Het decryptiebevel en het nemo-teneturbeginsel. Nopen ontwikkelingen sinds 2000 tot invoering van een ontsleutelplicht voor verdachten?

Koops, E.J.

Publication date:
2012

Document Version
Publisher's PDF, also known as Version of record

Het decryptiebevel en het nemo-teneturbeginsel

305

Onderzoek en beleid

Het decryptiebevel en het nemo-teneturbeginsel

Nopen ontwikkelingen sinds 2000 tot invoering van een ontsleutelplicht voor verdachten?

B.J. Koops

Universiteit van Tilburg

BOOM LEMMA UITGEVERS

Wetenschappelijk Onderzoek- en Documentatiecentrum
Ministerie van Veiligheid en Justitie

Onderzoek en beleid

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

Exemplaren van dit rapport kunnen worden besteld bij het distributiecentrum van Boom Lemma uitgevers:
Boom distributiecentrum te Meppel
Tel. 0522-23 75 55
Fax 0522-25 38 64
E-mail budh@boomdistributiecentrum.nl

Voor ambtenaren van het Ministerie van Veiligheid en Justitie is een beperkt aantal gratis exemplaren beschikbaar.
Deze kunnen worden besteld bij:
Bibliotheek WODC
Postbus 20301, 2500 EH Den Haag
Deze gratis levering geldt echter slechts zolang de voorraad strekt.

De integrale tekst van de WODC-rapporten is gratis te downloaden van www.wodc.nl.
Op www.wodc.nl is ook nadere informatie te vinden over andere WODC-publicaties.

ISBN 978-90-5931-934-9
NUR 820

Voorwoord

Het beginsel van nemo tenetur vormt een essentieel onderdeel van het Nederlandse stelsel van strafvordering. Met dit beginsel wordt bedoeld dat niemand mag worden gedwongen aan zijn eigen veroordeling mee te werken. Het beginsel van nemo tenetur wordt ook op Europees niveau beschermd, namelijk door artikel 6 van het EVRM (recht op een eerlijk proces).
In sommige gevallen is het echter vrijwel onvermijdelijk dat de verdachte op enigerlei wijze meewerkt aan het opsporingsonderzoek. Tot nu toe is die noodzaak vooral aan de orde bij het afnemen van lichaamsmateriaal van de verdachte. Inmiddels zijn er in het Nederlandse recht dan ook uitzonderingen op dit beginsel aanvaard, zoals de verplichting voor een verdachte om mee te werken aan een bloedalcoholonderzoek of de afgifte van speeksel of wangslijmvlies voor de vergelijking van DNA-profielen. Maar voor de verklaringsvrijheid van een verdachte geldt het beginsel van nemo tenetur tot nu toe vrijwel onverkort.
De technische ontwikkelingen maken het steeds eenvoudiger om elektronische gegevens te versleutelen en daarmee voor de overheid af te schermen. De techniek is geavanceerd en voor de opsporingsdiensten steeds lastiger te doorbreken. Daarom is vanuit de opsporing en de politie de roep steeds luider om de verdachte te kunnen dwingen tot de afgifte van beveiligingscodes of wachtwoorden. Hierbij is verwezen naar wetgeving in het Verenigd Koninkrijk die in de mogelijkheid voorziet van een bevel van een opsporingsambtenaar aan een verdachte om mee te werken aan het ontsleutelen van versleutelde gegevens.
In reactie hierop heeft de Minister van Veiligheid & Justitie aangegeven dat een zorgvuldige belangenafweging is vereist en dat de juridische haalbaarheid van een decryptiebevel, in het licht van het in artikel 6 EVRM vervatte nemo-teneturbeginsel, nauwgezet zou moeten worden bezien. Aan Bert-Jaap Koops, hoogleraar regulering van technologie bij het Centrum voor Recht, Technologie en Samenleving (TILT) van de Universiteit van Tilburg, is begin 2012 gevraagd hiernaar onderzoek te verrichten. In 2000 heeft Koops reeds de publicatie 'Verdachte en ontsleutelplicht: hoe ver reikt nemo tenetur?' geschreven. Daarin kwam hij tot de slotsom dat een dergelijke regeling een inbreuk op het nemo-teneturbeginsel maakte en dat er onvoldoende argumenten waren om die inbreuk te rechtvaardigen. Hij liet echter ruimte voor een andere afweging indien de ontwikkelingen daartoe aanleiding zouden geven. Die ontwikkelingen – in het bijzonder ten aanzien van kinderpornografie en encryptietechniek, maar ook dat er landen zijn die sedertdien een ontsleutelplicht hebben ingevoerd – hebben aanleiding gegeven professor Koops te vragen zijn onderzoek uit 2000 te actualiseren.
Het resultaat van dit verzoek is vervat in deze studie. Koops beschrijft de veranderingen sinds 2000 in het gebruik van cryptografie door verdachten, evenals de processen die de handhaafbaarheid van een ontsleutelplicht beïnvloeden. Vervolgens behandelt hij de ontwikkeling van het nemo-teneturbeginsel

sinds 2000 aan de hand van jurisprudentie van het Europees Hof voor de Rechten van de Mens. Daarna geeft hij het Nederlands recht ten aanzien van het ontsleutelbevel weer en de Nederlandse jurisprudentie rond het nemo-teneturbeginsel. Vervolgens maakt hij een rechtsvergelijkende uitstap naar België, Frankrijk, het VK en de VS, en in het kort naar andere landen waar sinds 2000 een ontsleutelplicht is ingevoerd. Tot slot analyseert hij deze ontwikkelingen in het licht van de factoren die in het onderzoek uit 2000 een rol speelden en bespreekt en waardeert hij op basis daarvan verschillende opties voor een wettelijke regeling van een ontsleutelplicht.
Het onderzoek geeft een goed beeld van de EHRM-rechtspraak over het nemo-teneturbeginsel sinds 2000, aangevuld met relevante rechtspraak uit Nederland, het VK en de VS. Daarbij heeft Koops geprobeerd de hoofdlijnen van de jurisprudentie te schetsen, en worden de criteria voor de beoordeling van een mogelijke schending van nemo tenetur helder uitgewerkt. Het is daarom ook voor strafrechtjuristen die niet direct met ICT-vraagstukken te maken hebben interessant om van deze studie kennis te nemen.

Prof. dr. Frans Leeuw
Directeur WODC

Inhoud

Afkortingen

BSv	Wetboek van Strafvordering [België]
c.	chapter [VK]
CCV	Cybercrime-Verdrag
CP	Code pénal [Frankrijk]
CPP	Code de procédure pénale [Frankrijk]
Cth	Commonwealth of Australia
EHRM	Europees Hof voor de Rechten van de Mens
EVRM	Europees Verdrag tot bescherming van de Rechten van de Mens en de Fundamentele Vrijheden
HCA	High Court of Australia
HR	Hoge Raad
ICT	informatie- en communicatietechnologie
NJ	*Nederlandse Jurisprudentie*
OM	Openbaar Ministerie
Parl.St.	Parlementaire Stukken [België]
Rb.	Rechtbank
RIPA	Regulation of Investigatory Powers Act 2000
r.o.	rechterlijke overweging
s.	section [VK]
Sr	Wetboek van Strafrecht
Sv	Wetboek van Strafvordering
TB	terabyte
U.S.C	United States Code
VK	Verenigd Koninkrijk
VoIP	Voice over Internet Protocol [spraaktelefonie via internet]
VS	Verenigde Staten
Wiv 2002	Wet op de inlichtingen- en veiligheidsdiensten 2002
WODC	Wetenschappelijk Onderzoek- en Documentatiecentrum

Samenvatting

Achtergrond en vraagstelling

Wanneer een misdadiger gegevens op zijn computer of zijn communicatie versleutelt, wordt het lastig voor de opsporing om informatie te verzamelen via computeronderzoek en aftappen. Een van de mogelijke oplossingen voor dit probleem is het dwingen van aangewezen personen om versleutelde gegevens te ontsleutelen. Nederland heeft daartoe al bij de Wet computercriminaliteit (1993) een ontsleutelplicht ingevoerd. Het bevel tot ontsleuteling kan momenteel echter niet aan verdachten worden gegeven. De Nederlandse wetgever is er tot nu toe van uitgegaan dat een ontsleutelbevel in strijd is met het beginsel dat verdachten niet aan hun eigen veroordeling hoeven mee te werken, oftewel het nemo-teneturbeginsel. Volgens vaste jurisprudentie van het Europees Hof voor de Rechten van de Mens (EHRM) is het nemo-teneturbeginsel een kernonderdeel van het recht op een eerlijk proces. De precieze reikwijdte van het beginsel is echter niet volledig uitgekristalliseerd en in wetgeving en rechtspraak zijn de nodige uitzonderingen op het beginsel geaccepteerd.
In een onderzoek uit 2000 (B.J. Koops, *Verdachte en ontsleutelplicht: hoe ver reikt nemo tenetur?*) werd geconcludeerd dat een ontsleutelplicht voor verdachten een ingrijpende inbreuk maakt op het beginsel, die niet kon worden gerechtvaardigd door het opsporingsbelang. Sinds 2000 is er echter het nodige gebeurd op het vlak van technologie en rechtspraak over het nemo-teneturbeginsel. Ook is in de Tweede Kamer, naar aanleiding van de Amsterdamse zedenzaak rond Robert M., de vraag opgeworpen of niet alsnog een ontsleutelplicht voor verdachten kan worden ingevoerd. Tegen die achtergrond wordt in dit rapport als hoofdvraag onderzocht in hoeverre, gelet op de ontwikkelingen sinds 2000, een decryptiebevel – een bevel tot het verlenen van medewerking aan het toegankelijk maken van beveiligde gegevens – verenigbaar is met het nemo-teneturbeginsel. Deze vraag is beantwoord aan de hand van literatuuronderzoek, analyse van de buitenlandse rechtsontwikkeling en vijf semigestructureerde interviews met deskundigen uit de opsporingspraktijk.

Het nemo-teneturbeginsel

De reikwijdte van het nemo-teneturbeginsel is in de rechtspraak van het Europees Hof (EHRM) niet significant veranderd sinds 2000. De kern van het beginsel ligt nog altijd in de verklaringsvrijheid: op een verdachte mag soms enige druk worden uitgeoefend om verklaringen te verkrijgen, maar die druk mag niet groot zijn en moet omkleed zijn met procedurele waarborgen, zoals de toegang tot een advocaat en het informeren van de verdachte welke gevolgen zijn houding kan hebben voor zijn procesgang. Buiten het afleggen van verklaringen geldt dat naarmate de verdachte actiever moet meewerken, en

met name als hij daarbij een intellectuele inspanning moet verrichten, een dwang om mee te werken eerder in strijd komt met nemo tenetur. Een ontsleutelplicht ligt dicht aan tegen het afleggen van een verklaring, omdat het wachtwoord in het hoofd van de verdachte zit en niet kan worden verkregen zonder diens (intellectuele) inspanning. Een decryptiebevel voor verdachten maakt daarom, net als in 2000, nog steeds inbreuk op het nemo-teneturbeginsel.
Deze inbreuk kan echter gerechtvaardigd zijn – er zijn immers uitzonderingen op het beginsel mogelijk. Het Europees Hof kijkt naar vier factoren die tezamen bepalen of een afgedwongen medewerking wel of niet aanvaardbaar is in het licht van het nemo-teneturbeginsel:
1 de aard en mate van dwang;
2 het gewicht van het publiek belang;
3 de aanwezigheid van relevante waarborgen in de procedure;
4 de manier waarop het afgedwongen materiaal wordt gebruikt.
Naarmate de dwang om mee te werken groter is en het afgedwongen materiaal een zwaardere rol heeft bij het bewijs, zal het publiek belang van afgedwongen medewerking des te groter moeten zijn en zullen er meer waarborgen moeten zijn voor rechtsbescherming. Bij een lagere mate van dwang of een ondergeschikte rol van afgedwongen bewijsmateriaal zal een ontsleutelplicht echter eerder de toets doorstaan.
Ook in de Nederlandse rechtsontwikkeling is de rol van het nemo-teneturbeginsel grotendeels hetzelfde gebleven als in 2000. Een decryptiebevel voor verdachten zou nog steeds afwijken van het systeem van de Nederlandse wet voor zover de weigering mee te werken strafbaar zou zijn. Wel blijkt uit de rechtspraak dat er goede mogelijkheden zijn om ontsleuteling aan verdachten te vragen wanneer zij zich kunnen verschonen van medewerking, vergelijkbaar met de regeling van het verhoor waarbij de verdachte mag zwijgen. De verdachte neemt dan een zeker procesrisico als hij niet meewerkt, omdat onder bepaalde omstandigheden (in situaties waarin de aanwezigheid van beveiligde bestanden duidelijk vragen oproept) de rechter zijn decryptieweigering kan gebruiken bij het bewijs, de straftoemeting of andere beslissingen ten nadele van de verdachte.

Ontwikkelingen in het buitenland

In 2000 waren er geen landen met een ontsleutelplicht voor verdachten, maar dat is inmiddels substantieel gewijzigd. In België mag het decryptiebevel niet aan verdachten worden gegeven, maar Frankrijk en het Verenigd Koninkrijk (VK) hebben wel een ontsleutelplicht voor verdachten ingevoerd. Het VK kent een uitgebreide wettelijke regeling voor wanneer en hoe een decryptiebevel mag worden gegeven, met diverse waarborgen voor rechtsbescherming. In Frankrijk beperkt de wettelijke regeling zich tot strafbaarstelling van het wei-

geren te ontsleutelen. Australië heeft een wettelijk decryptiebevel ingevoerd dat zich specifiek tot verdachten richt, terwijl in de Verenigde Staten (VS) zich een ontsleutelplicht voor verdachten uitkristalliseert in de rechtspraak, die onder bepaalde voorwaarden verenigbaar wordt geacht met (de vergelijkbare Amerikaanse variant van) het nemo-teneturbeginsel.
Uit de Britse en Amerikaanse rechtspraak komt naar voren dat het meewerken aan ontsleuteling lijkt op het afleggen van een verklaring, omdat het impliciet de band van de verdachte met het versleutelde materiaal erkent. Dit maakt inbreuk op nemo tenetur, maar die inbreuk is volgens Amerikaanse rechtspraak gerechtvaardigd: a) als het een uitgemaakte zaak is om welke bestanden het gaat en dat de verdachte in staat is te ontsleutelen, of b) als er bewijsuitsluiting wordt beloofd voor het (belastende) materiaal dat na ontsleuteling tevoorschijn komt. In het Verenigd Koninkrijk wordt de inbreuk van het decryptiebevel op nemo tenetur aanvaardbaar geacht vanwege de vele *checks and balances* in de Britse regeling en vanwege het feit dat de zittingsrechter altijd de mogelijkheid heeft om afgedwongen bewijs, als dat belastend blijkt, terzijde te leggen. Hoewel de rechtspraak in deze landen nog in ontwikkeling is, blijkt wel dat een ontsleutelplicht voor verdachten onder omstandigheden aanvaardbaar wordt geacht, waarbij in de rechtspraak de grenzen van het nemo-teneturbeginsel nader kunnen worden bepaald. De Britse wetgeving biedt daarmee aanknopingspunten voor de Nederlandse beleidsvorming, maar de regeling kan niet rechtstreeks worden overgezet. Het Verenigd Koninkrijk heeft gekozen voor een hoge mate van dwang (er staat 2-5 jaar gevangenisstraf op het niet meewerken), die alleen kan worden gerechtvaardigd door vergaande waarborgen, waaronder de mogelijkheid van bewijsuitsluiting maar ook enkele waarborgen die Nederland niet kent, zoals een onafhankelijke toezichthouder op de opsporing.

Handhaafbaarheid en ontwikkelingen in techniek

Het gebruik van cryptografie door verdachten is sinds 2000 toegenomen, met name door versleuteling van opgeslagen gegevens. Vooralsnog lijkt het gebruik van sterke encryptie vooral voor te komen bij bepaalde kinderpornonetwerken (die vaak voorop lopen met het gebruik van 'verbergtechnieken'), maar andere groepen misdadigers zouden kunnen volgen. Een belangrijke ontwikkeling is de opkomst van 'antiforensische' programma's, dat wil zeggen cryptoprogramma's om niet alleen bestanden te versleutelen maar ook om het bestaan van de versleutelde bestanden 'aannemelijk ontkenbaar' te maken. Bij dergelijke programma's is het moeilijk voor justitie om te bewijzen dat er überhaupt versleutelde gegevens op de harde schijf staan.
Aan de andere kant heeft justitie ook ruimere mogelijkheden dan in 2000 het geval leek, om te betogen dat een verdachte wél mogelijk belastend materiaal (zoals binnengehaalde kinderporno) op zijn computer heeft staan en in staat

is te ontsleutelen, bijvoorbeeld met aanwijzingen uit een internettap of verkeersgegevens. Ook de Britse en Amerikaanse rechtspraak toont aan dat er diverse gevallen mogelijk zijn waarin de verdachte 'iets uit te leggen heeft' als hij niet wil ontsleutelen.
Deze twee ontwikkelingen heffen elkaar niet op, maar betekenen eerder dat het sterk van de omstandigheden zal afhangen of een decryptiebevel handhaafbaar is. Anders dan in 2000 hoeft de problematische handhaafbaarheid dan ook niet te leiden tot een categorische afwijzing van een ontsleutelplicht voor verdachten; er kan eerder worden gekozen voor een wettelijke bevoegdheid die afhankelijk van de omstandigheden wel of niet kan worden gebruikt. Vermoedelijk zal een ontsleutelplicht weinig effectief zijn tegen zware en berekenende misdadigers die sowieso niet meewerken met justitie, en vermoedelijk eerder de kleinere of minder slimme misdadigers treffen. De ervaring in het Verenigd Koninkrijk is ook dat een decryptiebevel slechts in een beperkt aantal gevallen wordt opgelegd, waarbij minder dan de helft meewerkt en waarbij in vier jaar tijd slechts zes weigeraars veroordeeld zijn voor niet meewerken.

Conclusies en aanbevelingen

Uit bovenstaande bevindingen blijkt dat een decryptiebevel aan verdachten niet onverenigbaar is met het nemo-teneturbeginsel. Het hangt ervan af hoe het wettelijk wordt vormgegeven (bijvoorbeeld welke soort en mate van dwang kan worden gebruikt) en hoe het in een concreet geval wordt toegepast. Waar de studie uit 2000 concludeerde dat Nederland geen ontsleutelplicht voor verdachten zou moeten invoeren omdat die alleen effectief zou zijn bij een sterke mate van dwang maar daarmee een onaanvaardbare inbreuk op het nemo-teneturbeginsel zou opleveren, ligt de situatie nu enigszins anders. De ontwikkelingen in het buitenland en in de techniek suggereren dat een ontsleutelplicht voor verdachten wel verenigbaar is met het nemo-teneturbeginsel en – weliswaar voor een beperkt aantal gevallen – effectief zou kunnen zijn, mits de wettelijke regeling en uitvoering met voldoende waarborgen zijn omkleed.
Mocht de wetgever, zoals in het VK, voor een ontsleutelplicht met een hoge mate van dwang kiezen, dan zullen er aanzienlijke waarborgen moeten worden getroffen, zoals een schriftelijk bevel, toegang tot een advocaat, een redelijke bewijsvoeringslast, een discretionaire bevoegdheid voor de rechter om zelfbelastend materiaal alsnog uit te sluiten van bewijs, en toezicht op de praktijk door een onafhankelijk toezichthouder. Het is ook denkbaar om een lagere mate van dwang te kiezen door een weigering om te ontsleutelen niet zelfstandig strafbaar te stellen, maar deze weigering door de rechter te laten meewegen bij beslissingen over bewijs of strafoplegging. Daarnaast kan justitie in voorkomende gevallen ook overwegen om een verdachte bewijsuitslui-

ting toe te zeggen als hij ontsleutelt; het ontsleutelde materiaal kan dan niet tegen de verdachte worden gebruikt, maar wel tegen anderen of bijvoorbeeld voor het identificeren (of uitsluiten) van slachtoffers, wat in kinderpornozaken een belangrijk aspect kan zijn.
Wanneer de verschillende opties in samenhang worden bekeken, zijn er grofweg drie mogelijkheden voor de Nederlandse wetgever ten aanzien van de ontsleutelplicht voor verdachten.

1 *De huidige situatie handhaven.* Een ontsleutelbevel mag dan niet worden gegeven aan verdachten, maar politie en justitie kunnen verdachten wel verzoeken om vrijwillige medewerking. Onder omstandigheden kan de rechter binnen de huidige wet tot op zekere hoogte rekening houden met het feit dat een verdachte niet ontsleutelt, in de bewijsconstructie of bij de strafoplegging.
2 *Een decryptieregeling conform de regeling van het verhoor.* De praktijk van het vragen om ontsleuteling wordt geformaliseerd, in de wet of in lagere regelgeving, waarbij het verzoek wordt genormeerd op dezelfde wijze als het verhoor (art. 29 Sv). Dit zal voor de praktijk op zich niet veel verschil maken, maar het past beter in het systeem van de wet omdat het meewerken aan ontsleuteling meer lijkt op het afleggen van een verklaring dan op het uitleveren van voorwerpen. De normering van een decryptieverzoek conform de regeling van het verhoor heeft als voordeel dat de bijbehorende waarborgen van toepassing zijn, zoals de toegang tot een advocaat en de cautie. Dit kan de mogelijkheden versterken om binnen de grenzen van het nemo-teneturbeginsel negatieve conclusies te verbinden aan de proceshouding van de niet-meewerkende verdachte.
3 *Een decryptiebevel aan verdachten met strafbaarstelling van weigering.* Het niet-meewerken aan een decryptiebevel wordt strafbaar gemaakt op basis van artikel 184 Sr (maximaal drie maanden gevangenisstraf) of met een zelfstandige strafbaarstelling met een hogere maximumstraf. Vanuit de EHRM-eisen zal een zwaardere straf eerder aanvaardbaar zijn als die zich beperkt tot specifieke delicttypen waarbij versleuteling aantoonbaar een groot maatschappelijk probleem veroorzaakt. Een dergelijke wetswijziging maakt een grotere inbreuk op het nemo-teneturbeginsel dan de vorige mogelijkheid en zal met veel waarborgen moeten worden omkleed en zorgvuldig moeten worden gemotiveerd. Om het recht zichzelf niet te belasten niet van zijn betekenis te ontdoen, zal daarbij in elk geval altijd de zittingsrechter de mogelijkheid moeten hebben om alsnog de onder dwang ontsleutelde gegevens uit te sluiten van het bewijs.

De analyse van de EHRM-rechtspraak en het systeem van de Nederlandse wet wijst uit dat de tweede mogelijkheid te prefereren is boven de eerste mogelijkheid. Anders dan in 2000 hoeft de derde mogelijkheid echter niet op voorhand te worden afgewezen. Er is enige ruimte binnen de grenzen van het nemo-teneturbeginsel om een onder strafdreiging afgedwongen ontsleutelplicht voor verdachten in te voeren. De effectiviteit daarvan zal gezien de

zware eisen niet groot zijn, maar kan in incidentele gevallen wel aanwezig zijn. Het is daarom vooral een beleidsafweging of een strafbaarstelling van decryptieweigering – die binnen de grenzen van het nemo-teneturbeginsel mogelijk is als er voldoende waarborgen zijn – te prefereren is boven een decryptieregeling conform de regeling van het verhoor.
Gegeven deze conclusie verdient het aanbeveling dat de wetgever een hernieuwde afweging maakt of en onder welke omstandigheden een decryptiebevel aan verdachten zou kunnen worden gegeven. In elk geval zou de wetgever serieus de tweede mogelijkheid moeten overwegen. De keuze tussen de tweede en derde mogelijkheid (oftewel tussen weinig of veel dwang) komt vooral neer op een beleidsafweging. Het gaat daarbij niet om een zwart-witafweging tussen legitimiteit en effectiviteit; belangrijk is vooral dat bij een ontsleutelplicht voor verdachten een zorgvuldige combinatie wordt gekozen van uit te oefenen dwang, de manier waarop afgedwongen materiaal wordt gebruikt en procedurele waarborgen, en dat vanuit het publiek belang zorgvuldig wordt gemotiveerd waarom een gekozen regeling een aanvaardbare inbreuk op het nemo-teneturbeginsel oplevert.
Bij de beleidsafweging is het belangrijk om geen wonderen te verwachten van een decryptiebevel. Het zal alleen effect kunnen sorteren in een beperkt aantal gevallen waarin een verdachte duidelijk 'iets uit te leggen heeft' en waarin er al veel bewijs tegen de verdachte bestaat. De wetgever moet ook terughoudend zijn met een instrumentele inzet van het strafrecht; de bedoeling is immers om misdadigers te straffen voor feiten die zij hebben begaan, niet om verdachten te straffen voor het niet meewerken aan bewijsgaring. Verder verdient het aanbeveling om bij de beleidsvorming rond de ontsleutelplicht te kijken naar het bredere perspectief van problemen waar de digitale opsporing tegenaan loopt (zoals cloud computing) en naar alternatieve manieren om het probleem van encryptie aan te pakken, zoals Trojaanse politiepaarden die wachtwoorden of sleutels heimelijk kunnen onderscheppen.

1 Inleiding

> 'The invocation of the principle of non self-incrimination may well represent the polite end of the possible range of responses.' (Walsh, 1996)

1.1 Achtergrond

In de jaren negentig is veel gediscussieerd over de problemen die het gebruik van cryptografie door misdadigers zou (gaan) opleveren voor de opsporing en vervolging van strafbare feiten. Wanneer een misdadiger de gegevens op zijn computer of zijn communicatie versleutelt, wordt het lastig om informatie te verzamelen via computeronderzoek en aftappen. Een van de mogelijke oplossingen voor dit probleem is het dwingen van aangewezen personen om versleutelde gegevens te ontsleutelen. Nederland heeft daartoe al bij de Wet computercriminaliteit (1993) een ontsleutelplicht ingevoerd. Het bevel tot ontsleuteling kan echter niet aan verdachten worden gegeven, vanwege het nemo-teneturbeginsel dat stelt dat verdachten niet aan hun eigen veroordeling hoeven mee te werken. In de aanloop naar de Wet computercriminaliteit II heeft de minister van Justitie aanvankelijk voorgesteld om alsnog verdachten te dwingen om te ontsleutelen, maar bij nader inzien daarvan afgezien (zie paragraaf 5.1.2).
De Nederlandse wetgever is er tot nu toe dus van uitgegaan dat een ontsleutelbevel in strijd is met het nemo-teneturbeginsel. Volgens vaste jurisprudentie van het Europees Hof voor de Rechten van de Mens (EHRM, hierna ook te noemen: het Europees Hof) ligt het nemo-teneturbeginsel besloten in het hart van artikel 6 EVRM, het recht op een eerlijk proces. De precieze reikwijdte van het beginsel is in de jurisprudentie niet volledig uitgekristalliseerd. Volgens het Europees Hof ligt de ratio van nemo tenetur onder andere in het beschermen van verdachten tegen niet-passende dwang door de autoriteiten, waardoor het bijdraagt aan het voorkomen van justitiële dwalingen en het vervullen van de doeleinden van artikel 6, te weten het waarborgen van een eerlijk proces. Met die strekking in gedachten heeft het EHRM in het *Saunders*-arrest overwogen dat materiaal dat wordt afgedwongen, maar dat onafhankelijk van de wil van de verdachte bestaat, buiten de reikwijdte van het nemo-teneturbeginsel valt. Het gaat dan bijvoorbeeld om bloed- en urinemonsters, DNA-materiaal en opnames van stemgeluid. Ook documenten bestaan onafhankelijk van de wil van de verdachte en kunnen volgens de rechtspraak doorgaans worden gevorderd. Het afleggen van verklaringen wordt echter in de meeste gevallen beschermd door het nemo-teneturbeginsel.
Het is niet eenvoudig om een bevel om gegevens te ontsleutelen – wat vaak zal neerkomen op het afgeven van een wachtwoord waarmee gegevens beveiligd zijn – te positioneren binnen de EHRM-rechtspraak. Aan de ene kant gaat het om materiaal dat onafhankelijk van de wil van de verdachte bestaat (de verdachte kan immers met zijn wil niet het wachtwoord veranderen), aan

de andere kant kan justitie de ontsleuteling niet afdwingen als de verdachte niet wil meewerken (het wachtwoord zit immers in het hoofd van de verdachte). Het Europees Hof heeft zich over deze specifieke vraag nog niet uitgelaten.
In 2000 heb ik een omvangrijke studie gepubliceerd over het decryptiebevel aan de verdachte.[1] De conclusie van die studie was dat een dergelijke regeling een inbreuk op het nemo-teneturbeginsel maakt en dat er onvoldoende argumenten waren om die inbreuk te rechtvaardigen. Bij die conclusie speelde een belangrijke rol dat een ontsleutelplicht naar verwachting weinig effectief zou zijn vanwege de moeilijke bewijsbaarheid dat een verdachte daadwerkelijk in staat is mee te werken aan ontsleuteling. Ik liet echter ruimte voor een andere afweging indien latere ontwikkelingen daartoe aanleiding zouden geven. Inmiddels, ruim twaalf jaar later, zijn er de nodige ontwikkelingen in het encryptiegebruik door misdadigers, in de jurisprudentie over het nemo-teneturbeginsel en in wetgeving in andere landen. Deze ontwikkelingen roepen de vraag op of de conclusie uit 2000 nu anders zou uitvallen.
Deze vraag heeft een hoge beleidsrelevantie. In een parlementair overleg over de aanpak van kinderpornografie in 2011 is de vraag opgeworpen of het mogelijk is verdachten in kinderpornozaken van wie gegevensdragers in beslag zijn genomen, te verplichten medewerking te verlenen aan het ontsleutelen van versleutelde gegevens. Naar aanleiding hiervan heeft de minister van Veiligheid en Justitie toegezegd de behoefte aan een bevoegdheid tot het vorderen van de ontsleuteling van gegevens, de juridische haalbaarheid van zo'n bevoegdheid in het licht van het nemo-teneturbeginsel, de categorieën van delicten waarvoor dit wenselijk zou kunnen zijn en de procedurele waarborgen voor een zorgvuldige toepassing nader te zullen onderzoeken.[2]

1.2 Doelstelling en vraagstelling

Voor het onderzoek van de minister van Veiligheid en Justitie naar de mogelijkheden om een ontsleutelplicht voor verdachten in te voeren, is de reikwijdte van het nemo-teneturbeginsel een centrale vraag. Vanwege de complexiteit van deze vraag is besloten een extern onderzoek te laten verrichten. Het WODC heeft daartoe, op verzoek van de Directie Wetgeving van het Ministerie van Veiligheid en Justitie, een onderzoek uitgezet dat beoogt om de studie uit 2000 te actualiseren. Dit rapport is de verslaglegging van dat onderzoek.
De *doelstelling* van het onderzoek is, ter ondersteuning van het beleid, de verenigbaarheid te onderzoeken van een decryptiebevel aan verdachten met het in artikel 6 EVRM vervatte nemo-teneturbeginsel. In het licht van de ontwikkelingen in criminaliteit, technologie, rechtspraak en buitenlandse wet-

1 Koops 2000.
2 *Kamerstukken II* 2010/11, 32 500 VI, nr. 106, p. 3-4. Zie hierover paragraaf 5.1.3.

geving in het afgelopen decennium, wordt onderzocht of en onder welke voorwaarden de eventuele inbreuk op het nemo-teneturbeginsel te rechtvaardigen is.
In het kader van deze doelstelling is gekozen voor de volgende centrale *vraagstelling*:

> In hoeverre is een decryptiebevel – een bevel tot het verlenen van medewerking aan het toegankelijk maken van beveiligde gegevens – verenigbaar met het nemo-teneturbeginsel?

Deze vraagstelling wordt behandeld aan de hand van de volgende *deelvragen*.

1. Wat waren de factoren en argumenten die een rol speelden bij de conclusie in 2000 dat een decryptiebevel inbreuk maakt op het nemo-teneturbeginsel en dat deze inbreuk destijds niet te rechtvaardigen was?
2. Wat is de reikwijdte en achtergrond van het nemo-teneturbeginsel?
   a. Hoe heeft de Europese en Nederlandse rechtspraak over het nemo-teneturbeginsel zich sinds 2000 ontwikkeld?
   b. Welke typen inbreuken zijn sedert 2000 toegelaten op het nemo-teneturbeginsel en welke omstandigheden hebben daarbij een rol gespeeld?
3. Wat zijn de ervaringen in andere landen met een decryptiebevel?
   a. In welke landen is een decryptiebevel ingevoerd, en mag in die landen het bevel aan verdachten worden gegeven? Hoe wordt in die landen het decryptiebevel gepositioneerd, gesanctioneerd en beargumenteerd?
   b. Hoe verhoudt in deze landen het decryptiebevel zich tot het nemo-teneturbeginsel?
4. Wat valt er te zeggen over de verwachte effectiviteit en handhaafbaarheid van een decryptiebevel?
   a. Wat zijn relevante ontwikkelingen sinds 2000 op het gebied van kinderpornografie met betrekking tot encryptiegebruik, opsporing en bewijsgaring?
   b. Zijn er ontwikkelingen in de technologie die tot een andere conclusie leiden over de te verwachten effectiviteit dan in de 2000-studie?
   c. Hoe verhouden de ervaringen in andere landen met een decryptiebevel aan verdachten zich tot de bezwaren in de 2000-studie over de verwachte effectiviteit en handhaafbaarheid?
5. Gegeven de bevindingen uit de vorige deelvragen, in hoeverre is een decryptiebevel verenigbaar met het nemo-teneturbeginsel?

1.3 Afbakening

Bij de beantwoording van de vragen ligt de nadruk op een actualisering van de studie uit 2000. Voor zover nodig voor een goed begrip van de bevindingen wordt de situatie van voor 2000 kort uitgelegd, maar verder niet geanalyseerd. Het onderhavige onderzoek volgt grotendeels de opzet van de studie uit 2000, maar is in één opzicht beperkter. De studie uit 2000 besteedde niet alleen aandacht aan het commune strafrecht – de strafbaarstellingen en procedures in het Wetboek van Strafrecht en het Wetboek van Strafvordering – maar ook aan het bijzondere strafrecht, zoals strafbaarstellingen en bevoegdheden in sectorale wetgeving (zoals belasting en verkeer). Vanwege de aanleiding van het huidige onderzoek – primair gelegen in encryptie in kinderpornozaken – beperkt dit onderzoek zich tot het commune strafrecht. Een van de aandachtspunten daarbij is of een ontsleutelplicht specifiek dient te worden gericht op bepaalde delicten, zoals kinderporno, of generiek op alle typen (ernstige) strafbare feiten.
In een ander opzicht is dit onderzoek breder dan de studie uit 2000. De problematiek van niet-toegankelijke gegevens ligt deels in encryptie (versleuteling van gegevens) maar deels ook in beveiligde toegang tot computers (zoals wachtwoordbeveiliging). De aard van deze problematiek maakt geen verschil vanuit het oogpunt van het nemo-teneturbeginsel: in beide gevallen gaat het om de vraag of van een verdachte gevorderd kan worden dat hij beveiligde gegevens toegankelijk maakt, waarbij de toegang vrijwel altijd zal bestaan uit een wachtwoord. (Ook bij encryptie zal een ontsleutelbevel vaak neerkomen op het afgeven van een wachtwoord; de decryptiesleutel wordt namelijk door het encryptieprogramma opgeslagen op een gegevensdrager en beveiligd met een wachtwoord. Het encryptieprogramma zal na invoering van het wachtwoord de decryptiesleutel kunnen gebruiken om versleutelde gegevens te ontsleutelen.) Om deze reden behandelt dit onderzoek zowel het ontsleutelbevel als het bevel de toegang tot een beveiligde computer te verschaffen.
Ik beperk mij in dit onderzoek tot situaties waarin de beveiliging van gegevens gebaseerd is op een wachtwoord. Er zijn ook ontwikkelingen op het gebied van biometrische informatiebeveiliging, dat wil zeggen dat de toegang tot beveiligde gegevens (waaronder de door een cryptoprogramma opgeslagen decryptiesleutel) niet plaatsvindt via invoering van een wachtwoord maar met biometrische controle, zoals een vingerafdruk of irisscan.[3] De vragen rond het nemo-teneturbeginsel komen dan enigszins anders te liggen, omdat medewerking van de verdachte dan niet neerkomt op een intellectuele inspanning maar op een fysieke inspanning, namelijk (in het geval van beveiliging door vingerafdruk) het plaatsen van de vinger op een biometrielezer. Dit onderscheid is relevant vanuit nemo-teneturperspectief (zie paragraaf 7.4.2). Biometrisch gefaciliteerde informatiebeveiliging staat echter nog in de kinderschoenen. Bovendien lijkt het op voorhand niet wenselijk om een

3 Zie hierover Brenner 2011, p. 85.

onderscheid te maken tussen de precieze techniek waarmee gegevens beveiligd zijn, omdat misdadigers dan vanzelf zouden uitwijken naar de techniek die de meeste nemo-teneturproblemen oplevert.[4] Daarom wordt hier de potentieel meest inbreukmakende vorm van beveiliging onderzocht, namelijk met een wachtwoord dat in het hoofd van de verdachte zit. Voor zover een decryptiebevel daarvoor verenigbaar zou blijken met het nemo-teneturbeginsel, zal het decryptiebevel dan ook kunnen worden toegepast bij biometrische versleuteling.
Bij de beantwoording van de derde deelvraag, naar bevindingen in andere landen, worden in eerste instantie de ons omringende landen betrokken, omdat de rechtsstelsels van die landen over het algemeen beter vergelijkbaar zijn met het Nederlandse stelsel dan die van andere landen. Daarom worden in hoofdstuk 6 achtereenvolgens België, Frankrijk en het Verenigd Koninkrijk behandeld. Duitsland wordt echter niet zelfstandig besproken, omdat Duitsland geen expliciete ontsleutelplicht kent en de wetgever zich daarom ook niet uitgelaten heeft over de verhouding tussen een decryptiebevel en het nemo-teneturbeginsel. Wel wordt in aanvulling op de ons omringende landen aandacht besteed aan de Verenigde Staten, omdat daar in de afgelopen jaren interessante jurisprudentie is ontwikkeld over de relatie tussen een decryptiebevel en het nemo-teneturbeginsel (dat in het Amerikaanse strafrecht een veelal vergelijkbare rol vervult met die in het Europese recht). Voor de volledigheid wordt aansluitend kort de situatie in andere landen met een ontsleutelplicht, waaronder Australië, aangestipt.
Bij de opzet van het onderzoek is overwogen om naast het nemo-teneturbeginsel ook aandacht te besteden aan andere grondrechten waarop een ontsleutelplicht voor verdachten inbreuk zou kunnen maken. Daarbij werd vooral gedacht aan het recht op privacy. Het moeten vertellen van een wachtwoord kan de privacy van de verdachte raken – wat in zijn hoofd zit, behoort immers al snel tot de persoonlijke levenssfeer. Dit betekent dat artikel 8 EVRM – het recht op privacy – van toepassing kan zijn. Een decryptiebevel zal in dat geval moeten voldoen aan de eisen van artikel 8 lid 2 EVRM: het moet voorzien zijn bij wet (daaraan wordt voldaan door een specifieke regeling in het Wetboek van Strafvordering), een legitiem doel dienen (daaraan wordt voldaan omdat een decryptiebevel dient tot opsporing van strafbare feiten) en noodzakelijk zijn in een democratische samenleving. Aan deze laatste eis zal relatief makkelijk voldaan zijn, aangezien het vorderen van een wachtwoord betrekkelijk weinig ingrijpend is in verhouding tot allerlei andere gegevens waarvan de overheid in het kader van de strafvordering kennis kan nemen. Een wachtwoord is niet bijzonder privacygevoelig; het kan soms enige persoonlijke informatie bevatten (zoals het favoriete sigarettenmerk, vgl. noot 267), maar zal meestal weinig zeggen over de persoonlijke levenssfeer. Een wachtwoord is ook geen gedachte, maar iets van feitelijke aard,

4 'It makes little sense to allow the government's ability to decrypt computers to turn arbitrarily on the authentication method of an encryption program.' Ungberg 2009, p. 548.

vergelijkbaar met bijvoorbeeld personalia of identificerende gegevens die van verdachten kunnen worden gevorderd (art. 27a Sv). Een decryptiebevel fungeert daarbij hoofdzakelijk als steunbevoegdheid die wordt ingezet om gegevens te ontsluiten die anderszins in handen van justitie komen. Meestal zal dat gaan via bevoegdheden als doorzoeking en inbeslagneming van computers, een vordering tot uitlevering van computers of gegevens, of het aftappen van communicatie. Wanneer justitie een grondslag heeft om deze, veelal ingrijpende, bevoegdheden in te zetten, is de inbreuk op de privacy die het vergaren van de gegevens met zich meebrengt, gelegitimeerd.[5] Het vorderen van ontsleuteling (of ontsluiting van een computer) maakt in die gevallen niet of nauwelijks meer inbreuk op de privacy dan de bevoegdheid in zichzelf al met zich meebrengt. De toestemming tot een doorzoeking, gegevensvordering of tap impliceert immers al dat de gegevens vergaard mogen worden die op basis van die bevoegdheid te verkrijgen zijn.
De enige situatie waarin een ontsleutelplicht een zelfstandige inbreuk op de privacy zou maken, is als versleutelde gegevens van de verdachte niet via een opsporingsbevoegdheid bij de verdachte zijn verkregen maar op een andere manier, bijvoorbeeld wanneer een uitgeleende laptop bij een medeverdachte in beslag wordt genomen of wanneer een huisgenoot vrijwillig de computer van verdachte naar het politiebureau brengt. Dat zijn atypische gevallen die in de praktijk slechts sporadisch zullen voorkomen. Voor die enkele gevallen lijkt mij de eventuele inbreuk op de privacy van een ontsleutelplicht verdedigbaar op basis van de leerstukken van bijvangst (als bij een bevoegdheid onbedoeld meer of andere belastende gegevens naar voren komen, mogen deze worden gebruikt voor de opsporing) of van het zogenoemde presenteerblaadje (als justitie spontaan en ongevraagd onrechtmatig verkregen gegevens in handen krijgt, mogen deze toch worden gebruikt). Daarom zal in deze studie verder geen aandacht worden besteed aan het recht op privacy.

1.4 Gebruikte terminologie

Voor de leesbaarheid wordt gemakshalve in deze studie gesproken over een ontsleutelplicht en een decryptiebevel; daaronder moet dan (tenzij anders aangegeven) mede worden verstaan een plicht om de toegang tot een beveiligde computer[6] mogelijk te maken. Ik gebruik daarbij de termen 'ontsleutelplicht' en 'decryptiebevel' door elkaar als aanduiding voor een wettelijke bevoegdheid om een verdachte te vorderen zijn wachtwoord (en eventueel

5 Waarmee niet gezegd is dat de huidige regeling van opsporingsbevoegdheden altijd voldoende waarborgen biedt om het recht op privacy te beschermen. Er valt veel voor te zeggen om in het tijdperk van mobiele internettelefoons en 'ubiquitous computing' de bevoegdheden tot doorzoeking en inbeslagneming buiten de woning meer te clausuleren dan de huidige wetgeving doet, maar dat is een andere kwestie die voor dit onderzoek niet aan de orde is.

6 Onder een computer wordt in dit verband verstaan een geautomatiseerd werk (een inrichting bestemd om langs elektronische weg gegevens op te slaan, te verwerken en over te dragen, art. 80sexies Sr), wat een klassieke computer of laptop kan zijn maar ook een tablet-pc, mobiele telefoon of *smartphone*.

andere voor ontsleuteling nodige gegevens) af te geven dan wel zelf te ontsleutelen of de computer toegankelijk te maken. Daarbij gebruik ik vaak de termen 'sleutel' en 'wachtwoord' als functioneel synoniem van elkaar; daaronder moet dan worden verstaan alle informatie die nodig is om ontsleuteling of beveiliging ongedaan te maken, wat kan betekenen dat naast het wachtwoord of de sleutel ook het algoritme of encryptiedocumentatie moet worden overhandigd.[7] De term 'decryptieweigering' wordt gehanteerd voor het niet-meewerken van de verdachte aan een ontsleutelbevel, wat dus ook de weigering omvat om toegang tot een beveiligde computer te verschaffen. Voor een goed begrip van de tekst is het ook nuttig om te wijzen op enkele juridische termen. Het begrip 'gronddelict' of 'hoofdzaak' verwijst naar het strafbare feit waarvan een persoon wordt verdacht, ter onderscheiding van het 'instrumentele' delict van decryptieweigering (in het geval de wetgever zou besluiten om een weigering om mee te werken strafbaar te stellen). Een decryptieweigering kan ook op een andere manier een rol spelen in het strafrecht, namelijk doordat de rechter bepaalde conclusies trekt uit het feit dat de verdachte niet wil meewerken. Dit wordt aangeduid als het trekken van 'negatieve conclusies' of 'belastende gevolgtrekkingen' (in het Engels 'adverse inferences'). Tot slot moet de lezer voor ogen houden dat een onderscheid wordt gemaakt tussen de termen 'inbreuk' en 'schending'. Een opsporingsbevoegdheid kan inbreuk maken op een grondrecht – zoals het nemo-teneturbeginsel – maar dat betekent niet per se dat dit ontoelaatbaar is. Grondrechten zijn immers niet absoluut; er mag inbreuk op worden gemaakt. Wanneer de inbreuk echter de grenzen van toelaatbaarheid overschrijdt, is er sprake van een schending van het grondrecht. Waar in deze studie wordt gesteld dat een ontsleutelplicht inbreuk maakt op het nemo-teneturbeginsel, is dus steeds de vervolgvraag of deze inbreuk toelaatbaar is gelet op de grenzen die het Europees Hof stelt aan het recht op een eerlijk proces; zo niet, dan is er sprake van een schending van het nemo-teneturbeginsel.

1.5 Methoden van onderzoek

Het onderzoek is uitgevoerd op basis van literatuuronderzoek en enkele interviews. Het literatuuronderzoek bestond uit een analyse van de EHRM-rechtspraak over het nemo-teneturbeginsel sinds 2000, aangevuld met relevante rechtspraak uit Nederland, het VK en de VS en wetenschappelijke literatuur over de reikwijdte van het nemo-teneturbeginsel.
Het literatuuronderzoek is aangevuld met enkele semigestructureerde interviews met deskundigen uit de opsporingspraktijk. Voor Nederland zijn interviews in persoon gehouden met deskundigen van het KLPD, het regiokorps Amsterdam-Amstelland en de landelijk officier van justitie voor cybercrime, en telefonische interviews met een deskundige van de politie Oost-Neder-

7 Vgl. Kaspersen 1993, p. 142.

land en de landelijk officier van justitie kinderporno. Voor de situatie in België is een telefonisch interview gehouden met een onderzoeksrechter. In de interviews is gevraagd naar ervaringen met encryptie in de opsporingspraktijk en naar standpunten over de wenselijkheid en haalbaarheid van een ontsleutelplicht voor verdachten. In bijlage 4 staat een overzicht van de geïnterviewde personen.
Het onderzoek is uitgevoerd van januari tot en met juni 2012. De rapportage is afgerond in september 2012. Bij het uitvoeren van het onderzoek en het schrijven van de rapportage ben ik ondersteund door een begeleidingscommissie (zie bijlage 1). Ik dank de leden van de begeleidingscommissie voor hun waardevolle adviezen en suggesties. Ik dank voorts de geïnterviewde deskundigen voor hun bijdrage aan het onderzoek, alsmede Matthias Borgers, Tijs Kooijmans, Marcia Hofmann, Garry Trillet, Gregor Urbas en Pieter Verrest, die waardevolle informatie hebben geleverd over onderdelen van het onderzoek.

1.6 Leeswijzer

Hoofdstuk 2 biedt een samenvatting van de studie uit 2000. De volgende hoofdstukken brengen vervolgens de ontwikkelingen in kaart sinds 2000. In hoofdstuk 3 worden de ontwikkelingen in cryptografie en cryptografiegebruik behandeld, waarbij ingegaan wordt op het gebruik van cryptografie door verdachten, de kraakbaarheid van cryptografie en ontwikkelingen die de handhaafbaarheid van een ontsleutelplicht beïnvloeden. Vervolgens wordt in hoofdstuk 4 de ontwikkeling van het nemo-teneturbeginsel geschetst, aan de hand van de jurisprudentie van het Europees Hof voor de Rechten van de Mens. Hoofdstuk 5 belicht de ontwikkelingen in het Nederlandse recht, eerst de wettelijke regeling van het ontsleutelbevel en vervolgens de Nederlandse rechtspraak rond het nemo-teneturbeginsel, waarbij ook recente jurisprudentie aan bod komt waarin een decryptieweigering is gebruikt ten nadele van de verdachte. Hoofdstuk 6 bespreekt de ontwikkelingen sinds 2000 in België, Frankrijk, het VK en de VS en, voor de volledigheid maar beknopt, andere landen die sinds 2000 een ontsleutelplicht hebben ingevoerd.
In hoofdstuk 7 worden deze ontwikkelingen vervolgens geanalyseerd aan de hand van de factoren die een rol speelden in de studie uit 2000. Per factor wordt onderzocht of de ontwikkelingen sinds 2000 nopen tot een andere invulling of weging van deze factor bij de afweging of de inbreuk van een ontsleutelplicht op het nemo-teneturbeginsel aanvaardbaar is. Aan de hand van deze herziene invulling en weging van factoren worden vervolgens in paragraaf 7.7 de diverse opties voor een ontsleutelplicht, zoals behandeld in de studie uit 2000, opnieuw besproken en gewaardeerd. Dit leidt tot een conclusie over de verenigbaarheid van een ontsleutelplicht van verdachten met het nemo-teneturbeginsel.

In hoofdstuk 8 worden de bevindingen van het onderzoek samengevat in de vorm van een antwoord op de afzonderlijke deelvragen uit paragraaf 1.2. Op basis van de conclusies wordt aanbevolen dat de wetgever een hernieuwde afweging maakt of en onder welke omstandigheden een decryptiebevel aan verdachten zou kunnen worden gegeven. De afsluitende paragraaf geeft aanknopingspunten en overwegingen die de wetgever bij die afweging kan betrekken.

2 De ontsleutelplicht voor verdachten anno 2000

In de jaren negentig was er veel discussie over de problemen die cryptografie zou (kunnen gaan) opleveren voor de opsporing. In mijn proefschrift uit 1999 concludeerde ik dat er weinig concrete aanwijzingen waren dat het op dat moment daadwerkelijk een groot probleem voor de opsporing was, terwijl de voorgestelde maatregelen – een verbod of vergunningstelsel, een verplichting sleutels te deponeren of een verplichting voor verdachten om te ontsleutelen – onredelijk ingrijpend en ineffectief zouden zijn, terwijl er de nodige alternatieve opsporingsbevoegdheden waren om via een andere weg aan bewijsmateriaal te komen.[8] Mocht versleuteling in de praktijk een serieus probleem gaan worden, dan leek een ontsleutelplicht voor verdachten nog de minst slechte optie, aangezien dit de meest toegespitste oplossing is voor het probleem. Dit bracht mij ertoe om aansluitend nog nader te onderzoeken onder welke voorwaarden een ontsleutelplicht voor verdachten eventueel zou kunnen worden ingevoerd, mede in het licht van het nemo-tenetur-beginsel. Dat onderzoek leidde in 2000 tot de publicatie *Verdachte en ontsleutelplicht: hoe ver reikt nemo tenetur?*[9] In dat onderzoek stond de volgende vraag centraal:

> 'In hoeverre is een ontsleutelbevel aan verdachten verenigbaar met het nemotenetur-beginsel? Welke sanctie zou er kunnen en moeten staan op niet-naleving van het bevel, in aanmerking genomen dat het bevel de fundamentele rechten van de verdachte op een eerlijk proces niet onevenredig mag schaden, terwijl de sanctiedreiging de adressanten wel dient aan te zetten tot naleving ervan?'

Deze vraag werd beantwoord aan de hand van zeven aspecten. Ik geef hier de belangrijkste elementen van de analyse weer:[10]

1 Probleemschets

Cryptografie bemoeilijkt de opsporing, met name telefoontap en computeronderzoeken. Een ontsleutelplicht voor verdachten is een van de mogelijke 'oplossingen' voor dit probleem en moet daarom worden afgewogen tegen (of naast) de andere 'oplossingen' (verplichte of vrijwillige sleutelherwinning inbouwen; alternatieve opsporingsmethoden).

De bevindingen van de probleemschets suggereerden dat de specifieke omstandigheden van de cryptocontroverse weliswaar tot de specifieke bevoegdheid van een ontsleutelplicht voor verdachten kunnen nopen, te meer daar de alternatieven om het probleem aan te pakken minder wenselijk waren, maar dat de ernst en aard van het probleem vooralsnog geen gewichtige redenen leken te vormen voor een inbreuk op een rechtsbeginsel. Die

8 Koops 1999, p. 12.
9 Koops 2000.
10 Ibid., p. 91–99.

ernst en aard van het probleem zouden eerst beter in kaart moeten worden gebracht.

2 De internationale context

De internationale context liet zien dat de cryptocontroverse in vele landen speelde, waarbij een ontwikkeling gaande was van sleuteldepotmechanismen naar een ontsleutelplicht, al dan niet voor verdachten. Tot dusver waren er echter geen landen die een ontsleutelplicht voor verdachten hadden ingevoerd. Wel was in het VK daarvoor een voorstel gedaan, dat echter sterke weerstand had opgeroepen.
De internationale context suggereerde dat een ontsleutelplicht voor verdachten – vooralsnog – een bevoegdheid was die men in het buitenland niet kende. Dit gaf voor de wetgever in elk geval geen aanleiding om zich af te vragen waarom Nederland nog niet zo'n bevoegdheid had.

3 De reikwijdte van de toenmalige bevoegdheden

Bij het oordeel of een nieuwe bevoegdheid nodig is, moeten vanzelfsprekend de bestaande bevoegdheden beschouwd worden op hun effectiviteit. Naarmate deze minder geschikt zijn om het probleem aan te pakken, is een nieuwe bevoegdheid meer aangewezen. De volgende bestaande bevoegdheden waren hier relevant:

– De *ontsleutelplicht voor niet-verdachten*. Deze was nauwelijks effectief in het *commune* strafrecht. In het *bijzondere* strafrecht bestonden echter meer mogelijkheden voor een ontsleutelbevel.
– De mogelijkheden van de politie om versleutelde berichten te *kraken*. Deze zijn sterk afhankelijk van de gebruikte cryptografie en de zorgvuldigheid van de versleutelaar. Sommige programma's waren makkelijk kraakbaar, terwijl bij robuuste programma's ook korte sleutels goed te kraken waren. Er waren echter genoeg cryptoprogramma's beschikbaar via het internet, zoals PGP, waarmee de gebruiker lange sleutels kon genereren die alleen in honderden jaren te kraken waren.
  De politie had echter niet de meeste kans om het versleutelde bestand zelf te kraken, maar om het *wachtwoord* te vinden (neergeschreven op een geheugensteunpapiertje) of te *raden*. Men kan zich voorstellen dat berekenende misdadigers in het algemeen betere – moeilijker te raden – wachtwoorden kiezen, maar mij was niet bekend of dit in de praktijk steun vond. Ook hier gold dat een studie naar de cryptoproblemen in de praktijk een indicatie zou moeten geven.
– *Alternatieve opsporingsmethoden*. Met de Wet bijzondere opsporingsbevoegdheden was het arsenaal aan niet-klassieke opsporingsbevoegdheden gesystematiseerd en ook uitgebreid. Dit omvat bevoegdheden die niet door cryptografie worden gehinderd, zoals direct afluisteren en infiltratie. Dergelijke bevoegdheden konden tot op zekere hoogte een alternatief bieden voor de telefoontap en computeronderzoek als die door crypto-

gebruik geblokkeerd worden, maar ze waren aanzienlijk minder praktisch en leverden veelal andersoortige informatie op.

De toenmalige opsporingsbevoegdheden suggereerden dat de politie tot op zekere hoogte methoden had om cryptoproblemen aan te pakken. Wélke hoogte was moeilijk te zeggen, zonder inzicht in de aard en omvang van de cryptoproblemen in de praktijk.

4 De reikwijdte en achtergrond van nemo tenetur

Het nemo-teneturbeginsel is een essentieel onderdeel van het recht op een eerlijk proces (art. 6 EVRM), zo bleek uit het *Funke*-arrest. Iemand kan niet onder dwang van herhaalde boetes worden verplicht om bankafschriften uit te leveren, in elk geval niet als de overheid niet precies weet om welke bankrekeningen het überhaupt gaat. Uit het *Saunders*-arrest bleek dat iemand wel kon worden verplicht om mee te werken met de overheid zolang hij geen verdachte was, maar dat verklaringen die in een voorfase zijn afgelegd niet altijd in een latere rechtszaak tegen deze persoon mochten worden gebruikt. Uit dit arrest bleek ook dat het nemo-teneturbeginsel dicht aanligt tegen het zwijgrecht en vooral beschermt tegen het gedwongen afleggen van verklaringen; medewerking om fysiek bewijs te verzamelen, zoals een bloedproef, mocht wel worden afgedwongen.

Hoewel deze arresten vormgaven aan het nemo-teneturbeginsel, waren ze casusspecifiek en was het moeilijk om te zeggen wat het nemo-teneturbeginsel nu precies inhoudt; daarvoor is het een te complex beginsel. Duidelijk was wel dat de harde kern bestaat uit de verklaringsvrijheid, waar het beginsel een bijna absolute werking heeft. Ook bij vormen van actieve medewerking (zoals het uitleveren van documenten) heeft het beginsel vaak een sterke werking, terwijl het bij afgedwongen duldplichten (bijvoorbeeld een bloedproef of stemproef) een zwakke werking heeft.

