van de gegevensdragers van deze verdachte werden uiteindelijk (ook) gestolen gegevens aangetroffen.

Dat artikel 139g Sr niet het enige misdrijf is in een zaak en er bovendien een strafmaximum van één jaar op staat (meer hierover in paragraaf 3.3.5) kan ervoor zorgen dat het helen van gegevens niet altijd op de tenlastelegging komt. Eén van geïnterviewde officieren zegt hierover:

> Het is soms ook een afweging hè. Als je natuurlijk al 23 keer een 8-jaars feit hebt, (…) daar heb je je handen vol aan. Dan heeft het ook geen prioriteit om 139g ten laste te leggen (…). Een opportuniteitskeus.

Het Openbaar Ministerie heeft richtlijnen met betrekking tot strafeisen die gehanteerd kunnen worden. In de OM richtlijnenbundel 2024 wordt artikel 139g Sr genoemd, maar alleen in het kader van zaken die 'zien op het wederrechtelijk verkrijgen of vervaardigen van seksueel beeldmateriaal en handelingen die zien op wederrechtelijk bezit, verspreiden of openbaar maken van het beeldmateriaal'. Het gaat hierbij onder andere over het heimelijk filmen. Deze gedraging kan juridisch onder verschillende strafbaarstellingen vallen. Dit hangt af van de bedoeling van de dader en de omstandigheden (Openbaar Ministerie, 2024, p. 13). In de richtlijnenbundel worden drie categorieën weergegeven waarbinnen sprake kan zijn van misbruik van seksueel beeldmateriaal, inclusief de daarbij behorende strafoplegging die de officier van justitie

kan eisen: het verspreiden of dreigen met verspreiden, het vervaardigen en passief bezit (Openbaar Ministerie, 2024, p. 14). Op het gebied van cybercrime bestaan geen specifieke richtlijnen hoe met artikel 139g Sr om te gaan. Weliswaar is er een richtlijn strafvordering Cybercrime (Openbaar Ministerie, z.d) waarin aangegeven staat welke straf geëist moet worden bij een aantal cybercrimefeiten, maar het helen van gegevens staat hier niet tussen. Ook in de oriëntatiepunten voor straftoemeting en LOVS-afspraken (Landelijk Bureau Vakinhoud rechtspraak, 2025) komt artikel 139g Sr niet voor. Eén van de geïnterviewden vertelt dat een beleidsofficier een rol speelt bij de beslissing welke zaken wel en niet worden opgepakt. In de zaak van deze geïnterviewde is uiteindelijk verder onderzoek gedaan, omdat het om een bekende verdachte ging die 'al op een negatieve manier de aandacht had getrokken' en er bedreigingen waren vanuit de wijk richting de verdachte en het gezin waarvan hij onderdeel uitmaakte.

Hoofdpunten
- Het helen van gegevens komt zowel voor in de relatief eenvoudige opsporingsonderzoeken als in de meer complexe opsporingsonderzoeken.
- Geheelde gegevens kunnen het startpunt zijn voor een opsporingsonderzoek, maar ook 'bijvangst'.
- Het helen van gegevens komt niet altijd op de tenlastelegging.
- Op het gebied van cybercrime kent het Openbaar Ministerie geen richtlijnen welke straf geëist dient te worden wanneer sprake is van het helen van gegevens.

3.3.4 Voordelen voor de opsporingspraktijk

De meeste geïnterviewden vinden het positief dat artikel 139g Sr opgenomen is in het Wetboek van Strafrecht, omdat daardoor duidelijk is dat het helen van gegevens niet is toegestaan. Volgens één van de geïnterviewden, werkzaam bij het Openbaar Ministerie, is dat belangrijk, omdat mensen te gemakkelijk lijsten kopen via socialemediakanaal Telegram. Een andere geïnterviewde van het Openbaar Ministerie legt uit dat zij het 'principieel' een belangrijk artikel vindt. Verdachten kunnen zeer persoonlijke gegevens zoals patiëntendossiers in hun bezit hebben en volgens deze geïnterviewde mag de wet geen 'lacune' kennen waardoor het bezit van dit soort gegevens toegestaan zou zijn.

In de interviews zijn verschillende voordelen naar voren gekomen die artikel 139g Sr de opsporingspraktijk biedt. In de eerste plaats zou het artikel precies passen bij wat in de praktijk wordt gezien. Eén van de geïnterviewden geeft aan dat dit bijvoorbeeld het geval was in de zaak waarin een verdachte zelfgemaakte screenshots van berichten van zijn ex verspreidde op een socialemediaplatform (na ingebroken te hebben in haar computer). Juist voor de verspreiding van dit soort berichten is artikel 139g Sr in de ogen van deze opsporingsfunctionaris, werkzaam bij het Openbaar Ministerie, gemaakt.[30] In deze zaak was het artikel ook behulpzaam 'om een verhaal' te vertellen, namelijk over het soort gegevens dat de verdachte verspreidde. Voor de strafmaat was het artikel niet nodig, omdat ook andere feiten met een hogere strafmaat ten laste werden gelegd.

[30] In het kader van de heler-steler-regel is dit een interessante constatering, omdat het hier gegevens betreft die uit eigen misdrijf verkregen zijn. Daardoor zou de heler-steler-regel van toepassing kunnen worden geacht. De rechter heeft hier in deze zaak geen rekening mee gehouden en de verdachte veroordeelt voor het helen van gegevens die hij zelf door computervredebreuk verkregen had (zie ook paragraaf 3.3.5).

In de tweede plaats kan het artikel een alternatief zijn wanneer het vermoeden bestaat dat andere wetsartikelen het niet zullen halen bij de rechter en/of wanneer andere feiten te zwaar worden geacht. Dat gold voor een zaak waarin de verdachte wederrechtelijk een filmpje had gemaakt van een meisje dat seksuele handelingen verrichtte, maar waarin die handeling niet goed te zien was. Door artikel 139g Sr werd het mogelijk om de verdachte te vervolgen voor het verspreiden van het filmpje, iets wat misschien niet gelukt was als enkel een zedenfeit ten laste was gelegd. Bovendien wilde het Openbaar Ministerie geen zedenfeit in de tenlastelegging opnemen, omdat dat in te toekomst mogelijk een te zware belasting zou zijn voor de minderjarige (in verband met een VOG-aanvraag).

In de derde plaats wordt het door artikel 139g Sr mogelijk om gegevens verbeurd te verklaren of om geld dat met deze gegevens wordt verdiend, te ontnemen. Eén van de geïnterviewde officieren vermoedt dat in haar zaak de mogelijkheid tot verbeurdverklaring een rol heeft gespeeld bij het opnemen van artikel 139g Sr in de tenlastelegging, vooral omdat in de tijd dat de zaak speelde de Hoge Raad kanttekeningen plaatsten bij het vernietigen van gegevensdragers. Deze officier van justitie legt uit:

> [We] komen bijvoorbeeld bij een boef binnen. Dan nemen we al zijn gegevensdragers in beslag en (…) daarmee zijn [vaak] strafbare feiten gepleegd. Dus wij vinden dat ze verbeurd moeten worden verklaard. De Hoge Raad heeft daar wel wat kanttekeningen bij gemaakt. Nu heb je rechtbanken die niet zomaar gegevensdragers verbeurd verklaren. Dat houdt dus ook in dat, als jij [als officier] dus niet alert genoeg bent om te zeggen, goh maar op zo'n telefoon staan allemaal gegevens van anderen, die mogen niet meer in het verkeer komen, dan wordt zo'n telefoon gewoon weer teruggegeven. (…). Dus het kan best wel zijn dat ik heb gedacht (…) dat gaat niet gebeuren. Dat ik het er daarom op [de tenlastelegging] heb gezet. Het [artikel 139g Sr] heeft natuurlijk geen hoge strafbedreiging. Het is niet, je zet mensen er niet jaren voor vast. (…). Maar je kan dus wel (…) gegevensdragers ermee verbeurd verklaren.

In de vierde plaats is artikel 139g Sr volgens een geïnterviewde officier van justitie 'een essentiële schakel' om de 'criminele keten' aan te pakken. Dit geldt vooral voor zaken waarin geheelde gegevens worden gebruikt om criminaliteit te plegen, zoals bankfraude, en waarbij een bepaalde groep slachtoffers heel gericht wordt benaderd in plaats van via geheel willekeurig verspreidde e-mails en sms-berichten.

In de vijfde plaats maakt artikel 139g Sr het mogelijk een verdenking te creëren in zaken waarin dat vóór de komst van het artikel niet mogelijk was. Dat gold in elk geval in twee van de bestudeerde zaken. Bij de eerste zaak ging het om een onderzoek naar personen die op een online marktplaats pakketjes kochten met persoonsgegevens. Bij de start van het onderzoek was nog niet duidelijk waar deze personen de gegevens voor gebruikten. Artikel 139g Sr maakte het mogelijk om al wel een onderzoek te kunnen starten, zo legt een geïnterviewde rechercheur uit:

> Geïnterviewde: …En al die 30 verdachten hebben allemaal 139g gekregen, omdat we daar de verdenking op hebben geschreven. Dus dat was heel mooi, want als we dat [artikel 139g Sr] niet hadden dan hadden we ook geen verdenking kunnen maken.

Interviewer: En hoe zou je dat, want nu zei je van gelukkig hadden we 139g, hoe had je het gedaan als je dat [artikel 139g Sr] niet gehad had?
Geïnterviewde: Ja volgens mij hadden we dan gelijk, dan hadden we voor een heleboel verdachten geen verdenking kunnen maken. Dan [had] je echt eerst computervredebreuk moeten aantonen, of fraude of iets anders. Maar ja dat was nu niet nodig, dus dat was een hele mooie kapstok.

De tweede zaak betrof een zaak waarin de verdachte beschikte over miljoenen (buitenlandse) persoonsgegevens. Ook in deze zaak werd het onderzoek gestart op basis van artikel 139g Sr. In beide gevallen was de zaak waarschijnlijk niet opgepakt als artikel 139g Sr er niet was geweest.

Hoofdpunten

- Artikel 139g Sr biedt de opsporingspraktijk verschillende voordelen: 1) Het is een passende beschrijving voor handelingen van een verdachte die in de praktijk voorkomen; 2) Het artikel kan een alternatief zijn wanneer bij voorbaat het vermoeden bestaat dat andere artikelen niet volstaan; 3) Het artikel maakt verbeurdverklaring en ontneming van gegevens mogelijk; 4) Het artikel is behulpzaam bij de aanpak van de gehele criminele keten rondom bankfraudezaken; en 5) Het artikel zorgt ervoor dat opsporingsonderzoeken kunnen worden gestart die voorheen niet gestart konden worden.

3.3.5 Aandachtspunten

Op basis van de interviews en de vonnisanalyse is een aantal aandachtspunten naar voren gekomen met betrekking tot de toepassing van het artikel. In de komende paragrafen worden deze nader uitgewerkt. Allereerst wordt ingegaan op het strafmaximum van één jaar. Daarna zal de aandacht zich richten op de aard van de gegevens. Vervolgens komen de steler-heler-regel aan de orde en een aantal overige aandachtspunten.

Strafmaximum
De maximale straf die kan worden opgelegd voor het helen van gegevens is één jaar. Omdat het helen van gegevens zelden alleen voorkomt in een tenlastelegging, is het niet mogelijk om te achterhalen of dat ene jaar wordt opgelegd. Eén van de geïnterviewde officieren van justitie vertelt de rechter in een zaak, waarin meerdere feiten ten laste waren gelegd, gevraagd te hebben om in ieder geval voor het helen van gegevens het strafmaximum op te leggen. Daar is de rechtbank uiteindelijk niet in meegegaan[31]:

We hebben dat wel gevraagd, al meermalen. Wij [het Openbaar Ministerie] vinden dat in ieder geval voor 139g het strafmaximum opgelegd zou moeten worden. En dan nog wat erbij voor de rest, gelet op het volume (…), en als u [rechtbank] dat niet doet of wel doet, sowieso om daar een aparte overweging aan te wijden. Maar dat hebben ze nog nooit gedaan. Dus dat is nog niet gebeurd.

[31] Ruim nadat de dataverzameling voor dit onderdeel van de evaluatie plaatsvond, heeft in elk geval het Hof Amsterdam zich uitgesproken over de strafmaat van artikel 139g Sr. In deze zaak ging het om een verdachte die betrokken was bij de handel in politie-informatie. Over de strafmaat van één jaar zegt de rechtbank: 'De wetgever heeft echter blijkens artikel 139g Sr, waarin de strafbaarheid van de handel in niet-openbare politie-informatie is geregeld, op dit feit slechts een strafmaximum van één jaar gevangenisstraf gesteld. Gelet op de vergaande corrumperende werking die uitgaat van dit strafbare feit acht het hof dit strafmaximum volstrekt ontoereikend' (ECLI:NL:GHARL:2025:2408).

Eén deel van de geïnterviewden is verbaasd over de in hun ogen lage strafmaat van één jaar. Een officier van justitie zegt het een beperking te vinden dat degenen die de geheelde gegevens gebruiken, en dus de delicten plegen, een hogere straf kunnen krijgen dan degenen die de gegevens verstrekken. Die laatste groep kan maximaal één jaar gevangenisstraf krijgen waarbij dat maximum lang niet altijd zal worden opgelegd. Deze geïnterviewde merkt op dat de strafmaat van één jaar laat zien dat het beschermen van persoonsgegevens als 'niet zo belangrijk' wordt gevonden. De verbazing over de strafmaat heeft vooral te maken met de hoeveelheid gegevens die mensen in hun bezit kunnen hebben en het geld dat daarmee wordt verdiend. Het kan gaan om duizenden, maar ook om tienduizenden of miljoenen gegevens. Vooral wanneer deze gegevens met elkaar worden gecombineerd, kunnen weer andere strafbare feiten worden gepleegd. Zo kunnen door een combinatie van gegevens persoonlijke gegevens worden gevonden van ambtsdragers, zoals politiemensen en officieren van justitie. Gestolen databases kunnen ook gebruikt worden voor fraude, bijvoorbeeld bankfraude. Eén van de geïnterviewde officieren licht toe:

> Juist dat volume (…). En het is ook niet een opzichzelfstaand feit. Dit soort gegevens worden ook weer doorgehandeld, ze worden ook geraffineerd (…). Dus dat de lijsten worden gecombineerd waardoor je dus een lijst van een bank, bijvoorbeeld naast een lijst van een bitcoin bedrijf of naast een lijst van een telefoonbedrijf kunt leggen. Dan weet je opeens best wel veel van mensen. Je kunt gaan matchen op achternaam, initialen of op e-mailadres (…), telefoonnummer. En [de gegevens] worden geselecteerd op doelgroepen die interessant zijn voor andere digitale criminaliteit. Echt voorbeeld: vrouwen geboren in de jaren vijftig waarbij mijn vermoeden is dat dat is omdat dat gezien wordt als een aantrekkelijke doelgroep voor bankhelpdeskfraude en phishing.

Volgens deze geïnterviewde nemen gestolen gegevens een belangrijke plek in binnen de 'criminele voedselketen' en daar is het strafmaximum volgens deze geïnterviewde niet passend bij.

De beperkte strafmaat zou volgens een aantal geïnterviewden laten zien dat de wetgever de waarde van gegevens niet goed heeft ingeschat. Inmiddels zijn gegevens, vooral wanneer deze met elkaar gecombineerd worden, veel geld waard, zo wordt tijdens interviews aangegeven. Met de handel in data zouden 'tonnen, miljoenen' kunnen worden verdiend, al zou lang niet elk dataset zoveel geld opleveren. In dat opzicht zijn gegevens volgens één van de geïnterviewden 'het nieuwe goud' en is de huidige strafmaat meer passend bij 'puistige pubers op een zolderkamer' dan bij een 'volwassen criminaliteitsinstrumentarium'. Vanwege de waarde die gegevens kunnen hebben, verbaast deze geïnterviewde zich over het feit dat er grote verschillen bestaan tussen artikel 139g Sr en strafbaarstellingen die met goederen te maken hebben, zoals heling en witwassen. Zowel wat betreft het helen van goederen als witwassen is een parallel te trekken met hetgeen strafbaar is gesteld in artikel 139g Sr. Het verschil in strafmaat is echter groot. Op het helen van goederen staat maximaal vier jaar, en op witwassen maximaal zes. Eén van de geïnterviewde advocaten heeft niet zozeer bezwaar tegen de strafmaat die geldt voor het helen van gegevens, maar merkt op dat de wet 'consequent' moet zijn.

Het strafmaximum van één jaar leidt er niet altijd toe dat in zaken ook slechts één jaar wordt opgelegd. Dit komt vooral door het feit dat een veroordeling voor het helen van gegevens doorgaans samengaat met een veroordeling voor andere strafbare feiten (zie bijvoorbeeld ECLI:NL:RBAMS:2023:6967; ECLI:NL:RBAMS:2023:3748).

Gevolgen laag strafmaximum
Het strafmaximum van één jaar heeft een aantal gevolgen. Het eerste gevolg is dat kan worden gekozen voor een ander wetsartikel. Eén van die artikelen is artikel 234 Sr[32], geïntroduceerd in 2021. Wanneer deze route wordt gevolgd, ligt de nadruk niet op de herkomst van de gegevens, maar op hetgeen waarvoor de gegevens bestemd zijn. In artikel 234 Sr is vastgelegd dat het strafbaar is om gegevens in bezit te hebben voor het plegen van bijvoorbeeld oplichting. Daarbij moet het doel zijn om een niet-contant betaalmiddel te verkrijgen. Eén van de geïnterviewde officieren van justitie legt uit dat dit artikel, in tegenstelling tot artikel 139g Sr, 'rekenschap geeft van de financiële waarde' die gegevens kunnen hebben. Dit artikel kent een hoger strafmaximum, namelijk vier jaar. Daarnaast is artikel 234 Sr volgens deze geïnterviewde passender omdat veel van de geheelde gegevens gebruikt worden voor gedigitaliseerde criminaliteit, bijvoorbeeld bankfraude (een combinatie van diefstal met valse sleutel en oplichting). Toch zal dit artikel niet in alle situaties passend zijn, zo vermoedt een andere officier van justitie, bijvoorbeeld wanneer sprake is van bankhelpdeskfraude in plaats van fraude met een account om via het internet te bankieren. Afhankelijk van de modus operandi van criminelen kan dit artikel uitkomst bieden. In één van de zaken in de vonnisanalyse komen beide artikelen samen voor, zowel artikelen 139g als 234 Sr (ECLI:NL: RBDHA:2023:14140). Daarin is ook meteen een ander artikel te vinden dat als mogelijk alternatief kan dienen, namelijk computervredebreuk (art. 138ab Sr). Op die manier wordt, net zoals dat bij artikel 234 Sr het geval is, de mogelijk gepleegde fraude als uitgangspunt genomen. Een ander alternatief – wanneer het wachtwoorden of toegangscodes betreft - kan artikel 139d, lid 2 onder b Sr zijn.

Een tweede gevolg is dat, zo geeft één van de officieren van justitie aan, extra nagedacht wordt of dit artikel op de tenlastelegging moet komen of dat verder onderzoek moet worden gedaan naar de gegevens. Er kan zich namelijk een situatie voordoen waarin geen verder onderzoek plaatsvindt, omdat dat 'het niet waard is' gezien het strafmaximum. Ook kan de bewijsbaarheid lastig zijn (zie verderop in deze paragraaf), waardoor de keuze kan worden gemaakt om artikel 139g Sr niet mee te nemen. Volgens deze officier zijn er in het cyberdomein 'best wel veel feiten' waaruit kan worden gekozen. Op het moment dat in verband met de bewijsbaarheid van een bestanddeel vragen kunnen ontstaan, en er een strafmaximum is van één jaar, kan de keuze worden gemaakt om het helen van gegevens niet in de tenlastelegging op te nemen.

Een derde mogelijk gevolg is dat een zaak die draait om het helen van gegevens misschien niet altijd prioriteit zal krijgen in verband met het lage strafmaximum. Andere 'ernstigere delicten' zullen meer prioriteit krijgen, aldus een andere geïnterviewde officier van justitie.

Een vierde gevolg is gerelateerd aan de mogelijkheid tot voorlopige hechtenis. In één van de interviews komt naar voren dat het ingewikkeld is om een verdachte in voorlopige hechtenis te plaatsen wanneer deze wordt verdacht van het helen van

[32] Het volledige wetsartikel luidt:
1 Hij die stoffen, voorwerpen of gegevens vervaardigt, ontvangt, zich verschaft, verkoopt, overdraagt, verwerft, vervoert, invoert, uitvoert, verspreidt, anderszins ter beschikking stelt of voorhanden heeft waarvan hij weet dat zij bestemd zijn tot het plegen van een der in de artikelen 226, eerste lid, onderdelen 2° tot en met 5°, 231, eerste lid, 231a, eerste lid, 231b en 232, eerste lid, omschreven misdrijven dan wel een der misdrijven omschreven in de artikelen 310, 311, 312, 317, 321 en 326, voor zover deze feiten betrekking hebben op de verkrijging van een niet-contant betaalinstrument, wordt gestraft met gevangenisstraf van ten hoogste vier jaar of geldboete van de vierde categorie.
2 Artikel 225, derde lid, is van overeenkomstige toepassing.

gegevens. De geïnterviewde legt uit dat hij de verdachten waarmee hij doorgaans te maken krijgt in voorlopige hechtenis wil (laten) plaatsen, omdat het personen zijn die feiten zoals het helen van gegevens al langere tijd plegen en er (gedeeltelijk) hun geld mee verdienen. Echter, hoewel artikel 139g Sr een voorlopige hechtenis-feit (art. 67 lid 1 Sr) is, zijn er vaak geen gronden op basis waarvan een verdachte in voorlopige hechtenis kan worden geplaatst. Net als de grond 'vrees voor gevaar voor goederen', zou er in de ogen van deze geïnterviewde ook eenzelfde grond voor gegevens moeten komen. Op die manier kunnen gegevens op eenzelfde manier worden beschermd als goederen.

Tijdens de interviews zijn, op verzoek, suggesties gedaan over de strafmaat. Eén van de geïnterviewde officieren van justitie oppert 'een aantal jaren' en een ander zou de strafmaat gelijktrekken met witwassen, inclusief de verschillende varianten: schuld, opzet en gewoonte. Daarbij zou ook het stappenplan dat bij witwassen gehanteerd wordt (Anti Money Laundering Centre, 2025) moeten gelden: een verdachte moet zelf kunnen aantonen dat de gegevens niet geheeld zijn. Zo'n optie wordt belangrijk gevonden, omdat, zo legt een andere geïnterviewde officier van justitie uit, het bij een onlinedatabase 'bijna nooit te herleiden is' wat de oorsprong is geweest van de gegevens.

In het voorgaande is beschreven dat het strafmaximum als aandachtspunt wordt gezien. Dat geldt vooral in de zaken waarin het draait om een groot aantal (verschillende) soorten databestanden. In andere, kleinere zaken wordt het strafmaximum gezien als passend.

Hoofdpunten

- Een belangrijk aandachtspunt met betrekking tot artikel 139g Sr is het strafmaximum van één jaar. Zeker wanneer het gaat om een groot aantal gegevens dat geheeld is, zou dit strafmaximum niet passend zijn.
- Het lage strafmaximum heeft een aantal gevolgen. Het artikel wordt niet meegenomen in de tenlastelegging of er wordt gekozen voor een alternatief artikel in de tenlastelegging, namelijk artikel 234 Sr. Dit artikel kent een hoger strafmaximum, maar is alleen geschikt wanneer de gegevens worden gebruikt om een niet-contant betaalmiddel te verkrijgen, bijvoorbeeld bankfraude. De lage strafmaat kan er ook voor zorgen dat een zaak minder prioriteit krijgt. Verder is het opleggen van voorlopige hechtenis ingewikkelder.

Aard gegevens lastig aantoonbaar

Een tweede aandachtspunt heeft te maken met de aard van de gegevens en dat die lastig te bewijzen kan zijn. Daarbij gaat het om de bestanddelen 'niet-openbaar' en 'van misdrijf afkomstig'. Beide bestanddelen kunnen met elkaar samenhangen, maar worden op deze plek apart besproken.

Niet-openbaarheid gegevens

In één van de interviews wordt aangegeven dat het niet altijd duidelijk is wanneer gegevens wel of niet openbaar zijn, zoals gegevens die op socialemediakanaal Telegram gekocht worden om *phishing*aanvallen uit te voeren. De kans is groot dat die gegevens door meerdere mensen worden gekocht, en dus ook bij meerdere mensen bekend zijn. Eén van de geïnterviewde officieren van justitie vraagt zich af in hoeverre die gegevens dan nog niet-openbaar zijn. Hetzelfde geldt, zo legt een andere geïnterviewde uit, voor databases die zijn gehackt, bijvoorbeeld van een prostitutierecensie website. De vraag is hoe lang nog sprake is van het helen van

gegevens wanneer een verdachte deze gegevens in bezit heeft. Eén van deze twee geïnterviewden zou graag zien dat explicieter wordt gemaakt dat het bij niet-openbare gegevens om persoonsgegevens gaat.

In acht vonnissen wordt aandacht besteed aan de niet-openbaarheid van gegevens. Op basis hiervan wordt duidelijk dat het bij niet-openbare gegevens in elk geval gaat om (bijzondere) persoonsgegevens. In een eerder besproken zaak (ECLI:NL:RBDHA:2021:14871) waarin het helen van gegevens bewezen is verklaard betroffen de geheelde gegevens lijsten met persoonsgegevens, onder andere zogenoemde '*leads*' die de verdachte aangeschafte op Telegram. Bij deze verdachte zijn verschillende niet-openbare gegevens aangetroffen waaronder naam, adres, woonplaats, geboortedatum, telefoonnummer, e-mailadres en IBAN-nummer. Een ander voorbeeld komt de zaak ECLI:NL:RBAMS:2023:3748. Daar is het volgens de rechter de gevoelige aard en de combinatie van persoonsgegevens en medische gegevens die maakt dat sprake is van niet-openbare gegevens.[33]

Naast persoonsgegevens zijn niet-openbare gegevens ook gegevens waarvan het duidelijk niet de bedoeling is dat deze openbaar zijn, bijvoorbeeld een combinatie van inlognamen en wachtwoorden (ECLI:NL:RBAMS:2023:3358) en digitale cadeaukaarten (ECLI:NL:GHDHA:2024:226). Van het laatste soort gegevens heeft de rechtbank geoordeeld dat deze niet-openbaar zijn, omdat zij een unieke code hebben die vertrouwelijk is en alleen bij de bezitter bekend is. Niet-openbaar betekent ook dat de gegevens niet vrij toegankelijk zijn via het internet, zo blijkt uit het vonnis in een andere zaak (niet-openbaar vonnis). In deze zaak had de verdachte honderden buitenlandse telefoonnummers in zijn bezit, aangeschaft via Telegram en geselecteerd op het criterium 'vrouw'. Zulke lijsten zijn volgens de rechtbank niet vrij toegankelijk op het internet te vinden, wat maakt dat ze niet-openbaar zijn.

Tot slot zijn gegevens niet-openbaar waarvan 'algemeen bekend' is dat deze niet-openbaar zijn en niet worden verkocht. Het gaat daarbij om gegevens uit systemen van de politie (ECLI:NL:RBMNE:2023:5582) en om gegevens met de extensie 'aml' (*anti money laundering*) (ECLI:NL:RBAMS:2023:3748). In één van de eerdergenoemde zaken (ECLI:NL:RBAMS:2023:3358) besteedde de rechter ook aandacht aan gegevens die niet kunnen worden aangemerkt als niet-openbaar. Het ging hierbij om proxy IP-adressen en gegevensdragers waarop inlognamen en wachtwoorden werden gevonden. Wat betreft de gegevensdrager merkte de rechtbank op dat een gegevensdrager niet aangemerkt kan worden als een niet-openbaar gegeven. Dit geldt wel voor de inlognamen en wachtwoorden die op die gegevensdrager stonden opgeslagen. De rechtbank heeft de gegevensdrager uit de tenlastelegging gestreept en de verdachte veroordeeld voor het helen van gegevens. Wat betreft de proxy IP-adressen staat in het vonnis dat van de proxy IP-adressen onvoldoende vastgesteld kon worden in hoeverre het ging om niet-openbare gegevens. In een andere zaak (niet-openbaar vonnis) merkte de rechter op dat het dossier niet duidelijk maakte dat het niet-openbare gegevens betrof. Toch kwam de rechtbank wel tot een veroordeling voor het helen van gegevens, omdat de gegevens van misdrijf afkomstig waren. Het ging in deze zaak om NAW-gegevens (naam, adres en woonplaats) en/of telefoonnummers van een groot aantal personen.

[33] Andere overwegingen die een rol speelden zijn de verklaring van de verdachte, het feit dat de gegevens te koop werden aangeboden op een hackersforum en de extensie 'aml' (*anti money laundering*) die inherent 'naar hun aard in beginsel niet openbaar zijn'.

Hoofdpunten

- Met betrekking tot het bestanddeel 'niet-openbare gegevens' is voor opsporingsfunctionarissen niet altijd duidelijk wat niet-openbaar precies inhoudt. Op basis van de vonnisanalyse gaat het in elk geval om: 1) (bijzondere) persoonsgegevens; 2) gegevens waarvan het duidelijk de bedoelding is dat ze niet openbaar zijn; 3) gegevens die niet vrij via het internet toegankelijk zijn; en 4) gegevens waarvan algemeen bekend is dat zij niet verkocht worden.

Van misdrijf afkomstig

Naast het bestanddeel 'niet-openbare gegevens' zou ook het bestanddeel 'van misdrijf afkomstig' volgens enkele geïnterviewden niet altijd gemakkelijk aan te tonen zijn, bijvoorbeeld wanneer iemand een naaktfoto krijgt toegestuurd zonder dat de ontvanger daar om gevraagd heeft. Op het moment dat die foto door een eerste persoon rechtmatig is verkregen, is al geen sprake meer van door misdrijf verkregen. In twaalf vonnissen is expliciet aandacht besteed aan het bestanddeel 'van misdrijf afkomstig'. In drie zaken is onvoldoende vast komen te staan dat van dit soort gegevens sprake was. In twee zaken (ECLI:NL:RBMNE:2022:677; ECLI:NL:RBMNE:2022:655) kon bijvoorbeeld niet worden bewezen dat de *leads* (lijsten met rekeningnummers en personen en lijsten met rekeningnummers en telefoonnummers) door middel van een misdrijf waren verkregen, en in een andere zaak (ECLI:NL:RBZWB:2023:5123) schreef de rechtbank 'dat het zich laat raden hoe de gegevens op de telefoons en laptops terechtgekomen zijn. Een andere legale reden voor de beschikking hierover is niet zonder meer uitgesloten'. In deze zaak is van één niet-openbaar gegeven, een creditcard met CVC-nummer, wel vast komen te staan dat deze door een misdrijf was verkregen. Het betrof hier echter een misdrijf dat de verdachte zelf had gepleegd waardoor die persoon niet vervolgd kon worden voor het helen van gegevens (de heler-steler-regel – zie volgende paragraaf). In de andere zaken is voldoende vast komen te staan dat de gegevens uit een misdrijf waren verkregen. Zo was in één van de zaken (ECLI:NL:RBAMS:2023:3358) volgens de rechter geen aannemelijk scenario voorstelbaar dat degene die de gegevens (inlognamen en wachtwoorden) aan de verdachte verstrekte (een onbekend gebleven persoon) de gegevens op een eerlijke manier had verkregen. In een andere zaak maakte het aantal gegevens gecombineerd met de informatie uit de rest van het dossier dat sprake was van 'van misdrijf afkomstig' (niet-openbaar vonnis). In de andere zaken is vast komen te staan dat de verdachte op de hoogte was van de herkomst van de gegevens, bijvoorbeeld omdat de verdachte wist dat deze door hacken verkregen waren (ECLI:NL:RBAMS:2023:3748) of het algemeen bekend was dat sommige gegevens niet legaal beschikbaar zijn. Daarbij ging het bijvoorbeeld om Excel-lijsten met persoonsgegevens van honderden personen (ECLI:NL:RBDHA:2024:4472; niet-openbaar vonnis) en politiegegevens (ECLI:NL:RBMNE:2023:5582). In één van de zaken (niet-openbaar vonnis) bekende de verdachte dat hij wist dat de gegevens afkomstig waren van een misdrijf.

Hoofdpunten

- Met betrekking tot het bestanddeel 'van misdrijf afkomstig' laat de vonnisanalyse zien dat in drie zaken niet aangetoond kon worden dat het om gegevens ging die van een misdrijf afkomstig waren.
- In vijf zaken was wel duidelijk geworden dat het gegevens betrof die van een misdrijf afkomstig waren, bijvoorbeeld omdat duidelijk was dat een verdachte dit wist of omdat algemeen bekend was dat sommige gegevens niet-legaal beschikbaar zijn.

Heler-steler-regel
Uit een klein deel van de vonnissen en interviews volgt dat geen veroordeling voor het helen van gegevens plaats heeft gevonden wanneer de verdachte de geheelde gegevens zelf door een misdrijf had verkregen. Dit naar analogie van de wijze waarop met de heling van goederen wordt omgegaan (de 'heler-steler-regel'). Deze regel heeft betrekking op artikel 416 Sr (opzetheling) en is gebaseerd op een uitspraak van de Hoge Raad waarin de Hoge Raad oordeelde dat iemand die een helingshandeling verrichtte ten aanzien van een voorwerp wat hij zelf door enig misdrijf verkreeg, niet veroordeeld kon worden voor heling (ECLI:NL:HR:2001:AD5149). Hoewel deze regel geldt voor goederen, is het in drie zaken (ECLI:NL:RBZWB:2023:5123; ECLI:NL:RBZWB:2021:6062; ECLI:NL:RBAMS:2023:6967), vanwege deze regel, niet tot een (volledige) veroordeling of strafoplegging gekomen voor het helen van gegevens. In één van de zaken (ECLI:NL:RBZWB:2023:5123) ging het om een creditcard met CCV-nummer die de verdachte zelf mogelijk had verkregen middels digitale oplichting. In de andere zaak (ECLI:NL:RBZWB:2021:6062), waarin het draaide om inlognamen en wachtwoorden, besteedde de rechter expliciet aandacht aan zijn overweging om over te gaan tot vrijspraak ten aanzien van het helen van gegevens. De rechter merkt op dat het de bedoeling is geweest van de wetgever om 'heling van niet-openbare gegevens strafbaar te stellen in situaties waarin niet kan worden aangetoond dat de persoon deze gegevens zelf heeft overgenomen, al dan niet na een geautomatiseerd werk te zijn binnengedrongen'. Verder wordt in het vonnis verwezen naar artikel 416 Sr (opzetheling) waarbij het voor een bewezenverklaring van dat feit nodig is dat een ander het misdrijf pleegde waarmee de goederen werden verkregen, de heler-steler-regel.

Uit de vonnisanalyse komt ook naar voren dat niet elke rechter de heler-steler-regel hanteert. In vijf zaken (vier niet-openbare vonnissen; ECLI:NL:RBNHO:2022:921) is de verdachte veroordeeld voor het helen van gegevens die hij door een eigen misdrijf had verkregen. Twee geïnterviewde officieren van justitie vertellen over één van deze zaken waarin een verdachte afbeeldingen van een socialemediaplatform had verspreid (helen van gegevens) die hij zelf verkregen had middels computervredebreuk. Eén van hen had er rekening mee gehouden dat de heler-steler-regel mogelijk een rol zou gaan spelen tijdens de rechtszaak, maar dat is niet gebeurd. Deze verdachte is zowel veroordeeld voor computervredebreuk als voor het helen van gegevens (niet openbaar vonnis). Op basis van deze ervaring geeft deze officier aan dat, redenerend vanuit het feit dat de heler-steler-regel niet is toegepast, misschien niet een parallel moet worden getrokken tussen het helen van goederen en het helen van gegevens, maar dat het helen van gegevens beter te vergelijken is met witwassen.[34] Ook in twee andere zaken (beide niet-openbaar vonnis) zijn de verdachten zowel veroordeeld voor computervredebreuk als voor het helen van gegevens. Het ging hier om werknemers die klantgegevens overnamen, gedeeltelijk met andermans accounts, en deze verspreidden. In de laatste twee zaken draaide het om een verdachten die stiekem een filmpje maakten van seksuele handelingen en dit filmpje verder verspreidde (tegen de zin van het slachtoffer in). In beide zaken is de verdachte zowel veroordeeld voor het helen van gegevens als voor het opzettelijk en wederrechtelijk vervaardigen van een afbeelding (art. 139f Sr) (niet openbaar vonnis; ECLI:NL:RBNHO:2022:921).

Hoofdpunten
- Naar analogie van de wijze waarop met een veroordeling voor de heling van goederen kan worden omgegaan (de 'heler-steler-regel'), heeft de zittingsrechter in

[34] Hoewel de geïnterviewde dit niet nader toelicht, wordt waarschijnlijk gedoeld op het feit dat witwassen betrekking kan hebben op geld dat door eigen misdrijf verkregen is.

drie 139g-zaken een verdachte niet veroordeeld of geen straf opgelegd voor het helen van gegevens, omdat de verdachte deze gegevens zelf door een misdrijf had verkregen. In vijf zaken heeft de zittingsrechter de heler-steler-regel niet toegepast en is de verdachte veroordeeld voor de heling van gegevens die hij zelf door een misdrijf verkregen had.

3.4 Tot slot

De wetgever heeft artikel 139g Sr geïntroduceerd om burgers te beschermen van wie gegevens, ontvreemd door een ander, bekend worden gemaakt, verkocht of op het internet worden geplaatst. Vóór de introductie was dit niet (altijd) mogelijk. In dit hoofdstuk is duidelijk geworden dat, sinds de inwerkingtreding van de Wet CCIII, verdachten vervolgd zijn voor het helen van gegevens. In de periode maart 2019-april 2024 zijn 93 zaken ingestroomd bij het Openbaar Ministerie. In 85 zaken was artikel 139g Sr het enige CCIII-feit in de tenlastelegging en in 8 zaken was sprake van een combinatie van CCIII-feiten. In 42 zaken was een eindvonnis beschikbaar. In een ruime meerderheid van die zaken (36) is de verdachte veroordeeld voor het 139g-feit en legde de rechter een straf op. In dat opzicht zijn gegevens in de praktijk beter beschermd, omdat voor verdachten een risico op vervolging bestaat. Of de nieuwe wettelijke bepaling daadwerkelijk een afschrikwekkende werking heeft, kan op basis van deze evaluatie niet worden gezegd.

In de meeste zaken waarin artikel 139g Sr ten laste is gelegd draaide het, naast het helen van (vooral) offline en online persoonlijke gegevens, om meerdere feiten. In ruim de helft van de zaken in de vonnisanalyse kwam het artikel samen voor met een vorm van fraude waardoor burgers financieel benadeeld werden. Soms waren het helen van gegevens en de andere feiten direct aan elkaar gerelateerd. Dat wil zeggen dat de geheelde gegevens gebruikt werden voor het plegen van de andere feiten die in de tenlastelegging stonden opgenomen.

De evaluatie van dit artikel heeft een aantal aandachtspunten zichtbaar gemaakt. De eerste heeft betrekking op de gekozen strafmaat. De wetgever heeft gekozen voor een strafmaximum van één jaar, vergelijkbaar met het wederrechtelijk overnemen of aftappen van gegevens die via telecommunicatie of een geautomatiseerd werk verwerkt of overgedragen worden (art. 139c Sr). Ook komt deze strafmaat overeen met schuldheling (art. 417bis Sr). Er is (bewust) geen aansluiting gezocht bij opzetheling (art. 416 Sr) dat een strafmaximum kent van vier jaar. Op basis van dit onderzoek zijn hierbij twee kanttekeningen te plaatsen. De eerste kanttekening is dat het de vraag is of deze keuze wetsystematisch gezien de meest logische keuze is geweest, zeker in gevallen dat een verdachte weet dat de gegevens van een misdrijf afkomstig zijn. In die gevallen zou het vanuit wetsystematisch oogpunt meer voor de hand liggen om de strafmaat van opzetheling en het helen van gegevens in overeenstemming met elkaar te brengen, al dan niet door meerdere varianten van het helen van gegevens te onderscheiden. Op die manier komt de wijze waarop met goederen en gegevens wordt omgegaan meer in lijn met elkaar. Daarnaast laat dit onderzoek zien dat er grote variatie kan bestaan wat betreft de hoeveelheid gegevens die wordt gestolen. De vraag is in hoeverre dit strafmaximum aansluit bij deze variatie, zeker gezien het strafmaximum ertoe kan leiden dat het helen van gegevens niet op een tenlastelegging komt, of dat er geen nader onderzoek wordt gedaan naar de geheelde gegevens waardoor gegevens minder goed beschermd kunnen worden. Er worden inmiddels alternatieve wetsartikelen gebruikt die een hogere strafmaat

kennen, bijvoorbeeld artikel 234 Sr. Dit artikel is passend in situaties dat de geheelde gegevens gebruikt worden voor bijvoorbeeld bankfraude. Bij andere vormen van fraude, zoals bankhelpdeskfraude, kan dit artikel weer niet worden gebruikt, omdat sprake moet zijn van handelingen gericht op het verkrijgen van een niet-contant betaalinstrument.

Het tweede aandachtspunt heeft betrekking op het kunnen veroordelen voor het helen van gegevens, als deze gegevens door een eigen misdrijf verkregen zijn. In het wetsartikel zelf is hier niks over opgenomen, maar uit de memorie van toelichting volgt dat de strafbaarstelling bedoeld is voor situaties waarin niet aangetoond kan worden dat degene die de gegevens bekend maakt, ook degene is die de gegevens overgenomen heeft. Daaruit kan worden afgeleid dat dit artikel dus geen betrekking heeft op situaties waarin dit wel het geval is en de verdachte bijvoorbeeld de gegevens zelf middels een misdrijf verkregen heeft. De jurisprudentie laat zien dat rechters verschillend oordelen over dit punt. Mogelijk wordt in de toekomst nog verder doorgeprocedeerd over de vraag of de heler-steler-regel ook van toepassing is bij het helen van gegevens.

4 Online handelsfraude (art. 326e Sr)

Dit hoofdstuk richt de aandacht op de strafbaarstelling van online handelsfraude, artikel 326e Sr. Allereerst wordt het juridisch kader van dit wetsartikel uiteengezet (paragraaf 4.1). Vervolgens wordt de noodzaak (volgens de wetgever) van dit wetsartikel besproken alsmede de veronderstellingen die aan deze bepaling ten grondslag liggen (paragraaf 4.2). In dit gedeelte wordt ook de doelstelling van artikel 326e Sr geschetst. Hierna volgt een uiteenzetting van de toepassing van het artikel in de opsporings- en vervolgingspraktijk, waarbij onder andere de voordelen voor de opsporingspraktijk en de aandachtspunten besproken worden (paragraaf 4.3). In de slotparagraaf worden de door de wetgever beoogde veronderstellingen vergeleken met de praktijk (paragraaf 4.5).

4.1 Juridisch kader

Met de inwerkingtreding van de Wet CCIII is 'online handelsfraude' expliciet strafbaar gesteld. Het nieuwe wetsartikel, artikel 326e Sr, 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 gevangenisstraf van ten hoogste vier jaren of geldboete van de vijfde categorie.

Om tot een strafbaarstelling van online handelsfraude te komen zijn de volgende delictsbestanddelen van belang (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 92-93):

1 Het beroep of gewoonte maken van het te koop aanbieden van een goed of het aanbieden van een dienst. Een gewoonte betekent dat meerdere keren gelijksoortige feiten zijn gepleegd. Eenmalig een goed te koop aanbieden of een dienst verlenen valt hier niet onder.
2 Er dient sprake te zijn van 'het door middel van een geautomatiseerd werk met gebruikmaking van een communicatiedienst aanbieden'. Dit houdt in dat sprake is van een aanbod van de verkoop via het internet (inclusief e-mail). Verkoop in een winkel, aan de deur, in een kantoor of telefonische verkoop vallen hier niet onder.
3 Het oogmerk bij het verkopen van goederen of diensten dient erop gericht te zijn niet of niet volledig te leveren en zichzelf of een ander de beschikking te verzekeren over de betaling. Het moet hier gaan om een 'moedwillige wanprestatie.' Als oogmerk kan ook worden aangemerkt de intentie om na betaling gedeeltelijk te leveren.

Online handelsfraude is een fenomeen dat veel slachtoffers kent, aldus de wetgever in de memorie van toelichting. Daarnaast is bij online handelsfraude vaak sprake van meerdere slachtoffers tegelijkertijd, wat wil zeggen dat veel aangiften die binnenkomen bij de politie betrekking hebben op dezelfde verkoopaanbieding (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 73). Het doel van de nieuwe strafbaarstelling is om (grootschalige) online handelsfraude te kunnen vervolgen. Naast het online aanbieden van producten heeft dit artikel ook betrekking op het aanbieden van diensten. Daarbij kan het gaan om het aanbieden van tickets voor

concerten, treinkaartjes, reizen, boeken- en cadeaubonnen (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 93).

4.2 Noodzaak en veronderstellingen

Een belangrijke reden voor de komst van de nieuwe strafbaarstelling, blijkend uit de memorie van toelichting, is dat vervolging van online handelsfraude op basis van het al bestaande artikel oplichting (art. 326 Sr) beperkt succesvol was. Hoewel er jurisprudentie is waaruit blijkt dat vervolging op basis van dat artikel mogelijk kan zijn, is er ook jurisprudentie die het tegenovergestelde laat zien.[35,36] De strafbaarstelling van online handelsfraude (art. 326e Sr) moet in die laatste gevallen uitkomst bieden.

Op basis van de memorie van toelichting kunnen de volgende veronderstellingen geformuleerd worden:

1 Ontwikkelingen op het internet zorgen ervoor dat online handelsfraude een toenemend maatschappelijk probleem is. Bij de aanpak van dit probleem hebben zowel private als publieke partijen een rol. De aanpak van online handelsfraude verloopt echter moeizaam. Maatregelen van private partijen werken niet altijd, omdat fraudeurs kunnen werken met tijdelijke websites. Dat leidt ertoe dat slachtoffers een aanbieder niet kunnen verzoeken zijn verplichting na te komen of een schadevergoeding te eisen. Daardoor worden slachtoffers benadeeld. De nieuwe strafbaarstelling maakt het mogelijk dat slachtoffers zich als benadeelde partij bij het strafproces voegen. Dat leidt ertoe dat slachtoffers gecompenseerd kunnen worden.
2 De politie heeft meer mogelijkheden dan de 'gewone' burger om online handelsfraude te bestrijden. Het resultaat van haar werkzaamheden leidt echter niet altijd tot een vervolging, omdat het bestaande artikel oplichting (art. 326 Sr) hiervoor onvoldoende wettelijke basis biedt. Dat leidt ertoe dat verdachten van

[35] In 2013 oordeelde een feitenrechter dat het enkel niet leveren van een goed beschouwd moet worden als het aannemen van een valse hoedanigheid, omdat hiermee in strijd wordt gehandeld met het goed vertrouwen dat in het maatschappelijk verkeer gebruikelijk is (zie onder meer Hof Arnhem-Leeuwarden 21-06-2013, ECLI:NL:GHARL:2013:4498). In 2014 oordeelde Hoge Raad (HR 11 november 2014, ECLI:NL:HR:2014:3144) echter dat het zich voordoen als een bonafide verkoper niet zonder meer oplevert het aannemen van een valse hoedanigheid in de zin van artikel 326 Sr. Om tot strafbaarheid in de zin van artikel 326 Sr te komen moeten de gedragingen meer omvatten en moet dit gepaard gaan met het doelbewust verstrekken van onbruikbare contactgegevens aan de potentiële koper, terwijl die persoon niet van plan is over te gaan tot daadwerkelijke levering. Tegelijkertijd zegt de Hoge Raad over een andere uitspraak van het Amsterdamse Gerechtshof (ECLI:NL:HR:2014:3546), waarin de rechter oordeelde dat 'de enkele omstandigheid dat de verdachte die via een website goederen te koop aanbood en bestellingen en betalingen van kopers accepteerde, terwijl hij wist dat hij niet tot levering zou overgaan, niet kan worden aangemerkt als het aannemen van een valse hoedanigheid' (Kamerstukken II 2015/16, 34 372, nr. 3, p. 74) geen blijk geeft van een onjuiste rechtsopvatting. Deze uitspraak volgend zou online handelsfraude niet kunnen worden vervolgd op basis van artikel 326 Sr.

[36] Voorbeelden van jurisprudentie waarin het voordoen als bonafide verkoper geen valse hoedanigheid opleverde zijn: ECLI:NL:RBNHO:2013:BZ9266; ECLI:NL:HR:2014:3546; ECLI:NL:HR:2001:AD4320; ECLI:NL:RBNHO:2013:BZ9266; ECLI:NL:GHSGR:2012:BW:5086; ECLI:NL:GHDHA:2013:3425. In andere zaken is wel sprake van oplichting. Bij één zaak (ECLI:NL:GHSHE:2013:3013 en ECLI:NL:HR:2014:3144) was wel sprake van oplichting, omdat de verdachte gebruikmaakte van foutieve emailadressen. In een andere zaak (ECLI:NL:GHARL:2013:4093), waarin ook sprake was van oplichting, gebruikte de verdachte zijn eigen rekeningnummer en die van een ander. In de zaak met ecli-nummer ECLI:NL:RBNHO:2013:11557 oordeelde de rechter dat het voordoen als bonafide verkoper een valse hoedanigheid opleverde waardoor ook sprake was van oplichting. In nog een andere zaak (ECLI:NL:RBBRE:2011:BP9283) was sprake van oplichting en maakte de verdachte gebruik van een andere naam en emailadressen die niet in gebruik waren. Verder werd in één zaak (ECLI:NL:RBBRE:2008:BC8213) oplichting bewezen op basis van het feit dat verdachte en medeverdachte zich hadden bevoordeeld door het aannemen van een valse hoedanigheid door zich voor te doen als betrouwbare verkoper.

online handelsfraude niet kunnen worden vervolgd. De nieuwe strafbaarstelling maakt vervolging van online handelsfraude wel mogelijk.

3 De capaciteit van opsporingsinstanties is te beperkt om alle gevallen van online handelsfraude te vervolgen. Dat leidt ertoe dat niet alle gevallen van online handelsfraude strafrechtelijk kunnen worden aangepakt en dat alleen strafrechtelijk wordt opgetreden in zaken waarin dit noodzakelijk is. Door de nieuwe strafbaarstelling wordt het Openbaar Ministerie in staat gesteld vervolging in te stellen in zaken waarin sprake is van grootschalige online handelsfraude.37 Andere fraudegevallen worden in gezamenlijkheid aangepakt door zowel private als publieke partijen.

4.3 Artikel 326e Sr in de praktijk

In de rest van het hoofdstuk wordt de aandacht gericht op de wijze waarop artikel 326e Sr is toegepast in de praktijk. Eerst wordt ingegaan op de aangiftes die binnenkomen bij de politie, waarna wordt stilgestaan bij de wijze waarop het Openbaar Ministerie en de rechtbank 326e-zaken hebben afgedaan. Vervolgens wordt, op basis van de vonnisanalyse en de uitgevoerde interviews, ingegaan op de aard van de 326e-zaken. Daarna richt de aandacht zich op de aanpak van online handelsfraude, de voordelen voor de opsporingspraktijk en de aandachtspunten.

4.3.1 LMIO en aangiften bij de politie

Het Landelijk Meldpunt InternetOplichting (hierna: LMIO)[38] ontvangt alle aangiften van online handelsfraude en is verantwoordelijk voor de analyse en het routeren, ofwel doorsturen van deze aangiften. Het meldpunt, opgericht in 2010, is een publiek-privaat samenwerkingsverband dat in het leven geroepen is door onder andere de politie, het Openbaar Ministerie, online handelsplaatsen en verscheidene banken. LMIO verzorgt de landelijke coördinatie als het gaat om de aanpak, bestrijding en preventie van online handelsfraude. Ook is het LMIO een belangrijk aanspreekpunt voor de regionale politie-eenheden als het gaat om internetoplichting (LMIO, 2022, p. 5, 9).

In 2023 zijn bij het LMIO 40.365 aangiftes gedaan van oplichting met online handel (persoonlijke communicatie, 9-1-2025). Dat is zo'n 4000 aangiften minder in vergelijking met 2021. Toen waren er 44.318 aangiftes. Een medewerker van het LMIO legt uit dat het bij deze cijfers niet alleen gaat om online handelsfraude, er zijn bijvoorbeeld ook 'enkelvoudige aangiftes', dat wil zeggen dat iemand één keer online opgelicht is. Bovendien zou ongeveer 20% van de aangiftes weer worden ingetrokken.

Sinds 1 juli 2024 worden alle aangiften, mits deze betrekking hebben op een Nederlands bankrekeningnummer, vanuit het LMIO doorgestuurd naar de politie-eenheid in de woonplaats van de verdachte.[39] Voorheen was dit anders. Wanneer slachtoffers bij de regionale politie aangifte deden, kwamen de aangiftes daar binnen, terwijl aangiftes via het LMIO op één centraal punt binnenkwamen. Het doorsturen

37 Wat precies onder grootschalige online handelsfraude wordt verstaan wordt niet gedefinieerd in de memorie van toelichting.

38 LMIO maakt deel uit van Operatie Centurion. Operatie Centurion is in het leven geroepen vanwege de krapte in capaciteit en de ontwikkelingen op het gebied van gedigitaliseerde criminaliteit. Het is een samenwerking tussen de Openbaar Ministerie en de politie (OM, Operatie Centurion, p. 4).

39 Overige aangiftes, die bijvoorbeeld betrekking hebben op buitenlandse rekeningnummers, gaan momenteel nog naar een centrale database die niet is gekoppeld aan een specifieke eenheid. In de toekomst zullen niet-gerouteerde aangiftes doorgestuurd worden naar de eenheid van de aangever (persoonlijke communicatie, 1-10-2025).

moet ervoor zorgen dat een 'werkstroom' ontstaat waarin aangiften worden gebundeld (indien er meerdere bestaan) en worden doorgestuurd naar het basisteam van de woonplaats van de verdachte (Openbaar Ministerie, 2022, p. 5). Dit moet voorkomen dat deze aangiftes verspreid blijven liggen over het hele land. Het LMIO heeft daarbij een voorbereidende rol, bijvoorbeeld bundeling van aangiftes, en handelt zelf geen zaken af. De voorbereidingshandelingen getroffen door het LMIO vormen de basis waarmee de regionale eenheden verder zouden moeten kunnen. Soms past het LMIO bijzondere opsporingsbevoegdheden toe. Vaak staat in een aangifte een rekeningnummer van de tegenpartij (verdachte). Door een koppeling met het Verwijzingsportaal banken, waarbij alle Nederlandse banken aangesloten zijn, vraagt het LMIO middels een vordering op wie de rekeninghouder is. Vervolgens kunnen aangiftes met betrekking tot dezelfde rekeninghouder worden gebundeld en kunnen deze worden doorgestuurd naar de politie-eenheid van de woonplaats van de verdachte (LMIO, 2022, p. 7).

4.3.2 Instroom en afdoening Openbaar Ministerie

In de tabel 4.1 wordt een overzicht gegeven van de wijze waarop het Openbaar Ministerie 326e-zaken heeft afgehandeld. Deze gegevens zijn gebaseerd op cijfers uit RAC-min. Daarin staat informatie over de instroom van zaken bij het Openbaar Ministerie en over de afhandeling van die zaken door het Openbaar Ministerie en door de rechter in eerste aanleg (Verweij & Tollenaar, 2020, p. 12).

Tabel 4.1 Afdoening Openbaar Ministerie artikel 326e Sr

Afdoening Openbaar Ministerie	Aantal
Dagvaarding	167
➢ Geen sepot 326e Sr	112
➢ Sepot 326e Sr	12
➢ Gedeeltelijk sepot 326e Sr	43
OM-strafbeschikking	19
➢ Geen sepot 326e Sr	16
➢ Sepot 326e Sr	2
➢ Gedeeltelijk sepot 326e Sr	1
Sepots	92
➢ Onvoorwaardelijk	82
➢ Voorwaardelijk	10
Transactie	1
Totaal	**279**

Tabel 4.1 laat zien dat het Openbaar Ministerie in de periode maart 2019-april 2024 279 zaken heeft behandeld waarin artikel 326e Sr ten minste één keer voorkwam in de tenlastelegging. Het gaat om zaken met een pleegdatum van het gepleegde strafbare feit in de periode van 1 maart 2019 tot en met 30 april 2024.
Van de 167 zaken waarbij een dagvaarding heeft plaatsgevonden zijn er 54 zaken waarin sprake was van een gedeeltelijk sepot, dat wil zeggen dat in een zaak niet alle

tenlastegelegde 326e-feiten geseponeerd zijn. In 12 zaken was sprake van een volledig sepot. Verder zijn 92 zaken geseponeerd zonder dat een dagvaarding is uitgereikt. Hierbij gaat het om 82 onvoorwaardelijke sepots en 10 voorwaardelijke sepots. Tot slot is in 19 zaken een OM-strafbeschikking opgelegd, waarvan bij 3 zaken ook een gedeeltelijk sepot plaatsvond.

Er zijn verschillende redenen voor het seponeren van een 326e-feit. Deze redenen zijn weergegeven in tabel 4.2. Bij de categorieën onvoorwaardelijk sepot en voorwaardelijk sepot is expliciet onderscheid gemaakt tussen het aantal zaken en unieke sepotgronden per feit. In één zaak kunnen namelijk meerdere 326e-feiten ten laste zijn gelegd, die ieder hun eigen sepotgrond kennen. Indien in één zaak aan meerdere 326e-feiten dezelfde sepotgrond werd toegekend, is deze sepotgrond één keer meegeteld.

Tabel 4.2 Sepotgronden artikel 326e Sr

Sepotgronden	Aantal
Dagvaarding	55
➢ Feit dubbel ingeboekt	47
➢ Feit niet strafbaar	1
➢ Onvoldoende bewijs	7
Strafbeschikking	3
➢ Feit dubbel ingeboekt	2
➢ Onvoldoende bewijs	1
Onvoorwaardelijk sepot	82
➢ Civiel en administratief recht	3
➢ Feit niet strafbaar	1
➢ Gering (aandeel in) feit	2
➢ Onvoldoende bewijs	41
➢ Feit dubbel ingeboekt	12
➢ Onvoldoende bewijs en dubbel ingeboekt	1
➢ Beëindiging executie strafbeschikking: Niet ontvankelijk	1
➢ Beëindiging executie strafbeschikking: oud feit	1
➢ Recente bestraffing	1
➢ Ten onrechte als verdachte aangemerkt	3
➢ Ten onrechte als verdachte aangemerkt en onvoldoende bewijs	w
➢ Verhouding tot de benadeelde geregeld	2
➢ Oud feit	12
➢ Gewijzigde omstandigheden	1
Voorwaardelijk sepot	10
➢ Gering feit	1
➢ Gering aandeel feit en feit dubbel ingeboekt	2
➢ Gewijzigde omstandigheden en feit dubbel ingeboekt	1

Sepotgronden	Aantal
➢ Verhouding tot benadeelde geregeld	2
➢ Verhouding tot de benadeelde geregeld en feit dubbel ingeboekt	1
➢ Recente bestraffing	1
➢ Beperkte kring	1
➢ Onbekend	1

4.3.3 Vonnissen rechtbank

In de periode maart 2019-april 2024 zijn 91 zaken ingestroomd bij de rechtbank. Het gaat hierbij om ingestroomde zaken bij de rechtbank waarvan ook een eindvonnis beschikbaar was. Tabel 4.3 geeft weer hoe deze 326e-zaken zijn afgedaan. In een ruime meerderheid van de zaken (73) werd de verdachte veroordeeld voor het plegen van ten minste één 326e-feit. In 17 zaken sprak de rechter de verdachte vrij van online handelsfraude en in 1 zaak volgde ontslag van alle rechtsvervolging wat betreft online handelsfraude.

Tabel 4.3 Gerechtelijke afdoening artikel 326e Sr

Afdoening*	Aantal
Ontslag van alle rechtsvervolging	1
Strafoplegging	73
Vrijspraak	17
Totaal	**91**

* Hierin zijn 13 zaken meegenomen die ter terechtzitting gevoegd waren.

4.3.4 Aard artikel 326e Sr-zaken

Om zicht te krijgen op het soort zaken waarin het nieuwe artikel 326e Sr voorkomt is een vonnisanalyse uitgevoerd. In totaal zijn 195 uitspraken geanalyseerd. Hierbij gaat het om 167 beschikkingen op beklag, 18 uitspraken van de meervoudige kamer in eerste aanleg, 2 uitspraken in hoger beroep, 7 uitspraken van de politierechter en 1 zaak van de kinderrechter. Van de geanalyseerde uitspraak in hoger beroep is ook de uitspraak in eerste aanleg meegenomen in de analyse, waardoor 28 vonnissen (of uitspraken) worden geteld als 27 zaken. Van de andere uitspraak in hoger beroep hebben we niet kunnen achterhalen of de uitspraak in eerste aanleg ook meegenomen is in de analyse, aangezien het een vonnis van de politierechter betrof. Zulke vonnissen worden doorgaans niet gepubliceerd, ook niet in het e-archief. In de komende paragrafen worden eerst de beklagzaken besproken. Hierna wordt dieper ingegaan op de zaken waarin de rechter een vonnis uitsprak. Daarbij wordt eerst korst stilgestaan bij de vonnissen waarbij artikel 326e Sr het enige strafbare feit was op de tenlastelegging. Daarna worden de vonnissen besproken waarbij ook andere feiten dan artikel 326e Sr op de tenlastelegging stonden.

Beklagschriften
Een medewerker van het LMIO vertelt hoe beklagzaken doorgaans tot stand komen. Als binnen zes maanden niet duidelijk blijkt dat meerdere aangiftes tegen dezelfde verdachte bekend zijn of er geen verzoek vanuit een politie-eenheid is gekomen om

een zaak op te pakken, seponeert het Openbaar Ministerie een zaak vrijwel automatisch. Indien dit het geval is, krijgt het slachtoffer de mogelijkheid om een klacht in te dienen op grond van artikel 12 Sv. Dit wordt ook wel een '12 Sv-procedure' genoemd en is voor iedere belanghebbende zonder bijstand van een advocaat toegankelijk (OM, z.d.). Het Hof kan dan alsnog beslissen dat de zaak moet worden opgepakt. In de periode maart 2019-april 2024 waren er 249 klachten niet-vervolging ingediend bij het Gerechtshof Amsterdam.[40] In deze beklagschriften ging het in alle gevallen over internetoplichting. Uiteindelijk zijn 167 klachten nader geanalyseerd.[41] Van de 167 beklagschriften zijn 154 klachten afgewezen en in 13 gevallen werd het beklag toegewezen. In vrijwel alle geanalyseerde beklagzaken legde het LMIO de aangiftes van de klagers voor aan de officier van justitie. In veel gevallen ging het om klagers die een aankoop deden via Marktplaats zonder levering. In een ander deel van de zaken ging het om een aankoop via een (andere) website of Facebook Marketplace. Vaak betroffen dit zaken waarbij geen of weinig andere soortgelijke aangiftes bekend zijn geworden tegen de beklaagde, wat maakt dat niet gesproken kan worden van een 'gewoonte' en er geen sprake is van online handelsfraude. Wel kon het in dit soort zaken gaan om oplichting indien aan de bestanddelen van artikel 326 Sr is voldaan – zoals wanneer sprake was van een valse naam of oplichtingsmiddel, zo blijkt uit de niet-openbare beschikkingen.

In dertien zaken achtte het Gerechtshof het beklag gegrond, bijvoorbeeld omdat: 1) sprake was van meerdere soortgelijke aangiften en een hoge totale schade; 2) niet-vervolging onredelijk zou zijn; 3) het dossier voldoende aanwijzingen bevatte voor vervolging; of 4) omdat sprake was van een minderjarige verdachte. In zeven van deze beklagschriften werd online handelsfraude expliciet genoemd. De schade van de klager varieerde van 50 euro tot meer dan 700 euro.

Het Hof achtte 154 beklagschriften ongegrond. De motivering van het Hof heeft in veel afwijzingen van het beklag een soortgelijke inhoud. De overwegingen voor afwijzing zijn als volgt samen te vatten. In algemene zin wees het Hof beklagschriften af vanwege een gebrek aan opsporingscapaciteit bij politie en justitie. In de beschikkingen stelt het Hof in haar overwegingen voorop dat in veel gevallen geen sprake is van een strafbaar feit maar van civielrechtelijke wanprestatie, waardoor de weg naar de civiele rechter openstaat. Verder bekijkt het Hof in hoeverre er aanwijzingen zijn voor oplichting (art. 326 Sr) dan wel online handelsfraude (art. 326e Sr) die nopen tot vervolging. In alle afgewezen en toegekende beklagschriften (167 in totaal) beoordeelde het hof of sprake was van oplichting. In 44 beklagschriften werd eveneens online handelsfraude genoemd en beoordeeld. Mogelijk heeft dit verschil (167 versus 44) te maken met het feit dat niet alle internetoplichting online

[40] Tot september 2023 kwamen in principe alle klachten binnen bij het Gerechtshof Amsterdam. Vanaf september 2023 is gefaseerd het 'routeren' van zaken ingevoerd waardoor klachten ook bij andere Gerechtshoven terecht (hebben) kunnen komen. Op die aantallen hebben wij geen zicht kunnen krijgen.

[41] 82 beschikkingen op beklag zijn uiteindelijk niet nader geanalyseerd. 32 klachten betroffen feiten gepleegd vóór de inwerkingtreding van de Wet CCIII. Deze klachten zijn buiten beschouwing gelaten. Datzelfde geldt voor 11 zaken die gingen over feiten die geen online handelsfraude betroffen in de zin van artikel 326e Sr, zoals een klager die iets verkocht of een slachtoffer van internetfraude. Denk aan bijvoorbeeld vriend-in-nood-fraude of cryptovalutascams. Deze zaken zijn ook buiten beschouwing gelaten. Verder verklaarde het Hof 29 zaken niet-ontvankelijk, veelal omdat geen sprake was van niet-vervolging. In 27 van de 30 zaken liep het onderzoek nog of werd de zaak alsnog strafrechtelijk vervolgd. In 1 van de 3 overige zaken was het Hof Amsterdam niet bevoegd. De tweede zaak betrof een dubbele aangifte en van de derde zaak was het klaagschrift incompleet. Van deze laatste zaak is ook het complete klaagschrift opgenomen in de analyse, dit betrof een afwijzing. Verder zijn 10 beklagschriften ingetrokken door de beklager, bijvoorbeeld omdat de schade reeds was terugbetaald door de beklaagde.

handelsfraude betreft en een beklag normaliter gaat over één aangifte, waardoor niet zonder meer sprake is van een gewoonte.

In bijna alle afwijzingen ontbraken aanwijzingen voor oplichting door gebrek aan valse naam of oplichtingsmiddel – twee belangrijke bestanddelen uit het oplichtingartikel. De redenen voor afwijzing in de beklagschriften waarin online handelsfraude (44 in totaal) werd overwogen zijn als volgt samen te vatten. In 24 beklagzaken waren er volgens het Hof niet genoeg andere aangiften voor vervolging van artikel 326e Sr. In een deel van deze beklagzaken waren bij de politie meer dan drie aangiften bekend, wat doorgaans als een gewoonte wordt aangemerkt. Echter, in deze beklagzaken billijkte het Hof alsnog de door het Openbaar Ministerie genomen beslissing om niet te vervolgen vanwege een gebrek aan capaciteit. In de rest van de zaken was sprake van een variëteit aan redenen: te laag schadebedrag, te laag aantal aangiftes, buitenlandse rekeninghouder, capaciteit, katvanger, onvoldoende aanwijzing voor artikel 326e Sr of een combinatie van redenen, inclusief een te laag aantal aangiftes. Vaak noemt het Hof dat nader onderzoek wellicht meer aanwijzingen zou kunnen opleveren voor online handelsfraude, maar dat gelet op de grote hoeveelheid aangiften in relatie tot de (beperkte) opsporingscapaciteit van politie en justitie alsnog kan worden afgezien van verder strafrechtelijk onderzoek. Er zijn dus fraudezaken met een online handels aspect waarvoor zowel artikel 326 Sr als artikel 326e Sr geen grond bieden voor strafrechtelijke vervolging. In zulke gevallen is artikel 326 Sr niet toereikend door gebrek aan valse naam of oplichtingsmiddel en artikel 326e Sr slaagt niet vanwege een gebrek aan capaciteit of gebrek aan aangiften om tot een gewoonte te komen of om voor vervolging in aanmerking te komen.
De producten waar het in deze beklagschriften om ging lopen ver uiteen, van een helm, horloge, gouden tientje, verschillende elektronica – zoals een cameralens, fietsaccu of Dyson-stofzuiger – tot een monstrans[42], auto's of vliegtickets.

Hoofdpunten

- Het Openbaar Ministerie kan beslissen om in een 326e-zaak niet over te gaan tot vervolging. Op basis van deze evaluatie is geen zicht gekregen op het totaal aantal zaken waarin hier sprake van was. In deze evaluatie zijn in elk geval 167 beschikkingen op beklag geanalyseerd. 154 klachten zijn afgewezen en in 13 zaken moest het Openbaar Ministerie toch tot vervolging overgaan. Elke beklagzaak werd aangedragen door één slachtoffer. Soms waren meer aangiftes bekend in een beklagzaak.
- Het Hof wees de klachten grotendeels af vanwege een gebrek aan opsporingscapaciteit. In de afgewezen beklagzaken waarin online handelsfraude expliciet werd genoemd is de klacht vooral afgewezen vanwege een gebrek aan andere aangiftes. De gekochte producten varieerden van elektronica, auto's en vliegtickets tot een monstrans of horloge. De schade in de toegekende beklagschriften waar online handelsfraude expliciet werd genoemd varieerde eveneens, van 50 euro tot meer dan 700 euro.

Vonnissen – artikel 326e Sr als enige feit
Uit de vonnisanalyse blijk dat artikel 326e Sr in het totaal 30 keer als feit ten laste gelegd in de 28 geanalyseerde vonnissen (beklagschriften niet meegenomen). In 8 van de 28 vonnissen (beklagschriften wederom niet meegenomen) was artikel 326e Sr het enige ten laste gelegde feit. In 2 van deze 8 uitspraken zijn in eerste aanleg en hoger

[42] Een monstrans is een versierd (Rooms-Katholiek) vaatwerk van metaal of edelmetaal waarin een geconsacreerde hostie ter verering wordt getoond of in een processie wordt vertoond (Algemeen Nederlands Woordenboek, z.d.).

beroep wel artikelen subsidiair of meer subsidiair ten laste gelegd. In 1 zaak was het 326e-feit subsidiair ten laste gelegd aan een 326-feit. De overige 5 uitspraken betroffen 4 uitspraken door de politierechter en 1 door de kinderrechter. In deze uitspraken wordt niet duidelijk om hoeveel slachtoffers het gaat noch wat voor producten frauduleus zijn verkocht. Wel is duidelijk geworden dat in vier zaken één tot vier personen zich als benadeelde partij hebben gevoegd om een schadevergoeding te vorderen. Op één na alle vorderingen werden toegekend door de rechter. In de vijfde zaak dienden vijftien benadeelde partijen een schadevordering in en voor veertien personen kende de rechter de vordering toe. Deze vonnissen worden in dit hoofdstuk verder buiten beschouwing gelaten.

Combinatie met andere feiten

Op basis van de overige 28 vonnissen, die betrekking hebben op 27 zaken, en op basis van interviews is een aantal categorieën zaken onderscheiden wat betreft het soort zaken waarin artikel 326e Sr voorkomt. Soms is artikel 326e Sr het enige feit in een zaak, maar veel vaker komt het samen voor met andere bepalingen uit het Wetboek van Strafrecht. In de zaken waarin artikel 326e Sr samen voorkomt met andere bepalingen uit het Wetboek van Strafrecht kunnen de volgende categorieën worden onderscheiden[43]:

- combinatie met fraude;
- combinatie met diefstal en misbruik van persoonsgegevens;
- combinatie met cyberfeiten;
- combinatie met strafbaarstellingen niet gerelateerd aan het 326e-feit.