De achtergrond van het nemo-teneturbeginsel leek gelegen in een samenstel van vier ratio's; afhankelijk van de vorm van medewerking speelde soms de ene en dan weer de andere ratio een grotere rol. De procesautonomie en de menselijke waardigheid betekenden dat de verdachte als autonome procespartij zijn eigen houding moet kunnen bepalen; daarbij past het in beginsel niet de verdachte als onderzoeksvoorwerp te zien en hem zelf bewijs op tafel te laten leggen. Daarnaast stelden ook het pressieverbod en de betrouwbaarheid van resulterend bewijsmateriaal grenzen aan de medewerking die van verdachten kan worden verlangd. Deze aspecten verklaarden waarom nemo tenetur sterker werkt bij afgedwongen actieve medewerking en vooral bij verklaringen: naarmate de verdachte zelf meer moet doen en vooral wanneer hij zijn geest moet gebruiken, is het bewijsmateriaal meer afhankelijk van zijn wil om mee te werken en bestaat er meer kans dat hij het manipuleert.

Nemo tenetur werkt bovendien op twee niveaus: het is een beginsel dat de wetgever moet afwegen tegen andere belangen, en het is een beginsel voor de rechter bij de selectie en waardering van het bewijs.

Voor de ontsleutelplicht had dit tot gevolg dat de wetgever in de afweging om een ontsleutelplicht voor verdachten in te voeren een zwaar gewicht moest toekennen aan het nemo-teneturbeginsel. De ontsleutelplicht betreft immers een vorm van actieve medewerking, die dichtbij het afleggen van een verklaring in de buurt komt als de verdachte zijn wachtwoord moet geven en de politie niet zeker weet dat de verdachte het wachtwoord (of de sleutel) kent – in die gevallen brengt het vertellen van het wachtwoord immers de verklaring met zich mee dat de verdachte over het wachtwoord beschikte. Aangezien in de meeste gevallen er geen zekerheid of hoge mate van waarschijnlijkheid bestaat dat de verdachte in staat is te ontsleutelen, zou een ontsleutelplicht meestal de verklaringsvrijheid raken. De wetgever moest daarom zeer zwaarwegende belangen aanvoeren om toch een ontsleutelplicht voor verdachten in te voeren.

5 Het systeem van de wet en toenmalige inbreuken

Het commune strafrecht kende feitelijk geen actieve medewerkingsplichten of verklaringsplichten voor verdachten. Soms kunnen bevelen tot medewerken of verklaren wel tot hen worden gericht, maar dan kunnen zij zich verschonen van medewerking zonder dreiging van een sanctie. In het bijzondere strafrecht (sectorale wetgeving zoals het belasting-, milieu- of verkeersstrafrecht) bestonden meer inbreuken op de kern van het nemo-teneturbeginsel: in bepaalde gevallen worden ook verdachten gedwongen actief mee te werken of zelfs te verklaren. De reden daarvoor is dat sectorale wetgeving anders moeilijk te handhaven zou zijn; het gaat vrijwel steeds om situaties waarin er geen of nauwelijks alternatieven zijn om de noodzakelijke gegevens te verkrijgen. Bovendien betreft het wetten met een beperkt bereik (van personen en situaties) en gaat het om een beperkte sanctiedreiging (bijna nooit hoger dan drie maanden gevangenisstraf).

Het systeem van de wet suggereerde dat een ontsleutelplicht voor verdachten (een actieve medewerking op de grens van een verklaring) in het commune strafrecht een unieke bevoegdheid zou zijn; de wetgever moest dus zeer zwaarwichtige redenen hebben om zo'n bevoegdheid in te voeren. In bijzondere wetgeving zou een ontsleutelplicht voor verdachten mogelijk beter passen.

6 Handhavingsperikelen

Een wettelijke ontsleutelplicht voor verdachten zou alleen zinvol zijn als er enige druk bestaat om mee te werken – anders kan de politie het ook gewoon vriendelijk vragen. Er moet dus een sanctie staan op niet-medewerking. Dit gaat echter alleen op voor de opzettelijke weigering om mee te werken; anders zou er een onwenselijke risicoaansprakelijkheid op cryptogebruik worden gezet.

Voor de oplegging van een sanctie op opzettelijke niet-medewerking zou het Openbaar Ministerie (OM) aannemelijk moeten maken dat de verdachte in

staat was te ontsleutelen – anders was zijn weigering immers niet opzettelijk. Hier nu zouden grote bewijsproblemen ontstaan. Weliswaar kan het OM diverse ervaringsregels en omstandigheden aanvoeren waarom een verdachte in staat zou zijn te ontsleutelen, maar daartegenover heeft de verdachte een keur aan verweren om aannemelijk te maken dat hij daadwerkelijk niet kon ontsleutelen. Deze veelal technische verweren zouden moeilijk te weerleggen zijn. Bovendien kunnen berekenende misdadigers voorzorgsmaatregelen treffen die hun verweer ondersteunen. Bij niet-berekenende misdadigers zou een vergeetverweer ('Oeps, wachtwoord vergeten…!') vaak slagen, terwijl bij berekenende misdadigers allerlei verweren kansrijk zouden zijn.
Er zou dus weinig dreiging uitgaan van een sanctie op niet-medewerking. Dit kon ook niet als argument gelden om daarom maar zware straffen te zetten op niet-medewerking, omdat daarbij (nog) hogere bewijseisen aan het opzet – en dus het in staat zijn te ontsleutelen – worden gesteld en het onmogelijk zou worden voor het OM om iemand voor decryptieweigering te veroordelen. De handhavingsperikelen suggereerden dat een ontsleutelplicht voor verdachten in de praktijk weinig effectief zou zijn. Een hoge sanctie op niet-medewerking, laat staan een omkering van de bewijslast in de hoofdzaak, moest worden afgewezen, en een lage sanctie had minder kans het beoogde effect – daadwerkelijke ontsleuteling van verdachte bestanden – te bereiken.

7 Opties voor een ontsleutelplicht

Als de theoretisch mogelijke opties voor een ontsleutelplicht, met verschillende modaliteiten van hoe een bevel tot meewerking wordt gegeven en welke sanctie op niet-medewerking staat, opnieuw werden bekeken, dan bleken de meeste opties niet realistisch. De uitgezette lijnen toonden aan dat de verdergaande opties voor een ontsleutelplicht voor verdachten (waarbij het resultaat voor het bewijs kan worden gebruikt) een ernstige inbreuk op het nemo-teneturbeginsel maakten, en dat er zeer zwaarwichtige redenen moesten zijn om zo'n inbreuk te rechtvaardigen.
Die redenen konden alleen worden gevonden in de bijzonderheid en de ernst en omvang van de problematiek. De bijzonderheid van het probleem legde enig gewicht in de schaal: cryptografie is het eerste verschijnsel waarbij bewijsmateriaal dat op zich onafhankelijk van verdachtes wil bestaat alleen mét zijn medewerking kan worden gevonden, terwijl de alternatieven om het probleem aan te pakken onwenselijk waren vanwege zware inbreuk op andere grondrechten. Maar de aard en omvang van het probleem zouden zeer ernstig moeten zijn, wilden zij opwegen tegen de inbreuk op de kern van nemo tenetur en het systeem van de wet, en er waren geen afdoende gegevens dat het cryptoprobleem voor de opsporing ook maar in de buurt kwam van een dermate ernstig opsporingsprobleem. En zelfs al zouden er aanwijzingen zijn dat cryptografie in ernstige mate veel belangrijke opsporingsonderzoeken definitief zou belemmeren, dan nog zou een ontsleutelplicht

mank gaan aan gebrekkige effectiviteit vanwege de handhavingsproblemen. Waar een inbreuk op nemo tenetur nog te rechtvaardigen zou zijn door een uitermate ernstig opsporingsprobleem, dat alleen maar kan worden aangepakt door de bewuste medewerkingsplicht, zou die medewerkingsplicht in elk geval effectief moeten zijn om het probleem daadwerkelijk (in hoge mate) op te lossen. Bij cryptografie was die effectiviteit twijfelachtig, en daar zou – bij de toenmalige stand van de techniek en cryptogebruik – niets aan te doen zijn. Het viel ook niet te verwachten dat dat in de toekomst anders zou worden. Als er al een ontwikkeling zou plaatsvinden dat cryptogebruikers waarschijnlijker dan destijds in staat zouden zijn te ontsleutelen, zouden er tegelijkertijd meer cryptosystemen worden ontwikkeld waarbij de gebruiker juist waarschijnlijk niet in staat zou zijn te ontsleutelen op bevel – een ontwikkeling die men destijds reeds kon waarnemen.
De conclusie moest zijn dat in het commune strafrecht voor een afgedwongen ontsleutelplicht voor verdachten geen plaats was. De enige optie die nemo tenetur open liet, was om de toenmalige bepaling van artikel 125m lid 1 Sv, dat het ontsleutelbevel niet aan de verdachte werd gegeven, te wijzigen in een verschoningsrecht, met bijpassende cautie, voor verdachten. In de praktijk zou deze constructie weinig uitmaken, ook al kon dit misschien het systeem van de wet verhogen. In het bijzondere strafrecht zou de wetgever iets meer speelruimte hebben in een belangenafweging om een zwaardere optie te kiezen, maar ook daar ging een afgedwongen ontsleutelplicht voor verdachten waarschijnlijk mank aan gebrek aan effectiviteit.

Op basis van bovenstaande analyse concludeerde het rapport uit 2000 dat een onder strafdreiging afgedwongen ontsleutelplicht voor verdachten inbreuk maakte op het nemo-teneturbeginsel en dat voor een dergelijke inbreuk onvoldoende rechtvaardigingsgronden waren aan te voeren. Het rapport bood echter wel een opening voor een andere conclusie in de toekomst:

> ‘De aanbeveling voor de wetgever is daarom om geen ontsleutelplicht voor verdachten in te voeren. Omdat dit echter het probleem niet oplost, is het denkbaar dat de discussie over een ontsleutelplicht aan verdachten weer naar boven zal komen, telkens als een aflevering in de wetgevingsserie Computercriminaliteit wordt gelanceerd. De wetgever zal dus alert moeten blijven op de ontwikkelingen, en hij zal periodiek de afweging moeten maken tussen niets doen, een ontsleutelplicht voor verdachten en andere methoden om het probleem te verlichten. Vanwege de gebrekkige effectiviteit van een ontsleutelplicht, waar weinig aan te doen is, lijkt het onwaarschijnlijk dat de wetgever in de toekomst wel zal moeten besluiten tot een dergelijke bevoegdheid, maar de alternatieven (verplichte BEDOT-systemen [die een achterdeur voor de overheid bevatten] of vergaande alternatieve opsporingsmethoden) zijn ook onaantrekkelijk

> in het licht van grondrechten, terwijl ook niets doen zijn grenzen kan hebben. De wetgever zal dus steeds moeten kiezen uit het minste van drie of vier kwaden.'[11]

De vraag die nu voorligt is of de omstandigheden sinds 2000 dusdanig zijn veranderd dat een andere conclusie gerechtvaardigd is. De volgende hoofdstukken behandelen diverse ontwikkelingen die de verschillende aspecten uit de analyse van 2000 in een potentieel ander licht plaatsen. Het betreft veranderingen in de techniek en het gebruik van cryptografie door misdadigers (hoofdstuk 3; aspecten 1, 3 en 6); ontwikkelingen in de Europese rechtspraak rond nemo tenetur (hoofdstuk 4; aspect 4); ontwikkelingen in het Nederlandse recht en in diverse andere landen (hoofdstuk 5; aspecten 2, 3 en 5). In het slothoofdstuk worden de factoren opnieuw gewaardeerd in het licht van de vraag of een ontsleutelplicht voor verdachten inmiddels wel als verenigbaar met het nemo-teneturbeginsel kan worden beschouwd (hoofdstuk 6; aspect 7).

11 Ibid., p. 102.

3 Ontwikkelingen in cryptografie en cryptogebruik

3.1 Het gebruik van cryptografie door verdachten

In 2000 constateerde ik dat misdadigers in de praktijk cryptografie gebruiken, maar dat dat vooralsnog beperkt leek te blijven tot enkele (georganiseerde of computerdeskundige) boeven, die het vooral toepassen op opgeslagen gegevens en niet op communicatie, terwijl deze zaken uiteindelijk niet stukliepen op versleutelde gegevens omdat er genoeg ander bewijs was of omdat de misdadiger zijn wachtwoord had opgeschreven of slechte crypto had gebruikt.[12] Inmiddels ligt dat iets anders. 'Encryptie komt veel meer voor en is onkraakbaarder geworden.'[13]
Er zijn grofweg twee situaties waarin opsporing kan stuiten op door een verdachte versleutelde gegevens, samenhangend met de toepassing van verschillende opsporingsbevoegdheden: het kan gaan om opgeslagen gegevens (meestal vergaard via doorzoeking en inbeslagneming van gegevensdragers) of om gegevens die onderweg zijn en die via een tap worden vergaard.

3.1.1 Opgeslagen gegevens

Bij opgeslagen gegevens komt de opsporing vaker encryptie tegen, veelal in kinderpornozaken.[14]

> 'Een jaar of vijf, zeven geleden zag je bijna nooit iets. Nu zie je overal TrueCrypt of BestCrypt. Iedereen gebruikt het ook, het is eerder regel dan uitzondering.
>
> De meeste verdachten bekennen overigens gewoon dat ze kinderporno in het bezit hebben, alleen willen ze vaak niet de inhoud van bestanden laten zien omdat dat altijd tegen hen werkt. (Bijvoorbeeld omdat het dan blijkt dat het gaat om jonge kinderen of heel veel materiaal.)
>
> We hebben eigenlijk nog nooit een zaak gezien waarbij echt helemaal niets te bewijzen was. Het zou best kunnen dat die ooit gaan voorkomen. Tot op heden hebben we altijd wel een deel van het bewijs (door minder goed beveiligde containers, slordigheden in beveiliging of gewoon grif bekennende verdachten), maar het is de vraag of dit zo blijft.'[15]

Of cryptografie nu op redelijk grote schaal of systematisch wordt gebruikt door misdadigers en of dat een substantieel opsporingsprobleem oplevert, is

12 Ibid., p. 10-11.
13 Interview officier van justitie.
14 Interview officier van justitie, interview onderzoeksrechter België, Nationaal Rapporteur Mensenhandel 2011, p. 61.
15 Interview officier van justitie.

de vraag. In Engeland en Wales lijkt er niet direct een significante toename te zijn van cryptogebruik, ondanks de brede beschikbaarheid van programma's via internet.[16] Ook in de VS nemen misdadigers tot nu toe meestal niet de moeite hun harde schijf te versleutelen, met uitzondering van cybermisdadigers.[17]
Op grond van geluiden uit de opsporingspraktijk is mijn indruk dat encryptie in de afgelopen jaren steeds meer wordt aangetroffen in opsporingsonderzoeken en dat het vaker voorkomt dat de encryptie niet te doorbreken valt omdat de gebruiker zorgvuldig met de versleuteling is omgegaan. Dit komt het meeste voor in kinderpornonetwerken, waarbinnen gebruikers vaak zeer bewust proberen hun communicatie en gegevensopslag op robuuste wijze te versleutelen.

> 'Fans van kinderporno die actief zijn in het grootschalig maken en uitwisselen van kinderporno zijn early adapters, ze zijn al jaren bezig met versleuteling. Men maakt in ruime mate gebruik van encryptie, en loopt daarbij voor op gemiddelde gebruikers. Misschien verdwijnt het onderscheid over 5-10 jaar en is dit encryptiegebruik dan niet karakteristiek meer voor deze specifieke groep. Je moet het breder bekijken dus.'[18]

3.1.2 Afgetapte gegevens

Bij aftappen stuit de politie vaker op encryptie, wat het onderscheppen van communicatie steeds moeilijker maakt.[19] Het gaat daarbij echter niet om versleuteling toegepast door eindgebruikers zelf (waaronder verdachten) maar om versleuteling door dienstaanbieders, met name bij VoIP-diensten (internettelefonie)[20] maar ook bij gratis e-maildiensten.[21] Dit levert vooral problemen op wanneer de aanbieders in het buitenland zijn gevestigd en niet onder de Telecommunicatiewet vallen.[22] Een ontsleutelplicht voor verdachten is evenwel niet relevant voor dit type encryptie, aangezien de verdachte zelf niet is betrokken bij de encryptie of decryptie van de communicatie.
Interessant vergelijkingsmateriaal om te beoordelen in hoeverre encryptie een probleem oplevert bij de tap, is te vinden in Amerikaanse statistieken; sinds 2000 wordt in de VS bijgehouden in hoeveel gevallen opsporingsdien-

16 Chatterjee 2011, p. 277 ('In sum, the increased availability of developed cryptography alone does not seem to translate into a significant increase in criminal instances of use. As the Head of the Metropolitan Police's Digital and Electronic Forensic Services has observed, only a 'handful' of cases are coming to light as many criminals – even serious ones – appear too complacent to use it').
17 Brenner 2011, p. 81 ('There are only a few cases involving defendants who took the additional step of encrypting their hard drives, and they involve cybercriminals rather than street criminals. It seems there are no reported cases, or anecdotal evidence, involving street criminals who made an effort to encrypt their cell phones (or computers)').
18 Interview officier van justitie.
19 Odinot et al. 2012, p. 30.
20 Ibid., p. 165-166.
21 Interview politie.
22 Nederlandse aanbieders zijn verplicht om hun eigen versleuteling ongedaan te maken als zij een tap faciliteren; als het gaat om via andere aanbieders getapte communicatie kan een aanbieder bevolen worden de communicatie te ontsleutelen op basis van art. 126m/t/zg lid 6 Sv.

sten encryptie tegenkomen bij een telefoon- of e-mailtap.[23] De rapporten van de Administrative Office of the United States Court vermelden de volgende aantallen (tabel 1):[24]

Tabel 1 Aantal encryptiegevallen in Amerikaanse tapzaken

	Aantal tapbevelen	Aantal tapzaken waarin encryptie voorkomt	Aantal gevallen waarin klare tekst niet kan worden achterhaald
2000	1.139	22	0
2001	1.405	16	0
2002	1.273	34	0
2003	1.367	1	0
2004	1.633	2	0
2005	1.694	13	0
2006	1.714	0	0
2007	2.119	0	0
2008	1.809	2	0
2009	1.764	1	0
2010	2.311	6	0
2011	2.189	12	0

Bron: Cijfers afkomstig van www.uscourts.gov/Statistics/WiretapReports.aspx

De rapporten vermelden niet hoe deze cijfers tot stand komen; men is afhankelijk van meldingen van de uitvoeringsinstanties. De afname van encryptie na 2002 zou veroorzaakt kunnen zijn door een daadwerkelijke afname van versleutelde communicatie, maar ook door een lagere bereidheid van diensten om encryptiegevallen te melden (bijvoorbeeld omdat de encryptie toch geen probleem opleverde, zodat de noodzaak van melding niet urgent is). Wat daar ook van zij, duidelijk is dat in de VS-tappraktijk versleuteling in het afgelopen decennium niet is toegenomen en in geen enkel geval een (onoverkomelijk) probleem voor de opsporing heeft opgeleverd. De rapporten constateren elke keer dat 'in none of these cases was encryption reported to have prevented law enforcement officials from obtaining the plain text of communications intercepted'.[25]

Dat in de VS, in tegenstelling tot in Nederland, encryptie nog steeds weinig wordt aangetroffen bij de tap, heeft wellicht als verklaring dat de VS-cijfers voor het overgrote deel betrekking hebben op de telefoontap (zowel vast als mobiel). In 2010 betroffen bijvoorbeeld slechts 16 van de 2.311 taps een 'electronic' tap (waaronder vallen digitaal, semafoon, fax en computer); in 2011 waren van de 2.189 taps er 4 elektronisch en 87 gecombineerd (dat wil zeggen een combinatie van telefoon, elektronisch en direct afluisteren).[26] De Nederlandse toename in versleutelde gegevens wordt hoofdzakelijk veroorzaakt door internettelefonie en betreft dus internettaps.

23 Dat is wettelijk verplicht op basis van 18 U.S.C. § 2519(2)(b).
24 Samengesteld uit de jaarlijkse Wiretap Reports, die beschikbaar zijn op www.uscourts.gov/Statistics/WiretapReports.aspx (geraadpleegd 1 september 2012).
25 Administrative Office of the United States Courts 2001, p. 5.
26 www.uscourts.gov/Statistics/WiretapReports.aspx (geraadpleegd 1 september 2012).

3.1.3 Perspectief

Waar bewust en robuust cryptogebruik nu nog voornamelijk voor lijkt te komen bij opgeslagen gegevens binnen kinderpornonetwerken, zou het in de toekomst een breder probleem kunnen worden. Kinderpornonetwerken bestaan uit 'early adapters', en andere groepen zouden iets later kunnen volgen in het gebruik van cryptografie. Anderzijds moet versleuteling door verdachten ook worden gezien in het bredere perspectief van andere technische uitdagingen voor de opsporing. Bijvoorbeeld het bestaan van 'kogelvrije' aanbieders die communicatie- en gegevensopslagdiensten aanbieden die toegang door derden, waaronder opsporingsdiensten, maximaal proberen tegen te houden en de ontwikkeling van cloud computing (waarbij je niet weet waar gegevens zijn opgeslagen) kunnen voor de opsporing grotere bedreigingen vormen dan versleutelde harde schijven die bij doorzoekingen worden aangetroffen.[27] Ook lijkt het probleem van versleuteling van communicatie door internettelefonieaanbieders die niet of niet makkelijk aanspreekbaar zijn voor de Nederlandse justitie, momenteel prangender dan cryptogebruik door verdachten zelf.[28]

3.2 De (on)kraakbaarheid van cryptografie

Op het gebied van kraken van cryptografie is er niet veel veranderd. De sterkte van cryptografie is gebaseerd op de sleutellengte: wanneer een lang genoege sleutel wordt gebruikt, is de cryptografie in eeuwen niet te kraken.[29] Volstrekt onkraakbare sleutellengtes van 256 bits zijn inmiddels geen uitzondering meer (bijvoorbeeld AES-256). Weliswaar volgt de rekencapaciteit nog steeds grofweg de Wet van Moore (elke twee jaar verdubbelt de rekencapaciteit van een computerchip), maar dat maakt weinig uit voor het kraken van sterke cryptografie. Sommigen denken dat cloud computing, waarbij infrastructuur op afstand ingekocht kan worden voor onder andere grote rekenklussen, perspectieven biedt voor het kraken van versleuteling.[30] Dat biedt echter slechts een gradueel verschil – het zou ingezet kunnen worden om één bepaald bestand te kraken en daarbij dan een schaalvoordeel bieden, maar het kraken duurt dan nog steeds weken of maanden, zodat het niet bruikbaar is voor substantiële aantallen versleutelde bestanden. In de huidige situatie

27 Vgl. hierover Koops et al. 2012 (te verschijnen).
28 Ibid.
29 '[W]anneer bijvoorbeeld een verdachte met een container kinderporno – dat is een computerbestand met tienduizenden foto's – via een encryptieprogramma verstuurd [sic], dan zit daar een versleuteling op die met de huidige technologie met 10.000 computers in geen 10.000 jaar te breken is!' Aldus Frans Kolkman, geciteerd in *Allround Politie Nieuws* april 2012, p. 23.
30 Zie Koops et al. 2012 (te verschijnen).

lukt het justitie soms ook om sterke cryptografie te kraken als er maar genoeg rekencapaciteit wordt ingezet.[31]
Een radicale ontwikkeling valt alleen te voorzien bij quantumcomputers, die door gebruik te maken van quantumeffecten van elektronen of fotonen een exponentieel grotere rekencapaciteit hebben dan de huidige elektronische computers.[32] Quantumcomputers hebben zich weliswaar flink ontwikkeld sinds 2000, maar een doorbraak laat nog op zich wachten en een realisatie in de praktijk valt op de korte of middellange termijn niet te verwachten. (Bovendien zal justitie dan wel andere problemen aan het hoofd hebben dan cryptogebruik door verdachten: quantumcomputers bieden een goudmijn voor de misdaad omdat daarmee ook het versleutelde bankverkeer en staats- en bedrijfsgeheimen te kraken zijn.)
Het kraken van cryptografie komt daarom nog steeds neer op het gebruik maken van zwaktes in het cryptogebruik door de verdachte, in plaats van een programma te laten draaien dat alle sleutels uitprobeert. De sleutel wordt opgeslagen op de harde schijf en beveiligd met een wachtwoord. Verdachten in kinderpornozaken blijken vaak slordig om te gaan met hun wachtwoorden: die worden in een boekje opgeschreven of de systematiek ervan is makkelijk te raden of uit te proberen.[33] Ook daarin lijkt (nog) niet veel veranderd sinds 2000.
Mogelijk zit er wel een verschil tussen het kraken van versleutelde bestanden en het doorbreken van de beveiliging van een computer. Computers die met wachtwoorden beveiligd zijn, worden regelmatig gekraakt; bepaalde schermbeveiligers en sommige smartphones zijn echter weer moeilijker kraakbaar.[34] Brenner stelt dat 'an increased use of encryption and other data-protection measures will make it increasingly difficult, if not impossible, for officers to access a cell phone's contents'.[35] Ook hiervoor geldt dat een slordige omgang met wachtwoorden door de gebruiker kan helpen om toch toegang te krijgen.

3.3 De opkomst van TrueCrypt als contramethode

Naast de slordige omgang met wachtwoorden die veel verdachten nog blijken te vertonen, staat echter een ontwikkeling van zeer bewuste omgang met cryptografie. Dit komt (vooralsnog) voornamelijk voor binnen bepaalde netwerken van kinderpornogebruikers en -verspreiders. Het wordt gefaciliteerd

31 In de Amstelveense zedenzaak wist het NFI bijvoorbeeld een versleuteld deel van de harde schijf van verdachte te kraken, waarbij 66 filmbestanden en 244 afbeeldingen van kinderpornografische aard naar voren kwamen (Rb. Amsterdam 23 juli 2012, LJN BX2326). Vgl. de zaak-*Rajib Karim*, waarin 'a former British Airways worker was arrested by counter terrorism officers. Police encountered what was described as an "encryption fortress" on Karim's laptop and external hard drive. A programme called "Windows Washer" had also been used to delete electronic traces. Despite the encryption in *Karim* being the most sophisticated yet encountered by the Intelligence services, they did manage to decrypt the files and a thirty year sentence for planning terrorism was achieved', Chatterjee 2011, p. 282.
32 Zie http://nl.wikipedia.org/wiki/Kwantumcomputer (geraadpleegd 1 september 2012).
33 Interview officier van justitie.
34 Interview politie.
35 Brenner 2011, p. 82.

door programma's en handleidingen die precies uitleggen hoe je op een onkraakbare manier cryptografie kunt gebruiken. Zo zijn er webpagina's die gebruikers

> 'stap voor stap meenemen in het gebruik van particuliere encryptiesoftware. Binnen een groep waarin mensen actief worden aangespoord om vooral van dit soort technieken gebruik te maken, is het niet gek dat er inderdaad mensen zijn die dat soort dingen willen uitleggen. Overigens heeft ook TrueCrypt een uigebreide handleiding en FAQ die het zelfs voor de digibeet nog uitleggen.'[36]

TrueCrypt is een programma dat steeds terugkeert, niet alleen in opsporingsonderzoeken maar ook in discussies over cryptografie en een eventuele ontsleutelplicht.[37] Het is een contramethode die valt binnen de brede categorie 'anti-forensics', oftewel 'research and developments dedicated to the idea of manipulating data to undermine the reliability of digital forensic investigations'.[38] TrueCrypt is een gratis, *open source*-programma waarmee je zogeheten 'containers' op je harde schijf aanmaakt, waarin een grote hoeveelheid bestanden versleuteld kunnen worden opgeslagen.[39] Het grootste probleem voor de opsporing is dat je met TrueCrypt binnen een container een nieuwe container kunt aanmaken.

> 'Daarnaast heb je het probleem van een container in een container, bij TrueCrypt en Bestcrypt bijvoorbeeld. De verdachte geeft zijn eerste password, en als je dan denkt dat er een tweede container in zit (wat je niet kunt zien) en om het password daarvan zou vragen, zegt hij: "hoezo tweede password, ik heb mijn password toch al gegeven?" Daar kun je niets mee. Technisch ziet het eruit als een bulk spaghetti, je kunt niet hardmaken dat in die tweede container nog relevant materiaal zit.'[40]

> 'We zijn vaker tegengekomen dat verdachten TrueCrypt gebruiken. TrueCrypt is wel het meest gangbare encryptieprogramma. Het is vrijwel onkraakbaar als je het goed gebruikt. Ze adviseren elkaar op internet het ook te gebruiken. Je hebt dan te maken met containers in containers in containers. Verdachten kunnen dan een sleutel geven die de eerste container opent, en daarin zie je dan misschien wat oninteressante bestanden en verder niets van de onderliggende containers. Wat doe je dan? We zijn al meermalen tegen het probleem aangelopen dat we denken dat er verborgen containers op een schijf staan, maar dat niet kunnen aantonen. Het is voor verdachten niet moeilijk die te verstoppen, zodat je ook nooit

36 Interview officier van justitie.
37 Zie onder andere Behr 2008, Diehl 2008, Palfreyman 2009, Paredes 2009, Chatterjee 2011.
38 Behr 2008, p. 10.
39 Zie www.truecrypt.org/ (geraadpleegd 1 september 2012).
40 Interview politie.

kunt zeggen dat iemand niet meewerkt aan het geven van een wachtwoord van een container waarvan je niet kunt bewijzen dat die er is.'[41]

Dat je niet kunt zien of er binnen een container nog meer versleuteld materiaal (in een subcontainer) staat, komt doordat TrueCrypt de niet-gebruikte ruime vult met willekeurige bits. Versleutelde bestanden zien er (bij robuuste crypto) ook uit als willekeurige bits.[42] Het is voor een forensisch onderzoeker dan moeilijk om met voldoende zekerheid een onderscheid te maken tussen delen van de harde schijf die versleuteld zijn en delen die leeg zijn (vgl. de zaak-*John Doe* in paragraaf 6.4.6). Dat wil niet zeggen dat bij dit soort cryptografie helemaal niets meer mogelijk is – soms kan bij versleutelde bestanden worden gezocht aan de hand van bestandsnamen en de namen van verzamelde series, bezochte websites of de namen van slachtoffers (de mappen waarin dat materiaal zit zijn vaak vernoemd naar series of slachtoffers).[43] Ook zijn er programma's als TCHunt die in staat zijn om op een harde schijf te zoeken naar (mogelijk) versleutelde volumes; ze kunnen daarbij echter geen onderscheid maken tussen versleutelde schijfruimte en schijfruimte die TrueCrypt met willekeurige data heeft overschreven.[44]
Door antiforensische programma's als TrueCrypt wordt het een stuk moeilijker om een versleuteld bestand te identificeren. Deze programma's faciliteren aldus 'plausible deniability', dat wil zeggen dat ze het mogelijk maken voor de gebruiker om, met een redelijke mate van aannemelijkheid, het bestaan van het versleutelde bestand te ontkennen.[45]

3.4 De (on)aannemelijkheid van vergeetachtigheid

In 2000 was een van mijn belangrijkste argumenten tegen een ontsleutelplicht voor verdachten dat het zeer moeilijk aannemelijk te maken is dat iemand in staat is te ontsleutelen, wanneer de verdachte stelt het wachtwoord te zijn vergeten. Zo'n vergeetverweer is redelijk plausibel – immers, ook verdachten is niets menselijks vreemd – om in elk geval voldoende twijfel te zaaien om door de rechter niet te worden veroordeeld voor opzettelijke decryptieweigering.[46]
Inmiddels hebben het ICT-gebruik van verdachten en de opsporingspraktijk zich echter dusdanig ontwikkeld dat ik nu de handhaafbaarheid van een (onder strafbedreiging afgedwongen) ontsleutelplicht positiever inschat. Dat komt omdat verdachten – bijvoorbeeld in kinderpornozaken – inmiddels

41 Interview officier van justitie.
42 Anders is via patroonherkenning de cryptografie makkelijker te kraken. Het is daarom een ontwerpvereiste van cryptosystemen dat de versleutelde tekst dezelfde eigenschappen heeft als willekeurige getallen.
43 Interview officier van justitie.
44 Zie http://16s.us/TCHunt/faq/ (geraadpleegd 1 september 2012).
45 Zie www.truecrypt.org/docs/?s=plausible-deniability (geraadpleegd 1 september 2012). Zie ook de in noot 37 genoemde literatuur.
46 Zie Koops 2000, p. 79-90, 97. Vgl. de maatstaf die in de Britse regeling wordt gehanteerd voor de aannemelijkheid dat verdachte in staat is te ontsleutelen (zie paragraaf 6.3.1).

vaak langdurig of regelmatig online zijn, waarbij hun internetgedrag via een internettap kan worden gevolgd. Als de hele harde schijf van de verdachte versleuteld is, terwijl hij – blijkens de tap – wel elke dag zijn computer gebruikt, is dat een sterke aanwijzing dat de verdachte toegang heeft tot de harde schijf.[47] Ook kan uit een tap blijken dat een verdachte op bepaalde dagen grote hoeveelheden data binnenhaalt. Wanneer justitie bij een doorzoeking dan de computer van verdachte onderzoekt maar geen gegevens kan vinden van computeractiviteit op de dagen waarin via de tap grote computeractiviteit is geconstateerd, dan is dat een sterke aanwijzing dat er iets verborgen wordt gehouden. Ook komt het voor dat een verdachte naast zijn gewone computer nog vijftien externe harde schijven heeft met een capaciteit van 1 Terabyte; als op die schijven TrueCrypt is gebruikt en de schijven leeg lijken – of na ontsleuteling door de behulpzame verdachte slechts een beperkte omvang aan plaatjes van Anna Kournikova tevoorschijn komt – dan zal de verdachte toch moeten uitleggen waarom hij zoveel opslagcapaciteit in huis heeft die hij niet gebruikt.[48] In de casus van John Doe, waarin het hof oordeelde dat niet voldoende aannemelijk was gemaakt dat er versleutelde bestanden in TrueCrypt-containers stonden (paragraaf 6.4.6), valt misschien ook te betogen dat er toch voldoende bewijs was dat er versleutelde kinderpornografie op de harde schijven stond, omdat onomstreden was dat er kinderporno was binnengehaald vanaf drie IP-adressen van hotelkamers waar Doe verbleef, en er buiten de inbeslagggenomen computers geen andere gegevensdrager was die Doe kon hebben gebruikt.[49]
Nu biedt dit soort informatie als zodanig geen afdoende bewijs dat verdachte ontsleuteling heeft gebruikt en in staat is te ontsleutelen. Het draagt echter wel bij aan het gehele plaatje. In combinatie met ander ondersteunend bewijsmateriaal kan dan toch een dusdanig beeld ontstaan dat de verdachte iets aan het verbergen is. En nu het vrij eenvoudig (via een internettap of via metadata in een onderzochte computer) aan te tonen is dat een verdachte nog zeer recent – gisteren of vanmorgen – zijn computer heeft gebruikt, kan ook de bewijsvoeringslast of de verdachte in staat is te ontsleutelen in bepaalde gevallen (wanneer er *prima facie* bewijs is dat de verdachte zeer recent zijn computer of cryptosleutel heeft gebruikt) weer bij de verdachte worden neergelegd (vergelijk de *John Murray*-zaak, zie paragraaf 4.1.3).
De rechtspraak in de Verenigde Staten (zie paragraaf 6.4) toont aan dat een zinvolle discussie in de rechtszaal mogelijk is (die dan overigens wel goed gevoerd moet worden door justitie en verdediging) over de vraag of de verdachte in staat is te ontsleutelen. In lang niet alle gevallen zal het voldoende aannemelijk gemaakt kunnen worden dat de verdachte daadwerkelijk in staat

47 Interview politie.
48 Interview officier van justitie.
49 Aldus betoogt Sean Harrington in zijn commentaar op *United States* v *Doe*, zie 'Eleventh Circuit Rules Defendant Cannot Be Compelled to Divulge Encryption Password', http://mntech.typepad.com/msba/2012/02/eleventh-circuit-rules-defendant-cannot-be-compelled-to-divulge-encryption-password.html (26 February 2012) (geraadpleegd 1 september 2012).

is te ontsleutelen, maar er zijn ook genoeg gevallen denkbaar waarin dat wel zo is. Het argument van de gebrekkige handhaafbaarheid vanwege het 'vergeetverweer' van verdachte acht ik daarom minder sterk dan in 2000. De vraag of een verdachte wel of niet in staat moet worden geacht te ontsleutelen is een vraag die zich goed leent voor casuïstische rechtsontwikkeling (zie paragraaf 6.4).

3.5 Het risico van averechtse crypto-ontwikkeling

De vorige paragrafen beschreven in zekere zin tegengestelde bewegingen. Aan de ene kant maken verdachten bewuster gebruik van antiforensische technieken, in het bijzonder van programma's als TrueCrypt die 'aannemelijke ontkenbaarheid' bieden. Aan de andere kant heeft justitie ook mogelijkheden om argumenten aan te dragen om voldoende aannemelijk te maken dat de verdachte in staat is bepaalde gegevens toegankelijk te maken. Of iemand kan worden veroordeeld voor een weigering te ontsleutelen, komt dan neer op een beoordeling van de argumenten van beide kanten. Dat is typisch iets wat gebeurt in rechtszaken, en zou dus goed overgelaten kunnen worden aan de rechter.
Diverse bronnen wijzen echter op het gevaar dat, als de wetgever een ontsleutelplicht voor verdachten invoert, een nieuwe wapenwedloop ontstaat – of de nu al bestaande wapenwedloop verergert – tussen misdadigers en justitie rond cryptografiegebruik.

> 'Het bedrijfsmodel van bedrijven als Bestcrypt is er ook op gebaseerd dat ze iets aanbieden waarmee je materiaal uit handen van de politie kunt houden. Als wij een tegenactie verzinnen, passen zij hun product weer aan.'[50]

In het Verenigd Koninkrijk is bij invoering van de ontsleutelplicht ook gewezen op een mogelijk averechts effect:

> 'I think putting the powers on the statute book will make it more, not less, likely that police will encounter encrypted material because people will become aware of dual key systems and see how easy they are to use.'[51]

Ook zou een ontsleutelplicht kunnen leiden tot de (verdere) ontwikkeling van handleidingen over welke verweren je allemaal kunt gebruiken tegen een ontsleutelbevel.[52] Dat is tot nu toe niet gebeurd, maar wanneer het decryptiebevel in de praktijk in het VK grootschaliger toegepast zou worden, is het niet

50 Interview politie.
51 Richard Clayton, geciteerd in 'Court of Appeal orders men to disclose encryption keys', www.out-law.com/page-9514 (geraadpleegd 1 september 2012).
52 Vgl. Koops 2000, p. 79-90, 97.

uitgesloten dat ook de mogelijke verweren tegen een ontsleutelbevel verder tot wasdom komen.[53]
In hoeverre dit risico reëel is en gewicht in de schaal legt tegen invoering van een wettelijke ontsleutelplicht, zal bij de beleidsvorming rond een eventuele ontsleutelplicht moeten worden beoordeeld.

3.6 Conclusie

Het gebruik van cryptografie door verdachten neemt toe, met name bij opslag van gegevens en met name, vooralsnog, bij bepaalde groepen kinderpornonetwerken. Dit wordt gefaciliteerd door antiforensische programma's als TrueCrypt, waarmee bestanden niet alleen makkelijk versleuteld kunnen worden maar waarmee ook het bestaan van het versleutelde bestand 'aannemelijk ontkenbaar' wordt. Daartegenover staat dat justitie de nodige opsporingsbevoegdheden kan inzetten waarmee aannemelijk gemaakt kan worden dat verdachte bepaalde bestanden heeft en gebruikt, waarna de bewijsvoeringslast of een verdachte in staat is te ontsleutelen weer bij de verdachte zou komen te liggen. Deze ontwikkelingen betekenen vooral dat (onkraakbare) cryptografie meer zal voorkomen in opsporingsonderzoeken en dat er dan vaker gediscussieerd zal moeten worden over de aannemelijkheid dat er versleutelde bestanden op de harde schijf staan, dat deze belastend materiaal bevatten en dat de verdachte in staat is te ontsleutelen. Die discussie zou casuïstisch in de rechtspraak ontwikkeld kunnen worden, zoals lagere rechtspraak in de VS inmiddels laat zien. Het betekent mijns inziens dat de problematische handhaafbaarheid van een ontsleutelplicht, die in 2000 zwaar woog in mijn afweging, inmiddels minder gewicht hoeft te krijgen in de beoordeling van de mogelijkheid van een ontsleutelplicht. Wel dient de wetgever voor ogen te houden dat de invoering van een ontsleutelplicht mogelijk als een rode lap op een stier zou kunnen werken en juist de verdere ontwikkeling van 'loochenbare cryptografie' zou kunnen stimuleren.

53 Ministerie van Veiligheid en Justitie 2011.

4 Ontwikkelingen in de Europese rechtspraak van artikel 6 EVRM

Artikel 6 van het Europees Verdrag tot Bescherming van de Rechten van de Mens en de fundamentele vrijheden (EVRM) bevat het recht op een eerlijk proces. De voor dit rapport belangrijkste onderdelen ervan zijn:

> '1. Bij het vaststellen van zijn burgerlijke rechten en verplichtingen of bij het bepalen van de gegrondheid van een tegen hem ingestelde vervolging heeft een ieder recht op een eerlijke en openbare behandeling van zijn zaak, binnen een redelijke termijn, door een onafhankelijk en onpartijdig gerecht dat bij de wet is ingesteld. (…)
> 2. Een ieder tegen wie een vervolging is ingesteld, wordt voor onschuldig gehouden totdat zijn schuld in rechte is komen vast te staan.
> 3. Een ieder tegen wie een vervolging is ingesteld, heeft in het bijzonder de volgende rechten: (…)
> c. zich zelf te verdedigen of daarbij de bijstand te hebben van een raadsman naar eigen keuze of, indien hij niet over voldoende middelen beschikt om een raadsman te bekostigen, kosteloos door een toegevoegd advocaat te kunnen worden bijgestaan, indien de belangen van een behoorlijke rechtspleging dit eisen (…).'

Hoewel het nemo-teneturbeginsel (in het Engels: 'privilege against self-incrimination') niet expliciet in artikel 6 wordt genoemd, heeft het Europees Hof voor de Rechten van de Mens (in dit hoofdstuk verder aangeduid als 'EHRM' of 'Hof') vaak uitgesproken dat het nemo-teneturbeginsel samen met het zwijgrecht in de kern ligt van het begrip van een eerlijk proces (*John Murray*, §45).[54]
De uitwerking van het beginsel is echter, zoals alle EHRM-rechtspraak, casusspecifiek. Het Hof formuleert weliswaar soms algemene uitgangspunten en richtlijnen, maar beoordeelt uiteindelijk steeds of in een zaak, gelet op alle omstandigheden van het geval, het recht op een eerlijk proces is geschonden. Het nemo-teneturbeginsel speelt daarbij vaak een belangrijke rol, maar meestal samen met het zwijgrecht en bijvoorbeeld het recht op bijstand door een advocaat. Vanwege de verwevenheid van het nemo-teneturbeginsel met andere elementen van het recht op een eerlijk proces en vanwege de casusspecifieke uitspraken, is het moeilijk om in het algemeen te zeggen wat de strekking en reikwijdte is van het nemo-teneturbeginsel. Enig houvast kan worden gevonden in een beschrijving van verschillende samenhangende zaken waarin diverse elementen naar voren komen die kennelijk van belang zijn bij het beginsel. De nadruk die het Hof daarbij legt op bepaalde aspecten kan vervolgens worden gebruikt om te beredeneren of een nieuw geval – zoals een ontsleutelplicht voor verdachten, waarover het Hof zich nog niet heeft uitgelaten – al dan niet onder het nemo-teneturbeginsel zou vallen.

54 Een overzicht van de in dit hoofdstuk gebruikte arresten is te vinden in bijlage 5.

Vanwege de complexiteit van de materie is het belangrijk om eerst een algemeen overzicht te geven van de nemo-teneturjurisprudentie, zonder deze meteen toe te passen op het decryptiebevel, om de mogelijk relevante elementen voldoende uit de verf te laten komen. Deze elementen zullen dan later in dit rapport (zie paragraaf 7.4 en volgende) worden toegepast op de vraag of een verdachte tot ontsleuteling kan worden verplicht.
In dit hoofdstuk beschrijf ik de ontwikkeling van de EHRM-rechtspraak rond nemo tenetur sinds 2000, waarbij ik ook de leidende zaken van voor 2000 kort weergeef aangezien het Hof daar vaak op teruggrijpt. De meeste zaken hebben betrekking op de verklaringsvrijheid (paragraaf 4.1), zowel in situaties waarin er (nog) geen formele aanklacht bestaat (paragraaf 4.1.1) als in situaties waarin een verdachte wordt verhoord (paragraaf 4.1.2). Een belangrijk aspect van de verklaringsvrijheid in die laatste situaties is de vraag in welke mate het zwijgen van verdachte tegen hem mag worden gebruikt in een strafzaak (paragraaf 4.1.3). Ook buiten de verklaringsvrijheid heeft nemo tenetur een zekere, zij het beperkte, slagkracht (paragraaf 4.2).

4.1 De verklaringsvrijheid

4.1.1 Spreekplichten

De controlefase en situaties zonder formele aanklacht
Voor verdachten geldt dat een wettelijke verplichting om te spreken in strijd is met het zwijgrecht, maar niet-verdachten kunnen in veel gevallen wel worden verplicht om verklaringen af te leggen. Artikel 6 EVRM geldt immers pas – voor wat betreft het strafrecht – wanneer tegen iemand een vervolging ('criminal charge') is ingesteld. In de fase voorafgaand aan de vervolgingsfase (vaak aangeduid als controlefase, namelijk waarin bijvoorbeeld toezichthouders controle uitoefenen op de naleving van sociaal-economische wetgeving) geldt het nemo-teneturbeginsel niet. Het kan echter wel van toepassing zijn op verklaringen die in de controlefase (bijvoorbeeld bij de handhaving van belastingwetgeving) afgedwongen zijn en in een later stadium in een strafzaak tegen de (latere) verdachte worden gebruikt. Het standaardarrest hier is *Saunders* (1996).
Saunders werd gehoord in een serie hoorgesprekken in het kader van een administratief onderzoek naar mogelijke beursfraude. Hij was verplicht mee te werken aan het onderzoek op grond van de Companies Act 1985 en hij voerde in de loop van zes maanden negen gesprekken. Halverwege deze periode werd Saunders beschouwd als verdachte in een strafrechtelijk onderzoek naar de zaak. In de hoofdzaak werden de verklaringen die Saunders aflegde voordat hij verdachte was, ter zitting aan de jury voorgelezen, om tegenstrijdigheid aan te tonen met Saunders' verklaring ter zitting dat hij onschuldig was. Hij werd schuldig bevonden en tot vijf jaar veroordeeld.

Volgens het Hof zijn de verklaringen in de administratieve fase onder dwang afgelegd, omdat weigeren te antwoorden strafbaar was met twee jaar gevangenisstraf en er geen zwijgrecht was. De verklaringen in casu waren ook belastend omdat daaruit bleek dat de verdachte kennis bezat die ertoe neigde hem te belasten; bovendien beperkt het nemo-teneturbeginsel zich niet tot direct belastende verklaringen, omdat ook andersoortige verklaringen in een strafzaak tegen de verdachte kunnen worden gebruikt. In casu werden de verklaringen ook als zodanig opgevoerd door de aanklager voor de jury, die daardoor allicht een zeer negatieve indruk van Saunders zou kunnen krijgen door de manier waarop de verklaringen werden voorgelezen, waardoor de druk op hem om ter terechtzitting te verklaren toenam. Zo'n 'marked departure (…) from one of the basic principles of a fair procedure' kan niet gerechtvaardigd worden door de specifieke noodzaak van fraudebestrijding:

> 'the general requirements of fairness contained in Article 6, including the right not to incriminate oneself, apply to criminal proceedings in respect of all types of criminal offences without distinction from the most simple to the most complex. The public interest cannot be invoked to justify the use of answers compulsorily obtained in a non-judicial investigation to incriminate the accused during the trial proceedings. (...) Moreover the fact that statements were made prior to his being charged does not prevent their later use in criminal proceedings from constituting an infringement of the right.' (§74)

Op grond hiervan concludeerde het Hof dat het nemo-teneturbeginsel geschonden was. Tot dezelfde conclusie kwam het Hof in de zaak *Kansal* (2004), waarin verklaringen die waren afgedwongen in een faillissementsprocedure een significante rol speelden bij het bewijs in de latere strafzaak. In *Zaichenko* (2010) werden ook verklaringen uit de controlefase gebruikt in een latere strafzaak op een voor de verdachte belastende manier. Een werkgever meldde de overheid dat hij werknemers ervan verdacht dieselbrandstof van de zaak te ontvreemden, waarna de politie een verkeerscontrole hield. In Zaichenko's auto werden twee benzineblikken aangetroffen waarvoor hij geen aankoopbewijs had. Tijdens de daaropvolgende ondervraging gaf hij toe dat hij de diesel van het bedrijf had meegenomen. Daarop werd Zaichenko veroordeeld voor diefstal. Het Hof stelt dat onder dergelijke omstandigheden de verklaringen, of ze nu direct zelfbelastend waren of niet, niet gebruikt hadden mogen worden, omdat er onvoldoende waarborgen waren geweest toen hij zijn verklaring aflegde. Feitelijk was bij de verkeerscontrole al sprake van een verdenking, en Zaichenko werd weliswaar op zijn zwijgrecht gewezen, maar pas nadat hij al een belastende verklaring had afgelegd.

> 'The Court considers that being in a rather stressful situation and given the relatively quick sequence of the events, it was unlikely that the

> applicant could reasonably appreciate without a proper notice the consequences of his being questioned in proceedings which then formed basis for his prosecution for a criminal offence of theft. Consequently, the Court is not satisfied that the applicant validly waived the privilege against self-incrimination before or during the drawing of the inspection record [het proces-verbaal van de voertuiginspectie, BJK].' (§55)

Hierdoor ontstond een 'breach of due process' in de fase van het vooronderzoek, die in het latere onderzoek ter terechtzitting niet werd gerepareerd omdat de veroordeling goeddeels gebaseerd werd op de verklaring en de verdachte onvoldoende ruimte had om het afgedwongen bewijsmateriaal ter zitting nog ter discussie te stellen. Daarom is artikel 6 geschonden.
Ook in *Heaney and McGuinness* (2000) was er sprake van een hybride situatie: geen formele aanklacht, maar wel feitelijk sprake van een vervolging. Beide verdachten waren gearresteerd 24 uur na een bomaanslag in de nabijheid van de plaats van de aanslag. Op basis van artikel 52 van de Ierse Offences Against the State Act 1939 konden verdachten worden gevorderd om alle informatie te geven over hun doen en laten tijdens het moment van de aanslag; een weigering te verklaren was strafbaar met zes maanden gevangenisstraf. Hoewel de verdachten tegelijkertijd werd gewezen op hun zwijgrecht, werden ze veroordeeld tot zes maanden gevangenisstraf wegens het weigeren te verklaren. De strafbedreiging van gevangenisstraf levert een aanzienlijke mate van dwang op om te verklaren. Hoewel Ierse rechters in latere zaken hebben bepaald dat aldus afgedwongen verklaringen alleen mochten worden gebruikt als dat 'fair and equitable' was, was dit op het moment dat Heaney en McGuinness werden ondervraagd nog geen rechtspraktijk, zodat verdachten moesten aannemen dat elke verklaring die ze zouden afleggen, tegen hen gebruikt zou kunnen worden. Dit leverde een dusdanige gradatie van dwang op dat de spreekplicht onder de 1939 Act 'in effect destroyed the very essence of their privilege against self-incrimination and their right to remain silent' (§55). Weliswaar neemt het Hof in overweging dat het publieke veiligheidsbelang dat aan de wettelijke spreekplicht ten grondslag ligt, een rol kan spelen in de beoordeling, maar het publiek belang kan geen enkele bepaling rechtvaardigen die de essentie van het zwijgrecht en het nemo-teneturbeginsel tenietdoet (§57). Een nagenoeg gelijke uitspraak over dezelfde wettelijke spreekplicht deed het Hof in de zaak *Quinn* (2000). In *Shannon* (2005) was sprake van een financieel strafrechtelijk onderzoek, waarbij het niet verschijnen op een hoorzitting op het politiebureau strafbaar was met zes maanden gevangenisstraf. Nu zou zo'n verplichting volgens het Hof aanvaardbaar kunnen zijn als iemand niet verdacht is en er geen intentie is om te gaan vervolgen, maar Shannon was al aangeklaagd in een gerelateerde zaak en daarom was er een grote kans dat verdachte informatie zou moeten verschaffen die later tegen hem gebruikt zou kunnen worden. Ook hier kon volgens het Hof

de 'security context' in dit geval de inbreuk op het nemo-teneturbeginsel niet rechtvaardigen.
In situaties in het grijze gebied tussen controlefase en vervolging werkt ook het recht op rechtsbijstand (art. 6 lid 3 onder c) door in de beoordeling van het nemo-teneturbeginsel. In *Shabelnik* (2009) werd iemand gehoord als getuige maar werd in het eerste verhoor al duidelijk dat hij zichzelf aan het incrimineren was. Hij werd echter pas tien dagen later aangeklaagd, en in de tussentijd werd hem gewezen op zijn verplichting als getuige om te spreken en tegelijkertijd op zijn recht zichzelf niet te belasten. Dat moet verwarrend zijn geweest, zeker omdat hij geen bijstand had van een advocaat in deze periode. Daarenboven vormde zijn verklaring het voornaamste of enige bewijs voor de veroordeling, zodat het recht op een eerlijk proces was geschonden. Ook in *Balitskiy* (2011) speelde een belangrijke rol dat de verdachte toegang tot een advocaat was onthouden door dubieus gesjoemel met de aanklacht. Door de verdachte te verhoren in het kader van een administratief delict in plaats van de moord waar hij feitelijk van werd verdacht, werd bijstand door een advocaat (die bij bepaalde delicten wettelijk verplicht is) omzeild. Aangezien het verhoor plaatsvond zonder raadsman en in omstandigheden die wijzen op (ontoelaatbare) dwang, achtte het hof het nemo-teneturbeginsel geschonden.
De zaak *Lutsenko* (2008) is in dit verband nog interessant omdat het Hof daarin bepaalde dat een in een vooronderzoek afgedwongen verklaring niet tegen een medeverdachte mocht worden gebruikt. In deze zaak was de heer N.L. gehoord als getuige, waarbij hij een bekennende verklaring aflegde. Het is niet duidelijk of daarbij sprake was van pressie in de vorm van mishandeling, maar L. was als getuige onder strafbedreiging verplicht te antwoorden en had bovendien geen toegang tot een advocaat. In het daaropvolgende onderzoek tegen L. heeft deze steeds volgehouden dat zijn bekentenis onder dwang was afgelegd. Dit maakte de verklaring onbetrouwbaar, en daarom zou deze alleen tegen medeverdachte Lutsenko mogen worden gebruikt met extreme voorzichtigheid. Lutsenko kon L. echter niet in een openbare zitting ondervragen over diens verklaring, terwijl deze verklaring wel een doorslaggevende rol speelde in de bewijsvoering tegen Lutsenko. Dit gebruik van de in strijd met het nemo-teneturbeginsel afgedwongen verklaring van L. betekende daarom een schending van het recht op een eerlijk proces van Lutsenko.

Verkeerswetgeving
Een groot deel van de nemo-teneturzaken voor het Europees Hof betreft gevallen waarin de verkeerswetgeving een kentekenhouder verplicht te vertellen wie de auto bestuurde ten tijde van een delict. De spreekplicht en de sanctie op het niet vertellen kunnen verschillende vormen aannemen, varië-

rend van strafbaarstelling van het niet vertellen tot omkering van de bewijslast.[55]
In *Weh* (2004) werd kentekenhouder Weh beboet omdat hij een onvolledig adres had opgegeven van de bestuurder. Volgens het Hof is een verplichting voor kentekenhouders om de bestuurder bekend te maken, niet als zodanig incriminerend:

> 'It was merely in his capacity as the registered car owner that he was required to give information. Moreover, he was only required to state a simple fact – namely who had been the driver of his car – which is not in itself incriminating.' (§54)

Weh heeft zichzelf ook niet belast, hij gaf slechts een onvolledig adres op. Bovendien is hij op geen enkel moment vervolgd voor te hard rijden. De link tussen de verplichting te spreken en een eventuele vervolging is hier 'remote and hypothetical' (§56). Daarom is het nemo-teneturbeginsel in deze zaak niet geschonden. Dit wordt bevestigd in *Rieg* (2005).
Ook in *O'Halloran and Francis* (2007) moesten kentekenhouders zeggen wie achter het stuur zat bij een snelheidsovertreding. O'Halloran vertelde dat hijzelf gereden had en werd daarvoor beboet; Francis weigerde te verklaren en werd beboet voor het niet vertellen wie gereden had. Evenals in *Weh* benadrukt het Hof dat de spreekplicht een beperkte strekking heeft – wie reed er op het bewuste moment – en daarmee afwijkt van de brede spreekplichten van *Heaney and McGuinness* en *Shannon* en ook van de brede verzoeken om documenten uit te leveren in *Funke* en *J.B.* (zie paragraaf 4.2). Er is wel sprake van dwang, maar het gaat om een kleine sanctie (maximaal 1000 GBP en drie tot zes strafpunten). Bovendien vormt de verklaring wie er reed slechts een onderdeel van het bewijs van te hard rijden, en de verdachte heeft de mogelijkheid om tegenbewijs aan te dragen. Ook legt het Hof, zoals in andere verkeerszaken, nadruk op de specifieke aard van de verkeerswetgeving, die moeilijk te handhaven is zonder bepaalde plichten op kentekenhouders te leggen.

> 'Those who choose to keep and drive motor cars can be taken to have accepted certain responsibilities and obligations as part of the regulatory regime relating to motor vehicles, and in the legal framework of the United Kingdom these responsibilities include the obligation, in the event of suspected commission of road-traffic offences, to inform the authorities of the identity of the driver on that occasion' (§57).

55 Zie Koops 2000, p. 64 e.v. voor een bespreking van verschillende typen spreekplicht binnen de Nederlandse verkeerswetgeving.

Vanwege deze bijzondere aard van de wetgeving en de beperkte strekking van de spreekplicht concludeert het Hof dat de essentie van het zwijgrecht en het nemo-teneturbeginsel niet is aangetast.
Dit wordt bevestigd in *Lückhof and Spanner* (2008). Het feit dat de boete in Oostenrijk voor het niet zeggen wie reed onder bepaalde voorwaarden gepaard gaat met een standaardgevangenisstraf van een tot twee dagen maakt de dwang niet anders dan bij *Heaney and McGuinness*. Bovendien is er de procedurele waarborg dat de kentekenhouder niet strafbaar is voor het niet geven van informatie wanneer 'such failure is not at least due to his negligence, for instance where he is not in a position to provide the information because the car had been used without his knowledge and consent' (§56).
Ook de Nederlandse regeling van risicoaansprakelijkheid voor kleine verkeersdelicten (waarbij de kentekenhouder aansprakelijk is ongeacht of hij zegt dat iemand anders had gereden – hij moet zelf de boete maar verhalen op de bestuurder) kan de toets van artikel 6 EVRM, inclusief de onschuldpresumptie, doorstaan, aldus de uitspraak in *Falk* (2004). Het Hof neemt daarbij in aanmerking dat de boete aanvechtbaar is voor de rechter en dat de kentekenhouder zich dus kan verdedigen. Voor die verdediging moeten dan wel voldoende procedurele waarborgen bestaan, zo blijkt uit *Krumpholz* (2010). Het feit dat verdachte weigerde te zeggen wie er reed, werd hier gebruikt als bewijs van het feit dat hij aansprakelijk was voor het strafbare feit. De zaak werd echter maar door één instantie (zonder beroep) beoordeeld, waarbij de verdachte zelf ook nog om een hoorzitting moest vragen als hij gehoord wilde worden, zodat hij niet alleen de bewijslast maar ook een proceslast droeg. Bovendien had de verdachte schriftelijk doorgegeven dat hij niet in Oostenrijk was toen het feit werd gepleegd en niet kon zeggen wie er reed omdat de auto regelmatig door meerdere mensen gebruikt werd. Dat betekent volgens het Hof dat er geen overtuigende 'prima facie' zaak was, zoals bij *John Murray* (zie paragraaf 4.1.3), die een omkering van de bewijslast zou kunnen dragen. 'The Court cannot find that in such a situation the only common-sense conclusion was that the applicant himself had been the driver' (§40). Omdat er een situatie was 'which did not clearly call for an explanation from the applicant' en door de gebrekkige procedurele waarborgen, achtte het Hof het zwijgrecht en de onschuldpresumptie geschonden.

4.1.2 Het verhoor

Het nemo-teneturbeginsel en het zwijgrecht zien vooral op bescherming van de verdachte tegen onoorbare dwang door de autoriteiten en het verkrijgen van bewijs onder dwang of druk in weerwil van de wil van de verdachte (*Allan*, §50). Ze zijn dus primair van toepassing in situaties waarin iemand als verdachte wordt verhoord.

Onoorbare dwang is evident aanwezig als de verdachte wordt gemarteld of onmenselijk of vernederend wordt behandeld bij het verhoor. Het folterverbod van artikel 3 EVRM werkt dan rechtstreeks door in het recht op een eerlijk proces van artikel 6. Dat was het geval in *Getiren* (2008), waarin er sterke aanwijzingen waren dat de verdachte mishandeld was om belastende informatie te verkrijgen. Hoewel de verklaring geen doorslaggevende rol in het bewijs speelde, leverde de toelating ervan tot het bewijs onder deze omstandigheden wel een schending op van het zwijgrecht en nemo-teneturbeginsel. Uit *Gäfgen* (2010) blijkt dat niet alleen een door een onmenselijke behandeling afgedwongen verklaring zelf niet als bewijs mag worden gebruikt, maar ook het materiaal dat een direct gevolg is van de verklaring. In dit geval was de verdachte door de politie bedreigd met fysiek en seksueel geweld om de verblijfplaats van een ontvoerde jongen aan te wijzen. De Duitse rechter had geoordeeld dat de verklaring over de verblijfplaats niet gebruikt mocht worden vanwege schending van het pressieverbod, maar dat het fysieke bewijs ('real evidence') dat als gevolg van de verklaring was gevonden – het lijk en de rugzak van het slachtoffer, autosporen, kleren van de verdachte – wel mocht worden gebruikt. Voor het Hof is doorslaggevend dat er een causaal verband bestond tussen het ontoelaatbare verhoor (een schending van art. 3) en het daaropvolgende fysieke bewijs, zodat dat ook niet toegelaten had mogen worden tot het bewijs. Dit zou een schending van artikel 6 hebben opgeleverd, ware het niet dat de verdachte ter zitting een tweede bekentenis aflegde, zodat het fysieke bewijs niet nodig was voor de bewijsconstructie. Uit *Nechiporuk and Yonkalo* (2011) blijkt dat latere bekentenissen niet altijd helpen om de schending van artikel 3 te compenseren voor het recht op een eerlijk proces. Volgens het Hof mag een bekentenis die het gevolg is van marteling nooit toegelaten worden tot het bewijs, ongeacht welk gewicht deze bekentenis heeft en ongeacht het feit dat de verdachte later nog herhaaldelijk tijdens het verhoor bekent. Wellicht speelt de mate waarin artikel 3 is geschonden hier mee in de precieze doorwerking in artikel 6 – waar bij Gäfgen sprake was van onmenselijke behandeling maar niet van marteling (*Gäfgen*, §108), waren Nechiporuk en Yonkalo gemarteld om bekentenissen te krijgen (*Nechiporuk and Yonkalo*, §159).

Ook wanneer een verdachte niet onmenselijk of vernederend wordt behandeld, kan er sprake zijn van ontoelaatbare druk bij het verhoor. In veel zaken legt het Hof de nadruk op het belang van bijstand door een advocaat om het zwijgrecht tijdens het politieverhoor te waarborgen. In *Magee* (2000) werd de verdachte 48 uur ondervraagd in bijzonder harde omstandigheden die waren gericht op het breken van de wil van de verdachte om te zwijgen. In een dergelijke situatie zou de verdachte toegang gehad moeten hebben tot een advocaat 'as a counterweight to the intimidating atmosphere specifically devised to sap his will and make him confess to his interrogators' (§43). Het algemene beginsel van toegang tot een advocaat in het kader van een politieverhoor ter bescherming van het nemo-teneturbeginsel is uitgewerkt in *Salduz* (2008):

> 'the Court underlines the importance of the investigation stage for the preparation of the criminal proceedings, as the evidence obtained during this stage determines the framework in which the offence charged will be considered at the trial (...). At the same time, an accused often finds himself in a particularly vulnerable position at that stage of the proceedings, the effect of which is amplified by the fact that legislation on criminal procedure tends to become increasingly complex, notably with respect to the rules governing the gathering and use of evidence. In most cases, this particular vulnerability can only be properly compensated for by the assistance of a lawyer whose task it is, among other things, to help to ensure respect of the right of an accused not to incriminate himself. (…) Early access to a lawyer is part of the procedural safeguards to which the Court will have particular regard when examining whether a procedure has extinguished the very essence of the privilege against self-incrimination (...). The rights of the defence will in principle be irretrievably prejudiced when incriminating statements made during police interrogation without access to a lawyer are used for a conviction.' (§54)

Naast de toegang tot een advocaat speelt ook de cautie een rol, die des te belangrijker is wanneer de verdachte niet wordt bijgestaan door een advocaat. In *Brusco* (2010) benadrukt het Hof het feit dat de verdachte, die in verzekering zat en geen advocaat had gesproken, niet aan het begin was verteld dat hij het recht had te zwijgen en niet op vragen hoefde te antwoorden. Dit klemde te meer daar de verdachte onder aanzienlijke druk stond doordat hij een eed had moeten afleggen om de hele waarheid te vertellen (*Brusco*, §52, 54).

Gebreken in de toegang tot rechtsbijstand in het vooronderzoek kunnen het recht op een eerlijk proces onherstelbaar aantasten. In *Pavlenko* (2010) stelt het Hof onomwonden dat wanneer het recht op toegang tot een advocaat in het vooronderzoek zonder rechtvaardiging is ingeperkt (en inperking is alleen gerechtvaardigd met klemmende redenen in uitzonderingsgevallen), het recht op een eerlijk proces wordt geschonden, ongeacht de rol die een afgelegde verklaring (of bewijsmateriaal dat als gevolg daarvan verkregen is) precies speelt ter terechtzitting en ongeacht of de verdachte ter zitting het bewijs nog kan aanvechten. Dat blijkt ook uit *Todorov* (2012), waarin artikel 6 was geschonden ongeacht of de zonder rechtsbijstand afgelegde belastende verklaringen een basis hadden gevormd voor de veroordeling. Wel biedt het Hof hier een opening door te wijzen op verschillende wettelijke mogelijkheden die de Oekraïense autoriteiten hadden om gebreken in de rechtsbijstand te herstellen, zoals verwijzing van de zaak voor nader onderzoek of een formele uitspraak dat materiaal verkregen in strijd met het recht op rechtsbijstand zou worden uitgesloten van het bewijs ter zitting. Hiervan hadden de vervolgende instanties echter niet gebruikgemaakt.

Ook buiten het verhoor kan het nemo-teneturbeginsel nog een rol spelen, bijvoorbeeld wanneer de autoriteiten via informanten proberen het zwijgen van de verdachte tijdens verhoor te omzeilen. Dat was het geval in *Allan* (2002), waarin de verdachte zweeg tijdens langdurige verhoren maar na afloop in de cel tegen zijn celgenoot uit de school klapte; die celgenoot was een informant van de politie, die Allan flink doorzaagde over wat hij allemaal had gedaan. De politie maakte hier via de informant misbruik van Allans toestand, kwetsbaar als hij was om onder de druk van de langdurige politieverhoren een celgenoot in vertrouwen te nemen. Omdat de politie hier een truc gebruikte om informatie te verkrijgen die via het verhoor niet kon worden achterhaald, was de afgetroggelde verklaring verkregen in weerwil van de wil van de verdachte. Het gebruik van deze verklaring als bewijs leverde daarom een schending op van het zwijgrecht en nemo-teneturbeginsel. Dat lag anders in *Bykov* (2008), waarin de verdachte een politie-informant vrijwillig thuis ontving en met hem over het misdrijf sprak; hij zette vrijwillig de conversatie voort over het onderwerp dat de informant had aangesneden. Anders dan bij Allan was er hier dus geen sprake van enige druk om een verklaring af te leggen. Gecombineerd met het feit dat de verklaring slechts een indirecte en beperkte rol speelde in het complexe geheel van bewijsmiddelen, leverde dit geen schending op van het recht op een eerlijk proces.

4.1.3 Belastende gevolgtrekkingen

Uit de voorgaande paragrafen blijkt dat afgedwongen verklaringen vaak niet voor het bewijs mogen worden gebruikt. Maar als de verdachte, al dan niet onder druk om te verklaren, blijft zwijgen, mag zijn weigering te verklaren dan tegen hem worden gebruikt? Dat valt als zodanig niet onder het nemo-teneturbeginsel – de verdachte werkt door te zwijgen immers juist niet mee – maar het eventueel verbinden van belastende gevolgtrekkingen aan het zwijgen oefent wel druk op de verdachte uit om te verklaren, zodat ook hierbij het zwijgrecht en nemo-teneturbeginsel in het geding kunnen zijn.
Volgens het Hof mag onder bijzondere omstandigheden de bewijsvoeringslast bij de verdachte worden gelegd, wanneer er veel bewijsmateriaal tegen de verdachte is en een kennelijk belastende omstandigheid veel vragen oproept. Dat werd voor het eerst bepaald in *Salabiaku* (1988). Volgens de Franse Douanewet is de bezitter aansprakelijk voor goederen die niet bij de douane zijn aangegeven, tenzij hij overmacht kan aantonen. Salabiaku werd veroordeeld voor drugssmokkel op grond van zijn bezit van hasj in een koffer die hij in Frankrijk wilde invoeren. Een beroep op overmacht kwam hem niet toe, nu hij een waarschuwing van een vliegveldbeambte in de wind had geslagen en de koffer niet had onderzocht op het vliegveld. De Douanewet bevat evenwel geen onweerlegbare aanname van schuld, maar een weerlegbare aanname van feiten en aansprakelijkheid. Het Europees Hof liet in dit geval de veroordeling in stand, omdat de rechtbank niet automatisch tot

schuld had geconcludeerd maar op basis van het beschikbare bewijs had beargumenteerd dat er in dit geval geen aanleiding was om een overmachtssituatie aan te nemen voor het bezit van de drugs. Er was dus geen schending van de onschuldspresumptie.
Het belangrijkste arrest over het verbinden van belastende conclusies aan zwijgen van de verdachte is *John Murray* (1996). Murray weigerde uit te leggen waarom hij zich bevond in het huis waar een IRA-gijzelaar werd vastgehouden, en de rechter gebruikte dit als ondersteunend bewijs dat hij schuldig was. Volgens de Britse wet kan de rechter met zo'n weigering rekening houden in de mate waarin hij dat behoorlijk acht. Bij het verhoor was Murray herhaaldelijk gewezen op de mogelijke gevolgen van het nalaten ontlastende feiten te vermelden. Het Hof overwoog dat het zwijgrecht en het nemo-teneturbeginsel in de kern liggen van het recht op een eerlijk proces, maar dat deze immuniteiten niet absoluut zijn:

> 'On the one hand, it is self-evident that it is incompatible with the immunities under consideration to base a conviction solely or mainly on the accused's silence or on a refusal to answer questions or to give evidence himself. On the other hand, the Court deems it equally obvious that these immunities cannot and should not prevent that the accused's silence, in situations which clearly call for an explanation from him, be taken into account in assessing the persuasiveness of the evidence adduced by the prosecution. Wherever the line between these two extremes is to be drawn, it follows from this understanding of "the right to silence" that the question whether the right is absolute must be answered in the negative.
> (...)
> Whether the drawing of adverse inferences from an accused's silence infringes Article 6 is a matter to be determined in the light of all the circumstances of the case, having particular regard to the situations where inferences may be drawn, the weight attached to them by the national courts in their assessment of the evidence and the degree of compulsion inherent in the situation.' (§47)

In casu vond het Hof dat er geen onbehoorlijke druk was uitgeoefend (Murray wist immers zijn zwijgen te bewaren), terwijl het proces niet werd gevoerd voor een jury maar voor een ervaren rechter. Belangrijk is dat de regeling van bewijsgebruik omkleed was met diverse waarborgen:

1 de verdachte moet gewaarschuwd zijn dat aan zijn zwijgen conclusies kunnen worden verbonden;
2 er moet een 'prima facie case' tegen de verdachte zijn, dat wil zeggen 'a case consisting of direct evidence which, if believed and combined with legitimate inferences based upon it, could lead a properly directed jury to be satisfied beyond reasonable doubt that each of the essential elements of the offence is proved';

3 de rechter heeft een discretionaire bevoegdheid om aan het zwijgen conclusies te verbinden, en deze beslissing is onderworpen aan herziening door de appelrechter;
4 de rechter moet het gebruik van het zwijgen en het gewicht dat hij daaraan toekent motiveren.

Gegeven de omstandigheden was het gebruik van Murray's zwijgen niet in strijd met zijn recht op een eerlijk proces. De wettelijke regeling en de conclusies die de rechter aan zijn zwijgen verbond, voldeden aan de eisen. Er was een 'formidable case' tegen de verdachte, waarin de omstandigheden (zijn aanwezigheid in het huis van de gijzelaar) vroegen om een verklaring van de verdachte. Met gezond verstand kon men uit het zwijgen concluderen dat er geen ontlastende verklaring was en dat de verdachte schuldig was. Daarom was er geen strijd met de onschuldpresumptie en was het proces in dit opzicht eerlijk.

Wel was er sprake van een oneerlijk proces omdat Murray in het beginstadium van het politieverhoor geen toegang had gehad tot een raadsman. Juist omdat in dat stadium de verdachte moest kiezen tussen zwijgen (waaraan negatieve conclusies konden worden verbonden) en spreken (wat zijn mogelijkheden om zich ter zitting te verdedigen zou kunnen beïnvloeden), was rechtsbijstand bij het verhoor essentieel voor het recht op een eerlijk proces. Dat is bevestigd in de *Salduz*-uitspraak: 'National laws may attach consequences to the attitude of an accused at the initial stages of police interrogation which are decisive for the prospects of the defence in any subsequent criminal proceedings. In such circumstances, Article 6 will normally require that the accused be allowed to benefit from the assistance of a lawyer already at the initial stages of police interrogation' (§52).

Het belang van de raadsman in een vroeg stadium van het verhoor blijkt ook uit de zaak *Averill* (2000). De Criminal Evidence (Northern Ireland) Order 1988 staat het toe om bij het bewijs negatieve gevolgtrekkingen te verbinden aan het feit dat een verdachte tijdens het politieverhoor een bepaald feit verzwijgt dat hij later ter verdediging alsnog inbrengt. Hoewel het Hof de ratio daarvan (namelijk voorkomen dat de verdediging het onderzoek traineert en pas ter zitting met ontlastend bewijs komt) begrijpt, kunnen er ook legitieme redenen zijn waarom iemand iets tijdens een verhoor verzwijgt.

> 'In particular, an innocent person may not wish to make any statement before he has had the opportunity to consult a lawyer. For the Court, considerable caution is required when attaching weight to the fact that a person, arrested, as in this case, in connection with a serious criminal offence and having been denied access to a lawyer during the first twenty-four hours of his interrogation, does not provide detailed responses when confronted with incriminating evidence against him.' (§49)

De verdachte bleef echter ook zwijgen nadat hij wel dagelijks toegang tot een raadsman had gekregen, terwijl er een aanzienlijk hoeveelheid forensisch bewijs was die redelijkerwijs om een verklaring vroeg. Er waren vezels in het haar en de kleding van de verdachte aangetroffen die volgens forensisch onderzoek afkomstig waren van een bivakmuts en handschoenen die in de auto van de daders van de moordaanslag waren aangetroffen. Omdat er een aanzienlijke hoeveelheid bewijsmateriaal was, de rechtbank gedetailleerd motiveerde waarom hij geen redelijke verklaring kon vinden voor het feit dat de verdachte bij het verhoor geen verklaring voor die vezels had gegeven, anders dan dat de verdachte schuldig was, en de verdachte ook duidelijk was gewezen op de mogelijke negatieve gevolgen van zijn zwijgen, achtte het Hof het recht op een eerlijk proces niet geschonden.
Uit *Condron* (2000) blijkt dat het veel uitmaakt op welke manier precies het zwijgen van verdachten tijdens politieverhoor tegen hen ter terechtzitting wordt gebruikt. De heer en mevrouw Condron hadden wel toegang tot een advocaat bij hun verhoor. Hun weigering te verklaren wat voor pakje zij hadden uitgewisseld met een medeverdachte, werd ter zitting tegen hen gebruikt als bewijs van een drugsdelict. De zaak verschilt echter van *John Murray*, zegt het Hof, omdat de verdachten – anders dan Murray – ter terechtzitting wel een verklaring gaven voor het pakje en omdat de zaak niet door een rechter maar door een jury werd beoordeeld. En anders dan in *Averill* gaf de verdediging ook een niet onaannemelijke verklaring voor het feit dat zij bij het verhoor niets hadden gezegd: hun advocaat had hun geadviseerd te zwijgen omdat hij hen (als labiele drugsverslaafden) niet in staat achtte om goed een verhoor te doorstaan. Tegen deze achtergrond achtte het Hof het recht op een eerlijk proces geschonden omdat de rechter ter zitting de jury onvoldoende had geïnstrueerd over de beperkte mate waarin zij negatieve gevolgen mocht verbinden aan het zwijgen tijdens het politieverhoor. De rechter wees de jury weliswaar op de verklaringen die de verdachten ter zitting hadden gegeven, maar hij liet de jury de vrijheid om toch belastende gevolgtrekkingen te maken. Dergelijke gevolgtrekkingen zijn echter alleen toelaatbaar als er redelijkerwijs geen andere verklaring voor het zwijgen is dan het willen verzwijgen van schuld, en dat was hier niet het geval – er was immers een enigermate plausibele reden voorhanden waarom de verdachten tijdens het verhoor niets hadden gezegd. Aangezien de rechter had nagelaten de beoordelingsmarge voor de jury veel strikter in te perken, was het recht op een eerlijk proces geschonden.
Een soortgelijke uitspraak betreft *Beckles* (2002), waarin iemand op advies van zijn advocaat zweeg over hoe het slachtoffer van vier hoog uit het raam was gevallen. Onderweg naar het politiekantoor zei Beckles dat het slachtoffer niet uit het raam was geduwd maar zelf was gesprongen, maar de politie vertelde hem te wachten met een verklaring tot het verhoor. Tijdens het verhoor adviseerde zijn advocaat hem te zwijgen, en dat werd door de jury meegewogen in het bewijs van poging tot moord. Ook hier legt het Hof de nadruk

op onvoldoende instructie door de rechter aan de jury over welke gevolgen verbonden mochten worden aan het zwijgen tijdens het politieverhoor. De verdachte had ter zitting volgehouden dat het slachtoffer zelf was gesprongen, en hij wilde ook een nadere verklaring afleggen waarom zijn advocaat had geadviseerd te zwijgen tijdens het verhoor. Hij kreeg echter, om onverklaarde redenen, geen gelegenheid daarvoor. De rechter benadrukte bij zijn instructie aan de jury dat er geen 'onafhankelijk bewijs' was van wat de advocaat had geadviseerd – dit terwijl het advies wel in het proces-verbaal van het verhoor was opgenomen en de verdachte dit graag had willen toelichten ter zitting – en hij gaf de jury een verkeerde maatstaf mee, namelijk dat er een 'goede reden' moest zijn voor het feit dat de verdachte had gezwegen, in plaats van een reden die alleen consistent kan zijn met de schuld van de verdachte. Ongeacht de mate waarin de jury het zwijgen uiteindelijk heeft laten meewegen – wat ook niet vast te stellen is – achtte het Hof daarom het recht op een eerlijk proces geschonden.

4.2 Materiaal buiten de verklaringsvrijheid

Hoewel het nemo-teneturbeginsel in het algemene spraakgebruik ruim wordt uitgelegd als een beginsel van niet hoeven meewerken aan je eigen veroordeling, wat allerlei soorten meewerken kan omvatten, betreft het in de kern het niet gedwongen mogen worden om verklaringen af te leggen die tegen je (kunnen) worden gebruikt. In *Jalloh* (2006) formuleert het Hof het aldus:

> 'the privilege against self-incrimination is commonly understood in the Contracting States and elsewhere to be primarily concerned with respecting the will of the defendant to remain silent in the face of questioning and not to be compelled to provide a statement.' (§110)

In het *Saunders*-arrest had het Hof al een indicatie gegeven van wat er *niet* onder het beginsel valt:

> 'The right not to incriminate oneself is primarily concerned, however, with respecting the will of an accused to remain silent. (…) [I]t does not extend to the use in criminal proceedings of material which may be obtained from the accused through the use of compulsory powers but which has an existence independent of the will of the suspect such as, inter alia, documents acquired pursuant to a warrant, breath, blood and urine samples and bodily tissue for the purpose of DNA testing.' (§69)

Deze formulering is inmiddels een standaardformule geworden, die veel wordt gebruikt als argument dat een bepaalde vorm van meewerken niet onder het nemo-teneturbeginsel valt omdat het materiaal betreft dat onaf-

hankelijk van de wil van de verdachte bestaat. Zo mocht in *P.G. and J.H.* (2001) een opname van de stemmen van verdachten voor het bewijs worden gebruikt, omdat het niet ging om verklaringen maar om een stemproef, wat vergelijkbaar is met fysieke of objectieve monsters die worden afgenomen voor forensisch onderzoek, en daarop is het nemo-teneturbeginsel niet van toepassing.
Toch heeft het beginsel ook een zekere reikwijdte buiten de verklaringsvrijheid.[56] In *Jalloh* (2006) werd het onder dwang verkrijgen van de maaginhoud van de verdachte (om vermoedelijke drugsbolletjes te vinden) strijdig geoordeeld met het nemo-teneturbeginsel. De zaak is atypisch omdat de autoriteiten niet het geduld konden opbrengen om te wachten tot de maaginhoud langs natuurlijke weg naar buiten kwam, maar de verdachte via een neussonde een braakmiddel toedienden. Ook al betreft het dan materiaal dat onafhankelijk van de wil van de verdachte bestaat en betrouwbaar bewijs oplevert, de mate van dwang is hier dusdanig dat artikel 3 geschonden is, en dat vertaalt zich – zoals bij marteling of mishandeling tijdens het verhoor, zie paragraaf 4.1.2 – al snel in een schending van het recht op een eerlijk proces. Dat was hier mede het geval omdat de uitgebraakte drugs een doorslaggevende rol in het bewijs speelden. Maar het Hof gaat vervolgens nog specifiek in op de vraag of naast het recht op een eerlijk proces in het algemeen ook het nemo-teneturbeginsel in het bijzonder is geschonden:

> 'the degree of force used in the present case differs significantly from the degree of compulsion normally required to obtain the types of material referred to in the Saunders case. To obtain such material, a defendant is requested to endure passively a minor interference with his physical integrity (…) Even if the defendant's active participation is required, it can be seen from Saunders that this concerns material produced by the normal functioning of the body (such as, for example, breath, urine or voice samples). In contrast, compelling the applicant in the instant case to regurgitate the evidence sought required the forcible introduction of a tube through his nose and the administration of a substance so as to provoke a pathological reaction in his body.' (§114)

Vanwege deze abnormale vorm van dwang is het nemo-teneturbeginsel in het geding, ook al gaat het om 'onafhankelijk materiaal'. Gelet op de factoren die van belang zijn bij de beoordeling van een schending van nemo tenetur – de aard en mate van dwang, het gewicht van het publiek belang, relevante rechtswaarborgen en de manier waarop het materiaal wordt gebruikt – concludeert het Hof dat het nemo-teneturbeginsel is geschonden. De dwang was ernstig (een schending van artikel 3), het publiek belang was niet groot (het ging om een kleine straathandelaar), de waarborg van medisch toezicht was

56 Zie voor een overzicht Stevens 2007.

onvoldoende nageleefd, en de uitgebraakte drugs speelden een cruciale rol in de veroordeling.

Minder atypisch zijn zaken waarin verdachten worden gevorderd om documenten uit te leveren. Het uitleveren van documenten kan beschermd worden door het nemo-teneturbeginsel, zo bleek al in *Funke* (1993). De in Frankrijk wonende Duitse vertegenwoordiger Funke werd verdacht van overtreding van de regels voor financiële transacties met het buitenland. Franse douaneambtenaren vorderden inzage in bankafschriften van buitenlandse rekeningen. Funke gaf toe dat hij buitenlandse rekeningen bezat en zegde toe inzage te geven in bankafschriften, maar hij kwam deze toezegging niet na. Daarop begon men een rechterlijke procedure tegen Funke om inzage in de bankafschriften te verkrijgen; Funke werd veroordeeld tot een boete en bevolen om inzage te verstrekken op straffe van een dwangsom. Dit hield stand in hoger beroep en cassatie. Het Hof concludeerde echter dat artikel 6 geschonden was.

> 'The Court notes that the customs secured Mr Funke's conviction in order to obtain certain documents which they believed must exist, although they were not certain of the fact. Being unable or unwilling to procure them by some other means, they attempted to compel the applicant himself to provide the evidence of offences he had allegedly committed. The special features of customs law (…) cannot justify such an infringement of the right of anyone "charged with a criminal offence", within the autonomous meaning of this expression in Artikel 6, to remain silent and not to contribute to incriminating himself.' (§44)

Hoewel de formule uit het (latere) *Saunders*-arrest op het eerste oog in strijd lijkt met deze uitspraak – wat zou kunnen betekenen dat *Funke* door *Saunders* achterhaald is – hoeft dat niet zo te zijn. Bij *Funke* lijkt de inbreuk veroorzaakt door de bij de overheid heersende onzekerheid over het bestaan van de documenten ('they were not certain of the fact'). De overheid vraagt niet naar documenten die ze precies kent, maar is eigenlijk bezig met een 'visexpeditie': het uitgooien van een sleepnet in de hoop interessante vissen te vangen. Het onder druk uitleveren van bankafschriften zou dan neerkomen op een erkenning van het bestaan van mogelijk belastend bewijs, en dat komt min of meer neer op het afleggen van een bekennende verklaring. Deze interpretatie past ook bij de achtergronden van het beginsel. Het verplichten van een verdachte om (onzekere) documenten uit te leveren die de overheid zelf niet wil of kan zoeken, legt een te zware last op de vrijheid van de verdachte om zijn proceshouding te bepalen. Ook levert een bevel om mee te werken in dergelijke situaties niet per se betrouwbaar bewijs op, niet zozeer omdat geleverde documenten onbetrouwbaar zijn, maar omdat – als gevolg van de twijfelachtigheid van het bestaan van de documenten – geen conclusies kun-

nen worden getrokken voor het bewijs als er *geen* documenten worden geleverd. Een weigering om mee te werken kan immers zowel betekenen dat de verdachte niet *wil* meewerken als dat hij niet *kan* meewerken. Dat maakt het onredelijk om sancties – zoals herhaalde boetes – te verbinden aan het niet meewerken.
De interpretatie dat het Hof in *Funke* het nemo-teneturbeginsel gebruikte om visexpedities van de overheid aan banden te leggen, wordt versterkt door *J.B.* (2001). J.B. was verwikkeld in een belastingprocedure, waarin de autoriteiten hem vele malen sommeerden om informatie te geven en documenten te overhandigen over zijn inkomsten. De herhaalde weigering van J.B. leidde tot vier administratieve boetes. J.B. klaagde dat de autoriteiten een visexpeditie uitvoerden in de hoop om niet-opgegeven inkomsten aan te treffen. Bovendien was hij niet in staat om de gewraakte documenten uit te leveren, aangezien deze reeds waren vernietigd of bij derden (banken) lagen opgeslagen. De overheid stelde echter dat zij toch reeds weet had van de inkomsten en dat de informatieverzoeken slechts de oorsprong van deze inkomsten wilden ophelderen. Het Hof geeft dan een wat andere omschrijving van nemo tenetur dan de *Saunders*-formule:

> 'The right not to incriminate oneself in particular presupposes that the authorities seek to prove their case without resort to evidence obtained through methods of coercion or oppression in defiance of the will of the "person charged".' (§64).

Het Hof overweegt vervolgens dat J.B. niet kon uitsluiten dat de documenten nadere informatie zouden kunnen opleveren over belastingontduiking; er bestond dus een gevaar van zelfincriminatie. Ook gaat het – anders dan in de *Saunders*-formule – in dit geval niet om materiaal dat onafhankelijk van de persoon bestaat en dat niet onder dwang en in weerwil van de wil van de verdachte wordt verkregen – aldus een ingewikkelde passage in §68. Ik vermoed dat het Hof hier bedoelt dat documenten in dit soort situaties alleen kunnen worden verkregen als de verdachte zelf actief meewerkt, waarbij hij meestal ook een zekere geestelijke inspanning moet verrichten en niet enkel een lichamelijke, en dat het verkrijgen in die zin echt afhankelijk is van de wil van de verdachte. Dat maakt documenten anders dan bloed, urine en ander fysiek materiaal waarvan de verdachte vaak ook niet zal willen dat de politie het in handen krijgt, maar wat hij niet met zijn wil geheel kan tegenhouden. Bloedproeven en dergelijke zijn met lichte dwang uit te voeren, maar documenten waarvan de overheid geen idee heeft waar die liggen, kunnen alleen worden verkregen door de verdachte stevig onder druk te zetten om zijn wil te beïnvloeden; een dergelijke stevige druk komt echter al snel in strijd met het pressieverbod. Tot slot is het Hof ook niet overtuigd door de bewering van de Zwitserse overheid dat zij reeds de benodigde informatie kende. Juist de hardnekkigheid waarmee de informatie werd gevorderd (tot acht keer toe,

met oplegging van vier boetes) maakt dat ongeloofwaardig. Tegen deze achtergrond concludeert het Hof dat het nemo-teneturbeginsel hier is geschonden.
Het is lastig om het *J.B.*-arrest te interpreteren omdat de overwegingen van het Hof niet uitblinken in helderheid,[57] maar het arrest geeft in elk geval aan dat het veelgeciteerde *Saunders*-criterium niet zaligmakend is. Het gaat er niet alleen om of medewerking materiaal betreft dat onafhankelijk van de wil van de verdachte bestaat, maar ook of mogelijk belastende medewerking wordt afgedwongen in strijd met de wil van de verdachte. Dat sluit ook aan op een wat minder vaak geciteerde passage uit *Saunders*, die direct aan de onafhankelijk-materiaal-formule voorafgaat:

> 'The right not to incriminate oneself, in particular, presupposes that the prosecution in a criminal case seek to prove their case against the accused without resort to evidence obtained through methods of coercion or oppression in defiance of the will of the accused. In this sense the right is closely linked to the presumption of innocence' (§68).

Hierin zien we de ratio's van procesautonomie en het pressieverbod terug, die impliceren dat nemo tenetur vooral ook ziet op de bewijslast. Wil de overheid iemand vervolgen, dan moet zij eerst en vooral zelf het bewijs op tafel leggen; de verdachte mag niet onder (onoorbare) druk worden gezet om zelf bij te dragen aan dat bewijs als hij dat niet wil (wat natuurlijk onverlet laat dat er bepaalde situaties kunnen zijn waarin enige druk kan worden uitgeoefend – het beginsel is immers niet absoluut).

4.3 Conclusie

Het nemo-teneturbeginsel is in de rechtspraak van het Europees Hof nauw verweven met het zwijgrecht en ziet primair op de vrijheid van verdachten om, met name in verhoorsituaties, al dan niet iets te zeggen. Wetgeving die personen verplicht om verklaringen af te leggen is als zodanig niet in strijd met het zwijgrecht en het nemo-teneturbeginsel zolang de persoon niet feitelijk in een situatie van strafrechtelijke vervolging verkeert. Wel kan in dit soort situaties het bestraffen van niet meewerken een schending van het nemo-teneturbeginsel opleveren als de desbetreffende persoon redelijkerwijs kan verwachten dat zijn verklaringen later als bewijs in een strafzaak tegen hem gebruikt zullen worden. En als iemand verklaringen aflegt onder substantiële dwang (zoals de dreiging van gevangenisstraf voor niet meewerken), kan het gebruik van deze verklaringen in een latere strafrechtelijke procedure alsnog in strijd komen met het nemo-teneturbeginsel als de manier waarop deze

57 Zie Koops & Stevens 2003.

verklaringen als bewijs worden gebruikt de procespositie en verdedigingsmogelijkheid van de verdachte te veel aantast.
Wanneer de voorfase van een onderzoek dichter in de buurt komt van een feitelijke vervolgingssituatie (bijvoorbeeld als een bestuursrechtelijk traject parallel loopt met een strafrechtelijk traject in dezelfde of een aanpalende zaak), dan moeten er meer waarborgen in acht worden genomen, en dat geldt des te meer als er sprake is van een formele vervolging. Het pressieverbod, de cautie en vooral het recht op bijstand door een advocaat in een vroeg stadium spelen daarbij een belangrijke rol. In deze fase is de (mogelijke) verdachte immers extra kwetsbaar en kan hij de gevolgen van het al dan niet spreken vaak niet goed overzien. Eventuele lacunes in de rechtsbescherming gedurende deze voorfase kunnen ter terechtzitting alsnog worden gerepareerd, als de verdachte dan een reële mogelijkheid heeft om het bewijs aan te vechten. Dit is echter uitsluitend mogelijk als de dwang om te verklaren niet te groot is geweest en als het bewijs niet in substantiële mate wordt gebaseerd op de verklaring of daarvan afgeleid bewijsmateriaal.
Naast de mate van dwang en de procedurele waarborgen speelt ook nog het publiek belang dat met de spreekplicht gemoeid is, een rol. In bijzondere situaties kan het publieke belang een spreekplicht rechtvaardigen, zoals in de verkeerswetgeving waarin ten behoeve van de verkeersveiligheid bepaalde plichten aan autobezitters worden opgelegd. Maar dat kan alleen als het om een beperkte spreekplicht gaat (een enkel feit, niet een uitgebreide verklaring), als de dwang relatief klein is (een geldboete of een enkele dag gevangenisstraf) en als er voldoende procedurele waarborgen bestaan voor de verdachte om in te brengen dat hij niet aan de vordering kan voldoen. In de meeste gevallen lijkt het Hof echter weinig gewicht toe te kennen aan het publiek belang, dat in elk geval nooit ingeroepen kan worden om een ernstige mate van dwang (zoals dreiging met geweld) of het gebruik van een afgedwongen verklaring als essentieel bewijselement te rechtvaardigen.
Voor wat betreft het verbinden van negatieve gevolgen ('adverse inferences') aan het feit dat een verdachte geen verklaring geeft voor een bepaalde, kennelijk belastende omstandigheid, laat het Hof open waar precies de grens ligt. Enerzijds mag een veroordeling nooit alleen of hoofdzakelijk steunen op verdachtes zwijgen, maar anderzijds mag het zwijgen worden meegenomen bij het beoordelen van de overtuigendheid van het door justitie aangedragen bewijs in situaties die duidelijk om een verklaring van de verdachte vragen. Tussen deze twee extremen hangt het sterk van de omstandigheden van het geval af of het recht op een eerlijk proces is geschonden. In de casusspecifieke beoordeling spelen vooral de sterkte van de zaak (is er sprake van een 'prima facie case' tegen de verdachte?), het gewicht dat aan het zwijgen wordt toegekend, procedurele waarborgen (zoals bijstand door een raadsman bij het verhoor of de manier waarop een jury wordt geïnstrueerd over het bewijs) en de mate van dwang een belangrijke rol. Deze factoren fungeren als communicerende vaten. Naarmate de kennelijk belastende omstan-

digheid meer roept om een verklaring van de verdachte in het licht van het voorliggende bewijs, er meer procedurele waarborgen zijn en er minder dwang wordt uitgeoefend, mag er bij de bewijsconstructie meer gewicht worden toegekend aan de weigering van verdachte om de belastende omstandigheid te verklaren. Naarmate de dwang groter is of er minder procedurele waarborgen zijn, mag het zwijgen minder meewegen en zullen de andere bewijsmiddelen een des te overtuigender zaak ('formidable case') tegen de verdachte moeten opleveren.
Buiten de verklaringsvrijheid heeft het nemo-teneturbeginsel minder slagkracht, met name als het gaat om materiaal dat onafhankelijk van de wil van de verdachte bestaat (en dat hij dus niet met zijn wil kan beïnvloeden). Dat materiaal mag ook onder dwang worden afgenomen, waarbij de verdachte ook gedwongen kan worden actief mee te werken, zolang de dwang maar binnen de perken blijft van wat redelijk (pressieverbod) en nodig (publiek belang) is. Wanneer het gaat om materiaal dat in principe onafhankelijk van de verdachte bestaat maar dat niet zonder zijn medewerking kan worden verkregen – zoals documenten waarvan de overheid niet zeker weet of ze bestaan of waar ze zich bevinden – stelt het nemo-teneturbeginsel ook grenzen aan afgedwongen meewerking. Een uitleveringsbevel waarvan niet-naleving gesanctioneerd is, is alleen rechtvaardig als de overheid voldoende kan aantonen om welke documenten het gaat en dat de geadresseerde in staat is deze uit te leveren. Wanneer daarover twijfel blijft bestaan – en de overheid dus feitelijk aan het vissen is naar informatie in plaats van nauw omschreven, bekend materiaal te vorderen – zou meewerken door de verdachte neerkomen op het afleggen van een verklaring, namelijk over het bestaan van en zijn beschikkingsmacht over de documenten. In die gevallen raakt afgedwongen medewerking van wilsonafhankelijk materiaal alsnog de verklaringsvrijheid en wordt dit materiaal toch beschermd door het nemo-teneturbeginsel.

5 Ontwikkelingen in het Nederlandse recht

5.1 Het ontsleutelbevel

Het Nederlandse recht rond computercriminaliteit, waar het ontsleutelbevel een onderdeel van is, heeft vorm gekregen in de Wet computercriminaliteit en de Wet computercriminaliteit II. Aangezien Nederland partij is bij het zogenoemde Cybercrime-Verdrag, moet Nederland aan de eisen van dat verdrag voldoen; daarom begint deze paragraaf met het ontsleutelbevel uit het Verdrag. Vervolgens wordt de Nederlandse wetgeving beschreven, met bijzondere aandacht voor de discussie of een ontsleutelbevel ook aan verdachten moet kunnen worden gegeven.

5.1.1 Het Cybercrime-Verdrag

In het Cybercrime-Verdrag van de Raad van Europa uit 2001,[58] dat in 2004 in werking is getreden, is een ontsleutelplicht opgenomen bij de bevoegdheden tot doorzoeking en inbeslagneming. Artikel 19 lid 4 CCV bepaalt:

> 'Iedere Partij neemt de wetgevende en andere maatregelen die nodig zijn om aan haar bevoegde autoriteiten de bevoegdheid te verlenen een persoon die kennis heeft van het functioneren van het computersysteem of van de maatregelen ter bescherming van de zich daarin bevindende computergegevens, te bevelen, voorzover in redelijkheid mogelijk,[59] alle benodigde informatie te verstrekken teneinde de toepassing van de in het eerste en tweede lid bedoelde maatregelen mogelijk te maken.'

Volgens lid 5 is hierop artikel 15 van toepassing, wat wil zeggen dat bij de implementatie en uitvoering van deze bevoegdheid de rechten uit het EVRM in acht moeten worden genomen (art. 19 lid 5 jº art. 15 lid 1 CCV). De toelichting bij artikel 15 noemt expliciet het nemo-teneturbeginsel.[60] De toelichting bij de bevoegdheid van artikel 19 lid 4, de ontsleutelplicht, gaat echter niet in op de verhouding met het nemo-teneturbeginsel. De toelichting wekt ook niet de indruk dat het bevel (primair of mede) bedoeld is om verdachten aan te spreken, aangezien het de nadruk legt op systeembeheerders.

> 'A means to order the co-operation of knowledgeable persons would help in making searches more effective and cost efficient, both for law enforcement and innocent individuals affected. Legally compelling a system

58 Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, ETS 185, Boedapest, 23 november 2001, Nederlandse vertaling in *Trb.* 2004, 290. Engelse tekst, toelichting en ratificatieoverzicht zijn beschikbaar op http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG (geraadpleegd 1 september 2012).

59 Deze vertaling lijkt mij niet helemaal in lijn met de oorspronkelijke tekst, die spreekt van 'to provide, as is reasonable, the necessary information', wat blijkens de toelichting (Explanatory Memorandum, §202) slaat op wat redelijk is om te vorderen, niet op wat redelijkerwijs mogelijk is om te verstrekken.

60 Convention on Cybercrime, Explanatory Memorandum, §147.

> administrator to assist may also relieve the administrator of any contractual or other obligations not to disclose the data.'[61]

Vervolgens stelt de toelichting nog dat het in sommige omstandigheden redelijk zal zijn het wachtwoord te vorderen. In andere gevallen is het beter om de uitlevering van de gezochte bestanden in klare tekst te vorderen, met name wanneer het onredelijk is om het wachtwoord te vorderen 'where the disclosure of the password or other security measure would unreasonably threaten the privacy of other users or other data that is not authorised to be searched'.[62]
Uit de bepalingen en toelichting valt niet goed op te maken of de ontsleutelplicht uit het Cybercrime-Verdrag zich ook tot verdachten zou kunnen richten. Door de algemene bepaling dat het EVRM en het nemo-teneturbeginsel in acht moeten worden genomen bij implementatie en uitvoering, lijkt het Verdrag het aan de verdragspartijen dan wel aan de EHRM-rechtsontwikkeling over te laten om te bepalen in hoeverre een ontsleutelplicht voor verdachten verenigbaar is met het nemo-teneturbeginsel.

5.1.2 Wet computercriminaliteit en Wet computercriminaliteit II

In 1993 is met de Wet computercriminaliteit[63] in Nederland een ontsleutelplicht ingevoerd voor gevallen van bij een doorzoeking aangetroffen beveiligde computers of versleutelde gegevens (art. 125k Sv). Het bevel mag, volgens de heersende nemo-teneturleer, niet worden gegeven aan de verdachte (art. 125m lid 1-oud Sv, huidig art. 125k lid 3 Sv).

> 'Het eerste lid geeft uitwerking aan het beginsel dat de verdachte niet ware te verplichten mee te werken aan zijn eigen veroordeling. Weliswaar bestaan op dit beginsel uitzonderingen, doch deze hebben slechts zin indien er een verhouding valt aan te brengen tussen de straf die kan worden opgelegd wegens niet-nakoming van het bevel en wegens het delict dat voorwerp is van het onderzoek. Deze relatie is bij computercriminaliteit in de regel niet aanwezig, omdat het daarbij kan gaan om zeer ernstige delicten. Een dergelijke verplichting lijkt dan weinig zinvol omdat de naleving ervan in veel gevallen illusoir en niet handhaafbaar zal zijn.'[64]

De toelichting suggereert daarmee dat het nemo-teneturbeginsel bij het decryptiebevel om praktische redenen wordt gehonoreerd, maar niet per se een principiële grondslag heeft.[65]

61 Ibid., §201.
62 Ibid., §202.
63 *Stb.* 1993, 33.
64 *Kamerstukken II* 1989/90, 21 551, nr. 3, p. 28.
65 Wiemans 2004, p. 183.

In een conceptwetsvoorstel computercriminaliteit II uit 1998 was de mogelijkheid opgenomen het bevel wel aan de verdachte te geven, in geval van ernstige bezwaren en indien dit dringend noodzakelijk was voor de waarheidsvinding. De minister achtte dat in eerste instantie verenigbaar met artikel 6 EVRM omdat er 'geen sprake [is] van een verplichting om in eigen bewoordingen een oorspronkelijke weergave van bepaalde feiten of gebeurtenissen te geven'.[66] Na veel reacties – de meeste kritisch maar sommige ook positief – besloot de minister deze mogelijkheid te schrappen. 'Bij nader inzien ben ik van oordeel dat het verplichten van de verdachte tot medewerking aan de ontsleuteling een stap te ver gaat. (…) Hiermee is de verklaringsvrijheid en het zwijgrecht van de verdachte in het geding.'[67]
In de discussie over het wetsvoorstel computercriminaliteit II is kort gesproken over deze keuze. Leden van de D66-fractie vragen zich af de minister een juiste interpretatie hanteert van het *Saunders*-criterium wanneer een wachtwoord in het hoofd van de verdachte zit. 'Onafhankelijk van de wil van de verdachte bestaat het materiaal namelijk wel, alleen bestaat er geen toegang tot het materiaal.'[68] Bijna vijf jaar later antwoordt de minister hierop:

> 'Informatie die zich in het geheugen van de verdachte bevindt, zoals een wachtwoord of encryptiesleutel, kan evenwel niet worden gekwalificeerd als materiaal dat bestaat onafhankelijk van de wil van de verdachte. Het prijsgeven van deze informatie kan slechts plaats vinden met de wilsinstemming van de verdachte.[69] Gelet op het oordeel van het Hof zal een verplichting voor de verdachte tot het prijsgeven van de encryptiesleutel die zich in zijn geheugen bevindt, ontoelaatbaar moeten worden geacht. Naast het nemo tenetur-beginsel en het daaruit voortvloeiende zwijgrecht verzet overigens ook de onzekerheid of de verdachte daadwerkelijk nog over het wachtwoord beschikt, zich tegen een gedwongen afgifte van een encryptiesleutel door de verdachte (Zaak-Funke,EHRM 25 februari 1993, *NJ* 1993,485).'[70]

Verder vraagt de GroenLinks-fractie hoe het zit met iemand die een versleuteld bericht van een verdachte ontvangt, terwijl hij zelf (nog) geen verdachte is maar zich mogelijk wel incrimineert als hij op vordering het bericht ontsleutelt.[71] De minister geeft aan dat in zo'n situatie het nemo-teneturbeginsel niet geldt omdat er (voor de derde-ontvanger) nog geen 'criminal charge' is. 'Er is geen strafrechtelijk beginsel dat een niet-verdachte ontslaat van zijn medewerkingsverplichting.'[72] De minister gaat daarbij overigens niet in op

66 *Computercriminaliteit II. Voorstel van wet en Memorie van Toelichting. Concept*, januari 1998.
67 *Kamerstukken II* 1998/99, 26 671, nr. 3, p. 26.
68 *Kamerstukken II* 2000/01, 26 671, nr. 6, p. 12.
69 Hier lijkt de Minister het criterium 'onafhankelijk van de wil bestaan' gelijk te stellen aan 'onafhankelijk van de wil verkrijgen'. Bij de interpretatie van EHRM-rechtspraak speelt het onderscheid tussen deze criteria een belangrijke rol. Zie daarover paragraaf 7.4.2. [noot toegevoegd door auteur]
70 *Kamerstukken II* 2004/05, 26 671, nr. 10, p. 18.
71 *Kamerstukken II* 2000/01, 26 671, nr. 6, p. 13.
72 *Kamerstukken II* 2004/05, 26 671, nr. 10, p. 19.

het feit dat in *Saunders* is gesteld dat een niet-verdachte weliswaar kan worden verplicht mee te werken, maar dat de resultaten daarvan niet altijd als bewijs tegen hem mogen worden gebruikt als de manier waarop dat gebeurt zijn verdedigingsrechten te veel inperkt. Het is denkbaar dat het door de ontvanger versleutelde bericht, als hem dat incrimineert, van het bewijs moet worden uitgesloten als de ontvanger zelf wordt vervolgd.
Tot slot is in de Eerste Kamer nog gevraagd te reflecteren op de buitenlandse wetgeving. De minister antwoordt daarbij:

> 'De heer Franken vroeg naar de situatie in Frankrijk. Ook na onderzoek kan niet worden vastgesteld of Frankrijk een ontsleutelplicht heeft opgenomen op de wijze waarop wij dit doen. Ik weet wel zeker dat dit in het Verenigd Koninkrijk niet het geval is; daar komt men via een andere systematiek op hetzelfde resultaat uit. Ik ga er met de Kamer van uit dat de ontsleutelplicht niet wordt opgelegd aan de verdachte. Dat berust op artikel 19, vijfde lid van het Cybercrimeverdrag, dat uitdrukkelijk bepaalt dat de implementatie van de in het verdrag bedoelde bevoegdheden de waarborgen van onder andere artikel 15 van het verdrag in acht moet nemen. Een en ander betekent onder meer dat er een adequaat niveau van bescherming van mensenrechten moet zijn. In de toelichting op het verdrag is zelfs uitdrukkelijk vermeld dat dit onder meer het verbod van zelfincriminatie betreft. Ik ga ervan uit dat in de andere Europese landen dus ook geen medewerkingverplichting kan worden opgelegd. Dit is echter niet altijd op dezelfde wijze gedaan als in Nederland, met zijn bepaling in de wet.'[73]

Deze weergave van de buitenlandse situatie en de verdragsverplichtingen is niet in alle opzichten een goede beschrijving van de situatie in Frankrijk en het VK (zie hoofdstuk 6), maar duidelijk is wel dat de minister hier een ontsleutelplicht voor verdachten als strijdig met artikel 6 EVRM beschouwt.

Met de Wet computercriminaliteit II is het ontsleutelbevel uitgebreid met een verplichting om versleutelde afgetapte communicatie te ontsleutelen, waarbij wederom is bepaald dat het ontsleutelbevel niet aan de verdachte kan worden gegeven (art. 126m/t/zg leden 6-9 Sv).[74] Dit zal vooral van belang zijn in bovengenoemde situaties bij versleutelde e-mail waarin de communicatiepartner van de verdachte zelf niet verdacht is. Evenzo is bij de Wet vorderen gegevens[75] bepaald dat wanneer gevorderde gegevens versleuteld blijken, een ontsleutelbevel kan worden gegeven, wederom niet aan de verdachte (zie art. 126nh/uh/zp Sv). De gegevensverstrekker is overigens zelf toch al verplicht ontsleutelde gegevens te verstrekken (dat ligt besloten in de vordering

73 *Handelingen I* 30 mei 2006, 30-1350 – 30-1351.
74 *Stb.* 2006, 300.
75 *Stb.* 2005, 390.

tot verstrekken); de bepaling is dus vooral relevant indien hij gegevens opgeslagen houdt die door anderen versleuteld zijn en die hij niet zelf kan ontsleutelen.[76] Dat zal in de praktijk weinig voorkomen.
Bij de Wet bevoegdheden vorderen gegevens maakte de wetgever overigens wel een misslag door de tekst van artikel 125m-oud Sv te vervangen door een heel andere tekst, zonder de nemo-teneturbepaling voor het ontsleutelbevel die in dat artikel stond elders op te nemen. Dit is gerepareerd in de Wet computercriminaliteit II door invoering van een nieuw derde lid in artikel 125k Sv, dat regelt dat het ontsleutelbevel niet aan verdachten kan worden gegeven. Omdat de Wet computercriminaliteit II echter later in werking trad, is het tussen 1 januari en 1 september 2006 hierdoor theoretisch mogelijk geweest een ontsleutelbevel aan de verdachte te geven. Bij mijn weten is daar geen gebruik van gemaakt.
Overigens is de huidige ontsleutelplicht voor opgeslagen gegevens, los van de uitzondering voor verdachten, beperkt van aard, aangezien het bevel sinds de Wet computercriminaliteit II alleen kan worden gegeven in het kader van een doorzoeking ter vastlegging van gegevens of een netwerkzoeking, maar niet bij een gewone doorzoeking ter inbeslagneming. Evenmin kan het bevel worden gegeven in situaties waarin een computer of mobiele telefoon in beslag wordt genomen buiten de doorzoeking om, zoals bij aanhouding. Mij lijkt het wenselijk dat het ontsleutelbevel van artikel 125k Sv toegepast kan worden in alle gevallen waarin politie of justitie onderzoek uitvoert in een geautomatiseerd werk. Het zal immers steeds vaker voorkomen dat beveiligde mobiele apparaten (schoot-pc's, tabletcomputers, internettelefoons) in beslag worden genomen, waarbij er nog niet altijd sprake van een verdachte hoeft te zijn.[77]
Uit het overzicht van de computercriminaliteitswetgeving blijkt dat de minister weliswaar even overwogen heeft een ontsleutelplicht voor verdachten in te voeren, maar daarvan is teruggekomen. De wetgever heeft over het algemeen geoordeeld dat een ontsleutelplicht voor verdachten in strijd is met het nemo-teneturbeginsel. In lijn met de systematiek van het Wetboek van Strafvordering waarin verdachten niet tot actieve medewerking worden verplicht (met één uitzondering in art. 551 Sv, zie paragraaf 5.5), is daarom bepaald dat het ontsleutelbevel niet aan verdachten wordt gegeven. Opvallend daarbij is dat de implementatie aansluit bij de uitlevering van voorwerpen – het bevel kan niet worden gegeven aan verdachte – terwijl de motivering (zie het citaat van de minister naar aanleiding van de vraag van D66 hierboven) lijkt aan te sluiten bij het zwijgrecht. Het zou in dat licht beter in de systematiek van het Wetboek van Strafvordering passen om de nemo-teneturbescherming bij de ontsleutelplicht te normeren conform de regeling van het verhoor: de verdachte kan dan wel worden gevraagd om zijn wachtwoord, maar hij is niet tot

76 *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 11.
77 Zie Koops 2007, p. 127.

antwoorden verplicht en dat wordt hem vooraf meegedeeld, vergelijkbaar met de regeling van het verhoor in artikel 29 Sv.[78]

5.1.3 Hernieuwde discussie

Mede naar aanleiding van de Amsterdamse zedenzaak rond Robert M. en diens netwerk, is in de Tweede Kamer de vraag opgeworpen of niet alsnog een ontsleutelplicht voor verdachten moet worden ingevoerd. Bij brief van 10 juni 2011 heeft de minister op deze vraag gereageerd:

> 'Tijdens het voornoemd Algemeen Overleg is door het lid Van Toorenburg van de fractie van het CDA gepleit voor wetgeving die voorziet in de mogelijkheid om verdachten in kinderpornozaken, van wie gegevensdragers in beslag zijn genomen, te verplichten om versleutelde gegevens op die gegevensdragers toegankelijk te maken. Daarbij is verwezen naar bestaande wetgeving in het Verenigd Koninkrijk. Naar aanleiding van de inbreng van de CDA-fractie heb ik toegezegd om in overleg te treden met mijn ambtgenoot in het Verenigd Koninkrijk over zijn ervaringen met de desbetreffende wetgeving (…).
> Volgens informatie uit het Verenigd Koninkrijk zijn de ervaringen met de bevoegdheid tot het vorderen van de encryptiesleutel in zedenzaken, daaronder begrepen kinderpornografie, gevarieerd. Of de bezitter van de encryptiesleutel deze daadwerkelijk afgeeft, is afhankelijk van de ernst van de zaak. Het overleg met het Verenigd Koninkrijk over de effectiviteit van de regeling voor de aanpak van kinderpornografie wordt de komende tijd voortgezet. Daarbij is ook de verhouding met het nemo tenetur beginsel aan de orde. Dit betreft een fundamenteel beginsel in het Nederlandse strafproces, dat ook in de jurisprudentie van het Europese Hof voor de Rechten van de Mens is erkend.
> Ik acht het van essentieel belang dat de te treffen maatregelen daadwerkelijk effectief zijn. Op dit moment wordt overlegd met het Openbaar Ministerie over de behoefte aan een bevoegdheid tot het vorderen van de ontsleuteling van gegevens, de juridische haalbaarheid van een dergelijke bevoegdheid in het licht van het eerdergenoemde nemo tenetur beginsel, de categorieën van delicten waarvoor dit wenselijk zou kunnen zijn evenals de procedurele waarborgen voor een zorgvuldige toepassing. Daarbij worden ook alternatieve maatregelen betrokken, teneinde te kunnen komen tot het gewenste resultaat, namelijk dat door de politie daadwerkelijk toegang wordt verkregen tot de versleutelde bestanden. Dit vereist een zorgvuldige afweging van de betrokken belangen.'[79]

78 Zoals voorgesteld in Koops 2000, p. 101.
79 *Kamerstukken II* 2010/11, 32 500 VI, nr. 106, p. 3-4.

In deze brief laat de minister in beginsel open of een ontsleutelplicht voor verdachten verenigbaar is met het nemo-teneturbeginsel, maar de vermelding dat nemo tenetur 'een fundamenteel beginsel in het Nederlandse strafproces' is en de zware nadruk op de effectiviteit van maatregelen suggereren dat de minister (vooralsnog) geen ander standpunt inneemt dan bij de Wet computercriminaliteit II.