Combinatie met fraude

In het grootste deel van de zaken komt online handelsfraude samen voor met andere vormen van fraude, zoals oplichting, witwassen en verduistering. In 20 van de 27 zaken is dit het geval. Oplichting en witwassen komen verreweg het vaakst voor, gevolgd door verduistering.

Combinatie met gewone oplichting

In de meeste zaken (vijftien) komt artikel 326e Sr samen voor met 'gewone' oplichting (art. 326 Sr).[44] Oplichting wordt ook vaak subsidiair ten laste gelegd aan een 326e-feit. Daarnaast is in één zaak (ECLI:NL:GHDHA:2023:1431) online handelsfraude (art. 326e Sr) subsidiair ten laste gelegd met oplichting als het primaire feit. In deze zaak sprak de rechter de verdachte vrij van beide feiten. De redenen hiervoor komen niet duidelijk naar voren in het vonnis en om deze reden zal deze zaak verder niet worden besproken.

In de komende paragrafen wordt een beeld geschetst van het soort zaken waarin 'gewone' oplichting samen voorkomt met online handelsfraude. Eerst worden de uitspraken behandeld waarin artikelen 326 en 326e Sr worden gepresenteerd als één feit. Daarna worden de 326e-uitspraken behandeld waarin artikel 326 Sr als apart feit voorkomt.

[43] De scheiding tussen categorieën is overigens niet altijd even scherp en soms overlappen deze elkaar. Echter, omwille van de analyse worden de vonnissen toch op deze manier behandeld.

[44] Op basis van artikel 326 Sr, is iemand schuldig aan oplichting wanneer hij of zij, 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 tot het teniet doen van een inschuld, met het oogmerk om zich of een ander wederrechtelijk te bevoordelen.

Gewone oplichting als subsidiair of primair feit

Vóór de inwerkingtreding van de Wet CCIII werd online handelsfraude vervolgd op basis van artikel 326 Sr, als 'gewone' oplichting (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 73). De vonnisanalyse laat zien dat artikel 326 Sr nog steeds wordt gebruikt, maar dat het in zes zaken subsidiair aan een 326e-feit ten laste is gelegd. Het is niet duidelijk geworden wat hier de precieze reden voor was. Mogelijk speelt hierbij een rol dat artikel 326 Sr voor de zekerheid werd ingezet. Een geïnterviewde medewerker van het Openbaar Ministerie vertelt dat in één van de zaken artikel 326 Sr subsidiair 'als vangnet' ten laste was gelegd, mocht artikel 326e Sr niet wettig en overtuigend bewezen kunnen worden. In de zes zaken wordt het primaire 326e-feit overigens telkens bewezen geacht. In één zaak (niet-openbaar vonnis) die het Hof behandeld heeft, was juist artikel 326e Sr subsidiair ten laste gelegd aan een 326-feit. Het subsidiaire feit werd in eerste aanleg bewezen verklaard, maar de verdachte werd in hoger beroep vrijgesproken. De reden voor de vrijspraak is niet duidelijk geworden op basis van het vonnis.

Gewone oplichting als losstaand feit

Op basis van de vonnisanalyse kunnen drie groepen zaken worden onderscheiden waarin oplichting als losstaand feit in de tenlastelegging is opgenomen. Eén groep ziet op zaken waarin artikel 326 Sr ten laste is gelegd ter vervolging van online handelsfraude met een pleegdatum van vóór de inwerkingtreding van de Wet CCIII. Dit was het geval in drie zaken (ECLI:NL:RBZWB:2024:2031, ECLI:NL:RBNNE:2020:4739 en ECLI:NL:RBZWB:2021:6062). In een andere groep gaat het om zaken waarin het 326-feit ziet op vormen van oplichting zonder enige relatie met online handelsfraude.[45] Denk hierbij bijvoorbeeld aan bankhelpdeskfraude en vriend-in-nood fraude. De laatste groep is een restcategorie, welke ziet op zaken waarin óf het 326-feit inhoudelijk niet duidelijk wordt óf sprake is van oplichting van één persoon waarvan de verdachte is vrijgesproken. In zo'n geval kan niet gesproken worden van online handelsfraude.

Van de drie zaken waarin vormen van oplichting voorkwamen die geen relatie hebben met online handelsfraude, werd het 326e-feit in twee zaken vrijgesproken.[46] In één zaak (ECLI:NL:RBNHO:2024:2824) werd de verdachte vrijgesproken omdat de rechtbank niet kon bewijzen dat de verdachte zelf de 'intellectuele dader'[47] was. Onderzoek wees noch uit dat de verdachte de advertenties op marktplaats zette, noch werd bewezen dat hij hier vanaf wist. De verdachte in deze zaak was wel degene die de bedragen, verdiend met internetoplichting, ontving op zijn bankrekening. In deze zaak ging het om online handelsfraude via Marktplaats en Facebook Marketplace waarop producten zoals een Dyson airwrap, iPhones, speakers, Playstations, een videokaart en een iPad werden aangeboden. In de andere zaak (niet-openbaar vonnis) kwam artikel 326e Sr samen voor met het helen van gegevens (art. 139g Sr), met computervredebreuk (art. 138ab Sr), met het voorhanden hebben van technische hulpmiddelen voor het plegen van misdrijven (art. 139d Sr) en met diefstal. In deze zaak werd het onderdeel dat ziet op *beroep of gewoonte* uit artikel 326e Sr niet bewezen verklaard. Het ging hier om eenmalig aanbieden waarbij een klein aantal slachtoffers werd gemaakt binnen een tijdsbestek van een paar dagen. In de derde zaak (ECLI:NL:RBOBR:2022:565), waarin online handelsfraude wel werd bewezen, ging het om online handelsfraude via verschillende platformen, zoals Marktplaats,

[45] ECLI:NL:RBOBR:2022:565, ECLI:NL:RBNHO:2024:2824 en niet-openbaar vonnis.
[46] Hier gaat het om een niet-openbaar vonnis en ECLI:NL:RBNHO:2024:2824.
[47] Met 'intellectuele dader' wordt de daadwerkelijke dader bedoeld. Vanwege het feit dat online handelsfraude online gebeurt, is het voor de opsporing in sommige gevallen moeilijk om de eigenlijke dader te identificeren, omdat namen en bankrekeningen van andere mensen kunnen worden gebruikt.

Vinted, GSM-discount en Facebook. Deze zaak telde negen slachtoffers in de tenlastelegging en acht in de bewezenverklaring. Het ging hier om uiteenlopende producten, waaronder een tuinset, vloeistoffen voor e-sigaretten, hamburgerpersen, telefoons, trainingspakken en Uggs.

In de andere groep zaken (ECLI:NL:RBZWB:2024:2031, ECLI:NL:RBNNE:2020:4739 en ECLI:NL:RBZWB:2021:6062), waarin artikel 326 Sr naast artikel 326e Sr ten laste werd gelegd ter vervolging van online handelsfraude gepleegd vóór de Wet CCIII, ging het in alle drie de gevallen over Marktplaatsoplichting waarvan in één geval ook om oplichting via Facebook Marketplace. In alle zaken kwamen de 326- en 326e-feiten vrijwel geheel met elkaar overeen.

In de eerste zaak (ECLI:NL:RBZWB:2024:2031) bood de verdachte goederen aan op Marktplaats, ontving hij betalingen voor de aangeboden goederen, maar leverde deze goederen niet. In deze zaak werden verschillende soorten elektronica aangeboden, onder meer Fitbits, fietscomputers, speakers, e-readers en (sport)horloges. Bij beide feiten werd subsidiair verduistering (art. 321 Sr) ten laste gelegd. Zowel artikel 326 Sr (gepleegde online handelsfraude vóór de inwerkingtreding van de Wet CCIII) als artikel 326e Sr (gepleegde online handelsfraude na inwerkingtreding Wet CCIII) zijn in deze zaak bewezen verklaard.

In de tweede zaak (ECLI:NL:RBNNE:2020:4739[48]) kwamen online handelsfraude en oplichting samen voor met misbruik van identificerende persoonsgegevens (art. 231b Sr), schuldwitwassen (art. 420quater Sr) en diefstal (art. 311 Sr). Deze zaak draaide om een verdachte die advertenties zocht waarin bepaalde producten werden gevraagd. Daarna deed de verdachte zich voor als iemand die in het bezit was van de gezochte producten. Ook plaatste de verdachte zelf advertenties van producten die de verdachte niet bezat. Het ging om producten zoals spelcomputers (Playstation en Nintendo Switch), opblaasbare jacuzzi's, fotocamera's en tv-ontvangers.

In de derde zaak (ECLI:NL:RBZWB:2021:6062) stond de verdachte naast online handelsfraude terecht voor misbruik van persoonsgegevens (art. 231b Sr), oplichting (art. 326 Sr), computervredebreuk (art. 138ab Sr), onbruikbaar maken van gegevens (art. 350a Sr) en gewoontewitwassen (art. 420ter Sr). Al deze feiten werden bewezenverklaard door de rechtbank. Beide oplichtingsfeiten (artt. 326 en 326e Sr) kwamen op hetzelfde neer: het ging om internetoplichting van vóór de inwerkingtreding van de Wet CCIII en erna. De verdachte maakte zich schuldig aan de feiten in een aaneengesloten periode van meerdere jaren, waarin hij producten zoals hogedrukreinigers, mobiele airco's, opvouwbare zwembaden, jacuzzi's, airfryers, legotreinen en speakers aanbood en verkocht zonder te leveren. In deze zaak ging het om 'grootschalige' handelsfraude, gepleegd gedurende een 'lange periode' met een groot aantal slachtoffers, aldus het vonnis en de inhoudsindicatie bij het vonnis. In het vonnis wordt niet genoemd hoeveel slachtoffers zijn gemaakt in deze zaak. Wel wordt genoemd dat de verdachte ruim twee jaar mensen oplichtte. Hij gebruikte hiervoor reeds bestaande namen van onder meer ondernemingen, en gebruikte bankrekeningen op naam van anderen.

In de laatste groep met vier zaken ging het over twee uitspraken van de meervoudige kamer (ECLI:NL:RBNNE:2022:5570 en ECLI:NL:RBZWB:2022:3340) en twee zaken

[48] Dit ECLI-nummer betreft de uitspraak in eerste aanleg. Er is in deze zaak ook een hoger beroep geweest. Hetgeen in hoger beroep besproken is, heeft geen invloed op de strafbaarheid van de (internet)oplichtingsfeiten (ECLI:NL:GHARL:2022:4288).

behandeld door een politierechter. In de zaken die de meervoudige kamer behandeld heeft, werd het 326-feit in beide gevallen niet bewezen verklaard. Het ging hier telkens om de oplichting van maar één persoon. In beide zaken werd ook onder andere een vorm van witwassen bewezen verklaard. Deze zaken worden later besproken. Verder is in de twee politierechterzaken onduidelijk gebleven of de 326-feiten soortgelijk zijn aan artikel 326e Sr. In de vonnissen van de politierechter ging het om 'gewone' oplichting met een pleegperiode die lag vóór de inwerkingtreding van de Wet CCIII.

Hoofdpunten

- Naast de beklagzaken zijn 30 vonnissen geanalyseerd, die betrekking hadden op 28 zaken. In het merendeel van de zaken komt online handelsfraude samen voor met andere strafbare feiten in de tenlastelegging. In 8 van de 28 zaken die strafrechtelijk zijn vervolgd was artikel 326e Sr het enige feit dat ten laste was gelegd. In deze zaken is niet duidelijk geworden om wat voor producten of om hoeveel slachtoffers het ging.
- Uit de interviews en de vonnisanalyse blijkt dat in de meeste gevallen van online handelsfraude geen sprake was van 'echte grootschaligheid', ook al heeft de wetgever artikel 326e Sr geïntroduceerd om de vervolging van die vorm van online handelsfraude mogelijk te maken.
- Online handelsfraude komt verreweg het meest voor met andere vormen van fraude. 'Gewone' oplichting (art. 326 Sr) is de vorm van fraude waarmee online handelsfraude het vaakst voorkomt. Er zijn zowel zaken waarin de artikelen 326 en 326e Sr worden gepresenteerd als één feit, maar ook zaken waarin artikel 326 Sr als apart feit voorkomt. Die laatste categorie is weer onder te verdelen in drie subcategorieën, namelijk: 1) een categorie waarin artikel 326 Sr ziet op online handelsfraude gepleegd vóór de Wet CCIII; 2) een categorie waarin de oplichting ziet op andere vormen van oplichting dan online handelsfraude; en 3) een categorie waarin een duidelijke omschrijving van het oplichtingsfeit ontbreekt.
- In één zaak ging het volgens de rechtsbank expliciet om 'grootschalige' en langdurige online handelsfraude.
- De online handelsfraude was vooral gericht op speelgoed en verscheidene soorten elektronica.

Combinatie met witwassen

In tien zaken kwam online handelsfraude samen voor met witwassen. Meerdere vormen van witwassen kwamen naar voren. Het basisfeit witwassen, strafbaar gesteld in artikel 420bis Sr, kwam vijf keer voor. Een gewoonte maken van witwassen, artikel 420ter Sr, werd drie keer ten laste gelegd. Schuldwitwassen, artikel 420quater Sr, is twee keer ten laste gelegd, waarvan in één zaak als 'meer subsidiair' feit.[49] In bijna alle gevallen (negen) bestond een directe link met een 326e-feit en viel het witgewassen geld deels of geheel te herleiden tot het verdiende geld met de online handelsfraude. Van deze negen zaken, is in acht zaken witwassen ten laste gelegd als apart feit. In vijf zaken was witwassen het enige feit dat voorkwam naast artikel 326e Sr, en in drie zaken kwam artikel 326e Sr niet alleen voor met witwassen maar ook met andere feiten. In één uitspraak (ECLI:NL:RBOBR:2022:565) was witwassen (art. 420bis Sr dan wel art. 420quater Sr) niet gerelateerd aan online handelsfraude. In die

[49] 'Meer subsidiair' is een juridische term die duidt op een rangorde in vorderingen of eisen in de tenlastelegging. Binnen één tenlastegelegd feit kan naast het primaire feit sprake zijn van een subsidiair feit voor het geval dat het primaire feit niet bewezen wordt verklaard. Voor de zekerheid kan ook een 'meer subsidiair' feit ten laste worden gelegd. Dat is voor het geval ook het subsidiaire feit niet bewezen kan worden verklaard.

zaak kwam witwassen voort uit een ander soort oplichting, namelijk vriend-in-nood fraude. Deze uitspraak is eerder al besproken.

Schuldwitwassen

In twee zaken kwam schuldwitwassen (art. 420quater Sr) – het verhullen of verbergen van een voorwerp, zoals geld, dan wel van de rechthebbende van een voorwerp, terwijl hij of zij redelijkerwijs moet vermoeden dat dit voorwerp wederrechtelijk verkregen is – samen voor met online handelsfraude. In één zaak (ECLI:NL:RBGEL:2023:6844) stond de verdachte terecht voor internetoplichting van twaalf personen via verschillende internetplatforms, waaronder Marktplaats, Facebook en Ebay. Deze slachtoffers dachten dat zij producten – zoals dekens, dromenvangers, een iPhone, jassen en merkkleding – kochten van de verdachte, maar kregen niks geleverd. In deze casus was sprake van een gelaagde tenlastelegging, met artikel 326e Sr als primair feit, het medeplegen van artikel 326e Sr als subsidiair feit en schuldwitwassen (art. 420quater Sr) als meer subsidiair feit. De verdachte gebruikte verschillende accountnamen en vier bankrekeningnummers om mensen op te lichten. Uit de interviews is duidelijk geworden dat dit het bepalen van de 'intellectuele dader' doorgaans bemoeilijkt (zie ook paragraaf 3.3.8). Uiteindelijk heeft de rechtbank alle accountnamen en rekeningnummers kunnen herleiden en kunnen linken aan de verdachte, waardoor artikel 326e Sr als primair feit bewezen is en de verdachte is vrijgesproken van het subsidiaire (medeplegen) en meer subsidiaire feit (art. 420quater Sr). De andere zaak (ECLI:NL:RBNNE:2020:4739) is al besproken in de paragraaf *Oplichting.*

Eenvoudig witwassen

In vier zaken kwam online handelsfraude samen voor met eenvoudig witwassen (art. 420bis Sr)[50]. Eén van de zaken (ECLI:NL:RBROT:2023:6492) betrof 'grootschalige webwinkelfraude' door middel van verschillende webshops met bijna tweehonderd slachtoffers. Van alle geanalyseerde vonnissen was deze zaak verreweg het grootst. De verdachte verkocht, gedurende lange tijd, (merk)kleding, (merk)schoenen en (merk)accessoires. In de overige zaken (ECLI:NL:RBZWB:2024:731, ECLI:NL:RBMNE:2023:95 en ECLI:NL:RBZWB:2022:3340) waarin witwassen (art. 420bis Sr) ten laste was gelegd, was het aantal slachtoffers aanzienlijk kleiner (ten minste 8, 21 of 35 slachtoffers).[51]
Eén van deze zaken (ECLI:NL:RBMNE:2023:95) kende één verdachte en in de andere twee zaken (ECLI:NL:RBZWB:2024:731 en ECLI:NL:RBZWB:2022:3340) was sprake van medeplegen. In de genoemde zaken vond de internetoplichting plaats op verschillende online handelsplatformen, met name Marktplaats en Facebook Marketplace. Het ging in deze casus om de frauduleuze verkoop van betonplaten. In een andere zaak (ECLI:NL:RBZWB:2024:731) was sprake van medeplegen omdat de

[50] Eenvoudig witwassen komt kortgezegd neer op het verhullen/verbergen/verwerven/voorhanden hebben/gebruiken/omzetten van uit misdrijf afkomstige goederen of geldbedragen. Artikel 420bis Sr lid 1 luidt als volgt:
1 Als schuldig aan witwassen wordt gestraft met gevangenisstraf van ten hoogste zes jaren of geldboete van de vijfde categorie:
a hij die van een voorwerp de werkelijke aard, de herkomst, de vindplaats, de vervreemding of de verplaatsing verbergt of verhult, dan wel verbergt of verhult wie de rechthebbende op een voorwerp is of het voorhanden heeft, terwijl hij weet dat het voorwerp – onmiddellijk of middellijk – afkomstig is uit enig misdrijf;
b hij die een voorwerp verwerft, voorhanden heeft, overdraagt of omzet of van een voorwerp gebruikmaakt, terwijl hij weet dat het voorwerp – onmiddellijk of middellijk – afkomstig is uit enig misdrijf.

[51] Hier gaat het om het aantal slachtoffers vermeld in de tenlastelegging dan wel de bewezenverklaring. Uit interviews is duidelijk geworden dat lang niet alle slachtoffers opgenomen in het politiedossier genoemd worden op de tenlastelegging. Het is om deze reden moeilijk in te schatten wat het exacte aantal slachtoffers is in een zaak.

verdachte zijn pinpas en pincode aan een collega had gegeven waardoor deze geld voor hem kon opnemen. In deze zaak was sprake van acht slachtoffers aan wie zowel goederen als diensten werden aangeboden, waaronder een iPhone en diensten zoals stucen. De verdachte gebruikte zelf het geld uit zijn oplichtingspraktijken waardoor sprake was van witwassen. De derde zaak (ECLI:NL:RBMNE:2023:95) telde eenentwintig slachtoffers in de tenlastelegging. In deze zaak ging het over de verkoop van goederen (zoals handboeien, bouwsets, diverse gereedschappen en elektronica) via Marktplaats.

Gewoontewitwassen

De drie uitspraken waarin gewoontewassen (art. 420ter Sr)[52] samen voorkwam met online handelsfraude zien op internetoplichting via Marktplaats. In de eerste zaak (ECLI:NL:RBOVE:2024:2397) was sprake van een samenwerking tussen de verdachte en onbekend gebleven mededader(s). Het Openbaar Ministerie legde hier primair medeplegen van online handelsfraude ten laste en subsidiair medeplichtigheid. De verdachte in deze zaak was niet de 'daadwerkelijke verkoper' maar werkte mee aan de oplichting door tegen vergoeding zijn bankrekening ter beschikking te stellen, waardoor hij zich tevens schuldig maakte aan gewoontewitwassen (art. 420ter Sr). Op basis van het voorgaande bepaalde de rechtbank dat sprake was van medeplichtigheid. In deze zaak ging het over de frauduleuze verkoop van virtual reality-brillen, videokaarten, speakers, zilverbaren, keukenapparatuur en drones. Vijftien keer werd aangifte gedaan tegen de verdachte. Aangevers betaalden via een betaalverzoek (waaronder Tikkie) of bankoverschrijving aan verschillende bankrekeningnummers van drie verschillende banken die op naam stonden van de verdachte.

In de tweede zaak (ECLI:NL:RBNNE:2022:5570) werd geen gebruikgemaakt van iemand die zijn bankrekening beschikbaar stelde, maar werd middels gestolen ID-kaarten online handelsfraude gepleegd. In deze zaak kwam 326e Sr samen voor met computervredebreuk (art. 138ab Sr), misbruik van biometrische persoonsgegevens (art. 231a Sr) en gewoontewitwassen (art. 420ter Sr). De verdachte stal twee identiteitskaarten van hoogbejaarde personen. Vervolgens gebruikte de verdachte deze gegevens om bankrekeningen te openen zonder dat de twee slachtoffers hiervan wisten. Deze rekeningen zijn gebruikt om minstens vijftien personen op te lichten door het verkopen maar niet leveren van opblaasbare jacuzzi's, iPhones en spelcomputers.

In de derde zaak (ECLI:NL:RBZWB:2021:6062) – een zaak tevens besproken in de paragraaf *Combinatie met Oplichting* – was ook sprake van computervredebreuk, misbruik van (identificerende) persoonsgegevens (art. 231b Sr) en gewoontewitwassen, al ging hier geen diefstal van biometrische persoonsgegevens (zoals ID-kaarten) vooraf aan de computervredebreuk. In plaats daarvan was sprake van *phishing* van inloggegevens en wachtwoorden. De verdachte en zijn mededaders pleegden computervredebreuk in de online marktplaatsomgeving met inloggegevens die zij door *phishing* hadden verkregen. De gepleegde computervredebeuk leverde tevens een 350a-feit op (onbruikbaar maken van gegevens). Gewoontewassen kwam in de laatste twee zaken voort uit de constatering van de rechtbank dat de verdiende geldbedragen telkens zijn witgewassen.

[52] Artikel 420ter Sr luidt:
1 Hij die van het plegen van witwassen een gewoonte maakt, wordt gestraft met gevangenisstraf van ten hoogste acht jaren of geldboete van de vijfde categorie.
2 Met dezelfde straf wordt gestraft hij die zich schuldig maakt aan witwassen in de uitoefening van zijn beroep of bedrijf.

Hoofdpunten

- In tien zaken kwam online handelsfraude samen voor met een vorm van witwassen. In veel gevallen werd het geld, verdiend met online handelsfraude, uitgegeven of doorgesluisd.
- In deze zaken werden zowel goederen als diensten aangeboden, waaronder (merk)kleding, (merk)schoenen, (merk)accessoires, zilverbaren, dekens, dromenvangers, handboeien, gereedschappen, bouwmiddelen, elektronica en diensten als stuken.
- In veel zaken werden meerdere online accounts en bankrekeningen gebruikt om mensen op te lichten. Soms waren dit bankrekeningen op naam van vrienden of familie en soms werden bankrekeningen geopend met gestolen identiteitsgegevens.
- In twee zaken werd in het vonnis expliciet gesproken over 'grootschalige' online handelsfraude: in één zaak was sprake van meer dan 200 slachtoffers en in één zaak waren 35 personen opgenomen in de tenlastelegging. De overige zaken kenden een aanzienlijk kleiner aantal slachtoffers: tussen de 8 en 21.

Combinatie met verduistering (art. 321 Sr)

In vijf zaken kwam verduistering[53] samen voor met online handelsfraude. In vier van de vijf zaken was verduistering enkel subsidiair tenlastegelegd en niet bewezen. In twee van de vijf zaken had verduistering niets te maken met online handelsfraude. Het betrof één zaak (ECLI:NL:RBOBR:2022:565) waarin verduistering als op zichzelf staand feit ten laste was gelegd en één zaak (ECLI:NL:RBGEL:2023:6127) waarin verduistering subsidiair ten laste was gelegd aan diefstal. De eerste zaak ((ECLI:NL:RBOBR:2022:565) is eerder besproken en de andere zaak (ECLI:NL:RBGEL:2023:6127) wordt later besproken.

In één zaak (ECLI:NL:RBZWB:2024:2031) kwam verduistering twee keer voor als subsidiair feit in de tenlastelegging. Eenmaal in combinatie met een 326e-feit en eenmaal in combinatie met een 326-feit. Beide oplichtingsfeiten waren soortgelijk qua inhoud, namelijk oplichting via marktplaats. Deze zaak kwam eerder al aan de orde in de paragraaf *Combinatie met oplichting.* Het 326-feit had hier een pleegdatum van vóór de inwerkingtreding van de Wet CCIII. Beide oplichtingsfeiten zijn in deze zaak bewezen verklaard.

In twee andere zaken (ECLI:NL:RBZWB:2022:5028 en ECLI:NL:RBDHA:2021:11586) was verduistering respectievelijk subsidiair en meer subsidiair ten laste gelegd aan een 326e-feit. In de eerste zaak (ECLI:NL:RBZWB:2022:5028) ging het om de frauduleuze verkoop van warmwatertoestellen, gasniveau-indicatoren en gasdrukregelaars. Deze producten werden aangeboden op de bedrijfswebsite van de verdachte. Uit het vonnis blijkt dat 27 aangevers via verschillende internetplatformen, zoals Google en Marktplaats, de producten kochten op de bedrijfswebsite, maar niks geleverd kregen. Het primair ten laste gelegde 326e-feit werd bewezen. In de andere zaak (ECLI:NL:RBDHA:2021:11586), met acht slachtoffers in de tenlastelegging en zes in de bewezenverklaring, was sprake van een driedelig feit, waarin ook artikel 326 Sr ten laste was gelegd als subsidiair feit. Van de drie strafbaarstellingen is het primair ten laste gelegde 326e-feit bewezen. In deze zaak ging het om verkoop van accu's, een scooter en speelgoed via Facebook. De precieze redenen waarom verduistering in deze en in andere zaken subsidiair ten laste was gelegd aan 326e-feiten zijn onduidelijk gebleven. Wel komt naar voren in een interview dat verduistering en witwassen ten

[53] Bij verduistering gaat het om het wederrechtelijk toe-eigenen van een goed dat geheel of ten dele aan een ander toebehoort en wat iemand anders dan door misdrijf onder zich heeft (art. 321 Sr).

laste kunnen worden gelegd wanneer het niet zeker is of de verdachte de 'intellectuele dader' is of enkel een geldezel (zie paragraaf 4.3.8)

Combinatie met diefstal en misbruik van persoonsgegevens
In zeven zaken kwam online handelsfraude samen voor met diefstal, zoals neergelegd in de artikelen 310 Sr en 311 Sr, en/of met misbruik van persoonsgegevens, artikelen 231a en 231b Sr.[54] Het wederrechtelijk gebruikmaken van persoonsgegevens werd bewezen in totaal drie zaken en diefstal in zes zaken.
In drie zaken kwam wederrechtelijke gebruikmaking van persoonsgegevens samen voor met artikel 326e Sr (ECLI:NL:RBNNE:2020:4739, ECLI:NL:RBZWB:2021:6062 en ECLI:NL:RBNNE:2022:5570). Deze drie zaken zijn eerder al besproken. In alle zaken was sprake van een directe relatie tussen het 231b-feit en de online handelsfraude. Bij diefstal gold dit voor een deel van de zaken. In één zaak (ECLI:NL:RBNNE:2020:4739) had de diefstal (art. 311 Sr) niets te maken met online handelsfraude. In een andere zaak (ECLI:NL:RBNNE:2022:5570) was de diefstal direct gerelateerd aan het 231a-feit, omdat het ging om gestolen ID-kaarten.

In de overige vier zaken komt alleen diefstal samen voor met online handelsfraude. In deze zaken heeft de diefstal niets te maken met het 326e-feit. Twee van deze vier zaken zijn eerder besproken in de paragraaf over *oplichting*. In beide zaken (niet-openbaar vonnis; ECLI:NL:RBNHO:2024:2824) is de verdachte vrijgesproken van artikel 326e Sr. In de twee andere zaken maakte de verdachte zich zowel schuldig aan diefstal (artt. 310 Sr en 311 Sr) als aan het overtreden van de Wet Wapens en Munitie. In één van deze twee zaken (ECLI:NL:RBGEL:2023:6127) overtrad de verdachte ook de Opiumwet. In deze zaak ging het om webwinkelfraude. De verdachte verkocht producten zoals rugzakken, outdoor kleding, gasmaskers, luidsprekers en diverse gereedschappen zonder deze te leveren en maakte hiermee minstens tien slachtoffers. In de andere zaak (ECLI:NL:RBZWB:2024:803) werden oplichting (art. 326 Sr), mishandeling (art. 300 Sr), afpersing (art. 217 Sr), bedreiging van een politieagent (art. 267 Sr) en vandalisme (art. 350 Sr) bewezen. De internetoplichting betrof in deze zaak de frauduleuze verkoop van telefoons, elektronica, spelcomputers, speakers, en videokaarten op verschillende internetplatformen. In de bewezenverklaring werd gesproken over 22 slachtoffers.

Hoofdpunten

- In vijf zaken kwam verduistering samen voor met online handelsfraude. In bijna al die zaken werd verduistering als subsidiair feit ten laste gelegd. In alle gevallen waarin online handelsfraude samen voorkwam met verduistering werd het 326e-feit bewezen verklaard. In deze zaken ging het om webwinkel-, marktplaats- en Facebookfraude, waarin warmwatertoestellen, gasniveau-indicatoren, gasdrukregelaars, accu's, speelgoed en een scooter werden aangeboden. De meest omvangrijke zaak qua slachtoffers in deze categorie betrof een zaak met 27 aangevers.
- In zeven zaken stond online handelsfraude op de tenlastelegging samen met diefstal, en/of met misbruik van persoonsgegevens. In twee zaken bestond een directe relatie tussen online handelsfraude en misbruik van persoonsgegevens. Het ging om marktplaatsoplichting. Wanneer in het vonnis sprake was van diefstal, dan had dit feit doorgaans geen relatie met de gepleegde online handelsfraude. In deze zaken betrof de online handelsfraude het via verschillende internetplatformen

[54] Deze zeven zaken zijn gebaseerd op acht uitspraken, aangezien één uitspraak (ECLI:NL:GHARL:2020:4288) het hoger beroep betrof van een eerder besproken uitspraak in eerste aanleg (ECLI:NL:RBNNE:2020:4739).

'verkopen' van producten zoals elektronica, videokaarten, rugzakken, outdoor kleding, gasmaskers en gereedschappen. De grootste zaak in deze categorie betrof een zaak met 22 slachtoffers in de bewezenverklaring.

Combinatie met cyberfeiten

In drie vonnissen kwam online handelsfraude samen voor met één of meerdere cyberfeiten. Het gaat om computervredebreuk (art. 138ab Sr)[55], het helen van gegevens (art. 139g Sr), en/of het verwerven of voorhanden hebben van technische hulpmiddelen met het oogmerk tot het plegen van misdrijven (art. 139d Sr).[56] In één niet-gepubliceerd vonnis kwamen alle drie de feiten samen voor. Deze feiten hadden verder niets te maken met de online handelsfraude. Bovendien werd de verdachte vrijgesproken van artikel 326e Sr, omdat de verdachte maar één keer een product of dienst aanbood. Op basis van daarvan oordeelde de rechtbank dat het onderdeel 'beroep of gewoonte' niet bewezen kon worden. Verder werd de verdachte in deze zaak wel schuldig bevonden aan diefstal (art. 311 Sr), oplichting (art. 326 Sr) en het voorhanden hebben van computerwachtwoorden (art. 350d Sr). In deze zaak kwamen meerdere vormen van fraude samen, waaronder vriend-in-nood fraude, *phishing* en *spoofing*.[57] De overige twee zaken (ECLI:NL:RBNNE:2022:5570 en ECLI:NL:RBZWB:2021:6062) zijn eerder in dit hoofdstuk besproken. In één van die zaken (ECLI:NL:RBZWB:2021:6062) pleegden de verdachte en mededaders computervredebreuk in de online marktplaatsomgeving met inloggegevens die zij door *phishing* hadden verkregen. In deze zaak werd online handelsfraude gepleegd met de ingebroken marktplaatsaccounts. De gepleegde computervredebeuk leverde tevens een 350a-feit op (onbruikbaar maken van gegevens), omdat de verdachte en mededaders wachtwoorden wijzigden, nadat zij hadden ingebroken op de marktplaatsaccounts. In de tweede zaak (ECLI:NL:RBNNE:2022:5570) werd online handelsfraude gepleegd middels gestolen ID-kaarten. Met deze gegevens werd computervredebreuk (art. 138ab Sr) gepleegd in verschillende digitale bankomgevingen.

Combinatie met andere misdrijven

In zes zaken kwam online handelsfraude samen voor met andere misdrijven die niet eerder de revue passeerden. In alle zaken hadden de overige feiten geen link met het 326e-feit. Twee zaken behandeld door de meervoudige kamer (ECLI:NL:RBGEL:2023:6127 en ECLI:NL:RBZWB:2024:803) werden eerder al besproken. In de twee andere zaken van de meervoudige kamer (ECLI:NL:RBDHA:2021:11586 en ECLI:NL:RBZWB:2023:6656) werden naast online handelsfraude respectievelijk afdreiging (art. 318 Sr) en bedreiging (art. 285 Sr) bewezen verklaard. In beide zaken gebeurde de internetoplichting via Facebook en in de tweede zaak (ECLI:NL:RBZWB:2023:6656) ook via marktplaats, tweedehands.nl en nextdoor.nl. In het eerstgenoemde vonnis (ECLI:NL:RBDHA:2021:11586) ging het om zes slachtoffers in de bewezenverklaring en in het andere vonnis (ECLI:NL:RBZWB:2023:6656) werd gesproken over tien slachtoffers in de bewezenverklaring. In deze laatste casus kochten gedupeerden producten zoals een nagellakset, gereedschappen, Nintendospellen, spelcomputers, speakers, kleding en

[55] Computervredebreuk, strafbaar gesteld in artikel 138ab Sr, is het wederrechtelijk binnendringen in een geautomatiseerd werk of in een deel daarvan. Dit kan worden gedaan door het doorbreken van een beveiliging, door een technische ingreep, met behulp van valse signalen of valse sleutel, of door het aannemen van een valse hoedanigheid.

[56] Denk bijvoorbeeld aan het voorhanden hebben of verwerven van wachtwoorden en inloggegevens waarmee computervredebreuk kan worden gepleegd.

[57] *Spoofing* betekent dat iets of iemand een valse identiteit aanneemt door zich voor te doen als iets of iemand anders, bijvoorbeeld door een e-mail te verzenden vanuit een e-mailadres dat niet echt van de verzender is (Digital Trust Center, z.d.).

boeken. Zij kregen deze nooit geleverd. In de eerste genoemde zaak, waarin afdreiging voorkwam, ging het om de frauduleuze verkoop van accu's, een scooter en Lego. In die casus was sprake van ten minste acht slachtoffers.
In de twee andere uitspraken, gedaan door de politierechter, is zowel het slachtofferaantal onbekend gebleven als het soort producten waar het om ging. Naast online handelsfraude werd in één zaak opzetheling (art. 416 Sr) bewezen verklaard en in de andere zaak zowel oplichting (art. 326 Sr) als het overtreden van de Wet Wapens en Munitie. Ook werd in beide zaken niet duidelijk of er een relatie bestond tussen het 326e-feit en de andere feit(en) in de bewezenverklaring.

Hoofdpunten

- In drie zaken kwam online handelsfraude samen voor met één of meerdere cyberfeiten. Het ging om computervredebreuk, het helen van gegevens, en/of het verwerven of voorhanden hebben van technische hulpmiddelen met het oogmerk tot het plegen van misdrijven. In deze zaken werden middels diefstal en *phishing* gegevens verzameld om hiermee respectievelijk in te breken in digitale bankomgevingen of op Marktplaats accounts. In twee zaken zijn producten aangeboden op Marktplaatsaccounts waarop werd ingebroken.
- Online handelsfraude kwam ook samen voor met feiten die nog niet eerder genoemd zijn. Daarbij ging het bijvoorbeeld om bedreiging, afdreiging, opzetheling en overtredingen van de Wet Wapens en Munitie. In al deze zaken was er geen directe relatie tussen de ten laste gelegde online handelsfraude en de andere feiten. In deze zaken werden diverse producten aangeboden zoals nagellak sets, speelgoed, gereedschappen, spellen en spelcomputers, kleding, boeken, accu's en een scooter.

4.3.5 Slachtoffers, benadeelden en schade

In de vonnissen worden slachtofferaantallen en schadebedragen op verschillende plekken genoemd, zoals in de tenlastelegging, de bewezenverklaring, de schadevorderingen of in het oordeel van de rechtbank. Binnen één zaak komen deze aantallen en bedragen vaak niet met elkaar overeen.[58] Hierdoor is het lastig om een definitief aantal slachtoffers en definitieve omvang van de schade te noemen. Uit de vonnisanalyse blijkt in elk geval dat het aantal slachtoffers in de tenlastelegging tussen de 8 en 35 personen per zaak ligt, met een gemiddelde van afgerond 16 personen. Het aantal slachtoffers dat uiteindelijk in de bewezenverklaring wordt genoemd ligt iets lager, tussen de 6 en 27 slachtoffers, met een gemiddelde van afgerond 15 personen per zaak. Het aantal ingediende vorderingen ligt per zaak tussen de 1 en 31 vorderingen, met een gemiddelde van afgerond 9 vorderingen. Het aantal toegekende vorderingen varieert, namelijk tussen de 1 en 19 vorderingen, ook met een gemiddelde van 9 vorderingen.

[58] Hiervoor is een aantal redenen. Eén geïnterviewde werkzaam bij het Openbaar Ministerie legt uit dat alle bekende aangiften tegen een verdachte meegenomen worden in het dossier als een zaak voor de rechter verschijnt. Vervolgens kiest het Openbaar Ministerie welk aantal aangevers opgenomen wordt in de tenlastelegging, en dit aantal komt niet altijd overeen met het aantal in het dossier. Verder komt het voor dat een vonnis geen slachtoffers of schadebedragen in de tenlastelegging en de bewezenverklaring noemt. Bovendien vertelt een medewerker van het Openbaar Ministerie dat wanneer een zaak voor de rechter verschijnt, aangevers een brief krijgen met daarin de mogelijkheid om zich als benadeelde partij te voegen in het strafproces. Niet elke aangever kiest hiervoor, waardoor het aantal benadeelde partijen in veel gevallen verschilt van het aantal slachtoffers in zowel de tenlastelegging als de bewezenverklaring. Dat alles maakt dat het precieze aantal slachtoffer niet volledig duidelijk is, en afhankelijk van welk deel uit het vonnis geraadpleegd wordt. Het bepalen van het aantal slachtoffer en de schade is dus lastig te bepalen.

Het Openbaar Ministerie hanteert als uitgangspunt dat de schade van elk slachtoffer wordt vergoed (OM-richtlijnenbundel 2024). Op basis van de vonnisanalyse is in bijna alle zaken schade gevorderd. In één zaak (ECLI:NL:RBDHA:2021:11586) was dit niet het geval. De schade vermeldt in de tenlastelegging varieert tussen de 434 euro en 3.733,25 euro per zaak, met een gemiddeld schadebedrag van 2.143,43 euro. In de bewezenverklaring ligt het schadebedrag tussen de 481,75 euro en 8.205 euro, met een gemiddeld schadebedrag van 2.991,75 euro. De totale gevorderde schade ligt per zaak over het algemeen aanzienlijk hoger, met een gemiddelde van 5.096,53 euro. Hierbij bedraagt het laagste gevorderde schadebedrag 239,50 euro en de hoogste gevorderde schadebedrag 40.769,18 euro. In een paar zaken werd ook immateriële schade gevorderd. De rechtbank wees deze schade in alle gevallen af, omdat deze schade onvoldoende onderbouwd was. Enkel de schadevorderingen die gingen over direct geleden schade van de online handelsfraude werden toegekend.

Hoofdpunten

- Op basis van de vonnissen kan geen eenduidig beeld worden gegeven van het aantal slachtoffers van online handelsfraude en de geleden schade. Op verschillende plekken in het vonnis staan verschillende aantallen en bedragen genoemd. Doorgaans wordt enkel materiële schade vergoed, alle immateriële schadevorderingen werden afgewezen door de rechtbank. In de bewezenverklaring was sprake van gemiddeld vijftien slachtoffers.

4.3.6 Aanpak van online handelsfraude

Veel zaken die in voorgaande paragrafen besproken zijn, betreffen zaken die een meervoudige kamer behandeld heeft. Een groot deel van de online handelsfraude-zaken wordt echter afgedaan op andere manieren, zowel binnen als buiten het strafrecht. Om welk deel dat precies gaat is in deze evaluatie niet duidelijk geworden. Uit een klein aantal interviews komt naar voren dat online handelsfraude-zaken zich goed lenen voor deze andere manieren, omdat in de meeste gevallen van online handelsfraude geen sprake zou zijn van 'echte grootschaligheid'. In de volgende paragrafen worden deze manieren besproken, namelijk de ZSM-route en alternatieve interventies buiten het strafrecht om.

ZSM-route

Een deel van de zaken waarin sprake is van online handelsfraude wordt afgehandeld via de ZSM[59]-aanpak. Dit is doorgaans een snellere manier van afdoening dan wanneer de meervoudige kamer een zaak behandelt. De ZSM-route wordt doorgaans ingezet bij veelvoorkomende criminaliteit. De essentie van deze aanpak is dat in elke zaak maatwerk wordt geleverd zodat recht wordt gedaan aan de belangen van de dader, het slachtoffer en de maatschappij. Snelheid is hierbij belangrijk, zodat daders en slachtoffers snel weten waar zij aan toe zijn (OM, *Veelvoorkomende criminaliteit (ZSM)*). Uit een aantal interviews blijkt dat deze aanpak wordt gebruikt bij kleinere zaken van online handelsfraude. Op het precieze aantal zaken waarbij deze route wordt gekozen, hebben we helaas geen zicht op kunnen krijgen.

Via de ZSM-route kan zowel gekozen worden voor een afdoening binnen het strafrecht, zoals via de politierechter, of buiten het strafrecht. Een officier van justitie kiest in principe welke afdoening passend is op basis van de beschikbare informatie in het zaakdossier. Een geïnterviewde medewerker van het Openbaar Ministerie vertelt bijvoorbeeld dat ervoor gekozen kan worden om een zaak naar de rechtbank te sturen

[59] ZSM staat voor Zorgvuldig, Snel en op Maat.

wanneer de verdachte niet in staat is de schade terug te betalen aan de slachtoffers: indien een veroordeling plaatsvindt en een schadevergoedingsmaatregel is getroffen wordt de schade verhaald op de staat in plaats van op de verdachte. De staat verhaalt vervolgens schade op de verdachte. Deze weg kan ook worden gekozen wanneer een verdachte ontkent. Eén van de geïnterviewde officieren van justitie vertelt dat de strafrechtelijke weg binnen ZSM echter niet de norm is, gezien de schaarse zittingscapaciteit. Deze geïnterviewde officier vertelt dat enkel in het uiterste geval een zaak op zitting komt. Ook andere interviews laten zien dat alternatieve interventies, vanwege capaciteitsoverwegingen, over het algemeen de voorkeur genieten boven de strafrechtelijke afdoening van zaken van online handelsfraude. Een geïnterviewde officier vertelt hierover:

> [326e-zaken] proberen we zoveel mogelijk af te doen in onze interventie omgeving, via de ZSM, met name omdat (…) [het] heel veel laaghangend fruit is en we daar inderdaad de strafrechtketen niet al te (…) erg mee willen belasten.

Alternatieve interventies

De aanpak van online handelsfraude kan ook volledig buiten het strafrecht om plaatsvinden. De afgelopen jaren is wat betreft de aanpak van online handelsfraude ingezet op samenwerking tussen publieke en private partijen (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 75). Op basis van de interviews en verscheidene documenten is duidelijk geworden dat op dit moment ten minste drie alternatieve interventies worden ingezet binnen het Openbaar Ministerie en de politie (Intern document 1). Aan deze interventies komt geen zittingsrechter te pas. Het gaat om een waarschuwingsbrief, stopgesprek en (het toepassen van) directe aansprakelijkheid.

De waarschuwingsbrief betekent dat de politie de verdachte een waarschuwingsbrief stuurt. Deze interventie wordt voornamelijk gebruikt bij meerderjarige *first-offenders* en is gericht aan de rekeninghouder waartegen maximaal drie aangiften zijn gedaan of waarbij sprake is van een maximaal schadebedrag van 1.000 euro. Een stopgesprek betekent dat de politie langs gaat bij een verdachte. Ook deze interventie wordt ingezet bij meerderjarige *first-offenders*. Er moet dan wel sprake zijn van maximaal vijf aangiften. Deze interventie kan worden ingezet met of zonder schadevergoedingsverplichting. De voorkeur van het LMIO ligt doorgaans bij de variant met terugbetaling zodat slachtoffer genoeg worden gedaan (persoonlijke communicatie, 1-10-2025). Als de verdachte de schade terugbetaalt, krijgt hij geen strafblad (Intern document 1). De laatste alternatieve interventie, het toepassen van directe aansprakelijkheid, is een civielrechtelijke afdoening die volledig buiten het strafrecht om plaatsvindt en wordt uitgevoerd door drie private partijen: de Serviceorganisatie Directe Aansprakelijkheidstelling (SODA), de Landelijke associatie van gerechtsdeurwaarders (LAVG) of Aansprakelijkgesteld Nederland (AGN). Deze interventie vergt minimale politie-inzet en laat een civiele partij opkomen voor de belangen van slachtoffers door de schade rechtstreeks te verhalen op de dader. Bij de inzet van deze methode moet aan een aantal criteria worden voldaan (persoonlijke communicatie, 9-1-2025; intern document 1, 2025). Er dient sprake te zijn van een strafbaar feit en een verdachte die minimaal 18 jaar oud is, die niet gelabeld is als kwetsbaar[60] of voorkomt in het Centraal Curatele- en Bewindregister.[61] Bovendien moeten tegen de verdachte tussen de drie en vijf aangiften zijn gedaan. Verder mag geen sprake zijn van recidive en moet de verdachte de werkelijke dader zijn (en geen

[60] Dit label refereert naar personen die bijvoorbeeld laag verstandelijk beperkt, drugsverslaafd of dakloos zijn.
[61] In het centraal curatele- en bewindregister (CCBR) zijn mensen geregistreerd die onder curatele of bewind geplaatst zijn.

geldezel). SODA of LAVG stellen vervolgens de verdachte aansprakelijk met daarbij de mogelijkheid om over te gaan tot terugbetaling. Gebeurt dit niet, dan kan de zaak worden voorgelegd aan een civiele rechter. Bij deze interventie bepaalt de politie of er aan de eerdere criteria is voldaan en vervolgens wordt de aangever gevraagd om deel te nemen en zich te melden bij één van de partijen die de civiele aansprakelijkheidsstelling op zich neemt. In principe wordt deze interventie ingezet vanwege capaciteitsoverwegingen en vindt er geen 'opvolging' plaats. Door de inzet van 'directe aansprakelijkheid' wordt niet alleen betekenisvol gehandeld ten opzichte van het slachtoffer, zo is de geachte. Ook is het de bedoeling dat daarmee een signaal wordt afgegeven richting de verdachte, die de schade moet betalen, en dat de strafrechtketen wordt ontlast (persoonlijke communicatie, 1-10-2025).[62]

Buiten de hiervoor genoemde interventie is er nóg een directe aansprakelijkheidsstelling mogelijk waar de politie géén rol heeft. Bij deze alternatieve interventie is doorverwijzing door de politie niet noodzakelijk. Slachtoffers kunnen op eigen initiatief dan wel na verwijzing door de politie of een betaaldienstverlener zich aanmelden bij dezelfde civiele rechtsvertegenwoordigers, zoals SODA, LAVG en AGN, om via de civielrechtelijke weg hun geld terug te krijgen (Van Leuken et al., 2024). De slachtoffers kunnen dan via de Procedure Niet Bancaire Fraude (PNBF) de NAW-gegevens opvragen van de begunstigde bij hun bank.

Welke alternatieve interventie door de politie wordt voorgesteld, hangt onder andere af van het aantal aangiftes, de hoeveelheid schade en de omstandigheden van de verdachte. Een belangrijk uitganspunt is de 'genoegdoening van de slachtoffers', aldus een medewerker van het Openbaar Ministerie. In een brochure van het LMIO staat beschreven dat 'afdoeningen zoals de waarschuwingsbrief en het stopgesprek' ervoor kunnen zorgen 'dat het gedrag van de dader stopt en dat de slachtoffers de schade vergoed krijgen'.[63] Een evaluatie van een pilot 'directe aansprakelijkheid' concludeert dat directe aansprakelijkheid, als privaatrechtelijke afdoening, evenals de andere alternatieve interventies bijdraagt aan een betekenisvolle afdoening omdat zo meer zaken kunnen worden opgepakt (Hoorweg & Smallenbroek, 2022, p. 12). Bovendien ervaarde 87% van de daders (financiële) consequenties door deze interventie en 90% van de aangevers gaf aan in de toekomst opnieuw gebruik te willen maken van deze werkwijze (LMIO, 2022, p. 8-9). Een medewerker van het Openbaar Ministerie vertelt positief te zijn over directe aansprakelijkheid. Die interventie zorgt er volgende deze geïnterviewde voor dat mensen schadeloos kunnen worden gesteld. Bovendien is het volgens deze geïnterviewde 'een hele goede oplossing', omdat daarmee 'de politie, het Openbaar Ministerie en de rechtspraak worden ontzien'.

Hoofdpunten

- Een deel van de vooral kleine online handelsfraude-zaken wordt op een andere manier afgedaan dan via een behandeling in de meervoudige kamer. De ZSM-route is doorgaans een snellere manier van afdoening. Binnen deze route kan gekozen worden voor een afdoening binnen het strafrecht, maar uiteindelijk ook voor een route buiten het strafrecht om.
- De aanpak van online handelsfraude kan ook volledig buiten het strafrecht om plaatsvinden. Op dit moment wordt van ten minste drie alternatieve interventies gebruikgemaakt, namelijk: een waarschuwingsbrief, een stopgesprek en (het

[62] Ten tijde van het schrijven van dit rapport (juni 2025) wordt deze interventie toegepast binnen een pilot.
[63] Bij de waarschuwingsbrief is het terugbetalen van schade aan de aangevers geen vereiste, al wordt hier wel op aangestuurd. Dit volgt uit een intern document van de politie (Intern document 1).

toepassen van) directe aansprakelijkheid. Aan deze interventies komt geen zittingsrechter te pas.

4.3.7 Voordelen voor de opsporingspraktijk

Op basis van de vonnisanalyse en de interviews komt een aantal voordelen naar voren die artikel 326e Sr de opsporingspraktijk biedt in relatie tot de aanpak van online handelsfraude. Zo is online handelsfraude door de komst van artikel 326e Sr juridisch eenvoudiger te kwalificeren. Daarnaast is het nieuwe artikel gemakkelijker toepasbaar en duidelijker ten opzichte van artikel 326 Sr.

Eenvoudiger te kwalificeren
Een aantal geïnterviewde medewerkers van de politie en het Openbaar Ministerie zijn in het algemeen positief over de komst van de strafbaarstelling online handelsfraude, omdat artikel 326e Sr de aanpak en vervolging van alle vormen van online handelsfraude mogelijk maakt en vergemakkelijkt. Vóór de komst van het nieuwe artikel werd online handelsfraude soms vervolgd op basis van artikel 326 Sr. Het oplichtingsartikel wordt echter ervaren als ingewikkeld. Dit is bijvoorbeeld het geval wanneer het gaat om delictsbestanddelen die moeilijk te kwalificeren zijn bij online handelsfraude, zoals 'een valse naam of van een valse hoedanigheid' en 'listige kunstgrepen of een samenweefsel van verdichtsels'. Artikel 326e Sr is in dat opzicht 'makkelijker toepasbaar'.

In sommige online handelsfraude-zaken is geen sprake van een 'valse naam of van een valse hoedanigheid', bijvoorbeeld wanneer een verdachte een eigen naam gebruikt. Dit kan de vervolging van online handelsfraude op basis van oplichting onmogelijk maken. Een voorbeeld van zo'n zaak, waarin de verdachte zijn eigen naam gebruikte, was een zaak waarin de verdachte veelvuldig kleding, schoenen en accessoires verkocht via een webshop (ECLI:NL:RBROT:2023:6492). Deze zaak had meer dan 200 slachtoffers. In zulke gevallen wordt het nieuwe artikel 'noodzakelijk' geacht. Ook in andere zaken uit de vonnisanalyse volgt dat verdachten vaak (gedeeltelijk) eigen namen, telefoonnummers en/of rekeningnummers gebruiken, of gegevens gebruiken die te herleiden zijn tot de identiteit van de verdachten. Het is de vraag of het gewone oplichtingsartikel (art. 326 Sr) hier uitkomst had kunnen beiden.

Ten tweede kan het delictsbestanddeel uit artikel 326 Sr dat duidt op 'een listige kunstgreep of een samenweefsel van verdichtsels', de zogenoemde oplichtingshandeling, zorgen voor moeilijkheden in het kader van online handelsfraude. Beide zijn niet altijd duidelijk aanwezig. Eén van de geïnterviewden, werkzaam bij de politie, licht toe waarom zowel 'een valse hoedanigheid' als 'samenweefsel van verdichtsels' problematisch kunnen zijn:

> Op het moment dat je die [bestanddelen] dus niet kunt aantonen, die valsheid, want […] ik gebruik mijn eigen naam, ik gebruik mijn eigen woonadres, mijn eigen e-mailadres, mijn eigen bankrekeningnummer, mijn eigen telefoonnummer. Ik ben volledig bereikbaar en benaderbaar. Dan is dat niet strafbaar, ondanks dat ik natuurlijk één leugen heb verteld. […] Bij oplichting wordt gesteld dat er dus een opeenstapeling moet zijn van leugens [namelijk een samenweefsel van verdichtsels]. Als ik maar één leugen vertel dan is dat maar één leugen, en dan is dat niet strafbaar.

Ook in de eerdergenoemde zaak (ECLI:NL:RBROT:2023:6492) ontbrak het niet alleen aan een valse naam, ook het oplichtingmiddel was niet overduidelijk aanwezig. De verdachte leverde namelijk sporadisch via een webshop, waardoor niet gesproken kon worden van een valse webshop. Bovendien werd in deze zaak af en toe geleverd, waardoor geen sprake was van een vals voorwendsel. De nieuwe strafbaarstelling maakt het aantonen van de oplichtingshandeling, zoals beschreven in artikel 326 Sr, overbodig en zet 'het oogmerk om zonder volledige levering zich of een ander van de betaling van die goederen of diensten te verzekeren' centraal. Dit maakt artikel 326e Sr 'bewijstechnisch' gezien een 'veel eenvoudiger' artikel ten opzichte van artikel 326 Sr, aldus één van de geïnterviewde officieren van justitie.

Makkelijker toepasbaar en duidelijker
Daarnaast, zo komt uit een interview met de zojuist aangehaalde politiemedewerkers naar voren, is artikel 326e Sr efficiënter toe te passen dan artikel 326 Sr, vooral omdat dit laatste artikel voor relatief veel werk kan zorgen en lange ingewikkelde geformuleerde tenlasteleggingen vraagt. Bij online handelsfraude gaat het namelijk vaak over meerdere feiten, terwijl artikel 326 Sr, tekstueel gezien, ziet op één feit. De zojuist aangehaalde medewerker van de politie vertelt dat wanneer een verdachte mensen heeft opgelicht via online handel en er twintig keer aangifte is gedaan, het Openbaar Ministerie voor ieder slachtoffer afzonderlijk moet vaststellen wat het oplichtingsmiddel is. Dit leidt tot lange tenlasteleggingen. Met artikel 326e Sr is dit niet aan de orde vanwege het bestanddeel 'beroep of gewoonte'. Voor de kwalificatie van 'een beroep of een gewoonte', hoeft het Openbaar Ministerie enkel aan te tonen dat de verdachte mensen heeft bewogen tot afgifte van een goed, in dit geval geld, en dat de verdachte dit meerdere malen structureel heeft gedaan binnen een bepaalde periode. De constructie van de nieuwe strafbaarstelling is in dat opzicht meer werkbaar dan die van artikel 326 Sr.

Een ander voordeel voor onder de opsporingspraktijk, maar ook voor burgers, is dat het artikel duidelijkheid schept over wat online handelsfraude is en wanneer de strafbaarheid zich inzet. Een geïnterviewde officier van justitie vertelt dat artikel 326e Sr 'meer [is] toegesneden op wat er is gebeurd' 'en welk verwijt [de] verdachte wordt gemaakt'. Dat geeft volgens deze geïnterviewde duidelijkheid aan zowel de verdachte als de slachtoffers. Daarentegen ervaart een geïnterviewde advocaat artikel 326 Sr juist als een 'prettiger artikel' vanuit verdedigingsperspectief, aangezien dit artikel 'meer verdedigingsmogelijkheden' biedt in geval het gaat om een (deels) onschuldige verdachte. Deze advocaat geeft aan dat het moeilijker verdedigen is tegen verzameldelicten, zoals artikel 326e Sr, omdat 'alles op één hoop wordt gegooid'. Met artikel 326 Sr moet de oplichting per feit worden aangegeven.

Hoofdpunten
- Artikel 326e Sr biedt een aantal voordelen voor de opsporingspraktijk. Online handelsfraude is eenvoudiger te kwalificeren. Bovendien zijn er minder bestanddelen en passen deze bestanddelen goed bij de gedragingen van online handelsfraude in de praktijk.

4.3.8 Aandachtspunten

Op basis van de interviews en de vonnisanalyse kan een aantal aandachtspunten worden onderscheiden met betrekking tot de toepassing van artikel 326e Sr. Deze aandachtspunten worden in de komende paragrafen nader uitgewerkt. Allereerst wordt het delictsbestanddeel dat ziet op het maken van een 'beroep of gewoonte' besproken.

Daarna richt de aandacht zich op het delictsbestanddeel 'oogmerk'. Vervolgens wordt ingegaan op de opsporings- en vervolgingscapaciteit van de politie en het Openbaar Ministerie met betrekking tot de aanpak van online handelsfraude. Daarna wordt aandacht besteed aan de moeilijkheid om de intellectuele dader te vinden. Tot slot wordt aandacht besteed aan het thema buitenland.

Gewoonte

Online handelsfraude is strafbaar wanneer voldaan is aan een aantal delictsbestanddelen. Eén daarvan is 'een beroep of gewoonte'. Dit betekent dat de verdachte een beroep of gewoonte moet hebben gemaakt van het te koop aanbieden van een goed of een dienst en het niet leveren hiervan. Uit de memorie van toelichting blijkt dat voor 'gewoonte' is vereist 'het meermalen verrichten van gelijksoortige feiten (…) die niet slechts toevallig op elkaar volgen, maar onderling in zeker verband staan'. Dit verband moet zowel 'objectief' als 'subjectief' aanwezig zijn: een verband 'wat de aard van de feiten betreft' en een verband als het gaat om 'de psychische gerichtheid' van de dader om telkens hetzelfde soort feit te begaan (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 92). Dat sprake moet zijn van een 'gewoonte' komt terug in de geanalyseerde vonnissen. Soms wordt dat expliciet genoemd (ECLI:NL:RBOVE:2024:2397, ECLI:NL:RBMNE:2023:95, ECLI:NL:RBZWB:2022:3340 en ECLI:NL:RBZWB:2022:5028), maar in de meeste gevallen wordt echter volstaan met een vermelding van het aantal feiten/slachtoffers in een vastgestelde periode waaruit de gewoonte impliciet naar voren komt (ECLI:NL:RBZWB:2024:803, ECLI:NL:RBNNE:2020:4739, ECLI:NL:RBOBR:2022:565, ECLI:NL:RBDHA:2021:11586, ECLI:NL:RBZWB:2021:6062 en ECLI:NL:RBGEL:2023:6844).

Uit de interviews blijkt dat verschillend gedacht wordt over de vraag wanneer nu precies sprake is van een gewoonte. Enerzijds ervaren geïnterviewden geen moeilijkheden rondom het bestanddeel, anderzijds wordt onduidelijkheid ervaren over wanneer precies sprake is van een gewoonte. Een geïnterviewde medewerker van de politie vertelt dat 'net als bij flessentrekkerij' sprake is van een gewoonte wanneer minimaal drie keer hetzelfde feit is gepleegd 'in een periode van drie weken'. Dit is in lijn met de memorie van toelichting, waarin naar voren komt dat bij de formulering van artikel 326e Sr zoveel mogelijk is aangesloten 'bij de formulering van (het spiegelbeeldige) artikel 326a Sr (flessentrekkerij)'[64] (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 93). Daarnaast geeft een geïnterviewde medewerker van het Openbaar Ministerie aan dat in een zaak waarin sprake is van 'drie of vier aangiftes' het 'nog wel twijfelachtig' is of dat genoeg is voor een gewoonte. Deze geïnterviewde vertelt om die reden voor de zekerheid artikel 326 Sr subsidiair ten laste te leggen. Twee geïnterviewde medewerkers van het Openbaar Ministerie merken op dat 'het niet leveren van goederen' in combinatie met het oogmerk om zichzelf hierdoor wederrechtelijk te bevoordelen 'überhaupt' strafbaar zou moeten zijn. Een andere geïnterviewde deelt deze mening en zet vraagtekens bij de beperking van een 'beroep of gewoonte'. Volgens hem zou één keer misbruik maken van de digitale handel al moeten leiden tot straf. In een niet openbaar beoordelingskader van het Openbaar Ministerie is in ieder geval opgenomen dat minimaal sprake zou moeten zijn van een aantal aangiftes om tot vervolging over te gaan (Intern document 3).

[64] Artikel 326a Sr luidt als volgt: Hij die een beroep of een gewoonte maakt van het kopen van goederen met het oogmerk om zonder volledige betaling zich of een ander de beschikking over die goederen te verzekeren, wordt gestraft met gevangenisstraf van ten hoogste vier jaren of geldboete van de vijfde categorie.

Oogmerk
Een andere voorwaarde voor de strafbaarheid van online handelsfraude is 'het oogmerk om niet (volledig) te leveren en zichzelf of een ander van de betaling te verzekeren' (*Kamerstukken II* 2015-16, 34 372, nr. 3, p. 93). Het verkopen zonder te willen leveren wordt aangeduid als moedwillige wanprestatie. In de vonnisanalyse wordt een aantal keer geëxpliciteerd wanneer sprake is van 'oogmerk'. Een aandachtspunt dat daaruit naar voren komt is de verhouding tussen online handelsfraude en slecht ondernemerschap.

Eén vonnis in de vonnisanalyse laat zien dat het bestanddeel 'oogmerk' niet altijd gemakkelijk aan te tonen is. In deze zaak betekende dit niet alles bewezen kon worden verklaard, met als gevolg dat ook een deel van de schade niet werd toegekend. In deze zaak voerde de verdediging het verweer dat de verdachte wel een serieus bedrijf probeerde te voeren 'maar dat het hem op zeker moment boven het hoofd' groeide is. Volgens de raadsman betaalde de verdachte een leverancier in China voor de inkoop van (merk-)kleding, schoenen en accessoires. De verdachte leverde in sommige gevallen daadwerkelijk producten aan klanten. Op basis van het voorgaande betoogde de verdediging dat niet kon 'worden bewezen dat de verdachte het oogmerk heeft gehad om goederen te verkopen zonder deze te willen leveren'. De rechtbank ging mee in dit verweer in zoverre dat sprake was van reguliere handel gedurende de periode waarin de verdachte betalingen deed aan de leverancier. Voor dit deel van de ten laste gelegde periode sprak de rechter de verdachte vrij. Hierbij stelde de rechtbank dat slecht ondernemerschap kan overgaan in online handelsfraude wanneer een ondernemer die gewoonlijk goederen aanbiedt deze blijft aanbieden en verkopen terwijl hij weet dat hij niet (meer) kan leveren. De rechtbank besloot dus dat ook dat de verdachte tijdens de overige periode zich wel schuldig maakte aan online handelsfraude (ECLI:NL:RBROT:2023:6492). Eén van de geïnterviewde, werkzaam bij het Openbaar Ministerie, vraagt zich af in hoeverre sprake is van een maas in de wet: is een verdachte nog steeds strafbaar van online handelsfraude wanneer hij of zij niet of nauwelijks levert maar wel zo nu en dan een leverancier betaalt?

Hoofdpunten
- Bij het Openbaar Ministerie bestaat soms onduidelijkheid over wanneer voldaan is aan het bestanddeel 'gewoonte'. Vooral als het gaat om kleine zaken met weinig aangiften. In een deel van de vonnissen wordt soms expliciet en soms impliciet aangegeven dat sprake is van een gewoonte. In het laatste geval volgt dat uit het aantal genoemde feiten en slachtoffers.
- Het delictsbestanddeel 'oogmerk' kan lastig aan te tonen zijn. Dat bleek in één vonnis het geval, omdat sprake was van enige mate van reguliere handel. In deze zaak maakte de rechtbank onderscheid tussen slecht ondernemerschap en online handelsfraude.

Intellectuele dader
Uit de helft van de interviews komt naar voren dat opsporingsonderzoeken naar online handelsfraude vaak niet leiden naar de 'intellectuele dader'. Met intellectuele dader wordt de persoon bedoeld die verantwoordelijk is voor het online te koop aanbieden en verkopen van producten of diensten tegen betaling om deze vervolgens niet te leveren. Zoals eerder besproken ontvangt het LMIO alle aangiften en stuurt zij deze door naar de regionale politieteams met de in eerste instantie aangewezen verdachte. Alhoewel dit selectieproces van het LMIO vrijwel altijd een verdachte oplevert, is deze persoon niet altijd de dader die daadwerkelijk de advertenties op het internet plaatste. De interviews en de vonnisanalyse laten zien dat intellectuele daders op verschillende

manieren hun ware identiteit kunnen verhullen, namelijk door de inzet van een tussenpersoon of middels identiteitsfraude. Bij de inzet van een tussenpersoon is sprake van een 'geldezel' of 'katvanger' die een bankrekening ter beschikking stelt aan de intellectuele dader (vaak tegen betaling). Een geïnterviewde officier van justitie vertelt dat dit in veel gevallen personen zijn in kwetsbare posities, zoals minderjarigen of laagbegaafde personen. Deze officier van justitie, die zaken via de ZSM-route behandelt, vertelt:

> Wij hebben meestal dit soort types op zitting, want de rest komen we niet bij. We komen niet bij de echte dader. We komen bij de kwetsbare, lichtverstandelijk beperkte. De meeloper die even iets doet voor een vriend en ook wel in de gaten heeft 'dit is niet helemaal', maar zich daar niet tegen kan verweren, tegen die druk. (…) Dat irriteert mij natuurlijk mateloos, want ik wil helemaal zo'n jongen niet hebben. (…) Ik wil (…) degene [hebben die] hem hiertoe heeft aangezet.

In de vonnisanalyse komen twee zaken voorbij waarin de verdachte wordt vrijgesproken, omdat niet kan worden vastgesteld dat hij de persoon is geweest die de advertenties plaatste. In één van de zaken (ECLI:NL:RBNHO:2024:2824) volgde vrijspraak ten aanzien van artikel 326e Sr, omdat op basis van het strafdossier niet kon worden vastgesteld 'dat het de verdachte zelf is geweest die de advertenties op Marktplaats plaatste en afwikkelde en op die manier de kopers oplichtte, dan wel dat hij de wetenschap had (moeten hebben) dat een ander dit deed'. In een andere casus (ECLI:NL:RBOVE:2024:2397) werd de verdachte vrijgesproken van het medeplegen van online handelsfraude en veroordeeld voor medeplichtigheid voor het ter beschikking stellen van een bankrekening aan de werkelijke dader(s). In deze zaak was de rechtbank van oordeel dat uit het dossier onvoldoende bleek dat sprake was 'van een zodanig nauwe en bewuste samenwerking tussen de verdachte en de mededader(s)' dat kon worden gezegd 'dat verdachte de ten laste gelegde online handelsfraude tezamen en in vereniging met een ander' pleegde. In deze zaak stelde de verdachte naast zijn bankrekening ook zijn pinpas ter beschikking en werd geld gepind voor en door de onbekend gebleven dader(s).

Een tweede manier om de identiteit te verhullen is door middel van identiteitsfraude. In één van de zaken uit de vonnisanalyse was sprake van een verdachte die onder bewind stond en bankrekeningen opende op namen van anderen met gestolen persoonsgegevens (ECLI:NL:RBNNE:2020:4739). Er zijn meer zaken waarin identiteitsfraude voorafging aan online handelsfraude. Eén casus (ECLI:NL:RBNNE:2022:5570) betrof gestolen identiteitskaarten van twee bejaarde personen waarmee bankrekeningen werden geopend. Een andere casus (ECLI:NL:RBZWB:2021:6062) betrof gehackte bankrekeningen van mensen die eerder het slachtoffer werden van *phishing* en computervredebreuk. Het komt ook voor dat daders bankrekeningen openen op naam van partners, vrienden of familieleden. In de hiergenoemde zaken werd de dader overigens uiteindelijk toch gevonden en veroordeeld.

Wanneer de intellectuele dader onbekend blijft, kan de te naam gestelde van de bankrekening enkel vervolgd worden voor medeplichtigheid of voor het helen, bezitten of doorsluizen van geldbedragen verdiend met online handelsfraude. Uit interviews komt naar voren dat in dit soort gevallen de optie bestaat om primair dan wel subsidiair witwassen, opzetheling, verduistering of medeplichtigheid aan een 326e-feit ten laste te leggen. Deze andere bepalingen fungeren als 'vangnet', bijvoorbeeld wanneer een verdachte ontkent en het opsporingsonderzoek geen andere verdachte

heeft opgeleverd. Een geïnterviewde officier van justitie vertelt over een zaak waarin de verdachte werd vrijgesproken van artikel 326e Sr en in plaats daarvan werd veroordeeld voor witwassen, omdat de verdachte ontkende de advertenties te hebben geplaatst op Facebook Marketplace. Deze geïnterviewde officier van justitie weet verder niet in hoeverre de politie onderzoek heeft gedaan naar het account op Facebook Marketplace. Ook in de vonnisanalyse komt een zaak voor waarin de verdachte schuldig werd bevonden aan witwassen, namelijk schuldwitwassen, en werd vrijgesproken van artikel 326e Sr, omdat niet vastgesteld kon worden 'dat [de] verdachte de intellectuele dader is' (ECLI:NL:RBNHO:2024:2824). Ook in deze zaak is niet duidelijk geworden in hoeverre de echte dader gevonden is.

In de interviews komt een aantal andere redenen voorbij waarom het lastig is om een intellectuele dader te vervolgen. Voor het aanwijzen van een intellectuele dader zal vaak aanvullend opsporingsonderzoek nodig zijn om bij de intellectuele dader te komen. Op basis van enkele interviews komt naar voren dat er niet altijd ruimte is voor extra onderzoek als gevolg van de beschikbare capaciteit aan de kant van de politie en het Openbaar Ministerie. Dit zou een reden kunnen zijn waarom niet meer onderzoek wordt uitgevoerd dan hetgeen het LMIO normaliter doet voordat de aangiften worden gerouteerd. Bovendien, zo benadrukt één van de geïnterviewde medewerkers van het Openbaar Ministerie, kan politieonderzoek doodlopen wanneer een zaak vraagt om 'de uitvoering van officiersbevoegdheden'. Vooral in kleinere zaken zou dit aan de orde kunnen zijn, omdat deze zaken via de ZSM-route kunnen worden behandeld, waar een zaak meestal pas wordt beoordeeld door een officier van justitie of parketsecretaris als het bewijs al is vergaard. Eén van de geïnterviewde medewerkers van het Openbaar Ministerie noemt een oplossing. Deze geïnterviewde pleit voor het zetten van extra stappen aan de kant van het LMIO voordat zaken worden doorgestuurd naar de politieteams. De geïnterviewde noemt de HUB digitale criminaliteit in Oost-Nederland als voorbeeld. De HUB is een samenwerkingsverband tussen de politie en het Openbaar Ministerie waar aangiften van bijvoorbeeld bankhelpdeskfraude verder worden onderzocht om zicht te krijgen op de aard en omvang van een zaak. Op deze manier wordt zicht gekregen op tactische opsporingsmogelijkheden zodat op voorhand kan worden besloten welke zaken weinig kans van slagen hebben. Op deze manier kan capaciteit worden vrijgespeeld voor zaken met een grote maatschappelijke impact. Volgens deze geïnterviewde kan deze aanpak voorkomen dat zaken doodlopen bij de politie, als bijvoorbeeld opsporingsbevoegdheden nodig zijn die politie niet zonder een officier van justitie kan uitvoeren.

Een andere mogelijke reden voor het moeilijk kunnen vinden van de intellectuele dader komt naar voren uit een interview met een advocaat. Deze advocaat vertelt dat een online handelsplaats zoals Markplaats niet altijd in staat is om de ware dader aan te wijzen, omdat het mogelijk is om anoniem te blijven. Deze advocaat, die werd geïnterviewd naar aanleiding van een zaak waarin de verdachte (een geldezel) werd veroordeeld voor medeplichtigheid, merkt dat daders van online handelsfraude wel eens tijdelijke, anonieme of prepaid telefoonnummers en valse adressen gebruiken om hun 'identiteit af te schermen' op Marktplaats. Hij meent dat IP-adressen wellicht beter in staat zijn om de intellectuele dader aan te wijzen, omdat zo'n adres aangeeft vanaf welke plek en met welk geautomatiseerd werk de advertenties zijn geplaatst. Deze geïnterviewde advocaat erkent echter ook dat deze weg kan doodlopen, wanneer bijvoorbeeld het IP-adres wordt gebruikt van een openbare bibliotheek. Een andere mogelijke reden is dat het steeds makkelijker wordt om online rekeningen te openen. Een geïnterviewde medewerker van het Openbaar Ministerie geeft de Bunq bank als

voorbeeld, waar het eenvoudig zou zijn om 'een stuk of 15 bankrekeningen op je naam te openen'.

Er zijn overigens ook zaken waarin een artikel 126nc Sv-vordering wel voldoende is voor het opsporen van de intellectuele dader. Dit zijn vooral zaken waarbij het gaat om valse webshops. Een geïnterviewde medewerker van het Openbaar Ministerie vertelt dat elke webshop gebruikmaakt van een *Payment Service Provider* (PSP)[65]. Dit maakt de pakkans bij valse webshops 'nagenoeg 100 procent', omdat de oplichter naast een bankrekeningnummer ook een overeenkomend KvK-nummer en identiteitsbewijs moet opgeven bij de het afsluiten van het PSP-abonnement.

Hoofdpunten

- In online handelsfraude-zaken kan niet altijd de intellectuele dader worden vervolgd, omdat hun identiteit onbekend is. Met intellectuele dader wordt de persoon bedoeld die verantwoordelijk is voor het online te koop aanbieden en verkopen van producten of diensten tegen betaling om deze vervolgens niet te leveren. Er zijn twee manieren hoe deze intellectuele daders hun identiteit kunnen verhullen: 1) door het gebruikmaken van een tussenpersoon, ook wel geldezel of katvanger; 2) door identiteitsfraude.
- Wanneer de intellectuele dader niet gevonden wordt, kan dat leiden tot vrijspraak ten aanzien van artikel 326e Sr. Een mogelijke reden waarom de intellectuele dader niet gevonden wordt, is omdat het vinden hiervan vraagt om uitgebreider opsporingsonderzoek. Dat kan botsen met de beschikbare opsporings- en vervolgingscapaciteit.
- In zaken waarin het draait om een valse webshop is het vaak wel mogelijk om de intellectuele dader te vinden.

Beschikbare opsporingscapaciteit

De beschikbare opsporingscapaciteit van de politie en het Openbaar Ministerie is niet oneindig. Dat komt ook naar voren uit de interviews en de vonnisanalyse. Dit leidt ertoe dat niet alle online handelsfraude-zaken strafrechtelijk kunnen worden vervolgd. Sinds 1 juli 2024 ontvangt het LMIO alle aangiften van online handelsfraude op één centraal punt. Hoewel artikel 326e Sr de vervolging van online fraude vergemakkelijkt heeft, zijn er ook veel zaken waarin uiteindelijk geen vervolging plaatsvindt. Eén van de geïnterviewde medewerkers van het Openbaar Ministerie, tevens betrokken bij het LMIO, zegt hierover:

> Kijk, (…) met drie aangiftes heb je al een gewoonte. (…) [A]ls je dat (…) als maatstaf zou hanteren, dat zou betekenen dat je heel veel zaken zou moeten (…) vervolgen en dat kan gewoon simpelweg niet. Dus daar moeten we echt wel keuzes in maken en voorheen was die keuze relatief eenvoudig. (…) Als iemand gewoon een normale naam heeft gebruikt (…) dan kom je niet zo heel gauw toe aan de oplichtingshandeling die je dient te kwalificeren voor de 326. Dat hoeft natuurlijk met de 326e niet.

Het is in deze evaluatie niet duidelijk geworden hoeveel aangiftes met betrekking tot online handelsfraude uiteindelijk geen zaak worden. De politie en het Openbaar Ministerie beschikken over een niet-openbaar kader waarin criteria zijn geformuleerd op basis waarvan een keuze kan worden gemaakt welke zaak wel of niet wordt opgepakt. Mocht een zaak aan deze criteria voldoen, dan is het nog geen garantie dat

[65] Een *Payment Service Provider* (PSP), of betalingsverwerker, is een derde partij die digitale betalingen van klanten afhandelt voor webshops en andere ondernemingen.

de zaak wordt opgepakt, zo legt één van de geïnterviewde officieren van justitie uit. Bijvoorbeeld wanneer andere zaken 'met meer impact op de maatschappij' voorrang hebben. Over het algemeen geldt dat zaken met weinig aangiften en lage schadebedragen veelal niet strafrechtelijk worden vervolgd. In de geanalyseerde beslissingen op beklag noemt de rechter zoals eerder gezegd expliciet de beperkte opsporingscapaciteit. Bovendien wordt in één interview gesuggereerd dat ook in grote zaken vervolging uit kan blijven. Dit zou te maken hebben met de hoge werklast van dit soort zaken. Een geïnterviewde officier van justitie legt uit dat het 'ingewikkeld [is] om een strafzaak met 250 aangevers door de strafrechtsketen [heen] te krijgen'. Een andere geïnterviewde medewerker van het Openbaar Ministerie vertelt over een zaak met honderden slachtoffers. Deze geïnterviewde herkent de hoge werklast van grote zaken, omdat deze veel administratieve inzet vergen. In de vonnisanalyse is slechts sporadisch een 'grootschalige' zaak voorbij gekomen. Daarbij moet worden opgemerkt dat in de vonnissen niet altijd het daadwerkelijk aantal slachtoffers genoemd wordt.

Buitenland
Een laatste aandachtpunt met betrekking tot de toepassing van artikel 326e Sr betreft het buitenland. Wanneer een zaak op de een of andere manier een buitenlandcomponent in zich heeft, zoals een buitenlands rekeningnummer of een buitenlandse leverancier, kan dat moeilijkheden opleveren in het opsporingsonderzoek. In een eerder besproken casus (ECLI:NL:RBROT:2023:6492) uit de vonnisanalyse voerde de verdediging aan dat de verdachte een leverancier in China betaalde voor het leveren van de producten die de verdachte aan zijn klanten verkocht had. In deze zaak was het niet mogelijk contact op te nemen met de leverancier, waardoor dit punt niet geverifieerd kon worden.

Daarnaast vertelt een geïnterviewde medewerker, werkzaam bij de politie, steeds meer zaken te zien waarin slachtoffers het geld overgemaakt hebben naar buitenlandse banken en PSP's. Eerder werd al besproken dat het relatief gemakkelijk is om tot een verdachte te komen wanneer sprake is van Nederlandse bankrekeningen en valse webshops die gebruikmaken van Nederlandse PSP's. Bij buitenlandse bankrekeningen en webshops ligt dit anders. Het Openbaar Ministerie en de politie hebben geen vaste samenwerking met buitenlandse banken op dit terrein. Mocht de politie persoonsgegevens willen opvragen dan kan dat alleen met een rechtshulpverzoek. Een dergelijke procedure kost 'enorm veel tijd'. Bovendien is zo'n procedure geen garantie dat de politie uiteindelijk bij de intellectuele dader uitkomt, vanwege de eerdergenoemde redenen. Deze geïnterviewde ervaart dat zaken met buitenlandse verdachten veelal op de plank blijven liggen, puur vanwege capaciteitsoverwegingen. Bovendien wordt dit soort zaken direct naar de regionale eenheden gestuurd, omdat het LMIO geen buitenlandse rekeningen kan identificeren. Een regionale eenheid maakt vervolgens de keuze om zo'n zaak wel of niet op te pakken. Eerder constateerden Jansen en collega's dat buitenlandse daders van online handelsfraude 'vrij spel' hebben (Jansen et al., 2019, p. 13). Een mogelijke oplossing, volgens de eerder aangehaald geïnterviewde, is het creëren van een koppeling tussen de verwijzingsportalen van elk Europees land afzonderlijk. Op die manier kunnen buitenlandse rekeningnummers worden bevraagd.

Hoofdpunten
- Lang niet alle gevallen van online handelsfraude worden een zaak. Een belangrijke reden hiervoor is de bij de politie en het Openbaar Ministerie beschikbare capaciteit. Het is niet duidelijk geworden hoeveel casussen waarin sprake is van online handelsfraude uiteindelijk geen zaak worden. Er bestaan landelijke, niet-

openbare, kaders om keuzes te maken ten aanzien van het wel of niet oppakken van een zaak.
- De komst van artikel 326e Sr vereenvoudigt enerzijds de mogelijkheden ten aanzien van vervolging van online handelsfraude. Anderzijds botst deze vereenvoudiging met de beschikbare opsporingscapaciteit.
- Zaken waarin sprake is van online handelsfraude kunnen een buitenland component bevatten, bijvoorbeeld wanneer sprake zou zijn van een buitenlandse leverancier. Een buitenland component kan het lastig maken om daadwerkelijk over te gaan tot vervolging voor online handelsfraude, omdat geen zicht kan worden gekregen op de identiteit van de verdachte of omdat een rechtshulpverzoek moet worden ingediend dat relatief veel tijd kost. Als mogelijke oplossing voor zaken met een buitenlandcomponent wordt een koppeling tussen de verwijzingsportalen van elk Europees land afzonderlijk genoemd.

4.4 Tot slot

In dit hoofdstuk is duidelijk geworden op welke wijze artikel 326e Sr in de rechtspraktijk is toegepast sinds de inwerkingtreding van de Wet CCIII. Bij het Openbaar Ministerie zijn 279 zaken ingestroomd en in 91 zaken heeft de rechter een uitspraak gedaan. In een ruime meerderheid van de zaken werd de verdachte veroordeeld voor het plegen van ten minste één 326e-feit. In een grote meerderheid van de geanalyseerde vonnissen, 27 zaken, kwam online handelsfraude samen voor met andere feiten. In een groot deel van die zaken stond online handelsfraude op de tenlastelegging met andere vormen van fraude, zoals oplichting, witwassen en verduistering. Wanneer sprake was van witwassen betrof dit in bijna alle zaken het witwassen van geld verdiend met online handelsfraude. In de geanalyseerde vonnissen ging het voornamelijk om de frauduleuze verkoop van goederen, zoals elektronica, kleding en gereedschappen. Wanneer de online handelsfraude betrekking had op het aanbieden van diensten, betrof het vooral diensten in de bouw en als vervoerder. Het aantal slachtoffers op basis van de bewezenverklaring was gemiddeld vijftien slachtoffers per vonnis.

De wetgever heeft de nieuwe strafbaarstelling geïntroduceerd om online handelsfraude succesvol te kunnen vervolgen. Deze veronderstelling van de wetgever is juist gebleken. De cijfers in dit hoofdstuk laten zien dat artikel 326e Sr gebruikt kan worden om online handelsfraude (succesvol) te vervolgen. De nieuwe strafbaarstelling is duidelijker, makkelijker toepasbaar en eenvoudiger bewijsbaar gebleken in vergelijking met gewone oplichting, wat de aanpak en vervolging van online handelsfraude kan vergemakkelijken. Bovendien is artikel 326e Sr een *lex specialis*[66]*,* specifiek toegespitst op online handelsfraude, wat de kwalificatie van online handelsfraude heeft vereenvoudigd. Verder is duidelijk geworden dat (een deel van de) slachtoffers zich hebben gevoegd in een strafzaak, en wat betreft direct geleden schade is die schadevergoeding hen merendeels toegekend. Ook dat was een veronderstelling van de wetgever. De wetgever koppelde het belang van die voeging vooral aan het feit dat gewerkt zou worden met tijdelijke websites die snel uit de lucht zouden zijn gehaald. In heel veel zaken werd de fraude echter gepleegd middels bestaande online

[66] *Lex specialis* is de Latijnse benaming voor bijzondere wetgeving. Een juridisch principe dat regelt dat een bijzondere wet (een *lex specialis*) voorrang krijgt boven de algemene wetgeving (Mies, 2022). De algemene wetgeving in dit geval is artikel 326 Sr (gewone oplichting).

verkoopplatforms. Dat is een belangrijke nuancering bij de veronderstelling van de wetgever.

In dit hoofdstuk is ook duidelijk geworden dat een groot aantal online fraudezaken niet wordt vervolgd. Een belangrijke reden hiervoor is de beschikbare capaciteit bij opsporingsinstanties. Bij de introductie van artikel 326e Sr stelde de wetgever al dat niet alle zaken strafrechtelijk zouden kunnen worden opgepakt. Het nieuwe wetsartikel was om die reden bedoeld voor de aanpak van 'grootschalige online handelsfraude'. Dat laatste lijkt in de praktijk niet te gebeuren. Dit onderzoek heeft laten zien dat grootschaligheid veelal ontbreekt. Slechts in 3 van de 27 geanalyseerde zaken werd gesproken van 'grootschalige online handelsfraude'. De veronderstelling van de wetgever dat artikel 326e Sr vooral zou worden gebruikt voor grootschalige vormen van online handelsfraude is dus niet juist gebleken.

Het is in deze evaluatie niet duidelijk geworden hoe het komt dat dit soort zaken slechts sporadisch naar voren kwamen tijdens dit onderzoek. Een mogelijke verklaring hiervoor is wellicht dat het bij grootschalige vormen van online handelsfraude lastig is om bij de 'echte' dader terecht te komen. Ook omdat dit extra opsporingscapaciteit vraagt. Het kan ook zijn dat er nog geen vonnis is gewezen, omdat opsporingsonderzoeken naar dit soort fenomenen meer tijd in beslag nemen en het dus langer duurt voordat een zittingsrechter zich over de zaak buigt. Ook zou het kunnen zijn dat dergelijke vormen van online handelsfraude niet bestaan, of dat deze zich vooral in het buitenland afspelen.

Het voorgaande maakt duidelijk dat artikel 326e Sr een tegenstrijdigheid in zich heeft. Enerzijds is het artikel eenvoudiger, in vergelijking met het 'gewone' oplichtingsartikel waardoor vervolging van online handelsfraude gemakkelijker is geworden. Anderzijds is de beschikbare opsporingscapaciteit te beperkt om verdachten op basis van dit eenvoudigere artikel te vervolgen. Naast het gebrek aan capaciteit en het gebrek aan grootschaligheid is er nog een aantal aandachtspunten ten aanzien van de mogelijkheid tot vervolging op basis van artikel 326e Sr. De eerste is dat het niet altijd zou lukken de 'echte' dader te vervolgen. Daders kunnen gemakkelijk hun identiteit verhullen, bijvoorbeeld door gebruik te maken van geldezels. Een dergelijke geldezel komt nog wel op het netvlies van opsporingsinstanties, maar dat geldt niet voor het brein achter de online handelsfraude. In die zaken is het dus niet altijd mogelijk om online handelsfraude te vervolgen, een belangrijke nuancering bij de veronderstelling van de wetgever. Een tweede aandachtspunt betreft de buitenlandcomponent. Wanneer in een online handelsfraudezaak sprake is van een buitenlandcomponent, bijvoorbeeld een buitenlandse leverancier of een buitenlands rekeningnummer, is vervolging ingewikkeld, omdat het lastig is de identiteit van de verdachte te achterhalen, wederom een belangrijke nuancering bij de veronderstelling van de wetgever.

5 De ‘lokpuber’ in artikel 248e Sr en artikel 248a Sr

In dit hoofdstuk staan de aangepaste artikelen 248a en 248e Sr centraal, meer in het bijzonder de inzet van de zogenoemde ‘lokpuber’. Allereerst wordt het juridisch kader van deze wetsartikelen uiteengezet (paragraaf 5.1). Daarbij is ook aandacht voor de relatie met de Wet Seksuele Misdrijven. Sinds de inwerkingtreding van deze wet op 1 juli 2024 bestaan de artikelen 248a en 248e Sr niet meer. Wel is er nog steeds de mogelijkheid om de lokpuber te gebruiken. In deze evaluatie hebben we ons overigens op de artikelen 24a en 248e Sr gericht. Vervolgens wordt de noodzaak (volgens de wetgever) besproken, alsmede de veronderstellingen die aan de artikelen 248a en 248e Sr ten grondslag lagen (paragraaf 5.2). Daarna richt de aandacht zich op de inzet van de lokpuber in de praktijk (paragraaf 5.3). Hoe wordt door professionals binnen de strafrechtketen gekeken naar het middel, en welke ervaringen hebben zij daarmee? Zowel voordelen voor de opsporingspraktijk als aandachtspunten komen aan de orde (paragraaf 5.3.3 en 5.3.4). Het hoofdstuk sluit af met een conclusie waarin de beoogde veronderstellingen van de wetgever worden vergeleken met de toepassing in de praktijk (paragraaf 5.4).

5.1 Juridisch kader

Met de inwerkingtreding van de Wet CCIII zijn de artikelen verleiding van een minderjarige tot ontucht (art. 248a Sr) en *grooming* (art. 248e Sr) aangepast. Het nieuwe artikel 248a Sr (verleiding van een minderjarige tot ontucht) luidde als volgt:

> Hij die door giften of beloften van geld of goed, misbruik van uit feitelijke verhoudingen voortvloeiend overwicht of misleiding een persoon die de leeftijd van achttien jaren nog niet heeft bereikt of iemand die zich, al dan niet met een technisch hulpmiddel, waaronder een virtuele creatie van een persoon die de leeftijd van achttien jaren nog niet heeft bereikt, voordoet als een persoon die de leeftijd van achttien jaren nog niet heeft bereikt, opzettelijk beweegt ontuchtige handelingen te plegen of zodanige handelingen van hem te dulden, wordt gestraft met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie.

Het nieuwe artikel 248e Sr (*grooming*) stond als volgt opgenomen in het Wetboek van Strafrecht:

> Hij die door middel van een geautomatiseerd werk of met gebruikmaking van een communicatiedienst aan een persoon die de leeftijd van zestien jaren nog niet heeft bereikt of iemand die zich, al dan niet met een technisch hulpmiddel, waaronder een virtuele creatie van een persoon die de leeftijd van zestien jaren nog niet heeft bereikt, voordoet als een persoon die de leeftijd van zestien jaren nog niet heeft bereikt een ontmoeting voorstelt met het oogmerk ontuchtige handelingen met een persoon die de leeftijd van zestien jaren nog niet heeft bereikt te plegen of een afbeelding van een seksuele gedraging waarbij een persoon die de leeftijd van zestien jaren nog niet heeft bereikt is betrokken te vervaardigen, wordt, indien hij enige handeling onderneemt tot het verwezenlijken van die ontmoeting, gestraft met gevangenisstraf van ten hoogste twee jaren of een geldboete van de vierde categorie.

De belangrijkste wijziging in beide artikelen is dat de genoemde handelingen ook strafbaar zijn wanneer het slachtoffer een 'virtuele creatie van een persoon' betreft 'die zich voordoet als een persoon' die de leeftijd van 16 (art. 248e Sr) dan wel 18 jaar (art. 248a Sr) nog niet heeft bereikt. Dat biedt opsporingsinstanties de mogelijkheid een 'lokpuber' in te zetten. Hoewel niet expliciet in de memorie van toelichting opgenomen, is een lokpuber een rechercheur die zich voordoet als een minderjarige en die bezig is met een opsporingsonderzoek naar bijvoorbeeld *grooming*. Naast een politiefunctionaris kunnen ouders of een oudere broer of zus zich voordoen als een minderjarige (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 69).

In de memorie van toelichting van de Wet CCIII wordt de inzet van de lokpuber verder toegelicht. Een aantal aspecten wordt hier uitgelicht. Zo is uitlokking niet toegestaan. Dat betekent dat de lokpuber de verdachte niet mag brengen tot andere handelingen dan die waarop zijn opzet reeds tevoren was gericht: het Tallon-criterium[67]. Een politiefunctionaris zal dus 'in beginsel' de communicatie niet zelf starten (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 71). Verder heeft de Nederlandse Vereniging voor de Rechtspraak (NVvR) tijdens de consultatiefase rondom het wetsvoorstel in haar brief van 14 oktober 2014 gewaarschuwd dat de inzet van de lokpuber zich niet zou kunnen beperken tot een opsporingssituatie. Dat zou mogelijk tot allerlei burgerinitiatieven kunnen leiden om pedofielen op te sporen, zogenoemde 'pedojagers' of 'pedohunters'. In de memorie van toelichting wordt aangegeven dat het ontstaan van burgerinitiatieven niet volledig uit te sluiten is. Wanneer echter alle belangen worden gewogen, 'dient het belang van de bescherming van kinderen tegen gedrag op het internet of via communicatiemiddelen die gebruikt worden om kinderen te verleiden tot seksuele gedragingen (…) het zwaarst te wegen'. In verband hiermee zegt de wetgever toe dat het Openbaar Ministerie een 'prudent vervolgingsbeleid' zal hanteren (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 71).

5.1.1 Wet seksuele misdrijven

Een belangrijke ontwikkeling in het kader van de twee aangepaste strafbaarstellingen is de komst van de nieuwe Wet seksuele misdrijven (hierna Wsm). Dit wetsvoorstel is op 4 juli 2024 aangenomen door de Tweede Kamer en de Wsm is inmiddels in werking getreden. Het nieuwe artikel 251 Sr raakt aan één van de eerder besproken aanpassingen van het Wetboek van Strafrecht. Het is 'de rechtsopvolger' van diverse artikelen waarin het seksueel benaderen van kinderen jonger dan 16 jaar strafbaar is gesteld, waaronder *grooming* (art. 251 lid 1c Sr). Ook het seksueel corrumperen van kinderen (art. 251 lid 1b Sr) is strafbaar gesteld. Daarnaast is in dit artikel een nieuwe vorm van 'seksualiserende benadering' opgenomen, namelijk *sexchatting* (art. 251 lid 1a Sr).[68]

In het nieuwe artikel 251 Sr is niet meer opgenomen dat een lokpuber mag worden ingezet. Dit staat alleen nog vermeld in de memorie van toelichting van de Wsm. De inzet van de lokpuber is ook toegestaan bij opsporingsonderzoeken naar het corrumperen van een minderjarige (art. 251 lid 1b Sr) en naar *sexchatting* (art. 251 lid 1a Sr). Verder blijkt uit de memorie van toelichting dat bij de inzet van een lokpuber een 'uitlokkingsverbod' geldt. Daarnaast zal het optreden van

[67] Wat betreft het Tallon-criterium heeft de wetgever ervoor gekozen om geen nadere regeling voor de lokpuber op te nemen. De algemene taakstellende bepalingen van opsporingsambtenaren zoals de rechtspraak die genormeerd heeft, zouden voldoende moeten zijn. Wel wordt gekeken of het Tallon-criterium in het gemoderniseerde Wetboek van Strafvordering kan worden neergelegd als algemene bepaling van het voorbereidend onderzoek (Kamerstukken II 2015/16, 34 372, nr. 3, p. 71).

[68] *Sexchatting* betreft het indringend mondeling of schriftelijk seksueel benaderen op een wijze die schadelijk te achten is voor kinderen beneden de 16 jaar (art. 251, lid 1a Sr).

opsporingsambtenaren in dit soort zaken gebaseerd zijn op 'algemene taakstellende bepalingen' waarbij het 'instigatieverbod' gelding heeft. Het instigatieverbod, een andere term voor het uitlokkingsverbod, betekent dat opsporingsambtenaren burgers niet mogen brengen tot handelingen waarop hun opzet zich niet al richtte (Lindenberg, 2016, p. 950).[69] Ook staat in de memorie van toelichting beschreven dat niet-overheidsinstanties of burgers die lokprofielen gebruiken om een opsporingsonderzoek te assisteren niet in lijn ligt 'met het uitgangspunt van een integere en behoorlijke strafrechtspleging' (*Kamerstukken II* 2022/23, 36 223, nr. 3, p. 99).

5.2 Noodzaak en veronderstellingen

In de memorie van toelichting van de Wet CCIII wordt beschreven dat de ontwikkeling van informatietechnologie, zoals internet en mobiele telefonie, volwassenen nieuwe mogelijkheden biedt om kinderen te benaderen voor seksuele doeleinden. Bijvoorbeeld een volwassene die kinderen aanmoedigt om naakt te poseren voor een camera. Ook komt het voor dat een volwassene een minderjarige probeert te verleiden tot een ontmoeting om vervolgens seksueel misbruik te plegen (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 67-68). Aanpassing van de nieuwe strafbaarstelling moet ertoe leiden dat kinderen beter worden beschermd tegen benadering via het internet of via andere communicatiemiddelen voor seksuele doeleinden (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 69).

Vóór inwerkingtreding van de Wet CCIII waren dergelijke vormen van *grooming* al strafbaar gesteld, mede naar aanleiding van het Verdrag van de Raad van Europa inzake de bescherming tegen seksuele uitbuiting en seksueel misbruik (TRB. 2008, 58). Artikel 23 van dat Verdrag verplicht het strafbaar stellen van *grooming*.
Bij opsporingsonderzoeken naar het 'oude' artikel *grooming* werd in de opsporingspraktijk al gebruikgemaakt van een zogenoemde lokpuber: een rechercheur die zich voordoet als een kind van 16 jaar op jonger. Op het moment dat een verdachte deze lokpuber een voorstel deed tot een ontmoeting en handelingen verrichtte gericht op die ontmoeting, hield de politie de verdachte aan. Op basis van gerechtelijke uitspraken werd echter duidelijk dat in dergelijke situaties de verdachte niet veroordeeld kon worden, omdat het slachtoffer in werkelijkheid 16 jaar of ouder was (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 68). Hierdoor kon een lokpuber niet bijdragen aan bewijs en konden minderjarigen niet goed worden beschermd tegen *grooming*. Om die reden is het 'oude' wetsartikel herzien (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 69).

Dit geldt ook voor artikel 248a Sr, het verleiden van een minderjarige tot ontucht. Ook daar zou het gebruik van een lokpuber een probleem kunnen geven bij de vervolging. In de memorie van toelichting wordt het advies van het College van procureurs-generaal aangehaald. Hierin wijst het College erop dat de inzet van een lokpuber ook behulpzaam kan zijn bij opsporingsonderzoeken naar personen die verdacht worden van het verleiden van een minderjarige tot ontucht. Internet en sociale media zouden een grote rol spelen bij het binnenhalen van slachtoffers die seksueel misbruikt kunnen worden. Pooiers[70], bijvoorbeeld, doen pogingen om meisjes te verleiden zich voor een webcam uit te kleden en seksuele handelingen te verrichten. Deze beelden

[69] In relatie tot de modernisering van het Wetboek van Strafvordering is het instigatieverbod 'als regel van behoorlijkheid en integriteit (…) in de wettelijke regeling van het opsporingsonderzoek' centraal gesteld (Kamerstukken II 2022/23, 36 223, nr. 3, p. 99).

[70] In de memorie van toelichting wordt nog gesproken over de term 'loverboys'. Er is tegenwoordig meer kritiek op deze term.

worden vervolgens gebruikt om het slachtoffer onder druk te zetten om steeds opnieuw voor de camera te verschijnen of seksuele handelingen te verrichten die nog verder gaan (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 69).

Op basis van het voorgaande kan de volgende veronderstelling van de wetgever geformuleerd worden: vóór inwerkingtreding van de Wet CCIII kon informatie verzameld met behulp van de lokpuber niet worden gebruikt als bewijs in strafzaken. Dit leidde ertoe dat een verdachte niet kon worden vervolgd voor verleiding van een minderjarige of voor *grooming* als een lokpuber werd ingezet door de politie. De vernieuwde strafbaarstellingen (artt. 248a en 248e Sr) geven de opsporingspraktijk extra mogelijkheden, namelijk het inzetten van een lokpuber om bewijs te verzamelen. Dit leidt ertoe dat verdachten kunnen worden vervolgd, waardoor kinderen beter kunnen worden beschermd tegen benadering via het internet of via andere communicatiemiddelen voor seksuele doeleinden.

5.3 De lokpuber in de praktijk

In de komende paragrafen wordt het soort zaken besproken waarin gebruik is gemaakt van een lokpuber. Allereerst wordt kort toegelicht op welke manieren de lokpuber is ingezet, en bij welk type zaken. Daarop volgt een toelichting waarom de lokpuber is gebruikt in die zaken. In dit onderdeel worden ook zaken besproken waarin de lokpuber uiteindelijk niet is ingezet. Vervolgens richt de aandacht zich op de voordelen van de inzet van een lokpuber voor de opsporingspraktijk evenals enkele aandachtspunten. Het hoofdstuk besluit met een paragraaf waarin de veronderstellingen van de wetgever vergeleken worden met de praktijk.

5.3.1 Zakenanalyse

Uit de interviews en vonnisanalyse blijkt dat de lokpuber in de vorm van een politiefunctionaris die zich als een minderjarige voordeed, slechts enkele keren is ingezet.[71] Tussen maart 2019 en april 2024 zijn 92 zaken inzake artikel 248a Sr en 58 zaken inzake artikel 248e Sr ingestroomd bij de rechtbank. Van de 92 248a-zaken werd de verdachte in 76 zaken (deels) veroordeeld van artikel 248a Sr. Van de 58 248e-zaken was dat in 51 zaken het geval. Verder stroomden twee zaken in waarin beide artikelen ten laste waren gelegd. In beide zaken werd de verdachte in eerste aanleg veroordeeld voor de 248a en 248e-feiten.

Van de genoemde 248a-zaken, is van slechts één zaak bekend dat de politie een lokpuber inzette (ECLI:NL:RBROT:2021:3525). Dit betrof een zaak waarin artikel 248a Sr (verleiding van een minderjarige tot ontucht) ten laste was gelegd. In de genoemde zaak kwam de politie de verdachte op het spoor via een online advertentie op een datingwebsite, waarin werd gevraagd om een zogenoemde 'paydate' met een meisje van zestien jaar. De verdachte bood 100 euro om seksuele handelingen te verrichten en werd door de rechter schuldig bevonden aan *grooming* (art. 248a Sr) (ECLI:NL:RBOT:2021:3525). Daarnaast heeft de rechter recentelijk een uitspraak gedaan in een 248e-zaak waarin een lokpuber werd ingezet door de politie (ECLI:NL:RBZWB:2025:1759) (Van Uffelen, 2025).[72] Deze zaak valt buiten de zojuist genoemde periode van zaken die instroomde bij de rechtbank. In deze zaak dacht de

[71] Dit betekent onder andere dat uit sommige interviews relatief vaak zal worden geciteerd.
[72] Na afloop van de dataverzameling, verscheen een nieuwsbericht over een zaak waarin sprake was van *grooming* van een 15-jarige jongen, die in werkelijkheid een politiefunctionaris was.

verdachte een seksafspraak gemaakt te hebben met een 15-jarige jongen, dit bleek echter een rechercheur te zijn. Ook in deze zaak achtte de rechter de verdachte schuldig aan het tenlastegelegde feit. Verder, zo blijkt uit één van de interviews, is de lokpuber een aantal keer ingezet binnen lopende politieonderzoeken, waarbij het niet duidelijk is geworden of het om de artikelen 248a en/of 248e Sr ging. Het betrof zogenoemde 'brengzaken': zaken waarin al een aangifte gedaan was en eventueel een verdachte bekend was. Zo is naar aanleiding van een aangifte een onderzoek gestart naar een man die meisjes online onder druk zette om seks met hem te hebben. Daarnaast heeft de politie onderzoek gedaan naar een verdachte die via waarschijnlijk de chatfunctie op de Playstation contact legde met een minderjarige jongen en hem seksuele handelingen liet verrichten in ruil voor tegoed op zijn Playstationaccount.

De lokpuber is ook ingezet bij een aantal zaken waarin duidelijk was dat dit géén 248a- of 248e-zaak betrof, zo blijkt uit de vonnisanalyse en een aantal interviews. In die zaken was sprake van andere wetsartikelen, bijvoorbeeld seksueel misbruik van een minderjarige en mensenhandel. Eén van de zaken betrof seksueel misbruik van een twaalfjarig meisje. Dit meisje had mogelijk al seks gehad met de verdachte die online met haar chatcontact onderhield. De ouders deden hiervan aangifte bij de politie. Twee andere zaken betroffen mensenhandel zaken. In één zaak plaatste de politie een online advertentie van een zogenoemd minderjarige jongen die betaalde seks aanbod waarop de verdachte vervolgens reageerde. In de andere zaak (ECLI:NL:RBMNE:2021:4771) ging het om een verdachte die via een chatsite communiceerde met een politieagent die zich voordeed als een 16-jarige jongen. Deze chatgesprekken suggereerden dat de verdachte het doel had om de 16-jarige jongen bij hem thuis te laten prostitueren. De verdachte werd uiteindelijk vrijgesproken, omdat de rechtbank twijfelde of hij het daadwerkelijke doel had het plan uit te voeren.

Tot slot heeft het Team bestrijding kinderporno en kindersekstoerisme (hierna TBKK) van de Landelijke Eenheid na inwerkingtreding van de Wet CCIII een pilot gedraaid om in de praktijk te ervaren hoe de inzet van een lokpuber vormgegeven zou kunnen worden en wat de mogelijkheden zouden kunnen zijn. Binnen deze pilot werden fictieve profielen aangemaakt op een willekeurig gekozen (legaal) online platform. Gedurende een korte periode is gekeken tot welke soort reacties dit leidde. Deze pilot heeft voor zover bekend niet geleid tot een concrete zaak.

Hoofdpunten

- In vergelijking met het totaal aantal 248a en 248e-zaken waarover de rechter zich in de zittingszaal heeft gebogen (150) is de lokpuber zeer weinig ingezet. Voor zover bekend werd de lokpuber één keer ingezet in een 248a Sr-zaak (verleiding van een minderjarige). In deze zaak is de verdachte veroordeeld.
- De lokpuber werd ook ingezet in een aantal zaken waarin (mogelijk) geen sprake was van een 248a/248e-feit. In een deel van deze zaken ging het om andere wetsartikelen, onder andere mensenhandel.
- Het kinderpornoteam van de Landelijke Eenheid van de politie heeft één pilot gedraaid met betrekking tot het gebruik van de lokpuber. Hieruit is voor zover bekend geen concrete zaak voortgevloeid.

5.3.2 Redenen voor een inzet van de lokpuber

In de interviews noemen de geïnterviewden een aantal redenen voor de inzet van een lokpuber, al dan niet in het kader van de artikelen 248a en/of 248e Sr. Zo is een lokpuber in al lopende zaken gebruikt om mogelijk verlies van bewijs te voorkomen,

om een verdachte te identificeren en te lokaliseren, om het al verkregen bewijs te ondersteunen, of een combinatie van deze redenen. Wat betreft het voorkomen van mogelijk verlies van bewijs en het identificeren en lokaliseren van een verdachte geeft één van de geïnterviewde officieren van justitie een toelichting. Het betreft de eerdergenoemde zaak waarin het ging over het seksueel misbruik van een twaalfjarig meisje. In deze zaak nam een politiefunctionaris het account van het minderjarige slachtoffer over om geen argwaan te wekken bij de verdachte. Mogelijk zou deze verdachte bij het uitblijven van chatberichten van het werkelijke slachtoffer de chatgesprekken kunnen wissen, en daarmee het bewijs. Bovendien werd de lokpuber ingezet om de identiteit van de verdachte zeker te stellen, en zijn locatie te achterhalen. In een andere zaak, toegelicht door twee geïnterviewden werkzaam bij een regionale eenheid van de politie, werd de lokpuber gebruikt om de telefoon van de verdachte in beslag te nemen op het moment dat deze was ontgrendeld. Om dit te bewerkstelligen, voerde een politiefunctionaris, die zich voordeed als een minderjarige, het chatgesprek met de verdachte op het moment dat de politie zich bevond op de locatie van de verdachte.

Extra onderbouwing ten aanzien van al verkregen bewijs kan ook een reden zijn om de lokpuber te gebruiken. Eén van de geïnterviewden, waarnaar zojuist al werd verwezen en werkzaam bij een regionale eenheid van de politie, vertelt over een zaak waarin de verdachte meisjes onder druk zette tot het hebben van seks. Het meisje dat aangifte deed had de chatgesprekken gewist. De politie heeft toen een fictief account aangemaakt:

> (…) en als wij [de chatgesprekken] dan ook niet meer terug kunnen halen, ja, dan heb je dus een verhaal maar geen ondersteuning van dat verhaal. Dus je weet al, dan kan ik die jongeman ontbieden en vragen wat is er gebeurd, en als hij zegt, ik heb geen idee, dan is je onderzoek klaar. Dus wat wij toen wilden proberen is contact met hem leggen in de hoop dat hij datzelfde verhaal bij ons zou gaan ophangen, want dan heb je in ieder geval een bevestiging. En misschien is het niet als bewijsmiddel, maar wel net als plusje voor de overtuiging.

Naast bovengenoemde redenen, is de lokpuber ingezet na het aantreffen van een advertentie op een onlinedatingsite in het kader van een prostitutiecontrole.[73] Uit de advertentie was op te maken dat de makers van de advertenties graag seks wilden met een minderjarige tegen betaling, zo vertelt één van de geïnterviewde officieren van justitie.

Zoals eerder geconstateerd, is de lokpuber sinds de wijziging van artikelen 248a en 248e Sr slechts sporadisch gebruikt. Dit houdt voornamelijk verband met de (grote) hoeveelheid zaken waarover de politie en het Openbaar Ministerie zich moeten buigen, zo blijkt uit de interviews. Op dit punt wordt verder ingegaan in paragraaf 5.3.4. Een andere reden voor het niet inzetten van een lokpuber heeft te maken het feit dat het niet altijd nodig zou zijn een lokpuber in te zetten, vooral in zogenoemde ‘brengzaken’. Dat zijn zaken waarin er een aangifte of melding ligt op basis waarvan opsporingsinstanties aan de slag gaan. In dit soort zaken kan het zijn dat er al voldoende bewijs is om de verdachte aan te houden. Ook kan de inzet van de lokpuber

[73] In het interview licht de officier van justitie toe dat de politie als onderdeel van deze controles advertenties op verschillende websites bekijkt en bij nieuwe of opvallende advertenties een afspraak maakt met de prostituee. Zo kan de politie in gesprek gaan met de prostituee en beoordelen of er mogelijk sprake is van een mensenhandel situatie.

risico's met zich meebrengen. Zo zou de verdachte mogelijk door kunnen hebben dat hij met een lokpuber chat en om die reden besluiten bewijs te vernietigen.

Hoofdpunten

- Er zijn verschillende redenen voor de inzet van een lokpuber, zowel in 248a- en 248e-zaken als in andere zaken: 1) het voorkomen van verlies van mogelijk bewijs; 2) het identificeren en lokaliseren van de verdachte, ter ondersteuning van al verkregen bewijs; 3) een combinatie van deze redenen.
- De grote hoeveelheid 'brengzaken' maakt dat de keuze wordt gemaakt om de lokpuber nauwelijks in te zetten. Bovendien is het in brengzaken niet altijd nodig om de lokpuber in te zetten, omdat er al voldoende bewijs is. Ook kan het zijn dat de politie niet het risico wil lopen dat de verdachte door de inzet van een lokpuber iets doorheeft en om die reden bewijs vernietigt.

5.3.3 Voordelen voor de opsporingspraktijk

Zoals eerder gezegd zijn, voor zover bekend, twee verdachten veroordeeld, één in een 248a-zaak (ECLI:NL:RBROT:2021:3525) en één in een 248e-zaak (ECLI:NL:RBZWB:2025:1759) waarin de politie gebruik had gemaakt van een lokpuber. In dat opzicht kan de lokpuber, weliswaar tot nu toe sporadisch, behulpzaam zijn in zaken waarin sprake is van dit soort feiten.

Hoewel de lokpuber in de praktijk niet vaak is ingezet, zien verschillende geïnterviewden wel mogelijkheden met betrekking tot de inzet van een lokpuber, mits voldoende capaciteit beschikbaar is. Indien dat het geval is zou een proactieve inzet van de lokpuber een instrument kunnen zijn 'in de strijd' tegen seksueel misbruik van kinderen. Eén van de geïnterviewde officieren van justitie legt uit:

> Wat voor soort mensen doen dit soort feiten? Mensen die wel effectief bereid zijn om minderjarige kinderen te gaan gebruiken. Dus je kunt een soort van preventief wel heel veel bewerkstelligen als je die mensen aan kunt pakken. (…) als je genoeg capaciteit zou hebben, (…). En je zou specifiek geld en personen vrij [kunnen] maken binnen de politie om ook dit soort onderzoeken aan te pakken. Dan denk ik wel dat dat heel belangrijk kan zijn in de strijd tegen seksueel misbruik van kinderen.

Deze geïnterviewde geeft verder aan dat de lokpuber gebruikt zou kunnen worden om mensen in een vroeger stadium te waarschuwen en te voorkomen dat ze doorgaan met hun gedrag en een minderjarige daadwerkelijk schade toebrengen. Daarbij is het volgens deze geïnterviewde niet nodig om alle zaken strafrechtelijk af te doen. Een andere geïnterviewde, werkzaam bij de landelijke eenheid van de politie, spreekt van een meer algemene preventieve werking die de lokpuber eventueel zou kunnen hebben. Deze geïnterviewde was betrokken bij de eerdergenoemde pilot van TBKK. Eén van de veronderstellingen was dat als men zou weten dat de politie online actief is als lokpuber, zij mogelijk niet met een kind zouden gaan chatten.

Hoofdpunten

- Een voordeel voor de opsporingspraktijk van de aangepaste artikelen 248a en 248e Sr is dat verdachten kunnen worden vervolgd nadat de politie een lokpuber heeft ingezet. In 248a- en 248e-zaken is dit nog sporadisch gebeurd.
- Een ander voordeel is dat mogelijkerwijs een meer preventieve werking zou kunnen uitgaan van de inzet van de lokpuber. In dat geval is sprake van een proactieve inzet. Geïnterviewden merken op dat dan wel voldoende capaciteit beschikbaar moet zijn.

5.3.4 Aandachtspunten

In deze paragraaf wordt stilgestaan bij de uit de interviews naar voren gekomen aandachtspunten rondom de inzet van de lokpuber. Eerst wordt ingegaan op het gebrek aan beschikbare capaciteit om de lokpuber daadwerkelijk in te kunnen zetten en op de grens met uitlokking. Daarna richt de aandacht zich op de geloofwaardigheid van het lokprofiel en de beschikbaarheid van fotomateriaal. Vervolgens wordt ingegaan op het fenomeen pedojagers en het onder de aandacht brengen van het gebruik van de lokpuber binnen de politieorganisatie.

Capaciteit om de lokpuber in te zetten

De beschikbare capaciteit voor de inzet van de lokpuber vormt een belangrijk aandachtspunt. In de interviews komt naar voren dat de lokpuber vooral gezien wordt als een proactief middel, en daarmee vooral geschikt is voor zogenoemde 'haaldelicten'. Door de inzet van een lokpuber kan de politie bijvoorbeeld aanwezig zijn op online platforms waar mogelijk mensen actief op zoek zijn naar minderjarigen om te *groomen* of te verleiden tot ontucht. Op die manier kunnen zij in een vroeg stadium in beeld komen. Een dergelijke werkwijze werd gehanteerd in de eerdergenoemde pilot van TBKK, wat binnen korte tijd leidde tot een groot aantal in beeld gebrachte potentiële *groomers*. Een van de geïnterviewden, werkzaam bij de Landelijke Eenheid van de Nationale politie zegt hierover:

> Toen kwamen [we] er eigenlijk vrij snel achter dat [een lokprofiel] gewoon een enorme trigger is voor mensen. (…) We hebben in twee weken tijd denk ik 700 gesprekken gevoerd met mannen. En ik kan op 1 hand tellen hoeveel mannen tegen mij gezegd hebben, nee je bent 13, is echt te jong, gaan we niet doen. (…) Dus het werd ons vrij snel duidelijk, he wacht eventjes, dit is serieus.

Deze geïnterviewde vertelt verder dat de uitkomst van deze pilot (het grote aantal reacties) ertoe heeft geleid dat de lokpuber nadien niet meer is gebruikt. De pilot leverde in potentie veel meer zaken op dan waar capaciteit voor zou zijn.
Verder komt uit interviews naar voren dat er al voldoende 'brengzaken' zijn, waarbij, zoals gezegd, al een aangifte en een mogelijke verdachte in beeld is. De politie en het Openbaar Ministerie richten doorgaans alle capaciteit op dat soort zaken, zo geven een aantal geïnterviewden aan. Daardoor wordt die capaciteit niet gebruikt voor lokpuberzaken. Eén van de geïnterviewde officieren van justitie merkt bijvoorbeeld op niet aan de inzet van een lokpuber toe te komen, omdat er 'al zoveel zaken op de plank liggen van daadwerkelijk misbruik of daadwerkelijk verspreiden of het daadwerkelijk downloaden van kinderpornografisch materiaal'.

Naast dat het proactief gebruiken van de lokpuber arbeidsintensief is, kan het, vanwege de opsporingsfunctionarissen die benodigd zijn, lastig zijn om een verdachte aan te houden naar aanleiding van chatgesprekken die met een lokpuber zijn gevoerd.

Van tevoren weet de politie namelijk niet waar in Nederland de verdachte zich bevindt, en onder wiens verantwoordelijkheid diegene valt. Wanneer de politie meteen actie wil ondernemen, is er geen garantie dat direct capaciteit beschikbaar is in de betreffende eenheid.

Dat de beschikbare capaciteit aan andere zaken wordt besteed zorgt ervoor dat in de praktijk nog maar weinig ervaring is opgedaan met de inzet van de lokpuber. Volgens een geïnterviewde, werkzaam bij een regionale politie-eenheid, is het lastig om ervaring op te doen met de lokpuber door de drukte van 'de waan van de dag'. Het aandachtspunt van capaciteit speelt niet alleen een rol bij politie, maar ook bij het Openbaar Ministerie. Een geïnterviewde officier van justitie, die een lokpuberzaak behandelde, vertelt dat in deze zaak er in eerste instantie gekeken is naar vervolging op grond van artikel 248b Sr, het ontucht plegen met iemand die zich beschikbaar stelt voor het verrichten van seksuele handelingen met een derde tussen de leeftijd van 16 en 18 jaar tegen betaling. Uiteindelijk is echter besloten te vervolgen op grond van artikel 248a Sr. Dat daar bij aanvang van het strafrechtelijk onderzoek niet direct naar is gekeken, had onder meer te maken met het feit dat er nog maar weinig ervaring was met vervolging op grond van dit wetsartikel. In eerste instantie werd, mede vanwege het grote aantal zaken dat tegelijkertijd speelt, teruggegrepen op een artikel waarmee al veel ervaring was opgedaan.

Wat betreft de Wsm verwacht een aantal geïnterviewden een toename van (potentiële) zaken, gezien de drempel voor strafbaar gedrag in deze wet lager ligt dan bij *grooming* en verleiding van een minderjarige. Zoals in paragraaf 5.1 aangegeven wordt *sexchatten* ook strafbaar. Een groei aan (potentiële) zaken heeft gevolgen voor keuzes die gemaakt moeten worden wat betreft de inzet van middelen bij de politie en het Openbaar Ministerie. Sommige geïnterviewden vragen zich af of het wenselijk is om alle verdachten strafrechtelijk te vervolgen. Zo zou in eerste instantie gewaarschuwd kunnen worden, net als bij bijvoorbeeld *grooming*. Toch zullen er mogelijk ook verdachten tussen zitten die daadwerkelijk misbruik plegen of 'een alter ego hebben op het dark web', in de woorden van één van de geïnterviewde officieren van justitie.

Grens met uitlokking

Een aandachtspunt waar relatief veel over gesproken is in de interviews, betreft de grens met uitlokking. Tijdens het maken van de Wet CCIII is hier door de wetgever al rekening mee gehouden: in de memorie van toelichting wordt expliciet gesproken van een 'uitlokkingsverbod'. In de praktijk wordt aandacht besteed aan het voorkomen van uitlokking. Dat betekent over het algemeen dat de lokpuber zich passief op moet stellen zodat de verdachte zoveel mogelijk uit zichzelf berichten stuurt. Eén van de geïnterviewden, werkzaam bij een regionale eenheid van de politie, vertelt hier overleg over te hebben gehad met het Openbaar Ministerie, bijvoorbeeld bij het sturen van chatberichten of het kiezen van fotomateriaal voor het fictieve profiel. Een geïnterviewde officier van justitie merkt op extra scherp te zijn wanneer het over uitlokking gaat:

> Maar heel belangrijk is (…) van te voren afspraken erover maken. Dus wat ik in dit soort zaken [met risico op uitlokking] ook wel eens heb gedaan, is dat ik echt van te voren ging zitten met de politie en zeggen van nou oké, wat wil je voorstellen? En als hij of zij dan dit zegt, wat zeg je dan? Ik heb ook wel eens zaken gehad waarin ik 's avonds werd gebeld, ik ben nu aan het chatten en dit en dit en dit en vind je het goed als ik daar zo en zo op reageer. Dus gewoon echt wel dicht er bovenop zitten. Anders kan je zaak zomaar kapot gaan, als men te ver gaat.

In de praktijk kan het nog best lastig zijn om de grens met uitlokking te bewaken, zo merkt de hierboven aangehaalde medewerker van de politie op. Deze geïnterviewde vertelt over een lopend opsporingsonderzoek waarin de politie het account van een slachtoffer had overgenomen. In de chat deed de verdachte uit zichzelf geen seksuele voorstellen, waardoor de vraag rees hoe ver de politie kon gaan:

> Dus ja, je zet dat eerste stapje, dat komt natuurlijk vanuit ons initiatief inderdaad (…). We hebben dat toen met de officier besproken. Kan dat dan als we dat doen? (…) Maar (…) het blijft lastig hoor. Ook als je aan het chatten bent. Wij hebben dan gewoon de afspraak, wij reageren alleen maar op wat de ander vraagt. We stellen niks voor of doen niks. Maar toch die laatste [verdachte] met dat twaalfjarige meisje, die zat ook heel erg op, maar wat wil jij dan? En wat vind jij dan? Wij hoopten natuurlijk dat die zou zeggen, zullen we weer afspreken en weer seks hebben? (…), maar hij bleef het maar terugkaatsen naar ons, van hoe zit jij er dan in, en wat vond jij er dan van? (…). Als je dan echt net op de letter gaat zitten, dan is het echt nog wel complexer als je erin zit. [Om] [n]iet op die uitlokking te komen. Maar daar zitten wij ook altijd wel met elkaar van joh, kan dit? Hoe ver kunnen we gaan?

Niet alleen in de opsporingsonderzoeken, maar ook in rechtszaken komt de grens met uitlokking aan de orde. In de lokpuber-zaak (ECLI:NL:RBROT:2021:3525), waarbij de verdachte vervolgd werd voor verleiding van een minderjarige tot ontucht (art. 248a Sr), voerde de advocaat het verweer dat de verdachte was uitgelokt. Deze advocaat stelde dat de lokpuber de verdachte actief had benaderd en zelf seksuele handelingen had voorgesteld. De rechtbank ging hier niet in mee. Naast dat het verweer volgens de rechtbank onvoldoende onderbouwd was, beargumenteerde de rechtbank dat de verdachte met diens advertenties een jong meisje uitnodigde om te reageren. Dat de lokpuber direct aangaf 16 jaar te zijn terwijl de verdachte toch doorging met het maken van een seksafspraak, laat volgens de rechtbank zien dat de verdachte de opzet had om een minderjarige te bewegen tot het plegen van ontuchtige handelingen. Op basis hiervan had de lokpuber de verdachte 'niet uitgelokt tot meer dan waarop zijn eigen opzet van tevoren was gericht', aldus de rechtbank.

Hoofdpunten

- De politie heeft nog maar weinig ervaring opgedaan met de lokpuber, omdat de capaciteit bij zowel de politie als het Openbaar Ministerie voor andere zaken wordt benut.
- Vooral voor een proactieve inzet van de lokpuber ('haaldelicten'), die arbeidsintensief kan zijn, wordt niet gekozen, omdat er al genoeg 'brengdelicten' zijn.
- Met de komst van de Wsm verwachten enkele geïnterviewden een stijging van het aantal zedenzaken.
- Voor opsporingsfunctionarissen die werken met een lokpuber is uitlokking een belangrijk aandachtspunt.

Geloofwaardig online profiel

Meerdere geïnterviewden vertellen dat het lastig kan zijn om een geloofwaardig (online) profiel van een lokpuber te realiseren. Vooral het hebben van voldoende fotomateriaal is een aandachtspunt. Eén van de geïnterviewden, werkzaam bij een regionale eenheid van de politie, zegt:

> Maar hetgeen waar we heel erg tegenaan lopen is fotomateriaal. (…) Dat is echt een hele zoektocht geweest. Dat we hebben gekeken, is er niet iets binnen de politie. Een soort van databank met fakeprofielen die we kunnen gebruiken. (…) Dus daar zijn we eigenlijk heel erg lang mee bezig geweest en eigenlijk nog steeds mee bezig om dat voor elkaar te krijgen.

Het hebben van dit soort fotomateriaal is nodig omdat een verdachte tijdens het chatten om foto's kan vragen. Ook bij het gebruik van fotomateriaal wordt rekening gehouden met uitlokking en dat daar geen sprake van mag zijn. Zo vertelt deze geïnterviewde geen naaktmateriaal te gebruiken en een andere geïnterviewde, een officier van justitie, merkt op dat in een profieltekstje niet werd aangegeven dat het om een minderjarige ging.

Niet alleen foto's zijn een aandachtpunt. Het zo geloofwaardig en realistisch mogelijk maken van een profiel kan evengoed een uitdaging zijn. Dit heeft onder andere te maken met hoe de verschillende socialemediaplatforms zijn opgezet. Zo zijn er voor een geloofwaardig profiel op Instagram volgers nodig. Snapchat biedt de mogelijkheid voor het maken van *realtime* of live foto's. Het gebruik daarvan kan eveneens bijdragen aan de geloofwaardigheid van een profiel. Ook heeft dit platform de zogenoemde 'Snapscore[74]', die een reflectie vormt van de mate van activiteit van het account. Het is lastig om deze score kunstmatig op te hogen. Wanneer de politie zich voordoet als een relatief jong kind, dan is een lage score of weinig volgers geloofwaardiger dan wanneer het kind al wat ouder is, zo legt één van de geïnterviewden, werkzaam bij een regionale eenheid van de politie, uit. Daarnaast kan beleid van platforms het gebruik van een fictief account bemoeilijken, bijvoorbeeld wanneer extra checks worden gedaan om authenticiteit van accounts te waarborgen. Verder, en dit punt staat los van de geloofwaardigheid van een profiel, is het niet altijd mogelijk om screenshots te maken. Dit kan echter wel nodig zijn in het kader van het vastleggen van het gebruik van de lokpuber en bewijsvoering. Bij bijvoorbeeld Snapchat is dit het geval, wat de uitvoering van het opsporingsonderzoek lastiger maakt. Tot slot speelt geloofwaardigheid een rol wanneer de politie het account van een slachtoffer overneemt. Hoewel het dan gaat om een echt account met fotomateriaal en inhoud geplaatst door het slachtoffer zelf, kan het hier een aandachtspunt zijn om het slachtoffer zo goed mogelijk na te doen. Het taalgebruik mag bijvoorbeeld niet verschillen van het taalgebruik dat het betreffende slachtoffer bezigt.

Pedojagers

Pedojagers vormen eveneens één van de aandachtspunten bij de inzet van de lokpuber. Tijdens de consultatie van de Wet CCIII sprak de NVvR zich kritisch uit over het feit dat de wijziging in artikelen 248a en 248e Sr mogelijk leidde tot burgerinitiatieven om pedofielen op te sporen, zogenoemde 'pedojagers'. In de vonnisanalyse is te zien dat er in de periode maart 2019-april 2014 acht pedojager zaken zijn geweest. Dit betreft allemaal *grooming*-zaken, wat op zich niet verrassend is gezien pedojagers doorgaans een ontmoeting met en daarmee ontmaskering van de verdachte tot doel hebben. Enkele geïnterviewden, werkzaam bij de politie, merken op dat pedojagers de inzet van een lokpuber bemoeilijken. Zo kunnen verdachten voorzichtiger worden (uit angst voor een potentiële pedojager), en is het een grotere

[74] Te lezen op de website van Snapchat: 'Je Snapchat-score wordt bepaald door een supergeheime, speciale vergelijking die het aantal Snaps die je hebt verzonden en ontvangen combineert met de Verhalen die je hebt geplaatst en enkele andere factoren.' Wat is een Snapscore? – Snapchat-ondersteuning

uitdaging voor de politie om hun vertrouwen in een lokpuber te winnen. Eén van hen, werkzaam bij de Landelijke Eenheid van de Nationale Politie zegt:

> Zeker, dat hebben we ook wel gemerkt hoor. In die gesprekken is dat ook wel meerdere keren naar voren gekomen dat ze zeggen, ja maar afspreken, vind ik een beetje tricky nog. Laten we eerst even zorgen dat het vertrouwen goed is.

In datzelfde interview komt naar voren dat het voor dat vertrouwen extra belangrijk is om te beschikken over geloofwaardig foto- en beeldmateriaal, en ook dat kan, zoals gezegd, lastig zijn.

In een aantal van de zaken waarin sprake was van een pedojager, geeft de rechtbank aan dat dit niet afdoet aan de kwalijkheid van het gedrag van de verdachte dat deze heeft gechat met een fictieve minderjarige.[75] In deze zaken kwam de rechter tevens tot een veroordeling van de verdachte met een strafoplegging, wat tenminste de suggestie wekt dat het voor de strafbaarheid van *grooming* niet uitmaakt dat de pedojager de lokpuber was in plaats van een politiefunctionaris. De rechter oordeelde bijvoorbeeld in één van deze zaken dat de verdachte niet had stilgestaan bij de schade die hij zou toebrengen aan het slachtoffer, en er wordt toegelicht dat de verdachte 'uitging van een echt persoon'.[76] In twee zaken is het feit dat sprake was van een pedojager reden voor strafvermindering (ECLI:NL:RBOBR:2021:3080) en vrijspraak (ECLI:NL:GHARL:2024:3196). In de zaak waarin de rechter de verdachte vrij sprak, was het voor de rechter niet duidelijk van wie het initiatief voor de ontmoeting uitging. Ook schreef de rechter dat de pedojager onnodig druk uitoefende en dus niet uitgesloten kon worden dat de verdachte werd aangezet om tot bepaalde handelingen te komen.

Aandacht voor de inzet van de lokpuber binnen zedenteams

Enkele geïnterviewden werkzaam bij de politie ervaren dat het lastig is om de lokpuber onder de aandacht te brengen en te houden bij collega's binnen de zedenafdeling. Eén van hen vertelt:

> Interviewer: Zijn er nog andere knelpunten als je met [een lokpuber] aan de slag gaat?
>
> Geïnterviewde: Ik denk, voor onze afdeling is ook de werkdruk (…) best hoog. Dus dat ook gewoon de collega's het [inzet lokpuber] zien als extra tijd en inzet, dus dat is voor ons ook wel lastig om het een beetje onder de mensen te krijgen. Dat we zeggen, het helpt je onderzoek en het valt ook best mee. Dus wij moeten het ook goed verkopen in die zin, gebruik het gewoon en het is goed om te doen, maar dat is wel een knelpunt. Dat mensen het als last zien in plaats van als aanvulling op het onderzoek.

Toen de herziene strafbaarstellingen van artikelen 248a en 248e Sr in werking traden, werd hier volgens deze geïnterviewde vrij weinig aandacht besteed binnen de zedenafdeling wat de politie ermee zou kunnen doen, en was men er 'redelijk onbekend' mee. Wel wordt geprobeerd om die onbekendheid zoveel mogelijk weg te nemen door de inzet van digitale rechercheurs. Zij kijken mee met zaken en kunnen

[75] ECLI:NL:RBGEL:2021:4859; ECLI:NL:RBZWB:2024:4401; ECLI:NL:RBMNE:2021:1447; ECLI:NL:GHSHE:2023:716 en ECLI:NL:RBDHA:2020:11842.
[76] ECLI:NL:RBDHA:2020:11842.

de inzet van de lokpuber aandragen als een mogelijkheid binnen het opsporingsonderzoek.
Vergelijkbaar met deze ervaringen vertelt een officier van justitie dat het van belang is om de politie, met name ook de regionale eenheden, goed mee te nemen zodra er een wijziging is geweest in een wetsartikel. Daarbij kan worden ingegaan op wat de wijziging betekent voor het feitelijke werk van de politie. In de lokpuber-zaak waarbij deze officier van justitie betrokken was, had het mogelijk eerder tot een wijziging van de tenlastelegging naar artikel 248a Sr kunnen leiden:

> Interviewer: Wat heb je geleerd van deze zaak? Met betrekking tot dit artikel [art. 248a Sr]?
>
> Geïnterviewde: Dat het heel goed is om dat ook aan de voorkant, op het moment dat het opsporingsonderzoek begint, als een rechercheur begint, al bekend is, dit wetsartikel hebben we sinds een maand aangepast, het biedt hele mooie mogelijkheden om het zo en zo te gaan doen. En we lopen toch best wel vaak achter de feiten aan denk ik, in de waan van de dag. (…) Dus dat is denk ik wel wat ik hiervan heb geleerd. Als dit soort dingen komen, en als dit soort dingen gebeuren [wijzigingen wetsartikel]. Neem ook de politie daar in een vroeg stadium in mee.

Volgens een andere officier van justitie, die zich bezighoudt met de bestrijding van mensenhandel, is onvoldoende sprake van routine, en staat het gebruik van de lokpuber 'nog in de kinderschoenen'.

Hoofdpunten

- Het is ingewikkeld om een geloofwaardig (online) profiel van een lokpuber te realiseren, bijvoorbeeld vanwege een gebrek aan fotomateriaal en een actief online profiel met geloofwaardige inhoud en volgers. Ook het beleid van socialemediaplatforms en het geloofwaardig overnemen van een bestaand account kunnen het gebruik van een fictief profiel bemoeilijken.
- In de periode maart 2019-april 2024 zijn er acht rechtszaken geweest waarin sprake was van een pedojager en waarin de verdachte is veroordeeld. Dat sprake was van een pedojager kan leiden tot strafvermindering, maar dat hoeft niet.
- Het fenomeen pedojagers zou de inzet van een lokpuber kunnen bemoeilijken, omdat verdachten daardoor voorzichtiger zouden worden. Het is hierdoor niet makkelijk voor de politie om met een lokpuber het vertrouwen van een verdachte te winnen.
- Een mogelijke reden voor het niet inzetten van de lokpuber is dat opsporingsinstanties onvoldoende op de hoogte zijn van het bestaan van de gewijzigde artikelen 248a Sr en 248e Sr.

5.4 Tot slot

Met de Wet CCIII werden artikelen 248a (verleiding van een minderjarige tot ontucht) en 248e Sr (*grooming*) zodanig gewijzigd dat het mogelijk werd om verdachten te vervolgen in zaken waar een zogenoemde lokpuber is ingezet. Uit de memorie van toelichting volgt dat het hierbij vooral gaat om een politiefunctionaris die zich voordoet als minderjarige, al kunnen het ook ouders of oudere broers of zussen zijn. De vernieuwde strafbaarstelling moest ertoe leiden dat kinderen beter beschermd zouden worden tegen benadering via het internet of via andere communicatiemiddelen voor

seksuele doeleinden. In de praktijk zijn er nauwelijks zaken geweest waarin 248a en/of 248e Sr ten laste is gelegd en waarin sprake was van de inzet van een lokpuber zoals beschreven in beide artikelen. Voor zover bekend is dit in één zaak gebeurd en is de verdachte in die zaak veroordeeld voor het verleiden van een minderjarige (de lokpuber). Daarnaast heeft een pilot gedraaid om de inzet van een lokpuber te testen, maar daar is verder voor zover bekend geen zaak uit voortgekomen. Het is dus mogelijk om, in lijn met de veronderstelling van de wetgever, een verdachte te vervolgen in een zaak waarin een lokpuber is ingezet. Dit gebeurt echter zeer sporadisch. Hoewel de lokpuber in de praktijk niet vaak is ingezet zijn er in de interviews verschillende (potentiële) mogelijkheden naar voren gekomen met betrekking tot de inzet van een lokpuber, waaronder een meer proactieve inzet van de lokpuber. Een belangrijke voorwaarde hierbij is dat er voldoende capaciteit moet zijn die hieraan besteed kan worden. Een belangrijke veronderstelling van de wetgever was verder dat kinderen door de inzet van een lokpuber beter zouden kunnen worden beschermd. Op basis van deze evaluatie is niet te zeggen of kinderen inderdaad beter kunnen worden beschermd. Wel is duidelijk geworden dat de lokpuber hiervoor nauwelijks wordt benut.

Sinds de inwerkingtreding van de Wet seksuele misdrijven op 1 juli 2024 bestaan de artikelen 248a en 248e Sr niet meer. De inzet van de lokpuber blijft echter nog wel mogelijk, namelijk voor het seksueel corrumperen van een minderjarige en *sexchatting*. In dat opzicht kunnen de in dit onderzoek gesignaleerde aandachtspunten, bijvoorbeeld aandacht voor de grens met uitlokking, beperkte beschikbaarheid van capaciteit, het opstellen van een geloofwaardig profiel en bekendheid met de lokpuber binnen opsporingsorganisaties, van nut zijn voor de toepassing van de lokpuber in het kader van de nieuwe wet. Wel is het de vraag in hoeverre de lokpuber ook in het kader van deze nieuwe wet benut zal gaan worden. In 2024 was een stijging te zien van meldingen van seksuele delicten in vergelijking met 2023 en zijn er 131 meldingen van *sexchatting* gedaan (Politie, 2025). Dat laat zien dat er genoeg 'brengzaken' zijn. In deze evaluatie werd duidelijk dat in die gevallen vaak voor andere opsporingswegen wordt gekozen. Daarom lijkt het niet voor de hand te liggen dat de lokpuber in de toekomst vaker ingezet zal worden. Dit hoeft overigens geen probleem te zijn, zolang opsporingsfunctionarissen op de hoogte zijn dat de mogelijkheid van de lokpuber bestaat en er voldoende menskracht beschikbaar kan worden gesteld wanneer de inzet van de lokpuber noodzakelijk wordt geacht.

6 Ontoegankelijkmaking van gegevens (art. 125p Sv)

Dit hoofdstuk richt de aandacht op de bevoegdheid die ziet op de ontoegankelijkmaking van gegevens zoals neergelegd in artikel 125p Sv. Allereerst wordt het juridisch kader van dit wetsartikel uiteengezet (paragraaf 6.1). Vervolgens wordt de noodzaak (volgens de wetgever) besproken, alsmede de veronderstellingen die aan de nieuwe bevoegdheid ten grondslag liggen (paragraaf 6.2). Daarna wordt besproken hoe de artikel 125p Sv-bevoegdheid doorgaans in de praktijk wordt ingezet (paragraaf 6.3) en welke rol de vrijwillige Notice-and-Take-Downprocedure daarin speelt (paragraaf 6.3.1). Hierna zal op basis van de zakenanalyse[77] en interviews dieper worden ingegaan op de inhoud van zaken waarin artikel 125p Sv is ingezet (paragraaf 6.3.2). Vervolgens worden de voordelen beschreven die nieuwe bevoegdheid heeft voor de opsporingspraktijk en de aandachtspunten (paragraaf 6.3.3 en 6.3.4). Het hoofdstuk sluit af met een paragraaf waarin de veronderstellingen van de wetgever worden vergeleken met de toepassing van de bevoegdheid in de praktijk (paragraaf 6.4).

6.1 Juridisch kader

Met de inwerkingtreding van de Wet CIII is de ontoegankelijkmaking van gegevens toegevoegd aan het Wetboek van Stafvordering. Artikel 125p Sv luidt als volgt:

1 In geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, kan de officier van justitie aan een aanbieder van een communicatiedienst als bedoeld in artikel 138g[78] het bevel richten om terstond alle maatregelen te nemen die redelijkerwijs van hem kunnen worden gevergd om bepaalde gegevens die worden opgeslagen of doorgegeven, ontoegankelijk te maken, voor zover dit noodzakelijk is ter beëindiging van een strafbaar feit of ter voorkoming van nieuwe strafbare feiten.
2 Het bevel, bedoeld in het eerste lid, is schriftelijk en vermeldt:
   a het strafbare feit;
   b de feiten en omstandigheden waaruit blijkt dat ontoegankelijkmaking van de gegevens noodzakelijk is om het strafbare feit te beëindigen of nieuwe strafbare feiten te voorkomen;
   c welke gegevens ontoegankelijk moeten worden gemaakt.
3 Artikel 125o, tweede[79] en derde[80] lid, zijn van overeenkomstige toepassing.

---

77 Er wordt hier gesproken over een zakenanalyse en niet over een vonnisanalyse, omdat de analyse niet enkel gebaseerd is op vonnissen. Er zijn ook beslissingen van rechters-commissaris en informatie verstrekt naar aanleiding van een inventarisatie bij rechters-commissaris en bij het Openbaar Ministerie (officieren van justitie en coördinatoren Bijzonder OpsporingsBevoegheden (BOB-coördinatoren), meegenomen).

78 Onder aanbieder van een communicatiedienst wordt verstaan de natuurlijke persoon of rechtspersoon die in de uitoefening van een beroep of bedrijf aan de gebruikers van zijn dienst de mogelijkheid biedt te communiceren met behulp van een geautomatiseerd werk, of gegevens verwerkt of opslaat ten behoeve van een zodanige dienst of de gebruikers van die dienst (art. 138g Sv).

79 Onder ontoegankelijkmaking van gegevens wordt verstaan het treffen van maatregelen om te voorkomen dat de beheerder van het in het eerste lid bedoelde geautomatiseerd werk of derden verder van die gegevens kennisnemen of gebruikmaken, alsmede ter voorkoming van de verdere verspreiding van die gegevens. Onder ontoegankelijkmaking wordt mede verstaan het verwijderen van de gegevens uit het geautomatiseerd werk, met behoud van de gegevens voor strafvordering (art. 125o lid 2 Sv).