5.1.4 Wet op de inlichtingen- en veiligheidsdiensten 2002

Buiten het strafrecht heeft Nederland ook een ontsleutelplicht ingevoerd in de wetgeving betreffende nationale veiligheid. Artikel 24 Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002) geeft de AIVD en MIVD de bevoegdheid om computers te hacken en daarbij gegevens over te nemen die in de computer zijn opgeslagen of worden verwerkt. Wanneer deze gegevens versleuteld zijn, kan op basis van artikel 24 lid 3 een ontsleutelbevel worden gegeven:

> 'Een ieder die kennis draagt ter zake van het ongedaan maken van de versleuteling van de gegevens opgeslagen of verwerkt in het geautomatiseerde werk als bedoeld in het eerste lid, is verplicht het hoofd van de dienst op diens schriftelijk verzoek alle noodzakelijke medewerking te verlenen om deze versleuteling ongedaan te maken.'

Een ontsleutelbevel kan ook worden gegeven voor versleutelde communicatie die de inlichtingen- en veiligheidsdiensten hebben onderschept (art. 25 lid 7 Wiv 2002).
Het niet meewerken aan een ontsleutelbevel is strafbaar (art. 89 Wiv 2002). Opzettelijke weigering is een misdrijf en strafbaar met maximaal twee jaar gevangenisstraf. Niet-opzettelijke weigering is een overtreding en strafbaar met maximaal zes maanden gevangenisstraf. Hoewel niet-opzettelijke weigering suggereert dat ook personen strafbaar zijn die wel willen maar niet kunnen ontsleutelen, heeft de minister gezegd dat de geadresseerde '*uiteraard voor zover diens kennis reikt* verplicht [is] om – op een daartoe strekkend schriftelijk verzoek van het hoofd van de dienst deze kennis ter beschikking te stellen',[80] zodat iemand die aannemelijk maakt dat hij de sleutel niet heeft of kwijt is, vermoedelijk niet strafbaar zal zijn.
In de Memorie van Toelichting is nauwelijks ingegaan op deze bepalingen; bij artikel 24 lid 3 wordt slechts toegelicht dat onder versleuteling wordt verstaan 'vercijfering (encryptie), verhaspeling (scrambling) [en] versluiering (steganografie)'.[81] De strafbaarstelling wordt gemotiveerd door de 'aard van de delicten – voorkoming of bemoeilijking van het onderzoek door inlichtin-

80 *Kamerstukken II* 1999/2000, 25 877, nr. 8, p. 64 (cursivering toegevoegd). In gelijke zin *Kamerstukken II* 2000/01, 25 877, nr. 14, p. 73.
81 *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 40.

gen- en veiligheidsdiensten'.[82] De strafmaat wordt daarbij niet nader gemotiveerd, de toelichting zegt alleen dat aansluiting is gezocht bij de Telecommunicatiewet.[83] Dat kan erop duiden dat bij de strafbaarstelling of strafmaat vooral gedacht is aan het adresseren van dienstverleners die cryptografie aanbrengen bij hun dienst (en waarbij het niet meewerken vergelijkbaar is met een economisch delict), en niet zozeer aan eindgebruikers die zelf cryptografie toepassen. In de Nota naar aanleiding van het Verslag noemt de minister ook alleen internetaanbieders en Trusted Third Parties (TTP's), en niet eindgebruikers als voorbeelden van geadresseerden, maar dat kan aan de vraagstelling liggen die ging over de toepassing van de bevoegdheid 'in de internetpraktijk' en in relatie tot TTP's en het briefgeheim; ontsleuteling van opgeslagen gegevens op een computer van een eindgebruiker komt niet aan de orde.[84] In een latere nota noemt de minister wederom TTP's als mogelijke geadresseerde, maar hij zegt tegelijkertijd dat 'een ieder die kennis draagt' kan worden bevolen te ontsleutelen.[85] Hieruit kan worden afgeleid dat weliswaar primair gedacht lijkt te zijn aan dienstverleners, maar dat het ontsleutelbevel uit de Wiv 2002 aan iedereen kan worden gegeven, inclusief individuen die cryptografie toepassen. Het kan dus ook worden toegepast in terrorismeonderzoeken door de AIVD waarbij betrokkenen hun harde schijf of communicatie versleutelen.

Over de relatie van het ontsleutelbevel met het nemo-teneturbeginsel is niets gezegd bij de behandeling van het wetsvoorstel. Het beginsel is niet direct aan de orde omdat het niet gaat om strafrecht maar om handhaving van de nationale veiligheid. In theorie zou het bevel gegeven kunnen worden aan personen die object van onderzoek zijn door de AIVD en tegelijkertijd verdachte in een strafzaak. In zo'n situatie is het nemo-teneturbeginsel volgens de EHRM-rechtspraak wel aan de orde (zie paragraaf 4.1.1), waarbij het vooralsnog een open vraag is – de vraag die in dit onderzoek centraal staat – in hoeverre een ontsleutelbevel wordt beschermd door het nemo-teneturbeginsel. In elk geval lijkt de Wiv 2002 wel ruimte te bieden om in terrorismezaken waarbij ontsleuteling van gegevens van dringend belang is, bijvoorbeeld om een aanslag te voorkomen, de bevoegdheid van de AIVD in te zetten; wanneer daarbij immuniteit wordt verleend voor strafrechtelijke vervolging op basis van de ontsleutelde gegevens, zal er geen schending zijn van het nemo-teneturbeginsel (waarbij ik even in het midden laat hoe effectief een schriftelijk ontsleutelbevel door de AIVD, onder strafbedreiging van twee jaar, zou zijn om een aanslag te voorkomen).

82 *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 95.
83 Ibid.
84 *Kamerstukken II* 1999/2000, 25 877, nr. 8, p. 64.
85 *Kamerstukken II* 2000/01, 25 877, nr. 14, p. 73.

5.2 De ontwikkeling van het nemo-teneturbeginsel sinds 2000

In het Nederlandse recht zijn de systematiek en invulling van het nemo-teneturbeginsel niet fundamenteel veranderd sinds 2000.[86] De wetgever heeft geen substantiële veranderingen doorgevoerd die het nemo-teneturbeginsel raken. In een notitie uit 2001 heeft de minister de contouren geschetst van het nemo-teneturbeginsel, waarbij hij sterk aansluit bij de Europese rechtspraak. Het zwijgrecht is niet absoluut (zie *John Murray*) maar stelt wel de grens dat bewijs niet uitsluitend of hoofdzakelijk mag steunen op het zwijgen van verdachte (zie *Averill*). Het nemo-teneturbeginsel geldt vanaf de fase van een 'criminal charge'; inlichtingenplichten zijn voor die fase toegestaan, al mogen onder omstandigheden de resultaten daarvan niet als bewijs worden gebruikt (zie *Saunders*) – waarbij de minister opmerkt dat de reikwijdte van deze uitsluiting moeilijk te bepalen is in de Nederlandse situatie omdat de manier van bewijsgebruik, met juryrechtspraak, een belangrijke rol speelde in *Saunders*. De minister karakteriseert (ook op basis van *Saunders*) het zwijgrecht als de kern van het nemo-teneturbeginsel en geeft aan dat het beginsel zich niet uitstrekt tot materiaal dat onafhankelijk van de wil van de verdachte bestaat, waaronder documenten. Dat betekent onder andere dat maatregelen in het belang van het onderzoek (waarbij een verdachte bijvoorbeeld gedwongen kan worden aan een geuridentificatieproef of getuigenconfrontatie mee te werken) niet onder het nemo-teneturbeginsel vallen omdat het bewijs daarbij onafhankelijk van de wil van de verdachte wordt verkregen.[87]
Evenzo zet de Hoge Raad de bestaande lijnen van zijn nemo-teneturjurisprudentie voort. Het uitgangspunt is nog steeds

> 'dat in het Nederlandse recht niet een onvoorwaardelijk recht of beginsel is verankerd dat een verdachte op geen enkele wijze kan worden verplicht tot het verlenen van medewerking aan het verkrijgen van voor hem mogelijk bezwarend bewijsmateriaal. Wel brengt het aan artikel 29 Sv ten grondslag liggende beginsel mee dat een verdachte niet kan worden verplicht tot het afleggen van een verklaring – het verschaffen van schriftelijke inlichtingen daaronder begrepen – omtrent zijn betrokkenheid bij een strafbaar feit, waarvan niet kan worden gezegd dat zij in vrijheid is afgelegd.'[88]

In deze uitspraak ging het om een zaak waarin een bedrijf, conform de voorwaarden die aan de milieuvergunning waren verbonden, meetgegevens had geleverd die vervolgens als bewijs werden gebruikt van milieuvervuiling. Dit is niet in strijd met het nemo-teneturbeginsel, omdat de gegevens zijn gele-

86 Voor een overzicht van de systematiek en invulling, zie Koops 2000, p. 35-51 en recenter Stevens 2008.
87 *Kamerstukken II* 2001-2002, 28 176, nr. 1.
88 HR 19 september 2006, *LJN* AV1141, r.o. 6.5.1.

verd in het kader van legitiem milieutoezicht (waarin er geen sprake is van een 'criminal charge'). De meetgegevens mogen later worden gebruikt als bewijs in een strafzaak:

> 'Deze gegevens vallen immers buiten het bereik van het recht dat een verdachte kan ontlenen aan art. 29 Sv en art. 6 EVRM om te weigeren informatie en opheldering aan de overheid te verschaffen die in een strafzaak tot bewijs tegen hem kunnen dienen (Saunders tegen het Verenigd Koninkrijk, EHRM 17 december 1996, no 43/1994/490/572, *NJ* 1997, 699, rov. 68 en 69).'[89]

Interessant is hierbij dat de Hoge Raad hier een ruime uitleg geeft aan het zwijgrecht, in de zin dat het niet alleen gaat om het weigeren te verklaren maar ook om het weigeren 'informatie en opheldering' te verschaffen. Volgens Stevens kan dit worden opgevat, in lijn met *Funke* en *J.B.*, als een verbod op open vraagstellingen of visexpedities die 'testimonial aspects'[90] in zich bergen.[91]
De Hoge Raad motiveert overigens niet waarom de meetgegevens onafhankelijk van de wil van de verdachte bestaan; vermoedelijk spreekt dat vanzelf omdat meetgegevens van milieuwaarden vergelijkbaar zijn met alcoholmeting van bloed, dat expliciet in het *Saunders*-criterium wordt genoemd als wilsonafhankelijk materiaal. Maar ook een intern rapport dat een bedrijf naar aanleiding van een incident heeft opgesteld mag onder omstandigheden worden gevorderd, ook als het een verklaring bevat die de (latere) verdachte zelf heeft opgesteld:

> 'Beslissend voor de vraag of het nemo-tenetur-beginsel is geschonden, is immers of het gebruik tot het bewijs van een al dan niet in een document vervatte verklaring van de verdachte in een strafzaak zijn recht om te zwijgen en daarmee zijn recht om zichzelf niet te belasten van zijn betekenis zou ontdoen. Het antwoord op deze vraag hangt af van de aard van de in het document vervatte verklaring, waarbij de omstandigheid dat de verdachte de verklaring zelf heeft vervaardigd, niet beslissend is. De Rechtbank had derhalve kennis moeten nemen van de inhoud van de documenten.'[92]

Het gaat dus vooral om de aard van een verklaring. Naarmate deze meer zegt over de mogelijke betrokkenheid van verdachte bij het strafbare feit, zal deze de kern van de verklaringsvrijheid raken en zou het zwijgrecht zijn betekenis

89 Ibid., r.o. 6.5.2.
90 Denk aan handelingen die, hoewel feitelijk van aard, een verklarend element hebben, zoals het uitleveren van documenten waarbij verdachte impliciet het bestaan, de beschikkingsmacht of de authenticiteit van de documenten erkent; vgl. paragraaf 6.4.
91 Stevens 2007.
92 HR 21 december 2010, *LJN* BL0666, r.o. 4.3.

verliezen. Naarmate de verklaring meer feitelijk van aard is (of niets zegt wat in relatie tot het strafbaar feit van belang is), zal het zwijgrecht minder worden aangetast.[93] Dat blijkt in zekere zin ook uit een arrest waarin wordt bevestigd dat de plicht voor de kentekenhouder om te zeggen wie bij een misdrijf achter het stuur zat (art. 165 WVW) alleen geldt voor kentekenhouders zolang zij niet verdachte zijn.[94] De gedachte daarbij is dat een niet-verdachte kentekenhouder verklaart over een feit (wie bestuurde er?), terwijl een verdachte kentekenhouder verklaart over zijn eventuele betrokkenheid bij een strafbaar feit. Evenzo is het nemo-teneturbeginsel niet van toepassing wanneer iemand klaagt (ex art. 552a Sv) tegen een inbeslagneming als er op het moment van klagen nog geen 'criminal charge' is.[95]
Daarnaast maakt het ook uit in welke context een verklaring is afgelegd. Een verklaring van verdachte tegenover het Leger des Heils in het kader van een reclasseringsrapport dat voorlichting moet geven over de persoon, mag niet worden gebruikt als bewijs, ook niet als steunbewijs.[96]
Uit dit korte overzicht blijkt dat het Nederlandse recht rond nemo tenetur sinds 2000 niet substantieel is gewijzigd ten opzichte van de stand van zaken destijds, en dat sterk wordt aangesloten bij de rechtspraak van het Europese Hof. De Hoge Raad formuleert daarbij als maatstaf dat het gebruik van een verklaring (en in het verlengde daarvan (feitelijke) informatie en opheldering die elementen van een verklaring in zich bergen) in een strafzaak het zwijgrecht, en daarmee het recht zichzelf niet te belasten, niet van zijn betekenis mag ontdoen.
Wat die betekenis precies inhoudt, zegt de Hoge Raad daarbij overigens niet. Voor de doelstelling van dit onderzoek sluit ik aan bij de betekenis die Stevens geeft aan nemo tenetur, aangezien zij de meest diepgravende analyse heeft gemaakt van het beginsel in de huidige Nederlandse context.[97] Stevens verklaart de verklaringsvrijheid als kern van het nemo-teneturbeginsel vanuit de ratio van de procesautonomie, dat wil zeggen de vrijheid van de verdachte om zijn procespositie te bepalen. De verdachte moet vrij zijn om al dan niet mee te werken aan het bewijs, althans voor zover hij invloed kan uitoefenen op de verkrijging en inhoud ervan. Die invloed hangt samen met een intellectuele inspanning; materiaal dat onafhankelijk van zijn wil kan worden verkregen, dat wil zeggen zonder dat de verdachte een intellectuele inspanning hoeft te leveren, mag wel worden afgedwongen. Immers, '[o]p de inhoud of samenstelling ervan kan de verdachte geen invloed uitoefenen. De procesautonomie van de verdachte is in deze uitleg dan ook een intellectuele, inhoudelijke autonomie.'[98] Bij het afdwingen van wilsonafhankelijke mede-

93 Vgl. Hoge Raad CPG 11/03167 B, *LJN* BV3004, waarin de verdediging het gebruik van diverse gevorderde verklaringen bestreed maar niet klaagde over het oordeel van de rechtbank dat in patiëntendossiers opgenomen gegevens betrekking hebben op buiten klager liggende, feitelijke en geobjectiveerde omstandigheden en daarom niet de verklaringsvrijheid aantasten.
94 HR 16 september 2008, *LJN* BD1707. Vgl. over deze wat gekunstelde constructie Koops 2000, p. 65.
95 HR 5 juli 2011, *LJN* BP5144.
96 HR 18 september 2007, *LJN* BA3610, r.o. 3.3.
97 Stevens 2005, 2008.
98 Stevens 2007.

werking moeten echter wel de grenzen van subsidiariteit en proportionaliteit in acht worden genomen (die bij *Jalloh* duidelijk waren overschreden, ook al hoefde Jalloh geen intellectuele inspanning te leveren om de cocaïne uit te braken).[99] Het pressieverbod stelt daarom ook grenzen aan het meewerken door verdachten buiten de verklaringsvrijheid om. Kortom, het zwijgrecht wordt van zijn betekenis ontdaan als een verdachte wordt gedwongen een intellectuele inspanning te leveren die mogelijk invloed heeft op de samenstelling of de inhoud van bewijsmateriaal, en het recht zichzelf niet te belasten wordt van zijn betekenis ontdaan a) als het zwijgrecht wordt uitgekleed of b) als er onnodige of disproportionele druk op de verdachte wordt uitgeoefend om materiaal te verkrijgen.[100]

5.3 Het gebruik van zwijgen bij het bewijs

5.3.1 Algemeen

Voor dit onderzoek is ook van belang, naast de in de vorige paragraaf behandelde vraag in hoeverre medewerking van een verdachte mag worden afgedwongen, de vraag of een weigering van een verdachte te ontsleutelen tegen hem mag worden gebruikt bij het bewijs. Het is immers denkbaar dat een ontsleutelplicht niet wordt vormgegeven als een bevoegdheid een decryptiebevel te geven die onder strafbedreiging wordt afgedwongen (vergelijkbaar met het algemene art. 184 Sr dat straf stelt op het niet meewerken aan een bevel), maar als de mogelijkheid om een weigering van een verdachte om in te gaan op een verzoek (niet een vordering) om te ontsleutelen een rol te laten spelen in de bewijsconstructie ter onderbouwing van het oordeel dat de verdachte het feit heeft gepleegd. Daarvoor is weinig ruimte (omdat het neerkomt op omkering van de bewijslast), maar wel enige ruimte, zoals kan worden afgeleid uit *John Murray*.
De stand van zaken in 2000 voor het trekken van belastende conclusies ('adverse inferences') was dat het zwijgen van een verdachte mag worden gebruikt

1 om een verweer van verdachte te verwerpen dat een alternatief scenario ('onschuldig') het bewijsmateriaal beter verklaart dan het voorliggende scenario ('schuldig'), als de verdachte weigert uit te leggen hoe een belastend feit in dat alternatieve scenario past;

99 Ibid.

100 Deze betekenis van het nemo-teneturbeginsel sluit vrij nauw aan op de betekenis die er in het Angelsaksische recht aan wordt toegekend, in elk geval voor wat betreft de rol van de verklaringsvrijheid. Zie paragraaf 6.4 over de uitwerking van het centrale begrip 'testimonial'. Vgl. Pardo 2008, die het onderscheid tussen 'testimonial evidence' (wel nemo tenetur) en 'physical evidence' (niet nemo tenetur) verklaart vanuit het feit dat bij 'testimonial evidence' voor het bewijs een beroep moet worden gedaan op de 'epistemic authority' van de verdachte, dat wil zeggen dat de kennis of overtuiging van de verdachte wordt aangesproken. Dit sluit nauw aan bij de intellectuele inspanning die centraal staat in de Nederlandse verklaringsvrijheid.

2 in de overwegingen omtrent het bewijs als 'een verdachte voor een omstandigheid, die op zichzelf of in samenhang met de verdere inhoud van de bewijsmiddelen beschouwd redengevend moet worden geacht voor het bewijs van het aan hem telastegelegde feit, geen redelijke, die redengevendheid ontzenuwende, verklaring heeft gegeven'.[101] Anders gezegd, als de verdachte *geen* alternatieve verklaring geeft voor een bezwarende omstandigheid (terwijl hij wel in staat moet worden geacht om opheldering te verschaffen), kan de rechter zijn zwijgen gebruiken als overweging om aan te nemen dat die omstandigheid waar en belastend is en deze aldus – in samenhang met ander bewijsmateriaal – mee laten wegen.[102]

In het kader van het eventueel trekken van belastende gevolgtrekkingen uit een decryptieweigering is de tweede mogelijkheid het meest relevant. Hierin zijn enkele ontwikkelingen zichtbaar sinds 2000.

In de eerste plaats wordt in witwaszaken regelmatig bij de bewijsconstructie gebruikgemaakt van het feit dat de verdachte geen redelijke verklaring geeft voor een grote hoeveelheid geld in zijn bezit. Als iemand onder verdachte omstandigheden (zoals op reis zonder ruimbagage; 500 biljetten van 50 euro verstopt in spijkerbroek en toilettas; vrijwillig afstand doen van het geld) een grote hoeveelheid geld bij zich heeft op Schiphol, kan worden aangenomen dat het geld uit misdrijf is verkregen als de verdachte steeds wisselende en tegenstrijdige verklaringen aflegt over hoe hij aan het geld is gekomen.[103] 'Het uitblijven van een afdoende en verifieerbare verklaring en een aantal bijzondere omstandigheden van het geval maken dat witwassen [dan] bewezen kan worden verklaard.'[104] Als de verdachte voor zijn verklaring over de herkomst van het geld 'geen verifieerbare gegevens heeft kunnen verschaffen op punten die eenvoudig te achterhalen moeten zijn en van belang zijn om aan zijn stellingen een begin van geloofwaardigheid te verlenen', mag worden aangenomen dat het geld uit misdrijf afkomstig is. Dat daarbij de 'hoogst onwaarschijnlijke' verklaring van verdachte terzijde wordt geschoven, betekent niet dat de bewijslast over de afkomst van het geld op de verdachte wordt gelegd.[105] Het blijft aan het OM om aan te tonen dat geld uit misdrijf is verkregen, maar dat wil niet zeggen dat het OM dit onomstotelijk moet aantonen. De bewijsvoeringslast[106] is daarbij zodanig dat

– het OM eerst aannemelijk moet maken dat er sprake is van witwassen (zodat 'zonder meer sprake is van een vermoeden van witwassen');

101 HR 3 juni 1997, *NJ* 1997, 584.
102 Bij dit arrest ging het om een strippenkaart in het bezit van verdachte, die was afgestempeld rond de tijd en plaats van het delict. Nu de verdachte niet verklaarde hoe hij in het bezit kwam van deze strippenkaart, kon de rechter zijn bezit van de strippenkaart redengevend achten voor het bewijs dat *hij* het was die het feit had begaan (in samenhang met de herkenning door een getuige).
103 HR 27 september 2005, *LJN* AT4094.
104 Verloop 2012, p. 169.
105 HR 13 juli 2010, *LJN* BM2471.
106 Zie over dit begrip Corstens & Borgers 2011, p. 678-679.

– vervolgens, met inachtneming van de omstandigheden van het geval, van de verdachte kan worden verlangd dat hij een verklaring geeft voor de herkomst van het geld;
– als de verdachte 'een concrete, min of meer verifieerbare en niet op voorhand als volslagen onwaarschijnlijk aan te merken herkomst' noemt, de bewijsvoeringslast terugschuift naar het OM;
– het OM dan de alternatieve verklaring nader moet onderzoeken en daarbij voldoende aannemelijk moet maken dat het geld uit misdrijf afkomstig is en niet uit de door verdachte gesuggereerde bron.[107]

In de tweede plaats is er ook een nadere uitwerking gekomen van de rol die het zwijgen kan spelen bij het bewijs in andere dan witwaszaken. In een recente zaak ging het om een brandstichting waarbij camerabeelden lieten zien dat de bivakmuts van de dader enige tijd in brand stond. Forensisch onderzoek van de verdachte toonde aan dat de haren van verdachte blootgesteld waren aan een hittebron; verdachte weigerde daarvoor een verklaring te geven, wat het gerechtshof liet meewegen in samenhang met divers ander bewijsmateriaal. De Hoge Raad verwerpt, na te hebben gewezen op de algemene regel uit zijn arrest uit 1997 (zie punt 2 hierboven), het cassatiemiddel dat klaagt over dit gebruik van verdachtes zwijgen:

> 'De klacht steunt (…) op de opvatting dat een omstandigheid als hiervoor onder 3.4 bedoeld [d.w.z. een omstandigheid als hierboven onder 2) beschreven, BJK] eerst dan door de rechter in de bewijsvoering mag worden betrokken indien sprake is van een "formidable case", waarmee blijkens de toelichting op het middel beoogd is te zeggen dat pas conclusies uit het stilzwijgen van de verdachte mogen worden getrokken op de voorwaarde dat "de zaak bewijsbaar moet zijn zonder rekening te houden met het stilzwijgen van de verdachte", en dat de rechter expliciet moet vaststellen dat aan die voorwaarde is voldaan. Die opvatting vindt echter geen steun in hetgeen hiervoor onder 3.4 is vooropgesteld [d.w.z. de maatstaf als hierboven onder 2) beschreven, BJK] en evenmin in de op dit thema betrekking hebbende rechtspraak van het EHRM (vgl. bijvoorbeeld het overzicht daarvan in EHRM 18 maart 2010, nr. 13201/05 (Krumpholz tegen Oostenrijk)).'[108]

Vervolgens verwerpt de Hoge Raad het middel zonder verdere uitleg.[109] Hiermee schept de Hoge Raad meer ruimte dan op basis van de *John Murray*-uitspraak (1996) leek te bestaan voor belastende gevolgtrekkingen. In *John*

107 HR 13 juli 2010, *LJN* BM0787. Deze bewijslastverdeling wordt ook gehanteerd in de Britse wetgeving voor de ontsleutelplicht, ten aanzien van de vraag of een verdachte in staat is om (vermoedelijk belastende) gegevens te ontsleutelen; zie paragraaf 6.3.1.
108 HR 5 juni 2012, *LJN* BW7372, r.o. 3.5.
109 Vermoedelijk omdat in casu de ondergrens van een 'prima facie' case wel duidelijk bereikt was; vgl. §10 van de conclusie bij het arrest.

Murray speelde immers mee dat de Engelse wet het alleen toestond om 'adverse inferences' te trekken als er een 'prima facie case' tegen de verdachte was, wat lijkt neer te komen op voldoende bewijs voor een veroordeling.[110] Kennelijk leest de Hoge Raad in de EHRM-rechtspraak, zoals samengevat in *Krumpholz*, dat er niet per se sprake hoeft te zijn van een 'formidable case', of wellicht dat de formidabiliteit van een 'formidable case' niet betekent dat er al voldoende bewijs moet zijn om, ook zonder de door het zwijgen onverklaarde omstandigheid mee te laten wegen, tot een veroordeling te komen. In de visie van de Hoge Raad mag dus een belastende omstandigheid waarvoor de verdachte geen redelijke verklaring geeft, meewegen om de stap te zetten naar een bewezenverklaring, ook als de andere bewijsmiddelen (zonder de onverklaarde belastende omstandigheid) op zich onvoldoende zijn voor het bewijs. Met andere woorden, de belastende omstandigheid mag in samenhang met het zwijgen van de verdachte worden gebruikt als het laatste puzzelstuk in de bewijsconstructie.
Of dat een juiste lezing van *Krumpholz* is, is overigens niet direct duidelijk. De samenvatting in *Krumpholz* lijkt toch wel te benadrukken dat de andere bewijsmiddelen tegen verdachte wel heel sterk moeten zijn, wil een door verdachte onverklaarde belastende omstandigheid mogen meewegen in het algehele bewijs.[111] Anderzijds heeft het EHRM al sinds *John Murray* opengelaten waar precies de grens ligt voor het trekken van 'adverse inferences' (*John Murray*, §47, zie paragraaf 4.1.3). In zaken over belastende gevolgtrekkingen herhaalt het Hof vaak de twee extremen (nooit respectievelijk in sterke mate iemands zwijgen gebruiken voor het bewijs), om vervolgens een genuanceerde beschouwing te geven of in het specifieke geval 'adverse inferences' waren toegestaan.
De EHRM-rechtspraak zoals samengevat in *Krumpholz* en de uitspraak van de Hoge Raad in het recente arrest kunnen denk ik worden geïnterpreteerd in de zin dat een 'formidable case' (in de zin van (bijna) voldoende bewijs voor een veroordeling) een voldoende maar geen noodzakelijke voorwaarde is voor het mogen maken van belastende gevolgtrekkingen (mits de kern van het zwijgrecht niet door andere factoren wordt tenietgedaan). Binnen de bandbreedte van de twee extremen (een veroordeling hoofdzakelijk baseren op het zwijgen tegenover het nooit gebruiken van zwijgen bij bewijs) funge-

110 Zo interpreteerde ik in 2000 in elk geval de overweging in *John Murray t. Verenigd Koninkrijk*, app.nr. 18731/91, §51 dat 'the prosecutor must first establish a prima facie case against the accused, i.e. a case consisting of direct evidence which, if believed and combined with legitimate inferences based upon it, could lead a properly directed jury to be satisfied beyond reasonable doubt that each of the essential elements of the offence is proved'.

111 In *Krumpholz* brengt het Hof in herinnering dat er in *John Murray* sprake was van 'a formidable case against the applicant' (*Krumpholz*, §32). Vervolgens verwijst het Hof naar *Telfner*, waar het stelde dat belastende gevolgtrekkingen mogelijk zijn 'where the courts freely evaluate the evidence before them, provided that the evidence is such that the only common-sense inference to be drawn is that the accused has no answer to the case against him' (*Krumpholz*, §33). Dat komt mijns inziens ook neer op een 'formidable case'. Tot slot grijpt het Hof terug op *Salabiaku*, waarin in het algemeen werd gesteld dat 'presumptions of fact or law operate in every criminal-law system and are not prohibited in principle by the Convention, as long as States remain within reasonable limits, taking into account the importance of what is at stake and maintaining the rights of the defence' (*Krumpholz*, §34).

ren het gewicht van zwijgen in de bewijsconstructie, procedurele waarborgen en de mate van dwang als communicerende vaten. Naarmate er meer procedurele waarborgen zijn en er minder dwang wordt uitgeoefend, mag er (iets) meer gewicht worden toegekend in de bewijsconstructie aan de weigering van verdachte om een belastende omstandigheid te verklaren; naarmate de dwang groter is of er minder procedurele waarborgen zijn, mag het zwijgen minder meewegen en zullen de andere bewijsmiddelen een des te 'formidabelere' zaak moeten opleveren. Daarbij zal overigens ook de belastendheid van de omstandigheid zelf een rol spelen – enkele verschroeide hoofdharen zijn een meer belastende omstandigheid dan een kassabon van een tankstation, maar minder belastend dan een halfverbrande bivakmuts in verdachtes slaapkamer waarvoor de verdachte geen alternatieve verklaring wil aandragen.

5.3.2 Het gebruik van decryptieweigering bij het bewijs

In Nederland is recentelijk een decryptieweigering gebruikt in de bewijsconstructie. In de Amstelveense zedenzaak werd bij verdachte Matthijs van der M. een grote hoeveelheid beeldmateriaal aangetroffen dat dubieus van aard was – het was geen evidente kinderpornografie, maar het wekte wel die indruk. Enkele afbeeldingen werden door de rechtbank als kinderpornografie gekwalificeerd. De verdediging betoogde dat verdachte niet opzettelijk kinderpornografie in zijn bezit had, omdat hij zich weliswaar '"op het randje" begaf, maar dat zijn opzet gericht was op het verzamelen van niet-strafbare foto's'. De rechtbank verwerpt dit verweer:

> 'Het dossier bevat hierover echter geen verklaring van verdachte zelf. Verdachte heeft ervoor gekozen om te zwijgen. Bovendien heeft verdachte een zwaarbeveiligde computer in zijn bezit gehad en zijn wachtwoorden daarvoor niet prijsgegeven. Daarmee heeft verdachte de rechtbank eventuele ontlastende informatie over zijn intenties onthouden. De rechtbank ziet voor de stelling van de raadsman over de aard van het verzamelen dan ook geen steun in het dossier. Dat deze foto's als kinderpornografisch beoordeeld worden, dient dan ook voor risico van verdachte te komen.'[112]

In de zaak van de medeverdachte, Flovin O., was ook een computer aangetroffen met een versleutelde container. Het NFI bleek in staat deze container te kraken, waarbij een aanzienlijke hoeveelheid kinderpornografie werd blootgelegd. Interessant in deze zaak is dat de rechtbank de weigering van de verdachte om de wachtwoorden van zijn computer te geven gebruikt om een verweer te verwerpen dat de doorzoeking disproportioneel was (waardoor verdachte in shock zou zijn geraakt). Immers, het feit dat de verdachte bij de doorzoeking weloverwogen in staat was om bepaalde vragen, waaronder die

112 Rb. Amsterdam 23 juli 2012, *LJN* BX2326, r.o. 4.4.4.

naar zijn wachtwoorden, niet te beantwoorden, gaf aan dat dit verweer niet aannemelijk was.[113] Evenzo wordt een beroep op psychische overmacht verworpen onder verwijzing naar onder meer verdachtes cryptografiegebruik:

> 'Verdachte was zeer goed in staat om doordacht en weloverwogen te handelen zonder daarbij gehinderd te worden door "heftige gemoedsbewegingen". Hij koos voor het TOR, een "ondergronds" deel van het internet, en wisselde van nicknames/pseudoniemen om niet traceerbaar te zijn. Hij versleutelde delen van zijn computer om die ontoegankelijk te maken voor derden. Hij verwijderde VMware, een versleuteld gedeelte van zijn computer, na de aanhouding van [medeverdachte] en ging met zijn medeverdachte door het huis om sporen te wissen om te voorkomen dat belastend materiaal bij hem zou kunnen worden aangetroffen.'[114]

Een curieus ander geval betreft de verdachte van verduistering van een laptop, die aan justitie verzocht om hem kopieën van versleutelde gegevens op zijn laptop te verstrekken omdat hij die nodig zou hebben voor zijn verdediging. De rechtbank stelde hem in de gelegenheid om bij een politieverhoor zo specifiek mogelijk aan te duiden welke bestanden hij wilde en hoe daartoe toegang kon worden verkregen, waarbij hij zo nodig de gelegenheid zou krijgen om daartoe benodigde wachtwoorden te verschaffen. De verdachte weigerde bij het verhoor echter om zijn wachtwoorden af te geven; hij wilde zelf de wachtwoorden invoeren, omdat hij bang was dat de politie anders gegevens van zijn laptop zou verwijderen. De politie wilde echter alleen meewerken onder de voorwaarden die de rechtbank had gesteld, namelijk door de wachtwoorden van de verdachte te krijgen. De verdachte bepleitte vervolgens niet-onvankelijkverklaring vanwege tegenwerking van de verdediging. De rechtbank ging daar niet in mee en bepaalde dat het weigeren van de verdachte om zijn wachtwoorden af te geven voor zijn eigen rekening moet komen. De vrees dat de politie bestanden zou gaan verwijderen, was ongegrond. De verdachte werd op basis van het beschikbare bewijsmateriaal veroordeeld voor de verduistering.[115]
Uit de uitspraak kan niet worden afgeleid of de verdachte wellicht bang was dat door het afgeven van de wachtwoorden nog andere, mogelijk belastende, bestanden in handen van de politie zouden komen; in elk geval heeft hij de vrees voor zelfbelasting niet als argument aangevoerd. De zaak maakt wel duidelijk dat het verschil kan maken of de verdachte wachtwoorden afgeeft of zelf ontsleutelt en dat verdediging en justitie verschillende belangen kunnen hebben om voor de ene of voor de andere modaliteit te kiezen.

113 Rb. Amsterdam 23 juli 2012, *LJN* BX2325, r.o. 4.4.1.
114 Ibid., r.o. 7.1.4.
115 Rb. 's-Gravenhage 16 juni 2010, *LJN* BM7979.

5.4 Het gebruik van zwijgen bij straftoemeting

Een andere modaliteit is om een decryptieweigering niet te gebruiken bij de waardering van het bewijs, maar bij de straftoemeting. Bij de straftoemeting mag immers de proceshouding van de verdachte worden meegewogen. Het argument dat het laten meewegen van de proceshouding van de verdachte bij de straftoemeting in strijd zou zijn met het nemo-teneturbeginsel, wordt verworpen door de Hoge Raad. '[D]e keuze van de factoren die – na bewezenverklaring van het feit – voor de strafoplegging van belang zijn te achten, is voorbehouden aan de rechter die over de feiten oordeelt. Geen rechtsregel belet de rechter daarbij ook de opstelling van de verdachte te betrekken.'[116] Zoals de A-G toelicht:

> 'Een gebrek aan inzicht in de laakbaarheid van het eigen gedrag kan nog steeds een factor zijn die de rechter bij de straftoemeting in ogenschouw neemt. Het beginsel "nemo tenetur" geeft de verdachte een zekere procesautonomie om zijn eigen houding te bepalen tijdens het strafproces, maar daarmee is die houding van verdachte niet gevrijwaard van waardering door de rechter. Die autonomie is niet vrijblijvend.'[117]

Dit is recentelijk toegepast in de Amstelveense zedenzaak. Matthijs van der M. werd veroordeeld tot negen maanden gevangenisstraf (waarvan drie voorwaardelijk) voor bezit en vervaardiging van kinderpornografie. Bij de straftoemeting overwoog de rechtbank:

> 'In strafverzwarende zin overweegt de rechtbank het volgende. (…) Verder heeft verdachte zich bij de politie op alle vragen gerelateerd aan de ten laste gelegde feiten op zijn zwijgrecht beroepen. Hij heeft geen wachtwoorden willen verschaffen van zijn zwaar beveiligde computer terwijl het beschikken over dusdanig beveiligde hardware wel vragen opwierp. Ook is verdachte tijdens de inhoudelijke behandeling op geen enkel moment ter terechtzitting verschenen. Daarmee heeft verdachte er geen blijk van te geven verantwoordelijkheid voor zijn handelen te nemen. De rechtbank houdt bij het opleggen van de straf rekening met deze proceshouding.'[118]

Het omgekeerde is ook mogelijk, namelijk dat een meewerkende houding van de verdachte meeweegt in het opleggen van een lagere straf. De verdediging in de zaak Robert M. had aangevoerd dat het geven van zijn wachtwoorden aan de politie een strafverlichtende omstandigheid was. De rechtbank 'ziet onder ogen dat zonder de coöperatieve houding van verdachte tijdens

116 HR 14 maart 2006, *LJN* AU9353, r.o. 4.3.
117 Conclusie bij HR 14 maart 2006, *LJN* AU9353, §4.7.
118 Rb. Amsterdam 23 juli 2012, *LJN* BX2326, r.o. 8.3.

de politieverhoren, nog geen fractie van hetgeen nu aan het licht is gekomen, zou zijn geopenbaard'. Dit verbleekt echter ten opzichte van 'de afschuw die verdachte alom heeft gewekt met zijn handelingen'. De rechtbank heeft het afgeven van zijn wachtwoorden door Robert M. daarom niet in voor de verdachte gunstige zin laten meewegen in de straftoemeting.[119]

5.5 Het gebruik van zwijgen bij onttrekking aan het verkeer

Naast de straftoemeting kan een decryptieweigering ook meewegen bij een beslissing over onttrekking aan het verkeer van inbeslaggenomen gegevensdragers. In de zaak-Van der M. werden de computer en een harde schijf onttrokken aan het verkeer 'aangezien deze voorzien zijn van encryptie en de rechtbank niet kan vaststellen of verdachte met behulp daarvan de bewezen geachte feiten heeft begaan.'[120]
Een interessante parallel is de ontneming van wederrechtelijk verkregen voordeel. Op basis van artikel 36e Sr kan iemand die veroordeeld is voor een strafbaar feit, verplicht worden het voordeel terug te betalen dat hij uit het misdrijf heeft verkregen. Op basis van lid 3 mag, bij misdrijven met een geldboete van de vijfde categorie, ook voordeel worden ontnomen als uit onderzoek blijkt dat het 'aannemelijk is dat ook dat feit of andere strafbare feiten er op enigerlei wijze toe hebben geleid dat de veroordeelde wederrechtelijk voordeel heeft verkregen'. Bij de berekening van dat voordeel mag gebruik worden gemaakt van een bewijsvermoeden, waarbij het aan de verdachte is om dat vermoeden te weerleggen:

> 'Geen rechtsregel en met name niet art. 6 EVRM verzet zich ertegen dat in zaken als de onderhavige, waarin de grondslag van de vordering tot ontneming van het wederrechtelijk verkregen voordeel – hier het strafbare feit door middel van of waaruit dat voordeel is verkregen – in rechte is komen vast te staan, de bewijslast op redelijke en billijke wijze wordt verdeeld tussen het openbaar ministerie en de betrokkene.
> Daarbij dient in aanmerking te worden genomen dat de rechter steeds bevoegd is het door de betrokkene te betalen geldbedrag lager vast te stellen dan het voordeel dat hij volgens de schatting heeft verkregen.'[121]

De conclusie van A-G Machielse geeft een toelichting op de bewijslastverdeling:

> 'Zowel de wetgeschiedenis als de literatuur geven derhalve aanknopingspunten om voor de vaststelling van de omvang van het wederrechtelijk

119 Rb. Amsterdam 21 mei 2012, *LJN* BW6148, r.o. 8.1.3 onder 3.B.
120 Ibid., r.o. 10.3.
121 HR 28 mei 2002, *LJN* AE1182, r.o. 4.4 en 4.5.

> verkregen voordeel terzake van art. 36e lid 3 Sr gebruik te mogen maken van een rechterlijk vermoeden.
> Dat vermoeden is hierop gebaseerd dat in het geval iemand zich met (zware) georganiseerde criminaliteit bezig houdt en wanneer diens vermogen in de periode waarover die bezigheden zijn vastgesteld een spectaculaire groei ondergaat, minstgenomen het vermoeden rijst dat die inkomsten afkomstig zijn uit strafbare feiten. Het is geen onweerlegbaar vermoeden, maar de betreffende persoon zal zoals gezegd om de rechter te overtuigen van het tegendeel met een (aannemelijke) verklaring moeten komen, zeker wanneer het om zulke grote bedragen gaat als in de onderhavige zaak. (…)
> Het gebruik van een redelijk rechterlijk vermoeden kan nadrukkelijk niet als omkering van de bewijslast worden gekwalificeerd. In civilibus leidt de toepassing van een rechterlijk vermoeden ertoe dat een stelling van de partij op wie de bewijslast rust als voorlopig vaststaand wordt beschouwd. De wederpartij is vervolgens bevoegd tegenbewijs te leveren. Dat tegenbewijs behoeft niet te bestaan uit bewijs van het tegendeel; het zaaien van voldoende twijfel kan volstaan en het vermoeden doen vervallen.'[122]

Het model van ontneming van wederrechtelijk verkregen voordeel op basis van een bewijsvermoeden is interessant voor de vraag wanneer inbeslaggenomen beveiligde computers die de verdachte weigert te ontsleutelen, aan het verkeer mogen worden onttrokken. Evenals bij een voor bepaalde feiten veroordeelde persoon het bezit van een onverwacht grote hoeveelheid geld vragen oproept waarvoor de veroordeelde voldoende twijfel moet zaaien dat dit *niet* uit misdaad is verkregen (anders zal het in beslag worden genomen), zal bij een veroordeelde van bijvoorbeeld kinderpornografie het bezit van een onverwacht grote hoeveelheid opslagcapaciteit (zoals diverse harde schijven) vragen oproepen die hij moet beantwoorden als hij de inbeslaggenomen gegevensdragers wil terugkrijgen. Indien de verdachte de harde schijven niet wil ontsluiten, zal hij enigszins aannemelijk moeten maken waarom hij zoveel schijfcapaciteit heeft en waarom hij niet wil of kan ontsleutelen; als hij niet voldoende twijfel weet te zaaien over de stelling van de officier van justitie dat de schijven ook versleutelde kinderporno bevatten, zullen de gegevensdragers aan het verkeer kunnen worden onttrokken. Een soortgelijke redenering zou kunnen opgaan voor een veroordeelde van kinderpornografie die diverse harde schijven heeft met TrueCrypt erop, waarbij na het geven van een wachtwoord slechts een beperkt aantal onschuldige bestanden tevoorschijn komt en veel schijfruimte opengelaten is; de verdachte zou dan het vermoeden moeten weerleggen dat de ongebruikte schijfruimte nog een verborgen container met kinderpornografie bevat.
Het gebruiken van een decryptieweigering bij de beslissing om beveiligde computers aan het verkeer te onttrekken zal niet snel in strijd komen met het

122 Conclusie bij HR 28 mei 2002, *LJN* AE1182, §§3.21-3.22.

nemo-teneturbeginsel, zolang de verdachte maar in de gelegenheid wordt gesteld om enigszins aannemelijk te maken (in de zin van het zaaien van voldoende twijfel) dat de beveiligde computers geen strafbare feiten verhullen. Daarbij kan ook in aanmerking worden genomen dat artikel 551 Sv het toelaat om, bij verdenking van onder andere kinderpornografie, de uitlevering te vorderen van elk voorwerp ter verbeurdverklaring of onttrekking aan het verkeer, en dat bevel mag ook worden gegeven aan de verdachte.

5.6 Conclusie

In 1993 heeft de Nederlandse wetgever een ontsleutelplicht ingevoerd in het kader van een doorzoeking (later uitgebreid met andere situaties waarin versleutelde gegevens kunnen voorkomen), waarbij het bevel vanwege het nemo-teneturbeginsel niet aan verdachten mag worden gegeven, overigens meer vanwege moeilijke handhaafbaarheid dan om principiële redenen. De implementatie sluit aan bij de uitlevering van voorwerpen – het bevel kan niet worden gegeven aan verdachte – terwijl de motivering meer lijkt aan te sluiten bij het zwijgrecht. In dat licht zou het beter in de systematiek van het Wetboek van Strafvordering passen om de nemo-teneturbescherming bij de ontsleutelplicht te normeren conform de regeling van het verhoor in artikel 29 Sv.
Het Nederlandse recht rond nemo tenetur is sinds 2000 niet substantieel gewijzigd. De Hoge Raad sluit sterk aan bij de Europese rechtspraak en hanteert daarbij als maatstaf of het gebruik van een verklaring in een strafzaak het zwijgrecht, en daarmee het recht zichzelf niet te belasten, van zijn betekenis zou ontdoen. Dat is vooral het geval als een verdachte wordt gedwongen een intellectuele inspanning te leveren die mogelijk invloed heeft op de samenstelling of de inhoud van het bewijsmateriaal. Het recht zichzelf niet te belasten wordt daarom van zijn betekenis ontdaan a) als het zwijgrecht wordt uitgekleed of b) als er onnodige of disproportionele druk op de verdachte wordt uitgeoefend om materiaal te verkrijgen. Omdat een decryptiebevel dicht in de buurt komt bij de verklaringsvrijheid, zou een decryptiebevel voor verdachten, voor zover de weigering mee te werken strafbaar zou zijn, nog steeds afwijken van het systeem van de Nederlandse wet.
Ook als er geen strafrechtelijk gesanctioneerde plicht is om mee te werken, kan het niet meewerken soms toch worden gebruikt tegen de verdachte. De ruimte voor de rechter om negatieve gevolgen te verbinden aan de proceshouding van verdachten is er sinds 2000 zeker niet kleiner op geworden. Een belastende omstandigheid waarvoor de verdachte weigert een enigszins plausibele verklaring te geven, mag worden gebruikt om de stap te zetten naar een bewezenverklaring. Dit biedt ruimte voor rechters om, als een verdachte weigert een harde schijf of versleutelde bestanden toegankelijk te maken, in situaties waarin de aanwezigheid van de beveiligde bestanden dui-

delijk vragen oproept, dit mee te laten wegen in het bewijs. Ook kan een decryptieweigering worden gebruikt bij de verwerping van bepaalde verweren, bij de straftoemeting of bij andere beslissingen ten nadele van de verdachte.

6 Ontwikkelingen in het buitenlandse recht

6.1 België

In België is in 2001 een ontsleutelplicht ingevoerd. Het wetsontwerp, dat op 3 november 1999 werd gepubliceerd, viel buiten de periode van mijn onderzoek uit 2000, zodat dit een nieuwe ontwikkeling betreft. Deze ontwikkeling is bijzonder relevant voor het onderhavige onderzoek, aangezien het wetsontwerp een mogelijkheid bevatte verdachten te dwingen om cryptosleutels of wachtwoorden af te geven. Het wetsontwerp stelde de volgende bepaling voor in het Belgische Wetboek van Strafvordering (BSv):

> 'Art. 88quater. – §1. De onderzoeksrechter, evenals in zijn opdracht een officier van de gerechtelijke politie, hulpofficier van de procureur des Konings, kan personen waarvan hij vermoedt dat ze een bijzondere kennis hebben van een informaticasysteem dat het voorwerp uitmaakt van onderzoek of van diensten om gegevens, die worden opgeslagen, verwerkt of overgedragen via een informaticasysteem, te beveiligen of te versleutelen, bevelen inlichtingen te verlenen over de werking ervan en over de wijze om er toegang toe te verkrijgen of in een verstaanbare vorm toegang te verkrijgen tot de gegevens, die door middel daarvan worden opgeslagen, verwerkt of overgedragen.
> § 2. Indien nodig, kan de onderzoeksrechter iedere relevante persoon bevelen om zelf het informaticasysteem te bedienen of de pertinente gegevens, die door middel daarvan worden opgeslagen, verwerkt of overgedragen, naargelang het geval, te zoeken, toegankelijk te maken, te kopieren, ontoegankelijk te maken of te verwijderen, in de door hem gevorderde vorm. Deze personen zijn verplicht hieraan gevolg te geven, voorzover dit in hun mogelijkheden ligt.
> Het bevel om zelf de pertinente gegevens te zoeken kan niet worden gegeven aan de verdachte en aan de personen bedoeld in artikel 156.'[123]

De voorgestelde bepaling maakte een onderscheid tussen twee typen medewerking. Lid 1 betreft het geven van inlichtingen. 'Hierbij wordt onder andere gedacht aan de toegangsmogelijkheden, de configuratie, de beveiliging en de cryptografische sleutels.'[124] Lid 2 betreft het zelf bedienen van de computer, 'bijvoorbeeld het doen functioneren van de computer, het opvragen van bepaalde files, …'.[125] Dit omvat vermoedelijk ook, hoewel de toelichting dat niet expliciet vermeldt, het bevel aan iemand om zelf versleutelde gegevens te ontsleutelen en vervolgens de ontsleutelde gegevens aan de bevoegde ambtenaar te overhandigen. Daarbij wordt vooral gedacht aan 'importeurs/

123 Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nrs. 213/1 en 214/1, Voorontwerp van wet, p. 38 (§3-5 weggelaten uit citaat). Artikel 156 BSv betreft naaste bloed- en aanverwanten en (ex-)echtgenoten van de beklaagde.

124 Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nrs. 213/1 en 214/1, Memorie van Toelichting, p. 27.

125 Ibid.

verdelers van computers of software, "trusted third parties", dienstenverstrekkers, operatoren, bedrijfsingenieurs die een specifieke informaticaconfiguratie hebben uitgewerkt, beveiligingsspecialisten, …'.[126] De toelichting legt uit dat de medewerking bij lid 2 onder het nemo-teneturbeginsel valt, maar de medewerking bij lid 1 niet:

> 'De verplichting om bepaalde data te zoeken kan evenwel niet worden opgelegd aan de verdachte, gezien de bescherming tegen zelf-incriminatie.
> De verdachte moet hier immers, zoals in de context van de getuigenverklaring, zijn zwijgrecht kunnen laten gelden. De andere verplichtingen zijn in dit opzicht evenwel niet onverenigbaar met de vereisten die worden gesteld door het EVRM (zie bijvoorbeeld het arrest Saunders tegen het Verenigde Koninkrijk van 17 december 1996).'[127]

Het zelf ontsleutelen moet, volgens de toelichting, dus worden gezien als een actieve medewerking van de verdachte die vergelijkbaar is met het afleggen van een verklaring. Het geven van inlichtingen in de vorm van een wachtwoord of cryptosleutel is echter wel verenigbaar met het nemo-teneturbeginsel; kennelijk is het vergelijkbaar met het overhandigen van materiaal dat onafhankelijk van de wil van de verdachte bestaat. Daarom maakt het voorstel slechts een uitzondering voor de verdachte in lid 2, maar niet in lid 1.

De bepaling werd echter geamendeerd waarbij het bevel van lid 1 niet meer aan de verdachte mag worden gegeven. De laatste zin van lid 2 is gewijzigd in de tekst zoals aangenomen door de commissie voor de justitie in de Kamer en vervolgens door de Kamer en Senaat. De definitieve bepaling luidt aldus:[128]

> 'Art. 88quater. § 1. De onderzoeksrechter, of in zijn opdracht een officier van gerechtelijke politie, hulpofficier van de procureur des Konings, kan personen van wie hij vermoedt dat ze een bijzondere kennis hebben van het informaticasysteem dat het voorwerp uitmaakt van de zoeking of van diensten om gegevens die worden opgeslagen, verwerkt of overgedragen door middel van een informaticasysteem, te beveiligen of te versleutelen, bevelen inlichtingen te verstrekken over de werking ervan en over de wijze om er toegang toe te verkrijgen, of in een verstaanbare vorm toegang te verkrijgen tot de gegevens die door middel daarvan worden opgeslagen, verwerkt of overgedragen. De onderzoeksrechter vermeldt de omstandigheden eigen aan de zaak die de maatregel wettigen in een met

126 Ibid.
127 Ibid., 27-28.
128 Wet van 28 november 2000 inzake informaticacriminaliteit, *Moniteur belge / Belgisch staatsblad* 3 februari 2001, 2909-2914 (cursivering toegevoegd).

redenen omkleed bevelschrift dat hij meedeelt aan de procureur des Konings.
§ 2. De onderzoeksrechter kan iedere geschikte persoon bevelen om zelf het informaticasysteem te bedienen of de ter zake dienende gegevens, die door middel daarvan worden opgeslagen, verwerkt of overgedragen, naargelang het geval, te zoeken, toegankelijk te maken, te kopiëren, ontoegankelijk te maken of te verwijderen, in de door hem gevorderde vorm. Deze personen zijn verplicht hieraan gevolg te geven, voorzover dit in hun mogelijkheden ligt.
Het bevel bedoeld in het eerste lid kan niet worden gegeven aan de verdachte en aan de personen bedoeld in artikel 156.
§ 3. Hij die weigert de in §§1 en 2 gevorderde medewerking te verlenen of de zoeking in het informaticasysteem hindert, wordt gestraft met gevangenisstraf van zes maanden tot één jaar en met geldboete van zesentwintig frank tot twintigduizend frank of met een van die straffen alleen.
§ 4. Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of daaraan zijn medewerking verleent, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.
§ 5. De Staat is burgerrechtelijk aansprakelijk voor de schade die onopzettelijk door de gevorderde personen aan een informaticasysteem of de gegevens. die door middel daarvan worden opgeslagen, verwerkt of overgedragen, wordt veroorzaakt.'

In de parlementaire stukken[129] is echter niet te vinden waarop deze wijziging is gebaseerd. De amendementen voor artikel 88quater BSv die worden besproken in het verslag van de commissie[130] betreffen andere gedeelten van het artikel. Ik heb niet kunnen achterhalen welke motivatie ten grondslag heeft gelegen aan de wijziging.[131] Evenmin is duidelijk waarom de nemoteneturclausule van lid 2 alleen verwijst naar het bevel van lid 1, waardoor het lijkt alsof het bevel van lid 2 nu wel gegeven zou kunnen worden aan de verdachte. Dat zal niet zo gelezen moeten worden, aangezien de oorspronkelijke toelichting stelde dat het bevel van lid 2 meer inbreuk maakte op het nemoteneturbeginsel dan het bevel van lid 1. In de praktijk gaat men ervan uit dat de laatste zin van lid 2 het gehele artikel 88quater BSv betreft.[132]

Tegelijk met het medewerkingsbevel bij een doorzoeking is ook een medewerkingsplicht ingevoerd ten aanzien van versleutelde communicatie die

129 Beschikbaar op www.senate.be/www/?MIval=dossier&LEG=2&NR=392&LANG=nl (geraadpleegd 1 september 2012).
130 Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 214/005, p. 1 (Amendement nr. 10); nr. 214/006, p. 3 (Amendement nr. 19); nr. 213/004, Verslag namens de commissie voor de justitie, p. 67-68.
131 De uitvoerige studie van Dirk Merckx (Merckx 2001, p. 194-199, 213-220) bespreekt het wetsontwerp en de uiteindelijke wet zonder in te gaan op de verandering van lid 2; bij de bespreking van het verbod op zelfincriminatie gaat de auteur niet in op de Belgische wetgeving, maar bespreekt hij slechts buitenlandse literatuur.
132 Philippe van Linthout, persoonlijke mededeling, 25 april 2012.

wordt afgetapt, in artikel 90quater §4 BSv. Het wetsontwerp noemt daarbij dezelfde twee typen medewerking (geven van inlichtingen omtrent de beveiliging dan wel zelf de telecommunicatie toegankelijk maken in de gevorderde vorm), evenwel zonder een uitzondering te maken voor verdachten.[133] De bepaling ziet evenwel niet op een bevel aan de zender of de ontvanger, maar op een bevel aan de telecomaanbieder ('Deze bepaling regelt de medewerking van de personen verbonden aan een telecommunicatiedienst')[134] – vandaar dat er wordt toegevoegd dat de geadresseerden verplicht zijn mee te werken 'voorzover dit in hun mogelijkheden ligt'. De voorkeur zou daarbij moeten zijn om de geadresseerde zelf te laten ontsleutelen en niet om de sleutel af te geven.[135] De bepaling is wat dit betreft niet gewijzigd, zodat moet worden aangenomen dat, ook al ontbreekt een nemo-teneturclausule in de tekst van artikel 90quater §4 BSv, dit bevel niet aan verdachten kan worden gegeven. Het gaat dus om een vergelijkbare bepaling als het Nederlandse artikel 126m/t/zg leden 6-7 Sv.

In de rechtspraktijk wordt wel enige behoefte gevoeld aan een ontsleutelplicht voor verdachten. Een dergelijke mogelijkheid wordt niet als heel effectief gezien vanwege de technische mogelijkheden om encryptiegebruik te maskeren door programma's als TrueCrypt (zie paragraaf 3.3). Bij minder slimme criminelen zou een ontsleutelplicht echter wel kunnen werken, evenals bij misdadigers die encryptieprogramma's gebruiken zonder maskering. Dat zou de opsporing dan een stap verder helpen.[136]

6.2 Frankrijk

6.2.1 Achtergrond

Frankrijk heeft van oudsher een omvangrijke regulering van cryptografie.[137] De import, het gebruik en het aanbieden van cryptografie was lange tijd onderhevig aan een notificatie- en vergunningstelsel; in de tweede helft van de jaren negentig was gebruik van sterkere cryptografie onderworpen aan een plicht de sleutel te deponeren bij een speciale overheidsdienst. Rond de eeuwwisseling werd het regime geliberaliseerd in het kader van een nieuw beleid voor de informatiemaatschappij, waarbij het vergunningstelsel werd gehandhaafd voor het aanbieden van cryptodiensten[138] maar het gebruik van cryptografie door burgers en bedrijven werd vrijgegeven, zodat zij in de net-

133 Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nrs. 213/1 en 214/1, Voorontwerp van wet, p. 39-40.
134 Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 213/004, Verslag namens de commissie voor de justitie, p. 92.
135 Ibid.
136 Interview onderzoeksrechter België.
137 Voor een overzicht, zie http://rechten.uvt.nl/koops/cryptolaw/cls2.htm#fr (geraadpleegd 1 september 2012).
138 Zie Titel III, hoofdstuk 1 van Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (beschikbaar via www.legifrance.gouv.fr/ (geraadpleegd 1 september 2012)).

werksamenleving hun privacy goed konden beschermen. Het vrijgeven van cryptogebruik diende echter gepaard te gaan met veiligheidsmaatregelen:

> 'It is essential that freer use of encryption techniques be matched by a security policy.
> The first step in this policy must involve updating the government's tools for guaranteeing public freedoms and combating the use of encryption methods for criminal purposes. In legislative terms, this will mean strengthening the powers of judges to access non-encrypted versions of data records (requirement to turn over the decryption keys or an uncoded document), so that they can conduct the investigations required for proper functioning of the legal process. These broader powers shall comply with the provisions of the European Human Rights Convention.'[139]

Het beleid voor de informatiemaatschappij werd vertaald in een wetsvoorstel voor de informatiemaatschappij.[140] Dit wetsvoorstel is gestrand in het parlement, maar vele onderdelen ervan zijn gebruikt in andere wetsvoorstellen. Drie onderdelen beogen de gevolgen van het vrijgeven van cryptografiegebruik te compenseren.

6.2.2 Hulp bij het kraken van cryptografie

Het eerste onderdeel betreft het faciliteren van het kraken van cryptografie. Artikelen 230-1 tot en met 230-5 van de Franse Code de procédure pénale (CPP, Wetboek van Strafvordering) beogen dit te bevorderen door deskundigen in te schakelen. Artikel 230-1 CPP luidt:

> 'Onverminderd de bepalingen van artikelen 60, 77-1 en 156,[141] kan, wanneer blijkt dat gegevens, die in beslag genomen of verkregen zijn in de loop van het onderzoek of gerechtelijk vooronderzoek, op dusdanige wijze zijn bewerkt dat zij de toegang verhinderen tot klare informatie die erin is bevat of verhinderen deze te begrijpen, de procureur de la République, de juridiction d'instruction of de juridiction de jugement[142] die met de zaak is belast, elke gekwalificeerde natuurlijke of rechtspersoon aanwijzen om technische bewerkingen uit te voeren die het mogelijk maken de versie in klare tekst van die informatie te verkrijgen, evenals, wanneer een cryptologisch middel is gebruikt, de geheime decryptiesleutel wanneer dat nodig blijkt. (…)

139 Ministère de l'Économie des Finances et de l'Industrie 1999, paragraaf 3.4.
140 Projet de loi sur la société de l'information, Nº 3143, www.assemblee-nationale.fr/11/pdf/projets/pl3143.pdf (geraadpleegd 1 september 2012).
141 Deze artikelen zien op het doen van een beroep op gekwalificeerde personen om een technisch of wetenschappelijk onderzoek uit te voeren, uit een deskundigenregister of anderszins.
142 Deze functionarissen zijn vergelijkbaar met de officier van justitie, de rechter-commissaris en de zittingsrechter.

> Wanneer de straf gelijk is aan of hoger dan twee jaar gevangenisstraf en wanneer de eisen van het onderzoek of het gerechtelijk vooronderzoek het vereisen, kan de procureur de la République, de juridiction d'instruction of de juridiction de jugement die met de zaak is belast voorschrijven dat een beroep wordt gedaan op de middelen van de Staat die zijn onderworpen aan geheimhouding van de nationale defensie, op de wijze die bij dit hoofdstuk is voorzien.'[143]

De volgende artikelen regelen vervolgens hoe justitie een beroep kan doen op defensie.[144] De bepalingen zijn ingevoerd door de Wet op de dagelijkse veiligheid.[145] In maart 2001 was het wetsvoorstel daarvoor ingediend bij het parlement, maar dit bevatte oorspronkelijk geen cryptografiebepaling. Het voorstel lag in tweede lezing bij de Senaat toen de aanslagen van 11 september 2001 plaatsvonden. Deze dramatische gebeurtenissen toonden volgens de regering aan dat bepaalde instrumenten in het juridische arsenaal ontbraken om effectief het terrorisme te bestrijden. Vanuit de zorg dat snel maatregelen moesten worden genomen, werden diverse amendementen voorgesteld binnen het reeds aanhangige wetsvoorstel.[146] Een van deze betrof de mogelijkheid voor justitie om een beroep te doen op de defensiedeskundigen[147] om versleutelde gegevens die bij een strafrechtelijk onderzoek zijn verkregen te ontsleutelen.[148] Amendement nr. 10 stelde daarvoor de artikelen 230-1 tot en met 230-5 CPP voor, rechtstreeks overgenomen uit artikel 47 van het wetsvoorstel voor de informatiemaatschappij. De toelichting bij het amendement legt de nadruk op de moeilijke kraakbaarheid van de cryptografie die wordt gebruikt binnen terroristische netwerken. Voor het ontsleutelen daarvan is de hoogste expertise vereist, die binnen defensie beschikbaar is; de regeling beoogt die capaciteit te benutten op een manier dat de resultaten in een strafzaak gebruikt kunnen worden.[149]
De toelichting in de Assemblée nationale van 20 oktober 2001 plaatst de invoering van deze bepalingen eveneens in het kader van terrorismebestrijding door te wijzen op berichten dat de terroristen die de aanslagen van

143 Art. 230-1, eerste en derde lid CPP [mijn vertaling]. De integrale versie van de Franse wetgeving is te vinden in bijlage 3.
144 Caprioli 2002, p. karakteriseert de regeling als de 'organisatie van decryptie' van vercijferde berichten zonder de sleutel te kennen, oftewel het 'kraken', waarbij een complexe regeling nodig is om de juridische en organisatorische verschillen tussen justitie en defensie te overbruggen.
145 Art. 30 en 31 van Loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne.
146 Rapport nº 7 de M. Jean-Pierre Schosteck, Sénat, 10 octobre 2001, p. 8.
147 De tekst spreekt van 'moyens de l'Etat soumis au secret de la défense nationale', wat zowel op veiligheidsdiensten als defensie zou kunnen slaan. Ik laat de precieze betekenis hiervan buiten beschouwing en gebruik gemakshalve de term 'defensie'.
148 Ibid., p. 9.
149 'La transmission de messages cryptés par la voie de l'internet s'est révélée être une forme privilégiée de communication entre membres d'un réseau terroriste. Dans les cas les plus sophistiqués de cryptologie, le déchiffrement de ces messages suppose d'avoir recours à des experts de très haut niveau voire à des moyens d'Etat couverts par le secret de la défense nationale. Il est nécessaire d'organiser le recours à ces moyens de manière à assurer leur fiabilité juridique dans le cadre d'une procédure pénale.' Projet de loi nº 420 (2000-2001), 7, Amendement Nº 10 rect., 15 octobre 2001.

11 september pleegden, technieken gebruikten om bepaalde elektronische berichten onleesbaar te maken.

> 'Het lijkt daarom noodzakelijk en dwingend om aan de magistraten die het onderzoek leiden, of het nu gaat om de procureur of de rechter van instructie of de zittingsrechter, toegang te krijgen in klare tekst tot de inhoud van die berichten. Derhalve worden de genoemde autoriteiten bevoegd, wanneer zij geconfronteerd worden met een versleuteld bericht, om zich te wenden tot "iedere gekwalificeerde natuurlijke of rechtspersoon" teneinde bewerkingen uit te voeren die de versie in klare tekst doen verkrijgen.'[150]

De term 'gekwalificeerde personen' wordt in het wetboek veelal gebruikt voor (technische of wetenschappelijke) deskundigen (in art. 60, 77-1 en 157 CPP waar de bepaling naar verwijst) of anderszins personen met een bepaalde kwalificatie. Artikel 230-1 CPP is dus een bevoegdheid om cryptografisch deskundigen in te schakelen om te helpen berichten te kraken; ook kan gedacht worden aan aanbieders van cryptografiediensten die, afhankelijk van de inrichting van hun dienst, mogelijk in staat zouden zijn om de communicatie van hun klanten te ontsleutelen.

6.2.3 Strafbaarstelling van decryptieweigering

Het tweede onderdeel betreft de strafbaarstelling van een weigering mee te werken aan ontsleuteling in artikel 434-15-2 van de Franse Code pénal (CP, Wetboek van Strafrecht):

> 'Met drie jaar gevangenisstraf en een boete van € 45.000 wordt gestraft, voor eenieder die kennis heeft van de geheime decryptiesleutel van een cryptologisch middel dat gebruikt kan zijn om een misdrijf of een overtreding voor te bereiden, te faciliteren of te plegen, de weigering genoemde sleutel aan de justitiële autoriteiten te overhandigen of deze toe te passen, volgens de vordering van deze autoriteiten op basis van titels II en III van het eerste boek van het Wetboek van Strafvordering.
> Als de weigering is geschied terwijl de overhandiging of toepassing van de sleutel het mogelijk gemaakt zou hebben het plegen van een misdrijf of overtreding te voorkomen of de effecten ervan te verkleinen, wordt de straf verhoogd tot vijf jaar gevangenisstraf en een boete van € 75.000.'[151]

150 Rapport nº 3352 de M. Bruno Le Roux, Assemblée nationale, 20 octobre 2001, p. 14 [mijn vertaling].
151 Artikel 434-15-2 CP [mijn vertaling].

Deze bepaling is op dezelfde manier als de hiervoor behandelde bepalingen ingevoerd door de Wet op de dagelijkse veiligheid, via Amendement nr. 11.[152] De toelichting bij dat amendement geeft zonder verdere context aan dat artikel 434-15-2 CP met straf bedreigt zowel degene die een cryptosleutel kent en weet dat deze gebruikt is voor het voorbereiden of plegen van een strafbaar feit maar deze sleutel niet aan justitie overhandigt, als degene die de overhandiging weigert om het plegen van een strafbaar feit te voorkomen of de effecten ervan te verzachten.[153] Het gaat om alle personen die de sleutel kunnen kennen, zoals de houder van een bestand, de zender of ontvanger(s) van een bericht en de cryptografieaanbieder (als die binnen de context van zijn dienst toegang heeft tot sleutels).[154]
Deze bepaling is eveneens rechtstreeks overgenomen uit het eerdere wetsvoorstel over de informatiemaatschappij, waarin het niet verder was toegelicht,[155] en het amendement is zonder verdere toelichting of discussie aangenomen door het parlement. Waar het eerdere wetsvoorstel, in het verlengde van het hierboven geciteerde beleidsdocument, deze bepaling invoerde als compensatie voor het vrijgeven van cryptogebruik,[156] is het uiteindelijk door het parlement dus zonder discussie aangenomen onder het mom van terrorismebestrijding. Het is echter niet beperkt tot terroristische misdrijven maar geldt bij alle strafbare feiten, in beginsel zelfs bij overtredingen.
Titels II en III van boek 1 CPP, waar de strafbaarstelling naar verwijst, regelen het opsporings- en gerechtelijk vooronderzoek. Daarin is geen expliciete bepaling opgenomen voor de officier of rechter om iemand te bevelen te ontsleutelen. Kennelijk bevatten de reguliere bevoegdheden uit titels II en III een impliciete bevoegdheid om iemand te bevelen een decryptiesleutel af te geven of zelf te ontsleutelen in gevallen waarin bij een strafrechtelijk onderzoek versleutelde gegevens in het geding zijn die (vermoedelijk) in relatie staan tot een (gepleegd of te plegen) strafbaar feit. De strafbaarstelling fungeert daarmee als stok achter de deur voor verdachten om mee te werken wanneer justitie daarom vraagt.[157]

152 Projet de loi nº 420 (2000-2001), 7, Amendement Nº 11, 15 octobre 2001. Het amendement bevat ook een verplichting voor cryptografieaanbieders, die vergunningplichting waren, om sleutels in hun bezit te overhandigen, met een strafrechtelijke sanctionering. Om de discussie niet nog gecompliceerder te maken, laat ik deze bepalingen buiten beschouwing.

153 Ibid.

154 Caprioli 2002.

155 Zie art. 46 Projet de loi sur la société de l'information, Nº 3143, www.assemblee-nationale.fr/11/pdf/projets/pl3143.pdf (geraadpleegd 1 september 2012).

156 Volgens Warusfel 2002 zijn de bepalingen mede een uitvloeisel van Aanbeveling R 95(13) van de Raad van Europa: 'Measures should be considered to minimise the negative effects of the use of cryptography on the investigation of criminal offences, without affecting its legitimate use more than is strictly necessary.'

157 Ibid. ('Pour faire pression sur ces détenteurs, la [Loi sur la sécurité quotidienne] introduit dans le code pénal un nouvel article 434-15-2').

6.2.4 Strafverhoging bij encryptiegebruik

Een andere stok achter de deur betreft het derde onderdeel uit het wetsvoorstel voor de informatiemaatschappij,[158] dat is overgenomen in de Wet voor het vertrouwen in de digitale economie van 2004. Volgens een nieuw artikel 132-79 Code pénal wordt de maximumgevangenisstraf voor delicten één categorie verhoogd[159]

> 'wanneer een middel voor cryptologie (…) is gebruikt voor het voorbereiden van een misdrijf of overtreding, of om het voorbereiden of plegen ervan te faciliteren (…).
> De bepalingen van dit artikel zijn evenwel niet van toepassing op de pleger of medeplichtige van het strafbaar feit die, desgevraagd door de justitiële of administratieve autoriteiten, hun de versie in klare tekst van vercijferde berichten ter beschikking heeft gesteld zowel als de geheime decryptiesleutels die noodzakelijk zijn voor de ontcijfering.'[160]

Het gebruik van cryptografie bij het voorbereiden, faciliteren of plegen van een strafbaar feit is aldus een strafverzwarende omstandigheid, waarbij het meewerken aan een ontsleutelingsvraag helpt om aan een zwaardere straf te ontkomen. In deze vorm is er geen strafrechtelijk gesanctioneerde ontsleutelplicht voor verdachten, maar wel een strafverhogingsuitsluitingsgrond voor decryptie. De bepaling is niet nader toegelicht in het wetsvoorstel en was evenmin toegelicht in het wetsvoorstel voor de informatiemaatschappij. Het betreft kennelijk simpelweg een maatregel die beoogt compensatie te bieden voor het vrijgeven van cryptografie.

6.2.5 Inbreuk op het nemo-teneturbeginsel?

Waar het beleidsdocument dat aan de hier behandelde maatregelen ten grondslag ligt, nog opmerkt dat de wettelijke vereisten om decryptiesleutels of klare tekst aan justitie te overhandigen moeten voldoen aan het EVRM (zonder overigens specifiek art. 6 te noemen),[161] is er bij de totstandkoming van de wetgeving – voor zover ik in de parlementaire stukken heb kunnen vinden – niet gediscussieerd over de relatie tussen de strafbaarstelling van decryptieweigering en het nemo-teneturbeginsel. Uit de context van de strafbaarstelling en strafverhoging lijkt duidelijk te volgen dat verdachten kan worden gevorderd te ontsleutelen. Het Franse strafprocesrecht, dat klassiek inquisitoir is, kent voor zover mij bekend geen algemene nemo-teneturbepaling op basis waarvan verdachten zich zouden kunnen verschonen van

158 Art. 45 Projet de loi sur la société de l'information, Nº 3143.
159 Dat wil zeggen steeds één categorie hoger in de reeks 5 jaar, 7 jaar, 10 jaar, 15 jaar, 20 jaar, 30 jaar, levenslang; bij delicten met een gevangenisstraf tot 3 jaar wordt het maximum verdubbeld.
160 Art. 132-79 CP, ingevoerd door Loi nº 2004-575 de 21 juin 2004 pour la confiance dans l'économie numérique.
161 Zie boven, noot 139.

medewerking. Het nemo-teneturbeginsel speelt wel een rol in de doctrine in verband met artikel 6 EVRM,[162] zodat verdachten zich daar wellicht op zouden kunnen beroepen als zij worden vervolgd voor decryptieweigering of een hogere strafeis krijgen in de hoofdzaak. Of een dergelijk beroep zou worden gehonoreerd, is echter niet duidelijk bij gebrek aan rechtspraak over de onderhavige bepalingen. Potentieel relevant is de recente ontwikkeling van de nadere normering van het verhoor, waarbij, in navolging van de *Salduz*- en *Brusco*-jurisprudentie, is geregeld dat degene die in verzekering is gesteld, wordt geïnformeerd over zijn zwijgrecht en zijn recht op toegang tot een advocaat.[163] Het is voorstelbaar dat dit een bredere uitstraling krijgt naar andere vormen van medewerking tijdens het opsporingsonderzoek.[164] Wat daar verder van zij, de wettelijke regeling van artikelen 434-15-2 en 132-79 CP is in elk geval dusdanig dat een decryptiebevel wel aan verdachten kan worden gegeven, waarbij een expliciete nemo-teneturregeling ontbreekt.
Dat is opmerkelijk, omdat een strafbedreiging van drie jaar gevangenisstraf – zeker bij minder ernstige delicten – op zijn minst de vraag oproept of dit niet een ontoelaatbare vorm van druk oplevert voor verdachten om mee te werken. Daar komt bij dat de wet geen nadere aanduiding geeft van de maatstaven voor de strafrechtelijke aansprakelijkheid, in de zin van de aannemelijkheid dat iemand de sleutel heeft[165] of de waarschijnlijkheid dat de versleutelde gegevens verband houden met een strafbaar feit. Ook is er geen expliciete regeling van voorwaarden waaronder justitie iemand kan vragen of bevelen te ontsleutelen. Anders dan de Britse regeling kent de Franse regeling dus veel minder expliciete procedures of waarborgen voor het meewerken aan ontsleuteling door verdachten.
Caprioli stelt dan ook dat artikel 434-15-2 CP mogelijk in strijd zou kunnen zijn met het EVRM wegens strijd met het nemo-teneturbeginsel; hij werkt dat evenwel niet uit.[166] Warusfel stelt in zijn bespreking van de Wet op de dagelijkse veiligheid (waarin hij naast de cryptobepalingen ook de bewaarplicht voor verkeersgegevens bespreekt) dat bij deze complexe en te snel aangenomen wet bovenal de vraag blijft staan of de veiligheidsmaatregelen verenigbaar zijn met het noodzakelijke respect voor de burgerlijke vrijheden en de privacy van burgers; hij noemt daarbij echter niet expliciet het nemo-teneturbeginsel.[167]
Ik heb geen jurisprudentie kunnen vinden over de toepassing van artikel 230-1 CCP of de bepalingen uit de Code pénal. Een standaardhandboek over het Franse recht rond cybercriminaliteit beperkt zich, na een korte weergave

162 Pieter Verrest, persoonlijke mededeling 29 augustus 2012.
163 Art. 63-1 CCP, aangepast door artikel 3 Loi n° 2011-392 du 14 avril 2011 relative à la garde à vue.
164 Pieter Verrest, persoonlijke mededeling 29 augustus 2012.
165 Caprioli (2002) stelt de vraag (zonder deze te beantwoorden) wat er gebeurt als iemand zijn sleutel verloren of per ongeluk vernietigd heeft en wel wil maar niet kan meewerken. Op een weblog van cryptografiefanaten wordt gesteld dat 'ik ben de sleutel vergeten' geen verweer zou zijn bij art. 434-15-2 CP en dat men daarom alle ooit gebruikte sleutels zou moeten bewaren. www.artiflo.net/2011/02/la-loi-truecrypt-et-le-chiffrement-de-disque-en-france/, bijdrage van Florian Cristina d.d. 6 maart 2011.
166 Ibid.
167 Warusfel 2002, p. 22.

van de cryptobepalingen zonder verdere uitleg, tot de constatering dat tot op heden de bepalingen om een beroep te doen op defensie 'nog niet in een significant aantal zaken zijn toegepast'; het vermeldt niet of de strafverzwaring in de praktijk wordt toegepast.[168]

6.3 Verenigd Koninkrijk

In mijn onderzoek uit 2000 beschreef ik dat in het Verenigd Koninkrijk (VK) in 1999 een ontsleutelplicht was voorgesteld in een consultatiedocument en vervolgens in een wetsvoorstel was opgenomen, de *Electronic Communications Bill*. Het bevel zou gegeven kunnen worden aan verdachten en was gesanctioneerd met maximaal twee jaar gevangenisstraf. Dit zou geen inbreuk maken op het nemo-teneturbeginsel omdat het ging om het begrijpelijk maken van bewijs dat al in handen is van de opsporingsinstanties, niet om een verdachte te bevelen om bewijs te onthullen. Vanwege de vele kritiek op dit voorstel werd het uit dit wetsvoorstel gehaald met de bedoeling het terug te laten komen in het wetsvoorstel Regulation of Investigatory Powers Bill, dat ten tijde van mijn onderzoek uit 2000 nog niet beschikbaar was.[169] Bij mijn afweging in 2000 over een Nederlandse ontsleutelplicht voor verdachten woog mee dat in het VK het voorstel (vooralsnog) niet was ingevoerd en dat het sterke weerstand had opgeroepen.[170]

6.3.1 De Regulation of Investigatory Powers Act 2000

Inmiddels is wel een ontsleutelplicht in het Verenigd Koninkrijk ingevoerd. De Regulation of Investigatory Powers Bill, die in februari 2000 werd aangeboden aan het parlement, bevatte een bevel voor geadresseerden, inclusief verdachten, om cryptosleutels af te geven. Op het voorstel kwam de nodige kritiek, vanwege gebrekkige onderbouwing van de noodzaak van deze maatregel, en ook vanwege het gebrek aan procedurele en technische waarborgen voor omgang met afgegeven sleutels en het feit dat het ook mogelijk zou moeten zijn om geadresseerden zelf te laten ontsleutelen, omdat dit minder privacybedreigend is (de opsporingsdienst krijgt dan alleen toegang tot de specifiek benodigde bestanden of berichten in plaats van tot alle, ook irrelevante, bestanden).[171] Dit laatste werd mogelijk gemaakt door aanpassing van het wetsvoorstel; ook kwam de bewijslast meer te liggen bij de autoriteiten om aan te tonen dat de geadresseerde in staat is te ontsleutelen, in plaats van dat de geadresseerde primair aannemelijk moest maken dat hij de sleutel niet had.[172]

168 Quéméner & Charpenel 2010, p. 175-176 [mijn vertaling].
169 Koops 2000, p. 24-25.
170 Ibid., p. 93.
171 Gladman 2000; zie ook Chatterjee 2011, p. 268-269.
172 Chatterjee 2011, p. 269.

De wet werd aangenomen en in juli 2000 gepubliceerd als de Regulation of Investigatory Powers Act 2000 (hierna: RIPA).[173] Deel III (dat pas later in werking trad, zie onder) bevat een omvangrijke en complexe regeling van het ontsleutelbevel (zie bijlage 2 voor de integrale tekst). Samengevat bepaalt Title III dat een ambtenaar van politie, veiligheidsdienst of douane die versleutelde informatie heeft verkregen, een schriftelijk bevel kan geven aan iemand die redelijkerwijs geacht kan worden de sleutel te hebben, om de beschermde informatie vrij te geven ('impose a disclosure requirement in respect of the protected information') (s. 49). De begrippen 'sleutel' en 'beveiligde informatie' zijn ruim omschreven en zien ook op wachtwoordbeveiliging van een computer; onder 'sleutel' wordt ook verstaan het algoritme of andere informatie die nodig is om toegang te krijgen tot elektronische gegevens of om gegevens in begrijpelijke vorm om te zetten (s. 56(1)).
Voor het geven van een ontsleutelbevel is toestemming nodig van een bevoegde autoriteit, conform de (tamelijk complexe) regeling van Schedule 2. In het kader van opsporing is de bevoegdheid tot het geven van een ontsleutelbevel grotendeels gekoppeld aan de bevoegdheid die nodig is (of was) om de beveiligde gegevens te verkrijgen. Als de gegevens verkregen zijn op basis van een wettelijke bevoegdheid die een rechterlijke machtiging vereist, zal de desbetreffende rechter (of een andere rechter) toestemming moeten geven voor een ontsleutelbevel (s. 2 van Schedule 2). Als data verkregen zijn op basis van een wettelijke bevoegdheid waarvoor geen rechterlijke machtiging nodig is, is de opsporingsambtenaar (van politie of douane) zelf bevoegd het ontsleutelbevel te geven (s. 4 van Schedule 2), als hij ten minste een *superintendent* (of hoger) is of toestemming heeft van een *superintendent* (of hoger) (s. 6 van Schedule 2). Wanneer data verkregen zijn zonder uitoefening van een wettelijke bevoegdheid, moet de politie terugvallen op de algemene bepaling van s. 1 van Schedule 2, namelijk dat in alle gevallen een rechter[174] toestemming kan geven voor een ontsleutelbevel.
Het bevel moet voldoen aan de beginselen van proportionaliteit en subsidiariteit (s. 49(2)(c-d)) en noodzakelijk zijn in verband met nationale veiligheid, opsporing of voorkoming van misdaad of het economisch welzijn van het VK (s. 49(3)). Het bevel moet specificeren welke beveiligde informatie wordt bedoeld (s. 49(4)(b)). Het bevel mag niet de uitlevering vorderen van een sleutel die alleen wordt gebruikt om elektronische handtekeningen te plaatsen (s. 49(9)). Voor situaties, met name binnen bedrijven, waar meerdere personen vermoedelijk toegang hebben tot de sleutel, moet de hoogst verantwoordelijke binnen het bedrijf worden aangesproken (s. 49(5-7)).
De geadresseerde kan zelf ontsleutelen dan wel de sleutel afgeven (s. 50(1-2)). Als er meerdere sleutels beschikbaar zijn, kan de geadresseerde volstaan met

173 Regulation of Investigatory Powers Act 2000, 2000 Chapter 23. De wet is beschikbaar op www.legislation.gov.uk/ukpga/2000/23/contents/enacted (originele versie); de actuele versie van RIPA is beschikbaar op www.legislation.gov.uk/ukpga/2000/23/contents (geraadpleegd 1 september 2012).

174 Dat wil zeggen een 'Circuit judge' in Engeland en Wales, een sheriff in Schotland, en een 'county court judge' in Noord-Ierland.

de minimale hoeveelheid sleutels die nodig is om de beveiligde informatie vrij te geven (s. 50(4-7)). Als de geadresseerde de sleutel niet meer heeft maar wel informatie die kan helpen bij het vinden van de sleutel of het toegankelijk maken van de beveiligde informatie, dan is hij verplicht deze informatie te geven (s. 50(8-9)). Onder bijzondere omstandigheden kan, wanneer de bevoegde autoriteit dat bepaalt, worden bevolen dat het bevel alleen kan worden nagekomen door de sleutel af te geven maar niet door zelf te ontsleutelen; dit kan wanneer het onderzoeksbelang zou worden geschaad door het zelf laten ontsleutelen en als het proportioneel is om de sleutel te laten afgeven, waarbij gelet moet worden op andere, niet-benodigde, informatie die met dezelfde sleutel is versleuteld en de schade die het vrijgeven van die sleutel zou opleveren (s. 51). Het bevel de sleutel af te geven zal in de praktijk vooral worden uitgeoefend bij verdachte personen waarvan vermoed wordt dat zij relevant bewijsmateriaal hebben versleuteld.[175] S. 52 bepaalt dat de Secretary of State een regeling moet treffen voor vergoeding van eventuele kosten die de geadresseerde maakt bij uitvoering van het bevel. Bij het ontsleutelbevel kan ook geheimhouding worden opgelegd, waarvan de overtreding zwaar (tot vijf jaar gevangenisstraf) wordt gesanctioneerd (s. 54). Wanneer iemand het ontsleutelbevel opzettelijk ('knowingly') niet nakomt, is hij strafbaar met een gevangenisstraf van maximaal twee jaar en/of een boete bij een gerechtelijke procedure ('on conviction of indictment'); de maximumstraf is zes maanden gevangenisstraf en/of een boete bij versnelde afdoening ('on summary conviction') (s. 53(1 jº 5)). De bewijslastverdeling bij het aantonen dat iemand opzettelijk weigert – dat wil zeggen dat hij weigert terwijl hij in staat is te ontsleutelen – is complex:

> '53.- (2) In proceedings against any person for an offence under this section, if it is shown that that person was in possession of a key to any protected information at any time before the time of the giving of the section 49 notice, that person shall be taken for the purposes of those proceedings to have continued to be in possession of that key at all subsequent times, unless it is shown that the key was not in his possession after the giving of the notice and before the time by which he was required to disclose it.
> (3) For the purposes of this section a person shall be taken to have shown that he was not in possession of a key to protected information at a particular time if—
> (a) sufficient evidence of that fact is adduced to raise an issue with respect to it; and
> (b) the contrary is not proved beyond a reasonable doubt.'

Volgens lid 2 zal justitie aannemelijk moeten maken dat de geadresseerde op enig moment de sleutel in bezit heeft gehad. Wanneer de verdachte vervol-

175 Home Office 2007, paragraaf 3.8.

gens stelt de sleutel niet (meer) te hebben, zal hij dit moeten motiveren. Voldoende daarvoor is dat hij voldoende argumenten aandraagt die vragen doen rijzen ('raise an issue') omtrent zijn mogelijkheid te ontsleutelen. Het is dan aan justitie om alsnog aan te tonen, 'beyond reasonable doubt', dat de verdachte de sleutel in bezit heeft.
De uitoefening van het ontsleutelbevel is bovendien onderworpen aan onafhankelijk toezicht. Het toezicht bestaat niet alleen uit een rechter die (volgens wet of praktijk) toestemming moet geven voor een decryptiebevel in individuele gevallen,[176] maar ook uit een onafhankelijke toezichthouder die onderzoekt en rapporteert hoe de bevoegdheid in het algemeen wordt uitgeoefend. Het VK kent diverse van dergelijke toezichthouders die de naleving van de wetgeving rond bijzondere opsporingsbevoegdheden controleren. Een Interception of Communications Commissioner ziet toe op de uitoefening door de Secretary of State van de bevoegdheden en plichten van Deel III van de RIPA (s. 57 RIPA). Daarnaast heeft de Chief Surveillance Commissioner – die reeds toezicht uitoefende op basis van de Police Act 1997 – de taak toe te zien op de uitoefening door niet-rechterlijke instanties van de bevoegdheden en plichten uit Deel III RIPA (s. 62 RIPA).

Deel III van de RIPA trad pas veel later in werking. Voor de implementatie was een Code of Practice nodig, die pas in 2006 in consultatie werd gegeven.[177] (In de literatuur wordt daarbij fijntjes opgemerkt dat de grote vertraging in implementatie de argumentatie van de wetgever uit 2000 onderuithaalt dat er dringende behoefte zou zijn aan invoering van het ontsleutelbevel.[178]) De Code of Practice werd in 2007 aangenomen en trad in werking op 1 oktober 2007.[179] Op die datum trad ook Deel III van de RIPA in werking. [180]
De Code of Practice geeft een overzicht van de eisen en modaliteiten van het ontsleutelbevel, waarbij overigens grotendeels de bepalingen uit Deel III van de RIPA in iets andere bewoordingen worden uitgelegd. In het licht van de vraag naar de verenigbaarheid met artikel 6 EVRM is wel van belang dat de Code of Practice bepaalt dat het ontsleutelbevel (dat altijd schriftelijk wordt gegeven) moet verduidelijken dat als de ontvanger enige twijfel heeft over wat hij moet doen in reactie op het bevel, hij contact op moet nemen met een juridisch adviseur; dit geldt ook voor bevelen waarin geheimhouding wordt opgelegd.[181] Dit is van belang in verband met de verwevenheid van het nemo-teneturbeginsel met het recht op bijstand door een advocaat (zie paragraaf 4.1.2). Nieuw is ook dat elke autoriteit die overweegt een ontsleutelbe-

176 Zie noten 174 en 188.
177 Home Office 2006.
178 Chatterjee 2011, p. 275, met literatuurverwijzingen.
179 Home Office 2007; The Regulation of Investigatory Powers (Investigation of Protected Electronic Information: Code of Practice) Order 2007, *Statutory Instruments* 2007 No. 2200.
180 The Regulation of Investigatory Powers Act 2000 (Commencement No. 4) Order 2007, *Statutory Instruments 2007*, No. 2196 (C. 85).
181 Home Office 2007, paragraaf 4.21.

vel uit te vaardigen, vooraf het National Technical Assistance Centre (NTAC) moet consulteren (paragraaf 3.10 van de Code of Practice). Het NTAC geeft schriftelijk toestemming voor een bevel als het van oordeel is dat de aanvragende autoriteit bevoegd is een ontsleutelbevel te geven. Deze poortwachterfunctie is een onderdeel van de checks & balances waarmee het ontsleutelbevel is omkleed:

> 'In this way NTAC will support public authorities to ensure that the exercise of the powers in Part III is undertaken appropriately, expertly and with the highest regard for compliance with the requirements and principles of the Act and this code. The role of NTAC as a guardian and gatekeeper of the use of Part III will provide assurance to the Commissioners that the scope for inappropriate use of the powers is mitigated. Equally the Commissioners' oversight extends to NTAC itself.'[182]

Ondertussen was de RIPA in 2006 al aangepast door de Terrorism Act 2006. Om een aantal redenen werd het nodig geacht om de maximumstraf op decryptieweigering bij terroristische zaken te verhogen. Gevallen waarin de nationale veiligheid in het geding is, rechtvaardigen een hogere straf; het gaat om gevallen waarin snelheid en vroegtijdig ingrijpen van het grootste belang zijn, en bovendien kan ontsleuteling helpen om slachtoffers dan wel andere verdachten te identificeren.[183] S. 53(5)(a) RIPA bepaalt nu dat bij een gerechtelijke procedure de maximumstraf vijf jaar is in terroristische zaken en twee jaar in andere zaken.[184]
Vervolgens is de strafbedreiging ook verhoogd voor kinderpornografiezaken. Dit was een van de voorstellen die werden gelanceerd in het consultatiedocument voor de Code of Practice uit 2006. Aangezien de maximumstraf op bezit van (virtuele) kinderpornografie tien jaar is, zou een strafbedreiging van twee jaar op decryptieweigering te laag kunnen zijn. Het consultatiedocument gaf daarop in overweging om de straf te verhogen naar maximaal vijf jaar in gevallen waarin iemand eerder is veroordeeld voor kinderpornografie, of waarin versleuteld materiaal wordt aangetroffen op of in samenhang met een drager waarop ook kinderporno staat, of waarin de rechter oordeelt dat de beveiligde informatie waarschijnlijk kinderporno betreft ('is likely to contain an indecent photograph or pseudo-photograph of a child (on the basis, for example, of evidence from a witness)').[185] De consultatie leidde niet tot wetsaanpassing, maar in 2009 werd het voorstel overgenomen in een wetsvoorstel van parlementslid Paul Beresford; de voorgestelde omstandigheden voor strafverhoging waren een eerdere veroordeling wegens kinderporno, of het aantreffen van kinderporno in bezit van de verdachte, of een oordeel van de rechter dat het waarschijnlijker dan niet ('more likely than not') is dat ver-

182 Ibid., paragraaf 3.11.
183 Chatterjee 2011, p. 271.
184 Zoals aangepast door s. 15 van de Terrorism Act 2006, c. 11.
185 Home Office 2006, p. 5-6.

sleutelde informatie kinderporno betreft.[186] Het voorstel werd ingetrokken omdat tegelijkertijd de Policing and Crime Act 2009 een vergelijkbare bepaling invoerde. De straf op decryptieweigering in s. 53(5)(a) is nu verhoogd naar maximaal vijf jaar in gevallen van 'child indecency', wat wil zeggen 'a case in which the grounds specified in the notice to which the offence relates as the grounds for imposing a disclosure requirement were or included a belief that the imposition of the requirement was necessary for the purpose of preventing or detecting an offence' van kinderpornografie.[187]

6.3.2 Uitoefening van de bevoegdheid in de praktijk

In de jaarverslagen van de Interception of Communications Commissioner[188] wordt niet gerapporteerd over uitoefening van het ontsleutelbevel, wellicht omdat het nog niet aan de orde is geweest in relatie tot versleutelde gegevens die via aftappen zijn verkregen. De Chief Surveillance Commissioner rapporteert wel over de uitoefening van de bevoegdheid. Hij maakt daarbij gebruik van de poortwachtersfunctie van het National Technical Assistance Centre (NTAC), omdat elke opsporingsambtenaar die een ontsleutelbevel wil uitvaardigen dit altijd eerst aan dit expertisecentrum moet voorleggen,[189] en daar dus bekend is hoeveel decryptiebevelen zijn aangevraagd. Wanneer het NTAC oordeelt dat het bevel (in technisch-formele zin) doorgang kan vinden, wordt de aanvraag doorgestuurd naar een rechter; hoewel een rechterlijke machtiging volgens de wet niet altijd vereist is, worden de vorderingen in de praktijk wel altijd aan een rechter ter toetsing voorgelegd.[190]
De jaarverslagen van de Chief Surveillance Commissioner[191] laten zien dat de bevoegdheid enkele tientallen keren per jaar wordt aangevraagd en tenuitvoergelegd. Een kleine meerderheid van de geadresseerden weigert mee te werken, waarvan een deel wordt vervolgd voor de weigering. De jaarverslagen van de Commissioner sinds 2008-2009 (waarbij het jaar loopt van 1 april tot 31 maart) laten de volgende cijfers zien.

186 Protection of Children (Encrypted Material) Bill, 2008–2009, beschikbaar op www.publications.parliament.uk/pa/cm200809/cmbills/018/09018.i-i.html (geraadpleegd 1 september 2012).
187 Zie s. 26 Policing and Crime Act 2009, c. 26.
188 Beschikbaar op www.intelligencecommissioners.com (geraadpleegd 1 september 2012).
189 Zie noot 182 en bijbehorende tekst.
190 Ministerie van Veiligheid en Justitie 2011.
191 Beschikbaar op http://surveillancecommissioners.independent.gov.uk/about_annual.html (geraadpleegd 1 september 2012).

Tabel 2 Overzicht van ontsleutelbevelen in Verenigd Koninkrijk

	2008-2009	2009-2010	2010-2011	2011-2012
Aangevraagd bij NTAC	27[a]	*	30	57
– waarvan goedgekeurd	26	38	26	57
– waarvan afgekeurd	1	*	4	0
Aangevraagd bij rechter	17[b]	*	18	54
– waarvan goedgekeurd	17	22	17	33
– waarvan afgekeurd	0	*	1	*
Bevelen uitgevaardigd	15	17[c]	12[d]	20
– waarbij is meegewerkt	4	6	4	9
– waarbij is geweigerd	11	7	2	15[e]
Aantal vervolgingen voor niet-meewerken	7	5	3	9
– waarvan vrijgesproken	*	*	*	*
– waarvan veroordeeld	2	1	1	2
Soorten misdrijven	Antiterrorisme, kinderpornografie, binnenlands extremisme	Vooral bezit van kinderpornografie; overig: handel met voorkennis, illegaal uitzenden, diefstal, accijnsontduiking, gekwalificeerde inbraak	Vooral bezit van kinderpornografie; overig: binnenlands extremisme, handel met voorkennis, fraude, accijnsontduiking, drugshandel, drugsbezit ter verspreiding	Veroordelingen voor import van verboden goederen, fraude; overig: binnenlands extremisme, bezit kinderpornografie, handel met voorkennis, fraude, accijnsontduiking, drugshandel, drugsbezit ter verspreiding

* Onbekend.

[a] Eén bevel is uitgevaardigd buiten het NTAC om. De geadresseerde weigerde mee te werken maar werd daarvoor niet vervolgd. Chief Surveillance Commissioner 2009, p. 12.

[b] Negen aanvragen werden teruggetrokken omdat andere zaken prioriteit kregen. Ibid.

[c] Bij vier bevelen liep de procedure nog. Chief Surveillance Commissioner 2010, p. 11.

[d] Bij zes bevelen liep de procedure nog. Chief Surveillance Commissioner 2011, p. 12.

[e] Inclusief bevelen uitgevaardigd in de vorige periode. Chief Surveillance Commissioner 2012.

Er zijn geen overzichten beschikbaar van de straffen die zijn opgelegd voor het niet-meewerken. Berichten uit de media geven aan dat in een terrorismezaak een gevangenisstraf van 9 maanden is opgelegd,[192] en in een kinderpornografiezaak een verdachte tot 16 weken gevangenisstraf is veroordeeld,[193] op basis van Deel III van RIPA.

Het is moeilijk om de cijfers uit tabel 2 te interpreteren. Het wordt niet geregistreerd in hoeveel gevallen de opsporing stuit op encryptie en in hoeveel gevallen dit een serieus probleem oplevert; daarom is het moeilijk te zeggen of enkele tientallen ontsleutelbevelen per jaar veel of weinig is. Uit de jaarverslagen blijkt ook niet precies de ernst van de zaken, bijvoorbeeld niet of het om prepuberale of puberale kinderpornografie gaat of om ernstige of lichtere gevallen van handel met voorkennis. Tekenend is wel dat de Surveillance Commissioner in het verslag over 2009-2010 opmerkt, met een subtiel kriti-

192 'UK jails schizophrenic for refusal to decrypt files', *The Register* 24 november 2009, www.theregister.co.uk/2009/11/24/ripa_jfl (geraadpleegd 1 september 2012).

193 'Teen jailed over failure to hand over computer password', *Out-law.com*, www.out-law.com/page-11424 (geraadpleegd 1 september 2012).

sche ondertoon, dat slechts één van de 38 bevelen betrekking had op een terrorismezaak.[194]
In de literatuur wordt opgemerkt dat er in elk geval geen lawine aan decryptiebevelen is gevolgd sinds de invoering van de RIPA, en dat de indruk bestaat 'that s 49 notice powers are being used as a broader sweeper mechanism to catch lesser, more indeterminate cases whilst the core and major targets of terrorism and child pornography – both considered the main justifications for the powers – are underrepresented'.[195] Chatterjee bekritiseert de strafverhoging in terrorismezaken als zijnde 'neither pressing, compelling nor effective in practice' en vindt tevens dat de wetgevingsretoriek over de noodzaak voor het ontsleutelbevel in kinderpornozaken niet gedragen wordt door de praktijk – het gebruik is minimaal en biedt geen bewijsbare aanvullende bescherming voor kinderen.[196] Zij wijst ook op het gevaar van het hellend vlak als de bevoegdheid, zoals wordt beweerd, ook wordt ingezet tegen muziekpiraterij: 'The potential for the increased use of encryption provisions to pursue illegal file sharing would clearly seem to go beyond the core motivations of terrorism and child pornography, and are strongly suggestive of an insidious and problematic "mission creep".'[197]
Daarentegen stelt de Britse justitie dat in de praktijk wordt getracht het instrument terughoudend in te zetten, dat wil zeggen alleen bij een verdenking van ernstige misdrijven. Daarbij wordt ook de relatie tussen het misdrijf en het feit dat door de verdachte encryptie is toegepast in de beoordeling betrokken. Die relatie is sterker in kinderpornozaken, waarin veelal encryptie bewust gebruikt wordt om bewijsmateriaal te verbergen, en minder sterk in gevallen waarin bijvoorbeeld een mobiele telefoon met wachtwoordbeveiliging in een opsporingsonderzoek wordt aangetroffen. Daarbij gaat er ook voldoende dreiging uit van de strafbaarstelling van decryptieweigering; vaak volstaat het om de verdachte te wijzen op deze strafbaarstelling. Hoewel het ontsleutelbevel zeker niet wordt gezien als een wondermiddel, vormt het volgens justitie een nuttig en effectief instrument in het arsenaal aan instrumenten die de opsporingsautoriteiten ter beschikking staan in opsporingsonderzoeken waarbij sprake is van encryptie.[198]

6.3.3 Inbreuk op het nemo-teneturbeginsel?

Bij de invoering van de RIPA-wetgeving heeft geen uitvoerig debat plaatsgevonden of het ontsleutelbevel inbreuk zou maken op het nemo-tenetur-

194 'It is of note that only one notice was served in relation to terrorism offences', Chief Surveillance Commissioner 2010.
195 Chatterjee 2011, p. 277.
196 Ibid., p. 284.
197 Ibid., p. 283.
198 Aldus vertegenwoordigers van het ministerie van Justitie van Engeland en Wales in een bijeenkomst met medewerkers van het Nederlandse ministerie van Veiligheid en Justitie (Ministerie van Veiligheid en Justitie 2011).

beginsel.[199] In de aanloop naar RIPA stelde het consultatiedocument voor de *Electronic Communications Bill* dat nemo tenetur niet in het geding was:

> The Government does not believe that its proposals would amount to self-incrimination. The proposed power will enable evidence already in the possession of law enforcement agencies to be made comprehensible, rather than requiring a suspect to disclose evidence. There are numerous examples where suspects are required to comply with statutory obligations for the purpose of maintaining the effectiveness of criminal investigations (e.g. requirements to provide fingerprint and DNA samples, or to produce documentary evidence of vehicle insurance cover). Without powers to make electronic evidence comprehensible, criminals would be able to conceal their activities with complete impunity. The Government does not believe that this would be in the public interest.[200]

Ook in het RIPA-wetgevingsproces is gesteld dat het ontsleutelbevel verenigbaar is met het EHRM, aangezien de sleutel zelf niet incriminerend is en onafhankelijk van de wil van de verdachte bestaat, zodat het volgens het *Saunders*-criterium buiten nemo tenetur valt.[201]
In de literatuur wordt dit evenwel in twijfel getrokken. S. 53(2) bepaalt dat wanneer justitie aantoont dat de verdachte ooit in bezit is geweest van de sleutel, de verdachte vervolgens aannemelijk moet maken dat hij niet in staat is te ontsleutelen. Akdeniz et al. vinden deze omkering van de bewijslast in strijd met artikel 6 EVRM. Hoewel de uiteindelijke versie 'dramatisch verbeterd' is ten opzichte van de eerdere versies doordat de verdachte alleen twijfel hoeft te zaaien en dus geen zware bewijslast heeft, zou de bewijslast dat de verdachte in staat is te ontsleutelen altijd bij het Openbaar Ministerie moeten liggen. Ook blijven andere aspecten onderbelicht die zouden moeten meewegen in de beoordeling van de eerlijkheid van het proces conform artikel 6 EVRM, zoals de aard van het misdrijf, de beschikbaarheid van ander bewijs en toegang tot een advocaat.[202] Andere critici, voornamelijk uit de mensenrechtenhoek, betwijfelden of de regeling voldoende gebalanceerd was in het licht van de menselijke vergeetachtigheid of van legitieme redenen die mensen kunnen hebben om materiaal niet te willen ontsleutelen, zoals politieke vluchtelingen voor wie het vrijgeven van de sleutel veiligheidsrisico's zou kunnen opleveren. Volgens critici van de wet kwam de ontsleutelplicht dan ook neer op 'an uncomfortable attempt to punish by proxy where a more serious suspected offence could not be adequately proven', die niet de drempel van noodzakelijkheid haalde die het EVRM vereist voor inbreuken op grondrechten.[203]

199 Ministerie van Veiligheid en Justitie 2011.
200 Department of Trade and Industry 1999, p. 30.
201 Lord Bassam, House of Lords Debates, vol. 614 col. 972, 28 June 2000, geciteerd in Akdeniz et al. 2001, p. 88.
202 Ibid., p. 87-88.
203 Chatterjee 2011, p. 269, met verwijzingen.

De vraag of het ontsleutelbevel verenigbaar is met het nemo-teneturbeginsel, is aan de orde geweest in de zaak *R* v *S and A*. S. en A. werden verdacht van terroristische samenzwering, namelijk om ene H., die huisarrest had in Leicestershire onder de Prevention of Terrorism Act 2005, te ontvoeren en over te brengen naar een geheim adres in Sheffield. Op 9 september 2007 bracht S. H. daadwerkelijk over naar Sheffield, waar de politie het pand waar zij verbleven binnenviel. S. werd in de kamer naast die waar H. zich bevond, aangetroffen met een computer waar de sleutel tot een versleuteld bestand gedeeltelijk ingevoerd leek. Na inbeslagneming werden van de harde schijf verwijderde bestanden naar boven gehaald die verdenking opleverden van het verboden bezit van terrorismefaciliterende documenten, maar de versleutelde bestanden konden niet worden geopend. In januari 2008 kreeg S. op basis van s. 53 RIPA een bevel de bestanden te ontsleutelen; A. kreeg een soortgelijk bevel in maart. Beiden weigerden omdat het bevel hun recht tegen zelfincriminatie zou schenden. Zij werden daarop aangeklaagd voor decryptieweigering. Hun verzoek om deze aanklacht te seponeren werd afgewezen door Judge Stephens, aangezien het materiaal dat werd gevorderd onafhankelijk van de geesten van de appellanten bestond en aangezien hoe dan ook de beweerde inbreuk op het nemo-teneturbeginsel (als die er zou zijn) legitiem en proportioneel was.[204] Tegen deze afwijzing gingen zij in beroep bij de Court of Appeal (Criminal Division).
Het Hof wees het beroep van S. en A. af op 28 juli 2008.[205] Het Hof overwoog dat het nemo-teneturbeginsel diep geworteld is in de *common law*, maar dat het geen absoluut recht betreft en dat er talrijke wettelijke uitzonderingen bestaan, zowel om materiaal uit te leveren als om antwoorden te geven. De resultaten mogen onder omstandigheden voor het bewijs worden gebruikt en weigering mag strafrechtelijk worden gesanctioneerd. Men kan dan ook niet stellen dat de strafbaarstelling in s. 53 RIPA als zodanig onverenigbaar is met artikel 6 EVRM; zoals in *Brown* v *Stott* werd gesteld:

> 'Limited qualification of these rights [comprised within article 6] is acceptable if reasonably directed by national authorities towards a clear and proper public objective and if representing no greater qualification than the situation calls for.'[206]

Voordat het Hof toekomt aan de beoordeling of een eventuele inbreuk op artikel 6 in casu gerechtvaardigd is, beantwoordt het eerst de vraag of het nemo-teneturbeginsel – dat immers niet ziet op materiaal dat onafhankelijk van de wil van de verdachte bestaat – überhaupt in het geding is:

204 *R* v *S and A*, [2008] EWCA Crim 2177, §15.
205 *R* v *S and A*, [2008] EWCA Crim 2177.
206 *Brown* v *Stott [Procurator Fiscal, Dunfermline] and another* [2003] 1 AC 681, geciteerd in *R* v *S and A*, [2008] EWCA Crim 2177, §17.

> 'the debate in argument concentrated on the rival contentions whether the key to each appellants' protected data was properly to be catalogued as a piece of information with an existence separate from his "will". The problem which presents itself in the present appeals, is not, in our judgment, susceptible of quite such rigid compartmentalisation.
> On analysis, the key which provides access to protected data, like the data itself, exists separately from each appellant's "will". Even if it is true that each created his own key, once created, the key to the data, remains independent of the appellant's "will" even when it is retained only in his memory, at any rate until it is changed. (…) In this sense the key to the computer equipment is no different to the key to a locked drawer. The contents of the drawer exist independently of the suspect: so does the key to it. The contents may or may not be incriminating: the key is neutral. In the present cases the prosecution is in possession of the drawer: it cannot however gain access to the contents. The lock cannot be broken or picked, and the drawer itself cannot be damaged without destroying the contents. (…)
> The actual answers, that is to say the product of the appellants' minds could not, of themselves, be incriminating. The keys themselves simply open the locked drawer, revealing its contents. In much the same way that a blood or urine sample provided by a car driver is a fact independent of the driver, which may or may not reveal that his alcohol level exceeds the permitted maximum, whether the appellants' computers contain incriminating material or not, the keys to them are and remain an independent fact. If however, as for present purposes we are assuming, they contain incriminating material, the fact of the appellants' knowledge of the keys may itself become an incriminating fact. For example, to know the key to a computer in your possession which contains indecent images of children may itself tend to support the prosecution case that you were knowingly in possession of such material. (...)
> In our judgment the correct analysis is that the privilege against self-incrimination may be engaged by a requirement of disclosure of knowledge of the means of access to protected data under compulsion of law.' [207]

Het Hof zegt met andere woorden dat een sleutel of wachtwoord onafhankelijk van de wil van verdachten bestaat en in die zin neutraal is; het wachtwoord zelf is niet belastend. Het feit dat de verdachte het wachtwoord *kent* (wat blijkt als hij het vertelt) kan echter wel belastend zijn, bijvoorbeeld omdat de kennis van het wachtwoord bewijs oplevert dat de verdachte opzet-

207 *R* v *S and A*, [2008] EWCA Crim 2177, §19-21, 24.

telijk kinderporno in zijn bezit heeft. Vervolgens stelt het Hof[208] dat de vraag of de kennis van de sleutel incriminerend is, afhangt van wat er uit het versleutelde materiaal naar voren komt. Als het versleutelde bestand immers ontlastend of neutraal is, zou het feit dat de verdachte kennis heeft van de sleutel ook ontlastend of neutraal zijn. De kennis van de sleutel is alleen incriminerend als het onderliggende materiaal feitelijk ook belastend is. Omdat het dus niet a priori te beoordelen valt of de gevorderde ontsleuteling incriminerend is, maar dit alleen na ontsleuteling kan worden vastgesteld, mag het bevel wel worden gegeven. Indien vervolgens zou blijken dat de ontsleuteling incriminerend was – en dus het nemo-teneturbeginsel aan de orde is – dan heeft de zittingsrechter altijd nog de mogelijkheid om de sleutel, de kennis van de sleutel en/of de ontsleutelde bestanden uit te sluiten van bewijs, op basis van de algemene bewijsuitsluitingsregel van s. 78 van de Police and Criminal Evidence Act 1984[209]. Het Hof concludeert op basis van deze overwegingen het volgende:

> 'In these appeals the question which arises, if the privilege is engaged at all, is whether the interference with it is proportionate and permissible. A number of issues are clear and stark. The material which really matters is lawfully in the hands of the police. Without the key it is unreadable. That is all. The process of making it readable should not alter it other than putting it into an unencrypted and intelligible form that it was in prior to encryption; the material in the possession of the police will simply be revealed for what it is. (...) The requirement for information is based on the interests of national security and the prevention and detection of crime, and is expressly subject to a proportionality test and judicial oversight. (...) The notice is in very simple form. Procedural safeguards and limitations on the circumstances in which this notice may be served are addressed in a comprehensive structure, and in relation to any subsequent trial, the powers under section 78 of the 1984 Act to exclude evidence in relation, first, to the underlying material, second, the key or means of access to it, and third, an individual defendant's knowledge of the key or means of access, remain. Neither the process, nor any subsequent trial can realistically be stigmatised as unfair.'[210]

208 Zo interpreteer ik althans §24, die een wat moeilijk te volgen formulering bevat: 'In short, although the appellants' knowledge of the means of access to the data may engage the privilege against self-incrimination, it would only do so if the data itself – which undoubtedly exists independently of the will of the appellants and to which the privilege against self-incrimination does not apply – contains incriminating material. If that data was neutral or innocent, the knowledge of the means of access to it would similarly be either neutral or innocent. On the other hand, if the material were, as we have assumed, incriminatory, it would be open to the trial judge to exclude evidence of the means by which the prosecution gained access to it. Accordingly the extent to which the privilege against self-incrimination may be engaged is indeed very limited.'

209 Dit artikel luidt: '*Exclusion of unfair evidence.* (1) In any proceedings the court may refuse to allow evidence on which the prosecution proposes to rely to be given if it appears to the court that, having regard to all the circumstances, including the circumstances in which the evidence was obtained, the admission of the evidence would have such an adverse effect on the fairness of the proceedings that the court ought not to admit it. (2) Nothing in this section shall prejudice any rule of law requiring a court to exclude evidence.'