80 Zodra het belang van de strafvordering zich niet meer verzet tegen opheffing van de maatregelen, bedoeld in het tweede lid, bepaalt de officier van justitie dan wel, indien deze de doorzoeking heeft verricht, de rechter-commissaris dat de gegevens weer ter beschikking van de beheerder van het geautomatiseerd werk worden gesteld (art. 125o lid 3).

4 Het bevel, bedoeld in het eerste lid, kan slechts worden gegeven na voorafgaande schriftelijke machtiging, op vordering van de officier van justitie te verlenen door de rechter-commissaris. De rechter-commissaris stelt de aanbieder tot wie het bevel is gericht in de gelegenheid te worden gehoord. De aanbieder is bevoegd zich bij het horen door een raadsman te doen bijstaan.

Samenvattend betekent dit wetsartikel dat gegevens, na een machtiging van de rechter-commissaris, ontoegankelijk kunnen worden gemaakt. In eerste instantie voorlopig omdat een rechter nog een beslissing zal nemen over definitieve ontoegankelijkmaking. Toetsing door een rechter-commissaris moet zorgen voor het zorgvuldig afwegen van belangen, onder andere de bescherming van de vrijheid van meningsuiting (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 58). Ontoegankelijkmaking is alleen toegestaan wanneer sprake is van een verdenking van een strafbaar feit zoals bedoeld in artikel 67 Sv (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 58). Ontoegankelijk gemaakte gegevens kunnen uiteindelijk vernietigd worden via de procedure van artikel 354 of artikel 552fa Sv (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 97).

6.2 Noodzaak en veronderstellingen

Vóór de inwerkingtreding van de Wet CCIII bestonden al verschillende routes waar langs gegevens ontoegankelijk konden worden gemaakt, namelijk 1) via artikel 54a Sr en 2) via de vrijwillige Notice-and-Take-Down Gedragscode (hierna Gedragscode).[81] Deze tweede route bestaat nog steeds. Op basis van artikel 54a Sr was de ontoegankelijkmaking mogelijk via de benadering van een tussenpersoon die een telecommunicatiedienst verleent die bestaat uit de doorgifte of opslag van gegevens die van een ander afkomstig is. De wetgever vond het echter vanuit wetsystematisch oogpunt van belang dat de bevoegdheid in het Wetboek van Strafvordering werd opgenomen. In de memorie van toelichting wordt niet geëxpliciteerd wat dat wetsystematisch argument precies is, maar uit een verwijzing naar het rapport van Schellekens en collega's (2007) blijkt dat het gaat om het feit dat de ontoegankelijkmaking van gegevens, dat moet worden gezien als een bevoegdheid, niet is opgenomen in het Wetboek van Strafvordering (waarin bevoegdheden doorgaans staan), maar in het Wetboek van Strafrecht.[82] Verder meende de wetgever,

[81] Een officier van justitie kan ook besluiten een einde te maken aan strafbare feiten middels een doorzoeking ter vastlegging van gegevens of middels een onderzoek in een geautomatiseerd werk. Indien bij een van deze twee bevoegdheden gegevens worden aangetroffen die betrekking hebben op een strafbaar feit of waarmee een strafbaar feit is begaan, dan kunnen die op grond van het voorgestelde artikel 126cc Sv ontoegankelijk worden gemaakt (als dat nodig is voor het beëindigen van strafbare feiten of ter voorkoming van nieuwe strafbare feiten) (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 60).

[82] Naast dit 'rechtssystemisch' argument noemen Schellekens en collega's (2007) nog een aantal andere argumenten waarom artikel 54a Sr niet kan dienen als grondslag voor een bevel tot ontoegankelijkmaking. 1) Bij de totstandkoming van artikel 54a Sr heeft de regering aangegeven dat de toepassing van artikel 54a Sr gebaseerd kan worden op de bevoegdheid in artikel 125o Sv. Daarmee zou artikel 54a Sr geen grondslag zijn (wetshistorisch argument). 2) Behalve een machtiging door een rechter-commissaris zijn in artikel 54 Sr geen waarborgen geregeld die doorgaans verbonden zijn met een bevoegdheid in strafvordering, denk bijvoorbeeld aan de notificatieplicht en beklagmogelijkheden (rechtsbeschermend argument). 3) In het artikel staat niet dat de officier van justitie bevoegd is een bevel af te geven (tekstueel argument) (Schellekens et al., 2007, p. 18-19). Verder wijzen Schellekens en collega's (2007, p. 19) erop dat artikel 125o Sv, dat in de memorie van toelichting bij artikel 54a Sr genoemd wordt als grondslag voor ontoegankelijkmaking, volgens de 'juridische dogmatiek' problematisch is. Belangrijke bezwaren bij dit artikel zijn dat de bevoegdheid in dit artikel is gekoppeld aan een doorzoeking (hiervan zal lang niet altijd sprake zijn) en dat medewerking van een derde, zoals een aanbieder, uitzonderlijk is. Dat laatste is in geval van de ontoegankelijkmaking van gegevens juist niet het geval (Schellekens et al, 2007, p. 21-22). Hun algemene conclusie is dat het 'zeer twijfelachtig' is dat een bevel tot ontoegankelijkmaking kan worden gegeven op grond van artikel 54a Sr of artikel 125o Sv.

op basis van jurisprudentie[83], dat opname in het Wetboek van Strafvordering meer overzichtelijkheid en duidelijkheid voor de praktijk zou scheppen (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 56-57). Door opname in het Wetboek van Strafvordering bevindt een bevelsbevoegdheid zich op een logischere plek en wordt de uitvoering minder complex: één wetsartikel laat duidelijk blijken wat moet gebeuren en de bevoegdheid tot ontoegankelijkmaking en de strafuitsluitingsgrond[84] zijn uit elkaar getrokken. Op die manier zou de toepassing ervan gemakkelijker zijn waardoor de samenleving beter wordt beschermd tegen gedragingen waarvoor de bevoegdheid wordt ingezet. De wetgever heeft het rapport van Schellekens en collega's (2007) gebruikt om de nieuwe bevoegdheid in het Wetboek van Strafvordering vorm te geven.

Een tweede (vrijwillige) route die kan worden gevolgd om gegevens ontoegankelijk te maken is via de Gedragscode. Deze Gedragscode wordt later uitgebreider besproken (paragraaf 6.3.1) en houdt kortgezegd in dat 'tussenpersonen die in Nederland een openbare telecommunicatiedienst aanbieden op het internet' 'onmiskenbaar onrechtmatige of strafbare inhoud' kunnen verwijderen, bijvoorbeeld naar aanleiding van een melding. Indien onduidelijkheid bestaat over de onrechtmatigheid en strafbaarheid van de inhoud en de aanbieder verwijdering weigert, kan de melder aangifte doen of de rechter betrekken (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 57). In sommige gevallen blijkt de Gedragscode echter onvoldoende houvast te bieden, zo blijkt uit de memorie van toelichting. Niet alle aanbieders van een communicatiedienst hebben de Gedragscode bijvoorbeeld ondertekend, denk aan *hosting providers* en beheerders van een website. Daarnaast kan het zijn dat een aanbieder, die de Gedragscode wel ondertekend heeft, niet bereid is gegevens ontoegankelijk te maken, omdat hij met de officier van justitie van mening verschilt over de aard van de inhoud van de gegevens. In gevallen waarin de route via de Gedragscode niet voldoet, moet de nieuwe bevoegdheid ervoor zorgen dat strafbare feiten kunnen worden beëindigd en/of nieuwe strafbare feiten kunnen worden voorkomen (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 57).

De voorgestelde bevoegdheid is ingrijpend, omdat de vrijheid van meningsuiting in het geding kan zijn. Toetsing vooraf door een rechter-commissaris moet ervoor zorgen dat een zorgvuldige belangenafweging wordt gemaakt en dat ontoegankelijkmaking sneller plaats vindt dan wanneer gewacht moet worden op een uitspraak van een zittingsrechter. De wetgever vond het 'vanuit het oogpunt van de bescherming van de maatschappij' niet wenselijk dat gegevens pas ontoegankelijk zouden worden gemaakt wanneer een zittingsrechter een uitspraak heeft gedaan, bijvoorbeeld naar aanleiding van het niet voldoen aan een ambtelijk bevel of vanwege het deelnemen aan of plegen van een strafbaar feit. Een definitieve uitspraak kan in zo'n geval maanden op zich laten wachten. Dat ontoegankelijkmaking snel moet kunnen volgt ook uit de Europese Richtlijn inzake elektronische handel. Naar aanleiding van deze richtlijn zijn daarom de

[83] Er wordt verwezen naar drie uitspraken over dezelfde zaak. De eerste in eerste aanleg, de tweede in hoger beroep waarbij de zaak terug wordt verwezen naar de rechtbank die in eerste aanleg een uitspraak doet (derde uitspraak). Kern van deze zaak en de betreffende uitspraken is dat het Openbaar Ministerie een aanbieder verzocht heeft gegevens ontoegankelijk te maken, zonder dat de officier van justitie beschikte over een machtiging van de rechter-commissaris. Die had zonder inhoudelijke argumentatie afgezien van de machtiging. Het Openbaar Ministerie heeft daarop toch de ontoegankelijkmaking gevraagd (waaraan de aanbieder niet heeft voldaan), omdat anders geen rechtsmiddel open zou staan tegen het soort (in de ogen van het Openbaar Ministerie) strafbare gegevens dat op het internet geplaatst stond. Tijdens de behandeling van de zaak in eerste aanleg heeft de rechtbank geoordeeld dat de verdachte zich niet heeft kunnen beroepen op de strafuitsluitingsgrond die artikel 54a Sr bevat. Het Openbaar Ministerie had niet tot vervolging mogen overgaan en wordt onontvankelijk geacht. Dat oordeel blijft staan als de zaak op een later moment door het Gerechtshof in Leeuwarden weer terug wordt verwezen naar de Rechtbank Assen.

[84] Deze strafuitsluitingsgrond staat in artikel 54a Sr.

woorden ‘terstond alle maatregelen’ in de nieuwe wettelijke bepaling opgenomen om deze snelheidswens te weerspiegelen. Strafbare feiten kunnen daardoor sneller worden beëindigd en nieuwe strafbare feiten kunnen sneller worden voorkomen, waardoor de samenleving beter beschermd is (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 96).

Op basis van het voorgaande zijn de volgende veronderstellingen geformuleerd:

1a Op het internet staan gegevens die een strafbaar feit betreffen. Er bestaan al verschillende routes (waaronder artikel 54a Sr en de Gedragscode), maar daarmee kunnen gegevens onvoldoende ontoegankelijk worden gemaakt. Bijvoorbeeld wanneer routes buiten het strafrecht om niet afdoende zijn om gegevens te verwijderen. Daarnaast kent de artikel 54a Sr-route wetsystematische en praktische beperkingen. Dit leidt ertoe dat gegevens onvoldoende ontoegankelijk worden gemaakt en gesignaleerde strafbare feiten op het internet blijven voortbestaan. Een nieuw artikel in het Wetboek van Strafvordering komt tegemoet aan deze beperkingen. Door opname in het Wetboek van Strafvordering bevindt een bevelsbevoegdheid zich op een logischere plek. Bovendien wordt de uitvoering minder complex: één wetsartikel laat duidelijk blijken wat moet gebeuren en de bevoegdheid tot ontoegankelijkmaking en de strafuitsluitingsgrond zijn uit elkaar getrokken. Het nieuwe wetsartikel leidt er daardoor toe dat gegevens ontoegankelijk worden gemaakt en dat strafbare feiten worden beëindigd of nieuwe strafbare feiten worden voorkomen. Daardoor wordt de samenleving beter beschermd.

1b Ook de route via de vrijwillige Gedragscode kent beperkingen. Niet alle aanbieders zijn aangesloten bij de Gedragscode en aanbieders die wel aangesloten zijn hoeven niet akkoord te gaan met de ontoegankelijkmaking. Dat leidt ertoe dat gegevens niet ontoegankelijk worden gemaakt en strafbare feiten kunnen blijven voortbestaan. Opname van de bevoegdheid in het Wetboek van Strafvordering zorgt voor een niet-vrijwillige optie om gegevens ontoegankelijk te maken. Daardoor kunnen ook gegevens ontoegankelijk worden gemaakt van aanbieders die hier vrijwillig niet toe bereid zijn of die zich niet hebben aangesloten bij de Gedragscode. Dat leidt ertoe dat strafbare feiten worden beëindigd of nieuwe strafbare feiten worden voorkomen die daarvoor niet konden worden beëindigd/voorkomen. Daardoor wordt de samenleving beter beschermd.

De nieuwe bevoegdheid is een ingrijpende bevoegdheid, omdat de vrijheid van meningsuiting in het gedrang kan komen. Daarom vindt eerst een (schriftelijke) toets plaats door de rechter-commissaris. Die toets, vastgelegd in artikel 125p Sv, zorgt er bovendien voor dat relatief snel een beslissing kan worden genomen over de ontoegankelijkmaking. Er hoeft niet gewacht te worden op een uitspraak door een zittingsrechter. Dit leidt ertoe dat strafbare feiten sneller kunnen worden beëindigd en nieuwe strafbare feiten sneller voorkomen kunnen worden. Daardoor wordt de samenleving beter beschermd.

6.3 Artikel 125p Sv in de praktijk

Het Openbaar Ministerie heeft een (vertrouwelijk) intern document opgesteld waarin wordt besproken hoe kan worden omgegaan met het verwijderen van strafbare content op internet (Intern document 2, 2023). Twee opties, die overigens ook aan de orde komen in de memorie van toelichting, worden daarin besproken: de ontoegankelijkmaking van gegevens ex. artikel 125p Sv en een vrijwillige

ontoegankelijkmaking op basis van de Notice-and-Take-Downprocedure (hierna NTD-procedure). In zowel het interne document als de memorie van toelichting wordt beschreven dat het de voorkeur geniet om eerst te proberen gegevens ontoegankelijk te maken via de NTD-procedure. Mocht dit niet lukken, dan kan de artikel 125p Sv-route worden gevolgd. Beide wegen richten zich op de aanbieder van een communicatiedienst (hierna aanbieder), zoals is neergelegd in artikel 138g Sv:

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

In de aankomende paragrafen worden beide procedures besproken. Daarnaast zijn er ook routes binnen het civiel recht en het bestuursrecht voor het ontoegankelijk maken en verwijderen van gegevens. Omdat deze routes buiten strafrecht vallen en deze evaluatie betrekking heeft op nieuwe/vernieuwde wettelijke bepalingen worden deze routes verder niet inhoudelijk besproken.[85]

6.3.1 Notice-and-Take-Downprocedure en artikel 125p Sv

De NTD-procedure bestond, zoals gezegd, al voor de inwerkingtreding van artikel 125p Sv en is ontwikkeld door de hostingbranche zelf. Deze procedure is neergelegd in de eerdergenoemde Gedragscode en is bedoeld om aanbieders te helpen zorgvuldig en 'binnen de bestaande wettelijke kaders' te werk te gaan bij een verzoek van derden om informatie te verwijderen van het internet. De Gedragscode richt zich op aanbieders en regelt de omgang met meldingen van onrechtmatige en strafbare inhoud (art. 1a Gedragscode). Het gaat daarbij om tussenpersonen of aanbieders die in Nederland een openbare (telecommunicatie-)dienst op internet leveren (art. 1b Gedragscode). Binnen het huidige kader zijn dit de online dienstverleners, zoals hostingproviders, maar ook platformen zoals bol.com, Facebook en Ebay. De procedure stelt eenieder in de gelegenheid een verzoek te doen om strafbare content te verwijderen. Dit is een vrijwillige weg, wat betekent dat de melder in essentie de aanbieder verzoekt bepaalde content ontoegankelijk te maken. Voor het Nederlandse deel op internet hebben veel online dienstverleners zich aangesloten bij de Gedragscode. Ook Europese regelgeving stuurt aan op het hebben van NTD-procedures. Zo stelt de Digital Service Act (DSA) dat 'alle aanbieders van hostingdiensten (…) gebruikersvriendelijke meldings- en actiemechanismen invoeren' via welke een aanbieder kan worden verzocht gegevens (vrijwillig) ontoegankelijk te maken (Verordening (EU) 2022/2065, 2022, par. 50). De Gedragscode kan worden gezien als een voorbeeld van zo'n meldings- en actiemechanisme en stelt eenieder in de gelegenheid om een melding of 'notice' te doen wanneer hij of zij onrechtmatige of strafbare inhoud tegenkomt op het web, zoals kinderporno, *phishing* websites en discriminerende beelden en teksten. Wanneer een aanbieder meent dat de gemelde content niet in strijd is met de wet gebeurt er niets, en wanneer dit wel het geval is wordt de content uit de lucht gehaald. De politie en het Openbaar Ministerie kunnen

[85] Voor een overzicht van deze civielrechtelijke en bestuursrechtelijke routes, zie Van Hoboken en collega's (2020). Zij deden onderzoek naar de wijze waarop, vooral juridisch, kan worden omgegaan met 'onrechtmatige uitingen die mensen in hun persoon als zodanig treffen' (Van Hoboken et al., 2020: p. 19). Daarnaast is er sinds 2024 de Autoriteit online Terroristisch en Kinderpornografisch Materiaal (ATKM) die de bevoegdheid heeft om verwijderingsbevelen te geven aan aanbieders wanneer deze kinderpornografisch of terroristisch materiaal op hun internetservers hebben staan. De ATKM heeft geen opsporingsbevoegdheden en kan geen strafrechtelijke vervolging instellen. De bevoegdheid tot het ontoegankelijk maken van online kinderporno komt hun toe op basis van de Wet bestuursrechtelijke aanpak online kinderpornografisch materiaal (Rijksoverheid, z.d.).

ook gebruikmaken van de NTD-procedure. Zoals besproken geeft het Openbaar Ministerie de voorkeur aan de NTD-procedure boven de artikel 125p Sv-procedure, omdat de vrijwillige weg vaak sneller en efficiënter is en minder capaciteit kost aan de kant van het Openbaar Ministerie en de politie (Intern document 2, 2023, p. 3). Hierbij is het wel van belang dat een aanbieder meewerkt. Wanneer een aanbieder niet vrijwillig meewerkt duurt het vaak langer voordat content van het internet wordt gehaald, omdat de artikel 125p Sv-procedure doorlopen moet worden. Uit interviews komt naar voren dat de NTD-procedure vaker wordt gebruikt dan het juridische verwijderingsbevel op grond van artikel 125p Sv. Helaas is niet duidelijk geworden hoe vaak dit precies gebeurt. Een geïnterviewde medewerker van het Openbaar Ministerie ervaart de NTD-procedure als de 'snelste' manier en dus een goede weg wanneer snelheid is geboden én de aanbieder meewerkt, bijvoorbeeld bij sextortion, cyberpesten of kinderporno.

Hoofdpunten
- Zowel de NTD-procedure als artikel 125p Sv kunnen worden benut om gegevens ontoegankelijk te maken. Het Openbaar Ministerie geeft, in lijn met de memorie van toelichting, de voorkeur aan de NTD-procedure boven artikel 125p Sv. Deze route is vaak sneller.

6.3.2 Aard artikel 125p Sv zaken

Om zicht te krijgen op het soort zaken waarin artikel 125p Sv wordt ingezet is een zakenanalyse uitgevoerd. Voor deze analyse is bij betrokkenen, onder ander rechters-commissarissen en het Openbaar Ministerie, geïnventariseerd in welke zaken en hoe vaak artikel 125p Sv is ingezet. In de periode maart 2019 tot en met oktober 2024[86] zijn er 14 zaken geweest waarin één of meerdere machtigingen zijn afgegeven om gegevens ontoegankelijk te maken. In één zaak is uiteindelijk geen bevel afgegeven door de officier van justitie, omdat het doel van het onderzoek met een andere bevoegdheid kon worden bereikt. Daarnaast is de inzet van artikel 125p Sv in vijf zaken overwogen maar niet ingezet. De hoeveelheid informatie met betrekking tot de zaken die wij tot onze beschikking hadden verschilde. Dat varieerde van geen informatie[87] tot informatie uit een rechterlijke uitspraak (vooral beschikkingen van een rechter-commissaris) en/of een interview of een korte e-mail met daarin één of twee zinnen over de inhoud van de zaak.

In de aankomende paragrafen worden de geanalyseerde zaken besproken. De zaken waarin artikel 125p Sv is ingezet worden ingedeeld in de volgende categorieën: ontoegankelijkmaking content Telegram, ontoegankelijkmaking content website, ontoegankelijkmaking IP-adres en ontoegankelijkmaking overig. De paragraaf eindigt met een paragraaf over zaken waarin het Openbaar Ministerie overwogen heeft artikel 125p Sv in te zetten, maar waarin uiteindelijk geen bevel is afgegeven.

Ontoegankelijkmaking Telegram
In drie zaken betrof de ontoegankelijkmaking kanalen of accounts op Telegram. Het ging hier overigens om een bijzondere toepassing van artikel 125p Sv, omdat ontoegankelijkmaking niet via de aanbieder verliep. In alle drie de zaken gaf de rechter-commissaris de officier van justitie toestemming om een bevel te geven aan een politiemedewerker om, via de inbeslaggenomen telefoon van een verdachte, gegevens ontoegankelijk te maken in Telegram-groepen beheerd door de verdachte.

[86] In die maand werd de laatste uitvraag gedaan bij het Openbaar Ministerie.
[87] Deze zaak wordt om die reden verder niet meer besproken.

In één zaak ging het over de ontoegankelijkmaking van Telegramgroepen waarin extremistische content, waaronder complottheorieën, werden verspreid (ECLI:NL:RBDHA:2021:11250). In deze groepen werd op strafbare wijze opgeruid tot geweld tegenover personen in publieke posities.[88] In deze zaak betrof het zoals gezegd geen gewone toepassing van artikel 125p Sv, maar werd het verzoek toegewezen op grond van artikel 181[89] juncto artikel 125p Sv. Dit is een toepassing naar analogie van artikel 125p Sv, waarbij van het horen van de aanbieder werd afgezien. Deze hoorplicht, neergelegd in artikel 125p lid 4 Sv, werd achterwegen gelaten op basis van de aanname dat Telegram (de aanbieder in deze zaak) niet zou meewerken met verzoeken van overheden, zo volgt uit de beslissing van de rechter-commissaris.[90] In zijn beslissing licht de rechter-commissaris toe dat aan de voorwaarden voor een toepassing naar analogie van artikel 125p lid 1 Sv was voldaan: het betrof een verdenking van misdrijven als omschreven in artikel 67 lid 1 Sv en de ontoegankelijkmaking van gegevens was noodzakelijk om de strafbare feiten te beëindigen of nieuwe strafbare feiten te voorkomen.

In de tweede zaak was sprake van een soortgelijke toepassing van artikel 125p Sv en ging het om de illegale verkoop van professioneel vuurwerk via Telegram. In deze zaak constateerde de rechter-commissaris dat, naast spoedeisendheid, aan de eisen van proportionaliteit en subsidiariteit werd voldaan. Verder beredeneerde de rechter-commissaris dat, hoewel het bevel zich niet richtte op de aanbieder maar op een politiemedewerker, de inbreuk voor de betrokkene niet groter was en het eindresultaat hetzelfde. Op deze toepassing naar analogie van artikel 125p Sv is kritiek geleverd. Zo schreef Berndsen (2021) dat deze toepassing in strijd is met de tekst en bedoeling van de wet, voornamelijk omdat de aanbieder niet is gehoord.

De derde zaak betrof een Telegramaccount waarmee de eigenaar van dat account onder andere vervalste zorgdiploma's, rijbewijzen, paspoorten en PCR-testbewijzen adverteerde in Telegramgroepen. Ook in deze zaak ontving de officier van justitie een machtiging om een opsporingsambtenaar op te dragen het Telegram account van de verdachte te verwijderen en een waarschuwing te plaatsen in de groepen waarin de gebruiker adverteerde.

Ontoegankelijkmaking website

In drie zaken had artikel 125p Sv betrekking op de ontoegankelijkmaking van een website. Eén van deze zaken, zo blijkt uit een interview met een medewerker van het Openbaar Ministerie, betrof de ontoegankelijkmaking van een malafide verkoopwebsite. Het ging hier om online handelsfraude (art. 326e Sr) waarbij de verdachte producten, waaronder telefoons, verkocht zonder deze te leveren. Een 'stopgesprek' met de verdachte, waarin deze gemaand werd zijn activiteiten te beëindigen, bleek tevergeefs en de aangiften bleven binnenstromen. Artikel 125p Sv is ingezet om hier een einde aan te maken. In deze zaak wees de serviceprovider een NTD-verzoek af, omdat de provider meende dat het zou gaan om een leveringsgeschil. Vervolgens is middels een artikel 125p Sv-vordering de website uit de lucht gehaald. Van de andere twee zaken is alleen duidelijk geworden waarop de ontoegankelijkmaking zag. In één zaak ging het om de ontoegankelijkmaking van een filmpje op een website en in de andere zaak werd een webshop uit de lucht gehaald

88 Het opruien tot geweld – wat strafbaar is op grond van artikel 131 Sr – leidde tot het verzoek tot ontoegankelijk making.

89 Op basis van artikel 181 Sv kan de officier van justitie gewenste onderzoekshandelingen vorderen bij de rechter-commissaris.

90 Inmiddels is deze situatie veranderd, omdat de CEO van Telegram na zijn aanhouding aangegeven heeft met opsporingsinstanties mee te zullen werken. Zie bijvoorbeeld: Krikhaar, 2024.

waarop illegale dopingmiddelen werden verhandeld. Een medewerker van het Openbaar Ministerie vertelt dat de website in kwestie eerst is neergehaald middels een NTD-verzoek, waarna deze later definitief ontoegankelijk is gemaakt middels een artikel 125p Sv-bevel. Opvallend aan deze laatste zaak is dat het lijkt alsof de aanbieder nooit is gehoord en dat artikel 125p Sv hier is gebruikt voor de definitieve ontoegankelijkmaking, terwijl het een tijdelijke maatregel betreft.

Ontoegankelijkmaking IP-adres

In drie zaken ging het om de ontoegankelijkmaking van IP-adressen. Soms gebeurde dit door middel van de ontoegankelijkmaking van een server. Dit was in één van deze zaken het geval. In de eerste zaak werd artikel 125p Sv ingezet in een onderzoek naar een hacker. Om welke gegevens het ging is niet duidelijk geworden. In de tweede zaak werden IP-adressen, waarop een grote hoeveelheid weggenomen persoonsgegevens, paspoortgegevens en andere marktgevoelige informatie stond opgeslagen, ontoegankelijk gemaakt. In deze zaak gaf de rechter-commissaris toestemming nadat de officier van justitie de zaak mondeling had toegelicht. Uit de machtiging blijkt niet in hoeverre de aanbieder van de communicatiedienst is gehoord. Wel achtte de rechter-commissaris de machtiging noodzakelijk en de mondelinge toelichting van de officier van justitie in overeenstemming met de vastgelegde feiten en omstandigheden in het proces-verbaal. De derde zaak betrof een geanalyseerde uitspraak op een artikel 552fa Sv vordering (ECLI:NL:RBROT:2021:1918). In deze vordering ging het om de vernietiging van gegevens op meerdere servers die eerder ontoegankelijk werden gemaakt middels vier artikel 125p Sv-machtigingen. Dit is een voorbeeld van een zaak waarbij IP-adressen ontoegankelijk zijn gemaakt door de ontoegankelijkmaking van een server. De ontoegankelijkmaking gebeurde in het kader van een Duits opsporingsonderzoek naar afpersing van een Duitse onderneming en sabotage van het computernetwerk van dat bedrijf.[91]

Ontoegankelijkmaking overig

De overige vier zaken betroffen zaken waarvan relatief weinig inhoudelijke informatie naar voren is gekomen of kan worden gegeven. De eerste zaak is een zaak waarin een machtiging voor een artikel 125p Sv-inzet is afgegeven. Dit onderzoek was onder andere gericht op het neerhalen van de digitale infrastructuur waarvan een *ransomware*groepering gebruik van maakte. In deze zaak is artikel 125p Sv uiteindelijk niet ingezet omdat de doelen die bereikt konden worden met de bevoegdheid via een andere weg zijn bereikt. In de tweede zaak is niet meer duidelijk geworden dan dat het ging om een aantal soortgelijk geformuleerde artikel 125p Sv-vorderingen en dat de aanbieder, voorafgaand aan het toekennen van de machtiging, is gehoord door de rechter-commissaris. De derde zaak betrof de ontoegankelijkmaking van een vals socialemedia-account van een functionaris betrokken bij de opsporing. In deze zaak werd de artikel 125p Sv procedure doorlopen maar niet voltooid, omdat de aanbieder niet reageerde op de hoorplicht. Als gevolg daarvan kon de rechter-commissaris geen machtiging afgegeven. In de vierde zaak zag de artikel 125p Sv-vordering op een zaak waarin gegevens werden gestolen van een bedrijf dat behoort tot de vitale infrastructuur van Nederland. In deze zaak is het 125p Sv-bevel mondeling afgegeven zonder de aanbieder te hebben gehoord. Mondelinge afgifte werd in deze zaak noodzakelijk geacht de urgentie van de zaak, zo vertelt een geïnterviewde officier van justitie.

[91] (Poging tot) afpersing is strafbaar gesteld in artikelen 253, 22, en 23 van het Duitse Wetboek van Strafrecht. Deze artikelen zijn binnen het Nederlandse recht vergelijkbaar met de artikel 317 lid 2 en artikel 318 Sr. Verandering van gegevens en computersabotage zijn strafbaar op grond van artikelen 303a en 303b van het Duitse Wetboek van Strafrecht. Vergelijkbaar met de artikelen 138ab, 139d en 350a Sr van het Nederlandse recht.

(Nog) niet ingezet
Uit de zakenanalyse en interviews blijkt dat in een aantal zaken overwogen is artikel 125p Sv in te zetten, maar dat dat uiteindelijk niet is gebeurd. In verschillende zaken zou gekozen zijn voor een alternatief waarbij helaas niet altijd duidelijk is geworden welk alternatief dat was. Uit meerdere interviews komt in elk geval naar voren dat de NTD-procedure vaak wordt ingezet in plaats van artikel 125p Sv. Een geïnterviewde medewerker van het Openbaar Ministerie omschrijft deze procedure als meestal 'sneller' en vertelt dat de meeste aanbieders vrijwillig meewerken als de politie het vraagt. Een geïnterviewde advocaat merkt op dat hij vermoedt dat artikel 125p Sv relatief weinig wordt ingezet, omdat hij vaak wordt 'overgeslagen'. Deze advocaat geeft aan dat opsporingsambtenaren in de praktijk, na een geweigerd verzoek tot vrijwillige verwijdering, in bepaalde zaken meestal overgaan tot alternatieven voor artikel 125p Sv, zoals inbeslagname van servers. Volgens deze advocaat heeft de rechtbank daar 'over het algemeen veel begrip voor', omdat hierover doorgaans geen discussie plaatsvindt.

Vrijheid van meningsuiting
Een belangrijke zorg bij de introductie van artikel 125p Sv was dat de vrijheid van meningsuiting in het geding zou kunnen komen. Onder andere om die reden is een schriftelijke machtiging van de rechter-commissaris vereist en dient de aanbieder gehoord te worden. Veel geïnterviewden, werkzaam als opsporingsfunctionaris, merken op dat de vrijheid van meningsuiting in veel artikel 125p Sv-zaken niet ter discussie staat, omdat het dikwijls zou gaan over gegevens die onmiskenbaar onwettig zijn. Eén van hen geeft aan dat het vaak om 'overduidelijk' strafbare content gaat, zoals kinderporno, *phishing* websites, online illegale handel, malware, botnets en weggenomen (gepubliceerde) persoonsgegevens. Bovendien merkt een andere geïnterviewde medewerker van het Openbaar Ministerie op dat in veel zaken waarin de vrijheid van meningsuiting wel een rol speelt, zoals bij belediging, smaad en laster, het niet gaat over een misdrijf zoals beschreven in artikel 67, lid 1 Sv, waardoor de inzet van artikel 125p Sv überhaupt niet aan de orde is.

Hoofdpunten
- In 14 zaken zijn gegevens ontoegankelijk gemaakt op basis van artikel 125p Sv of is dit geprobeerd. Het ging om de ontoegankelijkmaking van Telegram kanalen en -accounts, websites, IP-adressen. Daarnaast is een categorie overig onderscheiden.
- Verschillende soorten gegevens werden ontoegankelijk gemaakt: strafbare complottheorieën, de illegale verkoop van vuurwerk, vervalste documenten. Daarnaast ging het om een filmpje op een website, een malafide verkoopwebsite en een webshop waarop illegaal dopingmiddelen werden verkocht. Verder betroffen de gegevens die ontoegankelijk moesten worden gemaakt weggenomen bedrijfsgegevens, persoonsgegevens en andere marktgevoelige informatie en een vals account op sociale media.
- In de drie Telegram-zaken ging het om een bijzondere toepassing van artikel 125p Sv, namelijk artikelen 181 jo. 125p Sv, waarbij niet de aanbieder, maar een opsporingsambtenaar de gegevens ontoegankelijk maakte via een inbeslaggenomen telefoon. Van de hoorplicht werd afgezien, omdat aannemelijk werd geacht dat Telegram in deze gevallen niet zou meewerken.
- In sommige zaken wordt de keuze gemaakt om artikel 125p Sv niet te gebruiken, onder andere wanneer artikel 125p Sv niet goed werkbaar is. Vaak wordt dan gekozen voor een alternatief.
- Opsporingsfunctionarissen geven aan dat veel gegevens die onderwerp zijn van de ontoegankelijkmaking, zoals kinderporno, gehackte gegevens en malware, zo

overduidelijk strafbaar zijn dat de vrijheid van meningsuiting niet ter discussie zou staan. In zaken waarin de vrijheid van meningsuiting wel een rol zou kunnen spelen zou het dikwijls gaan om misdrijven waarvoor artikel 125p Sv niet mag worden ingezet, omdat het geen strafbaar feit betreft waarvoor hechtenis kan worden opgelegd.

6.3.3 Voordelen voor de opsporingspraktijk

De opname van artikel 125p Sv in het Wetboek van Strafvordering heeft een aantal voordelen voor de opsporingspraktijk, zo komt uit de interviews naar voren. Deze voordelen worden in de komende paragrafen nader uitgewerkt. Allereerst wordt besproken dat artikel 125p Sv de bevoegdheid tot ontoegankelijkmaking duidelijker maakt dan toen deze nog was opgenomen in het Wetboek van Strafrecht (art. 54a Sr) en dat het artikel alle betrokkenen betere bescherming kan bieden. Vervolgens komt aan de orde dat een artikel 125p Sv-bevel een alternatief is als de vrijwillige route niet werkt of de verwachting is dat dit het geval zal zijn. Daarbij gaat het om een gewone toepassing en een variant naar analogie van artikel 125p Sv.

Duidelijk(er) artikel en betere bescherming
Een deel van de geïnterviewden ervaren artikel 125p Sv als een duidelijk(er) artikel waaruit ieders verantwoordelijkheid, bijvoorbeeld die van de rechter-commissaris, goed naar voren komt. De wetgever achtte de komst van artikel 125p Sv onder andere gewenst vanuit 'wetsystematisch oogpunt', omdat het Wetboek van Strafvordering doorgaans alle bevoegdheden bevat (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 56). Een geïnterviewde medewerker van het Openbaar Ministerie merkt op dat sinds de komst van artikel 125p Sv de bevoegdheid 'op een goede plek [zit] als handhavingsinstrument'. Volgens deze geïnterviewde leverde de oude plek van de bevoegdheid, in het Wetboek van Strafrecht, moeilijkheden op in de uitvoering, vooral met betrekking tot de rechter-commissaris. Een rechter-commissaris gaat in principe enkel over bepalingen in het Wetboek van Strafvordering. Deze geïnterviewde vertelt te hebben ervaren dat de rechter-commissaris voorheen niet meewerkte vanwege het feit dat de bevoegdheid tot ontoegankelijkmaking in het Wetboek van Strafrecht stond. Een andere officier van justitie ervaart artikel 125p Sv als een 'ongecompliceerd en voor de hand liggende bevoegdheid'. Door de inzet van de bevoegdheid kon deze officier strafbare handelingen op een website (tijdelijk) stoppen. In deze zaak slechts tijdelijk, omdat de verdachte nieuwe soortgelijke websites maakte, aldus deze geïnterviewde officier. Ook een andere officier van justitie merkt op, dat artikel 125p Sv strafbaar handelen kan stoppen, waardoor de rechtsorde beter wordt beschermd.

Daarnaast zorgt artikel 125p Sv ervoor dat betrokken actoren beter worden beschermd. Eén van de geïnterviewden legt uit dat dit bijvoorbeeld geldt voor degene die de ontoegankelijkmaking uitvoert. Het is immers de rechter-commissaris, als 'onafhankelijke autoriteit' die toestemming moet geven. Daarnaast zou een artikel 125p Sv-bevel, volgens een geïnterviewde medewerker van het Openbaar Ministerie, de aanbieder betere bescherming kunnen bieden dan een NTD-verzoek, bijvoorbeeld indien een klant schade wil verhalen op de aanbieder. Denk aan schade die is geleden doordat een website uit de lucht is gehaald. Verder biedt een artikel 125p Sv-bevel de aanbieder bescherming tegen vervolging wanneer strafbare feiten zijn gepleegd door middel van zijn (telecommunicatie)diensten. Dit is geregeld middels de vervolgingsuitsluitingsgrond in artikel 54a Sr.[92] Deze vervolgingsuitsluitingsgrond kent

[92] Dit artikel bepaalt dat een aanbieder niet wordt vervolgd bij een strafbaar feit dat met gebruikmaking van zijn dienst wordt begaan indien hij voldoet aan een bevel ex. artikel 125p Sv.

ook grenzen. Sinds de inwerkingtreding van artikel 125p Sv is jurisprudentie (ECLI:NL:RBROT:2021:2040 en ECLI:NL:GHDHA:2022:1550) ontstaan die een voorwaarde toevoegt aan deze vervolgingsuitsluitingsgrond. Aanbieders mogen worden vervolgd als sprake is van een verdenking van medeplichtigheid aan strafbare feiten gepleegd door middel van hun (telecommunicatie)diensten én indien voldaan wordt aan bepaalde omstandigheden. Hierbij maakt het niet uit of een ontoegankelijkmakingsbevel ex. artikel 125p Sv is afgegeven. Van medeplichtigheid kan sprake zijn wanneer sprake is van een 'bad hoster'.[93]

Optie als aanbieder niet vrijwillig meewerkt

Uit de helft van de interviews komt naar voren dat artikel 125p Sv een oplossing kan bieden wanneer wordt vermoed dat een aanbieder niet vrijwillig zal meewerken aan ontoegankelijkmaking. Dit kan geschieden via de gewone toepassing van artikel 125p Sv, maar ook via een toepassing naar analogie van artikel 125p Sv. Een parketsecretaris vertelt over de gewone inzet van artikel 125p Sv in een zaak betreffende een frauduleuze verkoopwebsite, nadat een NTD-verzoek niets opleverde. In deze zaak was al een stopgesprek geweest, terwijl de aangiften binnen bleven komen. Een artikel 125p Sv-bevel was, volgens deze parketsecretaris, de enige manier in deze zaak om ervoor te zorgen dat het strafbaar handelen stopte. Daarnaast kan een 'gewone' inzet van artikel 125p Sv de voorkeur hebben in situaties waarin het onduidelijk is of de aanbieder kan worden vertrouwd. Dat geldt bijvoorbeeld in de eerdergenoemde dopingzaak waarbij de officier van justitie op dat moment zeker wilde weten dat de website ontoegankelijk zou worden. Als gevolg hiervan kon de verkoop van de doping tijdelijk worden gestopt. Deze geïnterviewde vertelt echter ook dat, na de ontoegankelijkmaking, soortgelijke nieuwe websites zijn opgedoken op het internet.

Voor een aantal opsporingsfunctionarissen biedt de komst van artikel 125p Sv, in zaken waarin een aanbieder niet meewerkt, een wettelijke basis voor een toepassing naar analogie van artikel 125p Sv. Zoals eerder besproken betreft het hier een aantal zaken waarin Telegramkanalen en -groepen ontoegankelijk zijn gemaakt via de telefoon van een verdachte. Een geïnterviewde officier van justitie vindt deze ontwikkelijking nuttig, omdat vóór de inwerkingtreding van het artikel een soortgelijke toepassing onmogelijk zou zijn geweest. Deze geïnterviewde overweegt dat de hackbevoegdheid wellicht ingezet zou kunnen worden, maar dat dit 'een hele zware inzet' is en bovendien enkel inzetbaar bij een 8-jaars feit. Bovendien zou een artikel 125p Sv-bevel beter passen, omdat artikel 125p Sv 'veel meer een maatregel [is] dan (…) een bijzondere opsporingsbevoegdheid', aldus de geïnterviewde. Deze geïnterviewde geeft ook aan dat deze analoge toepassing wellicht 'niet de standaardroute' van het artikel is. Zoals eerder opgemerkt is er ook kritiek op deze analoge toepassing, omdat het niet is wat de wetgever oorspronkelijk beoogde.

Hoofdpunten

- Artikel 125 Sv heeft een aantal voordelen voor de opsporingspraktijk: 1) door opname in het Wetboek van Strafvordering is de bevoegdheid tot ontoegankelijkmaking duidelijker geregeld en biedt het artikel betere bescherming aan de betrokkenen; en 2) de bevoegdheid is een oplossing als de aanbieder niet vrijwillig wil meewerken.

[93] *Bad hosters* zijn aanbieders binnen het criminele circuit. Dit kunnen aanbieders zijn die meewerken aan strafbare praktijken of die zelf strafbare handelingen verrichten.

6.3.4 *Aandachtspunten*

De zakenanalyse en de interviews hebben ook een aantal aandachtpunten naar voren gebracht. Allereerst richt de aandacht zich op lid 4 van artikel 125p Sv. Er wordt stilgestaan bij de toets door de rechter-commissaris en het horen van de aanbieder. Vervolgens wordt ingegaan op het tijdelijke karakter van de maatregel en de dimensie buitenland.

Rechterlijke toets vooraf (lid 4)
Uit de interviews met medewerkers van het Openbaar Ministerie komt naar voren dat lid 4 van artikel 125p Sv voor moeilijkheden kan zorgen in de toepassing van de bevoegdheid. Lid 4 regelt dat het bevel tot ontoegankelijkmaking slechts kan worden gegeven na een voorafgaande schriftelijke machtiging van de rechter-commissaris. Onderdeel van deze toets is dat de rechter-commissaris de aanbieder hoort voorafgaand aan de afgifte van de machtiging. Uit een aantal interviews komt naar voren dat deze voorafgaande machtiging of rechterlijke toets, 'een grote belemmerende factor' is voor effectief gebruik van artikel 125p Sv in de praktijk. Dat heeft zowel te maken met de machtiging door de rechter-commissaris als met het horen van de aanbieder. Hoewel beide punten met elkaar samenhangen, worden ze in deze paragraaf voor de duidelijkheid apart besproken.

Toets rechter-commissaris
Verschillende geïnterviewden merken op dat het verkrijgen van toestemming van de rechter-commissaris voorafgaand aan een artikel 125p Sv-bevel problematisch is wanneer het gaat om risicovolle situaties en situaties waarin snelheid geboden is. Zowel het opmaken van de vordering tot machtiging door een officier van justitie als het opmaken van de schriftelijke machtiging door de rechter-commissaris kost tijd, zeker wanneer verzoeken tot ontoegankelijkmaking binnenkomen op tijdstippen en momenten waarop een rechter-commissaris niet meteen bereikbaar is. Dat zorgt ervoor dat het verkrijgen van de machtiging al snel een aantal dagen in beslag kan nemen, wat een probleem kan zijn als gegevens snel ontoegankelijk moeten worden gemaakt.

Uit een groot deel van de interviews blijkt dat er verschillende soorten zaken zijn waarbij snelle ontoegankelijkmaking gewenst is. Een geïnterviewde officier van justitie legt uit hoe de rechterlijke toets een belemmering was in een zaak betreffende kinderporno. In deze zaak negeerde een grote Nederlandse aanbieder een melding van het Meldpunt Kinderporno over de aanwezigheid van kinderporno op servers van de aanbieder. Deze officier moest daarom voor elke afbeelding naar de rechter-commissaris ter verkrijging van een 125p Sv-bevel. Hierdoor bleef de 'kinderporno veel langer (…) staan dan gewenst', aldus deze geïnterviewde. Deze officier van justitie vertelt dat na veel aandringen en een waarschuwing voor potentiële vervolging de aanbieder uiteindelijk is gaan samenwerken met het Meldpunt. Een andere geïnterviewde, tevens medewerker van het Openbaar Ministerie, noemt een ander voorbeeld in het kader van kinderporno: een zaak waarin foto's van minderjarigen werden gedeeld op een online platform. Deze geïnterviewde legt uit dat dit soort foto's soms 'binnen een paar dagen misschien wel 80.000 keer (…)[worden] gedownload', waardoor het wenselijk is de gegevens zo snel mogelijk offline te halen. Volgens deze geïnterviewde kan het in de praktijk echter dagen duren voor de foto's weg zijn, omdat toestemming van de rechter-commissaris nodig is voor de ontoegankelijkmaking.

Snelle ontoegankelijkmaking kan niet alleen gewenst zijn in kinderpornozaken. Ook in zaken waarbij het gaat om 'cyberaanvallen' en gevoelige (bedrijfs-)gegevens die zijn gehackt, bestaat de behoefte om snel gegevens ontoegankelijk te maken, zo komt in een aantal interviews naar voren. In dit soort zaken kan artikel 125p Sv bijvoorbeeld worden ingezet om de gestolen gegevens of de infrastructuur waarmee de aanval wordt gepleegd, ontoegankelijk te maken. Snelheid kan in die gevallen belangrijk zijn, omdat cyberaanvallen vaak heel snel plaatsvinden, soms 'binnen vijf minuten', zo legt de eerder aangehaalde medewerker van het Openbaar Ministerie uit. Een aanval kan zich bovendien snel naar een andere server verplaatsen. Deze geïnterviewde merkt op dat artikel 125p Sv juist voor dit soort situaties was bedoeld, maar dat artikel 125p Sv, vanwege het gebrek aan snelheid, geen oplossing biedt.

In twee zaken is, vanwege het tijdsaspect, niet gekozen voor artikel 125p Sv, zo vertelt één van de geïnterviewde officieren van justitie. In de eerste zaak ging het om gehackte gegevens van een kantoor in het buitenland. Het betrof gevoelige klantgegevens die naar een Nederlandse server waren gesluisd. Deze geïnterviewde legt uit dat snelle ontoegankelijkmaking op basis van artikel 125p Sv in deze zaak cruciaal was, omdat de data gekopieerd konden worden zolang deze op de server stonden. In deze zaak kwam het verzoek tot ontoegankelijkmaking binnen op een vrijdagmiddag om 16:00 uur, waardoor er geen tijd was om vóór het weekend een schriftelijke machtiging van een rechter-commissaris te verkrijgen. De andere zaak betrof een soortgelijke situatie, waarin het verzoek laat in de avond binnenkwam. Dezelfde officier van justitie vertelt:

> Ik zei ook tegen de [rechter-commissaris], ik weet dat ik je nu kan vragen om een schriftelijk machtiging, maar ik weet ook dat je hem niet kan afgeven nu. Hoe gaan we dat oplossen? Daar zit de grootste bottleneck. En dat is ook de reden waarom we andere artikelen gebruiken of andere oplossingen.

Volgens deze geïnterviewde komt het in dit soort zaken vaak aan op alternatieve bevoegdheden, zoals ontoegankelijkmaking tijdens een doorzoeking van een geautomatiseerd werk op een plaats niet zijnde een woning (art. 125o Sv) of inbeslagname (art. 94a Sv) – twee bevoegdheden die een officier kunnen toekomen zonder machtiging van de rechter commissaris.[94] Twee andere geïnterviewde medewerkers van het Openbaar Ministerie, waaronder een officier van justitie, merken op dat artikel 125p Sv wat hen betreft onevenredige hoge eisen stelt in vergelijking met deze twee bevoegdheden. Bovendien kennen beide artikelen nadelen, zo komt uit een aantal interviews naar voren. Ten eerste is een officier van justitie bij artikel 125o Sv alsnog afhankelijk van de medewerking van het datacentrum om de server te lokaliseren. Ten tweede kan een doorzoeking, bijvoorbeeld in de eerdergenoemde casus waarin gevoelige data naar een Nederlandse server werd gesluisd, onwenselijk zijn. In die casus mochten Nederlandse autoriteiten de data niet inzien vanwege diens gevoelige aard. Inbeslagname van de gehele server was om die reden in deze zaak de enige werkbare optie. Een nadeel van de inbeslagname is dat deze soms ingrijpender kan zijn dan artikel 125p Sv, omdat de aanbieder harder geraakt kan worden dan de verdachte, zo legt de eerder aangehaalde officier van justitie uit. Een inbeslaggenomen server is het eigendom van het datacentrum (de aanbieder), wat betekent dat de eigenaar wordt getroffen en niet de verdachte. Bovendien kan de inbeslagname van

[94] Mogelijk heeft het 'Landeck-arrest' (Hof van Justitie EU 4 oktober 2024 in zaak C-548/21) invloed hierop. In deze uitspraak heeft het Europees Hof de voorwaarden verduidelijkt waaraan politie en justitie moeten voldoen om toegang te krijgen tot gegevens op inbeslaggenomen mobiele telefoons en computers. Bij het doorzoeken van inbeslaggenomen voorwerpen is, behalve in spoedeisende gevallen, voorafgaande toetsing door de rechter-commissaris vereist. Zie ook Hoge Raad (2025).

een gehele server minder proportioneel zijn, omdat inbeslagname betekent dat alle daarop staande gegevens (zoals websites) uit de lucht worden gehaald en niet slechts de gegevens die de officier van justitie ontoegankelijk wil maken. Een andere geïnterviewde officier vertelt dat dit negatieve gevolgen kan hebben, bijvoorbeeld als op een server een deel van de ziekenhuisadministratie staat.

Een aantal geïnterviewde officieren vindt dat een officier van justitie, bijvoorbeeld wanneer het gaat om overduidelijk strafbare content zoals kinderporno, zelf in staat zou moeten zijn de ontoegankelijkmaking van gegevens te toetsen zonder tussenkomst van een rechter-commissaris. Eén van de geïnterviewde officieren van justitie merkt op dat officieren in principe opgeleid zijn om bevoegdheden af te wegen en zorgvuldig toe te passen, waarbij zij de 'opportuniteit' en 'subsidiariteit continu (…) toetsen':

> Ik ben onderdeel van de rechterlijke macht, omdat ik de bevoegdheden heb gekregen om over dit soort items te beslissen. En daarom, als ik zeg dat ik heb gewogen en dat ik het kan verantwoorden. Dan kan de politie het uitvoeren en pleegt zij geen strafbare feiten in haar uitvoering. En zo is gewoon ons systeem gebouwd. En als ik niet deug dan krijg ik heel erg op mijn donder. Dat weet ik zeker.

Een belangrijke reden voor de introductie van de rechterlijke toets, is dat met de ontoegankelijkmaking van gegevens de vrijheid van meningsuiting in het geding kan komen (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 58). Hoewel een aantal geïnterviewden de rechterlijke toets belangrijk vindt in zaken waarin ontoegankelijkmaking van gegevens mogelijk de vrijheid van meningsuiting kan inperken, zoals bij uitingsdelicten, wordt aangegeven dat de vrijheid van meningsuiting vaak niet in het geding zou zijn wanneer het gaat om gegevens die een onmiskenbaar strafbaar misdrijf opleveren (zie ook eerder). Een artikel 125p Sv-bevel kan alleen worden afgegeven in geval van verdenking van misdrijven waarvoor voorlopige hechtenis mogelijk is (art. 67 Sv), waardoor een deel van de uitingsdelicten, zoals belediging, smaad en laster, worden uitgesloten. Een enkele officier van justitie vindt een rechterlijke toets overbodig in de gevallen waarbij het gaat om gegevens die onmiskenbaar strafbare misdrijven opleveren. Bovendien, zo benadrukt een officier van justitie, is artikel 125p Sv in principe een tijdelijke maatregel is, wat betekent dat de ontoegankelijkmaking alsnog in een eindbeslissing behoort te worden getoetst. Bij dat laatste moet overigens worden opgemerkt dat lang niet alle zaken waarin artikel 125p Sv is toegepast door een zittingsrechter worden behandeld (zie ook later in dit hoofdstuk).

Verder blijkt dat sommige rechters-commissaris voorzichtiger en strikter hun toets toepassen dan andere rechters-commissaris, waardoor de mogelijkheid én de snelheid waarmee gegevens ontoegankelijk worden gemaakt enigszins afhankelijk is van de interpretatie van de rechter-commissaris. Volledige eenduidigheid in toepassing ontbreekt hierdoor. Een voorbeeld hiervan is hoe rechters-commissaris omgaan met aanbieders waarvan (al bij voorbaat) duidelijk is dat zij niet aan een verzoek van de overheid zullen meewerken. In de ene zaak (Telegram) werd een machtiging verleend zonder het horen van een aanbieder, en in de andere zaak (vals socialemedia-account) was ten tijde van het interview nog geen machtiging afgegeven, omdat de aanbieder niet kon worden gehoord.

Veel van het bovengenoemde speelt overigens niet bij de NTD-procedure. De NTD-procedure behoeft, in tegenstelling tot artikel 125p Sv, geen schriftelijke machtiging van de rechter-commissaris en vereist niet dat de aanbieder wordt gehoord. Hoewel bij een NTD-procedure de reactietijd sterk kan verschillen per aanbieder, zo geeft één van de geïnterviewden aan, wordt deze procedure doorgaans ervaren als 'sneller', aldus een andere geïnterviewde. Veel geïnterviewde medewerkers van het Openbaar Ministerie geven aan dat de meeste aanbieders vrijwillig meewerken als de politie het vraagt. Eén van hen wijst op het belang van de politie die een NTD-verzoek doet, zeker in het licht van snelheid, omdat soortgelijke verzoeken door slachtoffers soms niks opleveren.

Het horen van de aanbieder
Ook een tweede aspect van lid 4, het horen van de aanbieder, kan voor moeilijkheden zorgen in de praktijk, zo komt in interviews naar voren. Moeilijkheden doen zich voor in de volgende gevallen: 1) wanneer aanbieders niet reageren of meewerken; 2) wanneer het onduidelijk is aan wie een bevel tot ontoegankelijkmaking gericht moet worden; en 3) wanneer de aanbieder mogelijk geen betrouwbare partij is. In deze gevallen lijkt snelle ontoegankelijkmaking nagenoeg uitgesloten.

Aanbieder reageert niet of werkt niet mee

Uit een deel van de interviews komt naar voren dat aanbieders soms niet reageren of meewerken. In dat geval kan ontoegankelijkmaking langer duren of kan artikel 125p Sv zelfs 'onuitvoerbaar' zijn, zo vertellen enkele geïnterviewden. Een voorbeeld van niet willen meewerken is de eerder besproken zaak over een vals socialemedia-account van een functionaris betrokken bij de opsporing. In deze zaak weigert het socialemediaplatform het account te verwijderen en ook de rechter-commissaris krijgt hier geen contact mee. Hierdoor is het voldoen aan de hoorplicht niet mogelijk, waardoor de rechter-commissaris geen machtiging kan afgeven. Als gevolg hiervan kan artikel 125p Sv niet worden voltooid en zijn de gegevens op het valse socialemedia-account, ten tijde dat het interview werd gehouden, nog steeds zichtbaar. Om die reden zou de geïnterviewde officier van justitie graag willen dat de hoorplicht optioneel was:

> [H]ier is de grote moeilijkheid dat de rechter-commissaris de aanbieder moet horen. (…) Wij wachten al [een] week of zes op het moment, tot de rechter-commissaris iemand te pakken krijgt van dat socialemediaforum. En als dat niet lukt, kan hij niet verder. Dus ik had het liever anders gezien. Ik had liever gezien dat er had gestaan: de rechter-commissaris mag gewoon, als hij niemand te pakken krijgt, een beslissing nemen.

Een andere geïnterviewde officier vertelt dat sociale media vaak andere belangen kunnen hebben dan het beperken van content, waardoor de samenwerking met 'open social media', zoals X, YouTube en Rumble, moeizaam kan verlopen. In veel gevallen geven deze aanbieders geen gehoor aan zowel vrijwillige verzoeken als aan een artikel 125p Sv-bevel. Voornamelijk omdat deze platformen andere belangen kunnen hebben en 'helemaal niet hun content [willen] beperken', aldus deze officier van justitie. Deze geïnterviewde legt uit waarom hij strafbare content op YouTube van een Nederlandse verdachte uiteindelijk niet ontoegankelijk maakte:

> … dan krijg je eerst vijftien vragen van advocaten terug en moet je in Amerika rechtshulp verzoeken. Dat is een campagne die duurt drie jaar.

Deze officier vraagt zich dan ook af of de Nederlandse wetgever 'misschien wel te veel [is] uitgegaan van de integriteit van de telecommunicatie aanbieder' bij de totstandkoming van artikel 125p Sv. De wettekst van artikel 125p Sv gaat er namelijk van uit dat de aanbieder *kan* worden gehoord en ook *wordt gehoord,* terwijl dit in de praktijk niet altijd het geval is. Ook de NTD-procedure biedt geen uitkomst in zaken waarin de aanbieder niet meewerkt of niet reageert op de hoorplicht. Dat betekent dat er casussen overblijven waarin zowel de NTD-procedure als het nieuwe artikel 125p Sv geen uitkomst bieden.

Onduidelijkheid wie aanbieder is

Ten tweede komt uit de interviews naar voren dat het niet altijd duidelijk is wie als aanbieder moet worden beschouwd, waardoor het onduidelijk is voor wie de hoorplicht geldt. Bijvoorbeeld in situaties waarin een datacentrum servers verhuurt aan andere (soms buitenlandse) partijen, de zogenoemde *reseller*-constructie. Een datacentrum kan bijvoorbeeld in tweeën zijn gesplitst waarbij de eigenaar van een datacentrum één deel zelf beheert en het andere deel doorverhuurt aan andere (vaak buitenlandse) partijen. Meerdere geïnterviewde medewerkers van het Openbaar Ministerie vertellen dat onduidelijk is wie in zo'n geval gehoord moet worden. Een geïnterviewde officier van justitie schetst een voorbeeld van een zaak waarin een dadergroep gebruikmaakte van een Nederlandse aanbieder die servers verhuurde aan het buitenland. In deze zaak was het onmogelijk om de hurende aanbieder in het buitenland te horen, terwijl deze officier wel naar deze hurende aanbieder werd doorverwezen. Een andere geïnterviewde en tevens officier zegt het volgende over deze 'resellerproblematiek':

> Ik zou zeggen [de hoorplicht moet worden gericht aan] degene die het weg kan halen, die dus toegang heeft. In Nederland zijn dat meestal niet de datacentra zelf. (…) Dus als je (…) zou willen weten welke server moet ik kopiëren, dan zal [de aanbieder] zeggen, 'dan moet je naar mijn klant, dat is een Oekraïens of Russisch bedrijf. Zij kunnen je vertellen welke van deze stekkers verbonden is met het juiste IP-adres.' En dat probleem komen we eigenlijk steeds meer tegen.

Als alternatief zou de Nederlandse aanbieder in feite de gehele server van de buitenlandse klant, of *reseller*, ontoegankelijk kunnen maken, zo legt deze officier van justitie uit. Het nadeel hiervan is dat dit ervoor zorgt dat alle gegevens op een server ontoegankelijk worden en niet alleen de beoogde gegevens. De meest ideale situatie, volgens een geïnterviewde, is dat het Openbaar Ministerie kan samenwerken met de *reseller*. Deze laatste optie is echter alleen werkbaar indien deze klant bereikbaar is.

Aanbieder mogelijk niet betrouwbaar

Ten derde kan sprake zijn van een onbetrouwbare aanbieder, ofwel *bad hoster*, waardoor de hoorplicht problematisch kan zijn. *Bad hosters* en *bulletproof hosters* kunnen zowel het verdienmodel hebben om klanten met criminele intenties te werven als het bieden van anonimiteit aan deze klanten (Andringa, 2019; Davidse, 2023). Het komt ook voor dat deze hosting partijen eigen illegale activiteiten faciliteren op eigen servers, zoals het verspreiden van malware en het faciliteren van online kinderporno. Een geïnterviewde officier legt uit dat deze aanbieders aantrekkelijk zijn voor klanten met criminele intenties. Het biedt hen de mogelijkheid om buiten bereik van de politie te blijven. Het verschil tussen deze *bad hosters* en *bulletproof hosters* is niet altijd scherp, alhoewel de samenwerking met beide groepen over het algemeen 'heel moeizaam' gaat, aldus een andere geïnterviewde officier van justitie.

De vraag in hoeverre een aanbieder mee wil werken of betrouwbaar is, is niet altijd goed te beantwoorden. Volgens een geïnterviewde medewerker van het Openbaar Ministerie zou een aanwijzing voor onbetrouwbaarheid kunnen zijn wanneer de aanbieder in een land zit waar Nederland niet veel mee samenwerkt of een slechte relatie mee heeft. Vaak blijkt gedurende het opsporingsonderzoek in hoeverre sprake is van een *bad hoster*, zo vertelt één van de geïnterviewde officieren van justitie. Er zijn ook private entiteiten die *bad hosters* in beeld brengen. Bijvoorbeeld de zogenoemde ROKSO-lijsten[95], opgesteld door Spamhaus. Dit is een non-gouvernementele organisatie die onder andere IP-adressen, online domeinen en aanbieders geassocieerd met cybercriminaliteit opspoort en op een lijst zet (Spamhaus, z.d.).

Het horen van *bad* en *bullet proof hosters* kan een afbreukrisico zijn voor het opsporingsonderzoek. Indien de onbetrouwbare aanbieder, of 'bad hoster', voorafgaand aan de ontoegankelijkmaking wordt gehoord zou deze een klant met criminele intenties op de hoogte kunnen stellen van het politieonderzoek. Ook kunnen back-ups worden gemaakt van de gegevens in kwestie of kunnen gegevens worden gewist of verplaatst. Meerdere geïnterviewden geven aan dat zij bij voorbaat artikel 125p Sv niet inzetten, indien sprake is van een *bad hoster*. Een geïnterviewde officier van justitie vertelt over een zaak waarin artikel 125p Sv is overwogen maar om deze reden niet is ingezet:

> [Die aanbieder was] gewoon geen betrouwbare partij. Dan kun je wel zeggen 'jij moet het ontoegankelijk maken. Dit is het (…) bevel, hier heb je m'n machtiging van de rechter commissaris.' Maar ja, ga daar maar naast staan en ga maar controleren dat ze niet even ook nog een kopietje ervan maken (…) Je beveelt eigenlijk een derde partij, dus die aanbieder, om dit uit te voeren en ze zijn gewoon niet allemaal betrouwbaar.

Ook in zaken waarin sprake is van onbetrouwbare hosters biedt de vrijwillige ontoegankelijkmaking via een NTD-procedure geen uitkomst. Een geïnterviewde officier van justitie vertelt dat *bad* of *bulletproof hosters* vrijwillige verzoeken tot ontoegankelijkmaking vaak volledig negeren. Daarnaast zou het voorkomen dat deze hosters juist meewerken om betrouwbaar over te komen. Het feit dat de goede uitvoering van de ontoegankelijkmaking op basis van zowel artikel 125p Sv als de NTD-procedure grotendeels afhankelijk is van de welwillendheid van de aanbieder vormt dus een struikelblok bij dit soort aanbieders. Om die reden oordeelt de zojuist geciteerde officier van justitie dat artikel 125p Sv een 'onhandig en onwerkbaar artikel' is wanneer sprake is van een *bad* of *bulletproof hoster*.

Verschillende geïnterviewden brengen oplossingsrichtingen naar voren met betrekking tot de moeilijkheden ten aanzien van lid 4. Bijvoorbeeld de toevoeging van een spoedprocedure aan artikel 125p Sv. Deze spoedprocedure zou op verschillende manieren kunnen worden vormgegeven, zoals: 1) een procedure waarbij de aanbieder achteraf mag worden gehoord; 2) een procedure waarbij het bevel mondeling kan worden gegeven of zelfs een procedure zonder voorafgaande schriftelijke machtiging; of 3) een procedure, waarin onder voorwaarden, zoals bij 8-jaarsfeiten en dringende noodzakelijkheid, van de hoorplicht kan worden afgezien. Het achteraf horen van de aanbieder kan bijvoorbeeld uitkomst bieden indien sprake is van *bad* of *bullet proof hosters*, zodat zij hun klant niet van tevoren zullen inlichten. Daarnaast zouden

[95] ROKSO is een afkorting voor Register of Known Spam Operations. Deze lijsten zijn niet meer openbaar, maar Spamhaus werkt op dit moment aan een nieuw alternatief (Spamhaus, z.d.).

maatregelen kunnen worden genomen die de verantwoordelijkheid van aanbieders vergroten. Eén van de geïnterviewde officieren van justitie merkt op dat hun verantwoordelijkheid op dit moment 'vrijwel nul' is. Een suggestie die naar voren komt in de interviews is de invoering van een vergunningstelsel, één die aanbieders verplicht om te weten wie hun klanten zijn, een zogenoemde '*know your customer*'-clausule. In een brandbrief ondertekend door onder andere de burgemeester van Amsterdam en de politie wordt eveneens aangedrongen op een 'ken je klant'-verplichting: de briefschrijvers vinden dat aanbieders moeten worden verplicht 'om hun klanten bij registratie om persoonsgegevens te vragen' (Rensen, 2025). Een andere geïnterviewde medewerker van het Openbaar Ministerie geeft aan dat de overkoepelende organisatie van hostingbedrijven (MIBB) maatregelen zou kunnen nemen. Bijvoorbeeld dat een 'hostingpartij uit de beroepsvereniging gezet wordt' indien deze aanbieder met zijn servers criminaliteit faciliteert. Deze geïnterviewde noemt nog een aantal andere alternatieven, zoals bestuurlijke boetes en het volledig weren van *bad* en *bulletproof hosters* in Nederland.

Hoofdpunten

- Voor de opsporingspraktijk is de toets door de rechter-commissaris, voorafgaand aan de inzet van artikel 125p Sv en vastgelegd in lid 4 van het artikel, een belangrijk aandachtspunt. Deze toetsing kan voor moeilijkheden zorgen in de opsporingspraktijk, vooral in zaken waarin spoed geboden is. Het alternatief is dat overgegaan wordt op andere bevoegdheden die minder procedurele eisen hebben, maar wel ingrijpender kunnen zijn, zoals een doorzoeking (art. 125o Sv) en inbeslagname (art. 94a Sv) van de gehele server.
- De toets door de rechter-commissaris is geïntroduceerd vanwege de vrijheid van meningsuiting die in het geding kan zijn. Wat de opsporingspraktijk betreft is in 125p-zaken meestal sprake van onmiskenbare strafbare content. In dat soort zaken zou ontoegankelijkmaking gemakkelijk mogelijk moeten zijn. Bovendien komen strafbare feiten, waarbij de vrijheid van meningsuiting in het geding is, zoals smaad en laster, niet in aanmerking voor een 125p-bevel, vanwege het voorlopige hechtenis-criterium.
- Eén van de onderdelen uit lid 4 die als problematisch wordt gezien is het horen van de aanbieder, voorafgaand aan het afgeven van de machtiging. Hiervoor zijn drie redenen: 1) aanbieders werken lang niet altijd mee; 2) het kan onduidelijk zijn wie de aanbieder is; en 3) een aanbieder is mogelijk niet betrouwbaar. Ook een NTD-verzoek voldoet niet altijd.
- Vanuit de opsporingspraktijk is een aantal oplossingsrichtingen geformuleerd: 1) de mogelijkheid voor een alternatieve toestemmingsprocedure, zoals horen achteraf, alvast een mondelinge machtiging afgeven of de mogelijkheid om onder voorwaarden volledig af te kunnen zien van de hoorplicht; 2) maatregelen vanuit overkoepelende organisaties en de overheid die de verantwoordelijkheid van aanbieders vergroten, bijvoorbeeld een vergunningstelsel waarin aanbieders verplicht worden om te weten wie hun klanten zijn; 3) invoering van bestuurlijke boetes en 4) het weren van *bad* en *bulletproof hosters*.

Tijdelijke maatregel

Artikel 125p Sv is in principe een tijdelijke maatregel, wat betekent dat een zittingsrechter over de definitieve ontoegankelijkmaking van gegevens moet beslissen. In de interviews komt naar voren dat zaken waarin artikel 125p Sv is ingezet niet altijd door een zittingsrechter worden behandeld. Zo is het vervolgen van een verdachte niet altijd het doel van een opsporingsonderzoek, bijvoorbeeld wanneer het opsporingsonderzoek een ander doel dient dan vervolging van een verdachte of

wanneer vervolging van de verdachte niet mogelijk is. Soms kan een verdachte niet worden vervolgd, bijvoorbeeld wanneer de identiteit van de verdachte onbekend is of enkel een *nickname* bekend is. Ook kan het zijn dat verdachten verblijven in het buitenland of in landen waarmee Nederland geen rechtshulprelatie heeft waardoor niet kan worden vervolgd. Dat een zittingsrechter zich niet over de zaak zal buigen, is volgens een geïnterviewde officier van justitie kenmerkend voor zaken in het cyberdomein. Eerder WODC-onderzoek liet zien dat 'opsporing en vervolging van misdrijven', bij cybercriminaliteit lastig is, omdat dit fenomeen vaak de grenzen overschrijdt (Van den Eeden et al., 2021, p. 15). In dit geval kan 'brede bestrijding', meer specifiek 'verstoring', het doel zijn, zo vertelt een andere officier van justitie. Het gevolg is dat er in die zaken geen eindbeslissing van een zittingsrechter komt over definitieve ontoegankelijkmaking, waardoor deze gegevens in feite 'eindeloos lang' bij de politie in beheer blijven, aldus deze geïnterviewde. Deze officier van justitie legt uit dat artikel 125p Sv soms niet wordt gebruikt, omdat de ontoegankelijk gemaakte gegevens dan 'strikt juridisch' weer online moeten komen na de afronding van het onderzoek. Een mogelijke oplossingsrichting om definitieve ontoegankelijkmaking te effectueren zou mogelijk zijn via een raadkamerprocedure, zo geeft een aantal geïnterviewden aan. Deze raadkamerprocedure is neergelegd in artikel 552fa Sv.[96] Op dit moment ontbreekt in dit artikel een verwijzing naar artikel 125p Sv, wat de vraag oproept of de wetgever de toevoeging van artikel 125p Sv aan artikel 552fa Sv misschien over het hoofd heeft gezien. In het nieuwe Wetboek van Strafvordering, dat op 1 april 2029 in werking zal treden, staat in elk geval een artikel met betrekking tot een raadkamerprocedure voor de vernietiging van 'ontoegankelijk gemaakte gegevens'. Daarin staat overigens geen verwijzing naar specifieke bevoegdheden (*Kamerstukken II 2022/23,* 34 327, nr. 2, p. 240).[97] De raadkamer beslist over verzoeken die worden ingediend door de officier van justitie, verdachten of belanghebbenden. Door middel van een raadkamerprocedure kan bijvoorbeeld over verzoeken omtrent de teruggave van inbeslaggenomen goederen worden beslist (De Rechtspraak, z.d.).

Hoofdpunten

- Niet alle zaken waarin gebruikgemaakt is van artikel 125p Sv zullen worden voorgelegd aan een zittingsrechter. In dat geval volgt geen beslissing over definitieve ontoegankelijkmaking. Dit kan aan de orde zijn wanneer het vervolgen van een verdachte niet het doel is van het opsporingsonderzoek.
- Vervolging van een verdachte is niet altijd mogelijk, bijvoorbeeld wanneer de identiteit van de dader niet kan worden achterhaald of wanneer verdachten verblijven in landen waarmee Nederland geen rechtshulprelatie heeft.
- Een mogelijke oplossingsrichting is dat definitieve ontoegankelijkmaking via een Raadkamerprocedure wordt geregeld.