210 *R* v *S and A*, [2008] EWCA Crim 2177, §25.

Belangrijk in deze overweging is dat het Hof – in lijn met de artikel 6 EVRM-rechtspraak – beoordeelt of de procedure als geheel eerlijk is geweest. In die beoordeling spelen de vele *checks and balances* van de regeling een belangrijke rol, evenals de mogelijkheid voor de zittingsrechter om eventueel incriminerend bewijs terzijde te leggen. Het Hof concludeert dan ook dat de vervolging op basis van s. 53 RIPA door kan gaan.[211]

Er zijn naast *S and A* geen andere uitspraken bekend over de verenigbaarheid van het Britse ontsleutelbevel met artikel 6 EVRM, in het VK zelf noch in Straatsburg. De literatuur over Deel III van RIPA, die na *S and A* langzaam op gang gekomen is, laat geen eenduidig beeld zien. Chatterjee concludeert dat 'the concerns on Article 6 ECHR seem to be allayed (albeit not in an entirely convincing manner)'.[212] Zij vindt met name de analogie die maar steeds gemaakt wordt van een cryptosleutel of wachtwoord met een fysieke sleutel van een kluis onterecht, omdat de essentie van digitale objecten is dat zij immaterieel zijn en dus niet fysiek bestaan, en daarom ook niet onafhankelijk van hun maker zijn.[213] Zij sluit hierbij aan op de kritiek van Roberts dat een sleutel (tenzij die ook ergens materieel is vastgelegd) een 'immaterieel psychologisch feit' is dat alleen in de geest bestaat. 'In such circumstances the key cannot be distinguished from the suspect's knowledge of it; it is merely a facet of that knowledge.' Daarom bestaat de encryptiesleutel volgens Roberts waarschijnlijk niet onafhankelijk van de wil van de verdachte en is dus het nemo-teneturbeginsel *prima facie* in het geding. Maar aangezien de wetgeving een proportionele inbreuk maakt om een ernstig maatschappelijk probleem aan te pakken en het hier om een terrorismezaak gaat, is de inbreuk op nemo tenetur in dit geval gerechtvaardigd.[214]

6.4 Verenigde Staten

Anders dan in de meeste Europese (*civil-law*-)systemen, hoeft een opsporingsbevoegdheid in de Verenigde Staten niet expliciet wettelijk te zijn vastgelegd. Politie en justitie mogen strafrechtelijk onderzoek uitvoeren, zolang

211 Ibid., §26. Terzijde ontsiert het Hof de zorgvuldig geconstrueerde uitspraak enigszins door in §27 als overweging ten overvloede te geven dat als S. en A. op basis van advies van hun advocaat hadden geweigerd maar nu alsnog (zij het veel te laat buiten de periode van het bevel) hun sleutel zouden afgeven, ze vermoedelijk niet meer vervolgd zouden worden voor decryptieweigering dan wel op een barmhartige rechter zouden kunnen rekenen, 'at any rate if the protected data turned out to be innocent or simply neutral.' Mij bevreemdt deze overweging ten eerste omdat, als de verdachten alsnog zouden ontsleutelen, het bijzonder formalistisch (en in strijd met de ratio van RIPA) zou zijn om de vervolging voor het niet binnen de gestelde termijn ontsleutelen door te zetten, en ten tweede omdat, als het ontsleutelde materiaal wel incriminerend zou blijken, een vervolging voor het gronddelict (waar het toch om begonnen was) meer voor de hand zou liggen dan een vervolging voor niet-tijdige sleutelafgifte. De overweging laadt hiermee de verdenking op zich dat de sanctionering van decryptieweigering inderdaad wel wordt gezien als een 'punishment by proxy' (zie noot 203 en bijbehorende tekst).

212 Chatterjee 2011, p. 284.

213 Ibid., p. 281.

214 Roberts 2009; in gelijke zin Chatterjee 2011.

zij daarbij maar binnen de grenzen van de Grondwet blijven.[215] Een van die grenzen is het nemo-teneturbeginsel, vastgelegd in het Vijfde Amendement ('No person (…) shall be compelled in any criminal case to be a witness against himself'). De reikwijdte hiervan is via rechtspraak in een fijnmazig systeem uitgekristalliseerd. Nieuwe ontwikkelingen worden door interpretatie in dit systeem ingepast. In de zaak-*Boucher* uit 2007 is dit voor het eerst gebeurd ten aanzien van een vordering te ontsleutelen, en sindsdien zijn er meer uitspraken verschenen, vooralsnog vooral van lagere rechters, die hieronder worden besproken.

Deze zaken gaan allemaal over een vordering van een *grand jury*, een breed samengestelde jury die onderzoekt of een verdachte kan worden aangeklaagd,[216] om te ontsleutelen; dit is enigszins vergelijkbaar met een vordering door een rechter-commissaris in een Nederlands opsporingsonderzoek. Decryptieverzoeken in een eerder stadium door de politie roepen andere vragen op in relatie tot het Vijfde Amendement, omdat er een andere vorm van dwang is; anders dan bij een *grand jury*, waarbij niet-meewerken neerkomt op 'contempt of court', is niet-meewerken bij een politieverhoor niet strafbaar. De combinatie van hechtenis en verhoor levert echter wel enige mate van dwang op om te verklaren; daarom spelen bij het politieverhoor de zogeheten 'Miranda rights' een belangrijke rol. De verdachte moet worden gewaarschuwd dat hij niet hoeft mee te werken ('You have the right to remain silent', enzovoorts).[217] Regelmatig doen verdachten in dit stadium, al dan niet voldoende geïnformeerd, afstand van hun *Miranda*-rechten, ook bij het afgeven van een wachtwoord. Dat roept vragen op over de toepassing van *Miranda* op een decryptiebevel bij politieverhoor.[218] Die vragen zijn echter nauw verweven met de precieze doctrine rond het Amerikaanse verhoor en het gebruik van bewijs dat in strijd met Miranda is verkregen, die niet altijd even goed vergelijkbaar is met de Europese of Nederlandse normering van het verhoor. Daarom beperkt deze paragraaf zich tot de jurisprudentie over een decryptiebevel in het kader van een *grand jury*-procedure.

Zaken in de VS worden over het algemeen aangeduid, net als in EHRM-rechtspraak, met de naam van de aangeklaagde. Wanneer de zaak anoniem wordt gepubliceerd, krijgt het echter altijd de fictieve naam John Doe (of bij vrouwen Jane Doe) mee. Bij *John Doe*-zaken moet men dus op het jaar en de vindplaats letten om te weten welke uitspraak precies wordt bedoeld.

215 Vgl. bijvoorbeeld de All Writs Act, op basis waarvan rechterlijke instanties allerlei soorten bevelen mogen uitvaardigen die passend zijn ('The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law', 28 U.S.C. §1651).

216 De *grand jury* (vaak bestaand uit 23 personen) heeft dus een andere rol, in een voorstadium van het strafproces, dan de – uit films en televisieseries meer bekende – *petit jury* (vaak bestaand uit 12 personen) die een oordeel uitspreekt over een aangeklaagde in een specifieke strafzaak.

217 *Miranda* v *Arizona*, 384 U.S. 436 (1966).

218 Zie daarover het debat tussen Gershowitz (2011) en Brenner (2011).

6.4.1 Boucher-I

In 2007 is voor het eerst een zaak aan de orde geweest waarin een verdachte zich op het Vijfde Amendement beriep toen hem werd gevorderd zijn versleutelde harde schijf toegankelijk te maken.[219] De auto van Sebastien Boucher werd aan de grens onderzocht door de douane. Een douaneambtenaar opende een laptop op de achterbank en kon, zonder een wachtwoord te hoeven invoeren, de laptop onderzoeken. Omdat sommige bestandsnamen wezen op een (mogelijk kinder)pornografische inhoud, werd de computer nader onderzocht. Daarbij werd een bestand gevonden getiteld '2yo getting raped during diaper change', dat niet kon worden geopend maar dat volgens de meta-informatie zes dagen geleden nog was bekeken. Ook werden duizenden (mogelijk kinderporno)plaatjes aangetroffen. Vervolgens werd Boucher verhoord. Desgevraagd liet Boucher het Z-station op de schijf zien waar hij al zijn uit nieuwsgroepen binnengehaalde bestanden opsloeg. Daarna vond de opsporingsambtenaar diverse kinderpornobestanden. Boucher werd gearresteerd en de laptop in beslag genomen. Later bleek het Z-station op de laptop echter niet meer toegankelijk voor forensisch onderzoekers; het bleek onkraakbaar met PGP (Pretty Good Privacy) versleuteld te zijn. Daarop werd Boucher door een *grand jury* gevorderd de bestanden op zijn laptop te overhandigen, dan wel zelf zijn wachtwoord in te voeren waarna justitie de laptop zelf zou kunnen onderzoeken. Boucher kwam in verweer tegen deze vordering.
De zaak draait nu om de vraag of het zelf invoeren van het wachtwoord beschermd wordt door het Vijfde Amendement. De rechter in eerste aanleg oordeelde dat dit zo is en honoreerde Bouchers verweer. Het Vijfde Amendement beschermt tegen afgedwongen medewerking die incriminerend is en een 'testimonial' karakter[220] heeft. Aangezien er sprake is van dwang (een *grand jury*-bevel) en incriminatie (de bestanden die worden blootgelegd bevatten kinderporno), gaat het om de vraag of het invoeren van een wachtwoord 'testimonial' is. Volgens de rechter is het invoeren van het wachtwoord in dit geval 'testimonial':

> 'Entering a password into the computer implicitly communicates facts. By entering the password Boucher would be disclosing the fact that he knows the password and has control over the files on drive Z. The procedure is equivalent to asking Boucher, "Do you know the password to the laptop?" (…) Boucher would be compelled to produce his thoughts and the contents of his mind. (…) Here, when Boucher enters a password he indicates that he believes he has access.

219 In re Boucher, 2007 WL 4246473 (D. Vt. Nov. 29, 2007).
220 Dat wil zeggen dat de handeling een element heeft van het afleggen van een verklaring. Het criterium 'testimonial' is min of meer vergelijkbaar is met het *Saunders*-onderscheid tussen materiaal dat onafhankelijk en afhankelijk van de wil van de verdachte bestaat.

> The Supreme Court has held some acts of production are unprivileged such as providing fingerprints, blood samples, or voice recordings. (…) Unlike the unprivileged production of such samples, it is not without question that Boucher possesses the password or has access to the files. In distinguishing testimonial from non-testimonial acts, the Supreme Court has compared revealing the combination to a wall safe to surrendering the key to a strongbox. [verwijzend naar *Doe* en *Hubbell*[221]] The combination conveys the contents of one's mind; the key does not and is therefore not testimonial.(…) A password, like a combination, is in the suspect's mind, and is therefore testimonial and beyond the reach of the grand jury subpoena.'[222]

Vervolgens is aan de orde of immuniteit voor het invoeren van het wachtwoord de vordering alsnog toelaatbaar maakt. Justitie had aangeboden de handeling, en dus Bouchers impliciete verklaring dat de resulterende bestanden bestaan en onder zijn controle vallen, niet als bewijs te gebruiken – daarvoor waren immers de processen-verbaal van de douaneambtenaren al voldoende. De rechter verwijst wederom naar *Hubbell*:

> 'The Court found that the act of production had testimonial aspects, because production communicated information about the existence, custody, and authenticity of the documents. (...) The compelled testimony of the production became the first in a chain of evidence which led to the prosecution. (…) In doing so, the Court reaffirmed its holding that derivative use immunity is coextensive with the privilege against self-incrimination. (…) Accordingly, the Court held that Hubbell could not be prosecuted based on the documents and only evidence wholly independent of the production could be used. (...)
> Here, as in Hubbell, the government cannot separate the non-testimonial aspect of the act of production, entering the password, from its testimonial aspect. The testimonial aspect of the entry of the password precludes the use of the files themselves as derivative of the compelled testimony.'[223]

Vervolgens beargumenteert justitie nog dat het invoeren van het wachtwoord niet onder het Vijfde Amendement valt, omdat het alleen informatie oplevert die een 'foregone conclusion' oftewel een uitgemaakte zaak is, dat wil zeggen

221 *United States* v *Doe*, 487 U.S. 201, 212 (1987); *United States* v *Hubbell*, 530 U.S. 27, 43 (2000). In *Hubbell* stond de vraag centraal of een vordering om documenten uit te leveren verenigbaar was met het Vijfde Amendement. Het Supreme Court besliste daarin dat het uitleveren van documenten (als justitie het bestaan en de plaats daarvan niet onafhankelijk kan aantonen) 'testimonial' is omdat de handeling informatie blootgeeft over het bestaan, de beschikkingsmacht en de authenticiteit van de documenten (vergelijkbaar met de EHRM-uitspraak in *J.B.*). Aangezien de uitlevering (die in strijd is met het Vijfde Amendement) de eerste schakel is in de bewijsketen, mag ook het resulterende bewijs niet worden gebruikt. Zie ook *Kirschner* hieronder, waarin de analogie met een combinatiecode nader wordt uitgelegd.

222 In re Boucher, 2007 WL 4246473 (D. Vt. Nov. 29, 2007).

223 Ibid.

dat op voorhand al vaststaat wat de uitkomst is. Volgens vaste rechtspraak is het Amendement niet van toepassing op het uitleveren van materiaal 'if the existence and location of the subpoenaed evidence is known to the government and the production would not "implicitly authenticate" the evidence'.[224] De rechter vindt echter dat het openen van de harde schijf geen uitgemaakte zaak is, omdat er op het Z-station meer incriminerende bestanden kunnen staan dan die de douane-inspectie gezien heeft. Bovendien:

> 'The password is not a physical thing. If Boucher knows the password, it only exists in his mind. This information is unlike a document, to which the foregone conclusion doctrine usually applies, and unlike any physical evidence the government could already know of. It is pure testimonial production rather than physical evidence having testimonial aspects.'[225]

De rechter concludeert daarom dat de vordering in strijd is met het Vijfde Amendement en willigt Bouchers verweer in.

6.4.2 Boucher-II

In beroep verwerpt het District Court van Vermont echter Bouchers verweer.[226] De rechtbank verwijst naar twee omstandigheden waarin het uitleveren van documenten 'testimonial' kan zijn: '(1) if the existence and location of the subpoenaed papers are unknown to the government; or (2) where production would "implicitly authenticate" the documents.' In tegenstelling tot de rechter in eerste aanleg, oordeelt de rechtbank in beroep dat er wel sprake is van een uitgemaakte zaak:

> 'Where the existence and location of the documents are known to the government, "no constitutional rights are touched," because these matters are a "foregone conclusion." The Magistrate Judge determined that the foregone conclusion rationale did not apply, because the government has not viewed most of the files on the Z drive, and therefore does not know whether most of the files on the Z drive contain incriminating material. Second Circuit precedent, however, does not require that the government be aware of the incriminatory contents of the files; it requires the government to demonstrate "with reasonable particularity that it knows of the existence and location of subpoenaed documents." (…)
> Boucher accessed the Z drive of his laptop at the ICE agent's request. The ICE agent viewed the contents of some of the Z drive's files, and ascertained that they may consist of images or videos of child pornography. The Government thus knows of the existence and location of the Z drive and

224 Vgl. de EHRM-zaken *Funke* en *J.B.,* waarin een soortgelijk criterium lijkt te zijn toegepast. Zie paragraaf 4.2.
225 In re Boucher, 2007 WL 4246473 (D. Vt. Nov. 29, 2007).
226 In re Boucher, 2009 WL 424718 (D. Vt. 2009).

> its files. Again providing access to the unencrypted Z drive "adds little or nothing to the sum total of the Government's information" about the existence and location of files that may contain incriminating information.
> Boucher's act of producing an unencrypted version of the Z drive likewise is not necessary to authenticate it. He has already admitted to possession of the computer, and provided the Government with access to the Z drive. The Government has submitted that it can link Boucher with the files on his computer without making use of his production of an unencrypted version of the Z drive, and that it will not use his act of production as evidence of authentication.'[227]

De rechtbank beargumenteert hier dat de rechter in eerste aanleg een verkeerde maatstaf heeft aangelegd. Bij de vraag of er sprake is van een 'foregone conclusion' (uitgemaakte zaak) gaat het niet om het feit dat vaststaat wat precies de (belastende) inhoud is van gevorderd materiaal, maar om het feit dat de overheid met voldoende precisie moet aantonen dat het weet dat de documenten bestaan en waar ze te vinden zijn (vergelijk de maatstaf die het Europees Hof aanlegt in *J.B.* inzake uitlevering van documenten, zie paragraaf 4.2). Omdat de overheid het bestaan en de locatie van het Z-station en de bestanden daarop kent, voegt de handeling van het ontsleutelen door Boucher niets toe aan wat de overheid toch al weet. Boucher kan daarom worden gevorderd om alsnog een onversleutelde versie van het Z-station aan te leveren. Justitie mag vervolgens niet gebruikmaken van Bouchers handeling die het Z-station en de inhoud daarvan authenticeert en moet via andere bewijsmiddelen de link tussen Boucher en de bestanden aantonen.[228]

6.4.3 Gavegnano

Het Court of Appeals for the Fourth Circuit oordeelde in een zaak tegen Derek F. Gavegnano eveneens dat er sprake was een 'foregone conclusion' bij het verkrijgen van zijn wachtwoord tot versleutelde bestanden.[229] Gavegnano gebruikte een laptop die hem door de overheid ter beschikking was gesteld en waarvoor hij een gebruikersverklaring had ondertekend met een 'acceptable use policy'. Toen Gavegnano werd verdacht van bezit van kinderpornografie terwijl hij in Qatar was, werd zijn computer in beslag genomen. Nadat hij zijn recht op toegang tot een advocaat had ingeroepen, werd hem gevraagd om zijn wachtwoord tot de computer, dat hij vervolgens gaf. Op de computer werd kinderpornografie aangetroffen, waarvoor hij werd veroordeeld. Gavegnano betoogt nu in beroep (iets wat hij overigens niet in eerste

227 Ibid. [met weglating van zaakverwijzingen].
228 Ibid.
229 *United States* v *Gavegnano*, 2009 WL 106370 (4th Cir. Jan. 16, 2009).

aanleg had aangevoerd) dat zijn recht onder het Vijfde Amendement is geschonden.
Het Hof besteedt weinig woorden aan de afwijzing van dit verweer:

> 'Gavegnano's Fifth Amendment claim, based on the fact that, after invoking his right to consult with an attorney, he was asked for, and revealed, the password to the computer, also fails. Any self-incriminating testimony that he may have provided by revealing the password was already a "foregone conclusion" because the Government independently proved that Gavegnano was the sole user and possessor of the computer.'[230]

Met andere woorden, het feit dat Gavagnano zijn wachtwoord had gegeven had geen element van authenticatie van de computer en de bestanden daarop, omdat justitie via andere bewijsmiddelen de band tussen verdachte en zijn computer en de bestanden daarop kon aantonen. In een dergelijk geval heeft het afgeven van een wachtwoord geen 'testimonial' karakter. Aangezien ook de andere verweren falen, blijft de veroordeling in stand.

6.4.4 Kirschner[231]

Thomas J. Kirschner werd verdacht van ontvangst van kinderpornografie en door de Assisant U.S. Attorney gevorderd te verschijnen voor een *grand jury*, en daarbij 'all passwords used or associated with the (...) computer (...) and any files' ter beschikking te stellen. Anders dan in *Boucher* of *Gavegnano* gaf justitie hierbij niet precies aan dat ze met andere bewijsmiddelen kon aantonen dat Kirschner de beschikking had over de wachtwoorden; er is eerder sprake van een visexpeditie naar alle mogelijk relevante wachtwoorden. Deze zaak is daarmee een voorbeeld van een geval waarin het geen 'uitgemaakte zaak' is dat de verdachte controle heeft over het wachtwoord.
De zaak is verder vooral interessant omdat een decryptiebevel wordt geplaatst in de context van eerdere rechtspraak over het afgeven van een combinatiecode tot een kluis. De Assistant Attorney had de vordering omschreven als 'It's like giving the combination to a safe', en de rechter baseert zich dan ook op twee eerdere zaken waarin verwezen werd naar de vraag of een (immateriële) toegangscode voor een kluis gevorderd mag worden. In *Doe*[232] werd verdachte gevorderd om een formulier te ondertekenen waarmee hij buitenlandse banken autoriseerde om informatie te geven over eventuele rekeningen aldaar, waarbij hij niet hoefde te erkennen of dergelijke rekeningen daadwerkelijk bestonden. Aangezien het zetten van een handtekening op zo'n formulier geen authenticerende werking heeft voor de band tussen verdachte en bankrekening (waarvan het bestaan immers in het mid-

230 Ibid.
231 *United States* v *Kirschner*, 2010 WL 1257355 (E.D. Mich. Mar. 30, 2010).
232 *United States* v *Doe*, 487 U.S. 201, 212 (1987). Deze zaak werd in *Boucher* aangehaald als Doe-II.

den gelaten werd) maar slechts een blanco autorisatie inhield, viel dit niet onder het Vijfde Amendement. Het Supreme Court vergeleek de blanco autorisatie met het afgeven van een materiële sleutel van een brandkast:

> 'In our view, such compulsion is more like "be[ing] forced to surrender a key to a strongbox containing incriminating documents," than it is like "be[ing] compelled to reveal the combination to [petitioner's] wall safe. (…) In Doe, the Court pointed out that "neither the form [het autorisatieformulier, BJK] nor its execution communicates any factual assertions, implicit or explicit, or conveys any information to the Government."'[233]

Het uitleveren van een materiële sleutel van een brandkast verschilt van het afgeven van een immateriële toegangscode tot een kluis, omdat bij het laatste het vertellen van de toegangscode een impliciet feit communiceert, namelijk dat de verdachte de toegangscode kent. Bij uitlevering van een materiële sleutel is er geen sprake van een dergelijke impliciete erkenning. De rechter in *Kirschner* gebruikt nu dit onderscheid om te betogen dat een wachtwoord vergelijkbaar is met de immateriële toegangscode tot een kluis en niet met een fysieke sleutel, en daarom een 'testimonial' karakter heeft:

> 'In the instant case, forcing the Defendant to reveal the password for the computer communicates that factual assertion to the government, and thus, is testimonial – it requires Defendant to communicate "knowledge," unlike the production of a handwriting sample or a voice exemplar.'[234]

Vervolgens past de rechter *Hubbell* toe, de zaak waarin de verdachte was gevorderd om een aantal documenten uit te leveren, die ook in *Boucher-I* een belangrijke rol speelde:

> '"The assembly of those documents was like telling an inquisitor the combination to a wall safe, not like being forced to surrender the key to a strongbox." [Hubbell at 2047.]
> In the instant case, even if the government provides Defendant with immunity with regard to the act of producing the password to the grand jury, that does not suffice to protect Defendant's invocation of his Fifth Amendment privilege in response to questioning that would require him to reveal his password. (…) This case is not about producing specific documents – it is about producing specific testimony asserting a fact. The Hubbell opinion further stated, directly relevant to the instant case: "Compelled testimony that communicates information that may 'lead to incriminating evidence' is privileged even if the information itself is not inculpatory."'

233 *United States* v *Kirschner*, citerend uit *United States* v *Doe*, 487 U.S. 201 (1987).
234 *United States* v *Kirschner*.

Het is met andere woorden niet genoeg om immuniteit voor de handeling van het wachtwoord zelf te geven; als die handeling een 'testimonial' karakter heeft, wat hier het geval is, zal de immuniteit zich ook moeten uitstrekken tot de resultaten van de handeling, oftewel de toegankelijk gemaakte bestanden. Omdat justitie echter geen immuniteit voor het resultaat had toegezegd, was de vordering in strijd met het Vijfde Amendement. De rechter vernietigde dan ook de vordering tot uitlevering van wachtwoorden en bestanden.

6.4.5 Fricosu[235]

Bij een doorzoeking van de woning waar Ramona Camelia Fricosu met haar kinderen en moeder woonde, werden drie pc's en drie laptops in beslag genomen, waaronder een laptop die in de slaapkamer van verdachte werd aangetroffen. Deze laptop bleek beveiligd met PGP Desktop en was niet te kraken. Het scherm dat bij opstarten werd getoond, identificeerde de computer als 'RS.WORKGROUP.Ramona' (de andere, onversleutelde, laptops hadden als 'Registered Owner' staan 'Scott' (de naam van de ex-echtgenoot) en 'Elena').
De volgende dag luisterde justitie een telefoongesprek af dat Fricosu had met haar voormalig echtgenoot, die destijds in hechtenis zat. Uit het gesprek blijkt dat Fricosu niet wil dat 'ze' iets ('it') vinden waarvan ze denkt dat het op haar laptop staat, waarbij ze zich afvraagt of de computer beveiligd was. Ook zegt ze dat haar advocaat heeft gezegd dat zij geen wachtwoorden hoeft te geven omdat 'ze' zelf hun zaken moeten uitzoeken. Gebaseerd op dit gesprek vordert justitie, op basis van de All Writs Act, dat Fricosu de onversleutelde inhoud van haar laptop ter beschikking stelt, waarbij immuniteit wordt aangeboden voor het testimoniale karakter van deze handeling. Zij weigert en roept het Vijfde Amendement in.
Ten aanzien van het recht gaat het wederom om de vraag of de handeling van het ontsluiten van documenten 'testimonial' is doordat (zoals *Hubbell* stelt) de uitlevering erkent dat het document bestaat, onder controle van de verdachte valt en authentiek is. De rechter bespreekt de 'small universe of decisions' omtrent het Vijfde Amendement in relatie tot ontsleutelbevelen, namelijk alle hierboven behandelde uitspraken. Vervolgens past hij dit toe op de feiten in deze zaak:

> 'There is little question here but that the government knows of the existence and location of the computer's files. The fact that it does not know the specific content of any specific documents is not a barrier to production. [See Boucher II] (…)
> Additionally, I find and conclude that the government has met its burden to show by a preponderance of the evidence that the Toshiba Satellite M305 laptop computer belongs to Ms. Fricosu, or, in the alternative, that

235 *United States* v *Fricosu* (D.CO. Jan. 23, 2012) (No. 10-CR-00509-REB).

> she was its sole or primary user, who, in any event, can access the encrypted contents of that laptop computer.'[236]

Dit oordeel is gebaseerd op het feit dat de laptop de naam 'RS.WORKGROUP.Ramona' toonde, in haar slaapkamer was aangetroffen, dat zij in het telefoongesprek duidelijk verwees naar een (versleutelde) laptop die zij had, en dat de andere inbeslaggenomen laptops niet versleuteld waren. Verweren als zou iemand anders de laptop verplaatst of 'Ramona' genoemd hebben, zijn onwaarschijnlijk. Het is daarom 'more likely than not' dat de computer toebehoorde aan Fricosu en door haar gebruikt werd.
Dat Fricosu niet alleen de laptop in gebruik had maar ook (nog steeds) bij de bestanden kan (oftewel dat zij haar wachtwoord nog kent), motiveert de rechter niet. Mogelijk heeft de rechter dit afgeleid uit de opmerking in het telefoongesprek dat haar advocaat had gezegd dat ze geen wachtwoorden hoefde te geven, terwijl Fricosu daarvoor zelf had gezegd 'because they will have to ask for my help uhm and in another way I don't want them to find it let them let them work for it', waarmee ze op zijn minst de verdenking op zich laadt wel te kunnen maar niet te willen ontsleutelen. Wellicht speelt ook mee dat de laptop in haar slaapkamer bovenop de laptophouder was aangetroffen, en dus vermoedelijk recent door haar was gebruikt.
De rechter concludeert dat het Vijfde Amendement niet in het geding is. Fricosu wordt bevolen een onversleutelde kopie van de harde schijf van haar laptop te overhandigen, waarbij de overheid de handeling van het overhandigen van deze onversleutelde gegevens niet tegen haar mag gebruiken.[237]

6.4.6 Doe (in re Grand Jury Subpoena Duces Tecum)[238]

Iemand met een YouTube-account werd verdacht van het verspreiden van kinderpornografie. Drie IP-adressen vanwaaraf het account was gebruikt, werden herleid tot hotels, en John Doe bleek de enige gemeenschappelijke hotelgast te zijn geweest. Daarop werd een hotelkamer waar Doe verbleef doorzocht en werden twee laptops en vijf externe harde schijven in beslag genomen. Bepaalde onderdelen van de harde schijven bleken ontoegankelijk voor forensisch onderzoekers. John Doe werd daarop gevorderd om voor de *grand jury* de onversleutelde inhoud van zijn laptops en harde schijven ter beschikking te stellen, met belofte van immuniteit voor de terbeschikkingstelling van het materiaal (maar niet voor afgeleid gebruik daarvan). Doe verscheen voor de *grand jury* (zonder raadsman) en beriep zich op het Vijfde Amendement, dan wel op het feit dat hij niet in staat was om te ontsleutelen. Voor deze weigering werd hij veroordeeld als schuldig aan 'contempt of

236 Ibid.
237 Ibid.
238 *United States* v *John Doe*, in re Grand Jury Subpoena Duces Tecum (11 Cir Feb. 23, 2012).

court'.[239] (Dat is enigszins vergelijkbaar met het niet voldoen aan een ambtelijk bevel, art. 184 Sr, maar met een discretionaire bevoegdheid voor de rechter om de strafmaat te bepalen.[240])
Het Court of Appeals for the 11th Circuit behandelt Doe's beroep tegen deze veroordeling. Een belangrijke rol in de zaak speelt de verklaring van forensisch onderzoeker McCrohan, die meer dan 5 TB aan data van de gegevensdragers had onderzocht. De schijven bleken versleuteld met TrueCrypt en er konden geen data worden achterhaald, maar de forensisch onderzoekers geloofden wel dat er data waren te vinden op de versleutelde delen van de harde schijven.

> 'In support of this belief, the Government introduced an exhibit with nonsensical characters and numbers, which it argued revealed the encrypted form of data that it seeks.
> In his testimony on cross-examination by Doe, however, McCrohan conceded that, although encrypted, it was possible that the hard drives contain nothing. Doe asked McCrohan, "So if a forensic examiner were to look at an external hard drive and just see encryption, does the possibility exist that there actually is nothing on there other than encryption? In other words, if the volume was mounted, all you would see is blank. Does that possibility exist?" McCrohan responded: "Well, you would see random characters, but you wouldn't know necessarily whether it was blank."[241]
> The forensic analysis was able to identify two passwords, neither of which revealed any information when entered. When pressed by Doe to explain why investigators believed something may be hidden, McCrohan replied, "The scope of my examination didn't go that far." In response to further prodding, "What makes you think that there are still portions that have data[?]," McCrohan responded, "We couldn't get into them, so we can't make that call." Finally, when asked whether "random data is just random data," McCrohan concluded that "anything is possible."'[242]

Het is niet omstreden dat de decryptie afgedwongen en incriminerend is; het gaat wederom om de vraag of de handeling van decryptie 'testimonial' is. Het hof verwijst naar de 'foregone conclusion'-doctrine uit *Fischer*, waarin werd gesteld dat het dwingen tot afgifte van belastingdocumenten buiten het Vijfde Amendement viel omdat de handeling van afgifte niet het bestaan, de

239 Het vonnis van de rechtbank op de dag zelf was dat Doe schuldig was aan 'criminal contempt', maar een herzien vonnis van twee dagen later wijzigde dit in 'civil contempt'. Hij bleef echter in voorlopige hechtenis totdat het hof van beroep zijn vrijlating beval.

240 18 U.S.C. 401.

241 'McCrohan's admission that blank space appears as random characters is supported by TrueCrypt's description on its website: "[F]ree space on any TrueCrypt volume is always filled with random data when the volume is created and no part of the (dismounted) hidden volume can be distinguished from random data." Hidden Volume, TrueCrypt, www.truecrypt.org/docs/?s=hidden-volume (last visited January 31, 2012).' [voetnoot in origineel]

242 *United States* v *John Doe*, in re Grand Jury Subpoena Duces Tecum (11 Cir Feb. 23, 2012).

beschikkingsmacht of authenticiteit van de documenten aantoonde; deze elementen waren immers een 'foregone conclusion', zodat het uitleveren nauwelijks iets toevoegde aan het totaal van kennis van de overheid. In *Hubbell* was er echter onvoldoende onafhankelijk bewijs van het bestaan van documenten, die in te algemene termen waren gevorderd:

> 'While in Fisher the Government already knew that the documents were in the attorneys' possession and could independently confirm their existence and authenticity through the accountants who created them, here the Government has not shown that it had any prior knowledge of either the existence or the whereabouts of the 13,120 pages of documents ultimately produced by respondent. The Government cannot cure this deficiency through the overbroad argument that a businessman such as respondent will always possess general business and tax records that fall within the broad categories described in this subpoena.'[243]

Volgens het hof zijn er twee situaties waarin het ter beschikking stellen van iets ('an act of production') niet 'testimonial' is. Ten eerste de situatie waarin het individu niet gebruik hoeft te maken van 'the contents of his or her mind', zoals bij allerlei vormen van fysiek bewijs; en ten tweede de situatie waarin de handeling weliswaar iets onthult over het bestaan, de beschikkingsmacht of authenticiteit van materiaal (en dus wel een beroep wordt gedaan op het gebruik van de geest voor de handeling), maar waarin de overheid met 'reasonable particularity' kan aantonen dat zij reeds bekend is met het materiaal. Toegepast op Doe, oordeelt het Hof dat decryptie een beroep doet op de inhoud van Doe's geest (en dus niet een puur fysieke handeling is) en neerkomt op het erkennen van zijn kennis van het bestaan en de locatie van mogelijk belastende bestanden, van zijn beschikkingsmacht erover en van het feit dat hij in staat is te ontsleutelen. Decryptie is dus 'testimonial'. De vervolgvraag is dan

> 'whether the purported testimony is a "foregone conclusion." We think not. Nothing in the record before us reveals that the Government knows whether any files exist and are located on the hard drives; what's more, nothing in the record illustrates that the Government knows with reasonable particularity that Doe is even capable of accessing the encrypted portions of the drives.
> To be fair, the Government has shown that the combined storage space of the drives could contain files that number well into the millions. And the Government has also shown that the drives are encrypted. The Government has not shown, however, that the drives actually contain any files, nor has it shown which of the estimated twenty million files the drives are capable of holding may prove useful. The Government has emphasized at

243 *United States* v *Hubbell*, 530 U.S. at 44–45, 147 L. Ed. 2d 24 (2000), geciteerd in ibid.

> every stage of the proceedings in this case that the forensic analysis showed random characters. But random characters are not files; because the TrueCrypt program displays random characters if there are files and if there is empty space, we simply do not know what, if anything, was hidden based on the facts before us. It is not enough for the Government to argue that the encrypted drives are capable of storing vast amounts of data, some of which may be incriminating. In short, the Government physically possesses the media devices, but it does not know what, if anything, is held on the encrypted drives. Along the same lines, we are not persuaded by the suggestion that simply because the devices were encrypted necessarily means that Doe was trying to hide something. Just as a vault is capable of storing mountains of incriminating documents, that alone does not mean that it contains incriminating documents, or anything at all.'

De casus in kwestie valt daarom veel meer aan de *Hubbell*-kant dan aan de *Fischer*-kant van het spectrum van 'foregone conclusions' (in EHRM-termen zou men kunnen zeggen dat *Doe* eerder valt aan de *Funke*- en *J.B.*-kant dan aan de *Saunders*-kant van het spectrum).
De rechtbank zou de vordering nog steeds hebben kunnen doorzetten door immuniteit te verlenen, maar vanwege 18 U.S.C. §§ 6002-6003[244] moet deze immuniteit zich niet alleen uitstrekken over de gevorderde handeling maar ook over het verdere gebruik van het resulterende materiaal. 'Use *and derivative-use immunity* establishes the critical threshold to overcome an individual's invocation of the Fifth Amendment privilege against self-incrimination. No more protection is necessary; *no less protection is sufficient*.'[245] Aangezien het decryptiebevel alleen immuniteit verleende voor de handeling maar niet voor afgeleid gebruik, was dit in strijd met het Vijfde Amendement. Doe wordt daarom vrijgesproken van civiele belediging van het hof.

6.4.7 Conclusie

De Amerikaanse rechtspraak levert een interessante blik op de verhouding tussen een ontsleutelplicht en het nemo-teneturbeginsel. De zaken gaan over een vordering door een *grand jury* (enigszins vergelijkbaar met een vordering door een rechter-commissaris). Centraal hierin staat de vraag of de handeling van decryptie (of dat nu het uitleveren van een wachtwoord of sleutel is of het zelf ontsleutelen) 'testimonial' is, dat wil zeggen een element heeft van het afleggen van een verklaring. Aangezien de sleutel of het wachtwoord zich in

244 §6002 bepaalt dat 'no testimony or other information compelled under [an immunity] order (or any information directly or indirectly derived from such testimony or other information) may be used against the witness in any criminal case, except a prosecution for perjury, giving a false statement, or otherwise failing to comply with the order'.

245 *Kastigar* v *United States*, 406 U.S. 441, 460 (1972), geciteerd in *United States* v *John Doe*, in re Grand Jury Subpoena Duces Tecum (11 Cir Feb. 23, 2012) (mijn cursivering).

het hoofd van de verdachte bevindt, is er geen sprake van een fysieke handeling maar moet verdachte zijn geest gebruiken. Daarmee geeft hij in beginsel toe dat hij kennis heeft van het bestaan van en beschikkingsmacht heeft over de resulterende documenten of geeft hij impliciet de authenticiteit ervan toe. Dat maakt decryptie in beginsel 'testimonial'. De vordering is dan alleen toegestaan als het bestaan van de documenten een 'foregone conclusion' is, dat wil zeggen dat de overheid met voldoende specificiteit moet kunnen bewijzen dat de documenten bestaan. Dit vergt een casusspecifieke beoordeling. In *Boucher-II* en *Fricosu* was het voldoende duidelijk dat er incriminerende bestanden op de harde schijf stonden; in *Kirschner* en *Doe* was dat niet zo. In *Gavegnano* had verdachte zelf zijn wachtwoord gegeven waarna kinderporno was aangetroffen, en omdat de overheid onafhankelijk daarvan kon aantonen dat hij de enige gebruiker van de computer was, gaf de ontsluiting door verdachte van de kinderporno geen (voor het bewijs nodige) verklaring van beschikkingsmacht of authenticiteit.
Iets minder expliciet motiveren de uitspraken of de verdachte in staat is te ontsleutelen, maar ook dat zal in de casusspecifieke beoordeling hebben meegewogen. Boucher had zelf aan de grens zijn wachtwoord ingevoerd en Gavegnano had zijn wachtwoord na overleg met de advocaat gegeven; bij Fricosu wees het afgetapte telefoongesprek erop dat zij beschikkingsmacht had over de bestanden op haar laptop. In *Kirschner* en *Doe* (in re Grand Jury Subpoena Duces Tecum) was het niet nodig om verder in te gaan op de vraag of verdachte in staat was te ontsleutelen, omdat de vordering te vaag was en, in het geval van Doe,[246] het zelfs niet voldoende was aangetoond dat er wel versleutelde bestanden op de harde schijf stonden.
In gevallen waarin justitie niet voldoende onafhankelijk bewijs heeft van het bestaan van belastende bestanden en verdachtes beschikkingsmacht daarover, schendt een ontsleutelbevel het nemo-teneturbeginsel. Die schending kan worden gecompenseerd door immuniteit te beloven, maar die moet zich dan niet alleen uitstrekken over de ('testimonial') handeling van decryptie zelf maar ook over de bestanden die worden ontsleuteld. Die bestanden kunnen dus niet voor bewijs in strafzaken tegen verdachte worden gebruikt[247] (maar eventueel wel tegen anderen, en ze kunnen informatie opleveren over bijvoorbeeld slachtoffers).

246 Daarbij merkt het hof in die zaak ook nog op dat '[a]t the show cause hearing, there was no evidence that Doe was the only person who had access to his hard drives. Nor was there any evidence that he was capable of decrypting the drives' contents.' *United States* v *John Doe*, in re Grand Jury Subpoena Duces Tecum (11 Cir Feb. 23, 2012)

247 Behalve als bewijs van meineed of het afleggen van een valse verklaring; vgl. de Nederlandse regeling in art. 30 en 32 Wet op de parlementaire enquête.

6.5 Overige landen

Voor het doel van dit onderzoek is de analyse van buitenlandse wetgeving beperkt tot ons omringende landen, aangevuld met de VS vanwege de specifieke jurisprudentie aldaar. In bovenstaand overzicht is *Duitsland* niet zelfstandig behandeld, omdat het geen expliciete ontsleutelplicht heeft ingevoerd. Volgens de literatuur kan aan niet-verdachte derden door de Duitse autoriteiten wel worden gevraagd om wachtwoorden of sleutels af te geven, op basis van de standaardbevoegdheden voor het horen van getuigen en uitlevering van voorwerpen.[248] Voor de oplossing van het cryptoprobleem voor de opsporing zet Duitsland niet in op een ontsleutelplicht maar op het onderscheppen van informatie 'bij de bron' (door manipulatie van de communicatiesoftware van de eindgebruiker) dan wel door een doorzoeking op afstand. Hiervoor zijn Trojaanse paarden (in de literatuur 'Bundestrojaner' genoemd) ontwikkeld die op afstand geplaatst worden op computers van verdachten. De regulering van deze bevoegdheden is echter nog niet uitgekristalliseerd.[249]

Voor de volledigheid van het inzicht in de situatie in het buitenland bespreek ik in deze paragraaf nog kort diverse *andere landen* die een ontsleutelplicht kennen. Voor zover mij bekend, gaat het om Antigua & Barbuda, Australië, Ierland, India, Maleisië, Singapore, Thailand, Trinidad & Tobago en Zuid-Afrika. Voor een beschrijving van deze wetgeving verwijs ik naar mijn *Crypto Law Survey*.[250]

Van deze landen heeft alleen *Australië* een algemene ontsleutelplicht, ingevoerd door de Cybercrime Act (2001) (Cth), door invoeging van s. 3LA in de Crimes Act 1914. Deze ontsleutelplicht geldt bij alle strafbare feiten uit de Crimes Act 1914.[251] De meeste landen hebben de ontsleutelplicht opgenomen in een cybercriminaliteitswet, waarbij een ontsleutelbevel mag worden gegeven bij misdrijven die onder die wet strafbaar zijn gesteld of waarbij bevoegdheden uit die wet zijn toegepast. India en Zuid-Afrika kennen de ontsleutelplicht voor eindgebruikers alleen bij afgetapte communicatie. Ierland heeft een ontsleutelplicht in de Electronic Commerce Act 2000 voor onderzoek naar fraude met digitale handtekeningen.

In de meeste landen omvat het decryptiebevel zowel het meewerken door de geadresseerde aan ontsleuteling als het afgeven van een sleutel of wachtwoord. In Trinidad & Tobago kan alleen om de sleutel worden gevraagd. In Ierland kan de geadresseerde alleen worden bevolen zelf te ontsleutelen maar niet om de sleutel af te geven. Dat zal ingegeven zijn doordat het gaat

248 Gerhards 2010, p. 301-302.
249 Zie Brunst & Sieber 2010, p. 69-70.
250 http://rechten.uvt.nl/koops/cryptolaw (geraadpleegd 1 september 2012).
251 Zie www.austlii.edu.au/au/legis/cth/consol_act/ca191482/s3la.html (geraadpleegd 1 september 2012). Daarnaast is door de Cybercrime Act 2001 (Cth) een identieke ontsleutelplicht ingevoerd in s. 201A van de Customs Act 1901 voor doorzoekingen door de douane.

om onderzoek naar digitale handtekeningen, waarbij afgifte van de privésleutel alle daarmee geplaatste handtekeningen waardeloos zou maken.
Het niet meewerken aan het ontsleutelbevel wordt in de meeste landen gesanctioneerd met substantiële gevangenisstraffen, variërend van één jaar (Ierland) of twee jaar (Australië,[252] Trinidad & Tobago) tot zeven jaar (India) of zelfs tien jaar (Zuid-Afrika). Thailand heeft gekozen voor een andere modaliteit, namelijk een boete van maximaal 200.000 baht (ongeveer € 5.000) met een dwangsom van 5.000 baht (ruim € 100) per dag totdat de geadresseerde voldoet aan het bevel.
In geen van deze landen is bij de formulering van de ontsleutelplicht een nemo-teneturclausule opgenomen. Dat zou kunnen betekenen dat het ontsleutelbevel ook aan verdachten mag worden gegeven, maar dat hangt af van de wetssystematiek van het land; mogelijk bestaat er een algemene nemo-teneturbepaling in het recht dat ook op dit bevel van toepassing is – iets wat binnen het bestek van dit onderzoek niet onderzocht kon worden.
Voor dit rapport lijkt vooral Australië van belang, omdat het een generieke ontsleutelplicht heeft en als land met een *common law*-rechtsstelsel vaak aansluit bij ontwikkelingen in andere Angelsaksische landen, zoals het VK en de VS. Het ontsleutelbevel in s. 3LA van de Crimes Act 1919 mag expliciet ook aan de verdachte worden gegeven – dat is ook de belangrijkste geadresseerde, aangezien de opsomming van geadresseerden in s. 3LA(2)(b) begint met de persoon 'reasonably suspected of having committed the offence stated in the relevant warrant'. De vraag is dan of de verdachte zich kan beroepen op het in de *common law*-rechtspraak ontwikkelde 'privilege against self-incrimination'. Dat lijkt niet het geval.
De decryptiebepalingen zijn ingevoerd mede als uitvloeisel van aanbevelingen uit het zogeheten Walsh Report uit 1996, dat had opgemerkt ten aanzien van het toenemende cryptogebruik door misdadigers: 'The invocation of the principle of non self-incrimination may well represent the polite end of the possible range of responses.' Omdat de opsporing te veel geblokkeerd zou worden als cryptosleutels niet toegankelijk zouden worden, deed het rapport de aanbeveling een decryptiebevel in te voeren 'notwithstanding the principle of self-incrimination'.[253] Ondanks protest van onder andere burgerrechtenorganisaties werd de bepaling ingevoerd.[254] Daarmee is het *common law*-beginsel van nemo tenetur niet meer van toepassing: een wettelijke bepaling die voldoende expliciet is, geldt als speciale regel die voorgaat boven de algemene regel, en de bepaling van s. 3LA lijkt voldoende expliciet.[255] Daarom kunnen verdachten zich niet verschonen van het ontsleutelbevel. Er lijkt overigens weinig of niet te worden vervolgd voor het niet nakomen van het bevel; in de praktijk fungeert de bepaling vooral als stok achter

252 In Australië was bij invoering van de bepaling de straf op decryptieweigering zes maanden; dit is later verhoogd tot twee jaar. De straf op decryptieweigering bij douaneonderzoek is nog steeds zes maanden.
253 Walsh 1996, §§1.1.14, 3.2.4, 3.5.3 en 6.2.22.
254 James 2004, p. 20.
255 Gregor Urbas, Australian National University, persoonlijke mededeling 11 augustus 2012.

de deur en er wordt vaak meegewerkt. De aandacht gaat daarbij echter vooral uit naar niet-verdachte systeembeheerders.[256] Tekenend is ook dat de beschikbare literatuur over s. 3LA Crimes Act 1914 niet de mogelijke inbreuk op het nemo-teneturbeginsel bekritiseert, maar een op Foucault gebaseerde kritiek geeft op het verplichten van niet-verdachte derden om te ontsleutelen, waarmee de overheid (onschuldige) computergebruikers disciplineert en hun handelingsvrijheid inperkt.[257] In de online gepubliceerde rechtspraak[258] komt s. 3LA ook niet voor (behalve in één zaak waarin het wordt genoemd als voorbeeld van een omissiedelict waarbij iets niet doen strafbaar is gesteld ongeacht eventuele schade[259]). Daarom is het al met al moeilijk te zeggen hoe in de Australische rechtspraktijk het decryptiebevel aan verdachten functioneert.

6.6 Conclusie

Uit dit hoofdstuk blijkt dat, in tegenstelling tot in 2000, inmiddels de nodige landen een ontsleutelplicht voor verdachten hebben. De ons omringende landen met een met Nederland vergelijkbaar rechtssysteem hebben uiteenlopende wetgeving: Duitsland kent geen ontsleutelplicht, België heeft – net als Nederland momenteel – een decryptiebevel dat niet aan verdachten mag worden gegeven, terwijl Frankrijk een decryptiebevel aan verdachten kent met een substantiële strafbaarstelling op weigering (3-5 jaar gevangenisstraf) en de mogelijkheid om de straf op het gronddelict te verhogen bij decryptieweigering. Ook in Angelsaksische landen is inmiddels een ontsleutelplicht ingevoerd; in het VK en Australië via wetgeving en in de VS via rechtspraak. Van deze landen kent het VK de meest uitvoerige regeling, waarbij gedetailleerd wordt bepaalde onder welke omstandigheden en hoe een decryptiebevel kan worden gegeven en wat de bewijslastverdeling is als de verdachte beweert de sleutel niet (meer) te hebben. Weigering mee te werken is in het VK strafbaar met maximaal twee jaar gevangenisstraf (of maximaal vijf jaar bij kinderporno of terrorisme); in Australië staat er eveneens maximaal twee jaar op. In de VS kan de verdachte bij weigering worden veroordeeld wegens (civiele of strafrechtelijke) 'contempt of court' (enigszins vergelijkbaar met het niet voldoen aan een ambtelijk bevel, art.184 Sr, maar met een discretionaire bevoegdheid voor de rechter om de strafmaat te bepalen).
De landen die een ontsleutelplicht voor verdachten hebben ingevoerd, beschouwen het decryptiebevel als een (kennelijk) aanvaardbare inbreuk op het nemo-teneturbeginsel. In het VK is in de enige rechtszaak tot nu toe over dit onderwerp geoordeeld dat een decryptiebevel niet in strijd is met het nemo-teneturbeginsel. In een handvol rechtszaken in de VS worden langza-

256 Ibid.
257 James 2004.
258 www.austlii.edu.au (geraadpleegd 1 september 2012).
259 *Commonwealth Director of Public Prosecutions* v *Poniatowska* [2011] HCA 43 (26 October 2011).

merhand contouren duidelijk van de voorwaarden waaronder een decryptiebevel verenigbaar is met het 'privilege against self-incrimination', dat qua invulling grote gelijkenissen vertoont met het nemo-teneturbeginsel in de interpretatie van het EHRM. Een gemeenschappelijke bevinding uit deze rechtspraak is dat een sleutel of wachtwoord weliswaar feitelijk van aard is, maar dat de handeling van het afgeven van de sleutel of het zelf ontsleutelen een 'testimonial' karakter heeft, omdat het impliciet de band van verdachte met het versleutelde materiaal erkent. Het decryptiebevel maakt daarom inbreuk op nemo tenetur, maar die inbreuk is volgens Amerikaanse rechtspraak gerechtvaardigd, hetzij als het een uitgemaakte zaak ('foregone conclusion') is om wat voor bestanden het gaat en dat de verdachte de sleutel kent, hetzij als er immuniteit wordt beloofd voor het resulterende (belastende) materiaal. In de uitspraak in het VK speelt een belangrijke rol dat de regeling vele *checks and balances* kent en dat de zittingsrechter een discretionaire bevoegdheid heeft om eventueel incriminerend bewijs terzijde te leggen.

De vraag is welke lessen Nederland kan trekken uit dit overzicht van de buitenlandse wetgeving. Rechtsfiguren uit een buitenlands stelsel kunnen nooit zomaar worden overgeplant in de nationale wetgeving; elke rechtsregel fungeert immers binnen de context van het eigen systeem. De Belgische wetgeving op het gebied van computercriminaliteit vertoont de meeste gelijkenissen met die in Nederland; als de Nederlandse wetgever wil aansluiten bij vergelijkbare rechtsstelsels, dan biedt het Belgische recht geen argument om een ontsleutelplicht voor verdachten in te voeren.

De Franse wetgeving kan om twee redenen bezwaarlijk als voorbeeld dienen. Ten eerste is de historische ontwikkeling van cryptografieregulering fundamenteel anders in Frankrijk; de ontsleutelplicht voor verdachten dient daar vooral als compensatie voor het loslaten van het eerdere, restrictieve, vergunningstelsel met sleuteldeponering. Ten tweede is de wetgeving zonder veel discussie ingevoerd, in de hectiek van terrorismebestrijding in de directe nasleep van de aanslagen van 11 september 2001. Om deze redenen kunnen moeilijk argumenten worden ontleend aan de Franse wetgeving om een ontsleutelplicht voor verdachten in Nederland in te voeren.

De Amerikaanse rechtspraak kan weliswaar inspiratie bieden voor de dogmatische discussie waarom en hoe een ontsleutelplicht precies inbreuk maakt op nemo tenetur en in welke gevallen die inbreuk aanvaardbaar is, maar kan vanwege de verschillen in rechtssysteem niet direct aanknopingspunten bieden voor een regeling in Nederland. De regeling van opsporingsbevoegdheden in het Nederlandse continentale (*civil law*-)systeem is gebaseerd op specifiek vastgelegde wettelijke bevoegdheden van officier van justitie en rechter-commissaris, terwijl de Amerikaanse opsporingsbevoegdheden in het *common law*-systeem veel algemener zijn geregeld en zich uitkristalliseren in rechtspraak over de verenigbaarheid van specifieke opsporingsmethoden met de Amerikaanse grondwet.

Mijns inziens biedt de Britse regeling de meeste aanknopingspunten voor de Nederlandse beleidsvorming. Weliswaar staat het Britse recht ook in de *common law*-traditie, maar de opsporingsbevoegdheden vallen tegelijkertijd onder het EVRM en moeten dus voorzienbaar zijn geregeld, wat zich onder andere vertaalt in gedetailleerde wetgeving, zoals bij het decryptiebevel dat een onderdeel is van de enigszins met de Wet BOB vergelijkbare Regulation of Investigatory Powers Act 2000. Wel moeten twee aspecten van de Britse context goed voor ogen worden gehouden wanneer de Nederlandse wetgever inspiratie zou willen putten uit de Britse regeling.
Ten eerste gaat het VK (of in elk geval Engeland en Wales) over het algemeen zeer ver in het toestaan van opsporingsmethoden die een inbreuk op grondrechten maken; het VK wordt daarom vaak aangehaald als het voorbeeld van een land dat het meest in de buurt komt bij een 'surveillance society' of Big Brother-maatschappij.[260] Zo is de Britse regulering van DNA-databanken uiteindelijk in Straatsburg afgeschoten omdat deze qua omvang en bewaartermijn veel verder ging dan andere Europese landen.[261] Ook wat betreft het gebruik van 'adverse inferences' is de Britse wetgeving vergaand, zoals blijkt uit de diverse zaken die daarover het Europees Hof hebben bereikt (*John Murray*, *Averill*, *Conlon*, *Beckles*).
Ten tweede – en dat moet gezien worden als een tegenwicht van het vorige – is de Britse wetgeving niet alleen zeer gedetailleerd maar ook met veel waarborgen omkleed. Een onderdeel van de regeling van bijzondere opsporingsbevoegdheden is de controle door de Interception of Communications Commissioner en de Chief Surveillance Commissioner, die als onafhankelijk toezichthouder jaarlijks onderzoek doen naar de uitoefening van bevoegdheden en daarover openbaar rapporteren. Nederland kent een dergelijke toezichthouder niet, en zou daarom goed moeten kijken naar het algehele stelsel van *checks and balances* als het opsporingsbevoegdheden uit de Britse regeling zou willen navolgen in het Nederlandse recht.
Een ander belangrijk onderdeel in het Britse systeem is de algemene bewijsuitsluitingsregel van s. 78 van de Police and Criminal Evidence Act 1984. In de zaak-*R* v *S and A* overwoog de rechter dat bij een decryptiebevel niet op voorhand kan worden bepaald of versleuteld materiaal belastend is – daarvoor moet het immers eerst ontsleuteld worden – en dat daarom niet direct gevaar voor zelfbelasting aanwezig is. Een decryptiebevel is daarom aanvaardbaar omdat, als het ontsleutelde materiaal inderdaad belastend blijkt te zijn, de rechter alsnog kan besluiten om dit materiaal uit te sluiten van het bewijs omdat het onder dwang is verkregen en daarmee – achteraf – in strijd blijkt met het nemo-teneturbeginsel. Voor Nederland betekent dit dat als het de Britse regeling zou navolgen, artikel 359a Sv (op basis waarvan de rechter bewijs kan uitsluiten als vormen zijn verzuimd) een belangrijke rol zou (moeten) gaan spelen, waarbij de zittingsrechter dan van geval tot geval moet

260 Murakami Wood 2006, House of Commons Home Affairs Committee 2008.
261 EHRM 4 december 2008, *S. en Marper t. Verenigd Koninkrijk*, App.nrs. 30532/04, 30566/04.

beoordelen of de dwang die op de verdachte is uitgeoefend om te ontsleutelen, zijn recht om zichzelf niet te belasten van zijn betekenis heeft ontdaan. Het is dus niet gezegd dat het invoeren van een wettelijke regeling naar het model van de Britse RIPA een algemeen antwoord geeft op de vraag of een ontsleutelbevel aan verdachten verenigbaar is met het nemo-teneturbeginsel; dat zal nog steeds casuïstisch moeten worden beantwoord.
Al met al betekent dit dat de buitenlandse wetgeving laat zien dat er diverse regelingen mogelijk zijn voor een ontsleutelbevel voor verdachten en dat die – volgens de systemen in die landen – onder bepaalde voorwaarden verenigbaar zijn met het nemo-teneturbeginsel. De Britse regeling lijkt daarbij het meest uitgewerkt en doordacht. Als de Nederlandse wetgever de Britse regeling zou willen navolgen, is het wel belangrijk dat hij daarbij oog heeft voor de context daarvan, namelijk enerzijds de Britse tendens van een *surveillance*-maatschappij en anderzijds de *checks and balances*, zoals onafhankelijk toezicht en de mogelijkheid voor de zittingsrechter om achteraf bewijsmateriaal uit te sluiten.