Zaken met een internationale component

Het komt voor dat een aanbieder of eigenaar van gegevens in het buitenland verblijft. Het buitenlandaspect kan op verschillende manieren naar voren komen in zaken waarin opsporingsinstanties gegevens ontoegankelijk willen maken:

- Buitenlandse groeperingen met criminele intenties die online infrastructuur, zoals *ransomware* en botnets, op servers in Nederland hebben staan, plegen strafbare feiten met Nederlandse en buitenlandse slachtoffers.

[96] Op grond van het huidige artikel 552fa Sv kan een officier van justitie een vordering indienen om ontoegankelijk gemaakte gegevens op grond van artikelen 125o of 126cc lid 5 Sv te vernietigen.
[97] Zie artikel 6.4.13 van dit wetsvoorstel.

- Nederlandse servers kunnen worden beheerd vanuit het buitenland, waardoor sprake kan zijn van buitenlandse aanbieders.
- Gegevens kunnen verspreid staan over verschillende servers, waarvan één of meerdere servers in het buitenland staan.

De genoemde buitenlandcomponenten kunnen op verschillende manieren ontoegankelijkmaking belemmeren. Een aantal punten passeerden eerder al de revue. Deze worden daarom kort genoemd, waarna een aantal nieuwe punten wordt besproken.

Wanneer een zaak een buitenlandse verdachte kent, volstaat de tijdelijke aard van artikel 125p Sv meestal niet. Verdachten worden in die gevallen niet altijd vervolgd, terwijl definitieve ontoegankelijkmaking zoals gezegd behoort te geschieden in een einduitspraak door de rechter. Daarnaast kunnen buitenlandse aanbieders slecht bereikbaar zijn voor de hoorplicht. Dit kan spoedige ontoegankelijkmaking in de weg staan, zo merkt één van de geïnterviewde officieren van justitie op. Een andere aspect dat spoedige ontoegankelijkmaking kan belemmeren en dat nog niet besproken is, zijn de procedures wanneer gewerkt wordt met rechtshulpverzoeken. Indien Nederlandse opsporingsinstanties hulp willen van het buitenland, dan moeten zij een rechtshulpverzoek indienen. Andersom geldt die verplichting ook. Voorbeelden van zaken waarbij dit speelde zijn een zaak waarin een buitenlands bedrijf was gehackt en waarbij de data naar een Nederlandse server waren gesluisd en een zaak waarin *ransomware* en botnets van buitenlandse criminelen werden gehost op servers in Nederland. Doorgaans neemt het werken via rechtshulpverzoeken veel tijd in beslag, zowel als Nederland een verzoek doet als wanneer het buitenland een verzoek doet, zo merkt een andere geïnterviewde officier van justitie op. Vertraging van de afhandeling van rechtshulpverzoeken kan hem zitten in de wijze waarop in het betreffende land wordt omgegaan met ontoegankelijkmaking of in de rechtshulprelatie die landen met elkaar hebben, zo merkt een aantal geïnterviewden, werkzaam bij het Openbaar Ministerie, op. Een concreet voorbeeld van een algemene casus waarin een rechtshulpverzoek ontoegankelijkmaking kan vertragen betreft verzoeken die gedaan moeten worden bij grote internationale technologie- en internetbedrijven, zoals Google. Deze werken niet automatisch mee aan een verzoek van het Nederlandse Openbaar Ministerie, zo legt één van de eerder aangehaald officier van justitie uit.[98] Google beschikt over een datacentrum in Nederland waarin veel informatie van zowel Nederlanders als Europeanen staat opgeslagen. Als een opsporingsteam informatie van die servers wil halen, kunnen zij niet rechtstreeks naar het Nederlandse datacentrum gaan, maar moeten rechtshulpverzoeken, via Amerika naar Ierland, worden gestuurd. Google Ierland beheert de servers in Nederland. Het 'snel' of 'terstond' ontoegankelijk maken van gegevens is dus vrijwel onmogelijk als het element buitenland betrokken is, zo merken twee geïnterviewden, werkzaam bij het Openbaar Ministerie, op. Alhoewel niet altijd mogelijk, komt het in dit soort situaties aan op alternatieven voor artikel 125p Sv, zoals wettelijke bevoegdheden als 'de netwerkzoeking' (art. 125o Sv), zoals eerder besproken, de Innovatiewet[99] en 'het direct inloggen op een [Google] account van de verdachte', aldus een eerder aangehaalde officier van justitie. Deze

[98] In één van de interviews met een officier van justitie komt naar voren dat Microsoft de bedrijfsvoering zo zou hebben ingericht dat verzoeken tot ontoegankelijkmaking door een advocatenkantoor worden ontvangen. Ook zouden deze verzoeken momenteel vrijwel altijd genegeerd worden op basis van administratieve redenen. Wanneer deze verzoeken wel worden behandeld, volgt een doorverwijzing naar Ierland.

[99] Op basis van deze wet (artikelen 556 en 558 Sv) kan een officier van justitie, na een machtiging van de rechter-commissaris, van gegevens op inbeslaggenomen geautomatiseerde werken kennisnemen en vastleggen. Bij dringende noodzaak kan het bevel ook mondeling worden gegeven. De ontoegankelijkmaking van gegevens wordt niet expliciet genoemd in deze artikelen.

officier merkt op dat bedrijven als Google meer verantwoordelijkheid zouden moeten nemen.

Een oplossingsrichting die naar voren komt, en die door deze officier van justitie wordt genoemd, is het creëren van meer eenduidigheid in wet- en regelgeving. Zo zouden buitenlandse bedrijven, die geld verdienen in Nederland, moeten kunnen vallen onder de in Nederland geldende wet- en regelgeving. Verder zou de Europese dan wel Nederlandse wetgever meer duidelijkheid kunnen verschaffen over wat verwacht zou moeten worden van aanbieders die geld in Europa verdienen. Bovendien kunnen zowel Europese als internationale initiatieven en samenwerkingen hierbij uitkomst bieden. Deze geïnterviewde officier zou graag betere internationale samenwerking zien tussen overheden en aanbieders en de mogelijkheid krijgen om zonder rechtshulpverzoek met een buitenlands bedrijf te kunnen communiceren ten aanzien van vorderingen zoals in het kader van artikel 125p Sv. Het inlichten van de buitenlandse autoriteiten zou dan voldoende kunnen zijn.

Vrijwillige verzoeken tot ontoegankelijkmaking zijn doorgaans wel mogelijk zonder rechtshulpverzoek. Geïnterviewde medewerkers van het Openbaar Ministerie vertellen dit soort vrijwillige verzoeken vaak sneller en beter werkbaar zijn dan artikel 125p Sv. Dit geldt doorgaans alleen voor de zaken waarin sprake is van een betrouwbare en bereikbare buitenlandse aanbieder.

Hoofdpunten

- Zaken waarin de ontoegankelijkmaking van gegevens gewenst is kunnen een buitenlandcomponent bevatten. Deze buitenlandcomponent kan een belemmering zijn voor (snelle) ontoegankelijkmaking van gegevens, zeker wanneer geen sprake is van een vrijwillig verzoek tot ontoegankelijkmaking. Een reden hiervoor is dat gewerkt moet worden met rechtshulpverzoeken en dat kost relatief veel tijd.
- Een mogelijke oplossingsrichting is het creëren van meer eenduidigheid in wet- en regelgeving, bijvoorbeeld dat buitenlandse aanbieders onder nationale regelgeving vallen.

6.4 Tot slot

Dit hoofdstuk heeft laten zien dat de bevoegdheid om gegevens ontoegankelijk te maken op basis van artikel 125p Sv in 14 zaken is ingezet. Het betrof de ontoegankelijkmaking van onder andere Telegramkanalen en -accounts, websites en IP-adressen. Wat opvalt aan deze gevallen is dat in drie zaken de rechter-commissaris toestemming heeft gegeven voor toepassing naar analogie van artikel 125p Sv (art. 181 jo. art. 125p Sv). In deze zaken heeft de rechter-commissaris geen aanbieder gehoord, omdat de veronderstelling was dat deze niet zou meewerken. In plaats daarvan kreeg de politie de opdracht om gegevens ontoegankelijk te maken. In de praktijk is het dus mogelijk gebleken om met behulp van de bevoegdheid, al dan niet middels een toepassing naar analogie van artikel 125p Sv, gegevens ontoegankelijk te maken, waarbij dat in veel gevallen op een andere manier niet lukte. Bovendien is duidelijk geworden dat de verplaatsing van de bevoegdheid om gegevens ontoegankelijk te maken naar het Wetboek van Strafvordering in sommige gevallen wordt ervaren als een verbetering en een verduidelijking van de bevoegdheid. Beide aspecten kwamen ook naar voren in de veronderstellingen van de wetgever.

Tegelijkertijd is duidelijk geworden dat er zaken zijn waarin een inzet van artikel 125p Sv niet nodig is. In de meeste zaken zouden aanbieders meer dan bereid zijn om gehoor te geven aan een vrijwillig Notice-and-Take-Downverzoek. Voor deze evaluatie hebben wij helaas geen zicht kunnen krijgen op het aantal zaken waarin dit het geval was. Er zijn ook zaken waarin noch de NTD-procedure, noch artikel 125p Sv uitkomst kon bieden. Meestal wordt in die gevallen gekozen voor alternatieven, zoals de inbeslagname en de netwerkdoorzoeking. Dit zijn belangrijke nuanceringen bij de veronderstellingen van de wetgever.

Een belangrijke reden waarom artikel 125p Sv niet altijd goed toepasbaar is, heeft te maken met de rechterlijke toets in lid 4 van artikel 125p Sv. Dit lid regelt dat een rechter-commissaris, voorafgaand aan de ontoegankelijkmaking, een schriftelijke machtiging moet afgeven én dat de rechter-commissaris voorafgaand aan de afgifte van de machtiging de aanbieder moet horen. Beide stappen kunnen veel tijd in beslag nemen, wat voor moeilijkheden kan zorgen in de opsporingspraktijk. In deze evaluatie is duidelijk geworden dat het nodig kan zijn gegevens snel ontoegankelijk te maken, bijvoorbeeld om te voorkomen dat afbeeldingen met kinderporno nog verder verspreid worden, of dat gestolen gegevens verder gedeeld worden. In de wetstekst (lid 2) is opgenomen dat 'terstond alle maatregelen' moeten worden genomen om gegevens ontoegankelijk te maken. Dat wekt de suggesties dat snel handelen mogelijk moet zijn. In de praktijk blijkt dat laatste te botsen met de duur van het toetsingsproces door een rechter-commissaris (lid 4). Dat is opvallend, omdat die toets juist geïntroduceerd is om relatief snel, namelijk sneller dan wanneer een zittingsrechter een oordeel velt, gegevens ontoegankelijk te kunnen maken. Dit laat zien dat de tweede veronderstelling van de wetgever, het relatief snel ontoegankelijk maken van gegevens, nuancering behoeft. De praktijk laat zien dat een schriftelijke machtiging veel tijd in beslag kan nemen, tijd die er in de praktijk niet altijd is. Het tijdsaspect speelt ook een rol bij het horen van de aanbieder, een ander belangrijk aspect van lid 4. Ook de hoorplicht kan veel tijd in beslag nemen. Er zijn echter nog een aantal andere moeilijkheden met betrekking tot de hoorplicht. Zo zijn niet alle aanbieders bereid om mee te werken, is het niet altijd duidelijk wie als aanbieder moet worden gezien, bijvoorbeeld in het geval van een buitenlandse aanbieder, en blijken sommige aanbieders onbetrouwbaar. Dat laatst vormt een afbreukrisico voor het opsporingsonderzoek en daarmee voor het kunnen beëindigen of voorkomen van strafbare feiten. In deze evaluatie is een aantal oplossingsrichtingen naar voren gekomen wat betreft de medewerking van de aanbieder, namelijk: 1) maatregelen vanuit overkoepelende organisaties en de overheid die de verantwoordelijkheid van aanbieders vergroten, bijvoorbeeld een vergunningstelsel waarin aanbieders verplicht worden om te weten wie hun klanten zijn; 2) invoering van bestuurlijke boetes en 3) het weren van *bad* en *bulletproof hosters*.

Een schriftelijke toets door de rechter-commissaris is destijds ook geïntroduceerd, omdat artikel 125p Sv een ingrijpende bevoegdheid is. De vrijheid van meningsuiting kan immers in het gedrang komen. Opvallend is dat in zaken waarin gegevens ontoegankelijk moeten worden gemaakt op basis van artikel 125p Sv, en die in deze evaluatie aan bod zijn gekomen, het vaak zou gaan om onmiskenbaar illegale activiteiten. Denk bijvoorbeeld aan kinderporno, gehackte persoonsgegevens of een website die gebruikt wordt voor illegale handel. Dit zijn doorgaans geen feiten waarbij er discussie bestaat of de vrijheid van meningsuiting voorrang zou moeten krijgen op strafrechtelijk ingrijpen. Bovendien geldt voor een deel van de feiten waarbij de vrijheid van meningsuiting wel in het gedrang kan komen, denk aan een uitingsdelict als smaad, dat deze niet in aanmerking komen voor artikel 125p Sv. Dit alles neemt

niet weg dat er artikel 125p Sv-verzoeken kunnen komen, bijvoorbeeld ten aanzien van andere uitingsdelicten, die wel de vrijheid van meningsuiting kunnen beknotten, of waarbij dat een discussiepunt is. Gedegen toetsing van die verzoeken blijft belangrijk, omdat de vraag of een bepaalde uiting strafbaar is niet altijd gemakkelijk te beantwoorden is. Bovendien kan het zijn dat de vrijheid van meningsuiting moet prevaleren boven de mogelijke strafbaarheid van een uiting (Oerlemans et al., 2025, p. 161). Om die reden blijft een zorgvuldige toetsingsprocedure, een belangrijke pijler van de rechtsstaat, aangewezen. Voor de gevallen waarin uitgesloten is dat de vrijheid van meningsuiting in het geding is, kan worden gekeken of er meer variatie kan komen wat betreft de wijze waarop een rechter-commissaris toetst. Bijvoorbeeld de mogelijkheid voor een alternatieve toestemmingsprocedure. Uit de memorie van toelichting (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 97) volgt al dat de rechter-commissaris af kan zien van het horen van de aanbieder. Een mogelijk scenario is om dit mee te nemen in de wetstekst zelf.

Een ander belangrijk aandachtspunt tot slot is de mix van bestuursrechtelijke, civielrechtelijke en strafrechtelijke mogelijkheden die er is om gegevens ontoegankelijk te maken. Deze evaluatie heeft zich vooral gericht op de strafrechtelijke component. Het zou mooi zijn om tot een goed overzicht te komen welke optie voor welke situatie de meest wenselijke is, én dat daarbij nieuwe mogelijkheden worden betrokken die er sinds de inwerkingtreding van de Wet CCIII bijgekomen zijn zoals die van de Autoriteit online Terroristisch en Kinderpornografisch Materiaal.

7 Hackbevoegdheid (artt. 126nba, 126zpa en 126uba Sv)[100]

In dit hoofdstuk wordt ingegaan op de hackbevoegdheid (artt. 126nba, 126zpa en 126uba Sv). In september 2022 publiceerde het WODC (Van Uden & Van den Eeden, 2022) al een evaluatie van de hackbevoegdheid waarin vooral werd ingegaan op de uitvoering van de hackbevoegdheid aan de technische kant. Ook werd daarin gekeken naar de waarborgen die ervoor moeten zorgen dat de hackbevoegdheid op een zorgvuldige manier wordt ingezet en dat de gegevens die de politie met behulp van de hackbevoegdheid verzamelt betrouwbaar, integer en herleidbaar zijn. In deze evaluatie en in dit hoofdstuk ligt de nadruk op de tactische kant van de bevoegdheid, en vooral de vraag wat gegevens verzameld met de hackbevoegdheid opleveren binnen een tactisch opsporingsonderzoek. Dat neemt niet weg dat ook in dit hoofdstuk kort zal worden stilgestaan bij de hoofdpunten die in de eerdere evaluatie werden gesignaleerd. Deze terugblik volgt aan het einde van het hoofdstuk.

Dit hoofdstuk is als volgt opgebouwd. Allereerst wordt het juridisch kader van deze bevoegdheid uiteengezet (paragraaf 7.1). Vervolgens wordt de noodzaak (volgens de wetgever) besproken, alsmede de veronderstellingen die aan de bevoegdheid ten grondslag liggen (paragraaf 7.2). Daarna wordt ingegaan op de wijze waarop de hackbevoegdheid in de praktijk is benut (paragraaf 7.3). Er wordt onder andere aandacht besteed aan de aard van de zaken, bijvoorbeeld het soort misdrijven waarop de opsporingsonderzoeken zich richtten waarin de hackbevoegdheid is ingezet (paragraaf 7.3.1), de voordelen die de hackbevoegdheid kan hebben voor de opsporingspraktijk (paragraaf 7.3.4) en de aandachtspunten van de nieuwe bevoegdheid (paragraaf 7.3.5). Daarna volgt de al aangekondigde terugblik op de belangrijkste aandachtspunten in de eerdere evaluatie en de beleidsreactie die daarop volgde van de toenmalig Minister van Justitie en Veiligheid (paragraaf 7.4). Deze paragraaf heeft een wat andere invalshoek dan de rest van het hoofdstuk. De nadruk in deze paragraaf ligt niet zozeer op de veronderstellingen van de wetgever met betrekking tot de hackbevoegdheid en wat daarvan terecht is gekomen, maar op de in een eerdere evaluatie gesignaleerde aandachtspunten. Om hier uitspraken over te kunnen doen, is een aantal update-interviews gehouden. Het hoofdstuk besluit met een paragraaf waarin de door de wetgever beoogde doelstelling en veronderstellingen worden vergeleken met de praktijk (paragraaf 7.5).

7.1 Juridisch kader

Met de introductie van de Wet CCIII) heeft de hackbevoegdheid een grondslag gekregen in het Wetboek van Strafvordering (artt. 126nba, 126uba en 126zpa Sv). Het nieuwe wetsartikel luidt als volgt[101]:

[100] In het eerste deel van het hoofdstuk is deels gebruikgemaakt van teksten uit de eerdere WODC-evaluatie (Van Uden & Van den Eeden, 2022).

[101] Artikelen 126uba en 126zpa Sv wijken op kleine punten af van artikel 126nba Sv. Artikel 126uba Sv kan worden ingezet bij opsporingsonderzoeken naar het beramen of plegen van ernstige misdrijven in georganiseerd verband. Artikel 126zpa Sv bij de opsporing van terroristische misdrijven. Ten behoeve van de overzichtelijkheid wordt in dit hoofdstuk alleen artikel 126nba Sv volledig uitgewerkt.

1 In geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, dat gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert, kan de officier van justitie, indien het onderzoek dit dringend vordert, bevelen dat een daartoe aangewezen opsporingsambtenaar binnendringt in een geautomatiseerd werk dat bij de verdachte in gebruik is en, al dan niet met een technisch hulpmiddel, onderzoek doet met het oog op:
   a de vaststelling van bepaalde kenmerken van het geautomatiseerde werk of de gebruiker, zoals de identiteit of locatie, en de vastlegging daarvan;
   b de uitvoering van een bevel als bedoeld in de artikelen 126l of 126m;
   c de uitvoering van een bevel als bedoeld in artikel 126g, waarbij de officier van justitie kan bepalen dat ter uitvoering van het bevel een technisch hulpmiddel op een persoon wordt bevestigd;

   en, ingeval van een misdrijf, waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaren of meer is gesteld, dan wel een misdrijf dat bij algemene maatregel van bestuur is aangewezen;
   d de vastlegging van gegevens die in het geautomatiseerde werk zijn opgeslagen, of die eerst na het tijdstip van afgifte van het bevel worden opgeslagen, voor zover redelijkerwijs nodig om de waarheid aan de dag te brengen;
   e de ontoegankelijkmaking van gegevens, bedoeld in artikel 126cc, vijfde lid. Artikel 11.7a van de Telecommunicatiewet is niet van toepassing op handelingen ter uitvoering van een bevel als bedoeld in de eerste volzin.
2 Het bevel, bedoeld in het eerste lid, is schriftelijk en vermeldt:
   a het misdrijf en indien bekend de naam of anders een zo nauwkeurig mogelijke aanduiding van de verdachte;
   b zo mogelijk een nummer of een andere aanduiding waarmee het geautomatiseerde werk kan worden geïdentificeerd en, indien bekend, dat de gegevens niet in Nederland zijn opgeslagen;
   c de feiten of omstandigheden waaruit blijkt dat de voorwaarden, bedoeld in het eerste lid, zijn vervuld;
   d een aanduiding van de aard en functionaliteit van het technische hulpmiddel, bedoeld in het eerste lid, dat wordt gebruikt voor de uitvoering van het bevel;
   e het onderdeel of de onderdelen, genoemd in het eerste lid, met het oog waarop het bevel wordt gegeven en, als dit het onderdeel a, d of e betreft, een duidelijke omschrijving van de te verrichten handelingen;
   f ten aanzien van welk deel van het geautomatiseerde werk en welke categorie van gegevens aan het bevel uitvoering wordt gegeven;
   g het tijdstip waarop, of de periode waarbinnen aan het bevel uitvoering wordt gegeven;
   h in het geval het een bevel, bedoeld in het eerste lid, onderdeel c, betreft, een melding van het voornemen om een technisch hulpmiddel op een persoon te bevestigen.
3 Het bevel, bedoeld in het eerste lid, wordt gegeven voor een periode van ten hoogste vier weken. Het kan telkens voor een periode van ten hoogste vier weken worden verlengd.
4 Het bevel, bedoeld in het eerste lid, kan slechts worden gegeven na schriftelijke machtiging op vordering van de officier van justitie te verlenen door de rechter-commissaris. De machtiging vermeldt de onderdelen van het bevel en de periode waarvoor de machtiging van kracht is.
5 Het bevel, bedoeld in het eerste lid, kan schriftelijk en met redenen omkleed worden gewijzigd, aangevuld, verlengd of beëindigd, met dien verstande dat de officier van justitie voor wijziging, aanvulling of verlenging een machtiging van de

rechter-commissaris behoeft. Bij dringende noodzaak kunnen de beslissing van de officier van justitie en de machtiging van de rechter-commissaris mondeling worden gegeven. De officier van justitie en de rechter-commissaris stellen deze in dat geval binnen drie dagen op schrift.

6 Nadat het onderzoek is beëindigd wordt het technische hulpmiddel verwijderd. Indien het technische hulpmiddel niet of niet volledig kan worden verwijderd en dit risico's oplevert voor het functioneren van het geautomatiseerde werk stelt de officier van justitie de beheerder van het geautomatiseerde werk daarvan in kennis en stelt de nodige informatie ter beschikking ten behoeve van de volledige verwijdering. Het bepaalde in artikel 126cc, eerste lid, is van overeenkomstige toepassing.

7 Het toezicht op de uitvoering van het bevel, bedoeld in het eerste lid, door de ambtenaren, bedoeld in artikel 141, onderdeel d, en de personen, bedoeld in artikel 142, eerste lid, onderdeel b, wordt uitgeoefend door de inspectie, bedoeld in artikel 65 van de Politiewet 2012, overeenkomstig het bepaalde in hoofdstuk 6 van de Politiewet 2012.

8 Bij of krachtens algemene maatregel van bestuur worden regels gesteld omtrent:
   a de autorisatie en deskundigheid van de opsporingsambtenaren die kunnen worden belast met het binnendringen en het onderzoek, bedoeld in het eerste lid, en de samenwerking met andere opsporingsambtenaren;
   b de geautomatiseerde vastlegging van gegevens over de uitvoering van het bevel, bedoeld in het eerste lid.

9 Bij algemene maatregel van bestuur kunnen regels worden gesteld over de toepassing van de bevoegdheid, bedoeld in het eerste lid, in de gevallen waarin niet bekend is waar de gegevens zijn opgeslagen.

Samenvattend maken de nieuwe bepalingen het mogelijk dat opsporingsambtenaren, 'onder voorwaarden een geautomatiseerd werk, dat bij een verdachte in gebruik is, op afstand heimelijk [kunnen] binnendringen met het oog op bepaalde doelen op het gebied van de opsporing van ernstige strafbare feiten'. Na het binnendringen van een geautomatiseerd werk (bijvoorbeeld een telefoon of een server) mag de politie een beperkt aantal onderzoekshandelingen verrichten, namelijk a) de vaststelling van bepaalde kenmerken van het geautomatiseerd werk of van de gebruiker, zoals de identiteit of locatie, en de vastlegging daarvan; b) de uitvoering van een bevel tot het opnemen van vertrouwelijke communicatie of het aftappen en opnemen van telecommunicatie; c) de uitvoering van een bevel tot stelselmatige observatie; d) de vastlegging van gegevens die in het geautomatiseerd werk zijn of worden opgeslagen; en e) de ontoegankelijkmaking van gegevens. Deze handelingen mogen alleen worden verricht door speciaal daartoe aangewezen opsporingsambtenaren die onderdeel uitmaken van een specialistisch team van de Nationale Politie. Op het moment van het schrijven van dit evaluatierapport (juni 2025) is de uitvoering van de hackbevoegdheid ondergebracht bij de Eenheid landelijke expertise en operaties (LX). De Wet CCIII kent verder een aantal grondslagen om bij of krachtens Algemene Maatregel van Bestuur regels te stellen met betrekking tot de uitvoering van de hackbevoegdheid. Dat is bijvoorbeeld gebeurd in het Besluit onderzoek in een geautomatiseerd werk (hierna Besluit).

7.2 Noodzaak en veronderstellingen

In de memorie van toelichting wordt duidelijk dat de hackbevoegdheid een oplossing moet bieden voor het feit dat opsporingsinstanties niet goed meer in staat zijn om computercriminaliteit en andere vormen van ernstige criminaliteit aan te pakken (*Kamerstukken II* 2015/16 34 372, nr. 3). Een belangrijke reden hiervoor is dat de bestaande (bijzondere) opsporingsbevoegdheden niet altijd bruikbaar zijn om de in een opsporingsonderzoek benodigde gegevens te verzamelen (*Kamerstukken II* 2015/16 34 372, nr. 3, p. 7-13).[102] Hieraan ligt een aantal oorzaken ten grondslag waarvan de opkomst van nieuwe technologische ontwikkelingen de meeste aandacht krijgt in de memorie van toelichting. Drie technologische ontwikkelingen worden genoemd: versleuteling, draadloze netwerken en *cloud computing (Kamerstukken II* 2015/16 34 372, nr. 3, p. 7-13*)*.

7.2.1 Technologische ontwikkelingen

Versleuteling van gegevens, ook wel encryptie, betekent dat met behulp van een wiskundig algoritme leesbare data zodanig worden omgevormd dat ze niet meer leesbaar zijn (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 7). Zowel individuele gegevensbestanden als bijvoorbeeld een gehele harde schijf kunnen op eenvoudige wijze worden versleuteld. Versleuteling is mogelijk, zo blijkt uit de memorie van toelichting, van vastgelegde gegevens (zoals een harde schijf) én van stromende gegevens[103] (zoals communicatie via WhatsApp) (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 8).

De tweede ontwikkeling is het toenemende gebruik van draadloze netwerken om toegang te krijgen tot het internet (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 10). In de memorie van toelichting wordt uitgelegd dat draadloze netwerken, ook wel wifi-netwerken, op veel plaatsen aanwezig zijn, bijvoorbeeld in huis, hotspots op straat, in het openbaar vervoer en in horecagelegenheden. Een individuele internetgebruiker benut doorgaans in een week tijd, of zelfs op één dag, meerdere netwerken en daarvoor gebruikt hij of zij meerdere toegangspunten (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 10). Beide ontwikkelingen zorgen ervoor dat reeds bestaande bevoegdheden niet goed bruikbaar zijn. Een voorbeeld hiervan is de tap. Middels het plaatsen van een telefoon-, e-mail- of internettap (artt. 126m, 126t en 126zg Sv) kan communicatie afgetapt en opgenomen worden. Indien communicatie wordt versleuteld, dan zijn deze (bijzondere) opsporingsbevoegdheden[104] niet bruikbaar. Opsporingsinstanties kunnen zien dat communicatie plaatsvindt, maar zij zijn niet in staat om de inhoud ervan te achterhalen, zo blijkt uit de memorie van toelichting (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 9).

Ook het gebruik van draadloze netwerken zorgt ervoor dat het bestaande tappen (de internettap) niet meer goed bruikbaar is (*Kamerstukken II* 2015/16, 34 372, nr. 3, p.

[102] Er wordt nog een andere reden genoemd, maar deze reden komt veel beperkter aan bod, namelijk dat de bestaande bevoegdheden niet altijd proportioneel zijn (o.a. *Kamerstukken II* 2015/16 34 372, nr. 3, p. 10).

[103] Opgeslagen gegevens zijn gegevens die staan opgeslagen in een computer. Stromende gegevens zijn gegevens 'die in een proces zijn van verwerking of overdracht tussen computers' (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 18). Koops & Oerlemans (2019, p. 118) maken onderscheid tussen 'reeds bestaande (opgeslagen) gegevens' en 'niet reeds ergens vastgelegde gegevens'.

[104] De telefoontap wordt in de memorie van toelichting genoemd, maar de problemen die worden geschetst hebben betrekking op de internet- en de e-mailtap. Er is wel een ander probleem met betrekking tot de telefoontap, namelijk dat de inzet hiervan steeds minder effectief is, omdat gebruik wordt gemaakt van alternatieve communicatiemiddelen (Odinot & De Jong, 2012, p. 10). Dit wordt overigens niet expliciet genoemd in de memorie van toelichting.

10). Eén van de redenen is dat een tapbevel per toegangspunt tot het internet wordt afgegeven. Op het moment dat meerdere toegangspunten in het spel zijn, betekent dit dat meerdere taps moeten worden geplaatst (bij elke netwerk- en dienstenaanbieder een tap). Dat is praktisch niet werkbaar vanwege de grote hoeveelheid data die verzameld wordt. Hierdoor wordt het moeilijker om volledig zicht te krijgen op de communicatie van een verdachte (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 10).

De derde ontwikkeling is *cloud computing*. In de memorie van toelichting wordt uitgelegd dat veel bedrijven en burgers tegenwoordig gebruikmaken van '*webbased* toepassingen om hun gegevens op te slaan', bijvoorbeeld een al dan niet verspreide opslag van gegevens in de *cloud.* Een gebruiker bewaart zijn of haar gegevens in dat geval niet (alleen) op zijn of haar harde schijf, maar ook op servers die zich elders in Nederland, of zelfs in het buitenland bevinden. Op verschillende servers slaan deze diensten, langs geautomatiseerde weg, de gegevens op. Waar en op welke servers dat gebeurt, heeft de gebruiker geen invloed op en in sommige gevallen is dat ook voor de aanbieder onbekend. Meestal worden bestanden in gedeelten opgeslagen, verspreid over meerdere servers die zich deels op buitenlands grondgebied bevinden (*Kamerstukken II*, 2015/16, 34 372, nr. 3, p. 11). *Cloud computing* is voor opsporingsinstanties problematisch, omdat voor sommige bevoegdheden de opsporing afhankelijk is van de medewerking van een aanbieder (artt. 126n, 126na, 126ng, 126u, 126ua, 126ug, 126zi en 126zl Sv). Bij *cloud computing* is het echter niet altijd duidelijk of een aanbieder kan worden gezien als aanbieder in de zin van de wet, waardoor geen bevel tot medewerking kan worden gegeven. Mocht dit wel kunnen, dan kan het zijn dat een aanbieder niet onder de Nederlandse rechtsmacht valt. In zo'n geval is het indienen van een rechtshulpverzoek nodig. Dat is lastig als Nederland met dat land geen rechtshulprelatie onderhoudt (*Kamerstukken II*, 2015/16, 34 372, nr. 3, p. 11-12).

Op basis van het voorgaande kan de eerste veronderstelling geformuleerd worden. Duidelijk is geworden dat drie technologische ontwikkelingen (versleuteling, draadloze netwerken en *cloud computing*) de inzet van bestaande bevoegdheden belemmeren. De wetgever beargumenteert dat de hackbevoegdheid ervoor zorgt dat deze technologische ontwikkelingen niet langer een probleem zijn voor de opsporing.

1 Opsporingsinstanties kunnen met behulp van de nieuwe bevoegdheid toegang krijgen tot informatie voordat deze versleuteld is of nadat deze ontsleuteld wordt (versleuteling).
2 Opsporingsinstanties kunnen met behulp van de nieuwe bevoegdheid het geautomatiseerde werk en of de gebruiker ervan identificeren waardoor gerichter onderzoek mogelijk is en alle gegevens kunnen worden ontvangen van alleen de verdachte (draadloze netwerken).
3 Opsporingsinstanties worden met behulp van de hackbevoegdheid minder afhankelijk van gegevens die opgeslagen staan in de cloud, omdat zij gegevens kunnen krijgen die opgeslagen staan op het geautomatiseerd werk (cloud computing).

Dit alles zorgt ervoor dat opsporingsinstanties zicht krijgen op gegevens waarop zij met de bestaande bevoegdheden geen zicht zouden krijgen. Met behulp van deze gegevens kunnen computercriminaliteit en andere vormen van georganiseerde criminaliteit beter worden aangepakt.

7.2.2 *Bezwaren ten aanzien van andere bevoegdheden*

Het voorgaande heeft vooral laten zien dat bestaande bevoegdheden die opsporingsinstanties tot hun beschikking hebben niet altijd goed bruikbaar zijn vanwege versleuteling, draadloze netwerken en *cloud computing*. Het komt ook voor dat er praktische bezwaren kleven aan de reeds bestaande bevoegdheden en dat de inzet ervan kan leiden tot een niet noodzakelijke privacy inbreuk waardoor de proportionaliteit in het geding kan komen, aldus de wetgever in de memorie van toelichting. Dat geldt bijvoorbeeld voor het tappen. Dat er zowel bedenkingen zijn gerelateerd aan de proportionaliteit van een inzet als praktische bezwaren geldt voor meer bijzondere opsporingsbevoegdheden. Het gaat om het opnemen van vertrouwelijke communicatie, inbeslagname en observatie, stelselmatige inwinning informatie en de inkijkoperatie.

De bevoegdheid tot het opnemen van vertrouwelijke communicatie (artt. 126l, 126s en 126zf Sv) maakt het mogelijk om 'middels het plaatsen van een technisch hulpmiddel, zoals een "bug"[105] heimelijk communicatie op te nemen' (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 12). Om het hulpmiddel te plaatsen kan een besloten plaats of woning worden betreden. Het gebruik van deze bevoegdheid kent een aantal nadelen, aldus de memorie van toelichting (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 13). Ten eerste is het ingewikkeld om de bevoegdheid in te zetten wanneer de locatie van een geautomatiseerd werk niet bekend is. Ten tweede lopen opsporingsinstanties het risico dat zij betrapt worden of dat zij 'onvoorziene omstandigheden' tegenkomen. Ten derde wordt met de inzet van deze bevoegdheid, zeker wanneer het een woning betreft, inbreuk gemaakt op het grondwettelijk beschermde recht van de onschendbaarheid van de woning.[106]

Opsporingsinstanties hebben ook de mogelijkheid om een geautomatiseerd werk of gegevensdrager in beslag te nemen (artt. 95, lid 1; 96, lid 1; 96c, lid 1; 97, lid 1; 98, lid 1; 99, lid 1 Sv) (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 13). In de memorie van toelichting staat dat er nadelen kleven aan inbeslagname. Het eerste nadeel van het in beslag nemen van een gegevensdrager is dat een verdachte op de hoogte raakt van het feit dat opsporingsinstanties onderzoek naar hem doen. Verder zorgt deze bevoegdheid ervoor dat de politie kan beschikken over alle gegevens die op het geautomatiseerd werk staan opgeslagen (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 13). Als een object alleen in beslag wordt genomen om bepaalde gegevens vast te leggen, dan kan het inzetten van die bevoegdheid volgens de memorie van toelichting als disproportioneel aangemerkt worden (vanwege 'het kennisnemen van een grote hoeveelheid persoonsgegevens met het oog op het selecteren van voor opsporing relevante gegevens'). Om die reden mag de bevoegdheid alleen worden ingezet indien met de minder vergaande bevoegdheid tot het vorderen van gegevens niet kan worden volstaan (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 13). Een laatste nadeel die in de nota naar aanleiding van het verslag beschreven wordt, is dat het voor de inzet van deze bevoegdheden nodig is dat opsporingsinstanties op de hoogte moeten zijn op welke locatie een voorwerp zich bevindt. Technologische ontwikkelingen, zoals versleuteling en *cloud computing* maken dat lastig (*Kamerstukken II* 2015/16, 34 372, nr. 6, p. 11).

[105] Een 'bug' wordt in de memorie van toelichting beschreven als een kleine microfoon die in staat is opgenomen signalen draadloos te verzenden (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 12).

[106] Dit wordt ook opgemerkt ten aanzien van het betreden van een woning om een *keylogger* te plaatsen (*Kamerstukken II* 2015/16, 34 372, nr. 6, p. 24). Ook 'onderkenning' is een risico bij de plaatsing van een *keylogger*, net zoals de veiligheid en inzet van personeel (*Kamerstukken II* 2015/16, 34 372, nr. 6, p. 24).

Naast de in de voorgaande paragraaf beschreven bevoegdheden worden in de memorie van toelichting nog drie bevoegdheden genoemd die volgens de memorie 'evenmin soelaas' bieden om het opsporingswerk op een goede manier te kunnen doen (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 13). Het gaat om observatie (artt. 126g, 126o en 126zd, lid 1, sub a Sv), stelselmatig inwinning van informatie (artt. 126j, 126qa en 126zd, lid 1, sub c Sv) en de inkijkoperatie (artt. 126k, 126r en 126zd, lid 1, sub d Sv) (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 13). In de memorie van toelichting staat beschreven dat de belangrijkste beperking van deze bevoegdheden is dat ze geen betrekking hebben op de toegang tot gegevens die worden verwerkt via de elektronische weg. Een gevolg hiervan is dat met behulp van deze bevoegdheden geen inzicht kan worden verkregen in de gegevens die een verdachte heeft verzonden alsmede ontvangen en in de communicatie waaraan een verdachte deelneemt (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 13). Er kan immers geen zicht worden verkregen op gedrag in 'afgeschermde ruimten van het internet' (*Kamerstukken II* 2015/16, 34 372, nr. 6, p. 12)). Bovendien, zo komt in de nota naar aanleiding van het verslag naar voren, kan het voorkomen dat observatiemethoden te weinig resultaten opleveren of dat het onbekend is waar een verdachte zich bevindt. Middels de nieuwe bevoegdheid kan de locatie van een smartphone of gebruiker worden vastgesteld. In dat geval wordt een smartphone als peilzenderfunctie gebruikt (*Kamerstukken II* 2015/16, 34 372, nr. 6, p. 48).

Op basis van het voorgaande kan veronderstelling 2 geformuleerd worden. Duidelijk is geworden dat verschillende bijzondere bevoegdheden praktisch en proportioneel gezien niet altijd de aangewezen bevoegdheden zijn om in te zetten, omdat opsporingsinstanties fysiek toegang moeten hebben tot de locatie van het geautomatiseerd werk/kennis moeten hebben over de locatie (opnemen vertrouwelijke communicatie, inbeslagname en observatie, stelselmatige inwinning informatie en inkijkoperatie) en omdat de bevoegdheden (observatie, stelselmatige inwinning informatie en inkijkoperatie) niet gericht zijn op het verzamelen van elektronische gegevens. De hackbevoegdheid zorgt ervoor dat elektronische gegevens wel kunnen worden verzameld alsmede dat fysieke toegang niet langer noodzakelijk is. Door dat laatste kunnen gegevens verzameld worden wanneer een locatie onbekend is en zonder dat de verdachte hiervan op de hoogte raakt. Bovendien kunnen opsporingsinstanties gegevens verzamelen op een manier die proportioneler wordt geacht. Met deze gegevens kunnen computercriminaliteit en andere vormen van georganiseerde criminaliteit beter en/of niet ingrijpender dan strikt noodzakelijk aangepakt worden.

7.3 Hackbevoegdheid in de praktijk

In de komende (sub-)paragrafen wordt uiteengezet hoe de hackbevoegdheid in de praktijk benut is. Allereerst wordt ingegaan op de aard van de zaken waarin de hackbevoegdheid is ingezet. Er wordt onder andere ingegaan op het aantal en soort inzetten dat er geweest is. Ook richt de aandacht zich op de redenen om de hackbevoegdheid in te zetten en het doel van de inzet. Daarna wordt ingegaan op de opbrengst van de hackbevoegdheid en de behandeling door een zittingsrechter van zaken waarin de hackbevoegdheid is ingezet. Vervolgens worden de verschillende voordelen besproken die de hackbevoegdheid heeft voor de opsporingspraktijk. Ook komen verschillende aandachtspunten aan de orde.

Voor de leesbaarheid van het hoofdstuk is het volgende van belang: bij de inzet van de hackbevoegdheid heeft Digit (*Digital Intrusion Team*) een centrale rol. Digit zelf kent twee onderdelen: Digit-politie en Digit-OM. De uitvoering van de hackbevoegdheid is in handen van Digit-politie. Digit-politie wordt aangestuurd door Digit-OM, ondergebracht bij het Landelijk Parket. Digit ondersteunt een tactische onderzoekteam. Een inzet van Digit vindt plaats binnen een opsporingsonderzoek dat uitgevoerd wordt door een tactisch team van de politie, bijvoorbeeld een team van de districtsrecherche of Team High Tech Crime. Het tactisch team werkt onder gezag van een tactisch zaaksofficier van justitie. Deze zaaksofficier is eindverantwoordelijk voor het opsporingsonderzoek waarbinnen Digit een inzet doet en hij/zij dient verantwoording af te leggen in de rechtbank als de zaak op zitting wordt behandeld

7.3.1 Aard artikel 126nba Sv zaken

Van intake naar inzet

Niet alle verzoeken aan Digit leidden tot een daadwerkelijke inzet van de hackbevoegdheid. In de periode april 2021 t/m april 2024[107] heeft Digit in 131 van de 220 zaken uiteindelijk géén inzet gedaan. Hiervoor waren verschillende redenen. In net iets minder dan de helft van de zaken (64) was de reden technisch van aard. Technisch betekent dat het in die gevallen niet tot een aanvraagprocedure voor een inzet is gekomen, omdat er een gebrek aan technische mogelijkheden was of omdat Digit onvoldoende capaciteit had om met de zaak aan de slag te gaan. In 55 zaken werd de hackbevoegdheid vooral om een tactische reden niet ingezet. In het grootste deel van die zaken trok het tactisch team zich terug. De reden voor deze terugtrekking is lang niet altijd bekend, maar het kan bijvoorbeeld gaan om een aanhouding van de verdachte waarop de hack zich zou richten of dat het tactisch team zelf een aantal acties kon ondernemen, waardoor een inzet van Digit toch niet meer nodig was. In 4 zaken waren er zowel tactische als technische redenen en in 8 zaken was er een overige reden. In die gevallen was het bijvoorbeeld onbekend waarom er uiteindelijk geen inzet is geweest of is een zaak verder gegaan onder een andere naam.

Mocht op basis van de intake blijken dat een inzet van de hackbevoegdheid wel mogelijk is, dan doorloopt de tactisch officier van justitie, deels samen met het opsporingsteam, een uitgebreide procedure om toestemming te krijgen voor een inzet van de hackbevoegdheid.[108] Na toestemming van de rechercheofficier van het betreffende parket, stelt de officier van justitie, ondersteund door Digit-OM, een aantal schriftelijke stukken op voor de Centrale Toetsingscommissie (CTC)[109]. Zodra deze toestemming heeft gegeven, wordt toestemming gevraagd aan het College van Procureurs-Generaal. Pas als het College instemt met de inzet, vordert de officier van justitie een machtiging bij de rechter-commissaris. Na deze machtiging van de rechter-commissaris waarin zij/hij toestemming geeft voor de inzet, kan de officier van justitie een bevel afgeven aan de politie om de hackbevoegdheid in te zetten.

[107] Omdat in de eerdere evaluatie (Van Uden & Van den Eeden, 2022) al aantallen worden genoemd met betrekking tot de periode maart 2019-maart 2021 wordt voor de hackbevoegdheid in dit rapport een afwijkende rapportageperiode gehanteerd.

[108] Omdat in het eerste rapport uitgebreid in is gegaan op deze procedure (Van Uden & Van den Eeden, 2022, 78-84), volgt hier slechts een summiere beschrijving van deze procedure, gericht op de actoren die hierbij betrokken zijn.

[109] De CTC is een intern adviesorgaan binnen het Openbaar Ministerie dat advies geeft aan het College van Procureurs-Generaal over onder andere de voorgenomen inzet van enkele bijzondere opsporingsbevoegdheden.

Soorten misdrijven

In de periode april 2021-april 2024 is in 89 zaken een eerste bevel afgegeven om de hackbevoegdheid in zetten. In tabel 7.1 is te zien op welk soort misdrijven de opsporingsonderzoeken, waarin een officier van justitie toestemming gaf om de hackbevoegdheid in te zetten, zich richtten. In tabel 7.1 wordt duidelijk dat net iets meer dan de helft van de inzetten zich op een paar soorten misdrijven heeft gericht. De meeste inzetten (27) hadden betrekking op een delict uit de Opiumwet. Daarna volgen moord en doodslag inclusief pogingen daartoe (19) en witwassen (12). De rest van de inzetten richtte zich op een scala aan misdrijven. Net zoals in het eerste rapport (Van Uden & Van den Eeden, 2022, p. 86) valt op dat het overgrote deel van opsporingsonderzoeken zich richt op traditionele vormen van criminaliteit, en dus niet cybercriminaliteit in enge zin zoals de naam van de Wet CCIII wellicht doet vermoeden.

Tabel 7.1 Soorten misdrijven*

Misdrijf	Aantal inzetten
Opiumwet	27
Moord/doodslag en of poging daartoe en of voorbereiding	19
Witwassen	12
Wet Wapens en Munitie (WWM)	5
Brandstichting	3
Misdrijven gerelateerd aan openbaar gezag en/of staatsveiligheid	3
Zeden	3
Georganiseerd verband	2
Ambtsmisdrijf	2
Mix	2
Terrorisme	2
Corruptie en openbaar maken gegevens	1
Diefstal met geweld	1
Fraude	1
Genocide en foltering	1
Hacken, diefstal gegevens, afpersing	1
Oplichting en georganiseerd verband	1
Verstrekken staatsinlichtingen	1
Wederrechtelijke vrijheidsberoving	1
Onbekend	1
Totaal	**89**

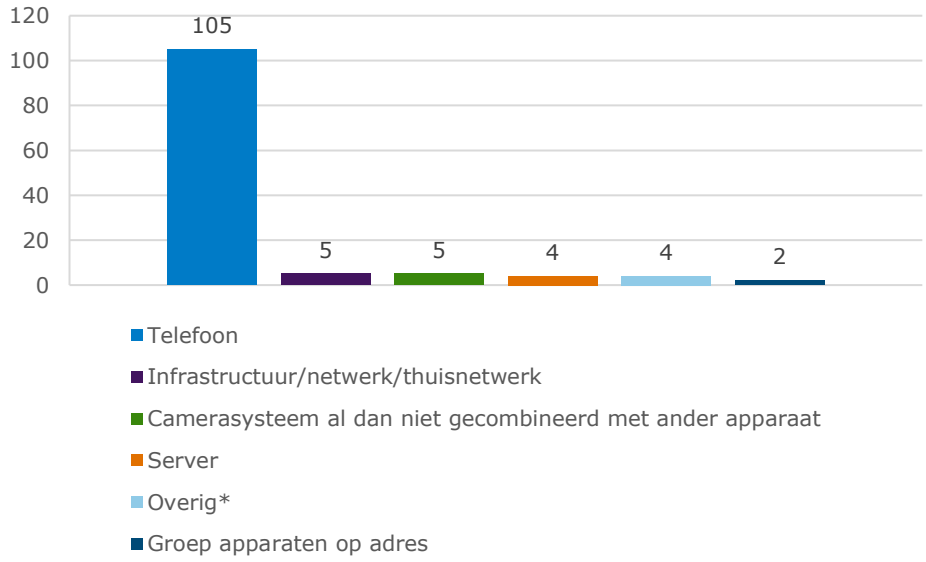
* In bijlage 5 staat een meer gedetailleerde tabel waarin ook de strafbare feiten gespecificeerd staan waarmee de strafbare feiten in deze tabel samen voorkwamen.

Inzetten van de hackbevoegdheid mogen worden verlengd. Dit is in 54 van de 89 zaken ten minste bij één geautomatiseerd werk één of meerdere keren gebeurd.

Geautomatiseerde werken

In het vorige rapport (Van Uden & Van den Eeden, 2022, p. 88) bleek dat in het overgrote deel van de zaken toestemming was verkregen de hackbevoegdheid in te zetten ten aanzien van een telefoon. Dat is ook in de huidige onderzoeksperiode het geval. Het overgrote deel van de geautomatiseerde werken dat mocht worden gehackt (105 van de 125) betreft een inzet op een telefoon, de zogenoemde standaardinzet. In totaal mochten 125 geautomatiseerde werken worden binnengedrongen bij 89 inzetten waarvoor een eerste bevel is afgegeven. In figuur 7.2 staat een overzicht van de soorten geautomatiseerde werken en het aantal waarop mocht worden binnengedrongen. Bij 9 inzetten is sprake van een zogenoemde maatwerkinzet (een inzet op een ander geautomatiseerd werk dan een telefoon) en 8 inzetten betroffen een gecombineerde inzet. Bij de (gecombineerde) maatwerkinzetten zijn 20 geautomatiseerde werken binnengedrongen. Grotendeels zijn dat dezelfde soorten geautomatiseerd werk als waarover werd gerapporteerd in de eerdere WODC-evaluatie (Van Uden & Van den Eeden, 2022).

Figuur 7.2 Soorten geautomatiseerd werk



* Onder de categorie overig vallen desktop computer, device X op adres, telefoon en thuisnetwerk en laptop.

Doel inzet hackbevoegdheid

Op basis van de afgenomen vragenlijsten kunnen verschillende doelen worden onderscheiden waarvoor officieren van justitie de hackbevoegdheid hebben ingezet. In tabel 7.3 staan de verschillende doelen weergegeven. Per opsporingsonderzoek kan de hackbevoegdheid voor meerdere doelen worden benut. De doelen in tabel 7.3 zijn gebaseerd op de doelen waarvan de wetgever verwachtte dat de hackbevoegdheid zou kunnen worden benut en zijn specifieker dan de doelen die uiteindelijk in het Wetboek van Strafvordering terecht zijn gekomen.

Tabel 7.3 Onderzoeksdoelen

Doel	Aantal	%
Het verkrijgen van opgeslagen gegevens	56	86%
Het aftappen en opnemen van versleutelde communicatie op het apparaat	43	66%
Het opnemen van vertrouwelijke communicatie met een technisch hulpmiddel	34	52%
Het achterhalen van identificerende gegevens	26	40%
Stelselmatige observatie	15	23%
Ander doel	6	9%
Het ontoegankelijk maken van gegevens waarmee strafbare feiten werden gepleegd	2	3%
Het verstoren van een botnet	0	0%

Op basis van tabel 7.3 wordt duidelijk dat het verkrijgen van opgeslagen gegevens in 86% van de opsporingsonderzoeken het doel, of één van de doelen was. Daarna volgt het opnemen van versleutelde communicatie op een apparaat (66% van de opsporingsonderzoeken) en het opnemen van vertrouwelijke communicatie (52% van de 66 opsporingsonderzoeken). Slechts een enkele keer is de hackbevoegdheid benut voor het ontoegankelijk maken van gegevens. In de vragenlijst is niet aangegeven dat de hackbevoegdheid is ingezet om een botnet te verstoren. Op basis van de eerdere WODC-evaluatie en berichten in de media (OM, 2010) is echter bekend dat Nederland, in het kader van een internationale samenwerking, een sub e-inzet op een botnet heeft gedaan ter uitvoering van een verzoek om rechtshulp.

Hoofdpunten

- In de periode april 2021 t/m april 2024 heeft Digit-politie in 131 van de 220 zaken géén inzet gedaan. Hiervoor waren zowel technische als tactische redenen.
- In dezelfde periode is in 89 zaken een eerste bevel gegeven om de bevoegdheid in te mogen inzetten.
- De hackbevoegdheid mocht vooral worden ingezet in het kader van drie soorten misdrijven: opium gerelateerd, (poging) moord/doodslag en witwassen.
- Er mocht voor 125 geautomatiseerde werken een eerste bevel afgegeven worden om binnen te dringen. Het overgrote deel hiervan betrof een telefoon.
- De hackbevoegdheid wordt het meest benut om inzicht te krijgen in opgeslagen gegevens en versleutelde communicatie.

Reden inzet hackbevoegdheid

In de memorie van toelichting worden verschillende redenen genoemd waarom de inzet van een hackbevoegdheid noodzakelijk kan zijn. In de praktijk is een groot aantal redenen terug te zien. Uit de ingevulde vragenlijsten, per vragenlijst konden meerdere redenen worden ingevuld, blijkt dat versleuteling van gegevensdragers de belangrijkste reden is voor de inzet van de hackbevoegdheid (54% van de opsporingsonderzoeken), gevolgd door dat bij de inzet van andere bevoegdheden het risico bestaat dat de verdachte op de hoogte raakt van het opsporingsonderzoek (40%). Ook de antwoordcategorie ‘anders’ scoort relatief hoog (40%). Wanneer de open antwoorden bekeken worden valt op dat het bij de antwoordcategorie ‘anders’ enerzijds gaat om antwoorden die raken aan een andere antwoord categorie (verdachte die op zijn hoede is) en anderzijds om een meer algemene reden, namelijk dat bevoegdheden niet volstaan of te weinig hebben opgeleverd. Verder worden het

feit dat andere bevoegdheden zich niet richten op het verzamelen van gegevens en het gebruik van draadloze netwerken relatief vaak genoemd (22%). In tabel 7.4 staan alle genoemde redenen weergegeven. Opvallend daarbij is dat de reden 'de inzet van een andere bevoegdheid zou niet proportioneel zijn' niet is aangekruist in de vragenlijst. Wel komt in één van de open antwoorden (onder meer) de reden het vermijden van een impactvollere bevoegdheid naar voren. Verder wordt in een deel van de interviews de proportionaliteit van de inzet van de hackbevoegdheid genoemd als voordeel ten opzichte van andere ingrijpende bijzondere opsporingsbevoegdheden (zie paragraaf 7.3.7).

Tabel 7.4 Reden inzet hackbevoegdheid

Reden	Aantal	%[a]
De benodigde gegevens waren versleuteld.	35	54%
Bij de inzet van andere bevoegdheden zou de verdachte dan wel medeverdachten op de hoogte raken van het opsporingsonderzoek.	26	40%
Andere reden*	26	40%
De verdachte(-n) maakte(n) gebruik van draadloze netwerken.	14	22%
Andere bevoegdheden hadden geen betrekking op de toegang tot gegevens via elektronische weg.	14	22%
De benodigde gegevens stonden opgeslagen in de *cloud*.	10	15%
Andere bevoegdheden konden niet worden ingezet, omdat de locatie van het geautomatiseerd werk onbekend was.	6	9%
De inzet van een andere bevoegdheid zou niet proportioneel zijn.	0	0%

* Bij andere reden worden de volgende redenen genoemd. Andere bevoegdheden hadden een beperkte opbrengst al dan niet gecombineerd met het vermijden van een impactvollere bevoegdheid of een verdachte die op zijn hoede is (5); andere bevoegdheden voldeden niet, al dan niet in combinatie met ander bevoegdheden beperkte opbrengst en risico op verlies aan informatie (7), de verdachte was op zijn hoede (5); bewijs verzamelen (2); ten behoeve van rest van het opsporingsonderzoek (2); communicatie via concept-mails(1); zicht krijgen op verdachte in de actualiteit (1); controle houden op verdachte (1); geen zicht op verdachte (1); en ontsleutelen en opnemen cryptocommunicatie (1).

a Berekend ten opzichte van het totaal aantal vragenlijsten dat is ingevuld en meegenomen in de analyse (65 = 100%).

In het vervolg van deze paragraaf wordt op basis van de interviews meer achtergrond gegeven bij de tactische redenen om de hackbevoegdheid in te willen zetten. Belangrijk om hierbij op te merken is dat de verschillende redenen los van elkaar worden besproken, terwijl in de praktijk sprake kan zijn van een mix van overwegingen. Alle in de interviews genoemde redenen om de hackbevoegdheid in te willen zetten komen neer op het feit dat er geen of onvoldoende opbrengst is uit andere opsporingsbevoegdheden of dat de verwachting bestaat dat andere opsporingsmiddelen te weinig informatie zullen opleveren. Een voorbeeld van een opsporingsonderzoek waarin andere opsporingsbevoegdheden te weinig opleverden is een onderzoek naar wapenhandel. In deze zaak was een verdachte in beeld en één van de bevoegdheden die voorafgaand aan de hackbevoegdheid was ingezet, was een observatie bij de woning van de verdachte. Dit leverde echter geen bruikbare informatie op. Ook andere bevoegdheden, zoals de printertap en de telefoontap, leverden te weinig informatie op waardoor uiteindelijk de keuze is gemaakt de hackbevoegdheid in te zetten.

Het komt ook voor dat niet eerst een aantal andere bijzondere opsporingsbevoegdheden wordt ingezet, bijvoorbeeld zaken waarin verdachten hun eigen afscherming zo goed hebben geregeld waardoor de inzet van andere opsporingsmiddelen 'haast onmogelijk' is. Of wanneer de dreiging dat een strafbaar feit gepleegd zal gaan worden, bijvoorbeeld in het geval van een terroristische dreiging, zo groot kan zijn, dat het 'proportioneel' is om een 'heftig middel' als de hackbevoegdheid in te zetten.

In de interviews en de vragenlijsten komen verschillende redenen naar voren voor het feit dat andere opsporingsbevoegdheden te weinig informatie opleveren. Zo kan er sprake zijn van versleuteling, een verdachte die op zijn hoede is of een gebrek aan tijd en capaciteit. Ook kan het zijn dat er geen duidelijke locatiegegevens beschikbaar zijn, dat een bevoegdheid zich niet richt op gegevens of kan in een zaak sprake zijn van een buitenlands element. In de komende paragrafen worden deze redenen nader uitgewerkt.

Versleuteling
Een belangrijke reden waarom andere opsporingsbevoegdheden te weinig opleveren is versleuteling. Daarbij gaat het in de eerste plaats om communicatie via applicaties zoals Signal en WhatsApp. Ook communicatie via conceptmails die nooit verzonden worden, wordt genoemd. Met de reguliere tapbevoegdheden, zowel telefoon als IP-tap lukt het niet om de inhoud van deze communicatie mee te krijgen. Eén van de geïnterviewde officieren van justitie zegt hierover:

> Je ziet natuurlijk steeds meer dat, mensen überhaupt, maar ook criminelen dus, niet meer gebruikmaken van regulier belverkeer. (…). Het is alleen maar Signal, WhatsApp, Snap [Snapchat].

Dit betekent overigens niet dat tapbevoegdheden in zijn geheel niet meer bruikbaar zijn. Dergelijke bevoegdheden kunnen bijvoorbeeld behulpzaam zijn om de locatie van een verdachte in beeld te brengen.

Versleuteling speelt niet alleen een rol in de zogenoemde standaardzaken, waarin het gaat om het binnendringen in telefoons. Ook in maatwerkzaken is versleuteling een belangrijke reden. In die zaken gaat het bijvoorbeeld om computers en harde schijven die versleuteld zijn, maar ook om het gebruik van een Tor-browser die het internetbezoek versleutelt. Een voorbeeld van het soort zaken waarvoor dit geldt zijn kinderpornozaken. Eén van de geïnterviewden officieren legt uit dat verdachten in kinderpornozaken doorgaans bezig zijn met het afschermen van hun activiteiten, onder andere door versleuteling. Door de inzet van de hackbevoegdheid wordt het mogelijk om die versleuteling te doorbreken en mee te kijken met wat de verdachten aan het doen zijn. In dit soort zaken is er nog een andere reden waarom de inzet van de hackbevoegdheid goed van pas kan komen. Vóór de komst van de hackbevoegdheid was het van belang dat bij de aanhouding van de verdachte zijn computer open bleef staan, omdat men anders vanwege de versleuteling geen zicht kon krijgen op de inhoud van de computer. Om dat voor elkaar te krijgen kon een 'gevaarzettende situatie' ontstaan, waarbij de politie, soms met geweld, een woning moest binnengaan om de verdachte te verrassen en zo snel mogelijk aan te houden. Op die manier zou hij geen tijd hebben om zijn materiaal te versleutelen of te vernietigen. Door de inzet van de hackbevoegdheid is het niet nodig een dergelijke aanhoudingssituatie met de daarbij behorende risico's te creëren.

Verdachte op zijn hoede
Een tweede reden waarom de inzet van andere bevoegdheden (mogelijk) niets of te weinig oplevert is dat veel van de verdachten waarnaar onderzoek wordt gedaan op hun hoede zijn, dat wil zeggen dat zij zich bewust zijn van het feit dat de politie mogelijk onderzoek naar hen doet en dat zij hier rekening mee houden. Eén van de officieren van justitie betrokken bij een opsporingsonderzoek naar drugshandel vertelt:

> De traditionele middelen gaven onvoldoende beeld. Je moet je voorstellen dat deze verdachten […] waren constant bewust van feit dat ze afgeluisterd konden worden. We hebben (…) OVC [in] een auto gehad, werd niet gesproken over criminele zaken, waren ze erg gedisciplineerd in. [OVC] in hun woning geplaatst, ook daar erg bewust. (…) Ook een camera op de woning, dan zie je wie er langskomt, dat zijn dan criminele contacten. Ging de radio hard [aan], gingen ze [in] een hoekje zitten en konden wij die gesprekken niet verstaan. Dus dan weet je in welke mate zij bewust zijn van de mogelijkheid om zelfs in je eigen woning afgeluisterd te worden. Observaties, [ook] lastig. Ze hadden constant contra-observaties georganiseerd. Dus dan was er ergens een ontmoeting. Maar dan gingen ze kijken of er een observatieteam achteraan reed.

Het bovenstaande schetst een situatie waarin andere opsporingsmiddelen wel worden ingezet maar te weinig bruikbare informatie opleveren. Het kan ook voorkomen dat de situatie bij een verdachte zodanig is dat het voor de politie bij voorbaat al als onmogelijk wordt gezien om een bepaalde bevoegdheid in te zetten. Het gaat dan om situaties waarin verdachten hun locaties zodanig beveiligen dat het plaatsen van apparatuur voor het opnemen van vertrouwelijke communicatie praktisch onmogelijk is. Denk bijvoorbeeld aan het ophangen van camera's of het nemen van andere maatregelen zoals het aanbrengen van verzegelingsvoorwerpen op een deur zodat de verdachte weet dat iemand anders dan hijzelf naar binnen is gegaan. Volgens één van de respondenten uit de vragenlijst, een officier van justitie die onderzoek doet naar georganiseerde criminaliteit (drugs en corruptie), zorgt deze alertheid ervoor dat bij dit soort criminaliteit de hackbevoegdheid 'de enige manier is om zicht te krijgen op communicatie' en daardoor op de strafbare feiten die worden gepleegd.

Gebrek aan tijd
Een derde reden die maakt dat andere bevoegdheden mogelijk te weinig informatie opleveren is dat de inzet ervan te veel tijd kan vragen, zo blijkt uit een aantal open antwoorden uit de vragenlijst. Uit deze antwoorden is verder niet op te maken om welke bevoegdheden het hier gaat. In een aantal verdiepende interviews brengen officieren van justitie het tijdsaspect ook naar voren. In deze interviews vertellen zij bijzondere opsporingsbevoegdheden als infiltratie en stelselmatige informatie-inwinning overwogen te hebben, maar hier vanwege het tijdsaspect vanaf te hebben gezien.[110] Het succesvol opzetten van dit soort trajecten vraagt tijd die er in sommige onderzoeken niet is.

Locatieproblemen
Een vierde reden waarom andere bevoegdheden mogelijk geen of een beperkte opbrengst hebben, is dat er geen duidelijke locatie is waarop de inzet van andere bevoegdheden zich kan richten. Zo vertelt één van de officieren van justitie, die onderzoek deed naar een moord, dat de verdachten 'overal en nergens' waren. Ook vanwege Corona werd het in die zaak lastig om andere middelen in te zetten en

[110] Dat bijzondere opsporingsbevoegdheden als infiltratie en stelselmatige informatie-inwinning niet hoeven te worden ingezet ziet een aantal opsporingsfunctionarissen als voordeel van de hackbevoegdheid.

bovendien was het plaatsen van OVC op het lichaam niet toegestaan. Mocht een locatie wel bekend zijn, ook dan kan het lastig zijn om andere opsporingsbevoegdheden, zoals een observatieteam, in te zetten. De beschikbaarheid van een observatieteam is doorgaans beperkt, omdat zij ook betrokken zijn bij andere opsporingsonderzoeken en dus niet zomaar kunnen worden ingezet, zo legt een officier van justitie uit. Ook voor een andere officier van justitie is onduidelijkheid over een locatie de reden geweest om geen andere bijzondere opsporingsbevoegdheid in te zetten. In dit geval ging het om het plaatsen van OVC-apparatuur. In dit opsporingsonderzoek naar wapenhandel waren er 'te weinig aanknopingspunten' om de juiste ruimte te kiezen voor het plaatsen van OVC-apparatuur. Locatie kan ook een probleem zijn wanneer een verdachte zich in het buitenland bevindt. Dat kan een onbekend buitenland zijn, maar ook een bekend buitenland dat niet wil samenwerken met Nederland. In beide gevallen kan de inzet van andere bevoegdheden problematisch zijn.

Alternatieve bevoegdheden niet gericht op gegevens
De vijfde en laatste reden is dat, in tegenstelling tot de hackbevoegdheid, niet alle bevoegdheden zicht richten op het verzamelen van digitale gegevens. Eén van de geïnterviewde officieren die onderzoek doet naar kinderporno legt uit dat dat soort feiten doorgaans online plaatsvinden. Met andere bevoegdheden, zoals observaties, is het lastig om zicht te krijgen op wat er op het beeldscherm van een computer gebeurt, in tegenstelling tot strafbare feiten die niet (volledig) online hoeven plaats te vinden, zoals drugshandel.

Geen inzet
Op basis de vragenlijst, maar vooral op basis van een aantal interviews blijkt dat in sommige zaken de keuze is gemaakt om de hackbevoegdheid niet in te zetten, ook al was daar in sommige gevallen wel toestemming voor. Hiervoor is een aantal redenen genoemd. De eerste is dat de verwachting was dat de inzet te weinig meerwaarde zou hebben voor het onderzoek. In één van de zaken waarvoor een vragenlijst is ingevuld, zijn twee toestemmingstrajecten tegelijkertijd gestart, namelijk die voor het plaatsen van een *keylogger* gecombineerd met artikel 126l Sv (het opnemen van vertrouwelijke communicatie) en voor de inzet van de hackbevoegdheid. Er was sneller toestemming voor de *keylogger* en die inzet leverde ook informatie op. Vanwege het 'afbreukrisico' van de hackbevoegdheid is gekozen om de hackbevoegdheid uiteindelijk niet in te zetten. Op welke afbreukrisico precies gedoeld wordt, is in de vragenlijst niet duidelijk geworden. De tweede reden die door één van de geïnterviewde officieren van justitie wordt genoemd is dat het soms een politieke afweging is om de hackbevoegdheid niet in te zetten. Dan gaat het bijvoorbeeld om het binnendringen van een computer in een land waarmee Nederland een minder goede rechtshulprelatie heeft. Om daadwerkelijk uitvoering te geven aan de hackbevoegdheid zou de soevereiniteit van dat land geschonden moeten worden, en dat werd in deze zaak niet wenselijk geacht. In een andere zaak, waarin hetzelfde probleem speelde, maar waarbij de zaak als ernstiger werd bestempeld, is overigens wel gekozen om een inzet te doen. Een derde reden, die door dezelfde geïnterviewde wordt aangedragen, is dat een inzet van de hackbevoegdheid soms niet heimelijk kan blijven wat een reden kan zijn om geen inzet te doen. Het betreft hier een botnetzaak waarbij het opsporingsteam bij voorkeur een deel van de wachtwoorden had willen aanpassen. Voor het onderzoeksteam was het echter niet goed te verantwoorden welk deel van de wachtwoorden dat moest zijn. Het alternatief was het aanpassen van alle wachtwoorden, maar in dat geval zou de verdachte onraad ruiken. Om die reden is gekozen de hackbevoegdheid niet in te zetten, maar in plaats daarvan het gehele botnet offline te halen. Twee andere

redenen tot slot die genoemd worden zijn dat de zaak te licht werd bevonden om de hackbevoegdheid in te zetten en dat er te weinig tijd was voor een inzet. Het tijdsaspect kan dus juist ook een reden zijn om de hackbevoegdheid niet in te zetten.

Hoofdpunten

- De hackbevoegdheid wordt ingezet als andere bevoegdheden te weinig informatie hebben opgeleverd of wanneer de verwachting is dat dat het geval zal zijn.
- De belangrijkste redenen die in de vragenlijst worden genoemd voor het feit dat dat andere bevoegdheden niet volstaan zijn: 1) de versleuteling van telefoons en andere gegevensdragers; 2) de verdachte kan op de hoogte raken dat een opsporingsonderzoek plaatsvindt; en 3) overig. Binnen deze laatste categorie wordt in net iets minder dan de helft van de antwoorden een meer algemeen antwoord geformuleerd, namelijk dat de bevoegdheden een beperkte opbrengst hadden of dat andere bevoegdheden niet voldeden.
- Andere redenen die in de interviews genoemd worden zijn: de inzet van andere bijzondere bevoegdheden kost te veel tijd en er is geen duidelijke locatie waar een inzet kan plaatsvinden.
- Er zijn ook redenen om de hackbevoegdheid (uiteindelijk) niet in te zetten. Eén daarvan is dat de inzet politiek gevoelig kan liggen en dat geldt voor zaken waarin sprake is van een buitenlandcomponent.

7.3.2 Opbrengst hackbevoegdheid

De inzet van de hackbevoegdheid garandeert niet dat een tactisch opsporingsteam daadwerkelijk gegevens ontvangt. Allereerst moet het Digit-politie lukken om het betreffende geautomatiseerd werk binnen te dringen. Uit de door Digit verstrekte gegevens blijkt dat dit in 65 van de 89 inzetten bij ten minste één geautomatiseerd werk is gelukt. Uit de ingevulde vragenlijsten blijkt dat het bij 55 van de 65 zaken (deels) gelukt is om binnen te dringen. In het overgrote deel van de zaken waarin het binnendringen niet is gelukt, waren hier technische redenen voor.

Op het moment dat het binnendringen lukt, kan de gegevensverzameling in principe beginnen. Ook in deze fase geldt dat er geen garantie is op succes. Cijfers van Digit laten zien dat in 63 van de 89 inzetten het gelukt is om gegevens te verzamelen. Uit de ingevulde vragenlijsten blijkt dat in 54 van de 65 opsporingsonderzoeken het (deels) gelukt is om gegevens te verzamelen.

Uit de vragenlijsten, maar ook uit de interviews blijkt dat er net zoals bij het binnendringen, technische factoren zijn waardoor (deels) geen gegevens verzameld kunnen worden. Op deze technische redenen kan, net als in het vorige rapport (Van Uden & Van den Eeden, 2022, p. 106), wegens de afscherming van onderzoeksmethoden, niet nader worden ingegaan. Naast technische factoren spelen factoren een rol die te maken hebben met (het gedrag van) de verdachte. Zo wordt lang niet altijd binnengedrongen op een geautomatiseerd werk dat zich in het buitenland bevindt. Daarnaast kan een verdachte het geautomatiseerd werk waarop zou worden binnengedrongen van de hand doen of kan hij bepaalde handelingen verrichten, al dan niet met het geautomatiseerd werk, waardoor het niet goed mogelijk is de gegevens te verzamelen.

Soort en bruikbaarheid gegevens
Wanneer het Digit-politie lukt gegevens te verzamelen, levert dat verschillende soorten gegevens op. In tabel 7.5 staat een overzicht weergegeven van het soort gegevens dat verzameld is, gebaseerd op de ingevulde vragenlijsten.

Tabel 7.5 Soort gegevens

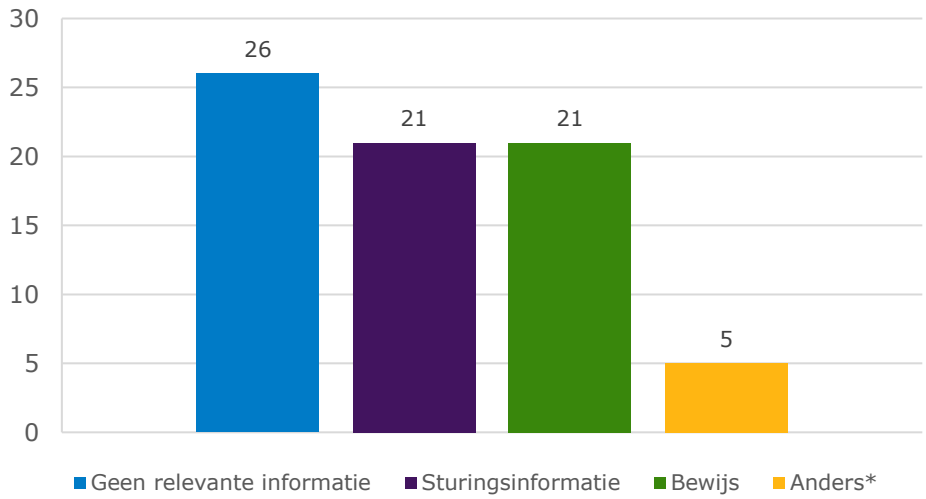
Soort gegevens	Aantal	%[a]
Versleutelde communicatieberichten via communicatieapps	34	52%
Locatie en of gebruiker geautomatiseerd werk	29	45%
Foto's	26	40%
Tekstberichten	25	38%
Filmpjes	16	25%
Locatiegegevens van het geautomatiseerd werk/de geautomatiseerd werken	14	22%
Live communicatie	13	20%
(Deels) onbekend	7	11%
Andere gegevens	6	9%
Inloggegevens	5	8%

a Berekend ten opzichte van het totaal aantal vragenlijsten dat is ingevuld en meegenomen in de analyse (65 = 100%).

Tabel 7.5 laat zien dat officieren van justitie het vaakst een vorm van communicatie ontvangen die verloopt via communicatie apps (in 52% van de opsporingsonderzoeken). Daarna volgen informatie over gebruiker en/of locatie van het geautomatiseerd werk en foto's en tekstbestanden. In 63% van de opsporingsonderzoeken zijn overigens meerdere soorten gegevens verkregen. In één van de opsporingsonderzoeken ging het bijvoorbeeld om de locatie van een geautomatiseerd werk, communicatie via tekst- en spraakberichten, filmpjes en foto's.

Net zoals dat er geen garantie is dat de hackbevoegdheid daadwerkelijk informatie oplevert, heeft een opsporingsteam ook niet de garantie dat de verzamelde gegevens bruikbaar zijn binnen het opsporingsonderzoek. Figuur 7.6 gaat in op de bruikbaarheid van de verzamelde gegevens.

Figuur 7.6 Bruikbaarheid van gegevens



* Bij anders ging het om minimale informatie (1), het onderzoek liep nog (1), de gegevens werden met een andere bevoegdheid ook verzameld (2) en onbekend (1). In één vragenlijst is zowel de antwoordcategorie 'anders' als de antwoordcategorie 'sturingsinformatie' aangekruist.

In 40% van de onderzoeken leidt de inzet van de hackbevoegdheid niet tot een bruikbare opbrengst voor het opsporingsonderzoek. In de vragenlijst en de interviews komt naar voren dat het bijvoorbeeld gaat om inloggegevens die uiteindelijk toch geen toegang gaven tot het geautomatiseerd werk. Daarnaast kwam het voor dat het geautomatiseerd werk geen informatie bleek te bevatten over strafbare feiten, bijvoorbeeld omdat onvoldoende over het strafbare feit werd gesproken. In ongeveer een derde van de onderzoeken leveren de gegevens sturingsinformatie op en in ongeveer een derde van de onderzoeken bewijs. Tussen deze categorieën zit overlap, omdat in negen onderzoeken de verzamelde gegevens én als sturingsinformatie én als bewijs hebben gediend. In de komende paragrafen worden meer diepgaand ingegaan op de wijze waarop de (bruikbare) gegevens in opsporingsonderzoeken kunnen worden benut.

Bewijs

Soorten bewijs

Zoals eerder besproken blijkt uit de vragenlijst dat in ongeveer een derde van de opsporingsonderzoeken gegevens uit de hackbevoegdheid bewijs hebben opgeleverd. Belangrijk om hierbij op te merken is dat het hier gaat om gegevens die een officier van justitie als bewijs heeft aangemerkt. Op basis van de vragenlijst kunnen verschillende soorten bewijs worden onderscheiden. Ten eerste bieden de verzamelde gegevens inzicht in strafbare feiten die een verdachte gepleegd heeft. Daarbij gaat het bijvoorbeeld om gesprekken over het voorbereiden van het plegen van een aanslag, communicatie over het overdragen van contante geldbedragen in een witwasonderzoek, communicatie in een chatapplicatie over drugshandel en materiaal dat wijst op het bezit en verspreiden van kinderporno. Wat betreft het laatste legt een officier van justitie uit dat de hackbevoegdheid niet alleen kan aantonen dat een verdachte zich hiermee bezig houdt, maar ook de intensiteit waarmee dat gebeurt. Met de verzamelde gegevens kon in de betreffende zaak én worden aangetoond dat een

verdachte gebruikmaakte van het Tor-netwerk én dat hij in het bezit was van een 'heftig' kinderpornofilmpje én dat hij dat filmpje van ongeveer een kwartier daadwerkelijk had bekeken. Dat laatste zegt volgens de officier van justitie iets over de mate waarin een verdachte zich bezig hield met strafbare feiten.

Het komt ook voor dat naast belastende informatie ten aanzien van feiten waarop de verdenking zich in eerste instantie richtte, belastende informatie wordt gevonden ten aanzien van andere strafbare feiten gepleegd door de verdachte. Dat gebeurde bijvoorbeeld bij een onderzoek dat zich richtte op wapenhandel. Uit de gegevens verzameld met behulp van de hackbevoegdheid bleek ook dat de verdachte betrokken was bij brandstichting en wederrechtelijke vrijheidsberoving.

Daarnaast heeft de hackbevoegdheid in sommige onderzoeken zicht gegeven op modus operandi en op de rol van een verdachte binnen een netwerk. Wat betreft dat laatste leverde de hackbevoegdheid in één van de opsporingsonderzoeken informatie op over het aansturen van leden van een criminele organisatie. Een andere officier van justitie legt uit op welke wijze de hackbevoegdheid informatie kan geven over iemands rol:

> En dan [gegevens verzameld met behulp van de hackbevoegdheid] kan het heel erg bijdragen aan het geven van inzicht in hoe de verhoudingen zijn, wat de rol van iemand is, hoe groot iemand is. Dus je hebt direct bewijs en achtergrondbewijs zal ik het dan eerder noemen. Van wat voor persoon hebben we het hier over? Hebben we het hier over een sulletje die gebruikt wordt? Of hebben we het hier over iemand die een aansturende rol heeft. Iedereen is tegenwoordig ZZP'er in onze criminele organisaties in Nederland. (…) [en] heeft een bepaalde rol, maar die zie je wel wisselen per keer.

Ten tweede bieden hackgegevens zicht op andere personen ('contacten') die betrokken zijn bij het plegen van strafbare feiten en bij criminele netwerken. Zo vertelt één van de geïnterviewden dat er in een onderzoek naar een moord twee verdachten waren waarop het opsporingsonderzoek zich in eerste instantie richtte. Uit gegevens verzameld met de hackbevoegdheid bleek vervolgens dat er nog een groep verdachten betrokken was die ook 'een rol bij de moord' hadden gespeeld. Een ander voorbeeld betreft een onderzoek waarin uit berichten in een chatapplicatie bleek dat iemand anders dan de hoofdverdachte afpersing, computervredebreuk en witwassen bekende.

Ten derde hebben gegevens verzameld met behulp van de hackbevoegdheid het mogelijk gemaakt om in elk geval in twee '*cybercrime* gerelateerde' onderzoeken gegevens ontoegankelijk te maken. In de eerste zaak ging het om het ontoegankelijk maken van de kwaadaardige software op verschillende bots. De tweede zaak richtte zich op twee *infostealers*. *Infostealers* zijn virussen, verstopt in bijvoorbeeld een PDF, die bij slachtoffers op hun computer worden geïnstalleerd en waarmee gegevens van slachtoffers gestolen worden (Vermaas, 2025).

Ten vierde kunnen de verzamelde gegevens laten zien dat een verdachte juist niet of op een andere manier dan in eerste instantie gedacht betrokken is bij het plegen van strafbare feiten. Een aantal officieren van justitie dat zich bezighoudt/bezig gehouden heeft met terrorismezaken legt uit dat de hackbevoegdheid ook kan helpen om te laten zien dat een mogelijke terroristische dreiging eigenlijk geen (serieuze) dreiging is. Eén van hen vertelt dat een aanhouding in het kader van een terrorisme onderzoek ingrijpend kan zijn voor een verdachte ('echt van betekenis voor een mensenleven') en

dat zij om die reden altijd gespitst zijn op ontlastend bewijs, hetgeen de hackbevoegdheid kan bieden. Deze officier van justitie heeft aan een zaak gewerkt waarin hij vermoedt dat, als er meer tijd was geweest voordat de politie tot een aanhouding was overgegaan, het onderzoek zou zijn 'afgeschaald' of in elk geval minder aanhoudingen verricht zouden zijn. Het uitstellen van de aanhouding was echter niet mogelijk in verband met een andere ernstige dreiging die zich gedurende het onderzoek voordeed.

Gewicht van het bewijs
Uit de interviews komt naar voren dat de zwaarte van het bewijs verschilt per zaak. Eén van de geïnterviewde officieren van justitie die goed zicht heeft op de zaken waarin de hackbevoegdheid is ingezet geeft aan dat in een (klein) aantal zaken de verzamelde gegevens 'essentieel bewijs' hebben opgeleverd die erop wijzen dat de verdachte één of meerdere strafbare feiten pleegde. Dat is bijvoorbeeld het geval in een zaak waarin de verdachte aan zijn partner heeft bekend dat hij een minderjarige heeft vermoord. Ook in een andere zaak heeft de hackbevoegdheid essentieel bewijs opgeleverd. Het betrof een verdachte in een kinderporno zaak waarin door de inzet van de hackbevoegdheid live kon worden meegekeken met de activiteiten waarmee de verdachte zich bezig hield. Met betrekking tot die laatste zaak zegt de betrokken officier van justitie:

> Het heeft best wel even geduurd, maar toen ze [de politie] uiteindelijk waren binnengedrongen, ik geloof dat hij echt binnen het uur online was en dat ze ook konden zien dat hij als Lucky23[111] inlogde en dat hij ook best wel naar het materiaal aan het bekijken was, dus meteen bingo.

In lang niet alle opsporingsonderzoeken levert de hackbevoegdheid dit soort bewijs op. De verzamelde gegevens vormen 'brokjes' waarmee een opsporingsteam kan aantonen dat de verdachte een strafbaar feit gepleegd heeft. In die zaken vormt het verzamelde materiaal één van de puzzelstukjes (soms groot, soms klein) op basis waarvan de officier van justitie heeft vastgesteld dat de verdachte betrokken is bij het plegen van het strafbare feit. Een voorbeeld van zo'n zaak is een verdachte die vervolgd gaat worden voor het medeplegen van witwassen. De betrokken officier van justitie legt uit dat het onderzoeksteam zich in dit opsporingsonderzoek richtte op een bonafide bedrijf waar de verdachte zich had 'ingemengd'. Op basis van gegevens verzameld met de hackbevoegdheid (camerabeelden) is één van de vennoten (niet de oorspronkelijke verdachte) aangemerkt als medepleger. Uit de beelden blijkt dat hij aanwezig was in de kamer waar de hoofdverdachte en een andere persoon met criminele intenties 'criminele zaken' aan het bespreken waren. Op basis van reguliere OVC wist het opsporingsteam wat voor zaken besproken werden en op camerabeelden was te zien dat deze medepleger daar kennis van moet hebben genomen. Zonder die camera was dat niet mogelijk geweest. De betreffende zaaksofficier van justitie vertelt:

> Voor (…) die medevennoot waar ik het over had, is het misschien wel het belangrijkste bewijs. Of zijn het eigenlijk twee heel belangrijke bewijsmiddelen. Je hoort het zeggen, het kan niet anders dan dat hij dat niet heeft gehoord. En je ziet hem op een meter afstand zitten. Dus dat is een cruciaal bewijsmiddel. (…) De wetenschap of een element van het verwijt wat tegen hem wordt gemaakt, witwassen, en dan moet je wetenschap hebben of dat je dat opzettelijk gedaan hebt of meegewerkt. Ja, dat blijkt hier eigenlijk onomstotelijk uit. Je hebt het

[111] Gefingeerde nickname.

> gewoon laten gebeuren en je vond het kennelijk gewoon ook prima. Je hebt niet op dat moment, nu ik dit hoor, ga m'n vennootschap eens uit. Dat niet.

Een andere officier van justitie legt uit dat de gegevens verzameld met behulp van de hackbevoegdheid als 'plusje' zijn gebruikt in een opsporingsonderzoek naar moord. Het ging hier om opgeslagen notities op de telefoon van de verdachte, waarin contacten met specifieke opdrachtgevers aan de orde kwamen. Op een bepaald moment in het opsporingsonderzoek vond de officier van justitie het niet meer verantwoord om de verdachte op vrije voeten te laten lopen. De notities vormde een belangrijk aanknopingspunt voor de aanhouding, omdat op basis daarvan ook het idee bestond dat de verdachte langer vastgehouden kon worden. De informatie uit de telefoon is op zitting uiteindelijk niet als bewijs gebruikt, omdat de betreffende notitie, en andere notities, ook in de in beslaggenomen telefoon te vinden waren. Dat laatste geldt overigens voor meer opsporingsonderzoeken, zo blijkt uit de interviews en de ingevulde vragenlijsten. Wanneer een gehackte telefoon in beslag wordt genomen wordt dezelfde informatie gevonden die voor het bewijs wordt gebruikt. In sommige gevallen is op zo'n telefoon nog extra bewijs te vinden.

Sturingsinformatie

In ongeveer een derde van de opsporingsonderzoeken hebben gegevens, verkregen met de hackbevoegdheid, sturingsinformatie opgeleverd. Sturingsinformatie is informatie die opsporingsfunctionarissen gebruiken om één of meer vervolgstappen te bepalen. Eén van de geïnterviewden spreekt om die reden van 'indirect bewijs'. Ook kan sturingsinformatie helpen om opbrengsten uit eerder onderzoek beter te begrijpen. Tijdens de interviews en in de ingevulde vragenlijsten worden diverse voorbeelden gegeven van sturingsinformatie. Het gaat vooral om (achtergrond-)informatie over het doen en laten van de verdachte. Bijvoorbeeld contacten die hij heeft, al dan niet met medeverdachten, de netwerken waarvan hij onderdeel uitmaakt en de werkwijze daarbinnen. Ook verblijfsplaatsen, de manier waarop de verdachte zich verplaatst en de geautomatiseerde werken die hij in bezit heeft, kunnen sturingsinformatie zijn.

Vervolgstappen

De vervolgstappen die op basis van sturingsinformatie ondernomen worden, doen zich zowel binnen het opsporingsonderzoek voor als daarbuiten. Binnen een opsporingsonderzoek wordt sturingsinformatie gebruikt om verdere richting te geven aan het opsporingsonderzoek. In de eerste plaats kan sturingsinformatie zicht bieden op locaties of personen die van belang zijn voor het verdere opsporingsonderzoek. Zo is in een zaak door de hackbevoegdheid zicht verkregen op berichtenverkeer waarin investeringsprojecten naar voren kwamen waarmee de verdachten zich 'in de actualiteit' bezighielden. Een deel van het witwasonderzoek heeft zich daar vervolgens op gericht. Een ander voorbeeld van sturingsinformatie zijn locatiegegevens. Eén van de geïnterviewde officieren van justitie vertelt:

> Als ik kijk naar [onderzoeksnaam], daar [zit een verdachte], die werkt heel erg afgeschermd. Daar zitten we al echt lang op te werken, echt meer dan een jaar en dan zijn wij het onderzoek, dat voortbouwt op een ander onderzoek. Daar kom je gewoon niet bij en het enige echte bewijs, ja ik denk het echte bewijs dat we daarin vinden, zijn een locatie [via] z'n sociale lijn (…) ergens in the middle of nowhere in [Land X]. (…) Dan heb je dus hele mooie sturingsinformatie. Ik weet nog niet wat daar ligt, maar het vermoeden is dat daar wel echt iets gebeurt.

Vervolgens kan sturingsinformatie helpen om te bepalen welke andere (bijzondere) opsporingsbevoegdheden een opsporingsteam kan inzetten. Zo vertelt één van de officieren van justitie die onderzoek naar wapenhandel deed dat uit communicatie verkregen met de hackbevoegdheid bleek dat de verdachte af zou reizen naar een vakantiepark voor een mogelijke wapenoverdracht:

> We hebben meegemaakt dat we een dump kregen van de dag daarvoor, waar we in lazen, één of twee dagen daarna (…) gaan we naar een locatie in het midden van het land (…). En dan kom ik dat in plaats X bij je ophalen. Daar werd niet gezegd dat wapen, maar het ding. Wat er dus voor zorgde, dat we aan de voorkant geprepareerd waren. (…) En daar hebben we het OT [observatieteam] achteraan laten rijden. We zagen ze dus ook daadwerkelijk naar de locatie vertrekken. (…) Toen heeft hij een ontmoeting gehad in plaats X met iemand op een bepaalde locatie, daar werd iets overgedragen in een grote doos, waarvan we niet wisten natuurlijk wat het was. Hij is teruggegaan (…) en de doos bleef in de auto.

Deze officier vertelt dat op basis hiervan is besloten om niet in te grijpen, omdat anders het onderzoek 'stuk' zou gaan en omdat het opsporingsteam niet 100% zeker wist dat er een wapen aanwezig zou zijn. Een ander voorbeeld komt naar voren in een eerder aangehaald opsporingsonderzoek. In deze zaak is binnengedrongen in een camerasysteem van een kantoor op basis waarvan kon worden bepaald welke ruimtes interessant waren voor verder onderzoek. De hackbevoegdheid is vervolgens gebruikt om een andere bijzondere opsporingsbevoegdheid, het opnemen van vertrouwelijke communicatie, goed uit te kunnen voeren.
Ten tweede geeft sturingsinformatie input voor het zo goed mogelijk kunnen vormgeven van een actiedag. Dat is de dag waarop een onderzoek 'klapt', één of meerdere verdachten worden aangehouden en de heimelijke fase van het opsporingsonderzoek eindigt. Eén van de geïnterviewde officieren vertelt dat de hackbevoegdheid heeft geholpen om te bepalen bij wie opsporingsteams moesten zijn op die betreffende actiedag:

> We zaten op dat moment in de fase, we waren natuurlijk met de klapdag aan het werk, we hadden natuurlijk ook al heel veel sturingsinformatie. We hadden ook al het nodige bewijs binnen dankzij Enchrochat en ook gewoon daarvoor al dankzij de traditionele opsporing. Maar we waren wel qua sturing op zoek naar bij wie moeten wij echt gaan klappen op die actiedag?

Het onderzoek waarover deze officier van justitie vertelt richtte zich op drugshandel. Op de actiedag is uiteindelijk een drugslab opgerold waarbij een grote hoeveelheid ketamine in beslag is genomen. Ook zijn die dag alle verdachten die het opsporingsteam op het oog had aangehouden en zijn er gegevensdragers in beslag genomen. Een ander voorbeeld van de wijze waarop sturingsinformatie ondersteuning kan bieden bij een actiedag heeft betrekking op kinderpornozaken. In zulke zaken kan de hackbevoegdheid onder andere informatie opleveren over de wijze waarop een verdachte zijn beveiliging heeft geregeld. Dit kan helpen om ervoor zorgen dat de inbeslaggenomen informatie beschikbaar blijft voor de opsporing, en niet ter plekke vernietigd of versleuteld wordt.

Het voorgaande richtte zich vooral op sturingsinformatie die richting geeft aan het onderzoek waarbinnen de hackbevoegdheid is ingezet. Informatie verkregen met de hackbevoegdheid kan ook, al dan niet indirect, van nut zijn voor andere opsporingsonderzoeken. Zo is bijvoorbeeld informatie over actuele *ransomware*

onderzoeken gedeeld met het buitenland. Een ander voorbeeld, van een meer indirecte bijdrage, is een onderzoek naar de gebruikers van een cryptocommunicatiedienst, een zogenoemd Titel V-onderzoek. Het doel van dit opsporingsonderzoek was om zicht te krijgen op de gebruikers van deze dienst omdat het vermoeden was dat deze dienst vooral personen met criminele intenties tot haar klantenkring rekende. Informatie verzameld met behulp van de hackbevoegdheid (sleutels) heeft er mede toe bijgedragen dat uiteindelijk (door de inzet van andere bevoegdheden dan de hackbevoegdheid) zicht kon worden verkregen op de gebruikers. De uitkomsten van het Titel V onderzoek zijn met andere opsporingsteams gedeeld zodat zij opsporingsonderzoeken konden starten naar individuele gebruikers van deze cryptocommunicatiedienst, de zogenoemde Titel IV-onderzoeken.

Sturingsinformatie wordt bewijs
Hoewel zojuist bewijs en sturingsinformatie los van elkaar zijn besproken, zijn beide type informatie in de praktijk niet altijd zo scherp van elkaar te scheiden. Informatie verzameld met de hackbevoegdheid hoeft niet altijd óf sturingsinformatie te zijn óf bewijs. Dat geldt bijvoorbeeld voor het eerdergenoemde onderzoek naar een moord waarin op basis van chatcommunicatie de betrokkenheid van twee verdachten duidelijk wordt. Tegelijkertijd blijkt uit deze communicatie ook dat nog andere mensen betrokken zijn geweest. In dit geval is de chatcommunicatie bewijs voor de eerste twee verdachten, en sturingsinformatie voor de betrokkenheid van anderen. Een geïnterviewde officier van justitie licht met een (ander) hypothetisch voorbeeld toe hoe informatie zowel als sturing en als bewijs kan worden gebruikt.

> Iets kan ook sturing zijn in die zin dat (..) je een bericht leest van, nou Danny[112] is eigenlijk niet meer zo betrouwbaar. Dan geeft mij dat dan sturing. Dan denk ik ja, ze vertrouwde Danny niet meer. Ze zullen (…) [hem] waarschijnlijk niet meer inzetten voor grote transporten. (…). Maar het kan ook wat zeggen over de verhoudingen in een criminele organisatie dat iemand anders kan besluiten: we zetten Danny niet meer in. Dat is dan in die zin ook weer bewijs. Iemand bepaalt wat Danny waard is.

Informatie die eerst sturingsinformatie was, kan op een later moment ook bewijs worden. Dat zou bij het eerdergenoemde moordvoorbeeld het geval kunnen zijn, wanneer uiteindelijk ook die ‘anderen’ dan de twee oorspronkelijke verdachten van het plegen van een moord, worden opgepakt en vervolgd.

Intelligence
Naast sturing en bewijs is er een derde manier waarop gegevens van de hackbevoegdheid worden benut, zo geven enkele officieren van justitie aan, namelijk als intelligence. In die gevallen waren de verzamelde gegevens een bijproduct van een concreet uitgevoerd opsporingsonderzoek. Het betreft informatie die niet direct relevant is voor een concreet opsporingsonderzoek, maar wel een beeld schetst dat voor toekomstige onderzoeken relevant kan zijn, bijvoorbeeld omdat de informatie helpt bij het duiden van criminele activiteiten en trends. Eén van de geïnterviewde officieren legt uit dat de informatie verzameld met behulp van de hackbevoegdheid zicht heeft gegeven op bepaalde ‘financiële en verdovende middelen lijnen’ die richting een bepaald land liepen. Een andere officier van justitie vertelt dat gegevens (indirect) verzameld middels een hack, ervoor hebben gezorgd dat opsporingsinstanties beter zicht hebben gekregen op de omvang van het fenomeen georganiseerde criminaliteit en op de verschillende (criminele) netwerken die er zijn. Deze officier is betrokken

[112] Gefingeerde naam.

geweest bij meerdere opsporingsonderzoeken ten aanzien van cryptocommunicatiediensten. Van de onderzoeken waaraan deze officier van justitie refereert, heeft Nederland in één onderzoek zelf uitvoering gegeven aan de hackbevoegdheid. Deze officier van justitie zegt:

> Gegevens [uit deze onderzoeken] worden met elkaar vergeleken (…) dat geeft echt wel een goed zicht op de netwerken en daardoor zie je hoe internationaal alles is. Voor criminelen bestaan grenzen natuurlijk helemaal niet. We denken dat alles in Amsterdam gebeurde, maar dat is gewoon internationaal natuurlijk. Ze vliegen overal naartoe, komen overal vandaan. Overal waar geld (…) te verdienen is. Dus dat geeft wel een heel goed beeld van. Wat je zonder dat je die telefoons zou kunnen bekijken, dan had je dat beeld niet.

Hoofdpunten

- In een ruime meerderheid van de inzetten lukt het om een geautomatiseerd werk binnen te dringen en gegevens te verzamelen. Wanneer dit niet lukt, liggen hier technische of tactische redenen aan ten grondslag.
- In 40% van de onderzoeken leidt de inzet van de hackbevoegdheid niet tot een bruikbare opbrengst voor het opsporingsonderzoek. In ongeveer een derde van de onderzoeken leveren de gegevens sturingsinformatie op en in ongeveer een derde van de onderzoeken bewijs. Tussen deze categorieën zit overlap, omdat in negen onderzoeken de verzamelde gegevens én als sturingsinformatie én als bewijs hebben gediend.
- Bij bewijs gaat het om verschillende soorten bewijs zoals inzicht in gepleegde strafbare feiten, zicht op andere personen die strafbare feiten plegen en de mate van betrokkenheid bij het plegen van strafbare feiten of juist een gebrek daaraan (ontlastend bewijs). De zwaarte van het bewijs verschilt. Soms is sprake van essentieel bewijs, maar er kan ook sprake zijn van brokjes bewijs.
- Bij sturingsinformatie gaat het om informatie waarmee vervolgstappen worden bepaald zowel binnen als buiten het opsporingsonderzoek waarbinnen de hackbevoegdheid is ingezet.
- In een enkel geval worden de verzamelde gegevens gebruikt als intelligence. De verzamelde gegevens zijn dan een bijproduct van een concreet uitgevoerd opsporingsonderzoek.

7.3.3 Behandeling door de rechtbank

Wanneer een opsporingsonderzoek is afgerond, beslist het Openbaar Ministerie of de zaak wordt voorgelegd aan een zittingsrechter. In tabel 7.7 staat weergegeven op welke wijze de zaken waarin de hackbevoegdheid is ingezet, zijn afgedaan.

Tabel 7.7 Behandeling zittingsrechter

Behandeling van de zaak	Aantal	%[a]
De zittingsrechter heeft een uitspraak gedaan over de zaak	19	29%
Er is alleen nog een pro forma zitting geweest.	14	22%
De zaak moet nog door een zittingsrechter worden behandeld.	13	20%
Andere afronding*	11	17%
De zaak zal niet door een zittingsrechter behandeld worden.	8	12%
De zaak wordt momenteel behandeld in de rechtbank, maar de zittingsrechter heeft nog geen uitspraak gedaan.	1	2%

* Bij andere afronding ging het onder andere om dat het onderzoek nog liep (2), de zaak deels op zitting behandeld was/ zal worden (2) en de zaak geseponeerd was (1). Andere antwoorden binnen deze categorie waren dat de zaak is opgelegd en wellicht als een cold case zal worden opgepakt (1) en dat de zaak een executiezaak betrof waarin de hackbevoegdheid is ingezet (1). Ook was het in sommige zaken onbekend of een zittingsrechter zich over de zaak heeft gebogen of zal gaan buigen (4).

a Berekend ten opzichte van het totaal aantal vragenlijsten dat is ingevuld en meegenomen in de analyse (65 = 100%).

Uit tabel 7.7 volgt dat een zittingsrechter zich inmiddels over 20 van de 65 zaken, waarover een vragenlijst is ingevuld, inhoudelijk heeft gebogen. In 19 van die zaken is een uitspraak gedaan, in elk geval in eerste aanleg. In 27 van de 65 zaken zal een zittingsrechter zich nog inhoudelijk over de zaak buigen.

Op basis van de vonnisanalyse blijkt dat in 8 van de 9 zaken de verdachte is veroordeeld voor één of meer van de ten laste gelegde feiten. Verder blijkt uit de vonnisanalyse, maar ook uit de interviews, dat de hackbevoegdheid doorgaans niet besproken wordt tijdens de zitting of terugkomt in het gepubliceerde vonnis. Slechts in één vonnis wordt expliciet verwezen naar Digit-dossiers.

Inhoud verweer

In drie zaken uit de vonnisanalyse heeft de advocaat, voor zover bekend, de inzet van de hackbevoegdheid ter discussie gesteld.[113] In al deze zaken richtte het verweer zich deels op dezelfde en deels op andere aspecten van de inzet van de hackbevoegdheid. Een deel van de verweren had expliciet het doel om tot bewijsuitsluiting te komen. In de eerste zaak, waarin het ging om voorbereidingshandelingen voor harddrugs gerelateerde feiten (Sky-ECC), het medeplegen van een woninginbraak, fraude met corona QR-codes en vuurwapenbezit, richtte het verweer zich op de waarborgen voorafgaand aan de inzet van de hackbevoegdheid. Uit het dossier zou niet blijken dat de juiste procedure is gevolgd. Het ging hierbij om de interne procedure van het Openbaar Ministerie die regelt dat het College van PG's uiteindelijk toestemming moet geven voor het vorderen van een machtiging bij de rechter-commissaris. De rechtbank verwerpt dit verweer, omdat deze interne regels 'geen recht in de zin van de wet op de rechterlijke organisatie' zijn. Bovendien maakt dat soort stukken geen onderdeel uit van het strafdossier waardoor de verdediging aan die stukken geen rechten kan ontlenen (ECLI:NL:RBDHA:2023:1960). In de tweede zaak luidde het verweer dat sprake zou zijn geweest van verschillende vormfouten, niet alleen gerelateerd aan de

[113] Het betreft hier alleen zaken waarin de zaak zelf een bevel is afgegeven voor de hackbevoegdheid én waarbij Nederlandse autoriteiten zelf de hackbevoegdheid hebben ingezet. De laatste paar jaar heeft een zittingsrechter ook zaken behandeld (zogenoemde Titel IV-onderzoeken) die zijn gestart op basis van een Titel V-onderzoek waarin de hackbevoegdheid is ingezet. Gevoerde verweren in het kader van deze Titel IV-onderzoeken zijn niet meegenomen in de vonnisanalyse.

hackbevoegdheid. Uit de reactie van de rechtbank blijkt dat het wat betreft de hackbevoegdheid gaat om de waarborgen voorafgaand aan de inzet, namelijk het bevel van de officier van justitie en de keuring van het technisch hulpmiddel. De rechtbank gaat alleen mee met het tweede verweer ten aanzien van de keuring, al heeft zij daar geen consequenties aan verbonden. Wat betreft het bevel merkt de rechtbank op dat het bevel pas is afgegeven na een machtiging van de rechter-commissaris. Bovendien lag aan het bevel een proces-verbaal ten grondslag dat voldoende grond vormde voor een verdenking (ECLI:NL:RBOVE:2024:2048). Wat betreft de inzet van een niet gekeurd middel merkt de rechtbank op dat de inzet van een niet-gekeurd middel mogelijk is, ook als dat niet gekeurd zal gaan worden, op basis van artikel 21, lid 4 Bogw. Wel stelt de rechtbank vast dat in de processtukken niets te vinden is van de vereiste vermeldingen op basis van artikel 21, lid 3 en 4 Bogw. De rechtbank stelt dat dit vormverzuim hersteld zou kunnen worden door de behandeling van de zaak aan te houden. De rechter besloot echter het onderzoek niet te heropenen, omdat de rechter dat niet nodig achtte. De belangrijkste reden hiervoor was dat, zelfs als het vormverzuim onherstelbaar zou zijn, de rechtbank het verweer uiteindelijk zou moeten verwerpen, omdat de verdediging onvoldoende duidelijk had gemaakt tot welke rechtsgevolg het vormverzuim zou moeten leiden (ECLI:NL:RBOVE:2024:2048).

In de derde en laatste zaak (ECLI:NL:RBOVE:2024:1255) heeft de advocaat twee verweren. Het eerste verweer, dat volledig is gericht op de hackbevoegdheid, bepleit dat er gegevens in het buitenland verzameld zouden zijn en dat hier in het dossier geen toestemming voor te vinden is. De rechtbank gaat hier niet in mee, omdat de bevoegdheid niet ingezet zou zijn terwijl de verdachte zich op buitenlands grondgebied bevond. Mocht dit wel het geval zijn geweest, dan zou de verdachte alsnog geen beroep kunnen doen op bewijsuitsluiting, omdat een eventuele inbreuk op de soevereiniteit van de staat geen belang van de verdachte is.

Mogelijke verklaring geen verweer

Het voorgaande laat zien dat, voor zover bekend, advocaten weinig verweer voeren ten aanzien van de inzet van de hackbevoegdheid. Ook uit een groot deel van de interviews blijkt dat advocaten doorgaans geen verweer voeren. Eén van de geïnterviewde officieren van justitie merkt overigens op dat dit niet alleen geldt voor de hackbevoegdheid, maar voor de inzet van bijzondere opsporingsbevoegdheden in het algemeen. Tijdens de interviews komen verschillende mogelijke verklaringen voorbij. Belangrijk om hierbij op te merken is dat deze verklaringen vooral door officieren van justitie worden aandragen. Het is helaas voor dit onderzoek nauwelijks gelukt om advocaten te spreken die zelf ervaring hebben met zaken waarin de hackbevoegdheid is ingezet.

Ten eerste zou een advocaat niet veel in te brengen hebben tegen de hackbevoegdheid. Daarbij gaat het bijvoorbeeld om bezwaren ten aanzien van de subsidiariteit en proportionaliteit van de inzet. Eén van de officieren, betrokken bij een onderzoek naar de handel in verdovende middelen, zegt:

> Ik denk dat ze totaal geen brood zagen om hier verweer op te voeren. Kijk, de inzet is natuurlijk gewoon gerelateerd in het dossier. Als je kijkt naar de ernst van de verdenking, haal je gewoon die hobbel heel makkelijk. En het dossier heeft ook voldoende aangetoond dat andere middelen, minder zware middelen, een minder goed beeld gaven. (….) Dat heeft natuurlijk ook te maken met de geraffineerdheid van de criminele organisatie. Hoe bewust zij zich waren van observaties, inzet van

> TAP en OVC enzovoorts. Dan is het natuurlijk ook vrij logisch dat je dan naar een middel als de hackbevoegdheid grijpt. Dus die proportionaliteit en de subsidiariteit die waren verantwoord. (…) Dan zou ik eerlijk gezegd ook niet zo goed weten welk verweer de verdediging op zinnige wijze kan voeren.

Deze officier merkt ook op dat er binnen het Openbaar Ministerie een interne toetsing is, de CTC-route, en deze zou strenger zijn dan de toetsing door de rechter-commissaris bij afgifte van een machtiging.

Een andere reden waarom een advocaat niks tegen de inzet van de hackbevoegdheid zou inbrengen, is dat het bewijs niet alleen afkomstig is uit gegevens verzameld met behulp van de hackbevoegdheid, maar ook uit andere bevoegdheden. Eén van de geïnterviewde officieren zegt bij voorkeur in zijn zaak niet alleen te leunen op de hackbevoegdheid:

> Iets als een hack is natuurlijk wel een beetje kwetsbaar. Alhoewel, ik denk eerlijk gezegd, bij de meeste hacks, als we dat gewoon netjes hebben opgebouwd, is dat niet zo'n probleem. Maar als je op één proces-verbaal, of dat nou een hack is, of een wat dan ook, de hele zaak bouwt, en dat ene pootje gaat er onder uit, dan heb je best een probleem. (…) Ik probeer altijd wel twee of drie steunpilaren onder een gebouw te zetten. Of dat nou een hack is of wat dan ook. Dat vind ik een beetje te kwetsbaar.

Een concreet voorbeeld van een combinatie van bevoegdheden die een aantal keer genoemd wordt, is de inbeslagname van een telefoon die (ook) gehackt is. Vaak gebeurt zo'n inbeslagname bij de aanhouding. Als daarop dezelfde gegevens als de hackgegevens (en soms meer) te vinden zijn, dan heeft de verdediging daar 'niks te winnen' aldus een andere geïnterviewde officier van justitie. Bovendien levert de hackbevoegdheid in dit geval geen 'direct bewijs' op. Eén van de geïnterviewde advocaten herkent dat er iets te winnen moet zijn. Deze advocaat legt uit dat een advocaat handelt vanuit het belang van zijn cliënt, zoals bijvoorbeeld verweer voeren met als doel het uitsluiten van belastend bewijs. Deze advocaat geeft echter aan dat 'bewijsuitsluiting in de Nederlandse rechtspraak een unicum aan het worden is'. Iets anders waar een cliënt wat aan zou kunnen hebben is strafvermindering. Deze advocaat richt zich, zeker bij cybercrimeverdachten, liever daarop. Hierbij is het volgens hem wel van belang dat een verdachte laat zien dat hij/zij inzicht heeft in zijn/haar handelen. Volgens deze geïnterviewde advocaat werkt het dan minder in het voordeel van de verdachte wanneer de verdediging zich richt op procedurele aspecten.

Een laatste reden is dat de inzet van de hackbevoegdheid mogelijk onvoldoende opvalt in het dossier. Een inzet van de hackbevoegdheid wordt altijd verantwoord in het zogenoemde 'methodiekendossier'. Op die plek zou een advocaat in elk geval kunnen zien dat de hackbevoegdheid is ingezet. Op andere plekken hoeft niet expliciet te worden genoemd dat de hackbevoegdheid is ingezet. Soms wordt de hackbevoegdheid verder niet genoemd, omdat uiteindelijk gegevens verzameld met andere bevoegdheden, zoals een inbeslagname, in het dossier komen. Het kan ook zijn dat vanwege afscherming niet expliciet gesproken wordt over de hackbevoegdheid. Eén van de geïnterviewde officieren legt uit dat in de zaak die deze officier van justitie behandelde in het 'relaas proces-verbaal' niet expliciet gesproken wordt over de inzet van de hackbevoegdheid. Dat is een bewuste keuze geweest om het gebruik van de hackbevoegdheid af te schermen. Een andere officier van justitie besteedt er in het tactisch dossier 'een notitie' aan, en verder niet meer dan nodig. Dat de

hackbevoegdheid is ingezet staat niet met 'koeienletters' op het dossier, aldus deze officier van justitie.

Hoofdpunten

- In net iets minder dan een derde van de opsporingsonderzoeken heeft een zittingsrechter zich inhoudelijk gebogen over de zaak, en in bijna al deze zaken is ook een uitspraak gedaan. In net iets meer dan een derde van de opsporingsonderzoeken zal een zittingsrechter zich nog over de zaak gaan buigen.
- In de gepubliceerde vonnissen wordt nauwelijks expliciet aandacht besteed aan de inzet van de hackbevoegdheid. Voor zover bekend heeft de advocaat slechts in drie zaken verweer gevoerd met betrekking tot de hackbevoegdheid.

7.3.4 Voordelen voor de opsporingspraktijk

De hackbevoegdheid heeft een aantal voordelen voor de opsporingspraktijk. In de eerste plaats kunnen opsporingsteams met behulp van de hackbevoegdheid toegang krijgen tot informatie waar zij voorheen met andere bevoegdheden geen of moeilijker toegang toe zouden hebben gehad. In veel onderzoeken, de standaardzaken, gaat het om informatie die zich op een telefoon bevindt, bijvoorbeeld communicatie. Een officier van justitie vertelt:

> Elke crimineel heeft constant communicatie nodig om zijn criminele werk goed te kunnen doen. En als je nou net op dat punt binnenkomt waar die lijnen bij elkaar komen, dan heb je goud in handen. En omdat men zich bewust is van andere middelen, maar niet dit los kan laten. (…) Al je telefoons wegdoen en alleen nog maar met briefjes werken of dingen influisteren, maar weinigen is dat gegeven. Uiteindelijk moet er toch gewoon constant gestuurd worden. En dan kom je vaak op telefoons uit. En als je juist op dat knooppunt mee kan kijken, is het geweldig interessant.

Ook in de maatwerkzaken hebben opsporingsdiensten toegang gekregen tot informatie waartoe zij voorheen niet of moeilijker toegang toe kregen. Daarbij gaat het bijvoorbeeld om het live kunnen mee kunnen kijken naar de inhoud van het Tor-verkeer. Een ander voorbeeld is dat toegang kan worden verkregen tot servers waardoor het bijvoorbeeld mogelijk is om een netwerk te ontmantelen dat zich met botnets bezighoudt.

Een tweede voordeel waarop verschillende geïnterviewden wijzen, is dat een opsporingsonderzoek door de inzet van de hackbevoegdheid soms minder ingrijpend kan zijn voor de verdachte en zijn omgeving. Dat heeft in de eerste plaats te maken met het feit dat een onderzoek met de hackbevoegdheid gerichter en zonder de inzet van sommige andere (ingrijpende) bijzondere opsporingsbevoegdheden kan plaatsvinden. Eén van de geïnterviewde officieren van justitie die onderzoek deed naar een versleutelde communicatiedienst legt uit dat wanneer de hackbevoegdheid er niet geweest was en er toch onderzoek had moeten plaatsvinden naar deze dienst, de totale privacy inbreuk groter was geweest. Die zou vooral zijn veroorzaakt door het feit dat er in dat scenario andere bijzondere opsporingsbevoegdheden ingezet hadden moeten worden ten aanzien van een grotere groep mensen, zoals bijvoorbeeld doorzoekingen en observaties. Een aantal officieren van justitie vraagt zich daarom hardop af of andere bevoegdenheden niet ingrijpender zijn dan de hackbevoegdheid. Eén van hen legt uit:

> Want wat je in een klassiek model optuigt, is een tap en een OVC in een woning, dan ben je bij iemand heimelijk naar binnen gegaan in zijn huis. Daar heb je afluisterapparatuur in iemands huis ingebracht. Je hebt misschien undercovers ingezet, je hebt alles opgetuigd. (…). Je zou kunnen zeggen, dit [inzet van de hackbevoegdheid] is ook een hele zware inbreuk (…), maar ik heb liever dat je in m'n telefoon zit dan dat je in m'n huis zit.

Een andere officier maakt onderscheid tussen de juridische en praktische ingrijpendheid. Deze officier van justitie legt uit dat juridisch gezien de hackbevoegdheid 'vrij ver' gaat, de impact van de hackbevoegdheid vanuit praktisch oogpunt meevalt, omdat in de praktijk opsporingsteams 'niet alles kunnen zien wat iemand doet'. Dat heeft onder andere te maken met het feit dat een inzet van de hackbevoegdheid lang niet altijd succesvol is. Een ander aspect waarom de inzet van de hackbevoegdheid volgens geïnterviewden als minder ingrijpend wordt beschouwd, is dat de hackbevoegdheid de mogelijkheid biedt om minder ingrijpende aanhoudingen te verrichten ('zonder het raam eruit te blazen'). Het gaat hierbij vooral om aanhoudingen waarbij de politie wil voorkomen dat een verdachte zijn gegevensdrager versleutelt.

Een derde voordeel tot slot, die een enkele officier van justitie noemt, is dat een opsporingsonderzoek door de inzet van de hackbevoegdheid efficiënter kan worden uitgevoerd. Dat heeft vooral te maken met het feit dat met de hackbevoegdheid sneller de benodigde gegevens verzameld kunnen worden dan met andere opsporingsbevoegdheden, zoals een infiltratietraject. Bovendien kan de hackbevoegdheid helpen om gerichter andere bijzondere opsporingsbevoegdheden in te zetten.

Hoofdpunten

- De hackbevoegdheid heeft een aantal voordelen voor de opsporingspraktijk: 1) opsporingsinstanties krijgen toegang tot gegevens waartoe zij voorheen geen toegang toe hadden; 2) opsporingsinstanties kunnen op een minder ingrijpende manier onderzoek doen; en 3) een opsporingsonderzoek kan efficiënter worden uitgevoerd.

7.3.5 Aandachtspunten

Vooral op basis van de interviews is, vanuit tactisch opsporingsperspectief, een aantal aandachtspunten onderscheiden. Ten eerste is de hackbevoegdheid geen wondermiddel. Ten tweede slaagt de inzet niet altijd. Ten derde is de capaciteit om een inzet uit te voeren beperkt. Ten vierde kunnen inzetten met een buitenland component problematisch zijn. Tot slot is de periode waarbinnen de hackbevoegdheid moet worden ingezet een aandachtspunt.

Geen wondermiddel

Het eerste aandachtspunt is dat de hackbevoegdheid geen wondermiddel is. Sommige geïnterviewden geven aan dat er soms het beeld bestaat dat de hackbevoegdheid altijd het doorslaggevende bewijs oplevert in een opsporingsonderzoek. De praktijk leert dat dit veel vaker niet dan wel het geval is. In dat opzicht werkt het met de hackbevoegdheid niet anders dan met andere bevoegdheden, zo legt één van de geïnterviewde officieren van justitie uit:

> Ik heb wel eens gedacht dat het een ei van Columbus was, maar dat is het niet. (…) Een soort hoop op iets, waar die hoop dan vandaan kwam, dat weet ik ook niet zo goed. Als je een observatieteam in laat zetten, of een tap of een OVC, ben je ook altijd afhankelijk van de juiste omstandigheden en de juiste momenten. Maar hier denk je natuurlijk, zo'n technische alleskunner, 'wauw, dit is echt, dit moet het zijn'. (…) En dan merk je ook, (…), daar ben je ook nog steeds afhankelijk van momenten, van techniek, wat wel of niet kan, wat haalbaar is, van capaciteit. Dus alle zelfde, in potentie denk ik, issues als bij de andere opsporingsmiddelen.

Deze officier van justitie merkt op dat de hackbevoegdheid wel 'een belangrijke uitbreiding' is op het bestaande arsenaal aan bevoegdheden. Bijvoorbeeld wanneer andere bevoegdheden niet kunnen worden gebruikt, omdat de politie te maken heeft met een zeer alerte verdachte ten aanzien van de gebruikelijke onderzoeksmogelijkheden van de politie. Een mogelijke verklaring voor het feit dat de hackbevoegdheid geen wondermiddel is kan liggen in het feit dat de hackbevoegdheid zich veel richt op zogenoemde 'voortdurende delicten', aldus een andere officier van justitie die goed zicht heeft op de opsporingsonderzoeken waarin een hack heeft plaatsgevonden. Deze geïnterviewde geeft drugshandel als voorbeeld. Om zo'n delict te bewijzen moeten vaak allemaal kleine brokjes bewijs worden verzameld die een 'totaalplaatje' moeten opleveren waaruit blijkt dat iemand zich bezighoudt met drugshandel.

Inzet lukt niet altijd

Het tweede aandachtspunt is dat de inzet van de hackbevoegdheid lang niet altijd succesvol is met betrekking tot de hoeveelheid bruikbare gegevens dat wordt verzameld. Een belangrijke reden hiervoor is dat het technisch steeds ingewikkelder wordt om bijvoorbeeld toegang te krijgen tot een telefoon. Eén van de geïnterviewden werpt in dat kader de vraag op in hoeverre in de toekomst ervoor gezorgd kan worden dat de politie mee kan lezen met communicatie die *end-to-end* versleuteld is, zodat er in dat opzicht 'geen soort van vrijbrief is voor criminelen'. Dit raakt aan (nog niet beslechte) discussies op Europees niveau over het mogelijk afzwakken van de versleuteling van chatdiensten (Spinner, 2024). Omdat het binnendringen van telefoons steeds lastiger wordt, merkt deze geïnterviewde ook op dat tactische opsporingsteams na zouden moeten gaan of zij ook via andere wegen dan de telefoon, bewijs zouden kunnen verzamelen. Ook andere geautomatiseerde werken kunnen worden binnengedrongen én bewijs opleveren.

Dat het niet altijd (meteen) lukt om de gewenste gegevens te verzamelen heeft drie gevolgen. De eerste is dat in opsporingsonderzoeken waarin haast geboden is, de bevoegdheid niet altijd even goed inzetbaar is. Dat geldt bijvoorbeeld voor kinderpornozaken waarin (vermoedelijk) sprake is van '*hands on*' misbruik. Dit laatste betekent dat vermoedens bestaan dat gedurende de onderzoeksperiode daadwerkelijk seksueel kindermisbruik plaatsvindt en/of zal gaan plaatsvinden. Een geïnterviewde officier van justitie legt uit dat in dat soort gevallen de inzet van de hackbevoegdheid, vanwege het tijdsaspect, bij voorbaat uitgesloten wordt. Het tweede gevolg is dat opsporingsteams terughoudend kunnen worden om de hackbevoegdheid in te zetten, omdat het in hun ogen niets of te weinig oplevert. Een derde gevolg is dat het tactisch onderzoek minder goed kan worden uitgevoerd. Dat geldt bijvoorbeeld voor situaties waarbij verdere acties van het tactisch opsporingsteam afhankelijk zijn van gegevens verzameld met de hackbevoegdheid. Een voorbeeld van zo'n situatie is als de hackbevoegdheid wordt gebruikt in het kader van 'een ruisstrategie' waarbij het doel van het opsporingsteam is om een bepaalde reactie van een verdachte te observeren.

Op het moment dat niet zeker is of de hack zal slagen, is het ook lastiger verdere acties in het kader van een ruisstrategie te plannen. Een ander voorbeeld van het niet goed uit kunnen voeren van een onderzoek is dat cruciale informatie gemist kan worden doordat niet continu gegevensverzameling plaatsvindt. Eén van de geïnterviewde officieren legt uit dat bij een terrorisme onderzoek uit de hack informatie naar voren kwam op basis waarvan het leek dat de verdachte betrokken was bij terroristische activiteiten. Pas veel later in het onderzoek, toen de verdachte al vastzat, kreeg het opsporingsteam zicht op het gehele gesprek dat had plaatsgevonden, waaruit duidelijk werd dat de verdachte juist expliciet afstand had genomen van het terroristische gedachtegoed.

Tijdinvestering en capaciteit

Het derde aandachtspunt is dat een inzet van de hackbevoegdheid arbeidsintensief is. Eén van de tijdrovende aspecten is de procedure die moet worden gevolgd om tot een inzet van de hackbevoegdheid te komen. Deze 'papierwinkel' wordt als lastig ervaren, zeker wanneer de inzet van de hackbevoegdheid niet (direct) lukt. Eén aantal geïnterviewde officieren van justitie vraagt zich af of de procedure zoals die nu is opgetuigd wel in alle gevallen nodig is. Eén van hen trekt bijvoorbeeld de vergelijking met het opnemen van vertrouwelijke communicatie en een tap in een woning en vraagt zich af of bij de hackbevoegdheid 'de privacy echt veel meer in het geding' is dan bij die andere twee bevoegdheden, waarbij de aanvraagprocedure minder tijd in beslag neemt. Eén andere officier van justitie, die het niet per se oneens is met de toetsingsmomenten die er zijn, merkt op dat in sommige gevallen gekeken zou kunnen worden naar een lichtere variant, bijvoorbeeld wanneer het gaat over het inloggen met inloggegevens ('*credentials*') die de opsporing toch al tot haar beschikking heeft. Dat is weliswaar nu mogelijk op basis van de Innovatiewet, maar dit is louter gekoppeld aan een inbeslagname. Nog een andere officier van justitie vertelt dat de inzet van de hackbevoegdheid bij zaken in het 'zwaarste segment' 'vrij standaard' is geworden. Deze officier vraagt zich af of het in die gevallen nog wel nodig is om altijd langs de CTC te gaan.

Een ander aspect dat de inzet van de hackbevoegdheid arbeidsintensief maakt, heeft te maken met de hoeveelheid informatie die met een hack verzameld kan worden. Wanneer het lukt om gegevens te verzamelen, is dat doorgaans een grote hoeveelheid. Verschillende officieren van justitie geven aan dat het uitlezen van deze informatie 'bewerkelijk' is. Eén van de officieren van justitie vertelt dat uiteindelijk gewerkt is met zoekwoorden, omdat het onderzoeksteam op zoek was naar 'toekomstgerichte afspraken'. Sommige officieren van justitie nemen de mogelijk grote hoeveelheid informatie mee in hun afweging op welke wijze de hackbevoegdheid gebruikt zal worden. Eén van hen merkt op dat het kunnen verwerken van de informatie die binnenkomt, een belangrijk criterium is voor de vraag of en hoe de bevoegdheid wordt ingezet.

> En wat soms ook natuurlijk zo is, is dat de informatiestroom 'huge' kan zijn. En dat is ook wel een leermoment voor mezelf geweest. Dat als je hem inzet, dat je misschien zelf ook wat strenger moet zijn in het kaderen. Dus dat je de periode bijvoorbeeld even beperkt tot een aantal dagen, omdat je merkt dat de informatiestroom zo groot is dat die ook niet meer behapbaar is voor de opsporing. (…). We kunnen heel veel informatie binnenhalen, maar als we het niet kunnen verwerken, je bent er wel eigenaar van, van informatie. (…) daar moet je ook steeds beter over nadenken van, kunnen we het ook bewerken? Of moeten we het inderdaad in porties gaan doen?

Net als tijd wordt ook capaciteit genoemd als aandachtspunt. In Nederland is één team beschikbaar, Digit-politie, dat uitvoering mag gegeven aan de hackbevoegdheid. Meerdere officieren van justitie geven aan dat er op dit moment eigenlijk te weinig capaciteit beschikbaar is om alle gewenste inzetverzoeken uit te voeren. Dat gebrek aan capaciteit betekent niet alleen dat niet alle zaken kunnen worden opgepakt, maar ook dat niet alle door het team gewenste onderzoekshandelingen kunnen worden uitgevoerd. Het gaat dan bijvoorbeeld om het opnemen van vertrouwelijke communicatie. De inzet van de hackbevoegdheid vraagt overigens niet alleen een inzet van Digit, maar ook van het tactisch onderzoeksteam, bijvoorbeeld wanneer politiemensen, in het kader van tactische waarborgen[114], ook de inzet van andere bijzondere opsporingsbevoegdheden moet bemensen, zoals een observatieteam. Die benodigde totale capaciteit maakt dat de toegevoegde waarde van de hackbevoegdheid in een onderzoek wel echt duidelijk moet zijn, aldus één van de geïnterviewde officieren van justitie.

Buitenland

Op welke wijze gehandeld moet worden wanneer sprake is van een inzet met een buitenlandcomponent is geregeld in de Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex art. 126nba Sv (Staatscourant, 26 februari 2019, nr. 10277) (hierna Aanwijzing). Kern van deze Aanwijzing is dat in principe toestemming gevraagd moet worden aan het buitenland. Hiervan kan in bepaalde gevallen worden afgeweken. Zoals in ons eerdere rapport opgemerkt regelt deze Aanwijzing alleen de inzet van de hackbevoegdheid in het buitenland en niet vice versa.

Het aantal inzetten met een buitenlandcomponent is relatief beperkt. Uit cijfers van Digit blijkt dat er in de afgelopen periode vijf zaken zijn geweest met een buitenlandcomponent, dat wil zeggen dat een inzet in het buitenland heeft plaatsgevonden. In ons eerdere rapport beschreven wij een aantal kernpunten ten aanzien van de inzet van de hackbevoegdheid in zaken met een buitenlandcomponent (Van Uden & Van den Eeden, 2022, p. 125). Een groot deel van deze kernpunten geldt nog steeds. Zo wordt ook nu nog, vanwege de gewenste afscherming, de keuze gemaakt om sommige maatwerkinzetten niet te doen, omdat anders het betreffende land op de hoogte moet worden gebracht van het feit dat een opsporingsonderzoek plaatsvindt waarin heimelijke bevoegdheden worden ingezet. Daarnaast spelen politieke afwegingen een rol bij de vraag of een inzet passend is. Bij een niet-bevriende natie wordt sneller de keuze gemaakt om de hackbevoegdheid achterwege te laten. In vergelijking met ons vorige rapport zijn er twee nieuwe bevindingen. De eerste is dat het hacken van een telefoon ten behoeve van interceptie van telecommunicatie eenvoudiger lijkt te zijn geworden. Twee officieren van justitie merken op dat er inmiddels jurisprudentie beschikbaar is die het hacken van een telefoon op buitenlands grondgebied gemakkelijker maakt. Zij baseren zich daarvoor op een vonnis van het Europees Hof van Justitie (ECLI:EU:C:2024:372) waarin het Hof schrijft dat het afluisteren van een telefoon, dat op basis van een EU-besluit slechts gemeld hoeft te worden aan het betreffende buitenland in plaats van dat een specifiek toestemmingstraject moet worden gevolgd, ook het infiltreren van een telefoon impliceert. Dat zou betekenen dat het infiltreren van een telefoon met een technisch hulpmiddel slechts gemeld hoeft te worden met behulp van een formulier dat als

[114] Bij aanvullende tactische waarborgen gaat het om maatregelen die een tactisch opsporingsteams neemt omdat gebruiktgemaakt wordt van een technisch hulpmiddel dat niet gekeurd is (Van Uden & Van den Eeden, 2022).

bijlage bij de Europees opsporingsbevel (EOB)-richtlijn is opgenomen. Nieuw aan dit vonnis is dat dit specifiek gaat over het binnendringen van een geautomatiseerd werk.

De tweede bevinding is dat de hackbevoegdheid in het buitenland en de voorwaarden die aan een inzet verbonden zijn niet overal hetzelfde zijn (zie ook Van Berkel et al., 2023). Dat zorgt ervoor dat een inzet in het buitenland doorgaans veel extra regel- en uitzoekwerk vraagt. Eén van de geïnterviewde officieren, die zich bezighoudt met verdachten die internationaal actief zijn, legt uit dat, in tegenstelling tot het opnemen van vertrouwelijke communicatie of een tap, het niet altijd duidelijk is hoe te handelen wanneer verdachten naar het buitenland reizen. Het feit dat de verdachten in de betreffende zaak de grens overgingen, betekende extra uitzoekwerk. Ook wanneer gegevens verzameld zijn en vervolgens gedeeld moeten worden met het buitenland, is extra afstemming nodig, onder andere om te bepalen of de verschillende landen het over hetzelfde hebben.

Inzetperiode
Een laatste aandachtspunt dat een enkele officier van justitie noemt, is dat bij het volgen van een verdachte gedurende een periode regelmatig moet worden gekeken of het verzamelen van gegevens doorgang kan vinden, of dat ingrijpen van de politie nodig is. Zodra strafbare feiten plaatsvinden, zoals bijvoorbeeld kindermisbruik of de handel in wapens, dan moet de politie onder andere op basis van artikel 126ff Sv ingrijpen. Dat betekent dat een onderzoek niet langer heimelijk is. Eén van de geïnterviewde officieren, betrokken bij een onderzoek naar wapenhandel, vertelt dat op een gegeven moment de keuze gemaakt is om nog niet in te grijpen:

> En toen hebben we in de stuurploeg ook voorgelegd van dit is wat we min of meer zien, maar we willen wel graag in de actualiteit komen, want we lezen niet hoe die [de verdachte] aan die wapens komt (…), en ook niet waar die ze bewaart en of die ze bewaart. Dat is nog maar de vraag natuurlijk. En dat werd akkoord bevonden, waarbij je natuurlijk ook weer te maken krijgt met het doorlaatverbod. Dus je moet heel goed nadenken. En in de actualiteit ook bemensen, wat zien we nu gebeuren en wanneer moeten we acteren?

Het verzamelen van informatie gedurende een wat langere tijd kan nodig zijn, omdat sommige feiten pas aangetoond kunnen worden als een verdachte gedurende een langere periode wordt gevolgd. Om te kunnen bewijzen dat iemand ergens een gewoonte van heeft gemaakt, is het bijvoorbeeld belangrijk dat kan worden aangetoond dat een verdachte zich daar niet slechts op één moment mee bezig heeft gehouden.

Hoofdpunten
- Er is een aantal aandachtspunten met betrekking tot de inzet van de hackbevoegdheid: 1) De nieuwe hackbevoegdheid is geen wondermiddel, maar eerder een toevoeging aan het palet van bijzondere opsporingsbevoegdheden; 2) het is geen garantie dat de inzet van de hackbevoegdheid slaagt; 3) een inzet van de hackbevoegdheid kost veel tijd en de opsporingscapaciteit is beperkt; 4) inzetten met een buitenlandcomponent zijn complex; en 5) het is van belang goed na te denken over de precieze periode dat een inzet zal plaatsvinden.

7.4 Sporenaanpak in de beleidsbrief

In deze paragraaf wordt de aandacht gericht op vijf kernaandachtspunten die in de eerste evaluatie naar voren kwamen en wat daarmee na het verschijnen van het eerdere WODC-rapport is gebeurd. Hiervoor wordt onder andere geput uit de beleidsreactie (Yeşilgöz-Zegerius, 2023) die de toenmalig Minister van Justitie en Veiligheid op 7 december 2023 aan de Tweede Kamer stuurde. In deze beleidsreactie neemt de minister niet alleen de WODC-evaluatie mee, maar ook de evaluatie van de PG Hoge Raad (Aben & Luining, 2022) en de periodieke rapportages van de Inspectie Justitie en Veiligheid (Inspectie JenV, 2020;2021;2022). De beleidsreactie kent zes sporen, grotendeels gebaseerd op de kernaandachtspunten die het WODC formuleerde. Alleen het zesde spoor wijkt af van de door ons geformuleerde aandachtspunten.[115] Achtereenvolgens worden de volgende thema's besproken: 1) de wijze waarop kan worden binnengedrongen; 2) de inzet van commerciële middelen; 3) de meldplicht van onbekende kwetsbaarheden; 4) het toezicht door de Inspectie JenV; en 5) de keuring van technische hulpmiddelen.

7.4.1 Wijze van binnendringen – steunbevoegdheid

Om een geautomatiseerd werk te kunnen binnendringen, is het soms nodig om in de buurt van het geautomatiseerd werk te zijn. In die zin vindt een inzet van de hackbevoegdheid niet altijd op afstand plaats, zoals de wetgever wellicht wel voor ogen had. In ons eerste rapport schreven we daarom dat een steunbevoegdheid, zoals die bij sommige andere bevoegdheden bestaat, de praktijk zou kunnen helpen (Van Uden & Van den Eeden, 2022, p. 107). In de beleidsbrief (Yeşilgöz-Zegerius, 2023) staat dat een wetsvoorstel voor het toevoegen van een 'betredingsbevoegdheid' zal worden voorbereid. Op die manier wordt wettelijk geregeld dat de politie 'kortstondig een besloten erf of plaats' mag betreden ten behoeve van de inzet van de hackbevoegdheid. Op het moment van schrijven zijn er voorbereidingen gestart voor dit nieuwe wetsvoorstel. Waarschijnlijk komt dat wetsvoorstel er pas in 2029, na de inwerkingtreding van het nieuwe Wetboek van Strafvordering. Dat betekent dat op dit vlak de situatie voor de opsporingspraktijk nog hetzelfde is. Mocht het voor het binnendringen noodzakelijk zijn in de buurt te zijn van het geautomatiseerd werk, dan wordt nog steeds gezocht naar tactische mogelijkheden die op dat moment beschikbaar zijn. In de eerdere evaluatie werd beschreven dan het dan gaat om de inzet van andere opsporingsbevoegdheden (al dan niet bijzonder) om toegang tot het geautomatiseerde werk mogelijk te maken (Van Uden & Van den Eeden, 2022, p. 90).

7.4.2 Inzet van commerciële middelen

Bij de introductie van de Wet CCIII is erkend dat het nodig zou kunnen zijn dat voor de inzet van de hackbevoegdheid commerciële producten zouden worden aangeschaft, meer specifiek ging het om het aanschaffen van commerciële binnendringingssoftware. Uit het Regeerakkoord (Regeerakkoord 2017-2021) van destijds volgde dat het gebruik van dit soort producten beperkt moest worden, vooral om de markt van onbekende kwetsbaarheden niet te stimuleren. In commerciële producten wordt doorgaans gewerkt met één of meer van dit soort kwetsbaarheden. Om de markt zo min mogelijk te stimuleren werd om die reden een licentiemodel afgesproken. Dit

[115] Het zesde spoort ziet op procedurele of aanvullende waarborgen, vernietigen van gegevens en overige punten. Het gaat om logging, uitbereiding van logging bij stelselmatige observatie, opmaken proces-verbaal, regisserende rol rechter-commissaris ten aanzien van de omgang net geheimhoudersgegevens, technische infrastructuur en stroomlijning regels die van toepassing zijn op de vernietiging van gegevens (Yeşilgöz-Zegerius, 2023, p. 27-32).

betekende dat de aangeschafte software slechts voor één zaak mocht worden gebruikt, en dat daarna een nieuwe licentie moest worden aangeschaft in plaats van dat bij voorbaat enkele licenties werden aangeschaft, die ook voor hergebruik in aanmerking kwamen. Omdat in het overgrote deel van de inzetten gebruik is gemaakt van een commercieel middel concludeerden we dat het afgesproken licentiemodel tot hoge kosten leidde en dat het de vraag was of het afgesproken licentiemodel ervoor zorgde dat de markt van onbekende kwetsbaarheden minder gestimuleerd werd (Van Uden & Van den Eeden, 2022, p. 107).

In de beleidsbrief (Yeşilgöz-Zegerius, 2023) geeft de toenmalig Minister van Justitie en Veiligheid aan dat het licentiemodel wordt afgeschaft: de aanschaf van software om te kunnen binnendringen wordt niet meer beperkt tot één zaak. Daarnaast schrijft deze minister dat het gebruik van binnendringingssoftware 'een uiterste middel' zal blijven. Tegelijkertijd merkt zij op dat in opsporingsonderzoeken waarin de hackbevoegdheid wordt ingezet, minder ingrijpende methoden vaak niet werken. Daarom vermoedt de minister dat commerciële producten 'relatief vaak' zullen worden ingezet. Dat vermoeden is juist gebleken. In deze evaluatie is duidelijk geworden dat in het overgrote deel van de inzetten (74 inzetten) gebruikgemaakt is van een commercieel middel. Dat roept de vraag op of het gebruik van commerciële middelen wel een uiterst middel moet worden genoemd. Uiterst middel wekt immers de suggestie dat het gebruik van een commercieel middel eerder uitzondering is dan regel. In de praktijk is eerder sprake van de omgekeerde situatie.

7.4.3 Meldplicht onbekende kwetsbaarheden

In de Wet CCIII is een wetsartikel (art. 126ffa Sv) opgenomen dat het uitstellen van het melden van een onbekende kwetsbaarheid regelt. In onze eerste evaluatie concludeerden we dat het wetsartikel geen onderscheid maakt wat betreft het soort onbekende kwetsbaarheden dat gemeld zou moeten worden. Dat betekent dat de politie ook kwetsbaarheden dient te melden die zich bevinden in systemen die voor en door personen met criminele intenties zijn ontwikkeld. Bovendien kan de meldplicht samenwerking met buitenlandse partijen bemoeilijken, onder meer wanneer de gebruikte kwetsbaarheid in het buitenland als staatsgeheim is bestempeld (Van Uden & Van den Eeden, 2022, p. 107). Zowel wat betreft het maken van een uitzondering voor systemen van personen met criminele intenties als wat betreft internationale samenwerking heeft de minister aangegeven dat nader onderzoek wordt gedaan naar de wijze hoe hier mee om te gaan. Op dit vlak worden op dit moment voorbereidingen getroffen voor in elk geval het maken van een uitzondering voor bepaalde soorten kwetsbaarheden. Dit wetsvoorstel zal pas gereed zijn na 1 april 2029. Op het terrein van internationale samenwerking moet nog besloten worden wat daarmee gebeurt.

7.4.4 Toezicht door de Inspectie JenV

De Inspectie JenV is nog steeds, zoals wettelijk vastgelegd, belast met het toezicht op de hackbevoegdheid. In onze eerdere evaluatie beschreven wij een aantal aandachtspunten met betrekking tot dit toezichtproces. In de eerste plaats zou in de praktijk gekeken moeten worden wat georganiseerd moet worden om het door de Inspectie gewenste systeemtoezicht van de grond te krijgen. Daarnaast merkten we op dat het goed zou zijn om meer duidelijkheid te krijgen over de wijze waarop het toezicht door de Inspectie tot haar recht kan komen met daarbij oog voor de uitvoering van de bevoegdheid. We kwamen tot die laatste conclusie omdat de Inspectie keer op keer een aantal dezelfde punten constateerden zonder dat duidelijk

was wat daar de consequentie van was (Van Uden & Van den Eeden, 2022, p. 177; p. 180). In de beleidsreactie merkt de minister drie punten op ten aanzien van het toezicht: 1) het hoogwaardig toezicht dient behouden te blijven; 2) het kwaliteitssysteem dient passend te zijn binnen de politieorganisatie en moet 'aansluiten bij het algemene stelsel van opsporingsbevoegdheden'; en 3) er moet voldoende ruimte bestaan voor het onvoorspelbare karakter van de inzet.

De afgelopen jaren is de reikwijdte van het toezicht veranderd. Ten tijde van het verschijnen van de eerste rapporten van de Inspectie was vooral sprake van een vorm van nalevingstoezicht. De Inspectie bekeek per individuele zaak of Digit zich aan de regels had gehouden. Op basis daarvan schreef zij jaarlijks een rapport. Omdat de Inspectie constateerde dat zij al een paar jaar dezelfde bevindingen had opgeschreven en het wettelijk kader en de uitvoering niet veranderden, heeft de Inspectie besloten de reikwijdte van het toezicht te wijzigen. In plaats van het beoordelen van individuele inzetten aan de hand van het wettelijk kader, is zij zich gaan richten op de inrichting en implementatie van een kwaliteitssysteem met behulp van zogenoemd ex-nunc toezicht. Dit betekent dat de Inspectie tijdens de uitvoering van deze inrichting en uitvoering toezicht houdt (De Kleuver, 2024, p. 2). Het kwaliteitssysteem is een belangrijke randwoordwaarde voor het uit kunnen voeren van systeemtoezicht, de vorm van toezicht die werd beoogd met betrekking tot de hackbevoegdheid (*Kamerstukken II*, Handelingen 13 december 2016, nr. 34). Een kwaliteitssysteem houdt simpel gezegd in, zo blijkt uit één van de gespreksverslagen en de reactie hierop van de geïnterviewden, dat Digit zelf een systeem inricht waarmee zij de kwaliteit en de naleving van de hackbevoegdheid realiseert en controleert. Zo'n systeem dient te bestaan uit een samenhangend geheel van onder andere beleid, processen en een controle-instrument. Om dit kwaliteitssysteem op te zetten heeft Digit processtappen geformuleerd: het in kaart brengen van een normenkader, het beschrijven van werkprocessen, het in kaart brengen van risico's en het formuleren van maatregelen om deze risico's te kunnen mitigeren. Er zijn verschillende soorten maatregelen waaraan kan worden gedacht, zoals werkinstructies en het inrichten van interne controles. Een andere processtap is de implementatie van maatregelen. Vervolgens moeten de maatregelen en de werkwijze doorlopend worden geëvalueerd en worden herzien.