7 Analyse

In hoofdstuk 2 is een samenvatting gegeven van de factoren en argumenten die een rol speelden in het onderzoek uit 2000 (deelvraag 1). In de hoofdstukken 3-6 zijn vervolgens de ontwikkelingen geschetst die zich sindsdien hebben voorgedaan in technologie en criminaliteit, het Europese recht, het Nederlandse recht en het buitenlandse recht (deelvragen 2-4). Nu komt het aan op een integratie van deze bevindingen in een hernieuwde afweging: in hoeverre is, gegeven de geschetste ontwikkelingen, een decryptiebevel verenigbaar met het nemo-teneturbeginsel? (deelvraag 5) Omdat het gaat om een hernieuwde afweging, structureer ik de analyse aan de hand van de zeven factoren uit de studie uit 2000, waarbij ik steeds beoordeel of en hoe de situatie sinds 2000 is veranderd.

7.1 Probleemschets

Wat zijn de gevolgen voor opsporing en vervolging wanneer misdadigers cryptografie gebruiken om mogelijk bewijsmateriaal te verbergen? Het probleem van crimineel cryptogebruik is conceptueel nog precies hetzelfde als in 2000: het is in potentie een serieus probleem waar weinig goede oplossingen voor bestaan. Een ontsleutelplicht voor verdachten is een van de weinige gerichte methoden die het probleem als zodanig aanpakken. In 2000 waren de precieze aard en omvang van het probleem echter onduidelijk bij gebrek aan concreet inzicht in de situatie in de praktijk. Er waren geen aanwijzingen dat cryptografie opsporingsonderzoeken substantieel hinderde, laat staan blokkeerde.
Dat is inmiddels enigszins veranderd. Het gebruik van cryptografie door verdachten is aanzienlijk toegenomen, met name bij opslag van gegevens en met name, vooralsnog, bij bepaalde groepen kinderpornonetwerken. Deze gebruiken niet alleen vrij beschikbare programma's als PGP – dat in de jaren negentig al verkrijgbaar was – maar ook nieuwe programmatuur als TrueCrypt, dat specifieke functionaliteiten biedt om bestanden niet alleen te versleutelen maar ook te verbergen in (sub)containers op de harde schijf, waardoor het niet makkelijk aan te tonen is dat er überhaupt versleutelde gegevens op de harde schijf staan. Dat betekent dat (onkraakbare) cryptografie inmiddels vaker voorkomt in opsporingsonderzoeken en dat het probleem voor de opsporing dus groter geworden is (maar ook dat de effectiviteit van een ontsleutelplicht er niet per se op vooruitgaat, zie paragraaf 7.6 hieronder).
Of het probleem nu dusdanige vormen aanneemt dat het een aanzienlijke inbreuk op grondrechten zou rechtvaardigen, valt echter niet te zeggen. Rond de Amsterdamse zedenzaak is de opsporing gestuit op beveiligde computers en versleutelde bestanden, maar dat heeft niet tot grote problemen bij de vervolging geleid. Robert M. gaf vrijwillig zijn wachtwoorden, de crypto van Flovin O. bleek door het NFI te kraken, en de weigering van Matthijs van der M.

werd door de rechter gebruikt bij de verwerping van bepaalde verweren, bij de beslissing over onttrekking aan het verkeer en als strafverzwarende omstandigheid. Men kan dus niet zeggen dat het toenemend gebruik van cryptografie een onneembaar obstakel is met het huidige arsenaal aan juridische middelen.
Wel blijkt uit de Amsterdamse zedenzaak dat er ook andere redenen kunnen zijn om de inhoud van versleutelde bestanden te achterhalen dan de vervolging van de verdachte. Wanneer Robert M. zijn wachtwoorden niet zou hebben gegeven, zou het veel moeilijker zijn geweest vast te stellen wie precies slachtoffer waren geweest van seksueel misbruik. Dit zou een reden kunnen zijn om in bepaalde gevallen een ontsleutelbevel te geven aan verdachten, met de belofte van immuniteit voor het daaruit voortvloeiende bewijs. Eventueel belastend materiaal dat na ontsleuteling tevoorschijn komt, kan dan niet voor het bewijs tegen de verdachte worden gebruikt, maar wel voor de hulp aan de slachtoffers en mogelijk ook voor het bewijs bij de vervolging van anderen dan de verdachte.

7.2 De internationale context

In 2000 waren er geen landen met een ontsleutelplicht voor verdachten en er waren ook geen directe aanwijzingen dat landen dat zouden gaan invoeren. Deze internationale context gaf in elk geval geen argument vóór invoering in Nederland van een decryptiebevel aan verdachten, eerder een argument daartegen.
Inmiddels is de internationale context substantieel gewijzigd. Het Cybercrime-Verdrag laat het aan de lidstaten en de rechtsontwikkeling over om te bepalen in welke mate een ontsleutelplicht verenigbaar is met het nemo-teneturbeginsel. Van de ons omringende landen heeft België een decryptiebevel ingevoerd dat niet aan verdachten mag worden gegeven, maar Frankrijk en het Verenigd Koninkrijk kennen inmiddels een ontsleutelplicht voor verdachten. Het VK heeft daartoe een uitgebreide wettelijke regeling getroffen voor de uitvoering en sanctionering van de ontsleutelplicht. In Frankrijk beperkt de wettelijke regeling zich tot sanctionering van een weigering te ontsleutelen met een zelfstandige strafbaarstelling en strafverhoging. Daarnaast heeft Australië een decryptiebevel ingevoerd dat zich specifiek tot verdachten richt, die zich niet mogen verschonen op basis van het nemo-teneturbeginsel; daarover is echter nog geen rechtspraak beschikbaar. In de VS bestaat een ontsleutelplicht voor verdachten die zich uitkristalliseert in de rechtspraak, waarbij langzamerhand de contouren duidelijk worden van wanneer een decryptiebevel aan verdachten wel of niet in strijd is met het 'privilege against self-incrimination' (dat veel gelijkenissen heeft met het nemo-teneturbeginsel zoals dat door het EHRM wordt geïnterpreteerd).

Hieruit blijkt dat wetgevers en rechters in het VK, de VS, Australië en Frankrijk een strafrechtelijk gesanctioneerde ontsleutelplicht voor verdachten onder bepaalde voorwaarden aanvaardbaar achten. Daarbij moet wel worden aangetekend dat de rechtspraak in het VK en de VS vooralsnog beperkt is tot lagere rechters en dat noch de hoogste nationale rechter noch het EHRM zich heeft uitgelaten over de verenigbaarheid van de ontsleutelplicht met het nemo-teneturbeginsel. Er zijn echter geen aanwijzingen dat de uitspraken van lagere rechters die een decryptiebevel aan verdachten aanvaardbaar achtten of het half dozijn veroordelingen voor decryptieweigering in het VK dermate grote juridisch-dogmatische vragen hebben opgeroepen dat de zaken spoedig voor de hoogste rechter worden gebracht. De verenigbaarheid van een decryptiebevel met het nemo-teneturbeginsel lijkt in deze landen geen vraag die ten principale negatief moet worden beantwoord, maar een vraagstuk dat in de rechtspraak casuïstisch kan worden bepaald.

7.3 De reikwijdte van de huidige bevoegdheden

De studie uit 2000 achtte de mogelijkheden van justitie om cryptografie te kraken gering, maar de mogelijkheden redelijk groot om papiertjes met wachtwoorden te vinden of een makkelijk wachtwoord te raden. Daarin is volgens mij weinig veranderd. Wel is het zo dat naarmate meer misdadigers cryptografie gebruiken – wat het geval is – het vaker zal voorkomen (in absolute zin maar niet per se in relatieve zin) dat justitie een wachtwoord niet kan achterhalen. Als dat ernstige zaken betreft, zal justitie andere bevoegdheden moeten kunnen inzetten om achter de onversleutelde inhoud te komen.
De studie uit 2000 noemde direct afluisteren en infiltratie – bevoegdheden die net waren ingevoerd met de Wet bijzondere opsporingsbevoegdheden – als potentiële alternatieve bevoegdheden om informatie te vergaren buiten het proces van versleuteling om, met de kanttekening dat het geen volwaardige alternatieven waren omdat ze andersoortige informatie opleveren. Inmiddels is wel duidelijk dat deze bevoegdheden maar beperkt soelaas kunnen bieden voor cryptogebruik door misdadigers. Infiltratie is een zware en risicovolle bevoegdheid die beperkt wordt ingezet, en die zeker bij kinderpornonetwerken problematisch is omdat nieuwkomers vaak alleen toegelaten worden als ze nieuw kinderpornomateriaal inbrengen. Nu mogen politieinfiltranten wel strafbare feiten plegen ten behoeve van de infiltratie, maar de politie wil geen 'vers' kinderpornomateriaal inbrengen in kinderpornonetwerken vanwege de gevolgen daarvan voor de slachtoffers.[262]

262 Nationaal Rapporteur Mensenhandel 2011, p. 164-165.

Direct afluisteren biedt op zich wel een interessante mogelijkheid, namelijk om een Trojaans paard[263] (meer in het bijzonder een *keylogger* of 'sleutelvanger') te plaatsen in het toetsenbord of de computer van verdachte, dat wil zeggen een programmaatje dat toetsaanslagen afvangt (al dan niet met automatische herkenning van wachtwoorden) en heimelijk doorstuurt. Op basis van artikel 126l/s/zf lid 2 Sv kan de politie een plaats of woning betreden om een afluisterapparaatje te plaatsen, waaronder ook een sleutelvangerprogramma valt. Een woning mag alleen betreden worden met rechterlijke machtiging en bij zeer ernstige misdrijven (met acht jaar of meer gevangenisstraf). Los van deze zware eisen is de bevoegdheid in de praktijk vaak moeilijk toepasbaar omdat het alleen toegestaan is om fysiek in te breken en een programmaatje te installeren, maar niet om via het internet het Trojaanse paard te installeren (bijvoorbeeld door de computer te hacken of het als een virus te versturen in de hoop dat de computer van de verdachte daarmee besmet raakt). Het fysiek installeren gaat gepaard met grotere risico's dat de opsporingsmethode ontdekt wordt, terwijl het bovendien niet altijd duidelijk is waar de computer van een verdachte zich in het huidige mobiele tijdperk bevindt. Vertegenwoordigers van justitie en politie ervaren het ontbreken van een bevoegdheid om op afstand computers van verdachten binnen te dringen als een van de grootste knelpunten in het huidige arsenaal aan digitale opsporingsbevoegdheden.[264] Voor de aanpak van het cryptoprobleem achten vertegenwoordigers van het Openbaar Ministerie het heimelijk kunnen afvangen van wachtwoorden met Trojaanse paarden veel effectiever dan het dwingen van verdachten om hun sleutel af te geven. Dat laatste zal vaak niet werken (tenzij er draconische en onaanvaardbaar hoge straffen zouden staan op niet-medewerking), terwijl Trojaanse paarden precies het probleem aanpakken, door het onderscheppen van onversleutelde gegevens of van een sleutel of wachtwoord.

> 'Al met al denk ik dat een ontsleutelplicht voor verdachten een beetje symboolwetgeving zou zijn. Waar ik meer in zie is in de voorfase het probleem van versleuteling aanpakken, door aftappen op afstand mogelijk te maken waardoor je wachtwoorden kunt onderscheppen, zodat je onderzoek kunt blijven doen zonder dat de verdachte het weet.'[265]

Ondertussen is ook een bevoegdheid ingevoerd voor inlichtingen- en veiligheidsdiensten om een decryptiebevel te geven bij gehackte of afgetapte gegevens (paragraaf 5.1.4). Vanwege de afwijkende context (nationale veiligheid)

263 Een Trojaans paard is een vorm van *malware* (kwaadaardige programmatuur) die een computer infecteert via een (ogenschijnlijk normaal) programma of bestand waarin een bepaalde functionaliteit verborgen zit (zoals de Grieken in het Paard van Troje), bijvoorbeeld om ingetoetste kredietkaartnummers te herkennen en heimelijk door te sturen of heimelijk een deur open te zetten waarmee de aanvaller op de computer kan kijken. Het lijkt in die zin op een computervirus maar verschilt daarvan omdat het zichzelf niet vermenigvuldigt. Zie verder http://nl.wikipedia.org/wiki/Trojaans_paard_(computers) (geraadpleegd 1 september 2012).

264 Interview officier van justitie. Zie ook Koops et al. 2012, paragraaf 5.2.4; Oerlemans 2011.

265 Interview officier van justitie.

valt hier niet direct een parallel te trekken met een ontsleutelplicht in strafzaken. Wel zou in voorkomende gevallen de AIVD de bevoegdheid kunnen inzetten bij terrorisme(dreiging), waardoor er iets minder noodzaak lijkt voor justitie om in terrorismeonderzoeken een ontsleutelbevel aan verdachten te kunnen geven.
Al met al is de reikwijdte van bestaande bevoegdheden sinds 2000 niet substantieel veranderd. Aangezien bevoegdheden als direct afluisteren en infiltratie weinig geschikte alternatieven blijken te zijn wanneer computeronderzoek of een tap stuit op encryptie, legt het argument dat er behoefte is aan bevoegdheden die het cryptoprobleem aanpakken nu wel meer gewicht in de schaal. Dat behoeft echter niet per se in de richting te wijzen van een ontsleutelbevel voor verdachten; het kunnen plaatsen van Trojaanse paarden die heimelijk wachtwoorden onderscheppen kan een goed, en mogelijk effectiever, alternatief zijn. Dat is echter ook een ingrijpende bevoegdheid, die meer inbreuk op de privacy maakt dan een ontsleutelplicht voor verdachten, onder andere omdat een Trojaans paard meestal meer zal afvangen dan alleen wachtwoorden en ook over langere tijd actief kan zijn. De wetgever zal dan ook een gemotiveerde belangenafweging moeten maken tussen de mogelijke alternatieven.

7.4 De reikwijdte en achtergrond van het nemo-teneturbeginsel

7.4.1 Algemeen

De studie uit 2000 leidde uit de literatuur, wetssystematiek en de (Europese) rechtspraak vier ratio's af die gezamenlijk ten grondslag liggen aan het nemo-teneturbeginsel: de procesautonomie van de verdachte, de menselijke waardigheid, het pressieverbod en de betrouwbaarheid van bewijs. Van deze ratio's wordt de menselijke waardigheid weinig genoemd in de EHRM-rechtspraak sinds 2000; het komt alleen voor in de Duitse zaken waarin een onmenselijke behandeling had plaatsgevonden (*Jalloh, Gäfgen*). De andere ratio's komen veelvuldig voor in de EHRM-rechtspraak. De procesautonomie blijkt bijvoorbeeld uit de nadruk die het Europees Hof vaak legt op de mogelijkheid die de verdachte moet hebben om bewijsmateriaal ter terechtzitting aan te vechten, waarbij in een voorfase afgedwongen verklaringen zijn procespositie niet te veel mogen beperken. Het pressieverbod komt vooral naar voren in zaken als *Gäfgen,* waarin druk is uitgeoefend die in strijd komt met het folterverbod, maar ook in zaken als *Magee,* waarin iemand in het beginstadium bij politieverhoor zonder rechtsbijstand onder druk wordt gezet. De betrouwbaarheid van het bewijs wordt vaak genoemd als overweging om onderscheid te maken tussen fysiek bewijs ('real evidence') en verklaringen. Ook de reikwijdte van het nemo-teneturbeginsel zoals vormgegeven in de rechtspraak is niet significant veranderd sinds 2000. De lijnen uit de voor

2000 gewezen standaardarresten *Funke* (uitlevering van documenten), *Saunders* (verklaringen in de voorfase) en *Salabiaku* en *John Murray* (trekken van negatieve conclusies) zijn voortgezet en verfijnd met nieuwe casuïstische invulling.
De kern van het nemo-teneturbeginsel ligt nog altijd in de verklaringsvrijheid, waar het een zeer sterke werking heeft. In de vervolgingsfase mag soms enige druk worden uitgeoefend om verklaringen te verkrijgen, maar die druk mag niet groot zijn en moet omgeven zijn met procedurele waarborgen als het voldoende informeren van de verdachte over zijn zwijgrecht en de eventuele gevolgen die zijn houding kan hebben op zijn procesgang, en vooral ook de toegang tot een advocaat.
Buiten het afleggen van verklaringen stelt nemo tenetur ook grenzen aan de medewerking die van verdachten kan worden geëist: naarmate de verdachte actiever moet meewerken, en met name als hij daarbij een intellectuele inspanning moet verrichten, zal een dwang om mee te werken eerder in strijd komen met nemo tenetur. Dat werkt vooral door in gevallen waarin bijvoorbeeld onder dwang uitlevering van documenten wordt gevorderd terwijl de overheid niet voldoende kan aantonen dat zij weet om welke documenten het precies gaat, waardoor het uitleveren door de verdachte in de buurt komt van het afleggen van een verklaring; in Amerikaanse termen is het uitleveren van documenten 'testimonial' wanneer het bestaan en de plaats van de documenten geen uitgemaakte zaak is. De Amerikaanse (*Hubbell*) en Europese (*J.B.*) rechtspraak vertonen hierin veel parallellen. Ook als de verdachte nauwelijks actief hoeft mee te werken omdat het gaat om wilsonafhankelijk materiaal waarvan het bestaan een uitgemaakte zaak is (zoals bij monsters van lichaamsmateriaal), kan het nemo-teneturbeginsel nog worden geschonden als de dwang die wordt gebruikt buitensporig en onnodig is (*Jalloh*).

7.4.2 Valt een wachtwoord binnen de reikwijdte van het nemo-teneturbeginsel?

In 2000 concludeerde ik dat bij een decryptiebevel aan verdachten een zwaar gewicht aan het nemo-teneturbeginsel toegekend moest worden. Het betrof een actieve medewerking die dichtbij het afleggen van een verklaring in de buurt komt als de verdachte zijn wachtwoord moet geven en de politie niet zeker weet dat de verdachte het wachtwoord (of de sleutel) kent – in die gevallen zou het vertellen van het wachtwoord immers de verklaring impliceren dat de verdachte over het wachtwoord beschikte. Destijds ging ik ervan uit dat er in de meeste gevallen geen zekerheid of hoge mate van waarschijnlijkheid zou bestaan dat de verdachte in staat is te ontsleutelen (wat inmiddels enigszins anders ligt, zie paragraaf 7.6) en dat daarom een ontsleutelplicht meestal de verklaringsvrijheid zou raken. Daarom zouden er zeer zwaarwegende belangen moeten zijn als de wetgever toch een ontsleutelplicht voor verdachten zou willen invoeren.

Hoe kan nu, gegeven de EHRM-rechtspraak sinds 2000, het afgeven van een wachtwoord gepositioneerd worden binnen het nemo-teneturbeginsel? Men zou geneigd zijn om, onder verwijzing naar het *Saunders*-criterium, voorop te stellen dat een wachtwoord als zodanig onafhankelijk van de wil van de verdachte bestaat; hij kan het immers niet met zijn wil veranderen. De *Saunders*-formule dat het nemo-teneturbeginsel niet ziet op materiaal dat onafhankelijk van de wil van de verdachte bestaat, wordt veelvuldig gebruikt in de rechtspraak en literatuur en is algemeen geaccepteerd. De rechtsontwikkeling sinds *Saunders* laat echter wel een verfijning van het criterium zien. In diverse arresten wijst het Europees Hof namelijk op de passage die in *Saunders* aan de befaamde formule voorafging:

> 'The right not to incriminate oneself, in particular, presupposes that the prosecution in a criminal case seek to prove their case against the accused without resort to *evidence obtained through methods of coercion or oppression in defiance of the will of the accused*.' (*Saunders*, §68, cursivering toegevoegd; herhaald in onder andere *Heaney and McGuinness*, §40, *J.B.*, §64, *Jalloh*, §100, *Gäfgen*, §168)

Hier ligt de nadruk dus niet op het *bestaan* van materiaal buiten de wil van de verdachte, maar op het *verkrijgen* van materiaal buiten de wil van de verdachte. Soms gaan deze twee gelijk op; dat is met name het geval bij de gevallen uit de *Saunders*-formule waarbij

> 'a defendant is requested to endure passively a minor interference with his physical integrity (for example when blood or hair samples or bodily tissue are taken). Even if the defendant's active participation is required, it can be seen from Saunders that this concerns material produced by the normal functioning of the body (such as, for example, breath, urine or voice samples).' (*Jalloh*, §114)

Wanneer het echter gaat om materiaal dat niet door de normale lichaamsfuncties wordt geproduceerd, gaan de criteria van wilsonafhankelijk materiaal en wilsonafhankelijke verkrijging meer uiteenlopen. De verdachte moet zich dan immers meer inspannen om materiaal dat onafhankelijk van zijn wil bestaat, te produceren. Wanneer de overheid onder dwang materiaal probeert te verkrijgen waarbij de verdachte moet meewerken op een manier die de passieve of beperkt (fysiek) actieve medewerking te boven gaat, legt het Hof meer de nadruk op het feit dat het materiaal wordt 'obtained in defiance of the will of the accused' en minder nadruk op het feit dat het materiaal onafhankelijk van de wil van de verdachte bestaat. Het pressieverbod speelt dan een belangrijkere rol (omdat vaak meer druk nodig zal zijn om de verdachte tot medewerking aan te zetten), evenals de procesautonomie (omdat

de bewijslast bij justitie ligt en het niet aan de verdachte is om actief mee te werken aan het op tafel leggen van bewijsmateriaal tegen hem).
Dat is een belangrijk gegeven als we kijken naar een van de kernvragen van het decryptiebevel: hoe moet een wachtwoord worden gekwalificeerd binnen de EHRM-rechtspraak? In theorie hangt het ervan af of het wachtwoord (ook) ergens is opgeschreven of (uitsluitend) in het hoofd van de verdachte zit. In het eerste geval is er alleen sprake van een vordering tot uitlevering van fysiek bewijs; in het tweede geval is een intellectuele inspanning van de verdachte nodig. In de praktijk zal justitie echter meestal niet (zeker) weten of het wachtwoord ergens is opgeschreven en waar dat papiertje zich bevindt; mocht dat wel het geval zijn, dan maakt een vordering tot uitlevering slechts een kleine inbreuk op het nemo-teneturbeginsel, omdat de handeling van uitlevering dan geen of weinig verklarende waarde heeft (zie het Amerikaanse leerstuk van de 'uitgemaakte zaak' en de Europese *Funke*- en *J.B.*-uitspraken). Maar in dat geval heeft het weinig meerwaarde om de verdachte tot medewerking te bevelen; als justitie immers precies weet waar een papiertje met het wachtwoord zich bevindt, kan zij net zo goed zelf dat papiertje gaan opzoeken en inbeslagnemen. We moeten dus uitgaan van situaties waarin justitie niet zeker weet of het wachtwoord is opgeschreven of geen idee heeft waar het wachtwoord dan wel opgeschreven is, oftewel situaties waarin aangenomen moet worden dat het wachtwoord feitelijk alleen in het hoofd van de verdachte bestaat.
Het gaat dan weliswaar om materiaal dat onafhankelijk van de wil van de verdachte bestaat, maar niet om materiaal dat onafhankelijk van de wil van de verdachte kan worden verkregen. Als de verdachte zijn mond wil houden, zal het wachtwoord niet te achterhalen zijn.[266] In die gevallen kan het bewijsmateriaal alleen worden verkregen door de verdachte stevig onder druk te zetten om zijn wil te beïnvloeden; een dergelijke stevige druk komt echter al snel in strijd met het pressieverbod (zie *Funke* en *J.B.* waarin de dwang om documenten uit te leveren niet aanvaardbaar werd geacht omdat het bestaan daarvan geen uitgemaakte zaak was). Voor het vorderen van een wachtwoord betekent dit, dat het alleen aanvaardbaar zou kunnen zijn als het bestaan van het wachtwoord in het hoofd van de verdachte wel een uitgemaakte zaak is, oftewel als justitie voldoende overtuigend kan aantonen dat de verdachte het wachtwoord (nog) kent. Deze constatering is vergelijkbaar met de Amerikaanse rechtspraak, die een nog wat scherpere afbakening maakt in het onderscheid tussen een fysieke sleutel en een toegangscode. Bij de uitlevering van het eerste hoeft de verdachte geen intellectuele inspanning te leveren (tenzij justitie aan het vissen is en niet weet of de sleutel bestaat), bij het laatste wel. Dat maakt het vorderen van een wachtwoord dat in het hoofd van

266 Behoudens revolutionaire ontwikkelingen in breinscans. Het valt echter niet te verwachten dat in de komende decennia hersenscans zo nauwkeurig kunnen worden dat zij wachtwoorden zouden kunnen uitlezen. Mocht dat wel zo zijn, dan wordt het 'uitlezen' van een wachtwoord meer vergelijkbaar met een bloedproef en komt de verenigbaarheid met het nemo-teneturbeginsel iets anders te liggen. Vgl. daarover Van Toor 2011.

de verdachte zit, per definitie 'testimonial'.[267] Het mag dan volgens de Amerikaanse rechtspraak alleen worden gevorderd a) als er immuniteit wordt verleend zowel voor de handeling van het afgeven van het wachtwoord (of decryptie) als voor het materiaal dat daaruit voortvloeit, of b) als het afgeven van het wachtwoord (of decryptie) geen enkele meerwaarde heeft voor het bewijs omdat de informatie die uit de decryptie naar voren komt (het bestaan, de beschikkingsmacht van verdachte over het materiaal en de authenticiteit daarvan) een 'uitgemaakte zaak' is.
Deze ontwikkelingen bevestigen dan ook de conclusie uit 2000 dat een decryptiebevel een vorm van medewerking betreft die dicht tegen de verklaringsvrijheid aanligt, omdat bewijsmateriaal onder dwang wordt verkregen tegen de wil van de verdachte. Een decryptiebevel voor verdachten maakt daarom (nog steeds) inbreuk op het nemo-teneturbeginsel. Anders dan in 2000, zou ik daar nu echter niet per se de conclusie aan willen verbinden dat er zwaarwegende redenen moeten zijn om een decryptiebevel voor verdachten in te voeren. Bij de beoordeling van de toelaatbaarheid van een inbreuk op nemo tenetur gaat het immers niet alleen om zwaarwichtige redenen van publiek belang. Het Hof noemt vier factoren die in gezamenlijkheid bepalen of een afgedwongen medewerking een schending oplevert van het nemo-teneturbeginsel:

1 de aard en mate van dwang;
2 het gewicht van het publiek belang in de opsporing en vervolging van het strafbare feit in casu;
3 de aanwezigheid van relevante waarborgen in de procedure;
4 de manier waarop het afgedwongen materiaal wordt gebruikt.[268]

Hoewel het publieke belang van een ontsleutelplicht voor verdachten niet te verwaarlozen is maar ook niet moet worden overdreven (zie paragraaf 7.1) en daarom niet in zijn algemeenheid veel gewicht in de schaal legt, betekent dit niet dat artikel 6 EVRM een ontsleutelplicht voor verdachten onmogelijk maakt. Er zijn immers allerlei modaliteiten en gradaties mogelijk die de inbreuk op nemo tenetur toch aanvaardbaar kunnen maken, zoals ook gesuggereerd wordt door de jurisprudentie uit het VK en de VS. Te denken valt aan een lage mate van dwang (het ontsleutelen betrekken bij het bewijs

267 Brenner 2002, Myers Morrison 2012. Contra Ungberg 2009, die betoogt dat een (encryptie)wachtwoord niet goed binnen het paradigma van het 'testimonial' karakter bij een uitleveringsbevel valt te positioneren. 'Encryption keys challenge courts in their application of the testimony/real evidence distinction; often a very minimal amount of testimony – sometimes a single password – shields thousands of documents that would otherwise be subject to government seizure with a simple search warrant.' Ungberg 2009, p. 554.
Terzijde wijs ik er hier nog op dat vaak gesteld wordt dat een wachtwoord als zodanig zelf niet 'testimonial' zal zijn (en mocht iemand als wachtwoord gebruiken 'ja-ik-heb-pietje-puk-vermoord' dan zal de rechter dat nooit willen gebruiken als bewijs van schuld). Soms kan een wachtwoord echter toch bewijswaarde hebben. Dat blijkt uit Rb. 's-Gravenhage 31 juli 2006, *LJN* AY5348, waarin de verdachte beweerde dat iemand anders de kinderporno op zijn harde schijf had geplaatst: 'De rechtbank acht voorts van belang dat het wachtwoord dat toegang geeft tot het kinderpornografische materiaal opgeslagen in het programma Privacy Master is opgebouwd uit het woord "[woord]", hetgeen een verwijzing bevat naar het sigarettenmerk dat verdachte volgens eigen zeggen in het algemeen rookt, en de cijfer [cijfer], hetgeen een verwijzing bevat naar de leeftijd (in 2003) en de geboortedatum van de verdachte.' Ook het wachtwoord zelf kan dus bewijs opleveren van de band van verdachte met het verborgen materiaal.

268 *Jalloh*, §117.

bij een 'formidable case', of een beperkte straf op decryptieweigering), de waarborgen (zoals de regeling in het VK waar veel *checks and balances* zijn ingebouwd) en het bewijsgebruik (zoals het verlenen van immuniteit voor decryptie of een discretionaire bevoegdheid van de rechter om gemotiveerd het afgedwongen materiaal al dan niet mee te wegen). Bij een ontsleutelplicht voor verdachten gaat het dus om een afgewogen geheel. Ik kom daar in paragraaf 7.7 op terug.

7.5 Het systeem van de Nederlandse wet

In de studie uit 2000 werd geconcludeerd dat, in het licht van het systeem van de Nederlandse wetgeving, een ontsleutelplicht voor verdachten (een actieve medewerking op de grens van een verklaring) in het commune strafrecht een unieke bevoegdheid zou zijn, en dat de wetgever daarom zeer zwaarwichtige redenen zou moeten hebben om zo'n bevoegdheid in te voeren. Tegelijkertijd suggereerde de studie dat het in het systeem van de wetgeving beter zou passen om het ontsleutelbevel wel aan verdachten te kunnen geven, waarbij verdachten zich echter zouden kunnen verschonen van nakoming van het bevel. Aangezien het decryptiebevel dicht tegen het afleggen van een verklaring ligt, zou immers beter aangesloten kunnen worden bij het zwijgrecht bij het verhoor (de verdachte mag worden verhoord maar is niet tot antwoorden verplicht en wordt daar ook vooraf op gewezen, art. 29 Sv) in plaats van het uitleveringsbevel (dat niet aan verdachten mag worden gegeven, art. 96a lid 2 Sv).
Het systeem van de Nederlandse wetgeving is niet veranderd sinds 2000. Er zijn geen strafrechtelijk gesanctioneerde plichten ingevoerd voor verdachten om actief mee te werken aan het verkrijgen van het bewijs. Een strafrechtelijk gesanctioneerd decryptiebevel voor verdachten zou daarom nog steeds een unieke bevoegdheid zijn.
In plaats van een zelfstandige sanctie op niet-meewerken aan een decryptiebevel, kan het niet meewerken echter wel op andere manier worden gebruikt tegen de verdachte. De ruimte voor de rechter om negatieve gevolgen te verbinden aan de proceshouding van verdachten is er sinds 2000 zeker niet kleiner op geworden. De Hoge Raad heeft eerder al bepaald dat als de verdachte *geen* alternatieve verklaring geeft voor een bezwarende omstandigheid, de rechter het zwijgen van de verdachte dan kan gebruiken als overweging om aan te nemen dat die omstandigheid waar en belastend is en deze aldus – in samenhang met ander bewijsmateriaal – mee kan laten wegen. Dit wordt frequent toegepast in witwaszaken, wanneer een verdachte niet enigszins aannemelijk weet te maken hoe hij aan een stapel geld is gekomen. Inmiddels heeft de Hoge Raad ook geëxpliciteerd dat het daarvoor niet nodig is dat het overige bewijsmateriaal op zich al genoeg zou zijn voor een veroordeling. Een belastende omstandigheid waarvoor de verdachte weigert een enigszins

plausibele verklaring te geven, mag dus worden gebruikt in samenhang met andere bewijsmiddelen om de stap te zetten naar een bewezenverklaring. Dit biedt ruimte voor rechters om een verdachte die weigert een harde schijf of versleutelde bestanden toegankelijk te maken, in situaties waarin de aanwezigheid van de beveiligde bestanden duidelijk vragen oproept, mee te laten wegen in het bewijs. Dat is in de praktijk inmiddels door een lagere rechter toegepast in de zaak-Matthijs van der M. Ook kan een decryptieweigering worden gebruikt bij bepaalde verweren (zoals een beroep op overmacht), bij de straftoemeting of bij de beslissing over onttrekking aan het verkeer (zie paragraaf 5.3-5.5).
Geconcludeerd kan worden dat een decyptiebevel voor verdachten nog steeds zou afwijken van het systeem van de Nederlandse wetgeving, voor zover de weigering mee te werken strafbaar zou zijn. Het past echter wel in het wetssysteem om de verdachte te vragen zijn wachtwoord te geven, waarbij hij zich desgewenst op zijn zwijgrecht kan beroepen. De verdachte neemt dan een zeker procesrisico om niet mee te werken omdat onder bepaalde omstandigheden de rechter zijn decryptieweigering kan gebruiken bij het bewijs, de straftoemeting of andere beslissingen ten nadele van de verdachte.

7.6 Handhavingsperikelen

In de studie van 2000 was een hoofdstuk gewijd aan de handhaving en technische bezwaren. In dit hoofdstuk werden enerzijds factoren genoemd die justitie zou kunnen gebruiken om te betogen dat een verdachte in staat is te ontsleutelen, maar anderzijds ook factoren die de verdediging zou kunnen gebruiken om te betogen dat de verdachte graag zou meewerken maar helaas de sleutel of het wachtwoord niet (meer) heeft. Ik schatte destijds in dat de laatstgenoemde factoren vaak sterker aanwezig zouden zijn dan de eerstgenoemde factoren. De studie concludeerde daarom dat vanwege handhavingsperikelen een ontsleutelplicht voor verdachten in de praktijk weinig effectief zou zijn. Een hoge sanctie op niet-medewerking, laat staan een omkering van de bewijslast in de hoofdzaak, zou alleen toelaatbaar zijn als het onomstotelijk zou vaststaan dat de verdachte in staat is te ontsleutelen (wat naar mijn inschatting nauwelijks zou voorkomen), terwijl een lage sanctie minder kans zou hebben het beoogde effect – daadwerkelijke ontsleuteling van verdachte bestanden – te bereiken. Daarbij kan ook nog worden gewezen op het argument van de wetgever uit 1993 om het ontsleutelbevel niet aan verdachten te geven, namelijk dat de sanctie op niet-naleving – anders dan bijvoorbeeld bij een bloedproef in het verkeer – moeilijk te relateren valt aan een gronddelict, waardoor de naleving in veel gevallen illusoir wordt (zie paragraaf 5.1.2).
Om twee redenen denk ik dat inmiddels de handhavingsproblemen minder gewicht in de schaal moeten leggen en in elk geval niet per se nopen tot een

categorische afwijzing van een ontsleutelplicht voor verdachten. Ten eerste heeft justitie waarschijnlijk ruimere mogelijkheden dan ik in 2000 inschatte om te betogen dat een verdachte in staat is te ontsleutelen. Het komt regelmatig voor dat versleutelde bestanden, bijvoorbeeld bij een doorzoeking, worden aangetroffen nadat in een voorfase de digitale activiteiten van de verdachte al heimelijk zijn onderzocht via een tap of het opvragen van verkeersgegevens. Daaruit kunnen significante aanwijzingen voortkomen dat de verdachte belastend materiaal, zoals kinderpornografie, in zijn bezit heeft (of heeft gehad). Daarbij bezitten verdachten, wederom vooral in kinderpornozaken, vaak meerdere beveiligde gegevensdragers; zeker als het om dragers met grote opslagcapaciteit gaat, kan dit vragen oproepen over de reden waarom de verdachte deze dragers in bezit heeft en waarom de inhoud beveiligd is. Ook kan uit de tap blijken hoe vaak en intensief de verdachte zijn computer gebruikt; als de doorzoeking kort volgt op een moment waarop de verdachte, blijkens de tap, zijn computer heeft gebruikt, is het aannemelijk dat de verdachte (nog) kennis heeft van het wachtwoord dat toegang geeft tot de computer. Dat geldt ook als uit de tap blijkt dat de verdachte zeer frequent zijn computer gebruikt. Daarbij geeft de ontwikkeling van de rechtspraak over negatieve gevolgtrekkingen (zie paragraaf 4.1.3 en 5.3) aan dat het niet nodig is dat justitie onomstotelijk aantoont dat de verdachte belastend materiaal heeft dat hij kan ontsleutelen, maar dat het voldoende is om dit aannemelijk te maken. Het is vervolgens aan de verdachte om een enigszins plausibele verklaring te geven voor de versleutelde bestanden dan wel om voldoende twijfel te zaaien dat hij niet (meer) in staat is om te ontsleutelen. De bewijsvoeringslast die wordt gehanteerd bij witwassen (zie paragraaf 5.3), die sterk lijkt op de bewijslastverdeling in de Britse wetgeving rond de vraag of de verdachte in staat is te ontsleutelen (paragraaf 6.3.1), biedt daarbij een interessant aanknopingspunt.

Ten tweede suggereren de ontwikkelingen in het buitenland eveneens dat er situaties zijn waarin in redelijkheid kan worden aangenomen dat de verdachte iets aan het verbergen is en waarbij zijn weigering om te ontsleutelen bestraft kan worden omdat het voldoende aannemelijk is dat hij wel kan maar niet wil ontsleutelen. De Britse en Amerikaanse rechtspraak tonen diverse gevallen waarin de verdachte 'iets uit te leggen heeft'. Nu zijn gevallen als *Boucher*, waarin een verdachte eerst zelf zijn kinderpornomateriaal aan de douane heeft laten zien, bepaald atypisch, maar er zijn ook situaties die zich met enige regelmaat kunnen voordoen, zoals *Fricosu* (waarin een afgeluisterd telefoongesprek belangrijke indicaties geeft) en *Doe* (in re Grand Jury Subpoena Duces Tecum) (waarin een vermoedelijke kinderpornodownloader vijf externe harde schijven heeft). Ook de handvol veroordelingen voor decryptieweigering in het VK suggereert dat een ontsleutelplicht voor verdachten als zodanig handhaafbaar is.

Op basis van deze twee ontwikkelingen kan worden geconcludeerd dat handhavingsproblemen geen doorslaggevend argument zijn tegen een ontsleutel-

plicht. Daarmee is echter niet gezegd dat handhaving van een ontsleutelplicht makkelijk zal zijn. De Amerikaanse rechtspraak toont ook gevallen waarin justitie niet voldoende aannemelijk kon maken dat de verdachte in bezit was van het wachtwoord (*Kirschner*) of dat er überhaupt gegevens op de harde schijf verborgen waren (*Doe* (in re Grand Jury Subpoena Duces Tecum)). Met name het laatste geval illustreert dat er nog steeds handhavingsproblemen zijn. Met programma's als TrueCrypt kunnen bestanden niet alleen makkelijk versleuteld worden maar kan ook het bestaan van de versleutelde bestanden 'aannemelijk ontkenbaar' worden gemaakt, dat wil zeggen dat de verdachte een wachtwoord kan geven om een cryptocontainer op de harde schijf te openen waarin alleen onschuldige bestanden zitten (maar die wel wat gênant zijn en die hij voor zijn vrouw verborgen wil houden), waarna het voor forensisch onderzoekers lastig aan te tonen is dat in de container nog een subcontainer verstopt zit die met een ander wachtwoord toegankelijk is.
De ontwikkeling van programma's als TrueCrypt roept twee vragen op over de zinvolheid van een ontsleutelplicht voor verdachten. Ten eerste de vraag wie je ermee 'vangt'. Vertegenwoordigers van politie en justitie zijn sceptisch over de meerwaarde van een strafrechtelijk gesanctioneerd decryptiebevel voor verdachten.

> 'Op zich zou het wel het makkelijkste zijn als je verdachte kan dwingen hun sleutel te geven, maar dat gaat misschien vijf jaar goed, daarna weet elke crimineel het en gaat niemand meer zijn sleutel geven. Je moet ook niet afhankelijk worden van medewerking van verdachten. Juist die verdachten die niet meewerken, moet je kunnen aanpakken. Anders vang je alleen de sukkels.'[269]

En specifiek ten aanzien van verdachten in kinderpornozaken:

> 'Een ontsleutelplicht zou misschien een stukje oplossing kunnen bieden, maar alleen bij bepaalde soorten verdachten; vooral de verzamelaars en/of de categorie "sufferds". Maar die werken nu ook al meestal gewoon mee; ze zijn soms blij dat hun dubbelleven ontdekt is. De hele grote jongens laten zich echt niet afschrikken. Die gebruiken de beste encryptie, [de anonimiseringstechnieken] Tor en proxies, en hebben hun beveiliging 15 lagen hoog opgestapeld; die kun je niet tappen laat staan materiaal in beslag nemen. Die zullen nooit onder strafbedreiging meewerken.
> Met een ontsleutelplicht zou je dan alleen de middengroep bereiken die tussen de verzamelaars en de grote jongens in zit. Maar dat zijn vaak verdachten die plussen en minnen en dan vaak liever zullen kiezen voor een veroordeling voor niet-meewerken dan het materiaal te ontsluiten en dan het risico te lopen van een hogere straf of TBS. Als het om zeer jonge kin-

269 Interview politie.

deren of extreem materiaal blijkt te gaan, loop je een hoger risico TBS of een langere vrijheidsstraf te krijgen.'[270]

Iets soortgelijks zal vermoedelijk ook voor andere typen misdaad opgaan, waarin er een groep van topcriminelen is die 'nergens aan meewerken, niets zeggen en de duurste advocaat bellen'[271] en een andere groep van kleine criminelen die meestal toch al meewerken. Alleen hoeft de tussencategorie niet altijd zo calculerend te zijn als bij kinderporno vaak voorkomt; het zou kunnen dat bij invoering van een strafrechtelijk gesanctioneerde ontsleutelplicht de groep mensen die meewerkt met justitie wel iets groter zou worden.[272]
De tweede vraag is welk effect de invoering van een ontsleutelplicht zou hebben op de ontwikkeling van cryptoprogramma's en het cryptogebruik van misdadigers. Sommigen vrezen een averechts effect, namelijk dat er meer programma's als TrueCrypt worden ontwikkeld waarmee verdachten plausibel kunnen weigeren mee te werken en dat misdadigers (nog) veel meer informatie gaan uitwisselen over hoe je je bestanden moet beveiligen (zie paragraaf 3.5). Of zo'n effect zal optreden is moeilijk te zeggen, maar het is niet onaannemelijk dat er een markt zou kunnen ontstaan (of de bestaande markt versterkt zou kunnen worden) voor cryptoprogramma's waarmee je versleutelde bestanden goed kunt verstoppen voor forensisch onderzoekers. Dat versterkt het punt van de eerste vraag, namelijk dat een ontsleutelplicht voor verdachten vermoedelijk hoofdzakelijk zal werken bij de categorie kleinere en niet-calculerende misdadigers (die vaak ook al vrijwillig zal meewerken bij het onderzoek).
Samenvattend levert de handhaafbaarheid een gemengd beeld op. Enerzijds lijkt een ontsleutelplicht voor verdachten in diverse gevallen wel handhaafbaar, in de zin dat justitie voldoende aannemelijk zal kunnen maken dat de verdachte met beveiligde gegevens 'iets uit te leggen heeft'. Anderzijds zal een ontsleutelplicht weinig effectief zijn bij zware en berekenende misdadigers en zullen vooral de kleinere of minder slimme misdadigers meewerken. Het is de vraag of een ontsleutelplicht daarvoor primair bedoeld moet zijn.

7.7 Opties voor een ontsleutelplicht

In de studie van 2000 onderscheidde ik, met een licht overdadige fijnmazigheid, vele mogelijke varianten van een ontsleutelplicht aan verdachten. Grofweg kwamen deze varianten neer op drie opties: A) een ontsleutelplicht met verschoningsrecht, dat wil zeggen dat het bevel van artikel 125k Sv wel aan de verdachte kan worden gegeven maar dat hij zich kan verschonen mee te werken, B) een ontsleutelplicht met bewijsuitsluiting en C) een ontsleutelplicht

270 Interview officier van justitie.
271 Interview politie.
272 Ibid.

die strafrechtelijk gesanctioneerd wordt, waarbij een decryptieweigering ofwel (1) zelfstandig strafbaar is ofwel (2) meegewogen wordt in het bewijs in de hoofdzaak. Bij optie C achtte ik het cryptoprobleem onvoldoende groot en de handhaafbaarheid te problematisch om de inbreuk op het nemo-teneturbeginsel van deze optie te rechtvaardigen. Optie B bood geen meerwaarde, omdat deze niet effectief is tegen de verdachte zelf en er voor het gebruik van ontsleuteld materiaal tegen anderen al juridische mogelijkheden bestonden. Optie A achtte ik evenmin effectief, maar wel beter passen in de systematiek van de strafvordering.
Het is nu tijd om deze opties te herwaarderen in het licht van bovenstaande bevindingen. Ik zal dat doen met als startpunt de conclusies uit paragraaf 7.4.2: het meewerken aan een decryptiebevel ligt dicht tegen de verklaringsvrijheid aan omdat bewijsmateriaal onder dwang wordt verkregen tegen de wil van de verdachte. Een decryptiebevel maakt daarom inbreuk op het nemo-teneturbeginsel. Bij de beoordeling of deze inbreuk gerechtvaardigd is moeten volgens het Europees Hof de mate van dwang, het publiek belang, de procedurele waarborgen en de manier waarop het afgedwongen materiaal wordt gebruikt in de afweging worden betrokken. Daarnaast zal ik expliciet aandacht besteden aan de effectiviteit, gezien de nadruk die de Minister van Veiligheid en Justitie hierop legt (zie paragraaf 5.1.3).

7.7.1 Optie A: een decryptieregeling conform de regeling van het verhoor

In de huidige situatie kan het bevel van artikel 125k Sv niet aan verdachten worden gegeven, maar kan politie of justitie wel de verdachte vragen om vrijwillige medewerking. De regeling van 125k Sv is geënt op de regeling van uitlevering van documenten of voorwerpen in artikel 96a Sv. Het vragen om een wachtwoord of ontsleuteling lijkt echter meer op het vragen om een verklaring dan om het uitleveren van een voorwerp (zie paragraaf 7.4.2). Het past daarom beter in het systeem van de Nederlandse wet om decryptie door verdachten te normeren conform de regeling van het verhoor dan conform de regeling voor het uitleveren van voorwerpen. Dit wil zeggen dat de verdachte wel formeel kan worden gevraagd te ontsleutelen, maar dat hij niet tot meewerken is verplicht, dat hem vooraf wordt meegedeeld dat hij niet hoeft mee te werken, en dat de rechter of opsporingsambtenaar geen (onevenredige) druk op hem uitoefent om mee te werken.
Dit zou kunnen worden geregeld door in het huidige artikel 125k Sv[273] het derde lid, dat zegt dat het bevel niet aan de verdachte wordt gegeven, te schrappen, waarmee geëxpliciteerd wordt dat een ontsleutelbevel aan de verdachte kan worden gegeven. Om duidelijk te maken dat het bij verdachten echter niet om een bevel gaat waarvan het niet-meewerken wordt gesanctio-

273 En de overige ontsleutelplichten bij gegevensvordering en aftappen (zie paragraaf 5.1.2), die mutatis mutandis kunnen worden gewijzigd. Voor de leesbaarheid beperk ik me hier tot de situatie van bij een doorzoeking aangetroffen opgeslagen gegevens.

neerd door artikel 184 Sr, zou een bepaling kunnen worden opgenomen (in de wet zelf of wellicht alleen in de Memorie van Toelichting) met de strekking dat artikel 29 Sv van overeenkomstige toepassing is. Dit is een wat ongemakkelijke constructie, omdat er sprake is van een 'bevel' waaraan de verdachte niet hoeft te voldoen. Een zuiverdere maar wat omslachtigere regeling zou kunnen zijn om het huidige artikel 125k lid 3 Sv intact te laten en een sui-generisbepaling in te voeren, bijvoorbeeld in een nieuw artikel 125ka Sv, dat analoog aan artikel 29 is geredigeerd. Een dergelijke bepaling regelt dan dat in alle gevallen waarin een verdachte wordt gevraagd toegang te verschaffen tot een beveiligde computer of versleutelde gegevens te ontsleutelen, de rechter of ambtenaar zich onthoudt van alles wat de strekking heeft een wachtwoord te verkrijgen waarvan niet kan worden gezegd dat dit in vrijheid is afgegeven; dat de verdachte niet tot medewerking verplicht is; dat voor het verzoek de verdachte medegedeeld wordt dat hij niet verplicht is mee te werken en dat deze mededeling in een proces-verbaal wordt opgenomen. Een derde mogelijkheid is om het decryptieverzoek niet op het niveau van de wet te regelen maar in lagere regelgeving, wat de mogelijkheid biedt om een meer uitgewerkte regeling te treffen.

Elk van deze mogelijkheden verschilt materieel niet veel van de huidige situatie, maar het zou nuttig kunnen zijn om de huidige informele praktijk van verzoeken om vrijwillige medewerking op enige wijze te formaliseren. Daardoor worden namelijk expliciet de waarborgen van toepassing die gelden bij verhoorsituaties, zoals de cautie en toegang tot een advocaat conform de *Salduz*-jurisprudentie. Deze waarborgen spelen een belangrijke rol in het oordeel van het Europees Hof of het nemo-teneturbeginsel is geschonden. Dat is relevant, omdat ook bij een decryptieverzoek (in plaats van een decryptiebevel) het nemo-teneturbeginsel in het geding is. Er gaat immers enige dwang uit van de context waarin de verdachte om zijn wachtwoord wordt gevraagd. De verdachte moet zich realiseren dat als er een mogelijk belastende omstandigheid is (zoals een onverklaarbaar grote hoeveelheid versleutelde schijfruimte) waar hij geen enigszins plausibele verklaring voor geeft, hij langer object zal blijven van onderzoek. Bovendien kan het zwijgen van de verdachte door de rechter worden gebruikt bij de afronding van het bewijs of bij de straftoemeting. Deze dwang is beperkt van aard en wordt door het Europees Hof als acceptabel gezien, zolang de rechter bij de bewijsvoering zich tenminste houdt aan de grenzen voor 'adverse inferences' die het Hof in *John Murray*, *Averill* en *Condron* heeft getrokken (en zolang de politie zich onthoudt van oneigenlijke druk in de vorm van Zaanse of nog ergere verhoormethoden of slinkse ontfutselmethoden van informanten in de politiecel). De procedurele waarborgen die samenhangen met de regeling van het verhoor kunnen helpen om enige (maar niet oneigenlijke) druk te rechtvaardigen op de verdachte om zijn wachtwoord te geven. Naast de cautie betreft dat vooral het kunnen consulteren van een advocaat wanneer een decryptiebevel wordt gegeven. Indien de politie de verdachte om de sleutel vraagt voordat

deze formeel wordt verhoord en zonder dat deze toegang tot een advocaat heeft gehad, bijvoorbeeld tijdens de doorzoeking zelf, zal het Hof vooral kijken naar de druk die daarbij op de verdachte is uitgeoefend en naar de situatie (bijvoorbeeld of de verdachte in de hectiek van de doorzoeking de gevolgen van het afgeven van zijn wachtwoord heeft kunnen overzien). Als de verdachte weigert, zal er geen sprake zijn van ontoelaatbare druk en kan hij in latere verhoren, na consultatie met zijn advocaat, bepalen of hij alsnog wil meewerken. Als de verdachte echter bij de doorzoeking wel (zonder toegang tot rechtsbijstand) zijn wachtwoord heeft afgegeven en dat tot belastend materiaal heeft geleid, zal het Hof kijken naar de manier waarop de rechter ter zitting het materiaal gebruikt en of de verdachte voldoende mogelijkheden heeft gehad om de authenticiteit en de betrouwbaarheid van het bewijs (waaronder de band tussen verdachte en het materiaal, die door het afgeven van de sleutel wordt bevestigd) aan te vechten.
Het vragen aan verdachten om hun wachtwoord te geven zal dus, vergelijkbaar met verhoorsituaties, verenigbaar zijn met het nemo-teneturbeginsel zolang politie en justitie de zorgvuldigheid in acht nemen die zij ook bij het verhoor en het gebruik van door de verdachte afgelegde verklaringen betrachten.
Maar zal een dergelijke vorm van een ontsleutelplicht voor verdachten ook effectief zijn? Aangezien de wil van verdachten om geen medewerking te verlenen moet worden gerespecteerd, hoeft een ontsleutelverzoek niet tot resultaat te leiden. De ervaring leert echter dat veel verdachten die zich bij het verhoor op hun zwijgrecht kunnen beroepen, toch bereid blijken verklaringen af te leggen. Dat zou ook kunnen gebeuren bij een ontsleutelingsverzoek. Een advocaat zou bijvoorbeeld het voorhanden bewijsmateriaal kunnen bekijken en inzien dat er sprake is van een *John Murray*- of *Averill*-achtige situatie die om een verklaring roept, en op basis daarvan de verdachte adviseren om desgevraagd zijn wachtwoord af te geven. Ook zal een meewerkende proceshouding beter kunnen uitpakken bij de strafoplegging dan een tegenwerkende houding.
Deze overwegingen gelden overigens ook voor de huidige situatie bij verzoeken om vrijwillige medewerking. Voor de effectiviteit zal het formaliseren van een decryptieverzoek vermoedelijk niet veel uitmaken. Niettemin kan een regeling die het decryptieverzoek normeert conform de regeling van het verhoor wel een zinvolle optie zijn, omdat het door de explicitering van de bijbehorende waarborgen betere garanties biedt dat het nemo-teneturbeginsel wordt gerespecteerd wanneer politie of justitie, met de dwang die inherent is aan de context, een verdachte vraagt om zijn wachtwoord af te geven.

7.7.2 Optie B: een decryptiebevel met bewijsuitsluiting

In deze optie wordt een ontsleutelbevel gegeven waarbij de verdachte een bepaalde mate van bewijsuitsluiting wordt toegezegd, namelijk dat het mee-

werken en eventueel ook de resultaten daarvan niet voor het bewijs tegen de verdachte zullen worden gebruikt. Dit zal met name van belang zijn in gevallen waarin een verdachte niet wil meewerken en waarin ontsleuteling relevant is om andere redenen dan de vervolging van de verdachte zelf (zie onder). Dit kan op zich al binnen het huidige wettelijke kader bij een verzoek om vrijwillige medewerking: het Openbaar Ministerie zou bij een decryptieverzoek – al dan niet geformaliseerd conform optie A – een schriftelijke toezegging kunnen doen het meewerken en eventueel ook de resultaten niet als bewijs tegen de verdachte te gebruiken. Een dergelijke toezegging heeft rechtskracht op basis van het vertrouwensbeginsel, ook als het niet wettelijk is geregeld. Niettemin zou een wettelijke regeling wenselijk kunnen zijn in de vorm van een decryptiebevel met de mogelijkheid om bewijsuitsluiting toe te zeggen, waarbij de wetgever deze toezegging nader kan inkaderen, vergelijkbaar met de regeling van het voorwaardelijk sepot (art. 244 Sv). Dit komt de rechtszekerheid ten goede, niet alleen van de verdachte maar ook van slachtoffers. De laatsten hebben volgens artikel 12 Sv immers het recht zich te beklagen over niet-vervolging, wat een mogelijk gevolg zou kunnen zijn van de toezegging van bewijsuitsluiting als er onvoldoende overig bewijs is.
De bewijsuitsluiting kan zich uitstrekken over:

- het wachtwoord[274] en de handeling van het ontsleutelen of het afgeven van het wachtwoord, waarmee de verdachte het bestaan, de authenticiteit en zijn beschikkingsmacht over de bestanden erkent;
- de bestanden die na ontsleuteling of het afgeven van het wachtwoord te voorschijn komen;
- het bewijsmateriaal dat (na doorrechercheren) wordt gevonden als uitvloeisel van het ontsleutelde materiaal.

Aangezien de inbreuk op nemo tenetur primair in het eerste aspect is gelegen – daarin ligt immers het karakter van het afleggen van een verklaring waardoor een decryptiebevel inbreuk maakt op het zwijgrecht – zou men kunnen stellen dat de bewijsuitsluiting uitsluitend voor dat aspect nodig is. Die redenering gaat echter niet op. De bestanden zijn weliswaar reeds in bezit van justitie, maar ze zijn niet toegankelijk en in die zin dus ook weer niet in bezit van justitie. Met het ontsleutelen geeft de verdachte aan justitie toegang tot de bestanden, zodat de handeling van het ontsleutelen feitelijk neerkomt op het uitleveren van de bestanden. Met andere woorden, de handeling van ontsleutelen en het beschikbaar komen van de bestanden zijn dusdanig met elkaar verbonden dat hiertussen geen scheiding niet te maken valt. Als de belofte van bewijsuitsluiting de verdachte ervan moet overtuigen mee te werken, dan zal de bewijsuitsluiting zich dus ook moeten uitstrekken over de

274 Zie noot 267 voor een voorbeeld waar het wachtwoord zelf bewijswaarde heeft.

resulterende bestanden zelf. De Amerikaanse rechtspraak ondersteunt deze conclusie.[275]

Kan eventueel wel gebruik worden gemaakt van afgeleid bewijs (het derde element)? Hier zitten er meer stappen tussen de handeling van het meewerken en het belastende bewijs, waardoor de handeling minder direct zelfbelastend is. Volgens de leer van de verboden vruchten (als de boom vergiftigd is, mogen de vruchten ervan ook niet worden gegeten) mag indirect afgeleid materiaal echter evenmin worden gebruikt voor het bewijs. Dat blijkt uit *Gäfgen*: als er een causaal verband is tussen de afgedwongen medewerking en het bewijs dat later wordt gevonden, mag het afgeleide bewijs niet worden gebruikt. Ook dit is in lijn met de Amerikaanse rechtspraak bij ontsleutelbevelen.[276]

Wanneer aan de verdachte bewijsuitsluiting wordt toegezegd voor het ontsleutelen en het daaruit resulterende materiaal, zal er geen inbreuk zijn op het nemo-teneturbeginsel. Er is immers geen sprake van gevaar voor zelfbelasting en dus ook niet van dwang om mee te werken aan het verkrijgen van belastend bewijsmateriaal.