Bij systeemtoezicht is het de bedoeling dat de organisatie zelf, in dit geval de politie, de interne controle organiseert. De Inspectie JenV hanteert hiervoor het zogenoemde '*three lines of defense-model'*, waarbij in principe eerst op drie niveaus binnen de politieorganisatie zelf een vorm van controle plaatsvindt. De Inspectie volgt pas na de zogenoemde derde lijn. Voor een dergelijke vorm van controle is het belangrijk dat binnen de organisatie een onafhankelijke afdeling aanwezig is die verantwoordelijk is voor deze kwaliteits- en nalevingsborging en de controle hiervan. Omdat binnen de politie op dit moment een dergelijke kwaliteitsafdeling die hiervoor verantwoordelijk is en aan wie gerapporteerd wordt, niet bestaat, is de verwachting dat dit door de Inspectie gehanteerde model niet volledig ingericht kan worden. Een groot deel van het werk komt als gevolg daarvan bij Digit zelf te liggen.

Als systeemtoezicht volledig kan worden uitgevoerd betekent dit dat de Inspectie zich voornamelijk zal gaan richten op de vraag of het kwaliteitssysteem als geheel functioneert, en of het systeem zodanig is ingericht dat op een goede manier risico's vooraf worden gemitigeerd. Daarnaast zal gekeken worden hoe Digit ermee omgaat als zich toch bepaalde risico's voordoen en of in die gevallen de juiste maatregelen worden genomen. Bovendien is het belangrijk dat risico's en maatregelen worden

aangepast indien omstandigheden wijzigen. Daarnaast zal de Inspectie JenV in principe ook de uitvoering van de hackbevoegdheid blijven controleren op individueel zaakniveau. Dit zal echter op een andere schaal gebeuren dan in de voorgaande jaren. Op het moment van het schrijven van het rapport, heeft Digit de risico's in kaart gebracht. De daarbij passende maatregelen moeten nog worden uitgewerkt.

Een belangrijk verschil met de periode waarin ons eerdere rapport verscheen, zo blijkt uit een aantal interviews, is dat de betrokken actoren, Inspectie, Digit-politie en Digit-OM, veel meer met elkaar in gesprek zijn, ook gedurende het toezichtjaar. Dat betekent dat bevindingen niet alleen aan het einde van een toezichtjaar worden gedeeld, maar dat ook door het jaar heen met elkaar gesproken wordt over hoe het gaat, feedback wordt gegeven en dat op basis daarvan al aanpassingen kunnen plaatsvinden. Een dergelijke werkwijze moet ertoe bijdragen dat 'effectief toezicht' plaatsvindt, zo legt één van de geïnterviewden uit. Dat wil zeggen toezicht waar zowel de samenleving als de politieorganisatie baat bij hebben. Een concreet voorbeeld hiervan is dat de Inspectie en Digit tijdig met elkaar in gesprek zijn gegaan over het door Digit opgestelde procesplan om tot een kwaliteitssysteem te komen, in plaats van achteraf hier uitspraken over te doen. Een ander voorbeeld is het gezamenlijk volgen van een training over wat nodig is om een kwaliteitssysteem en het daarbij behorende systeemtoezicht in te richten. Naast dit belangrijke verschil, zijn een aantal door de Inspectie in eerdere rapportage genoemde punten nog steeds aan de orde. Een deel hiervan is afhankelijk van onder andere wetswijzigingen waaraan gewerkt wordt.

7.4.5 Keuring van technische hulpmiddelen

In onze eerdere evaluatie constateerden wij dat Digit de keuring van technische hulpmiddelen, die bedoeld is om de integriteit, betrouwbaarheid en herleidbaarheid van de verzamelde gegevens te waarborgen, als groot knelpunt zag. Bovendien bleek het haast onmogelijk om met een vooraf goedgekeurd technisch hulpmiddel te werken, iets wat wel de voorkeur van de wetgever genoot. Om die reden pleitten wij ervoor dat alle betrokken actoren gezamenlijk zouden kijken op welke manier het beste gewaarborgd kon worden dat gegevens op een betrouwbare, integere en herleidbare manier verzameld konden worden, ook wanneer gebruik wordt gemaakt van commerciële middelen. Die laatste middelen werden niet ter keuring aangeboden, omdat de Digit officier van justitie, op basis van artikel 21, lid 4 Bogw, had besloten had dat de aard van het middel zich verzette tegen een keuring (Van Uden & Van den Eeden, 2022, p. 133-134; p. 180).

In haar beleidsbrief beschrijft de toenmalig Minister van Justitie en Veiligheid dat een voorstel zal worden uitgewerkt met het uitgangspunt dat alle technische hulpmiddelen 'hulpmiddelen die gegevens automatisch detecteren, registreren en transporteren' voor een keuring aangeboden worden bij een keuringsdienst. Daarnaast is het uitgangspunt niet langer dat bij voorkeur alleen vooraf goedgekeurde technische hulpmiddelen worden ingezet. Dat betekent dat ook technische hulpmiddelen zullen worden gebruikt die niet of niet volledig goedgekeurd zijn. In die gevallen kan een officier van justitie beslissen of het nodig is om 'aanvullende verificatiemaatregelen' te nemen. Dat wil zeggen dat op andere manieren, bijvoorbeeld aan de hand van tactische waarborgen de betrouwbaarheid van de verzamelde gegevens kan worden aangetoond. Voor de hier besproken verandering is een aanpassing van het Besluit nodig waarvoor het Openbaar Ministerie, de betreffende verantwoordelijken binnen de Nationale Politie en andere betrokken partijen overleg met elkaar dienen te voeren.

Dat overleg kan ook leiden tot 'alternatieve effectieve oplossingen' 'of nieuwe inzichten in de normstelling zelf', zo blijkt uit de beleidsbrief van de toenmalig Minister.

In de afgelopen periode is een klein aantal technische hulpmiddelen ter keuring aangeboden. In 2023 zijn twee technische hulpmiddelen gekeurd met een doorlooptijd van respectievelijk vier en vijf weken. In 2024 vonden twee herkeuringen plaats die elk vijf dagen duurde. Verder is er op het moment van schrijven van dit evaluatierapport (juni 2025) op hoofdlijnen niet veel veranderd qua keuringssituatie zoals wij die beschreven in ons eerste rapport. De toenmalig Minister van Justitie en Veiligheid heeft weliswaar een aantal wijzigingen aangekondigd, maar deze zijn nog niet gerealiseerd. Het Besluit is nog niet aangepast, waardoor het oorspronkelijke uitgangspunt geldt dat gewerkt dient te worden met een technisch hulpmiddel dat volledig goedgekeurd is voorafgaand aan een inzet ervan. De verwachting is dat het Besluit nog gewijzigd kan worden vóór inwerkingtreding van het nieuwe Wetboek van Strafvordering.

Daarnaast komt het in de beleidsbrief aangekondigde overleg zeer moeizaam van de grond. Pas eind 2024, ruim twee jaar na het verschijnen van het rapport en een jaar na het verschijnen van de brief van de minister, is het gelukt om een aantal belangrijke betrokkenen, Digit-politie, de Keuringsdienst (beide onderdeel van de Landelijke Eenheid) en het Openbaar Ministerie met elkaar aan tafel te krijgen om de eerste gesprekken te gaan voeren. Verder wordt op dit moment door externe partijen naar de keuring van technische hulpmiddelen gekeken. Het continueren van het moeizaam op gang gekomen overleg met alle betrokkenen blijft om die reden een aandachtspunt, zeker gezien het feit dat wij in onze eerste rapportage constateerden dat juist die gezamenlijke dialoog van belang is. Het is een belang van al deze actoren dat de gegevens die verzameld worden betrouwbaar, herleidbaar en integer zijn. Een ander belangrijk aandachtspunt is dat tot nu toe de hackbevoegdheid slechts sporadisch op zitting aan de orde is geweest. In een aantal interviews wordt aangegeven dat wanneer het keuringsregime aangepast wordt, en het uitgangspunt is dat ook niet (volledig) goedgekeurde hulpmiddelen kunnen worden ingezet, het aan de zittingsrechter zal zijn om de verkregen gegevens te beoordelen. Als het slechts sporadisch bespreken van een inzet op zitting zich in toekomst door zal zetten, dan zal in de praktijk die toets nauwelijks plaatsvinden.

Hoofdpunten

- Het ministerie van Justitie en Veiligheid werkt aan een wetswijziging die een steunbevoegdheid moet introduceren. Deze wijziging zal pas na 1 april 2029, de datum waarop het nieuwe Wetboek van Strafvordering in werking treedt, geïntroduceerd worden.
- Voor de aanschaf van commerciële producten wordt niet langer een licentiemodel gehanteerd: de aanschaf van software om te kunnen binnendringen wordt niet meer beperkt tot één zaak.
- Commerciële producten worden relatief vaak ingezet. Dat roept de vraag op of het gebruik van commerciële middelen wel een uiterst middel moet worden genoemd, zoals de toenmalig Minister van Justitie en Veiligheid in haar beleidsbrief deed. Uiterst middel wekt immers de suggestie dat het gebruik van een commercieel middel eerder uitzondering is dan regel. In de praktijk is eerder sprake van de omgekeerde situatie.
- Wat betreft de meldplicht van onbekende kwetsbaarheden worden op dit moment voorbereidingen getroffen voor in elk geval het maken van een uitzondering voor bepaalde soorten kwetsbaarheden. Dit wetsvoorstel zal pas gereed zijn na 1 april

2029. Op het terrein van internationale samenwerking en de meldplicht is nog geen beslissing genomen wat op dat terrein gewijzigd zou moeten worden.
- De Inspectie JenV is zich, in plaats van het beoordelen van individuele inzetten aan de hand van het wettelijk kader, gaan richten op de inrichting en implementatie van een kwaliteitssysteem met behulp van zogenoemd ex-nunc toezicht. Dit betekent dat de Inspectie tijdens de uitvoering van deze inrichting en uitvoering toezicht houdt. Digit-politie is op dit moment bezig met de ontwikkeling van een kwaliteitssysteem.
- Met betrekking tot het toezicht door de Inspectie JenV is een belangrijk verschil met de periode waarin ons eerdere rapport verscheen, dat de betrokken actoren, Inspectie, Digit-politie en Digit-OM, veel meer met elkaar in gesprek zijn, ook gedurende het toezichtjaar.
- De toenmalig Minister van Justitie en Veiligheid heeft in haar beleidsbrief aangekondigd dat een waarborg met betrekking tot het gebruik van technische hulpmiddelen wordt aangepast: alle technische hulpmiddelen moeten in principe gekeurd worden en er mag gebruikgemaakt worden van technische hulpmiddelen die niet vooraf (goed)gekeurd zijn. De wijziging die hiervoor nodig is van het Besluit is nog niet doorgevoerd. De verwachting is wel dat dit eerder zal gebeuren dan 1 april 2029. Een belangrijke aanname bij deze wijziging was dat een zittingsrechter uiteindelijk het bewijs, verzameld met de hackbevoegdheid, zal wegen. In deze evaluatie is duidelijk geworden dat de inzet van de hackbevoegdheid niet of nauwelijks inhoudelijk besproken wordt tijdens een zitting.
- De door ons geadviseerde dialoog tussen de verschillende betrokkenen bij het keuringsproces is moeizaam van de grond gekomen. Dit moeizaam op gang gekomen overleg blijft een aandachtspunt.

7.5 Tot slot

In dit hoofdstuk is duidelijk geworden dat in de periode april 2021-april 2024 in 89 opsporingsonderzoeken een eerste bevel is afgegeven om de hackbevoegdheid in te zetten. Bijna alle opsporingsonderzoeken richtten zich op één of meer vormen van traditionele criminaliteit. Eén overtreding van de Opiumwet, (poging tot) moord/doodslag en witwassen kwamen het vaakst voor. In tegenstelling tot de naam Wet computercriminaliteit III wellicht doet vermoeden is de hackbevoegdheid slechts sporadisch ingezet voor cybercrime in enge zin. In de opsporingsonderzoeken waarbinnen ten minste één bevel is afgegeven voor de inzet van de hackbevoegdheid mochten 125 geautomatiseerde werken worden binnengedrongen. Het overgrote deel betrof een inzet op een telefoon, de zogenoemde standaardinzetten.

Bij het overgrote deel van de inzetten werd gebruikgemaakt van een commercieel middel, zowel om binnen te dringen als om gegevens te verzamelen. Dit past bij de verwachting die de minister in haar beleidsbrief uitspreekt dat commerciële producten ‘relatief vaak’ zullen worden ingezet. Wel roept dit de vraag op of het gebruik van commerciële middelen een uiterst middel moet worden genoemd. De term uiterst middel wekt de suggestie dat het gebruik ervan een uitzondering is. Ook deze evaluatie heeft wederom laten zien dat het gebruik ervan eerder regel dan uitzondering is.

Er waren verschillende redenen waarom tactische opsporingsteams het noodzakelijk achtten om één of meerdere geautomatiseerde werken binnen te dringen. In de vragenlijst kwamen bijna nagenoeg alle redenen terug waarvan de wetgever

veronderstelde dat deze de komst van de hackbevoegdheid noodzakelijk achtte. Twee redenen sprongen eruit, namelijk de versleuteling van gegevensdragers en de vrees dat de verdachte op de hoogte zou raken van het opsporingsonderzoek. Eén reden werd niet genoemd, namelijk dat andere bevoegdheden minder proportioneel zouden zijn om in te zetten. Die bevinding is opvallend omdat tijdens de interviews juist werd aangegeven dat sommige bijzondere bevoegdheden ingrijpender kunnen zijn dan de hackbevoegdheid. Het voorgaande laat zien dat de veronderstelling van de wetgever grotendeels juist is gebleken.

In dit onderzoek is ook duidelijk geworden dat er zaken zijn waarin de keuze worden gemaakt om de hackbevoegdheid niet te benutten. Een deel hiervan betreft zaken waarvoor de hackbevoegdheid nog (steeds) geen oplossing kan bieden. Dit is een belangrijke nuancering bij de veronderstelling van de wetgever.

Toestemming hebben om de hackbevoegdheid in te zetten betekent niet dat het daadwerkelijk lukt om binnen te dringen en om gegevens te verzamelen. Bij ruim twee derde van de inzetten is het gelukt om binnen te dringen en gegevens te verzamelen. In de ingevulde vragenlijsten lag dat percentage zelfs wat hoger, ruim 80% van de officieren van justitie gaf aan dat het gelukt is om gegevens te verzamelen. Op het moment dat het lukt om een geautomatiseerd werk binnen te dringen, lukt het ook bijna altijd om (deels) gegevens te verzamelen. De verzamelde gegevens betroffen vooral een vorm van communicatie die verloopt via communicatie apps. In dat opzicht lukt om met behulp van de hackbevoegdheid gegevens te verzamelen, ook één van de veronderstellingen van de wetgever. Dat betekent niet dat al deze gegevens bruikbaar zijn gebleken voor een opsporingsonderzoek. In 40% van de onderzoeken leidt de inzet van de hackbevoegdheid niet tot een bruikbare opbrengst voor het opsporingsonderzoek. In ongeveer een derde van de onderzoeken leveren de gegevens sturingsinformatie op en in ongeveer een derde van de onderzoeken bewijs. Tussen deze categorieën zit overlap, omdat in negen onderzoeken de verzamelde gegevens én als sturingsinformatie én als bewijs hebben gediend. De wijze waarop de hackbevoegdheid een bijdrage levert aan de aanpak van computercriminaliteit en andere vormen van ernstige criminaliteit kan dus verschillen, wederom een belangrijke nuancering bij de veronderstelling van de wetgever.

In net iets minder dan een derde van de zaken heeft een zittingsrechter een uitspraak gedaan of zal deze dat op (korte) termijn doen en in ruim een derde van de zaken moet een zittingsrechter zich nog over de zaak buigen. Dit betekent dat een zittingsrechter uiteindelijk in ruim twee derde van de zaken een uitspraak zal doen.

Opvallend aan de zaken die tot nu toe behandeld zijn door een zittingsrechter is dat de inzet van de hackbevoegdheid maar in een zeer klein aantal zaken besproken is. In de betreffende zaken besteedde een advocaat in het verweer aandacht aan de hackbevoegdheid. Deze bevinding is van belang in het licht van de aangekondigde verandering ten aanzien van de keuring van technische hulpmiddelen. Deze keuring moet waarborgen dat de gegevens die verzameld zijn met de hackbevoegdheid betrouwbaar, integer en herleidbaar zijn. Eerder was het de bedoeling dat alleen gewerkt zou worden met vooraf goedgekeurde technische hulpmiddelen. In onze eerdere evaluatie lieten wij zien dat dat niet realistisch is gebleken, onder andere omdat vooral gewerkt werd met commerciële middelen waarvan de officier van justitie had besloten dat de aard ervan zich verzette tegen een keuring. De toenmalig Minister van Justitie en Veiligheid heeft, mede naar aanleiding van deze bevinding, de keuze gemaakt dat alle technische hulpmiddelen ter keuring aangeboden moeten worden en

dat gewerkt kan worden met technische hulpmiddelen die niet (volledig) goedgekeurd zijn. De inzet van een vooraf goedgekeurd middel is zodoende niet langer het uitgangspunt. Indien gewerkt wordt met een middel dat niet (volledig) goedgekeurd is, dan is het aan de officier van justitie om tactische waarborgen in te stellen en aan de zittingsrechter om het bewijs te wegen en daar een oordeel over te vellen. Een dergelijke wijziging, die overigens op dit moment nog niet is doorgevoerd, betekent dat er géén technische hulpmiddelen meer zijn die niet door een keuringsinstantie bekeken zijn. Dat is op zichzelf een goede ontwikkeling, omdat inzichtelijk zal zijn waar eventueel nog risico's zitten ten aanzien van de betrouwbaarheid van de gegevens. Een belangrijk aandachtspunt hierbij is dat deze evaluatie heeft laten zien dat de inzet van de hackbevoegdheid nog nauwelijks besproken is tijdens de behandeling van de zaak door een zittingsrechter. Dat betekent dat een zittingsrechter zich over dit specifieke onderwerp niet buigt en dat de inzet van de bevoegdheid slechts beperkt getoetst wordt. Gezien de ingrijpendheid van de bevoegdheid is dat een belangrijke beperking.

8 Conclusie

Op 1 maart 2019 is de Wet Computercriminaliteit III in werking getreden. Met deze Wet zijn zeven nieuwe of aangepaste wettelijke bepalingen geïntroduceerd: vijf strafbaarstellingen en twee (bijzondere) opsporingsbevoegdheden. De Wet is een opvolger van de Wet computercriminaliteit I en II en werd nodig geacht omdat daarmee 'het juridisch instrumentarium voor de opsporing en vervolging van computercriminaliteit zou kunnen worden versterkt' (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 2). Eerder verscheen een evaluatierapport (Van Uden & Van den Eeden, 2022) over de wijze waarop één bepaling uit de Wet CCIII, de hackbevoegdheid (o.a. art. 126nba Sv), in de praktijk werd toegepast. In dat onderzoek is vooral gekeken naar de technische kant van de inzet van de hackbevoegdheid en niet naar wat de hackbevoegdheid in een opsporingsonderzoek opleverde. Dit rapport bevat een evaluatie van de gehele Wet CCIII, waarbij wordt ingegaan op de opbrengsten van de hackbevoegdheid. De volgende onderzoekvraag stond centraal:

> In hoeverre worden de doelstellingen zoals geformuleerd in de Wet CCIII in de praktijk gerealiseerd?

Om deze onderzoekvraag te beantwoorden is per wettelijke bepaling gekeken naar de veronderstelling van de wetgever inclusief doelstelling, de uitvoering in de praktijk en de gevolgen in meer algemene zin, zowel bedoeld als onbedoeld. In dit concluderende hoofdstuk richt de aandacht zich op het beantwoorden van de hoofdvraag. Er is gekozen om elke strafbaarstelling apart te bespreken, omdat de nieuwe/aangepaste wettelijke bepalingen diverse thema's beslaan die lang niet altijd nauw met elkaar samenhangen. Het hoofdstuk besluit met de bespreking van een aantal overkoepelende thema's.

Voorafgaand hieraan nog het volgende. In dit onderzoek is een combinatie van kwantitatieve en vooral kwalitatieve onderzoeksmethoden gebruikt:
1) documentanalyse, 2) cijfermatige analyse van juridische databestanden (RAC-min), 3) interviews (zowel algemeen als verdiepend), 4) vonnisanalyse en 5) een vragenlijst. Een combinatie van onderzoeksmethoden komt de validiteit van het onderzoek ten goede.

Voor de vonnisanalyse zijn alle beschikbare vonnissen bekeken. Op die manier is een zo volledig mogelijk beeld verkregen van de toepassing van vooral de strafbaarstellingen in de praktijk. Bovendien beschikten wij over vonnissen die niet gepubliceerd zijn. Dat is een belangrijke meerwaarde van deze evaluatie. Wat betreft de afgenomen interviews is voor sommige wettelijke bepalingen met een relatief klein aantal personen gesproken. Deels was dit een bewuste keuze, omdat we ook andere onderzoeksmethoden gebruikten. Deels is het niet gelukt om meer mensen te spreken. Tegelijkertijd spraken we onder meer met personen voor wie de thema's waarop de wettelijke bepaling zich richtte hun specialisatie was, denk bijvoorbeeld aan de hackbevoegdheid en het helen en stelen van gegevens. In dat opzicht is het wel gelukt om de juiste personen te spreken en merkten we dat in gesprekken zo nu en dan naar deze personen verwezen werd. Ondanks de beperkte omvang van het aantal interviews, leveren de resultaten betrouwbare en relevante inzichten op.

8.1 Stelen van gegevens (art. 138c Sr)

Een belangrijke veronderstelling van de wetgever was dat gegevens door artikel 138c Sr beter zouden worden beschermd tegen misbruik ervan. In deze evaluatie is duidelijk geworden dat verdachten vervolgd zijn voor het overnemen van gegevens. In dat opzicht is sprake van betere bescherming, omdat een risico op vervolging bestaat. Of de nieuwe wettelijke bepaling daadwerkelijk een afschrikwekkende werking heeft, kan op basis van deze evaluatie niet worden gezegd.

In de periode maart 2019-april 2024 zijn 39 zaken ingestroomd bij het Openbaar Ministerie en in 15 zaken heeft de rechter een uitspraak gedaan. In 2 zaken is de zaak afgedaan met een OM-beschikking en in 13 zaken is de verdachte veroordeeld voor het 138c-feit. In bijna alle gevallen ging het om werknemers die in een werksituatie gegevens hadden overgenomen. In de meeste zaken is het overnemen niet het enige feit dat ten laste werd gelegd. Het feit werd bijvoorbeeld ten laste gelegd met misdrijven in de (relationele) levenssfeer. In de 138c Sr-zaken ging het vooral om persoonlijke gegevens (persoonsgegevens en foto's en afbeeldingen).

Het nieuwe wetsartikel biedt de opsporingspraktijk en soms ook burgers een aantal voordelen: de juridische omschrijving past goed bij situaties die zich voor kunnen doen in de praktijk, slachtoffers hebben de mogelijkheid om zich te voegen in een strafzaak en er kan uitgebreider opsporingsonderzoek worden gedaan. Daarbij moet meteen worden opgemerkt dat de rechtspraak zich inmiddels verder heeft ontwikkeld. In de wetsgeschiedenis komt naar voren dat artikel 138ab Sr (computervredebreuk) niet geschikt werd bevonden voor de overname van gegevens in werksituaties. Inmiddels heeft de Hoge Raad meerdere arresten gewezen waaruit blijkt dat ook in werksituaties sprake kan zijn van computervredebreuk waardoor niet altijd gekozen zal worden voor artikel 138c Sr. In die situaties is een belangrijke aanleiding voor artikel 138c Sr dus niet meer aanwezig. Tegelijkertijd wordt met betrekking tot dit soort zaken ook de vraag gesteld of het begrip computervredebreuk niet te ver wordt opgerekt (zie Berndsen & Visser, 2022, p. 163).

8.2 Helen van gegevens (art. 139g Sr)

Een belangrijke veronderstelling van de wetgever was dat door de komst van artikel 139g Sr gegevens beter strafrechtelijk zouden worden beschermd tegen misbruik ervan. In deze evaluatie is duidelijk geworden dat verdachten vervolgd zijn voor het overnemen van gegevens. In dat opzicht is sprake van een betere bescherming van gegevens, omdat voor verdachten een risico op vervolging bestaat. Of de nieuwe wettelijke bepaling daadwerkelijk een afschrikwekkende werking heeft, kan op basis van deze evaluatie niet worden gezegd.

In de periode maart 2019-april 2024 zijn 93 zaken ingestroomd bij het Openbaar Ministerie. In 85 zaken was artikel 139g Sr het enige CCIII-feit in de tenlastelegging en in 8 zaken was sprake van een combinatie van CCIII-feiten. In 42 zaken was een eindvonnis beschikbaar. In een ruime meerderheid van die zaken (36) is de verdachte veroordeeld voor het 139g-feit en legde de rechter een straf op. In de meeste zaken waarin artikel 139g Sr ten laste is gelegd draaide het, naast het helen van (vooral) offline en online persoonlijke gegevens, om meerdere feiten. In ruim de helft van de zaken in de vonnisanalyse kwam het artikel samen voor met een vorm van fraude waardoor burgers financieel benadeeld werden. Soms waren het helen van gegevens

en de andere feiten direct aan elkaar gerelateerd. Dat wil zeggen dat de geheelde gegevens gebruikt werden voor het plegen van de andere feiten die in de tenlastelegging stonden opgenomen, bijvoorbeeld geheelde gegevens die gebruikt werden voor fraude. Het aantal gegevens dat geheeld werd, loopt sterk uiteen, al is niet altijd duidelijk geworden om hoeveel gegevens het ging. Wanneer een 139g-zaak datasets met persoonsgegevens betreft kan het gaan om grote aantallen. Bij andersoortige gegevens, zoals fotomateriaal, zijn die aantallen doorgaans kleiner. Dat laatste zegt overigens niets over de mogelijke impact op het slachtoffer.

In deze evaluatie is een aantal aandachtspunten gesignaleerd. Twee belangrijke worden op deze plek uitgelicht. Het eerste aandachtspunt gaat over de strafmaat van één jaar. Wetstechnisch lijkt dit geen logisch keuze, omdat op het helen van goederen een hogere strafmaat staat. Bovendien laat de praktijk zien dat er grote variatie bestaat wat betreft het aantal gegevens dat gestolen kan worden. Het is de vraag of de strafmaat van één jaar in alle gevallen passend is.

Het tweede aandachtspunt heeft betrekking op het kunnen veroordelen voor het helen van gegevens, als deze gegevens door een eigen misdrijf verkregen zijn (naar analogie van de heler-steler-regel). De jurisprudentie laat zien dat rechters verschillend oordelen over dit punt. Mogelijk wordt in de toekomst nog verder doorgeprocedeerd over de vraag of de heler-steler regel ook van toepassing is wanneer gegevens geheeld worden.

8.3 Online handelsfraude (art. 326e Sr)

Een belangrijke veronderstelling van de wetgever was dat met de komst van artikel 326e Sr online handelsfraude strafrechtelijk vervolgd kon worden, en dan vooral grootschalige vormen van online handelsfraude. Hoewel in een groot aantal zaken, vooral vanwege capaciteitsoverwegingen, besloten is niet tot vervolging over te gaan, zijn op basis van artikel 326e Sr verdachten vervolgd en veroordeeld. In deze zaken was echter nauwelijks sprake van zogenoemde grootschalige online handelsfraude.

In de periode maart 2019-april 2024 zijn 279 zaken ingestroomd bij het Openbaar Ministerie. In 91 zaken heeft de rechter een uitspraak gedaan, waarvan in een ruime meerderheid van de zaken de verdachte is vervolgd voor ten minste één 326e Sr-feit. Uit de vonnisanalyse volgt dat in een grote meerderheid van de geanalyseerde vonnissen online handelsfraude samen met andere feiten ten laste is gelegd. Van deze andere feiten kwam oplichting het vaakst voor, gevolgd door witwassen. In bijna al deze zaken ging het om het witwassen van geld verdiend met online handelsfraude.

In de geanalyseerde vonnissen ging het voornamelijk om de frauduleuze verkoop van goederen. Ook kon het gaan om het aanbieden van online diensten. Gemiddeld lag het schadebedrag in de bewezenverklaring rond 2.000 euro per zaak. Het gemiddelde aantal slachtoffers in de bewezenverklaring was vijftien personen per zaak. In bijna alle zaken in de vonnisanalyse is een schadevergoeding geëist. Dat slachtoffers zich konden voegen in een strafzaak was ook een veronderstelling van de wetgever. Een nuancering hierbij is dat het in de vonnisanalyse vooral om zaken ging waarin sprake was van fraude gepleegd middels bestaande online verkoopplatforms en niet om zaken waarin sprake was van tijdelijke websites die ook weer snel de lucht uit gingen. Bij tijdelijke websites is het lastig om een schadevergoeding te vorderen.

Deze evaluatie heeft ook laten zien dat artikel 326e Sr een tegenstrijdigheid in zich heeft. Enerzijds is het artikel eenvoudiger, in vergelijking met het 'gewone' oplichtingsartikel waardoor vervolging van online handelsfraude in potentie gemakkelijker is geworden. Anderzijds is de beschikbare opsporingscapaciteit te beperkt om verdachten op basis van dit eenvoudigere artikel te vervolgen. In een groot aantal zaken heeft het Openbaar Ministerie besloten om niet tot vervolging over te gaan, en in het overgrote deel van deze zaken is een rechter, na een artikel 12-procedure, in deze beslissing meegegaan. De beperkte opsporingscapaciteit was hiervoor een belangrijke reden. Er zijn ook wegen buiten het strafrecht om waarmee online handelsfraude aangepakt wordt. Denk hierbij aan een stopgesprek met verdachten.

Naast de beschikbare opsporingscapaciteit en het ontbreken van grootschaligheid is er nog een aandachtspunt ten aanzien van de mogelijkheid tot vervolging op basis van artikel 326e Sr, namelijk de buitenlandcomponent. Wanneer in een online handelsfraudezaak sprake is van een buitenlandcomponent, bijvoorbeeld een buitenlandse leverancier of een buitenlands rekeningnummer, dan is vervolging ingewikkeld. Zo kan het lastig zijn om de identiteit van de verdachte te achterhalen. Ook dit is een belangrijke nuancering bij de veronderstelling van de wetgever.

8.4 Lokpuber (artt. 248a en 248e Sr)

Een belangrijke veronderstelling van de wetgever was dat minderjarigen beter konden worden beschermd door de artikelen 248a (verleiding minderjarige) en 248e Sr (*grooming*) op een zodanige manier te wijzigen dat de inzet van een lokpuber mogelijk werd. Deze evaluatie heeft laten zien dat het mogelijk is gebleken om een verdachte te veroordelen in een zaak waarin de lokpuber werd ingezet, maar dit is zeer sporadisch gebeurd. Of kinderen inderdaad beter kunnen worden beschermd valt op basis van deze evaluatie niet te zeggen. Wel is duidelijk geworden dat de lokpuber hiervoor nauwelijks is benut.

In de periode maart 2019-april 2024 is er, voor zover bekend, slechts één zaak geweest waarin een verdachte is vervolgd voor het verleiden van een minderjarige en waarin gebruik is gemaakt van een lokpuber. Dit aantal is zeer klein in verhouding tot het totaal aantal 248a- en 248e-zaken waarin de rechter een vonnis heeft uitgesproken (respectievelijk 92 en 58 zaken) en verdachten vervolgd zijn voor het verleiden van een minderjarige of *grooming*. Naast deze zaken is nog een aantal keer met een lokpuber gewerkt. In deze zaken draaide het om andere artikelen dan artikelen 248a en 248e Sr óf is het niet duidelijk geworden of het deze artikelen betrof. Het is dus mogelijk gebleken om een lokpuber ook voor andere strafbare feiten in te zetten. Tot slot heeft de Landelijke Eenheid een pilot gedraaid om in de praktijk te onderzoeken hoe de inzet van de lokpuber vormgegeven zou kunnen worden en wat de mogelijkheden zouden zijn. Deze pilot heeft voor zover bekend niet geleid tot een concrete zaak.

De lokpuber is in de praktijk dus niet vaak ingezet. Belangrijke redenen hiervoor waren de beschikbare capaciteit en het feit dat er al genoeg 'brengzaken' zijn waarin voor andere opsporingswegen gekozen worden. 'Brengzaken' zijn zaken waarin al een aangifte is gedaan en waarin eventueel al een verdachte bekend is. Hoewel de lokpuber in de praktijk niet vaak is ingezet, zijn er in de interviews verschillende mogelijkheden naar voren gekomen met betrekking tot de inzet van een lokpuber,

waaronder een meer proactieve inzet van de lokpuber. In tegenstelling tot een 'brengzaak' hoeft er dan nog geen concrete verdachte op het oog te zijn. Een belangrijke voorwaarde hierbij is dat voldoende capaciteit beschikbaar voor in elk geval de inzet van de lokpuber.

Sinds de inwerkingtreding van de Wet seksuele misdrijven (Wsm) op 1 juli 2024 bestaan de artikelen 248a en 248e Sr niet meer en zijn deze deels opgegaan in de Wsm. In dat opzicht kunnen de in dit onderzoek gesignaleerde aandachtspunten van nut zijn voor de toepassing van de lokpuber in het kader van deze nieuwe wet. De vraag is wel in hoeverre de lokpuber ook in het kader van deze nieuwe wet benut zal gaan worden. In 2024 was er een stijging te zien van meldingen van seksuele delicten in vergelijking met 2023 en zijn er 131 meldingen van *sexchatting* gedaan (Politie, 2025). Dat laat zien dat er genoeg 'brengzaken' zijn. In deze evaluatie werd duidelijk dat in dit soort brengzaken blijkbaar voor andere opsporingswegen wordt gekozen. Daarom lijkt het, vanwege het aantal 'brengzaken', niet voor de hand te liggen dat de lokpuber in de toekomst vaker ingezet zal worden. Dit hoeft overigens geen probleem te zijn, zolang opsporingsfunctionarissen op de hoogte zijn dat de mogelijkheid van de lokpuber bestaat én er voldoende menskracht beschikbaar kan worden gesteld wanneer de inzet van de lokpuber noodzakelijk wordt geacht.

8.5 Ontoegankelijk maken van gegevens (art. 125p Sv)

Een belangrijke veronderstelling van de wetgever was dat door de introductie van artikel 125p Sv, een bevoegdheid om via een aanbieder gegevens ontoegankelijk te maken, strafbare feiten sneller beëindigd zouden kunnen worden of zelfs voorkomen. Op die manier zou de samenleving beter worden beschermd. Deze evaluatie heeft laten zien dat gegevens ontoegankelijk zijn gemaakt op basis van artikel 125p Sv. In dat opzicht is het mogelijk gebleken, in lijn met de veronderstelling van de wetgever, strafbare content (tijdelijk) ontoegankelijk te maken. Op basis van deze evaluatie kan niet worden gezegd in hoeverre de samenleving hierdoor beter wordt beschermd. Tegelijkertijd zijn aanbieders vaak meer dan bereid om op vrijwillige basisgegevens ontoegankelijk te maken. Het precieze aantal zaken waarvoor dit geldt is overigens niet duidelijk geworden. Én zijn er zaken waarin de bevoegdheid nog steeds niet volstaat. Dit zijn belangrijke nuanceringen bij de veronderstelling van de wetgever.

In veertien zaken zijn op basis van artikel 125p Sv gegevens ontoegankelijk gemaakt. Het betrof de ontoegankelijkmaking van filmpjes, malafide en illegale verkoopwebsites, IP-adressen met gehackte gegevens, Telegram groepen waarin extremistische content werd verspreid en Telegram groepen waarin vervalste geschriften en illegaal vuurwerk werden verkocht. Wat opvalt aan deze gevallen is dat in drie zaken de rechter-commissaris toestemming heeft gegeven voor een toepassing naar analogie van artikel 125p Sv, namelijk een artt. 181 jo 125p Sv-combinatie. In deze zaken heeft de rechter-commissaris geen aanbieder gehoord, een verplichting opgenomen in het wetsartikel, omdat de veronderstelling van de officier van justitie en de rechter-commissaris was dat deze niet zou meewerken. In plaats daarvan heeft de politie de opdracht gekregen om gegevens ontoegankelijk te maken.

Zoals gezegd voldoet artikel 125p Sv niet altijd voor de opsporingspraktijk. Een belangrijke reden hiervoor is gelegen in lid vier van artikel 125p Sv: een schriftelijke machtiging van de rechter-commissaris waarbij de aanbieder voorafgaand aan de afgifte daarvan gehoord moet worden. De toets door de rechter-commissaris is

geïntroduceerd, omdat artikel 125p Sv een ingrijpende bevoegdheid betreft. Daarnaast moest de toets ervoor zorgen dat gegevens toch relatief snel ontoegankelijk konden worden gemaakt. Deze snelle ontoegankelijkmaking staat in lid 2. In de opsporingspraktijk botsen de toets door de rechter-commissaris en een snelle ontoegankelijkmaking met elkaar. Zowel het proces van afgifte van een schriftelijke machtiging als het horen van de aanbieder nemen (veel) tijd in beslag. Bovendien brengt het horen van een aanbieder nog andere moeilijkheden met zich mee. Snelle ontoegankelijkmaking is dus niet altijd mogelijk, een belangrijke nuancering bij de veronderstelling van de wetgever.

Tegelijkertijd is de toets door de rechter-commissaris er niet voor niets. Artikel 125p Sv is een ingrijpende bevoegdheid, omdat de vrijheid van meningsuiting in het geding kan zijn. In veel zaken waarin artikel 125p Sv gebruikt wordt zou het echter doorgaans gaan om onmiskenbaar illegale content, waar geen discussie bestaat over de strafbaarheid ervan, zoals dat bij zogenoemde uitingsdelicten wel het geval kan zijn. Dat neemt niet weg dat er verzoeken kunnen komen die wel degelijk de vrijheid van meningsuiting raken. Een zorgvuldige toetsingsprocedure, een belangrijk onderdeel van de rechtsstaat, blijft om die reden aangewezen. Wel kan gekeken worden of hetgeen nu alleen nog in de memorie van toelichting staat beschreven met betrekking tot het achterwege laten van het horen van de aanbieder ook in de wetstekst zelf opgenomen kan worden.

8.6 Hackbevoegdheid (artt. 126nba, 126uba en 126zpa Sv)

De wetgever heeft de hackbevoegdheid geïntroduceerd om computercriminaliteit en andere vormen van ernstige criminaliteit beter aan te kunnen pakken. Dat was een belangrijke veronderstelling achter de hackbevoegdheid. Vanwege technologische ontwikkelingen zouden reeds bestaande bevoegdheden te weinig opleveren. Bovendien, zo veronderstelde de wetgever, zouden bestaande bevoegdheden praktisch en proportioneel gezien niet altijd de meest aangewezen bevoegdheden zijn. Beide veronderstellingen, weliswaar met een aantal belangrijke nuanceringen, zijn juist gebleken.

In de periode april 2021-april 2024 is in 89 opsporingsonderzoeken een eerste bevel afgegeven om de hackbevoegdheid in te zetten. In de grote meerderheid van zaken ging het om een inzet op een telefoon, in het totaal 105 telefoons. Bijna alle opsporingsonderzoeken richtten zich, in tegenstelling tot wat de naam van de Wet CCIII wellicht doet vermoeden, op één of meer vormen van traditionele criminaliteit. Een overtreding van de Opiumwet, (poging tot) moord/doodslag en witwassen kwamen het vaakst voor. Bij het overgrote deel van de inzetten werd verder gebruikgemaakt van een commercieel middel, zowel om binnen te dringen als om gegevens te verzamelen. Deze bevindingen liggen in lijn met de eerdere WODC-rapportage (Van Uden & Van den Eeden, 2022).

Er waren verschillende redenen om de bevoegdheid in te zetten, allemaal redenen die aansloten bij wat de wetgever had voorzien. Twee sprongen eruit, namelijk de versleuteling van gegevensdragers en de vrees dat de verdachte op de hoogte zou raken van het opsporingsonderzoek. In dit onderzoek is ook duidelijk geworden dat er zaken zijn waarin de keuze wordt gemaakt om de hackbevoegdheid niet te benutten. Een deel hiervan betreft zaken waarvoor de hackbevoegdheid nog (steeds) geen oplossing kan bieden, bijvoorbeeld wanneer een zaak een buitenlandcomponent kent

of wanneer een inzet te veel tijd in beslag neemt. Dit is een belangrijke nuancering bij de veronderstelling van de wetgever.

Bij een ruime meerderheid van de inzetten is het gelukt om het geautomatiseerd werk binnen te dringen en gegevens te verzamelen. De verzamelde gegevens betroffen vooral een vorm van communicatie die verloopt via communicatie apps. In een derde van de opsporingsonderzoeken zijn deze gegevens als sturingsinformatie gebruikt en in een derde van de opsporingsonderzoeken als bewijs. Tussen deze categorieën zit overlap, omdat in negen onderzoeken de verzamelde gegevens én als sturingsinformatie én als bewijs hebben gediend. In 40% van de onderzoeken leidt de inzet van de hackbevoegdheid niet tot een bruikbare opbrengst voor het opsporingsonderzoek. De wijze waarop de hackbevoegdheid een bijdrage levert aan de aanpak van computercriminaliteit en andere vormen van ernstige criminaliteit kan dus verschillen, wederom een belangrijke nuancering bij de veronderstelling van de wetgever.

In iets minder dan een derde van de zaken heeft een zittingsrechter zich inhoudelijk gebogen over de zaak waarin de hackbevoegdheid is ingezet. In ruim een derde van de zaken zal een zittingsrechter dat nog gaan doen. Opvallend is dat de bevoegdheid in slechts een klein aantal zaken inhoudelijk op zitting besproken is. Deze bevinding is van belang met het oog op het feit dat in de toekomst het uitgangspunt zal zijn dat gewerkt mag worden met technische hulpmiddelen die niet volledig goedgekeurd zijn. Bij de introductie van de Wet CCIII was het uitgangspunt juist dat in principe gewerkt moest worden met een technisch hulpmiddel dat vooraf goedgekeurd was. De politie zet een technisch hulpmiddel in om gegevens te verzamelen en dat technisch hulpmiddel dient gekeurd te worden om een inschatting te kunnen maken over de betrouwbaarheid, herleidbaarheid en integriteit van de gegevens die met dat betreffende technisch hulpmiddel verzameld worden. Het is vervolgens aan de zittingsrechter om een oordeel te vellen over de kwaliteit van de verzamelde gegevens. Het nieuwe uitgangspunt, dat overigens op dit moment nog niet is doorgevoerd, betekent dat alle technische hulpmiddelen die ingezet zullen worden, gekeurd zijn. Voorheen was dat niet het geval, omdat een officier van justitie in veel gevallen besloten had dat een technisch hulpmiddel naar zijn aard niet te keuren was. Dat alles gekeurd zal gaan worden is daarom een goede ontwikkeling, omdat inzichtelijk zal zijn waar eventueel nog risico’s zitten ten aanzien van de betrouwbaarheid van de gegevens die verzameld worden met het ingezette technische hulpmiddel. Een belangrijk aandachtspunt hierbij is dat deze evaluatie zoals gezegd heeft laten zien dat de inzet van de hackbevoegdheid nauwelijks besproken is tijdens de behandeling van de zaak door een zittingsrechter. Dat betekent dat een zittingsrechter zich over dit specifieke onderwerp niet structureel buigt en dat de inzet van de bevoegdheid slechts beperkt getoetst wordt. Gezien de ingrijpendheid van de bevoegdheid is dat een belangrijke beperking.

Tot slot nog twee belangrijke aandachtspunten, één met betrekking tot de keuring en één met betrekking tot de inzet van commerciële middelen. De toenmalig Minister van Justitie en Veiligheid heeft in december 2023 aangekondigd dat de wijze waarop met technische hulpmiddelen zal worden omgegaan, gewijzigd zal worden. In haar brief kondigde zij aan dat alle betrokken partijen hierover met elkaar in overleg zouden gaan. Dat lag in lijn met een belangrijk aandachtspunt dat in de eerdere WODC-evaluatie (Van Uden & Van den Eeden, 2022) beschreven werd. Daarin werd geconstateerd dat dit gesprek belangrijk was, omdat het een gedeeld belang is van alle betrokkenen om betrouwbare gegevens te verzamelen. Deze evaluatie heeft laten

zien dat dit gesprek tot nu toe zeer moeizaam op gang gekomen is. Het moeizaam op gang gekomen overleg voorzetten blijft om die reden een aandachtspunt.

Het tweede aandachtspunt ziet op het gebruik van commerciële middelen. Bij het overgrote deel van de inzetten werd gebruikgemaakt van een commercieel middel, zowel om binnen te dringen als om gegevens te verzamelen. Dit past bij de verwachting die de toenmalig Minister van Justitie en Veiligheid in haar beleidsbrief uitspreekt dat commerciële producten 'relatief vaak' zullen worden ingezet. Wel roept dit de vraag op of het gebruik van commerciële middelen, net zoals in de wetsgeschiedenis, meer specifiek het Besluit (Besluit onderzoek geautomatiseerd werk, p. 15) beschreven staat, een uiterst middel moet worden genoemd. De term uiterst middel wekt de suggestie dat het gebruik ervan een uitzondering is. Deze evaluatie heeft wederom laten zien dat het gebruik ervan eerder de regel is.

8.7 Slotbeschouwing

Met de komst van de Wet CCIII is het juridisch instrumentarium versterkt voor de opsporing en vervolging van computercriminaliteit. Dit was ook wat de wetgever beoogde met de introductie van de nieuwe wet. Bij computercriminaliteit gaat het om computercriminaliteit in zeer brede zin, zo blijkt uit deze evaluatie. Dat betekent dat deels sprake is van meer traditionele vormen van criminaliteit waarbij ICT slechts een middel is om een strafbaar feit te plegen.

De versterking van het juridisch instrumentarium heeft vorm gekregen middels vijf nieuwe of aangepaste strafbaarstellingen in het Wetboek van Strafrecht en twee nieuwe bevoegdheden in het Wetboek van Strafvordering. Het grootste deel van de nieuwe strafbaarstellingen heeft ervoor gezorgd dat verdachten vervolgd kunnen worden voor feiten waarbij dat vóór de introductie van de wet minder goed mogelijk was, denk aan het helen en stelen van gegevens en online handelsfraude. Voor de aangepaste strafbaarstellingen artikelen 248a en 248e Sr is dat slechts sporadisch gebeurd. In dat opzicht is er wel een juridisch instrument bijgekomen, maar wordt dit in de opsporingspraktijk nauwelijks benut.

Net als een groot deel van de strafbaarstellingen worden de twee nieuwe opsporingsbevoegdheden, de ontoegankelijkmaking van gegevens en de hackbevoegdheid, in de praktijk gebruikt. Beide bevoegdheden hebben ervoor gezorgd dat opsporingshandelingen kunnen worden verricht die voorheen niet (hackbevoegdheid) of in mindere mate (ontoegankelijkmaking) mogelijk waren. Deze handelingen leveren, al dan niet indirect, een bijdrage aan de aanpak van computercriminaliteit en andere ernstige vormen van criminaliteit. Er doen zich echter ook situaties voor waarin deze twee nieuwe bevoegdheden niet de gewenste bijdrage kunnen leveren binnen een opsporingsonderzoek, vooral bij de ontoegankelijkmaking van gegevens.

In de rest van deze paragraaf richt de aandacht zich op een aantal aspecten die raken aan meerdere wettelijke bepalingen uit de Wet CCIII.

8.7.1 Nieuwe ontwikkelingen

Voor veel wettelijke bepalingen in de Wet CCIII waren nieuwe ontwikkelingen op ICT-gebied één van de redenen om de nieuwe/vernieuwde bepalingen te introduceren.

Ruim tien jaar geleden al werden deze ontwikkelingen gepresenteerd als belangrijke aanleiding voor de Wet CCIII. In deze evaluatie is duidelijk geworden dat in de periode nadat de wet inwerking is getreden zich ontwikkelingen op dit terrein voor zijn blijven doen. Dat hoeft overigens geen verbazing te wekken, omdat juist technologische ontwikkelingen doorgaans snel gaan. Naast technologische ontwikkelingen hebben zich ook ontwikkelingen voorgedaan op andere terreinen, zoals inmiddels ontstane jurisprudentie waarin het gebruik van de verschillende bepalingen getoetst is door een rechter. Deze ontwikkelingen, die verschillend zijn van aard, hebben invloed op de wijze waarop de nieuwe bepalingen op dit moment en mogelijk in de toekomst van nut kunnen zijn.

De eerste ontwikkeling is dat een deel van de noodzaak voor artikel 138c Sr (het stelen van gegevens) is verdwenen. Eén van de redenen voor de introductie van deze bepaling was dat personen die in een werksituatie gegevens overnamen daarvoor niet altijd strafrechtelijk konden worden vervolgd. Het artikel computervredebreuk (art. 138ab Sr) voldeed niet, omdat sprake moest zijn van wederrechtelijk binnendringen, hetgeen in een werksituatie niet het geval hoeft te zijn. Werknemers beschikken immers over inloggegevens. Inmiddels heeft jurisprudentie van de Hoge Raad laten zien dat in dat soort situaties toch ook sprake kan zijn van computervredebreuk in de zin van artikel 138ab Sr. In dat opzicht heeft artikel 138c Sr in dat soort zaken haar nut verloren, al bestaat ook kritiek op de interpretatie van de Hoge Raad waardoor deze wijze van toepassing mogelijk is geworden.

De tweede ontwikkeling betreft een ontwikkeling op technologiegebied, namelijk de hoeveelheid gegevens die gestolen kan worden en de impact die dat kan hebben. Deze ontwikkeling heeft impact op artikel 138c Sr, maar vooral op artikel 139g Sr. In een onlangs verschenen rapport van Europol (2025) wordt duidelijk dat illegale handel in gegevens toeneemt en dat datadiefstal een ‘significant gevaar’ vormt voor de samenleving. Grote hoeveelheden data worden gestolen en personen met criminele intenties misbruiken die. Het is de vraag of de wetgever destijds, meer dan 10 jaar geleden, de hoeveelheid gegevens die gestolen kan worden duidelijk op het netvlies had. Hetzelfde geldt voor de mogelijke impact daarvan. Hoewel de hoeveelheid gegevens dat gestolen, maar vooral geheeld is, varieert, is ook duidelijk geworden dat verdachten grote hoeveelheden persoonsgegevens in hun bezit kunnen hebben. De vraag is of vooral het strafmaximum voor het helen van gegevens (één jaar) hier voldoende in lijn mee is. Weliswaar is na inwerkingtreding van de Wet CCIII artikel 234 Sr geïntroduceerd dat een hoger strafmaximum kent en ook gebruikt kan worden wanneer sprake is van geheelde gegevens. Dit artikel volstaat echter niet in alle gevallen. Om die reden zou het goed zijn dat de wetgever de strafmaat van artikel 139g Sr heroverweegt. Dat is meteen een mooie gelegenheid om het artikel in lijn te brengen met de strafbaarstelling die ziet op het helen van goederen.

De derde ontwikkeling, vooral gerelateerd aan de hackbevoegdheid, is de versleuteling van gegevens(dragers). Technieken hiervoor ontwikkelen zich voortdurend en het wordt voor opsporingsinstanties steeds ingewikkelder om die versleuteling te doorbreken. Op Europees niveau wordt volop gediscussieerd hoe met deze versleuteling om te gaan. Eén van de mogelijke opties is dat voor opsporingsinstanties de mogelijkheid moet worden gecreëerd dat gemakkelijk ontsleuteling kan plaatsvinden. Het inbouwen van een zogenoemd ‘achterdeurtje’. Aanbieders van versleutelde communicatiediensten zijn hier fel op tegen, omdat altijd de mogelijkheid bestaat dat zo’n achterdeurtje misbruikt wordt. Op basis van deze evaluatie nemen wij geen standpunt in wat de meeste gewenste oplossing is. Wel is het van belang om na

te denken hoe met deze ontwikkeling om te gaan, en om daarbij zowel rekening te houden met én de bescherming van grondrechten zoals de persoonlijke levenssfeer van burgers én met de effectiviteit van de opsporing.

8.7.2 Beschikbare capaciteit

De beschikbare opsporingscapaciteit is een belangrijk aandachtspunt bij de toepassing van een aantal wettelijke bepalingen uit de Wet CCIII. Vooral bij de lokpuber, online handelsfraude en de hackbevoegdheid werd dit onderwerp als reden genoemd voor het mogelijk beperktere gebruik van de betreffende bepaling. De oplossing hiervoor is niet eenvoudig, omdat het niet realistisch is om te veronderstellen dat er op korte termijn een toename van beschikbare capaciteit zal zijn, zie onder andere de Veiligheidsagenda 2023-2026. Ook zijn capaciteitsvraagstukken geen nieuw fenomeen en zullen er altijd keuzes moeten worden gemaakt. Bovendien kan de vraag worden gesteld of strafrecht altijd de oplossing is. Daarom zou, wanneer het gaat om de brede aanpak van computercriminaliteit, gekeken kunnen worden naar een 'integrale en systemische aanpak', zoals genoemd door het Openbaar Ministerie (2004) en ook beschreven in Veiligheidsagenda 2023-206 (p. 12-13). In zo'n aanpak draait het, blijkens het cybercrimebeeld, niet alleen om het verstoren en vervolgen van cybercriminelen, maar ook om het 'verstoren van activiteiten, informeren van slachtoffers en preventie' (Openbaar Ministerie, 2024, p. 2). Ook private partijen kunnen hierbij betrokken zijn. Een belangrijke kanttekening hierbij is dat dit soort initiatieven nog beperkt geëvalueerd zijn. Het zou goed zijn wanneer dat in de toekomst meer gebeurt.

Wat betreft online handelsfraude in het bijzonder, is het raadzaam om te kijken welke mogelijkheden er zijn om het artikel daadwerkelijk te gebruiken voor die vormen van online handelsfraude waarvoor de wetgever het wetsartikel oorspronkelijk bedoeld had. Dat betekent dat eerst gekeken zou moeten worden of die vormen van online handelsfraude daadwerkelijk plaatsvinden. Indien dat het geval is, zou verkend kunnen worden hoe gerealiseerd zou kunnen worden dat de opsporingscapaciteit vooral daarop gericht wordt. Alternatieve interventies, ook andere interventies dan het strafrecht, zouden dan (meer) ingezet kunnen worden bij zaken waarin geen sprake is van grootschaligheid. De wetgever hintte hier ook al op in de memorie van toelichting van de wet. Daarbij kan bijvoorbeeld gekeken worden naar het weerbaarder maken van burgers en de samenwerking met bijvoorbeeld online handelsplatforms. Dit past goed in de zojuist genoemde 'brede aanpak'.

8.7.3 Zaken met een internationale component

Dat de geïntroduceerde strafbaarstellingen en bevoegdheden ook betrekking kunnen hebben op zaken die zich (deels) in het buitenland afspelen zorgt ervoor dat deze wettelijke bepalingen in de opsporingspraktijk niet optimaal benut kunnen worden. Het is bijvoorbeeld lastig om online handelsfraudeurs, die zich in het buitenland bevinden, op het spoor te komen en te vervolgen. Ook bij de hackbevoegdheid en de ontoegankelijkmaking van gegevens kan het feit dat verdachten zich deels in het buitenland bevinden ervoor zorgen dat de bevoegdheden niet ingezet kunnen worden. Een belangrijke reden hiervoor is dat Nederland geen jurisdictie[116] heeft in deze landen. Dat zorgt ervoor dat Nederland een rechtshulpverzoek zal moeten doen wanneer een zaak op een of andere manier de landsgrens overschrijdt. Dit neemt vaak

[116] Jurisdictie, ook wel rechtsmacht, heeft betrekking op 'het terrein waarover staten en hun organen bevoegd zijn regels te stellen en/of te handhaven' (Centrum voor internationaal recht, z.d.).

(veel) tijd in beslag. Bovendien is de rechtshulprelatie met sommige buitenlanden niet goed. Ook het horen van een aanbieder die zich in het buitenland bevindt, kan ingewikkeld zijn in het kader van het ontoegankelijk maken van gegevens. Vanwege de moeilijkheden rondom zaken met een internationale component, zou het goed zijn de aandacht te richten op meer internationale samenwerking. Bijvoorbeeld gezamenlijke Europese en internationale initiatieven over hoe kan worden omgegaan met het verantwoordelijk maken van aanbieders die strafbare content faciliteren. Wat betreft online handelsfraude zou gekeken kunnen worden in hoeverre het mogelijk is om een koppeling te realiseren tussen de verwijzingsportalen van elk Europees land afzonderlijk waardoor het gemakkelijker is om de mogelijke identiteit van een buitenlandse rekeninghouder te achterhalen.

8.7.4 (Rechtsstatelijke) waarborgen

De twee nieuwe bevoegdheden, de ontoegankelijkmaking van gegevens (art. 125p Sv) en de hackbevoegdheid (artt. 126nba, 126zpa en 126uba Sv), zijn beide ingrijpende bevoegdheden, omdat zij inbreuk (kunnen) maken op belangrijke grondrechten zoals de bescherming van de persoonlijke levenssfeer en de vrijheid van meningsuiting. Vanwege die ingrijpendheid zijn (rechtsstatelijke) waarborgen ingebouwd zodat deze bevoegdheden niet zomaar worden ingezet. Wanneer opsporingsteams gegevens ontoegankelijk willen maken op basis van artikel 125p Sv, dient de rechter-commissaris schriftelijk toestemming te geven nadat hij de aanbieder in de gelegenheid heeft gesteld om te worden gehoord. Voor de hackbevoegdheid geldt, naast een toets door de rechter-commissaris, dat technische hulpmiddelen die worden ingezet in principe nog vooraf (goed)gekeurd moeten worden. Hoewel in de praktijk doorgaans begrip bestaat voor de hier beschreven toetsingswaarborgen, brengen zij voor de opsporingspraktijk ook nadelen met zich mee, vooral omdat de toetsingstrajecten veel tijd in beslag nemen. In de praktijk is een spanningsveld zichtbaar tussen enerzijds de efficiency en effectiviteit van een inzet en anderzijds de rechtsstatelijkheid.

Vanwege de ingrijpendheid van de bevoegdheden is het van belang dat stevige toetsingsvoorwaarden blijven bestaan, zeker gezien het feit dat een zittingsrechter zich lang niet altijd buigt over zaken waarin deze bevoegdheden zijn ingezet. Tegelijkertijd zou de wetgever kunnen kijken of bepaalde voorwaarden anders ingevuld kunnen worden, bijvoorbeeld door bij artikel 125p Sv de mogelijkheid te verkennen van een mondelinge machtiging in geval van spoed, die later schriftelijk bevestigd moet worden. Of te verkennen of in de wet geëxpliciteerd kan worden dat onder bepaalde voorwaarden afgezien kan worden van het horen van de aanbieder.

Met betrekking tot de hackbevoegdheid heeft de toenmalig Minister van Justitie en Veiligheid al de keuze gemaakt de waarborg ten aanzien van de keuring van technische hulpmiddelen te wijzigen. Het is de bedoeling dat alle technische hulpmiddelen gekeurd worden én dat gebruik mag worden gemaakt van technische hulpmiddelen die niet (volledig) goedgekeurd zijn. Dit betekent dat meer gewerkt zal gaan worden op basis van risicoanalyses. Uiteindelijk is het aan een zittingsrechter om te beoordelen wat de waarde van de verzamelde gegevens is. Het is een goede ontwikkeling dat in principe geen gebruik meer gemaakt zal worden van technische hulpmiddelen die niet gekeurd zijn. Wel blijft een belangrijk punt van aandacht dat de door de wetgever veronderstelde toetsing door een zittingsrechter tot nu toe zeer sporadisch heeft plaatsgevonden. Dit betekent dat de inzet van de hackbevoegdheid

beperkt getoetst wordt en dat geen recht wordt gedaan aan een belangrijke veronderstelde rechtsstatelijke waarborg.

Summary

Evaluation of Computer Crime Act III

An empirical study of the Act's application in practice

The Computer Crime Act III (Act CCIII) came into force on 1 March 2019. This Act introduced six new/adapted legal regulations: five criminal offences and two (special) investigative powers. The five new/adapted offences concern the stealing of data (Section 138c Sr), fencing of data (Section 139g Sr), online trade fraud (Section 326e Sr), seduction of a minor (Section 248a Sr), and grooming (Section 248e Sr). The two new investigative powers concern the power to make data inaccessible (Section 125p Sv) and the power to hack (Sections 126nba, 126uba en 126zpa Sv). The Act, and the successor to the Computer Crime Act I and II, was seen as necessary to strengthen the legal toolkit for investigation and prosecution of computer crime (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 2). Previously, another evaluation on this Act was published, evaluating how one of the new regulations, namely the power to hack (i.e. Section 126nba Sv), has been applied in practice (Van Uden & Van den Eeden, 2022). The present evaluation concerns the entire Act CCIII. The main research question was:

To what extent are the objectives formulated in the Act CCIII being met in practice?

Three sub questions were formulated to answer the main research question.

1 What is the main objective of the various regulations of the Act CCIII and what presumptions underpin these regulations?
2 How are the various regulations of the Act CCIII implemented in practice?

What are the (intentional and unintentional) consequences of the regulations of the Act CCIII for investigative practice?

To answer the main research question, a combination of research methods was used: document analysis, numerical analysis of legal data (RAC-min), interviews, court case analysis, and a survey. This summary describes the evaluation's main findings and conclusions. For each legal regulation, we examined the legislator's presumptions about its necessity and functioning. This also includes the legislator's objectives at the time of the legal regulation's enactment. Furthermore, attention is focused on the implementation in practice and the intended as well as unintended consequences for, among other things, investigative practice. Besides that, per regulation, various possibilities and points of attention for the investigative practice are discussed. Furthermore, as each of these regulations touches upon various themes that are not always tightly connected, each new/amended regulation is discussed separately.

Before we continue, the following is of importance. This project used a combination of research methods to increase the validity of the research, among other reasons. For the court case analysis, all available court cases were studied. This way we were able to attain as complete a picture as possible with regard to the application of, especially,

the criminal offences. Moreover, we had access to court verdicts that are not published, which adds important value to this evaluation.

For a few regulations, only a relatively small amount of people were interviewed in comparison to the total amount of cases that were analysed. This was done partly on purpose, because we used a variety of other research methods. While, on the other hand, we were simply not able to secure more people to interview. For instance, because we did not receive any response to an interview request. At the same time, the persons we did interview were often specialised in themes concerning the regulations – such as the power to hack and the fencing and stealing of data. Despite the limited amount of interviews, the results have offered reliable and relevant insights.

Stealing of Data (Section 138c Sr)

Section 138c of the Dutch Penal Code (Sr) criminalises the unlawful copy data. An important presumption of legislation was that Section 138c Sr would improve the protection of data and would better protect data against abuse. This evaluation makes clear that suspects have been prosecuted for the unlawful copy of data. In that respect has the now existing risk of prosecution for suspects improved the protection of data in practice. Whether this new criminal offence also carries a deterrent effect in and of itself, can nonetheless not be determined on the basis of this evaluation.

From March 2019 until April 2024, 39 cases were submitted to the Public Prosecutor's Office en in 15 cases a judge reached a verdict. Two cases were settled with an penal order by the Public Prosecutor's Office and in 13 cases the suspect was convicted of the 138c-offence. Almost all cases involved employees who copied data within the workplace. In most cases, the unlawful copying of data was not the only offence charged in a case. This offence was for example charged together with other criminal offences in the (relational) spheres of life. All cases concerned broadly defined computer crime, meaning traditional crime committed with an IT-resource. Mostly, private data (personal data, photos and images) were stolen. The amount of data that was stolen was not always disclosed. Generally, it did not concern huge amounts of data. Except for one case involving hundreds of unlawfully copied foreign phone numbers.

Section 138c Sr offers citizens and, in particular, investigative practice a few benefits. First of all, it allows victims of stolen data to be added to the criminal case proceedings and enables more extensive investigation. Another added benefit of this law, as shown by the evaluation, is the addition of a legal description fitting to a situation in which an individual with lawful access to data copies such data unlawfully. Additionally, it should be noted that the judiciary has since further developed. Legislative history demonstrates that Section 138ab Sr (computer intrusion) has not been sufficient in prosecuting unlawful copying of data in the workplace. Meanwhile, the Dutch court of appeal has determined in several verdicts that copying data within the workplace can also be qualified as computer intrusion, as a result of which Section 138c Sr is not always chosen. For those situations, an important reason for why Section 138c Sr was enacted is thus no longer present. Simultaneously, this has raised the question whether this is stretching the concept of computer intrusion too far (see Berndsen & Visser, 2022, p. 163).

Furthermore, this evaluation highlights several points of interest. Firstly, the penalty range for this offence is not always regarded as fitting, depending on the amount of copied data. In addition, it is not always easy to prove the component 'unlawful'. Lastly, this evaluation demonstrates that the regulation specifically concerns data copied from computerized systems, excluding data copied from paper.

Fencing of Data (art. 139g Sr)

On the basis of Section 139g Sr, data fencing has become punishable by law. An important presumption of legislation was that the enactment of Section 139g Sr would better protect data against abuse under criminal law. This evaluation makes clear that suspects have been prosecuted for the fencing of data. From that perspective, data is better protected in practice, as suspects now run the risk of being prosecuted for this offence. To what extent such prosecution has a deterrent effect cannot be said on the basis of this evaluation.

Between March 2019-April 2024, 93 cases were submitted to the Public Prosecutor's Office. In 85 cases Section 139g Sr was the only charged CCIII-regulation and in 8 cases a combination of CCIII-regulations was charged, namely Section 139g Sr combined with Section 138c Sr or Section 326e Sr. A verdict was available in 42 cases. In a large majority of cases (36) de suspect was convicted for a 139g-offence en imposed with a sentence by a judge. Most cases in which Section 139g Sr was charged concerned, next to the fencing of (predominantly) offline and online personal data, multiple offences. In a large majority of cases the Section in question was charged alongside other criminal offences causing victims financial harm. In some cases, data fencing was directly related to other charged offences. Meaning, (a part of the) fenced data was used to commit other offences charged in the same case, for instance fenced data that were used for committing fraud. The amount of data fenced in the analysed cases differed greatly, while the precise amount of fenced data was not always made clear in the verdict. However, when a 139g-case concerns datasets of personal data it more often concerns large amounts of data. When other types of data are concerned, such as photo material, the amount of fenced data is usually smaller. This obviously does not take the possible impact of this crime on victims into account.

Section 139g Sr offers investigative practice several pros. Firstly, the description given in Section 139g Sr is considered as fitting for how this type of fencing occurs in practice. Moreover, this Section enables confiscation of laundered amounts. Section 139g Sr is also deemed useful in tackling the entire chain of bank fraud, since fenced data is being used to commit it. On top of that, the new Section can effectuate suspicion in cases whereas this was impossible before enactment. This also means that in such cases there are now grounds to start an investigation, while prosecution was unable to do so before.

Furthermore, the present evaluation sheds light on a few points of attention. Two important ones will be highlighted in this paragraph. The first concerns the one-year penalty. The chosen length of this penalty seems illogical from a legal and systematic perspective, as fencing of goods knows a higher penalty. Besides, practice shows that the amount of stolen data can vary greatly, which raises the question whether this variety is befitting the maximum penalty.

The second point of attention concerns whether a suspect can be convicted for data fencing in case the data is retrieved through their own crime (by analogy of the fencer-stealer-rule). Jurisprudence has not been unanimous and shows different judgements on the issue. It is possible that further future proceedings will determine whether or not the fencer-stealer-rule is also applicable when it comes to data fencing.

Online Trade Fraud (art. 326e Sr)

On the basis of Section 326e Sr online trade fraude has become punishable by law. An important presumption of legislation was that the enactment of Section 326e Sr would allow for the criminal prosecution of online trade fraud, especially large scale forms of online trade fraud. Although the Public Prosecutor's Office decided not to prosecute in a large amount of cases, mainly due to capacity considerations, suspects were prosecuted and convicted on the basis of Section 326e Sr. However, in these cases made was hardly any mention of so-called large-scale online trade fraud.

Between March 2019 and April 2024, 279 cases were submitted to the Public Prosecutor's Office. A judge reached a verdict in 91 cases, a large majority of which involved the prosecution of at least one count of online trade fraud. Our court case analysis demonstrates that in the large majority of analysed cases, online trade fraud is charged together with other criminal offences. Regular fraud occurred most often, followed by money laundering. Almost all of these cases concerned the laundering of money earned with online trade fraud.

The analysed cases mainly concerned the fraudulent sale of goods. Besides, some cases concerned the fraudulent offering of services. On average, the amount of damage stated in the judicial finding of facts was around 2,000 euro per case. The average amount of victims per case in the judicial finding of facts was 15 individuals. Damages were claimed in nearly all of the analysed cases. That victims were able to add themselves to criminal cases was also a presumption of legislation. An important nuance in this regard is that the court case analysis mainly concerned online fraud committed through existing online trade websites, not through temporary websites that were then quickly taken offline. In case of temporary websites, it is generally difficult to claim damages.

The foregoing shows that Section 326e Sr has indeed been used to (successfully) prosecute online trade fraud. Moreover, Section 326e Sr is a so-called *lex specialis*[117], meaning this law is specifically focused on fraud within online trade, which has simplified the qualification of the offence. In line with legislation's objective to better facilitate the prosecution of online trade fraud, this new Section is clearer, easier to apply and easier to prove, in comparison to the general law prohibiting fraud. This may simplify the prosecution of online trade fraud.

As previously mentioned, this new Section has barely been used to tackle and prosecute 'large-scale online trade fraud'. The court case analysis is largely void of such large-scale cases. In only 3 of the 27 analysed cases was spoken of 'large-scale online trade fraud'. The present evaluation leaves unclear as to why such cases emerged only sporadically in our research. One possible explanation could be that it may be difficult to find the "real" perpetrator in large-scale cases of online trade fraud.

[117] *Lex specialis* is a Latin term for a specialised law, referring to a legal principle that puts a specialised law (a *lex specialis*) before a more general one. In this case, general law being Section 326 Sr (simple fraud).

Perhaps, because this could require extra investigate capacity, which, as stated before, is not always available. It is also possible that no verdicts have been made (yet), since investigation into large-scale cases is more time consuming and therefore still ongoing. Another possibility is that such cases of online trade-fraud do not exist, or are committed from and/or in other countries.

Additionally, the evaluation sheds light on a contradiction in Section 326e Sr. On the one hand, this Section is simpler in comparison to the general law prohibiting fraud, which has simplified prosecution of online trade fraud. On the other hand, available investigative capacity is too limited to prosecute all suspects based on this simpler Section. In a large amount of cases a decision was taken by the Public Prosecutor's Office not to prosecute, and, after the initiation of a Section 12-procedure, a judge sided with this decision in a large majority of cases. Most importantly, because of a limited capacity to investigate. There are also ways outside criminal law in which are tackling online trade fraud. For instance, a so-called stop conversation, asking as well as urging suspects to stop their criminal behaviour.

Besides the available investigative capacity and the lack of large-scale cases of online trade fraud, there is one other point of interest in regards to the prosecution of Section 326e Sr, namely the foreign component. Such a component in an online trade fraud case, for example a foreign supplier or receiver bank account, complicates prosecution. It can especially be difficult to uncover the identity of a suspect. This too, forms an important nuance to the presumption of legislation. Linking the national referral portals – a portal that links all banks nationally – of all European countries could be a possible solution to this.

Teen Decoy (arts. 248a and 248 Sr)

The modification of Sections 248a Sr (seduction of a minor) and 248e Sr (grooming of a minor) has made it possible for police to deploy a teen decoy. An important presumption of legislation was that minors would be better protected by way of adapting Sections 248a Sr (seduction of a minor) and 248e Sr (grooming of a minor) to allow for the deployment of a teen decoy. This evaluation demonstrates that it is possible to prosecute a suspect in case involving a teen decoy. Although, such cases, in which a teen decoy was deployed, were very rare. Whether children can indeed be better protected cannot be determined on the basis of this evaluation. What is clear, however, is that teen decoys are hardly used by police for this purpose.

From what is known, only one case involving the seduction of a minor and deployment of a teen decoy by police was tried within the period March 2019 until April 2024. This number is rather small in proportion to the total number of 248a- and 248e- cases in which a judge reached a verdict (respectively 92 and 58 cases) and prosecuted suspects for either seduction of a minor or grooming. The police has made additional use of a teen decoy. Although, these cases either concerned other offences than Sections 248a and 248e Sr or it was not made clear which offences were concerned. This does demonstrate that a teen decoy can also be used for other offences. Finally, the National Police Force ran a pilot to assess how a teen decoy could be deployed and its possibilities. As far as is known, this pilot had not led to any concrete cases.

Teen decoys are thus not often deployed in practice. Important reasons for this were the available level of capacity and the fact that there already are many 'bring cases', in

which other investigative routes are taken. 'Bring cases' are cases in which a police report has been filed and a suspect has potentially been identified. Although teen decoys have not been deployed a lot, several possibilities regarding its deployment came forth during the interviews. One of which was deploying teen decoys proactively. In contrast to a 'bring case', a proactive deployment of a teen decoy does not require the presence of a concrete suspect. An important condition for such deployment is sufficient available capacity, at least for the actual deployment of the teen decoy.

Since the enactment of the Act Sexual Offences (in Dutch Wsm) on July 1st of 2024, Sections 248a and 248e Sr no longer exist and are instead partly included in the Wsm. Deployment of a teen decoy is still possible under this new act, especially for the sexual corruption of minors and for sex chatting. As such, the points of interests highlighted in this evaluation concerning teen decoys, for instance the boundaries around provocation, the limited availability in terms of capacity, the creation of credible online profiles, and the level of awareness around teen decoys within investigative authorities, can still be valuable for its application within the parameters of this new act. It remains questionable, however, to what extent teen decoys will be used within this new act. 2024 saw an increase in reports of sexual offences compared to 2023, and 131 reports of sex chatting were done (Police, 2025). This shows that there are plenty of 'bring cases'. In this regard, it has become clear in this evaluation that in those instances other investigative paths are often chosen. As such, future deployment of teen decoys is rather unlikely. This is not necessarily problematic as long as investigative officers are aware that deployment of teen decoys is a possibility and enough manpower is made available when such deployment is deemed necessary.

Making data inaccessible (art. 125 Sv)

The newly enacted Section 125p Sv enables law enforcement to make data inaccessible. An important presumption of legislation was that with the introduction of Section 125p Sv, the power to make data inaccessible via service providers, criminal offences could be terminated quicker or even be prevented. This, in turn, would be able to better protect society. This evaluation demonstrates that data were made inaccessible with Section 125p Sv. In that respect, it has been proven possible to make criminal content (temporarily) inaccessible, which is in line with legislation's presumption. To what extent society is better protected as a result cannot be determined on the basis of the present evaluation. It has also been shown in this evaluation that service providers are often times more than willing to make data inaccessible voluntarily. We were unable to gain insight into the number of cases in which this was the case. Besides, there are cases in which Section 125p Sv still offers no solution. These form notable nuances in the legislator's assumptions.

Data was made inaccessible on the basis of Section 125p Sv in fourteen cases. These were cases in which video clips, fraudulent and illicit sales websites, IP-addresses with hacked information, Telegram groups containing extremist content, and Telegram groups selling falsified documents and illegal fireworks, were made inaccessible. What is striking about these cases is that in three of these the delegated judge gave permission to apply the power embedded in Section 125p Sv by analogy, permitting such application based on Sections 181 jo. 125p Sv. No provider was heard in these cases under the presumption of the public prosecutor and the delegated judge that the provider would not cooperate. Instead, police issued an investigative officer to make the data inaccessible via a phone of a suspect in police custody.

As mentioned, Section 125p Sv is not always applicable to investigative practice. An important reason for this can be found in paragraph 4 of Section 125p Sv: a written authorisation from a delegated judge for which the service provider needs to be heard prior to the issuing of said authorisation. This judicial review by a delegated judge has been introduced because of the far-reaching nature of this power. Next to that, this review process had to ensure that data could still be made inaccessible relatively quickly. This is written in paragraph 2 of the law. The judicial review and the promise (enclosed in paragraph 2) to make data quickly inaccessible are at odds in investigative practice. Practice shows that both obtaining written authorization and hearing a service provider can take (a lot of) time. On top of that, hearing a service provider can involve other difficulties. Making data inaccessible quickly is thus not always possible, which forms an added important nuance to legislation's presumption.

A the same time, the judicial review by the delegated judge was introduced for a reason. Section 125p Sv is a far-reaching power, as it can compromise the freedom of speech. What is striking, however, is that many cases, wherein data had to be made inaccessible on the basis of Section 125p Sv, often concerned unmistakably illegal conduct. Meaning, the freedom of speech was not under discussion, in contrast to certain expression crimes. This does not take away from the possibility that Section 125p Sv could potentially curtail the freedom of speech in certain cases. Appropriate judicial testing of those requests, an important aspect of the rule of law, therefore remains important. What could be considered, however, is whether what has currently been stated in the explanatory memorandum, in regards to refraining from hearing the provider, could be included in the text of the law itself.

Lastly, there are three points of attention in regards to Section 125p Sv. The first concerns the temporary character of the power. In principle, making data permanently inaccessible happens only after a case is looked at by a judge in court. This evaluation shows that data is made inaccessible in some cases that never go to court. This means that a supposedly temporary measure can, in theory, stand indefinitely. A second point of attention, partly related to what has been already discussed, concerns cases with a foreign component. Prosecution does not usually happen in those cases, meaning no final judgements are made. Moreover, foreign providers can be hard to reach and requests for legal assistance of another country can be time consuming. Possible avenues for solutions mentioned by interviewees are more unequivocal legislation and regulation on how providers facilitating illegal content can be held more accountable, as well as the possibility to work without the need to issue a request for legal assistance, where informing the designated foreign authorities would be sufficient. A third point of attention points to the combination of options within administrative, civil, and criminal law to make data inaccessible. This evaluation put special focus on the criminal component. The creation of a good overview displaying what option would be most desirable for each situation would be advised. Especially, if the new possibilities that have entered the scene since the enactment of the Act CCIII are included, for instance those of the Authority for the Prevention of Online Terrorist Content and Child Pornography (Autoriteit Online Terroristisch en Kinderpornografisch Materiaal, ATKM).

Power to Hack (arts. 126nba, 126uba and 126zpa Sv)

In 2022, an earlier WODC-evaluation covering the power to hack was published. That publication focused on the technical side of its application (Van Uden & Van den Eeden, 2022). The present evaluation mostly focuses on the tactical side of the power to

hack's application, namely the way in which gathered information with this power is used within an investigation. This evaluation also assessed to what extent the Legislator's presumptions, including its objectives, have been actualized. To conclude, attention is paid to what has been done with the core points of attention that were formulated during the prior evaluation.

Legislation has introduced the power to hack (Sections 126nba, 126uba and 126zpa Sv) to ensure law enforcement agencies can better tackle computer crime and other form of serious crime. This was an important presumption underpinning the power to hack. Due to technological developments, existing powers would not be sufficient. On top of that, as presumed by the legislator other special investigative powers would practically and proportionally be inappropriate. This evaluation demonstrates that both presumptions, albeit with a few nuances, turned out to be correct.

In the period April 2021-April 2024, a first order to exercise the power to hack was issued in 89 criminal investigations. Almost all criminal investigations focused of one or more forms of traditional crime. A violation of the Opium Act, attempted murder/manslaughter and money laundering occurred most often. In contrast to what the name Computer Crime Act III might suggest, the power to hack was only sporadically exercised for narrowly defined cybercrime. A total of 125 computerized systems were invaded in criminal investigations in which at least one order was issued for the use of the hacking power. The bulk concerned intervention on a phone, so-called standard interventions. These findings correspond with our earlier WODC-report (Van Uden & Van den Eeden, 2022).

Several reasons were given for why tactical investigation teams deemed it necessary to intrude one or more computerized system, which are all reasons foreseen by legislation. Two reasons stood out, namely encryption of data carriers and the fear of informing a suspect about the investigation. This evaluation also demonstrates that there are cases in which the choice is made not to use the hacking power. A portion of these, are cases for which the power to hack (still) offers no solution. For example, criminal investigations who are in part conducted in a country with which the Netherlands does not have a good (legal assistance) relationship. Or cases in which there is not sufficient time to use the power to hack, for example, because a computerized system could not be accessed. This demonstrates an important nuance to the legislator's presumption.

A large majority of the interventions were successful in gaining access to a computerised system and gathering data. Often times, it concerned communication done over communication apps. In a third of the investigations the hacking power yielded information that guided investigation and in another third of the criminal investigation the yielded information was used as evidence. There is overlap between these latter two categories, since data collected in nine investigations served as both guiding information and evidence. In 40 percent of criminal investigations, the use of the hacking power did not lead to a usable yield for the criminal investigation. The way in which the hacking power contributes to tackling serious forms of crime and computer crime can thus vary, which forms another important nuance to the presumption of the legislator.

Slightly less than a third of cases, in which the hacking power was used, were brought before a court judge, and in more than a third of cases this is still to happen. What is striking about cases that have been judged in court is that the use of the hacking

power has been discussed in only a small portion of cases. In these cases, the defendant's lawyer discussed the use of the hacking power in his defence. This finding holds importance in respect to announced changes in terms of the inspection of technical tools. The police uses a technical tool to collect data. The inspection must ensure the reliability of the data gathered with the hacking power. At first the intention was to work with pre-approved technical tools only. Our prior WODC-evaluation proved this to be unrealistic, because, among other reasons, commercial tools – the nature of which the public prosecutor had decided precluded inspection – are most often worked with. In response to this finding, the former Minister of Justice and Security made the choice that all technical tools must be submitted for inspection and that working with not (fully) approved technical tools is allowed. The use of a pre-approved tools is thus no longer the norm. In case a tool is used that is not (fully) approved, it is up to the public prosecutor to install tactical safeguards and up to the court judge to weigh the evidence and make a judgment on it. Such a change, which has yet to be implemented, entails that technical tools not examined by an inspection body are no longer used. This is a positive development in itself, because it will grant insight into possible risks with respect to the reliability of the data gathered with said technical tool. In connection, an important point of attention brought forth by this evaluation is that the use of the hacking power has barely been discussed in court proceedings. Meaning, this topic is not structurally examined by a court judge and only subjected to limited assessment. This remains an important limitation, given the far-reaching character of the power.

Finally, two more important points of attention: one regarding the inspection and one regarding the use of commercial tools. As mentioned, in a letter in December 2023 the former Minister of Justice and Security announced a change in the way technical tools will be handled. This letter announced that all involved parties together would enter into consultation about this topic. This was in alignment with an important point of attention brought forth in the prior WODC-evaluation. This evaluation noted the importance of this conversation, as collecting reliable data is an interest shared among all involved parties. The present evaluation shows that, so far, this conversation has gotten off to a very slow start. Consequently, continuation of this conversation remains an important point of attention.

The second point of attention is focused on the use of commercial tools. The vast majority of cases made use of a commercial tool, both for intrusion and to gather data. This is in line with the former Minister’s expectation as formulated in her policy letter, stating that commercial tools will be used relatively often. This raises the question, however, whether the use of commercial tools should be called a tool of last resort, as it is called in legislative history, more specifically in the Investigations into Computerised Systems Decree (Besluit onderzoek geautomatiseerd werk, p. 15). The term ‘last resort’ gives rise to the suggestion that its use is exceptional, while this evaluation ultimately demonstrates that its use is rather the rule.

Conclusion

With the enactment of the Act CCIII, the legal toolkit for investigation and prosecution of computer crime has been strengthened. This was also envisioned by legislation when the Act was introduced. As shown in this evaluation, computer crime refers to computer crime in a very broad sense. In part, referring to more traditional forms of crime, using IT as a means to commit such crime.

The legal toolkit has been strengthened by five new or amended criminal offences in the Dutch Penal Code and two new powers in the Code of Criminal Procedure. Whereas before enactment, prosecution of suspects was not sufficiently possible, most of these new criminal offences now ensure such prosecution. To give examples, the fencing and stealing of data and online trade fraud. This is less so, when it comes to the amended criminal offences laid down in Sections 248a Sr (seduction of a minor) and 248e Sr (grooming). Whereas these offences gained a legal instrument (teen decoy), teen decoys are hardly used in practice.

As with many of the criminal offences, the two new powers, to make data inaccessible and to hack, have been used in practice. Both powers have ensured the carrying out of investigative actions that were previously impossible (power to hack) or only possible to a limited degree (power to make data inaccessible). These powers, directly or indirectly, contribute to tackling computer crime and other forms of serious crime. However, there are also situations, especially when it come to the power to make data inaccessible, in which these powers cannot make the desired contribution to a criminal investigation.

Finally, this evaluation highlights four aspects relevant to multiple legal provisions in Act CCIII: 1) new developments; 2) available capacity; 3) cases with an international component; and 4) (constitutional) safeguards for the use of special investigative powers.

Firstly, new developments. Part of the necessity for Section 138c Sr has disappeared. According to new jurisprudence, the Section for computer intrusion (Section 138c Sr) could also apply, especially when it comes to work situations. In regards to Section 139g Sr, recent numbers by Europol (2025) show that illegal data trade has increased, which has altered the possible impact of data fencing. As such, legislation might need to reconsider its penalty. Concerning the power to hack, it is becoming increasingly complicated to break encryption. As such, it might be of interest to legislation to reflect on how to approach this development, while taking into account the protection of fundamental rights of citizens, such a privacy, as well as the effectiveness of investigation

Secondly, we discussed available capacity. The available investigation capacity forms an important point of attention in the application of several legal provisions from the Act CCIII. This was mentioned as an important reason for why a provision, especially regarding the teen decoy, online trade fraud and the power to hack, is possibly used to a limited extent. Finding a solution for this is not simple: for instance, choices must always be made. On top of that, the question arises whether criminal law should always be the solution. As such, it might be good to look at the extent of how a broader approach, one surpassing the boundaries of criminal law, could be of (additional) use. This goes without saying that the careful evaluation of such initiatives would hold importance.

Thirdly, there are cases that have an international component. An international component in a case can impair the optimal use of some legal provisions in investigative practice. For that reason, it might be helpful to look at ways in which European and international initiatives together can increase the responsibility of service providers who facilitate criminal content. Regarding online trade fraud, it could be interesting to assess the extent in which national referral portals within Europe can

be linked to each other, so that the identity of a foreign bank account holder could be easier to identify.

The fourth and final aspect sees to the (constitutional) safeguards for the use of special investigative powers. There is a field of tension between efficiency and effectivity in the application of the evaluated powers on the one hand, and the rule of law on the other. Given the far-reaching character of these powers, the existence of strict assessment criteria is important. Nonetheless, in terms of the power to make data inaccessible, it could be examined whether certain criteria could be fulfilled differently. In terms of the hacking power, the former Minister of Justice and Security already made the choice to do so regarding the inspection of technical tools. In making this decision, this minister assumed that a court judge would assess the evidence gathered with the hacking power. However, until now court judges have only done so very sporadically. This means that an important constitutional guarantee, which is assumed to exist in practice, is not being upheld.

Literatuur

Algemeen Nederlands Woordenboek. (z.d.). Monstrans. In *Algemeen Nederlands Woordenboek.* Geraadpleegd op 30 september 2025, van anw.ivdnt.org/article/monstrans

Andringa, R. (2019, 28 mei). *Justitie en branche willen af van foute hostingbedrijven.* NOS nieuws. Geraadpleegd op 3 juni 2025, van nos.nl/artikel/2286613-justitie-en-branche-willen-af-van-foute-hostingbedrijven

Anti Money Laundering Centre. (2025, 24 maart). *Stappenplan Witwassen*. Geraadpleegd op 29 juli 2025, van www.amlc.nl/witwassen/stappenplan-witwassen/

Baarda, B., Bakker, E., Fischer, T., Julsing, M., Peters, V., Van der Velden, T., & De Goede, M. (2013). *Basisboek kwalitatief onderzoek: Handleiding voor het opzetten en uitvoeren van kwalitatief onderzoek.* (Derde druk). Noordhoff Uitgevers.

Berndsen, M. & Visser, C.J.J. (2022, 1 september). Niet elke grasduinende mol is een hacker. *Boom Strafblad*, 3(4), 160-164.

Berndsen, M. (2021). *Neerhalen Telgramkanaal in strijd met de wet.* Cybercrime Advocaten. Geraadpleegd op 30 mei 2025, van www.cybercrimeadvocaten.nl/blog/2021/11/05/neerhalen-telegramkanaal-in-strijd-met-wet

Braster, J.F.A. (2000). *De kern van casestudy's Cybercriminaliteit*. Van Gorcum en Corp.

Coinbase (z.d.). *Wat is een seed phrase?* Geraadpleegd op 2 september 2025, van www.coinbase.com/nl/learn/wallet/what-is-a-seed-phrase

Davidse, J. (2023, 24 november). Capture the red flags. *Cyber, Opportuun nummer 5.* Geraadpleegd op 14 mei 2025, van magazines.openbaarministerie.nl/opportuun/2023/05/schone-hosting

De Rechtspraak. (z.d.) *Selectiecriteria.* Geraadpleegd op 2 september 2025, van www.rechtspraak.nl/Uitspraken/Paginas/Selectiecriteria.aspx

De Rechtspraak. (z.d.). *Soorten strafrechters.* Geraadpleegd op 14 mei 2025, van www.rechtspraak.nl/Organisatie-en-contact/Rechtsgebieden/Strafrecht/Paginas/Soorten-strafrechters.aspx

Digital Trust Center. (z.d.). *Spoofing.* Ministerie van Economische Zaken. Geraadpleegd op 30 september 2025, van www.digitaltrustcenter.nl/spoofing

Europol (2025). *Steal, deal and repeat - How cybercriminals trade and exploit your data – Internet Organised Crime Threat Assessment*. Publications Office of the European Union. Geraadpleegd op 7 juli 2025, van www.europol.europa.eu/cms/sites/default/files/documents/Steal-deal-repeat-IOCTA_2025.pdf

Hoge Raad der Nederlanden. (2025, 18 maart). *Hoge Raad stelt naar aanleiding van de zaak Landeck zijn eigen rechtspraak op het punt van onderzoek aan elektronische gegevensdragers enigszins bij.* Geraadpleegd op 22 juli 2025, van www.hogeraad.nl/actueel/nieuwsoverzicht/2025/maart/hoge-raad-stelt-aanleiding-zaak-landeck-eigen-rechtspraak-punt/

Hoorweg, E. & Smallenbroek, J. (2022). *Evaluatierapport LMIO: Directe aansprakelijkheid.* Capgemini.

Hutjes, J.M. & Van Buuren, J.A. (1992). *De gevalsstudie: Strategie van kwalitatief onderzoek.* Boom.

Jansen, J., Westers, S. Twickler, S. & Stol, W. (2019). *Aankoopfraude vanuit het buitenland: Alternatieven voor opsporing*. Sdu Uitgevers, Politie & Wetenschap, NHL Stenden Hogeschool.
Krikhaar, K. (2024, 10 november). *Telegram deelt voor het eerst data met Nederlandse Openbaar Ministerie.* Tweakers. Geraadpleegd van 1 oktober 2025, van tweakers.net/nieuws/228558/telegram-deelt-voor-het-eerst-data-met-nederlandse-openbaar-ministerie.html#:~:text=Telegram%20deelt%20voor%20het%20eerst%20data%20met%20Nederlandse%20Openbaar%20Ministerie%20%2D%20Tweakers
Landelijk Bureau Vakinhoud rechtspraak. (2025, maart). *Oriëntatiepunten voor straftoemeting en LOVS-afspraken.* Geraadpleegd op 30 juni 2025, van www.rechtspraak.nl/SiteCollectionDocuments/Orientatiepunten-en-afspraken-LOVS.pdf
Lindenberg, K.K. (2016, december). De lokpuber verstop zich in het materiële strafrecht. *Ars Aequi.* 942-950. Geraadpleegd op 25 juli 2025, van arsaequi.nl/product/de-lokpuber-verstopt-zich-in-het-materiele-recht/
LMIO. (Landelijk Meldpunt InternetOplichting). (2022). *Aanpak fraude met online handel (F636): In de eenheden*. Politie.
Maesschalck, J. (2010). Methodologische kwaliteit in het kwalitatief criminologisch onderzoek. In T. Decorte & D. Zaitch (Eds.), *Kwalitatieve methoden en technieken in de criminologie* (119-145). (Tweede druk). Acco.
Mies, E. (2022, april). *Lex specialis.* Lawspot. Geraadpleegd op 30 september 2025, van www.lawspot.nl/lex-specialis/
Ministerie van Buitenlandse Zaken. (z.d.) *Rechtsmacht.* Geraadpleegd op 2 september 2025, van www.centruminternationaalrecht.nl/rechtsmacht
Ministerie van Justitie en Veiligheid. (2022, 15 december). *Veiligheidsagenda 2023-2026.* Rijksoverheid. Geraadpleegd op 2 september 2025, van open.overheid.nl/documenten/ronl-fefff06abdd2c99d8ad9be531c68a1df6deae72d/pdf
Notice-and-Take-down (2025, 13 december). *Gedragscode Notice-and-Take-Down 2018.* Geraadpleegd op 8 augustus 2025, van noticeandtakedowncode.nl/wp-content/uploads/2018/12/ECP_01054-Gedragscode-notice-and-takedown-pdf-2.pdf
NVB (Nederlandse vereniging van banken). (z.d.). *Samen werken tegen online fraude = samen informatie delen over online fraude.* Geraadpleegd op 1 september 2025, van www.nvb.nl/bank-wereld-online/samen-werken-tegen-online-fraude-samen-informatie-delen-over-online-fraude/#:~:text=Het%20Landelijk%20Meldpunt%20Internetoplichting%20(LMIO,van%20aangiftes%20van%20online%20handelsfraude.
Oerlemans, J.J. (2017). De wet computercriminaliteit III: meer handhaving op het internet. *Strafblad* 2017, (4), 350-359.
Oerlemans, J.J., De Hingh, A., Van der Wagen, W. (Red.) Verschijningsvormen van gedigitaliseerde criminaliteit. In: Van der Wagen, W., Oerlemans, J-J, Weulen Kranenbarg, M. (2024). *Basisboek cybercriminaliteit. Een criminologisch overzicht voor studie en praktijk* (pp. 105-163). Boom. Geraadpleegd op 13 oktober 2025, van verschijningsvormen-van-gedigitaliseerde-criminaliteit-oerlemans-de-hingh-van-der-wagen-2024.pdf
Openbaar Ministerie & Politie (2024). *Cybercrime beeld Nederland 2024.* Geraadpleegd op 2 september 2025, van open.overheid.nl/documenten/dpc-21ca9941df919886a1026bf06bff92299830f871/pdf
Openbaar Ministerie (2018, 1 februari). Richtlijn voor strafvordering cybercrime. *Staatscourant* 2018, (3271). Geraadpleegd op 30 juni 2025, van zoek.officielebekendmakingen.nl/stcrt-2018-3271.html

Openbaar Ministerie (2021, 27 januari). *Internationale politieoperatie LadyBird: Botnet Emotet wereldwijd ontmanteld.* Geraadpleegd op 1 juli 2025, van www.om.nl/actueel/nieuws/2021/01/27/internationale-politieoperatie-ladybird-botnet-emotet-wereldwijd-ontmanteld
Openbaar Ministerie (2022). *Operatie Centurion: landelijk actieplan OM en politie aanpak gedigitaliseerde criminaliteit.*
Openbaar Ministerie (2024, juni). *OM-richtlijnenbundel*.
Openbaar Ministerie (z.d.). *Artikel 12 Sv-procedures*. Geraadpleegd op 7 november 2024, van www.om.nl/onderwerpen/klachten/art-12
Openbaar Ministerie (z.d.). *Veelvoorkomende criminaliteit (ZSM).* Geraadpleegd op 1 september 2025, van www.om.nl/onderwerpen/veelvoorkomende-criminaliteit-zsm
Politie (2025, 9 maart). *Politie krijgt meer meldingen van seksuele misdrijven*. Geraadpleegd op 1 juli 2025, van www.politie.nl/nieuws/2025/maart/9/politie-krijgt-meer-meldingen-van-seksuele-misdrijven.html
Politie (z.d.). *Wat is grooming?* Geraadpleegd op 25 juli 2025, van www.politie.nl/informatie/wat-is-grooming.html
Rensen, F. (2025, 20 maart). Strengere wetten nodig tegen computercriminaliteit, vindt burgemeester Femke Halsema. *De Volkskrant.* Geraadpleegd op 22 juli 2025, van www.volkskrant.nl/tech/strengere-wetten-nodig-tegen-computercriminaliteit-vindt-burgemeester-femke-halsema~b50517cc/
Rijksoverheid (z.d.). *Autoriteit online Terroristisch en Kinderpornographisch Materiaal (ATKM)*. Geraadpleegd op 23 juli 2025, van www.rijksoverheid.nl/contact/contactgids/autoriteit-online-terroristisch-en-kinderpornografisch-materiaal-atkm
Schellekens, M.H.M., Koops, B.J. & Teepe, W.G. (2007). *Wat niet weg is, is gezien. Een analyse van art. 54a Sr in het licht van een Notice-and-Take-Down-regime*. Universiteit van Tilburg.
Spamhaus. (z.d.). *Frequently Ask Questions, Where can I access ROKSO?* Geraadpleegd op 14 mei 2025, van www.spamhaus.org/faqs/rokso/
Spamhaus. (z.d.). *Who is Spamhaus Project?* Geraadpleegd op 14 mei 2025, van www.spamhaus.org/who-is-spamhaus/
Spinner, Y. (2023, 25 juli). *Mogelijke grootste gebruiker illegale botmarktplaats Genesis Market opgepakt.* Tweakers. Geraadpleegd op 2 september 2025, van tweakers.net/nieuws/212048/mogelijke-grootste-gebruiker-illegale-botmarktplaats-genesis-market-opgepakt.html
Spinner, Y. (2024, 20 juni). *Europese Unie stelt stemming over omstreden wet voor encryptieachterdeur uit.* Tweakers. Geraadpleegd op 1 juni 2025, van tweakers.net/nieuws/223474/europese-unie-stelt-stemming-over-omstreden-wet-voor-encryptieachterdeur-uit.html
Van Berkel, J.J., Van Uden, A. & Goes, J.A. (2023). *De hackbevoegdheid in het buitenland: Een rechtsvergelijkend onderzoek naar wettelijke regelingen en waarborgen omtrent de kwaliteit van gegevens.* WODC. Geraadpleegd op 14 mei 2025, van repository.wodc.nl/handle/20.500.12832/3282
Van den Eeden, C.A.J., Van Berkel, J.J., Lankhaar, C.C. & De Poot, C.J. (2021). *Opsporing, vervolging en het tegenhouden van cybercriminaliteit*. WODC. Geraadpleegd op 14 mei 2025, van repository.wodc.nl/handle/20.500.12832/3114
Van Hoboken, J., Appelman, N., Van Duin, A., Blom, T., Zarouali, B., Ó Fathaigh, R., Seel, M., Stringhi, E. & Helberger, N. (2020). *WODC-onderzoek: Voorziening voor verzoeken tot snelle verwijdering van onrechtmatige online content.* Universiteit van Amsterdam: Instituut voor Informatierecht.
Van Leuken, M., Van der Rest, R. & Van 't Hof-De Goede, S. (2024, 15 november). *De civielrechtelijke afdoening van online fraude.* Secondant. Geraadpleegd op 17 juli

2024, van ccv-secondant.nl/platform/article/de-civielrechtelijke-afdoening-van-online-fraude
Van Uden, A., Van den Eeden, C.A.J. (2022). *Een empirisch onderzoek naar de uitvoering van de hackbevoegdheid (artikelen 126nba, 126uba, 126zpa Sv).* WODC. Geraadpleegd op 25 juli 2025, van repository.wodc.nl/bitstream/handle/20.500.12832/3202/Cahier%202022-8-volledige-tekst.pdf?sequence=1&isAllowed=y
Van Uffelen, J. (2025, 14 maart). Man (35) uit Zundert denkt seksdate met 15-jarige 'Delano' te hebben, maar van een ontmoeting komt het niet: 'Ik weet nu dat het echt niet kan'. *BN DeStem.* Geraadpleegd op 25 juli 2025, van www.pzc.nl/breda/man-35-uit-zundert-denkt-seksdate-met-15-jarige-delano-te-hebben-maar-van-een-ontmoeting-komt-het-niet-ik-weet-nu-dat-het-echt-niet-kan~ab4c6070/?referrer=https%3A%2F%2Fwww.google.com%2F
Vermaas, P. (2025, 21 februari). 'Is this real, or a damn joke?' Politie en OM verrasten infostealers op een internationale cyberklapdag. *Opportuun Nummer 1.* Geraadpleegd op 1 juli 2025, van magazines.openbaarministerie.nl/opportuun/2025/01/is-this-real-or-a-damn-joke
Verweij, S. & Tollenaar, N. (2020). *Recidivemeting adolescentenstrafrecht: Een onderzoek naar de haalbaarheid en eerste resultaten*. WODC. Geraadpleegd op 14 mei 2025, van repository.wodc.nl/handle/20.500.12832/936

Bijlage 1 Samenstelling begeleidingscommissie

Voorzitter	
Prof. mr. dr. M.F.H. (Marianne) Hirsch Ballin	Hoogleraar Straf- en Strafprocesrecht, Vrije Universiteit Amsterdam
Leden	
Mr. dr. J.M. (Jacqueline) Bonnes (tot 1 januari 2025)	Senior Officier van justitie Cybercrime en Digitaal Bewijs, Openbaar Ministerie, Rotterdam
Mr. K. (Koen) Hermans (vanaf 1 januari 2025)	Europees gedelegeerd officier van justitie, Europees Openbaar Ministerie
Dr. J. (Jurjen) Jansen	Lector digitale weerbaarheid, Politieacademie en NHL Stenden Hogeschool
Dr. J.J. (Jan-Jaap) Oerlemans	Universitair docent Strafrecht, Universiteit Leiden
Mr. M. (Madiha) Malik	Beleidsadviseur DGPenV, Ministerie van Justitie en Veiligheid

Bijlage 2 Werkwijze en selectie interviews

Interviews – hoe?

Topicgestuurde interviews

Net zoals voor de eerdere evaluatie is voor dit onderzoek gebruikgemaakt van topicgestuurde interviews. Om die reden is de tekst in deze paragraaf voor een groot deel overgenomen uit de eerdere evaluatie (zie ook Van Uden & Van den Eeden, 2022, p. 197-198). Voor elk interview was een topiclijst beschikbaar met daarop ook enkele voorbeeldvragen die aan de orde konden komen (Baarda et al., 2013; Hutjes & Van Buuren, 1992). De volgorde van de te bespreken topics en het aantal te stellen vragen lag van te voren niet vast. Dat had als voordeel dat gedurende het interview nader in kon worden gegaan op onderwerpen die door de geïnterviewde werden aangedragen en die voor de evaluatie interessant waren.

Bij het opstellen van de topics zijn de onderzoeksvragen leidend geweest. Zo is in elk interview gevraagd naar de inhoud van de verschillende onderdelen van de wet (indien uiteraard van toepassing). Tijdens de verdiepende interviews ging het vooral over de toepassing ervan. Afhankelijk van de geïnterviewde zijn accenten gelegd die voor de betreffende geïnterviewde relevant waren.

De wijze waarop dit evaluatieonderzoek is aangepakt was deels een inductief proces. Dat betekent dat informatie die werd verzameld gedurende het onderzoeksproces tussentijds geanalyseerd werd en waar nodig als input diende voor de rest van de dataverzameling. De informatie afkomstig uit de analyse van Kamerstukken en eerdere interviews waren daarom een belangrijke bron voor de samenstelling van de topiclijsten.

Personen die voor ons relevant waren werden via de e-mail benaderd of zij mee wilden werken aan het onderzoek. Indien zij hiermee instemden, werd een afspraak gemaakt. Het was aan de geïnterviewde of hij/zij het interview op locatie of online wilde laten plaatsvinden. Voorafgaand aan het interview werd een toelichting gegeven op het onderzoek en op de wijze waarop de in het interview verstrekte gegevens in het onderzoeksrapport konden worden gebruikt. Daarbij ging het vooral om de mogelijkheid dat één of meerdere citaten opgenomen zouden kunnen worden in het rapport. Bij deze introductie is ook aangegeven dat in het rapport de geïnterviewde niet met naam en toenaam genoemd zou worden, zodat voor de buitenwereld niet duidelijk zou zijn met wie we gesproken hebben en van welke persoon een bepaald citaat afkomstig was. Daarnaast is toestemming gevraagd om het interview op te mogen nemen. Eén geïnterviewde ging hiermee niet akkoord.

Een groot deel van de interviews is opgenomen en getranscribeerd. Nadat het transcriberen was afgerond, is de geluidsopname van het gesprek vernietigd. Het transcriberen van de interviews is tot en met november 2024 handmatig gebeurt. Daarna was software beschikbaar waarmee het interview grotendeels geautomatiseerd getranscribeerd kon worden. Elk transcript is vervolgens door een onderzoeker handmatig gecontroleerd en gecorrigeerd waar nodig. De uitwerking van de getranscribeerde interviews is in principe niet voorgelegd aan de geïnterviewden. Eén interview met twee personen vormt hierop een uitzondering. Deze geïnterviewden

wilden graag een gespreksverslag ontvangen in plaats van een letterlijke uitwerking. Met deze geïnterviewden is de afspraak gemaakt dat zij het gespreksverslag kregen toegestuurd. Enkele interviews zijn niet opgenomen, of omdat dit een telefoongesprek betrof (vier interviews) of omdat de geïnterviewde niet wilde dat het gesprek werd opgenomen (een interview). Van die interviews zijn zo snel mogelijk na afloop van het interview gespreksverslagen gemaakt. Deze verslagen zijn vervolgens voorgelegd aan de geïnterviewden met de vraag of er feitelijke onjuistheden in stonden. Vervolgens zijn de gespreksverslagen met aanvullende suggesties bekeken en beoordeeld of de suggesties konden worden overgenomen. Suggesties die betrekking hadden op een inhoudelijke aanvulling of iets dat niet klopte zijn doorgaans overgenomen. Zowel de versie met suggesties (vaak aangeven met wijzigingen bijhouden) als de versie die uiteindelijk in de analyse is meegenomen, is door de onderzoekers bewaard. In het uiteindelijke rapport zijn citaten gebruikt ter illustratie van de bevindingen. Daarbij is zo dicht mogelijk gebleven bij wat geïnterviewden hebben verteld. Hier en daar zijn woorden en zinnen weggelaten. Op die plekken is gewerkt met (…). Soms zijn woorden door de onderzoekers toegevoegd. Die woorden staan tussen […].

Selectie zaaksinterviews

Strafbaarstellingen
Over elke wettelijke bepaling is een aantal zaaksinterviews gehouden. Dit betroffen in principe interviews over zaken waarin de rechter een uitspraak had gedaan. De verwachting was dat dit soort interviews de meeste informatie zouden opleveren, omdat in die zaak alle stappen waren doorlopen. In eerste instantie was het idee om, met behulp van gegevens uit RAC-min, zaken op basis van toeval te selecteren. Op die manier zou het mogelijk zijn om enigszins te generaliseren. Om die reden zijn in excel alle parketnummers in een willekeurige volgorde geplaatst en zijn de eerste vijf 138c-parketnummers geselecteerd en de eerste 139g-parketnummers. Vervolgens is bij een contactpersoon van het Openbaar Ministerie gevraagd welke officier en/of parketsecretaris er bij deze zaak hoorde zodat die benaderd konden worden voor een zaaksinterview. We hielden acht zaaksinterviews en één officier van justitie beantwoordde een aantal vragen via de e-mail. Tijdens de eerste zaaksinterviews merkten we dat het voor officieren van justitie en parketsecretarissen lastig was om vragen te beantwoorden over zaken die al wat langer geleden op zitting behandeld waren. Om die reden hebben we ervoor gekozen om bij 326e-zaken niet meer geheel op basis van toeval te selecteren. Bovendien hadden we bij artikel 326e Sr al een groot deel van de vonnisanalyse gedaan waardoor het mogelijk was om gerichter te selecteren.

Bij de selectie van artikel 326e Sr-zaaksinterviews zijn we als volgt te werk gegaan. Op basis van de vonnisanalyse zagen we dat er variatie was wat betreft de grootte van de zaak. Omdat de wetgever dit wetsartikel in het leven heeft geroepen om grootschalige handelsfraude aan te pakken, wilden we in elk geval een aantal zaken selecteren die wat groter waren. We keken daarbij vooral naar het aantal slachtoffers in de bewezenverklaring. Daarnaast was het van belang dat de uitspraak in 2023 of in 2024 moest zijn geweest. Naast de wat grootschaligere zaken, kozen we ook twee kleinere zaken. Op basis van onze eerdere ervaringen namen we aan dat zaken die niet op rechtspraak.nl of in het e-archief stonden de wat kleinere zaken betroffen. Op basis van toeval kozen we twee zaken waarvan het vermoeden was dat het vonnis in 2024 uitgesproken was (parketnummer eindigend op 24). Helaas was niet iedereen beschikbaar die we benaderden voor een interview. Daarom zijn op een later moment nog drie aanvullende interviewverzoeken gedaan. Daarbij hebben we ook weer

geprobeerd om zaken te selecteren waarin niet al te lang geleden een vonnis was uitgesproken. Ook hier wilden niet iedereen meewerken/ontvingen we niet altijd een reactie. Uiteindelijk namen we vier zaaksinterviews af.

Op basis van RAC-min was er helaas geen overzicht beschikbaar van het aantal zaken waarin een lokpuber was ingezet. Op basis van de verkennende interviews was al duidelijk geworden dat het waarschijnlijk om een klein aantal zou gaan. Via de vonnisanalyse hebben we één zaak achterhaald waarin een politie lokpuber was ingezet. Daarnaast was er een aantal zaken (6) waarin de lokpuber een burger was. Hoewel dat niet was waar bij de inzet van de lokpuber de nadruk op lag in het wetgevingstraject, hebben we toch één zaaksinterview gehouden over een dergelijke zaak. De verwachting was dat deze vorm van een lokpuber wellicht waardevolle inzichten zou kunnen opleveren. Bovendien was in de wetgeschiedenis expliciet aandacht besteed aan 'burgerinitiatieven'. We benaderen twee officieren van justitie die recent een zaak behandeld hadden met zo'n lokpuber. Van één andere zaak waren geen contactgegevens en drie andere zaken waren langer dan een jaar geleden behandeld door de rechtbank. Eén van hen reageerde positief op ons verzoek. Daarnaast hebben we nog een interview gehad over een mensenhandelzaak. Ook daarin was gewerkt met een lokpuber, maar dat gebeurde niet op basis van de artikelen 248a en 248e Sr. Verder is in de verkennende interviews voor een groot deel gesproken over de inzet van een lokpuber waarbij het niet duidelijk was of het ging om de artikelen 248a en 248e Sr. We hebben deze interviews wel meegenomen in ons onderzoek, omdat de interviews inzicht gaven in de vraag wat het betekent om met een lokpuber te werken.

Bevoegdheden
Er zijn ook zaaksinterviews gehouden over de twee nieuwe bevoegdheden. Op basis van de vonnisanalyse en middels een uitvraag binnen het Openbaar Ministerie en de rechtspraak is duidelijk geworden dat, voor zover bekend, in veertien zaken gebruik is gemaakt van de bevoegdheid om gegevens ontoegankelijk te maken (art. 125p Sv). Van negen zaken beschikten wij over contactgegevens van de betreffende officier van justitie en of parketsecretaris. Sommige van hen waren betrokken bij meerdere zaken. Zij zijn allemaal benaderd voor een interview. Eén officier van justitie wilde niet meewerken aan een interview, vanwege 'strikte geheimhouding' waaraan deze officier van justitie gebonden was. Twee medewerkers van het Openbaar Ministerie hebben wij tweemaal gesproken, ook over redenen om artikel 125p Sv juist niet te gebruiken.

Wat betreft de hackbevoegdheid beschikten wij via de politie over een lijst van alle zaken waarin de hackbevoegdheid was ingezet. Daarnaast hebben wij in de periode maart 2019-april 2024 een vragenlijst verspreid onder alle officieren van justitie die de hackbevoegdheid één of meerdere keren in hun opsporingsonderzoek ingezet hadden. Zowel de lijst van de politie als (een deel van) de teruggestuurde vragenlijsten zijn door ons benut om zaaksinterviews te selecteren.

Op basis van de lijst van de politie hebben wij allereerst een onderscheid gemaakt tussen maatwerkzaken en standaard zaken. Bij de maatwerkzaken wilden wij graag een variatie wat betreft het geautomatiseerd werk dat was binnengedrongen meenemen, zaken waarin de buitenlandcomponent een rol speelde en een variatie wat betreft de wijze waarop gegevens werden binnengehaald. Ook namen we bij de selectie alleen zaken mee waarbij daadwerkelijk gegevens verzameld waren. We waren immers vooral benieuwd op welke wijze de verzamelde gegevens in een opsporingsonderzoek worden gebruikt. Verder ging onze voorkeur uit naar

opsporingsonderzoeken die al wat langer geleden hadden plaatsgevonden, omdat de kans dan groter was dat de zittingsrechter een uitspraak had gedaan. Uiteindelijk selecteerden we op basis van voorgaande criteria vier (van de negen) zaken.

Bij de standaardzaken keken wij in eerste instantie naar de misdrijven waarop de opsporingsonderzoeken zich richtte waarnaar een opsporingsonderzoek werd gedaan en of het gelukt was om gegevens te verzamelen. Omdat we tijdens het selecteren van zaaksinterviews ook een deel van de vragenlijsten binnen hadden gekregen en zagen dat in een deel van deze vragenlijsten aangegeven was dat een zittingsrechter een uitspraak had gedaan, hebben we eerst alle zaken in kaart gebracht waarbij een zittingsrechter een uitspraak had gedaan. Het kon daarbij ook gaan om zaken waarbij het niet gelukt was om gegevens te verzamelen. Eén van de door een zittingsrechter behandelde zaken was al geselecteerd bij de maatwerkzaken. Zes zaken bleven over en deze richtte zich op drie soorten misdrijven: moord, opium en witwassen. Dat waren toevallig ook de misdrijven in het kader waarvan de hackbevoegdheid het vaakst was ingezet. Eén van deze zaken viel af omdat deze officier van justitie al gesproken was voor de eerdere evaluatie. Een andere zaak hebben we niet meegenomen, omdat een zittingsrechter nog een uitspraak moest doen. Van de vier benaderde officieren van justitie hebben uiteindelijk drie officieren meegewerkt (twee moordzaken en één opiumzaak). Vervolgens hebben we op basis van toeval nog één witwaszaak geselecteerd, één zaak waarin het ging om brandstichting, één zaak waarin het ging om terrorisme en één wapenhandelzaak. Dat waren de strafbare feiten die het vaakst voorkwamen in opsporingsonderzoeken waarin de hackbevoegdheid was ingezet.

Bijlage 3 Zoektermen en selectie vonnissen

In deze bijlage staat beschreven op welke wijze gezocht is naar vonnissen met betrekking tot de wettelijke bepalingen uit de Wet CCII. Voor de artikelen 138c en 139g Sr hebben wij geen zoekslag uitgevoerd, omdat we op basis van RAC-min cijfers al een overzicht hadden van alle zaken waarin deze artikelen voorkwamen.

Artikel 326e Sr

Voor de vonnisanalyse inzake artikel 326e Sr zijn twee zoekslagen gedaan naar relevante vonnissen. De eerste zoekslag is gedaan op 28 augustus 2023 in het e-archief en leverde veertien resultaten op. Voor deze zoekslag is de zoekterm *326e handelsfraude* gebruikt. Deze zoekslag is gedaan met de selectie *Strafrecht* en verfijnd door te zoeken na de datum 1 maart 2019. De tweede zoekslag betrof dezelfde zoekterm en is gedaan op 6 mei 2024. Dit betrof een zoekslag in zowel het e-archief als op rechtspraak.nl. In het e-archief leverde de zoekslag 36 resultaten op en op rechtspraak.nl leverde het 18 resultaten op. Ook hierbij werd *Strafrecht* geselecteerd als rechtsgebied waarbinnen werd gezocht, na de datum 1 maart 2019. Later op 27 mei 2024 is één zaak toegevoegd die niet naar voren kwam in de zoekslag van 6 mei 2024, dit betrof een zaak in eerste aanleg (ECLI:NL:RBNNE:2020:4739) van een zaak in hoger beroep die wel naar voren kwam in de zoekslag van 6 mei 2024.

Artikelen 248a en 248e Sr

Voor de vonnisanalyse inzake artikelen 248a en 248e Sr is voor ieder artikel een zoekslag uitgevoerd op 15 mei 2024. Dit betroffen zoekslagen in zowel het e-archief als op rechtspraak.nl. Voor artikel 248a Sr is de zoekterm *248a lokpuber* gebruikt en dit leverde in zowel het e-archief als op rechtspraak.nl twee resultaten op. Hierbij werd *strafrecht* geselecteerd als rechtsgebied waarbinnen werd gezocht, na de datum 1 maart 2019. Voor artikel 248e Sr werd op dezelfde datum gezocht met de zoekterm *248e lokpuber.* De zoekslag leverde één resultaat op in het e-archief en één resultaat op rechtspraak.nl. Bij deze zoekslag werd eveneens *Strafrecht* geselecteerd als rechtsgebied waarbinnen werd gezocht, na 1 maart 2019.

Artikel 125p Sv

Voor de vonnisanalyse van de artikel 125p Sv zijn verscheidene zoekslagen uitgevoerd. De eerste zoekslag vond plaats enkel in het e-archief en vond plaats op zowel 24 als 28 augustus 2024. Dit leverde 32 resultaten op met de zoekterm *125p ontoegankelijk,* gezocht binnen *Strafrecht* en na 1 maart 2019.

Een tweede zoekslag vond plaats op 15 mei 2024 op zowel rechtspraak.nl als in het e-archief. De gebruikte zoekterm was eveneens *125p ontoegankelijk.* In het e-archief leverde dit 52 resultaten op en op rechtspraak.nl leverde dit 48 resultaten op. Ook hierbij is gezocht naar uitspraken na 1 maart 2019 binnen S*trafrecht*. Later op 22 mei 2024 is er 1 vonnis toegevoegd aan de vonnisanalyse die niet naar voren kwam met

de bovenstaande zoekslag. Dit vonnis is ons toegestuurd door het Kenniscentrum cybercrime van het Hof in Den Haag.

Een extra zoekslag vond plaats op 30 mei 2024. Hierbij werd een andere zoekterm gebruikt, namelijk *54a Sr notice and take.* Wel werd er eveneens gezocht binnen *Strafrecht* en na 1 maart 2019. Deze zoekopdracht leverde twee resultaten op in het e-archief en zes resultaten op rechtspraak.nl. Deze zoekslag leverde geen nieuwe relevante zaken op voor de vonnisanalyse. Omdat deze zoekopdracht geen relevante resultaten opleverde, is er een tweede zoekopdracht uitgevoerd op 26 juni 2024. Bij deze zoekopdracht werd gezocht op *Alle uitspraken* (alle uitspraken die een zgn. European Case Law Identifier (ECLI) hebben, zowel gepubliceerde als niet gepubliceerde uitspraken), eveneens met de selectie *Strafrecht* en na 1 maart 2019. In eerste instantie is toen gezocht met de term *54a,* dit leverde echter zeer veel resultaten op: 8.427 resultaten in het e-archief en 5.471 op rechtspraak.nl. Vervolgens is deze zoekopdracht verder verfijnd door in deze resultaten te zoeken met toevoeging van de term *ontoegankelijk* in *Alle velden*. Dit leverde 40 resultaten op in het e-archief en 37 resultaten op rechtspraak.nl.

Op 24 juni 2024 is een laatste zoekopdracht uitgevoerd. Hierbij is gezocht met de term *notice and take,* binnen *Alle uitspraken*, *Strafrecht* en na 1 maart 2019. Dit leverde 33 resultaten op in het e-archief en 32 resultaten op rechtspraak.nl.

Artikelen 126nba, 126uba en 126zpa Sv

Voor de vonnisanalyse van de hackbevoegdheid is een zoekslag uitgevoerd, deels in het e-archief en deels op rechtspraak.nl. De gebruikte zoektermen waren *~126nba ~126uba ~126zpa -encrochat.* De zoekslag op rechtspraak.nl vond plaats op 30 december 2024 en leverde 39 resultaten op. De zoekslag in het e-archief vond plaats op 6 januari 2025 en leverde 43 resultaten op. Bij de zoekslag werd gezocht binnen de selectie *Strafrecht* en na de datum 1 maart 2019.

Voor de vonnisanalyse hebben wij verder gebruik gemaakt van vonnissen over zaken die tijdens de zaaksinterviews besproken hebben. Deze vonnissen waren via onze zoekslagen niet te vinden omdat in het vonnis niet expliciet gesproken wordt over de inzet van de hackbevoegdheid. In tabellen B3.1, B3.2, B3.3, B3.4, B3.5 en B3.6 staat het totaal aantal geanalyseerde vonnissen opgenomen, en het aantal vonnissen dat uiteindelijk niet nader geanalyseerd is.[118]

[118] Wanneer een vonnis meerdere bepalingen uit de Wet CCIII bevatte, is dit vonnis bij alle betreffende bepalingen meegeteld.

Tabel B3.1 Aantal 138c-zaken vonnisanalyse

Vonnissen artikel 138c Sr	Aantal zaken
Geanalyseerde vonnissen	11
Niet geanalyseerde vonnissen	7
➢ Ontnemingsvordering	2
➢ Vonnis had betrekking op ontbinding arbeidsovereenkomst	1
➢ Geen (inhoudelijk) vonnis beschikbaar	3
➢ Artikel niet terug te vinden in tenlastelegging	1
Totaal aantal vonnissen	**18**

Tabel B3.2 Aantal 139g-zaken vonnisanalyse

Vonnissen artikel 139g Sr	Aantal zaken
Geanalyseerde vonnissen	44
Niet geanalyseerde vonnissen	11
➢ Ontnemingsvordering	4
➢ Beslissing op onderzoekswens	2
➢ Geen vonnis beschikbaar e-archief	5[119]
Totaal aantal vonnissen	**55**

Tabel B3.3 Aantal 326e-zaken in vonnisanalyse

Vonnissen artikel 326e Sr	Aantal vonnissen
Geanalyseerde vonnissen	195
➢ Vonnissen	28
➢ Beklagzaken	167
Niet geanalyseerde vonnissen	11
➢ Sprake van een civielrechtelijke kwestie	1
➢ Geen sprake van online handelsfraude	6
➢ Feiten gepleegd vóór inwerkingtreding Wet CCIII	1
➢ Gaat over gewone oplichting (art. 326 Sr)	3
Niet geanalyseerde beklagzaken	82
➢ Feit gepleegd vóór inwerkingtreding Wet CCIII	32
➢ Geen sprake van online handelsfraude	11
➢ Niet-ontvankelijk	29
➢ Intrekking beklag	10
Totaal aantal vonnissen	**288**

[119] In één zaak hadden we via een interview met een officier van justitie wel een tenlastelegging tot onze beschikking. Deze tenlastelegging hebben we, voor zover mogelijk, gebruikt in onze vonnisanalyse.

Tabel B3.4 Aantal 248a- en 248e-zaken in vonnisanalyse

Vonnissen artikelen 248a en 248e Sr	Aantal zaken
Geanalyseerde vonnissen	11
Niet geanalyseerde vonnissen	9
➢ Dader deed zich voor als een minderjarige en artikel 248a/e was niet van toepassing	1
➢ Geen sprake van een virtuele creatie	6
➢ Benadeelde bleek geen rechercheur te zijn	1
➢ Conclusie van de advocaat-generaal met betrekking tot duur van een Tbs-maatregel	1
Totaal aantal vonnissen	**20**

Tabel B3.5 Aantal 125p-zaken in vonnisanalyse

Vonnissen artikel 125p Sv	Aantal zaken
Geanalyseerde vonnissen	4
Niet geanalyseerde vonnissen	92
➢ Niet duidelijk of het over artikel 125p Sv gaat	2
➢ Artikel 125p Sv wordt niet genoemd	63
➢ Artikel 125p Sv wordt alleen genoemd maar is niet ingezet	3
➢ Beklagzaken, o.a. op grond van artikel 552a Sv	12
➢ Ontoegankelijkmaking wordt genoemd inzake artikel 350a Sr	9
➢ Verbeurdverklaring gegevensdragers en vernietiging van gegevens die ontoegankelijk zijn gemaakt ex artikel 125o Sv	1
Totaal aantal vonnissen	**96**

Tabel B3.6 Aantal 126nba-, 126uba- en 126zpa-zaken in vonnisanalyse

Vonnissen artikelen 126nba, 126uba en 126zpa Sv	Aantal zaken
Geanalyseerde vonnissen	10
Niet geanalyseerde vonnissen	39
➢ Verzoek om verschoning	1
➢ Zaak betreft een cryptocommunicatiedienst of onderzoek dat voortgevloeid is uit een cryptocommunicatiedienst	18
➢ Beslissing/beschikking rechter-commissaris	
Ex artikel 181 jo 177 Sv	3
Uitstel melding onbekende kwetsbaarheid	1
Onderzoekswensen	3
Ex artikel 126ng Sv	1
➢ (Tussen-)beslissing rechtbank	7
➢ Conclusie/Arrest HR – geen hackbevoegdheid ingezet	3
➢ Overweging verzoek raadsman	1
➢ Vonnis – geen inzet hackbevoegdheid	2
Totaal aantal vonnissen	**49**

Bijlage 4 Vragenlijst inzet hackbevoegdheid

Op 1 maart 2019 is de Wet Computercriminaliteit III (hierna Wet CCIII) in werking getreden. Met deze wet heeft de hackbevoegdheid een grondslag gekregen in het Wetboek van Strafvordering. Het WODC evalueert op aanvraag van het ministerie van Justitie en Veiligheid op dit moment de Wet CCIII en dus ook de hackbevoegdheid. Omdat u binnen één of meerdere opsporingsonderzoeken gebruik heeft gemaakt van de hackbevoegdheid, willen we u vragen onderstaande vragenlijst in te vullen. Het doel van deze vragenlijst is te achterhalen op welke wijze de hackbevoegdheid, en vooral het soort gegevens dat daarmee verzameld wordt, in een tactisch opsporingsonderzoek wordt gebruikt.
Uw antwoorden zijn van grote waarde voor onze evaluatie. Op basis van de evaluatie zal worden bekeken in hoeverre de wet voldoet en of aanpassingen nodig zijn.
Het invullen van de vragenlijst vraagt ongeveer 15 minuten van uw tijd. De vragenlijst bestaat uit 19 vooral gesloten vragen. Indien u in meerdere onderzoeken gebruik heeft gemaakt van de hackbevoegdheid, mag u zelf kiezen voor welk opsporingsonderzoek u de vragen beantwoordt. Deelname aan het onderzoek is vrijwillig en het heeft voor u geen consequenties als u de vragenlijst niet invult.

Na het invullen van de vragenlijst kunt u uw antwoorden opslaan en ze mailen naar a.van.uden@wodc.nl. Door uw antwoorden op te sturen geeft u toestemming deze te gebruiken voor de evaluatie van de Wet CCIII. Uw antwoorden zullen worden verwerkt in ons evaluatierapport. Alle antwoorden die u geeft, worden vertrouwelijk behandeld. Wij doen er alles aan uw privacy zo goed mogelijk te beschermen. Zo zullen de resultaten die wij in ons rapport gaan presenteren niet gekoppeld kunnen worden aan individuele officieren van justitie. Daarnaast wordt de e-mail met de door u ingevulde vragenlijst veilig opgeslagen. Deze e-mail wordt verwijderd nadat het onderzoek is afgerond. De onderzoeksgegevens (de ingevulde vragenlijsten) worden bewaard voor een periode van 20 jaar na afronding van het onderzoek. Uiterlijk na het verstrijken van deze termijn zullen de gegevens worden verwijderd.

Mocht u vragen hebben over het onderzoek of de vragenlijst, dan kunt u contact opnemen met Anne van Uden (hoofdonderzoeker) via a.van.uden@wodc.nl of 06-31105178.

Algemeen

1) In hoeveel Nederlandse opsporingsonderzoeken heeft u, sinds de invoering van de hackbevoegdheid (126nba, 126 uba, 126 zpa Sv), een bevel afgegeven om de hackbevoegdheid in te zetten?
LET OP: Deze vragenlijst gaat <u>niet</u> over opsporingsonderzoeken waarin het buitenland een verzoek heeft gedaan om in Nederland de hackbevoegdheid in te zetten of waarin aan het buitenland het verzoek is gedaan om de hackbevoegdheid aldaar in te zetten.
……
Indien u in meerdere Nederlandse opsporingsonderzoeken een bevel hebt afgegeven de hackbevoegdheid in te zetten, dan kunt u vanaf nu de vragen beantwoorden met betrekking tot één van deze opsporingsonderzoeken. U mag zelf kiezen welk opsporingsonderzoek dat is. Wel is het belangrijk om de vragen alleen voor het door u gekozen opsporingsonderzoek te beantwoorden.

2) In welk jaar heeft u in het opsporingsonderzoek waarover u nu de vragen beantwoordt, een bevel afgegeven de hackbevoegdheid in te zetten?
……
3) Hoeveel bevelen voor de inzet van de hackbevoegdheid zijn door u afgegeven in het opsporingsonderzoek waarover u nu deze vragen beantwoordt?
Aanklikken wat van toepassing is.

☐ Geen (u hoeft de vragenlijst niet verder in te vullen)
☐ 1 bevel
☐ 1 bevel en één of meer verlengingen
☐ 2 bevelen
☐ 2 bevelen, en één of meerdere verlengingen
☐ Meer dan 2 bevelen, namelijk……
☐ Meer dan 2 bevelen, inclusief één of meer verlengingen, namelijk……

4) Wat is het belangrijkste misdrijf waarvoor u een bevel heeft afgegeven de hackbevoegdheid in te zetten?
Meerdere antwoorden mogelijk. Aanklikken wat van toepassing is.

☐ Moord en/of doodslag (inclusief een poging daartoe en/of voorbereiding)
☐ Misdrijven gerelateerd aan de Opiumwet
☐ Valsheid in geschrifte en of oplichting
☐ Lidmaatschap criminele organisatie
☐ Witwassen
☐ Zedenmisdrijf
☐ Terrorisme (inclusief voorbereiding)
☐ Computervredebreuk
☐ Anders, namelijk ……

Doel en noodzaak inzet hackbevoegdheid
De volgende set vragen richt zich op het doel waarvoor de hackbevoegdheid is ingezet en de belangrijkste redenen om een bevel af te geven de hackbevoegdheid in te zetten.

5) Wat was het doel van de inzet van de hackbevoegdheid?
Meerdere antwoorden mogelijk. Aanklikken wat van toepassing is.

☐ Het achterhalen van identificerende gegevens, zoals identiteit en of locatie van de gebruiker en of van het geautomatiseerd werk **ten behoeve van de inzet van andere bevoegdheden**.
☐ Het achterhalen van identificerende gegevens, zoals identiteit en of locatie van de gebruiker en of van het geautomatiseerd werk **ten behoeve van het bepalen van de verdere richting van het opsporingsonderzoek**.
☐ Het achterhalen van identificerende gegevens, zoals identiteit en of locatie van de gebruiker en of van het geautomatiseerd werk **ten behoeve van verder tactisch optreden**.
☐ Het verkrijgen van gegevens die op een geautomatiseerd werk stonden opgeslagen op het moment dat het bevel werd afgegeven.
☐ Het verkrijgen van gegevens die op een geautomatiseerd werk werden opgeslagen gedurende de looptijd van het bevel.
☐ Het ontoegankelijk maken van gegevens waarmee strafbare feiten werden gepleegd.
☐ Het verstoren van een botnet.
☐ Het aftappen en opnemen van versleutelde communicatie op het apparaat.
☐ Het opnemen van vertrouwelijke communicatie met een technisch hulpmiddel.
☐ Stelselmatige observatie middels het activeren van de GPS-functie van een smartphone.
☐ Stelselmatige observatie middels locatiebepaling aan de hand van doorgifte wifi-netwerken.
☐ Stelselmatige observatie middels plaatsing op een persoon.
☐ Anders, nl……

6) Waarom was het nodig een bevel af te geven om de hackbevoegdheid in uw opsporingsonderzoek in te zetten?
Meerdere antwoorden mogelijk. Aanklikken wat van toepassing is.

☐ De benodigde gegevens waren versleuteld.
☐ De benodigde gegevens stonden opgeslagen in de cloud.
☐ De verdachte(-n) maakte(n) gebruik van draadloze netwerken.
☐ Andere bevoegdheden konden niet worden ingezet, omdat de locatie van het geautomatiseerd werk onbekend was.
☐ Bij de inzet van andere bevoegdheden zou de verdachte dan wel medeverdachten op de hoogte raken van het opsporingsonderzoek.
☐ De inzet van een andere bevoegdheid zou niet proportioneel zijn.
☐ Andere bevoegdheden hadden geen betrekking op de toegang tot gegevens via elektronische weg.
☐ Anders, nl ……

7) Welke andere bevoegdheden heeft u, voorafgaand aan het bevel voor de inzet van de hackbevoegdheid, overwogen om binnen uw opsporingsonderzoek in te zetten, en wat was het (eventuele) resultaat?
Meerdere antwoorden mogelijk. Aanklikken wat van toepassing is.

	Niet overwogen voorafgaand aan inzet hackbevoegdheid	Wel overwogen, maar niet ingezet voorafgaand aan inzet hackbevoegdheid	Wel overwogen en ingezet voorafgaand aan inzet hackbevoegdheid, maar leverde te weinig informatie op
Doorzoeking van een plaats (art. 125i Sv)	☐	☐	☐
Doorzoeking van een plaats (art. 110 Sv) en onderzoek van daar in beslaggenomen goederen	☐	☐	☐
Netwerkzoeking (art. 125j Sv)	☐	☐	☐
Ontsleutelbevel voor derden (art. 125k Sv)	☐	☐	☐
Verzoek tot afgifte van gegevens (art. 32b Cybercrime Verdrag)	☐	☐	☐
Vorderen van opgeslagen gegevens (art. 126ng)	☐	☐	☐
Tappen van gegevens (art. 126m, 126t en 126zg)	☐	☐	☐
Verstrekken van gegevens (art. 126n, 126na, 126ng, 126u, 126ua, 126ug, 126zh, 126zi en 126zl Sv)	☐	☐	☐
Opnemen van vertrouwelijke communicatie (artikelen 126l, 126s en 126zf Sv)	☐	☐	☐
Inbeslagname (art. 95, lid 1 Sv, art. 96, lid 1 Sv, art. 96c lid 1, 97, lid 1, 98, lid 1, 99, lid 1 Sv)	☐	☐	☐
Observatie (artikelen 126g, 126o en 126zd, lid 1, onderdeel a Sv)	☐	☐	☐
Stelselmatige inwinning van informatie (art 126j, 126qa en 126zd, lid 1, onderdeel c Sv)	☐	☐	☐
Inkijkoperatie (art. 126k, 126r en 126zd, lid 1, onderdeel d Sv)	☐	☐	☐
Inloggen op account van de verdachte na machtiging van de rechter-commissaris (art. 181 jo (177 jo) 126ng, lid 2 Sv)	☐	☐	☐

Netwerkzoeking na inbeslagname van de gegevensdrager (art. 557 Innovatiewet)	☐	☐	☐

Anders, nl……

Binnendringen
De volgende set vragen richt zich op het binnendringen in het geautomatiseerd werk/ de geautomatiseerde werken.

8) Welk geautomatiseerd werk mocht worden binnengedrongen?
Meerdere antwoorden mogelijk. Aanklikken wat van toepassing is.
☐ Telefoon
☐ Meerdere telefoons
☐ Telefoon in combinatie met ander geautomatiseerd werk
☐ Meerdere telefoons in combinatie met ander geautomatiseerd werk
☐ Server
☐ Meerdere servers
☐ Laptop
☐ Meerdere laptops
☐ Router/modem
☐ Meerdere routers/modems
☐ Wireless Access Point (WAP)
☐ Meerdere WAP's
☐ Anders, namelijk……

9) Welk aantal geautomatiseerde werken mocht worden binnengedrongen?

☐ 1 geautomatiseerd werk
☐ 2 geautomatiseerde werken
☐ Meer dan 2 geautomatiseerde werken, namelijk……

10) Is het gelukt om binnen te dringen in het geautomatiseerd werk/de geautomatiseerde werken?

☐ Ja, in alle geautomatiseerde werken (ga naar vraag 12).
☐ Ja, in een deel van de geautomatiseerde werken (ga naar vraag 11 en daarna naar vraag 12).
☐ Nee, in geen enkel geautomatiseerd werk is uiteindelijk binnengedrongen (ga naar vraag 11 en ga daarna naar vraag 16).

11) Indien het (deels) niet gelukt is het geautomatiseerd werk binnen te dringen, wat was hiervoor de reden?
☐ Technisch gezien is het niet gelukt om het geautomatiseerd werk/de geautomatiseerde werken binnen te dringen.
☐ Tactisch gezien was het niet meer nodig het geautomatiseerd werk/ de geautomatiseerde werken binnen te dringen, omdat de benodigde gegevens al op een andere manier waren verkregen.
☐ Tactisch gezien was het niet meer nodig het geautomatiseerd werk/ de geautomatiseerde werken binnen te dringen, omdat de zaak al rond was.
☐ Anders, namelijk……

Verzamelen van gegevens
De volgende set vragen gaat over het soort gegevens dat verzameld is met behulp van de hackbevoegdheid.

12) Is het gelukt om met behulp van de hackbevoegdheid gegevens te verzamelen?
☐ Ja (ga naar vraag 15)
☐ Deels (ga naar vraag 14)
☐ Nee (ga naar vraag 13)

13) Indien <u>geen</u> gegevens konden worden verzameld, wat was hiervoor de reden?
……(ga hierna naar vraag 16)

14) Indien <u>deels geen</u> gegevens konden worden verzameld, wat was hiervoor de reden?
……(ga hierna naar vraag 15)

15) Welke gegevens zijn verzameld?
Meerdere antwoorden mogelijk. Aanklikken wat van toepassing is.

☐ Locatie van het geautomatiseerd werk
☐ Gebruiker van het geautomatiseerd werk
☐ Versleutelde communicatieberichten (tekst) via communicatieapps
☐ Versleutelde communicatieberichten (spraak) via communicatieapps
☐ Filmpjes
☐ Foto's
☐ Tekstbestanden
☐ Live communicatie
☐ Locatiegegevens van het geautomatiseerd werk/de geautomatiseerde werken
☐ Inloggegevens
☐ Anders, namelijk……

Opbrengst binnen het opsporingsonderzoek
De volgende vragen richten zich op wat de middels de hackbevoegdheid verzamelde gegevens hebben opgeleverd binnen het opsporingsonderzoek.

16) Wat heeft de hackbevoegdheid opgeleverd binnen het opsporingsonderzoek?
Meerdere antwoorden mogelijk. Aanklikken wat van toepassing is.

☐ Geen relevante informatie (ga naar vraag 19)
☐ Sturingsinformatie (ga naar vraag 17)
☐ Bewijs (ga naar vraag 18)
☐ Anders, namelijk……(ga hierna naar vraag 19)

17) Wat voor sturingsinformatie heeft de hackbevoegdheid opgeleverd? Wordt bij het beantwoorden van de vraag svp zo concreet als mogelijk hoe de gegevens zijn gebruikt om het opsporingsonderzoek verder richting te geven.
…… (ga hierna naar vraag 18 en/of 19)

18) Wat voor bewijs heeft de hackbevoegdheid opgeleverd? Wordt bij het beantwoorden van de vraag svp zo concreet als mogelijk.
……(ga hierna naar vraag 19)

Afronding
De laatste vraag gaat over een eventuele behandeling van de zaak in de rechtbank.

19) Is de zaak inmiddels inhoudelijk door een zittingsrechter behandeld?

☐ Ja, en de zittingsrechter heeft een uitspraak gedaan.
☐ Ja, maar de zittingsrechter heeft nog geen uitspraak gedaan.
☐ Nee, er is alleen nog een pro forma zitting geweest.
☐ Nee, en de zaak zal niet door een zittingsrechter behandeld worden.
☐ Nee, maar een zittingsrechter zal zich nog wel over de zaak buigen.
☐ Anders, namelijk……

Dit was de laatste vraag van deze vragenlijst. Veel dank voor het invullen! Mocht u nog iets kwijt willen over uw ervaringen met de hackbevoegdheid waar we niet naar hebben gevraagd, maar die u wel belangrijk vindt om te delen, dan kan dat op deze plek. Ook opmerkingen over het evaluatieonderzoek kunt u hier kwijt.
……

Bijlage 5 Soorten misdrijven hackbevoegdheid

Tabel B5.1 Soorten misdrijven

Misdrijf	Aantal inzetten
Ambtsmisdrijf	2
➢ Combinatie misdrijf tegen openbare orde	1
➢ Combinatie met hacken	1
Brandstichting	3
➢ Brandstichting	2
➢ Combinatie met WWM	1
Corruptie en openbaar maken gegevens	1
Diefstal met geweld	1
Fraude	1
Genocide en foltering	1
Georganiseerd verband	2
➢ Georganiseerd verband	1
➢ Combinatie dreiging met geweld	1
Hacken, diefstal gegevens, afpersing	1
Misdrijven gerelateerd aan openbaar gezag en/of staatsveiligheid	3
Mix	2
Moord/doodslag	19
➢ Moord/doodslag en of poging daartoe en of voorbereiding	13
➢ Combinatie met misdrijf tegen openbare orde	1
➢ Combinatie met WWM	1
➢ Combinatie met WWM, brandstichting, uitbraak uit gevangenis en mogelijk terrorisme	1
➢ Combinatie met witwassen	1
➢ Combinatie met opium en georganiseerd	2
Opiumwet	27
➢ Opiumwet	12
➢ Combinatie met georganiseerd verband	2
➢ Combinatie met veiligheid goederen	1
➢ Combinatie met witwassen	3
➢ Combinatie met witwassen en georganiseerd verband	4
➢ Combinatie met witwassen en medicijnstoffenhandel	1
➢ Combinatie met witwassen en valsheid in geschrifte	1
➢ Combinatie met witwassen en WWM	2

Misdrijf	Aantal inzetten
➢ Combinatie met fraude en corruptie	1
Oplichting en georganiseerd verband	1
Verstrekken staatsinlichtingen	1
Terrorisme	2
WWM	5
Wederrechtelijke vrijheidsberoving	1
Witwassen	12
➢ Witwassen	7
➢ Combinatie met georganiseerd verband	2
➢ Combinatie met georganiseerd verband, fraude en corruptie	1
➢ Combinatie met georganiseerd verband en opium	1
➢ Combinatie met computervredebreuk en opzetheling	1
Zeden	3
Onbekend	1
Totaal	**89**

Het Wetenschappelijk Onderzoek- en Datacentrum (WODC), Kennisinstituut voor de rechtsstaat, is een onafhankelijk kennisinstituut dat valt onder het ministerie van Justitie en Veiligheid. Het WODC draagt bij aan behoud en verbetering van de rechtsstaat via het (laten) uitvoeren van kwalitatief hoog wetenschappelijk onderzoek. En door het aanbieden van gevraagde en ongevraagde kennis, verbeterpunten en (waar mogelijk) denkrichtingen.

Voor meer informatie, bezoek www.wodc.nl