Dat roept, evenals bij de vorige optie, wel de vraag op wat de effectiviteit is van een ontsleutelplicht met bewijsuitsluiting. Deze heeft geen meerwaarde in de zaak tegen de verdachte zelf, maar wel voor andere aspecten. Ten eerste kan het ontsleutelde materiaal bewijsmateriaal opleveren tegen medeverdachten of anderen. Tegen derden mag het bewijsmateriaal gewoon worden gebruikt (dat ligt alleen anders als het bewijsmateriaal door de manier van verkrijging onbetrouwbaar wordt – zie *Lutsenko* – maar dat is bij ontsleuteling niet aan de orde).

Ten tweede kan het materiaal relevant zijn om slachtoffers – bijvoorbeeld van seksueel misbruik – te identificeren (of mogelijke slachtoffers uit te sluiten) en de slachtofferhulp daarop toe te snijden. In zedenzaken waarbij het belangrijk is om de aard en omvang van het slachtofferschap vast te stellen, kan een ontsleutelplicht met toezegging van bewijsuitsluiting een belangrijk middel zijn. Het vergt wel een soms moeilijke afweging van justitie tussen het belang van vervolging van de verdachte en het belang van slachtofferhulp. Bovendien bestaat het gevaar dat de verdachte aan strafvervolging kan ontkomen door in een vroeg stadium mee te werken onder toezegging van bewijsuitsluiting, terwijl misschien uit ander onderzoek later alsnog hetzelfde

275 Ungberg vindt de Amerikaanse rechtspraak op dit punt te absoluut en suggereert een tussenvariant, namelijk om geen immuniteit te verlenen voor bestanden waar justitie specifiek naar op zoek is (zoals kinderporno of financiële gegevens over een bepaald belastingjaar), maar wel immuniteit te geven voor andere bestanden die met het wachtwoord bloot komen te liggen. Het ontsleutelbevel kan dan niet tot visexpedities leiden. Het betekent wel een inbreuk op het nemo-teneturbeginsel, maar die is voor Ungberg aanvaardbaar omdat het alternatief – zware heimelijke opsporingsmethoden – een grotere aantasting van grondrechten oplevert. Zie Ungberg 2009, p. 556.

276 Zie de regeling van 'derivative-use immunity' in noten 244-245 en bijbehorende tekst.

of ander overtuigend bewijs naar voren had kunnen komen.[277] Dat betekent dat deze optie alleen ingezet zou moeten worden in gevallen waarin het gezochte materiaal op geen enkele andere wijze kan worden achterhaald (dus als laatste redmiddel), of in gevallen waarin er al het nodige andere bewijsmateriaal voorhanden is voor een veroordeling met een substantiële straf.

7.7.3 Optie C1: een decryptiebevel met strafbaarstelling van weigering

In tegenstelling tot de vorige opties, waarbij medewerking min of meer vrijwillig (optie A) of vrijblijvend (optie B) is, is het ook mogelijk om daadwerkelijk dwang uit te oefenen om te ontsleutelen. Het decryptiebevel is dan minder snel verenigbaar met het nemo-teneturbeginsel, maar afhankelijk van de voorwaarden kan een afgedwongen decryptiebevel toch aanvaardbaar zijn in het licht van artikel 6 EVRM.
De meest directe vorm van dwang is de dreiging met straf als de verdachte niet meewerkt (minder directe vormen van dwang komen in de volgende opties aan bod). Dit kan ten eerste door simpelweg artikel 125k lid 3 (eerste volzin) Sv[278] te schrappen, waardoor het bevel ook aan de verdachte kan worden gegeven. Decryptieweigering is dan strafbaar op grond van artikel 184 Sr, het opzettelijk niet voldoen aan een ambtelijk bevel, waarop een maximumstraf staat van drie maanden gevangenis of een geldboete van de tweede categorie. Ten tweede is het mogelijk een zelfstandige strafbaarstelling van decryptieweigering in te voeren, zoals in de Britse, Franse en Australische wetgeving is gebeurd.
In beide gevallen zal een verdachte dan kunnen worden veroordeeld als hij weigert zijn wachtwoord af te geven, althans als dit opzettelijk gebeurt.[279] Dat wil zeggen dat een verdachte wel in staat is te ontsleutelen, maar hij bewust weigert dit te doen. Een veroordeling voor decryptieweigering is daarom alleen mogelijk als justitie voldoende aannemelijk maakt dat de verdachte het wachtwoord kent; wanneer de verdachte daartegenover argumenten stelt die voldoende twijfel zaaien dat hij het wachtwoord is vergeten – of dat er geen versleutelde gegevens in een container zijn verstopt – zal hij vrijuit gaan. Het zal van de omstandigheden van het geval afhangen of het bewijsbaar is dat een verdachte het wachtwoord kent (zie paragraaf 7.6). Van belang daarbij is dat de bewijslast of de verdachte in staat is te ontsleutelen, zo lijkt mij, zwaarder wordt naarmate de straf op decryptieweigering hoger is; de rechter moet er immers wel zeer van overtuigd zijn dat de verdachte opzettelijk wei-

277 Vergelijk de situatie bij parlementaire enquêtes naar bijvoorbeeld grootschalige fraude – waar een absolute spreekplicht bestaat maar waarbij verklaringen nooit als bewijs in rechte kunnen worden gebruikt, art. 30 Wet op de parlementaire enquête – waarbij moet worden voorkomen dat sleutelfiguren in de fraudezaak zo snel mogelijk zelfbelastende verklaringen bij de enquêtecommissie gaan afleggen waardoor ze vervolgens immuun voor strafvervolging worden.

278 En de nemo-teneturbepaling in de overige ontsleutelplichten, zie noot 273.

279 Het strafbaar stellen van niet-opzettelijke weigering te ontsleutelen, zoals in de Wiv 2002 is gebeurd (zie paragraaf 5.1.4), komt neer op een risicoaansprakelijkheid die een onaanvaardbare drempel zou opwerpen voor burgers en bedrijven om cryptografie te gebruiken; strafbaarstelling van decryptieweigering kan daarom alleen zien op opzettelijke weigering.

gert (in plaats van dat hij het wachtwoord is vergeten), wil hij hem een hoge gevangenisstraf opleggen.
Dat brengt ons bij een van de belangrijkste discussiepunten bij strafbaarstelling van decryptieweigering: welke strafbedreiging moet er worden gekozen? Bij voorkeur dient de strafbedreiging zowel effectief (aanzettend tot medewerking) als rechtmatig (verenigbaar met de dwang die het EHRM toestaat bij inbreuken op nemo tenetur) en redelijk (in verhouding staand tot het delict waarvan verdachte wordt verdacht) te zijn. Deze vereisten zijn echter moeilijk te combineren. Een hogere straf zal effectiever zijn maar ook sneller in de EVRM-gevarenzone komen, en omgekeerd. En het feit dat het moeilijk is de straf te relateren aan de straf op het hoofddelict, was voor de wetgever in 1993 al een reden om de verdachte uit te sluiten van het bevel.[280] De versleutelde bestanden zullen immers vaak juist inzicht moeten geven in wat de verdachte precies heeft gedaan:

> 'Bij alcoholcontrole is het relatief simpel: dan val je in de hoogste categorie als je weigert mee te werken. Maar bij kinderporno weet je niet wat een proportionele strafcategorie is, dat kun je niet inschatten als je geen inzicht hebt in de bestanden – gaat het om een verzameling van bestaand materiaal, of om beelden van eigen misbruik? Om prepuberale of puberale kinderporno? Om veel of weinig? Gáát het überhaupt wel om strafbaar materiaal of misschien ook om andere gegevens die de verdachte gewoon niet openbaar wil hebben? Als burger en als officier van justitie vind ik dat je hier niet de bewijslast zou moeten omdraaien. Bij kinderporno gaat het om een grote stap van een taakstraf naar vele jaren gevangenisstraf. Als je iedereen die niet meewerkt de hoogste categorie straf zou geven, zou je iedereen behandelen alsof het een Robert M. is. En als je de straf lager zou maken, dan heb je geen strafbedreiging meer die verdachten zou aanzetten om mee te werken.'[281]

Ondanks de moeilijkheid een passend strafmaximum te bepalen, hebben diverse landen toch een specifieke strafbaarstelling ingevoerd: Frankrijk heeft gekozen voor drie jaar (tot vijf jaar als decryptie de gevolgen van een misdrijf had kunnen verzachten), het Verenigd Koninkrijk voor twee jaar (met verhoging tot vijf jaar voor terrorisme- en kinderpornozaken) en Australië aanvankelijk voor zes maanden en later voor twee jaar. Daaruit kan worden afgeleid dat een bandbreedte van 2-3 jaar – met eventueel hogere straffen voor bijzondere categorieën – kennelijk als een goede middenweg wordt gezien tussen enerzijds een te lage, niet-effectieve straf en anderzijds een te hoge, disproportionele straf. Hoewel dit op basis van drie landen bezwaarlijk als internationale standaard kan worden beschouwd, kan het de Nederlandse

280 Zie paragraaf 5.1.2.
281 Interview officier van justitie.

wetgever enig houvast geven bij de keuze van een strafbedreiging die zowel effectief als redelijk zou kunnen zijn.
De vraag naar de rechtmatigheid van de strafmaat is echter moeilijker te beantwoorden. Toepassing van de Franse en Britse wetgeving is nog niet getoetst door het Europees Hof. Mij komt het voor dat de mogelijkheid van twee tot vijf jaar gevangenisstraf toch wel een hoge mate van dwang oplevert om mee te werken. In de meeste gevallen waarin het Hof het aanvaardbaar heeft geacht om onder strafbedreiging medewerking af te dwingen, bestond de dwang uit (niet al te hoge) boetes (*O'Halloran and Francis*) of maximaal twee dagen gevangenisstraf (*Lückhof and Spanner*). De strafdreiging van zes maanden gevangenisstraf vormde in *Heaney and McGuiness* een '"degree of compulsion" [which] in effect destroyed the very essence of their privilege against self-incrimination and their right to remain silent' (§55). Ook het herhaaldelijk opleggen van boetes is vaak al een ontoelaatbare vorm of mate van dwang (*Funke, J.B.*)
Dit betekent dat een enigszins effectieve strafbedreiging van 2-3 jaar bij een ontsleutelplicht een ernstige vorm van dwang (in aard en mate) oplevert. Het Europees Hof zou een dergelijke dwang vermoedelijk alleen accepteren als de andere criteria deze hoge mate van dwang rechtvaardigen of compenseren. Dat wil ten eerste zeggen dat het publiek belang dat met de ontsleutelplicht gemoeid is, zwaarwegend moet zijn, wat betekent dat de ontsleutelplicht alleen ingevoerd zou moeten worden ten aanzien van delicten die in abstracto ernstig zijn (bijvoorbeeld waar een gevangenisstraf van minstens vier jaar op staat) en dat het bevel alleen toegepast zou moeten worden in gevallen die ook in concreto ernstig zijn, bijvoorbeeld een kinderpornozaak waarin er niet alleen aanwijzingen zijn van bezit maar ook van vervaardiging. Ook een subsidiariteitseis – bijvoorbeeld dat ontsleuteling "dringend noodzakelijk" is – zal helpen om het publiek belang gewicht mee te geven in de nemo-teneturbeoordeling door het Europees Hof.
Ten tweede zullen er aanzienlijke relevante waarborgen in de procedure moeten zijn opgenomen. In dit licht verdient de Franse wetgeving, die geen specifieke procedure lijkt te kennen, geen navolging. De Britse wetgeving lijkt wel een afgewogen geheel van waarborgen te hebben, niet alleen vanwege de nauwkeurige beschrijving van de gevallen waarin ontsleuteling kan worden bevolen en de redelijke bewijsvoeringslast als de verdachte betoogt dat hij niet kan ontsleutelen, maar ook vanwege waarborgen als de poortwachtersfunctie van een expertisecentrum, rechterlijke toestemming (hoewel die niet in alle gevallen wettelijk is vereist), de schriftelijke vorm van het bevel (waardoor er minder druk op de verdachte is om acuut te beslissen en hij kalm met zijn advocaat kan overleggen) en het onafhankelijke toezicht door de Chief Surveillance Commissioner. De jaarlijkse rapportage van deze Commissioner over de uitoefening van de bevoegdheid draagt ook bij aan de transparantie en daarmee controleerbaarheid van het ontsleutelbevel in de praktijk. Een dergelijk uitgebreid stelsel van procedurele waarborgen zou wellicht kunnen

helpen om een hogere mate van dwang bij de ontsleutelplicht te compenseren.

Ten derde is relevant op welke manier het ontsleutelbevel en het daaruit voortkomende bewijsmateriaal wordt gebruikt. Dit hangt af van de situatie.
(a) Als de verdachte weigert en veroordeeld wordt voor decryptieweigering, zal het Hof kijken of met het opleggen van de straf het recht op een eerlijk proces (in de hoofdzaak) is geschonden. Dat zal dan afhangen van de feitelijk opgelegde straf – het maakt nogal uit of de rechter een forse boete, twee weken of vijf jaar vrijheidsstraf oplegt – maar vooral ook van de omstandigheden waaronder decryptie is gevorderd. Gaat het om een ernstige zaak, is er een 'formidable case' tegen de verdachte die dringend vraagt om ontsleuteling en is er sterk bewijs dat de verdachte wel kan ontsleutelen (en dus opzettelijk weigert)? Naarmate de omstandigheden zwaarder zijn – bijvoorbeeld wanneer er ernstige bezwaren zijn tegen een verdachte van moord of ontvoering en er sterke aanwijzingen zijn dat in een bepaald versleuteld bestand de begraaf- of verblijfplaats van het slachtoffer te vinden is, terwijl de verdachte geen aannemelijke verklaring weet te geven waarom hij dat bestand niet wil of kan ontsleutelen – zal een zwaardere straf sneller aanvaardbaar zijn. Dat betreft wel tamelijk hypothetische gevallen; in de meeste situaties zullen dergelijke zware omstandigheden zich niet voordoen en zal een substantiële gevangenisstraf al snel disproportioneel zijn.
(b) Als de verdachte meewerkt en belastende bestanden worden blootgelegd, zal veel afhangen van de rol die deze bestanden (en de band met de bestanden die de verdachte door het meewerken impliciet heeft erkend) in het bewijs spelen. Bij het onder dwang afleggen van verklaringen legt het Hof grote nadruk op de mogelijkheid die de verdediging moet hebben om het bewijs ter discussie te stellen – de afgedwongen medewerking mag de procesautonomie van de verdachte niet onherstelbaar aantasten. Kan de verdachte nog redelijkerwijs betogen dat bijvoorbeeld de kinderpornobestanden op de harde schijf niet door hem zijn geplaatst (maar door zijn puberzoon) of dat hij deze niet opzettelijk in bezit heeft gehad (omdat ze in bulk van een pornopagina zijn binnengehaald)? Als het wachtwoord dat verdachte gegeven heeft alleen toegang gaf tot de computer als geheel, zijn dergelijke verweren misschien nog mogelijk, maar als het gaat om wachtwoorden tot specifieke bestanden, mappen of containers met belastend materiaal, zal de verdachte de band tussen hem en het belastend materiaal nauwelijks meer kunnen ontkennen, wat zijn procespositie substantieel beïnvloedt. Daarnaast zal het afhangen van het gewicht van het ontsleutelde materiaal in de bewijsconstructie: gaat het om steunbewijs in een overigens toch al sterke zaak, of gaat het om bewijs dat onmisbaar is voor een veroordeling? Ook zal meespelen of justitie de band tussen verdachte en belastend materiaal kan bewijzen via andere middelen dan het feit dat de verdachte zijn wachtwoord heeft gegeven – als het bestaan van en verdachtes beschikkingsmacht over de bestan-

den een 'uitgemaakte zaak' zijn, heeft het afgeven van het wachtwoord immers minder verklarende waarde en is de zelfbelasting navenant minder (vergelijk daarover de Amerikaanse rechtspraak). Wanneer de rechter ter zitting aandacht besteedt aan al deze elementen en motiveert hoe en waarom hij het afgedwongen bewijs al dan niet laat meewegen, zal de onder hoge strafdreiging afgedwongen medewerking eerder aanvaardbaar zijn voor het Europees Hof.

Al met al betekent dit dat een substantiële strafdreiging die enigermate effectief zou kunnen zijn om verdachten tot medewerking te prikkelen (waarbij gedacht kan worden aan 2-3 jaar gevangenisstraf als maximum) alleen verenigbaar is met het nemo-teneturbeginsel als de hoge mate van dwang in sterke mate wordt gecompenseerd door andere waarborgen. De wettelijke regeling en de toepassing daarvan zullen zich moeten beperken tot ernstige gevallen (in abstracto en in concreto), er zal een afgewogen stelsel van procedurele waarborgen moeten zijn, en de rechter zal terughoudend moeten zijn bij het daadwerkelijk opleggen van straf voor de weigering of het daadwerkelijk gebruiken van ontsleuteld materiaal als bewijs.

Dat is een zware opgave, maar het lijkt mij niet ondoenlijk. Juist omdat het Europees Hof geen wetgeving in het algemeen beoordeelt, maar alleen de toepassing daarvan in individuele gevallen, is er ruimte om een wettelijke bevoegdheid in te voeren die inbreuk maakt op nemo tenetur, waarbij de grenzen van de uitoefening van de bevoegdheid vervolgens casuïstisch kunnen worden bepaald. Een hoog strafmaximum voor decryptieweigering hoeft niet te betekenen dat verdachten die weigeren in de praktijk steeds twee jaar gevangenis opgelegd krijgen, en er zijn extreme gevallen denkbaar waarin een hoge straf op decryptieweigering toch aanvaardbaar zou kunnen zijn. Wel valt te verwachten dat verdachten die onder druk – als de politie hen fijntjes wijst op het hoge strafmaximum voor weigering – hun wachtwoord afgeven, in de rechtszaal gaan betogen dat het nemo-teneturbeginsel is geschonden, wat tot langere processen (tot aan Straatsburg) kan leiden. Maar dat zou dan tot welkome jurisprudentie kunnen leiden over de gevallen waarin afgedwongen ontsleuteld materiaal voor het bewijs kan worden gebruikt, en het is aan justitie om af te wegen of zij in voorkomende gevallen het risico van bewijsuitsluiting dan wel een tik op de vingers van het Europees Hof wil nemen.

Van belang is ook dat een strafbaarstelling van decryptieweigering in de Nederlandse wetgeving als een systeembreuk kan worden gezien. Het commune strafrecht kent immers geen gesanctioneerde plichten voor verdachten om actief mee te werken (met uitzondering van het uitleveringsbevel van art. 551 Sv, dat niet ziet op bewijsvergaring maar op onttrekking aan het verkeer). Deze optie zou daarom tot ophef en een dogmatische discussie kunnen leiden. Dat lijkt mij echter geen overtuigend argument om (op voorhand) af te zien van strafbaarstelling. In het bijzondere strafrecht bestaan bijvoorbeeld al de nodige meewerkplichten voor verdachten die strafrechtelijk zijn gesanc-

tioneerd. Bovendien is het 'systeem' van nemo tenetur in de Nederlandse wet eigenlijk minder systematisch dan in de dogmatiek wel wordt aangenomen. Stevens heeft laten zien dat het nemo-teneturbeginsel een containerbegrip of 'smurfbeginsel' met een 'weinig coherente inhoud' is, dat voor uiteenlopende situaties en waarden wordt gesmurft. Het is volgens haar theoretisch breed vertakt maar stelt in de praktijk niet altijd grenzen aan afgedwongen medewerking. Bovendien wordt nemo tenetur vaak gebruikt in discussies als retorisch middel ('rechtsbeschermingsretoriek') dat dient om een bepaald standpunt kracht bij te zetten, terwijl de precieze inhoud van het nemo-teneturargument daarbij minder van belang lijkt.[282] Kritiek op een mogelijke 'systeembreuk' zou de wetgever dus kunnen pareren door inhoudelijk te beargumenteren dat afgedwongen medewerking in dit geval wel valt binnen de grenzen van het nemo-teneturbeginsel.
Wat de effectiviteit betreft, impliceren de zware voorwaarden die het Europees Hof aan een ontsleutelplicht met een substantiële straf op weigering stelt, dat het aantal gevallen waarin een decryptiebevel feitelijk effect heeft, vermoedelijk beperkt is. Dat blijkt ook wel uit de ervaringen tot nu toe in het VK (zie paragraaf 6.3.2), waar het ontsleutelbevel in zo'n 10-20 gevallen per jaar wordt opgelegd, waarbij een minderheid van de verdachten meewerkt. Degenen die weigeren worden niet altijd vervolgd voor decryptieweigering, en ongeveer een kwart van hen wordt veroordeeld voor het niet meewerken. Daarmee is niet gezegd dat een decryptiebevel niet effectief is: ook als in een beperkt aantal zaken verdachten hierdoor meewerken en dit bewijs oplevert dat anders niet zou zijn gevonden, kan het een belangrijk hulpmiddel zijn in het opsporingsarsenaal. Maar wonderen moeten niet worden verwacht.
Verder moeten ook enkele beleidsmatige overwegingen onder ogen worden gezien. Als de inschatting van de praktijk klopt dat in Nederland veel verdachten niet zullen meewerken aan een ontsleutelbevel,[283] dan zou de meerwaarde van een decryptiebevel vooral zijn dat verdachten vervolgd kunnen worden voor decryptieweigering in plaats van het gronddelict. Nu is zo'n veroordeling voor een weigering om mee te werken niet alleen geen sinecure, zoals hierboven betoogd, maar in zekere zin ook oneigenlijk:

> 'Je lost het probleem niet op; je krijgt er immers geen bewijs mee. Ik geloof niet in een afschrikwekkende werking van een decryptieplicht. (…) Je moet vooral weten waarom iemand zwijgt of niet verklaart, je kunt niet zomaar consequenties verbinden aan het enkele feit dat iemand zwijgt of niet meewerkt.'[284]

> 'Bovendien wil ik mensen vervolgen omdat ik weet wat ze hebben gedaan, niet omdat ze niet meewerken aan een onderzoek.'[285]

282 Stevens 2008, aantt. 5.41-5.42. Zie ook Stevens 2005.
283 Zie de tekst bij noten 269-272.
284 Interview officier van justitie.
285 Interview officier van justitie.

Het strafbaar stellen van decryptieweigering is met andere woorden 'an uncomfortable attempt to punish by proxy where a more serious suspected offence could not be adequately proven'.[286] Nu is een dergelijke instrumentele vorm van strafbaarstelling niet uniek; veel meewerkplichten zijn strafrechtelijk gesanctioneerd, al moet daarbij wel worden aangetekend dat het meestal gaat om sociaal-economische wetgeving en niet om strafprocesrecht. Voorkomen moet echter worden dat een decryptiebevel met een hoge strafdreiging een stok wordt waarmee justitie elke verdachte die niet met een onderzoek wil meewerken, kan slaan. In de beleidsafweging moet dan ook worden meegenomen dat de medewerkers van politie en justitie die ik voor dit onderzoek heb gesproken, over het algemeen sceptisch staan tegenover een decryptiebevel met strafbaarstelling, omdat het grotendeels niet effectief zou zijn en verdachten om de verkeerde redenen zou straffen.[287] Vertegenwoordigers van justitie zelf geven de voorkeur aan een alternatieve opsporingsmethode – het plaatsen van Trojaanse paarden – waarmee zonder inbreuk op het nemo-teneturbeginsel (maar met inbreuk op de privacy) wachtwoorden kunnen worden onderschept zodat verdachten – als er belastend bewijs wordt gevonden – voor het gronddelict kunnen worden vervolgd.[288]

7.7.4 Optie C2: een decryptiebevel met belastende gevolgtrekkingen bij weigering

Een andere vorm van dwang die bij het decryptiebevel kan worden toegepast, is de dreiging dat het weigeren van de verdachte om te ontsleutelen als bewijs tegen hem zal worden gebruikt. Dat zal alleen relevant zijn in gevallen waarin versleutelde bestanden voorkomen die echt 'verdacht' zijn en om een verklaring van de verdachte vragen, maar voor dat type gevallen – waarin justitie het bewijs niet op een andere manier rond kan krijgen – lijkt een ontsleutelplicht juist ook bedoeld. Het gebruiken van belastende gevolgtrekkingen ('adverse inferences') is al mogelijk binnen de huidige wet en is ook al eens toegepast bij decryptieweigering (zie paragraaf 5.3). Deze mogelijkheid zal echter beter tot zijn recht komen wanneer een decryptiebevel wordt gereguleerd op de manier van het verhoor conform optie A hierboven; binnen die context is het verbinden van belastende gevolgtrekkingen aan het zwijgen van verdachten immers vooral relevant. Daarbij zou het model kunnen worden gehanteerd van de bewijsvoeringslast die is ontwikkeld bij witwassen (zie noot 107) en die ook wordt gehanteerd in de Britse decryptiewetgeving ten aanzien van de vraag of een verdachte in staat is om (vermoedelijk belas-

286 Chatterjee 2011, p. 269, met verwijzingen.
287 Interviews officieren van justitie, politie.
288 Interviews officieren van justitie. Zie nader paragraaf 7.3 over Trojaanse paarden. Zie echter ook Ungberg 2009, die betoogt dat alternatieve opsporingsbevoegdheden een veel zwaarder middel zullen zijn dan een decryptiebevel. Clemens 2004, p. 27, vindt daarentegen dat het Vijfde Amendement juist moet worden gerespecteerd en dat justitie beter informanten en infiltranten kan inzetten.

tende) gegevens te ontsleutelen (zie paragraaf 6.3.1). Dat wil zeggen dat als justitie het aannemelijk maakt dat de verdachte 'iets heeft uit te leggen' ('wat doet die versleutelde map getiteld "Natasja" hier?'), de verdachte vervolgens een uitleg zal moeten geven die enigszins aannemelijk is ('dat is plasseksporno die ik voor mijn vrouw verborgen wil houden; ik ben het wachtwoord van die map helaas vergeten omdat ik inmiddels een andere fetisj heb'), waarna de bewijsvoeringslast terugschuift naar justitie om aan te tonen dat de verklaring van verdachte niet aannemelijk is en hij wel degelijk bewijsmateriaal verbergt ('uit ons onderzoek blijkt dat u drie weken geleden gezocht heeft op "peuter Natasja naaktfoto's" en dat de map "Natasja" vorige week nog is gebruikt').

Deze optie maakt inbreuk op het nemo-teneturbeginsel (in combinatie met het zwijgrecht), aangezien de dreiging van belastende conclusies dwang uitoefent op de verdachte, zeker als de verdachte erop gewezen wordt dat hij het recht heeft zich te verschonen maar dat zijn weigering eventueel tegen hem kan worden gebruikt. Het gaat hier echter om een indirecte dwang, die als zodanig minder zwaar is dan de directe dwang van een straf op weigering (optie C1) (*Condron*, §59). De dwang zal ook kleiner zijn als de verdachte bij een ontsleutelbevel met zijn advocaat kan overleggen om weloverwogen zijn procespositie te kunnen bepalen ('the physical presence of a solicitor during police interview, must be considered a particularly important safeguard for dispelling any compulsion to speak which may be inherent in the terms of the caution', *Condron*, §60). Wat betreft de reikwijdte van de gevraagde medewerking zit een decryptiebevel ergens tussen een beperkte feitelijke vraag ('wie was de bestuurder?', *Weh*) en een brede, open vraag naar betrokkenheid bij het misdrijf (*Heaney and McGuinness*) in. Enerzijds lijkt het vragen om een wachtwoord meer op een beperkte, feitelijke vraag, maar anderzijds gaat het om het ontsluiten van een in potentie grote hoeveelheid informatie, namelijk de inhoud van een map, container of harde schijf. In gevallen waarin justitie niet precies weet hoeveel en wat voor typen bestanden en inhoud achter een beveiliging verborgen zitten – en dat zal vaak zo zijn, behoudens *Boucher*-achtige uitzonderingen – lijkt het vragen om ontsleuteling meer op de visexpedities die het Hof in *Funke* en *J.B.* te vaag en te ruim vond. Een ontsleutelbevel zal daarom vaker aan de *Heaney and McGuinness*-kant dan aan de *Weh*-kant van het spectrum zitten, wat een zware last legt op het trekken van belastende conclusies.

Of de inbreuk op het nemo-teneturbeginsel aanvaardbaar is, zal dan naast de eerdergenoemde toegang tot een advocaat vooral ook afhangen van de sterkte van de zaak (is er sprake van een 'prima facie case' tegen de verdachte?) en het gewicht dat bij de bewijsconstructie aan het niet-meewerken wordt toegekend. De Hoge Raad staat toe om de weigering van de verdachte te verklaren over een bepaalde belastende omstandigheid (zoals een onverklaarbaar grote hoeveelheid beveiligde schijfruimte) te gebruiken bij de

'afronding' van het bewijs, wat erop neerkomt dat het zwijgen enig – maar niet overwegend – gewicht krijgt in de bewijsconstructie.
Aangezien de eisen die het EHRM aan 'adverse inferences' stelt streng zijn (er moet een behoorlijk 'formidabele' zaak tegen verdachte zijn en de belastende omstandigheid moet echt vragen om een verklaring), zal deze optie evenmin als de vorige in veel gevallen kunnen worden toegepast. De effectiviteit zal ook problematisch zijn in gevallen waarin verdachten TrueCrypt-achtige systemen gebruiken, omdat justitie dan vaak niet voldoende hard zal kunnen maken dat er überhaupt versleutelde gegevens verborgen zijn op de harde schijf. Daarnaast moeten rechters ook rekening houden met de mogelijkheid dat verdachten goede redenen kunnen hebben om niet te ontsleutelen, ook als er geen direct belastend materiaal verborgen wordt.

> 'In kinderpornozaken houden daders regelmatig dagboeken bij over hun fantasieën of hebben ze al dan niet door anderen geschreven en gedownloade, sadistische fantasieën en verhalen in bezit. Als die naar boven komen, kan dat in combinatie met de andere dossiergegevens en persoonlijke omstandigheden mogelijk leiden tot zwaardere straffen, zoals een TBS. Dat is iets wat veel verdachten in het huidige klimaat willen voorkomen. En niet zelden staan er ook andere niet-strafbare gegevens op de computer van de verdachte die mogelijk negatieve consequenties hebben voor bijvoorbeeld zijn huwelijk, zijn werk of de omgang met zijn kinderen. Ik kan me dus ook voorstellen dat verdachten huiverig zijn een inkijkje te geven in hun denkbeelden door hun hele privéleven op de computer open te gooien.'[289]

De vraag is dan welke conclusie de rechter in zo'n geval – waarin de verdachte vaak wel bekent dat hij kinderporno verzamelt maar niet precies inzicht wil geven in de aard en achtergrond – mag verbinden aan een weigering te ontsleutelen.
Een voordeel van deze optie boven de vorige optie is wel dat hier de wet niet hoeft te worden aangepast (dan wel de minder ingrijpende wetswijziging van optie A nodig is) en dat er meer ruimte is om in de rechtspraak de grenzen af te tasten. Bij de strafbaarstelling uit de vorige optie zal de rechtspraak zich vooral toespitsen op zaken waarin iemand vervolgd wordt voor niet-meewerken; voor een veroordeling en het opleggen van een (substantiële) straf zal een rechter dan uitvoerig moeten motiveren waarom van de verdachte verwacht had kunnen worden dat hij zijn wachtwoord gaf, en dan zullen vaak *John Murray*-achtige situaties nodig zijn die dringend vragen om een verklaring. Bij optie C2 kan de rechtspraak zich uitstrekken over een breder scala aan bewijsbeoordelingen, waarbij een decryptieweigering niet per se het kernpunt in de bewijsconstructie hoeft te zijn maar ook gebruikt kan worden bij de verwerping van bepaalde verweren, zoals in de zaak-Flovin O. is

289 Interview officier van justitie.

gebeurd.[290] Naar mijn inschatting zal het verbinden van negatieve conclusies dan ook in meer zaken gebruikt kunnen worden (met een beperkt maar niet te verwaarlozen effect op de bewijsconstructie in de hoofdzaak) dan het bestraffen van decryptieweigering.

7.7.5 Optie C3: een decryptiebevel met strafverzwaring

Een derde vorm van dwang bij een ontsleutelplicht is de dreiging dat als de verdachte niet meewerkt, hij een zwaardere straf kan krijgen als hij wordt veroordeeld voor het gronddelict. Deze optie heb ik in 2000 grotendeels als niet-effectief buiten beschouwing gelaten, omdat het geen oplossing biedt voor het probleem als zodanig: het werkt immers alleen als er al voldoende bewijs is voor een veroordeling, terwijl de ontsleutelplicht juist bedoeld was voor gevallen waarin justitie door de versleuteling onvoldoende bewijsmateriaal kon verzamelen.
Inmiddels blijkt echter dat Frankrijk een expliciete bepaling in het materiële strafrecht heeft opgenomen dat de straf verhoogd kan worden als iemand weigert een decryptiesleutel af te geven (paragraaf 6.2.4), terwijl in Nederland een rechter een dergelijke weigering ook al heeft gebruikt in de strafmaat (paragraaf 5.4). Het is ook niet ongebruikelijk voor de Nederlandse rechter om de (mee- of tegenwerkende) proceshouding van de verdachte mee te laten wegen bij de strafoplegging. Dat betekent dat deze optie wel het overwegen waard lijkt.
Het maakt daarbij uit of een decryptieweigering expliciet als strafverhogende omstandigheid wordt geregeld, dat wil zeggen dat het wettelijk strafmaximum op het gronddelict met een bepaalde factor wordt verhoogd (zoals in Frankrijk), of dat de weigering wordt betrokken bij het bepalen van de straf binnen de bestaande bandbreedte van het gronddelict. In het Nederlandse recht is het ongebruikelijk om strafverhoging te gebruiken als reguleringsinstrument. Het Nederlandse strafrecht kent wel twee algemene strafverhogende factoren, namelijk recidive (art. 43a Sr) en ambtelijk misbruik (art. 44 Sr), en diverse specifieke omstandigheden zoals het maken van een gewoonte van het plegen van een bepaald feit (bijvoorbeeld bij racisme, art. 137c Sr), maar geen algemene strafverhoging die voortvloeit uit een bepaalde modus operandi of uit de proceshouding van de verdachte. Mij lijkt daarom dat een algemene strafverhogingsgrond van encryptiegebruik-met-niet-willen-ontsleutelen niet goed past in het systeem van de Nederlandse wet. Wel is denkbaar dat de wetgever bij *specifieke* delicten een strafverhoging invoert. Er zou bijvoorbeeld een gekwalificeerde vorm van het bezit van kinderpornografie kunnen worden ingevoerd, waarbij een hoger strafmaximum geldt wanneer bij het plegen van het delict gegevens zijn versleuteld (en die de verdachte niet desgevraagd ontsleutelt). Daarnaast kan de rechter ook nu al, binnen het

290 Zie noot 113.

bestaande recht, het al dan niet ontsleutelen door de verdachte meewegen bij de strafoplegging.
Voor de inbreuk op het nemo-teneturbeginsel hoeft het overigens niet veel uit te maken of er een wettelijke strafverzwaring is of een discretionaire bevoegdheid van de rechter om binnen de strafmaat rekening te houden met decryptieweigering. In beide gevallen gaat er een redelijke mate van (indirecte) dwang uit, die vergelijkbaar is met de dwang uit de vorige optie. Of deze aard en mate van dwang verenigbaar zijn met het nemo-teneturbeginsel, zal ook grotendeels afhangen van dezelfde factoren als bij de vorige optie: hoe en onder welke omstandigheden om ontsleuteling is gevraagd, of de verdachte met zijn advocaat heeft kunnen overleggen om zijn procespositie te bepalen, en hoe de decryptieweigering wordt gebruikt in het vonnis – waarbij de rechter zal moeten motiveren waarom hij oordeelt dat de versleutelde bestanden vermoedelijk relevant waren geweest voor de opsporing en dat de verdachte in staat was te ontsleutelen.
Wat de effectiviteit betreft is het moeilijk te voorspellen in welke mate de dreiging van een hogere straf verdachten zou aanzetten tot ontsleuteling. Vermoedelijk zal in algemene zin de mogelijkheid dat de rechter de proceshouding van de verdachte mee kan wegen in de strafbepaling, in de nodige gevallen leiden tot een meewerkende verdachte; als er veel bewijs is, zal de advocaat immers vaak adviseren om mee te werken in de hoop op een lagere straf. Het meewerken aan ontsleuteling verschilt in dat opzicht niet substantieel van het antwoorden tijdens een verhoor of het afleggen van een bekentenis. In dat opzicht heeft een expliciete strafverzwaring denk ik ook niet veel meerwaarde; het lijkt me onwaarschijnlijk dat verdachten plotseling wel zouden willen gaan meewerken als de maximumstraf op kinderpornobezit niet vier jaar maar zes jaar zou zijn. Daar komt bij dat de rechter een zwaardere motiveringsplicht krijgt als hij een decryptieweigeraar voor een gekwalificeerd delict (kinderpornobezit met versleuteling) zou veroordelen, omdat hij dan expliciet bewezen moet achten dat de versleutelde bestanden gebruikt zijn bij het plegen van het delict en dat de verdachte in staat is deze te ontsleutelen.
Al met al is het gebruiken van een decryptieweigering bij de strafoplegging een interessante mogelijkheid om enige druk uit te oefenen op verdachten om mee te werken. Dat is al mogelijk binnen de bestaande wettelijke kaders, mits de nodige zorgvuldigheid in acht wordt genomen om de inbreuk op het nemo-teneturbeginsel – er is immers sprake van dwang – te rechtvaardigen, vergelijkbaar met de eisen voor het trekken van negatieve conclusies uit de vorige optie. Daarnaast zou de wetgever kunnen overwegen om voor bepaalde delicten een strafverzwarende omstandigheid in te voeren, maar het is de vraag of dat veel meerwaarde heeft.

7.7.6 Variabele 1: een generieke ontsleutelplicht of alleen voor specifieke delicten?

Binnen de bovenstaande optie zijn er nog twee variabelen die een rol spelen. De eerste is of een ontsleutelplicht voor verdachten wordt ingevoerd in het algemeen of alleen voor specifiek aangewezen delicten. De concrete aanleiding voor dit onderzoek betreft kinderpornozaken,[291] maar de problematiek is breder. Weliswaar wordt sterke cryptografie momenteel vooral gebruikt binnen kinderpornonetwerken, maar het zou in de toekomst een breder probleem kunnen worden.[292] Bovendien gaat het niet alleen om versleuteling van gegevens, maar in beginsel ook om wachtwoordbeveiliging. Beveiligde computers – waaronder ook smartphones, tablet-pc's en andere mobiele computers vallen – kunnen in elk opsporingsonderzoek naar voren komen. Het ligt dan ook in beginsel meer voor de hand om een generieke in plaats van een specifieke ontsleutelplicht in te voeren.
Niettemin kan er een reden zijn voor differentiatie, afhankelijk van welke variant wordt gekozen. Voor de hierboven behandelde opties onder C, die een substantiële inbreuk op het nemo-teneturbeginsel maken, zou het kunnen uitmaken of een specifieke of een algemene ontsleutelplicht wordt ingevoerd. Dat heeft vooral te maken met de rol van het publiek belang, dat voor het Europees Hof een rol speelt in de beoordeling of een inbreuk op nemo tenetur gerechtvaardigd is. We zien dat vooral in de zaken waarbij kentekenhouders de naam van de bestuurder kenbaar moeten maken: het Hof legt in deze zaken een sterke nadruk op de specifieke problematiek van de verkeersveiligheid en de handhaafbaarheid van de wetgeving op dat terrein. Een onder dwang opgelegd decryptiebevel zal sneller aanvaardbaar zijn als het specifiek geënt is op een concreet maatschappelijk probleem in een bepaalde sector; de noodzaak van de bevoegdheid kan dan makkelijker worden aangetoond dan bij een generieke opsporingsbevoegdheid. Zo zou de problematiek van de bewijsbaarheid van kinderpornobezit – gezien het toenemend gebruik van sterke encryptie binnen kinderpornonetwerken – een sterk argument van publiek belang kunnen zijn om de inbreuk op het nemo-teneturbeginsel van optie C1 (strafbaarstelling van weigering) te rechtvaardigen. Mede gezien de grote mate van dwang die uitgaat van een substantiële straf op weigering en de hoge eisen die daarom aan de verdere waarborgen worden gesteld (zie paragraaf 7.7.3), zal optie C1 eerder door een artikel 6 EVRM-toets komen als deze beperkt is tot bepaalde delicten waarvoor encryptie in het bijzonder een probleem vormt. Als de wetgever optie C1 overweegt, zou hij daarom beter kunnen kiezen voor een ontsleutelplicht die beperkt is tot kinderpornozaken (en eventueel andere delicttypen waarbij encryptie een aantoonbaar probleem voor de opsporing en vervolging vormt), dan wel om een lage straf te verbinden aan decryptieweigering in het algemeen (de drie maanden van

291 *Kamerstukken II* 2010/11, 32 500 VI, nr. 106, p. 3-4.
292 Zie noot 18 en bijbehorende tekst.

art. 184 Sr) met een hogere straf (denk aan 2-3 jaar) voor kinderpornozaken (en eventueel andere delicten waar dat aantoonbaar nodig is). In verband met het systeem van de wet ligt het niet voor de hand een dergelijke regeling op te nemen in het Wetboek van Strafvordering, waarin delictspecifieke bepalingen weinig voorkomen. Een delictspecifieke regeling past echter wel in het Wetboek van Strafrecht, waar een strafbaarstelling van decryptieweigering voor een bepaalde catalogus van delicten kan worden ingevoerd en waar voor bepaalde delicten een strafverzwarende omstandigheid kan worden ingevoegd in de bestaande bepaling.
Voor de opties die minder inbreuk maken op het nemo-teneturbeginsel (opties A en B, en ook opties C2 en C3 waarbij de dwang minder groot of minder direct is) is er minder reden om te differentiëren naar delicttypen, in elk geval niet vanuit het perspectief van de verenigbaarheid met artikel 6 EVRM.

7.7.7 Variabele 2: de sleutel afgeven of zelf ontsleutelen?

De tweede variabele is of een ontsleutelplicht de vorm heeft van een bevel tot het afgeven van een sleutel of wachtwoord of van een bevel tot het zelf ontsleutelen of toegankelijk maken door de verdachte. Het huidige decryptiebevel (dat niet aan verdachten mag worden gegeven) omvat beide vormen. Op zich ligt het voor de hand om bij verdachten te kiezen voor het afgeven van de sleutel of het wachtwoord; dan is er immers geen risico op manipuleren van (mogelijk ook ander) materiaal op de computer. In het Verenigd Koninkrijk is dit ook de standaardvariant bij verdachten (terwijl bij niet-verdachten het laten ontsleutelen de voorkeur heeft in verband met proportionaliteit) (zie paragraaf 6.3.1). Aan de andere kant wordt in Amerikaanse zaken meestal gevorderd dat de verdachte zelf – in een zitting voor de *grand jury* (enigszins vergelijkbaar met een onderzoeksrechter in het voorstadium van vervolging, en niet te verwarren met de *petit jury* die oordeelt over een aangeklaagde) – ontsleutelt, omdat volgens de Amerikaanse dogmatiek het afgeven van een wachtwoord een verdergaande inbreuk op het nemo-teneturbeginsel maakt dan het zelf ontsluiten van de computer (iets wat overigens in het eerste Belgische wetsontwerp precies omgekeerd werd gezien). De Franse wetgeving maakt geen onderscheid tussen beide mogelijkheden.
Gezien de uiteenlopende modaliteiten die in de buitenlandse wetgeving worden gehanteerd, ligt het niet voor de hand om op voorhand een keuze te maken bij een ontsleutelplicht tussen het geven van een sleutel/wachtwoord en het zelf ontsleutelen. Net als bij het huidige Nederlandse decryptiebevel is het zinvoller om beide mogelijkheden open te laten en het aan de praktijk over te laten welke van de twee modaliteiten, gezien de omstandigheden, het beste kan worden gevorderd.

7.7.8 Variabele 3: alleen voor versleutelde bestanden of ook voor beveiligde computertoegang?

Zoals in paragraaf 1.3 is opgemerkt, behandelt dit onderzoek zowel het ontsleutelbevel als het bevel om toegang tot een beveiligde computer te verschaffen. In het licht van het nemo-teneturbeginsel maakt de aard van de problematiek geen verschil: in beide gevallen gaat het om de vraag of van een verdachte gevorderd kan worden dat hij beveiligde gegevens toegankelijk maakt door het afgeven, of zelf invoeren, van een wachtwoord. Het ligt dan ook voor de hand om een eventueel ontsleutelbevel voor verdachten voor beide vormen te laten gelden, dus het bevel zowel van lid 1 (toegangsverschaffing) als van lid 2 (decryptie) van artikel 125k Sv.
Niettemin zit er in de praktijk wel enig verschil tussen beide vormen. Toegangsbeveiliging op een computer beschermt de gehele inhoud van de computer; versleuteling beschermt alleen die bestanden die versleuteld zijn. Een bevel tot toegangsverschaffing tot een computer heeft dan ook in potentie een breder bereik dan een bevel tot decryptie. Ook zal een bevel tot toegangsverschaffing vaak in een wat eerder stadium van onderzoek nodig zijn; als bij een doorzoeking beveiligde computers worden aangetroffen, zal justitie geïnteresseerd zijn in de inhoud maar vaak nog niet precies weten wat ze kan verwachten op de computer aan te treffen. Het zal dan ook niet altijd even aannemelijk te maken zijn dat er mogelijk belastende bestanden op de computer staan (al hangt dat af van het delict: bij verdenking van kinderporno zal het aannemelijker zijn dan bij verdenking van drugshandel). Bij specifieke versleutelde bestanden daarentegen zal vaak uit de context sneller op te maken zijn of het gaat om potentieel belastende informatie die justitie nodig heeft. In die zin ligt het meer voor de hand om een gesanctioneerd bevel tot medewerking te geven bij versleutelde gegevens dan bij toegangsverschaffing tot een computer, zeker als het gaat om het trekken van negatieve conclusies (optie C2).
Ondanks de verschillen in reikwijdte en toepassing, denk ik dat het niet zinvol is om in de wetgeving op voorhand een onderscheid te maken tussen een ontsleutelbevel en een bevel tot toegangsverschaffing. Ten eerste hangt het sterk af van de situatie of beveiligde gegevens voldoende vragen oproepen om de verdachte te willen dwingen deze te ontsluiten. Regelmatig zullen versleutelde gegevens vragen oproepen, maar dat hoeft niet altijd zo te zijn (bijvoorbeeld bij een versleutelde diskette die in een la stof heeft liggen vergaren). Omgekeerd kan een beveiligde computer ook voldoende vragen oproepen, bijvoorbeeld vanuit informatie uit afgetapte communicatie over het handelen van de verdachte. Er is in dit opzicht dus geen intrinsiek verschil tussen versleutelde gegevens en beveiligde computertoegang. Ten tweede convergeren toegangsbeveiliging en encryptie in de praktijk; cryptoprogramma's versleutelen vaak de gehele harde schijf of een grote hoeveelheid bestanden tegelijk (zoals de containers in TrueCrypt). Een bevel tot toe-

gangsverschaffing en een bevel tot ontsleuteling komen dan op hetzelfde neer. Om deze redenen zou mijns inziens de beleidskeuze die de wetgever maakt ten aanzien van het bevel aan verdachten om versleutelde gegevens te ontsleutelen, ook moeten gelden voor het bevel tot toegangsverschaffing tot een beveiligde computer.

7.8 Conclusie

Sinds 2000 is er op twee punten het nodige veranderd. Ten eerste is dat het toenemende gebruik van encryptie door misdadigers, waardoor de opsporing vaker in aanraking komt met het probleem van versleutelde gegevens. In het verlengde hiervan ligt het vraagstuk van handhaafbaarheid enigszins anders dan in 2000. Er zijn meer mogelijkheden gekomen voor justitie om aannemelijk te maken dat een verdachte 'iets uit te leggen heeft' als er beveiligde gegevens worden aangetroffen; tegelijkertijd zijn echter ook cryptoprogramma's ontwikkeld die het juist moeilijker maken om aan te tonen dat er überhaupt versleutelde gegevens aanwezig zijn. Dat maakt de handhaafbaarheid meer een casuïstisch probleem (afhankelijk van de situatie) en minder een principieel argument tegen een ontsleutelplicht als zodanig.
Ten tweede is de situatie in het buitenland aanzienlijk veranderd. In het VK, Frankrijk, de VS en Australië bestaat inmiddels een strafrechtelijk gesanctioneerde ontsleutelplicht voor verdachten, met overigens wisselende voorwaarden. Hoewel enige discussie plaatsvindt over de verenigbaarheid hiervan met het nemo-teneturbeginsel, lijkt de wetgeving of rechtspraak in deze landen niet bijzonder omstreden.
Beide ontwikkelingen suggereren dat de vraag of een decryptiebevel aan verdachten verenigbaar is met het nemo-teneturbeginsel, niet ten principale negatief moet worden beantwoord. Het is een vraagstuk waarvan de grenzen in de rechtsontwikkeling – door een wettelijk kader en invulling door rechtspraak – kunnen worden bepaald. Het Europees Hof laat ruimte voor inbreuken op nemo tenetur, maar verbindt daar wel zware voorwaarden aan als het gaat om een vorm van medewerking die dicht tegen de verklaringsvrijheid aanligt, wat het geval is bij een ontsleutelbevel.
Er zijn diverse varianten denkbaar waarbij meer of minder dwang wordt uitgeoefend op de verdachte om mee te werken. De belangrijkste opties voor een ontsleutelplicht – met een regeling conform het verhoor, bewijsuitsluiting, strafbaarstelling van weigering of het betrekken van decryptieweigering bij het bewijs of de strafoplegging – zijn in dit hoofdstuk besproken aan de hand van de criteria die het Europees Hof gebruikt (de mate van dwang, het publiek belang, de procedurele waarborgen en de manier waarop het afgedwongen materiaal wordt gebruikt) en de te verwachten effectiviteit. Omdat de varianten elkaar niet per se uitsluiten en de bespreking geen evidente voorkeursoptie heeft opgeleverd, zal een afweging nodig zijn tussen verschil-

lende (combinaties van) opties. In het afsluitende hoofdstuk zet ik de factoren op een rij waar de wetgever bij die afweging rekening mee zou moeten houden.

8 Conclusies en aanbevelingen

8.1 Conclusies

In dit rapport is onderzocht in hoeverre een decryptiebevel – een bevel tot het verlenen van medewerking aan het toegankelijk maken van beveiligde gegevens – verenigbaar is met het nemo-teneturbeginsel. In een eerder onderzoek uit 2000 werd geconcludeerd dat een ontsleutelplicht voor verdachten een ingrijpende inbreuk maakte op het nemo-teneturbeginsel, die niet kon worden gerechtvaardigd door het opsporingsbelang. In het huidige onderzoek is geanalyseerd of er ontwikkelingen zijn sinds 2000 die nu tot een andere conclusie zouden kunnen leiden. De conclusies uit deze analyse worden in dit hoofdstuk gepresenteerd aan de hand van de in paragraaf 1.2 geformuleerde deelvragen van het onderzoek.

1 *Wat waren de factoren en argumenten die een rol speelden bij de conclusie in 2000 dat een decryptiebevel inbreuk maakt op het nemo-teneturbeginsel en dat deze inbreuk destijds niet te rechtvaardigen viel?*

De conclusie uit 2000 was gebaseerd op een analyse van zeven factoren: de mate waarin cryptografie een probleem voor de opsporing oplevert, de internationale context (buitenlandse wetgeving), de reikwijdte van de destijds bestaande bevoegdheden, de reikwijdte en achtergrond van het nemo-teneturbeginsel, het systeem van de Nederlandse wet, de handhavingsperikelen, en de verschillende vormen die een ontsleutelplicht zou kunnen aannemen. Alles bij elkaar genomen was het probleem destijds niet aantoonbaar groot genoeg om een verdergaande inbreuk op het nemo-teneturbeginsel (zoals strafbaarstelling van decryptieweigering) te rechtvaardigen, terwijl minder vergaande opties (zoals een ontsleutelplicht met bewijsuitsluiting) niet effectief zouden zijn. Het rapport bood echter wel een opening voor een andere conclusie in de toekomst. De vraag is daarom of nu een andere weging van de genoemde factoren gerechtvaardigd is.

2 *Wat is de reikwijdte en achtergrond van het nemo-teneturbeginsel?*

De reikwijdte van het nemo-teneturbeginsel, dat onderdeel vormt van het recht op een eerlijk proces (art. 6 EVRM) is in de rechtspraak van het Europees Hof (EHRM) sinds 2000 niet significant veranderd. De lijnen uit de eerdere standaardarresten *Funke* (uitlevering van documenten), *Saunders* (verklaringen in de voorfase) en *Salabiaku* en *John Murray* (trekken van negatieve conclusies) zijn voortgezet en verfijnd. De achtergrond van het nemo-teneturbeginsel is gelegen in een combinatie van drie ratio's, die afhankelijk van het geval een meer of minder belangrijke rol spelen. De *procesautonomie* van de verdachte blijkt uit de nadruk die het Europees Hof vaak legt op de mogelijkheid voor de verdachte om bewijsmateriaal ter terechtzitting aan te vechten, waarbij in een voorfase afgedwongen verklaringen zijn procespositie niet te veel mogen beperken. Het *pressieverbod* komt vooral naar voren in zaken waarin druk is uitgeoefend die in strijd komt met het fol-

terverbod, maar ook in zaken als waarin iemand in het beginstadium bij politieverhoor zonder rechtsbijstand onder druk wordt gezet. De *betrouwbaarheid van het bewijs* wordt vaak genoemd als overweging om onderscheid te maken tussen fysiek bewijs ('real evidence') en verklaringen; afgedwongen medewerking beïnvloedt de betrouwbaarheid van verklaringen meer dan die van fysiek bewijs.

De kern van het nemo-teneturbeginsel ligt nog altijd in de verklaringsvrijheid, waar het een zeer sterke werking heeft. In de vervolgingsfase mag soms enige druk worden uitgeoefend om verklaringen te verkrijgen, maar die druk mag niet groot zijn en moet omgeven zijn door procedurele waarborgen zoals de toegang tot een advocaat en het informeren van de verdachte over de gevolgen die zijn houding kan hebben op zijn procesgang. Buiten het afleggen van verklaringen geldt dat, naarmate de verdachte actiever moet meewerken en met name als hij daarbij een intellectuele inspanning moet verrichten, een dwang om mee te werken eerder in strijd komt met nemo tenetur. Dat werkt vooral door in gevallen waarin bijvoorbeeld onder dwang uitlevering van documenten wordt gevorderd terwijl de overheid niet voldoende kan aantonen dat zij weet om welke documenten het precies gaat, waardoor het uitleveren door de verdachte in de buurt komt van het afleggen van een verklaring. Een ontsleutelplicht ligt in dit opzicht dicht aan tegen het afleggen van een verklaring, omdat het wachtwoord in het hoofd van de verdachte zit en niet kan worden verkregen zonder diens (intellectuele) inspanning. Een decryptiebevel voor verdachten maakt daarom, net als in 2000, nog steeds inbreuk op het nemo-teneturbeginsel.

Deze inbreuk kan echter gerechtvaardigd zijn als wordt voldaan aan de eisen die het Europees Hof stelt. Het Hof kijkt naar vier factoren die in gezamenlijkheid bepalen of een afgedwongen medewerking een schending oplevert van het nemo-teneturbeginsel:

1 de aard en mate van dwang;
2 het gewicht van het publiek belang;
3 de aanwezigheid van relevante waarborgen in de procedure;
4 de manier waarop het afgedwongen materiaal wordt gebruikt.

Hierbij fungeren de factoren 1 en 4 enerzijds en de factoren 2 en 3 anderzijds als communicerende vaten. Naarmate de dwang om mee te werken groter is, en naarmate het afgedwongen materiaal een zwaardere rol heeft bij het bewijs, zal het publiek belang van afgedwongen medewerking des te groter moeten zijn en zullen er meer waarborgen moeten zijn voor rechtsbescherming. Bij een lagere mate van dwang of een ondergeschikte rol van afgedwongen bewijsmateriaal zal een ontsleutelplicht echter eerder de toets van artikel 6 EVRM kunnen doorstaan.

Ook in de Nederlandse rechtsontwikkeling is de rol van het nemo-teneturbeginsel grotendeels hetzelfde gebleven als in 2000. Een decryptiebevel voor verdachten zou nog steeds afwijken van het systeem van de Nederlandse wet, voor zover de weigering mee te werken strafbaar zou zijn. Wel blijkt uit de

rechtspraak dat er goede mogelijkheden zijn om verdachten vragen te ontsleutelen wanneer zij zich kunnen verschonen van medewerking (vergelijkbaar met de regeling van het verhoor waarbij de verdachte mag zwijgen). De verdachte neemt dan een zeker procesrisico om niet mee te werken, omdat onder bepaalde omstandigheden (in situaties waarin de aanwezigheid van beveiligde bestanden duidelijk vragen oproept) de rechter zijn decryptieweigering kan gebruiken bij het bewijs, de straftoemeting of andere beslissingen ten nadele van de verdachte.

3 Wat zijn ervaringen in andere landen met een decryptiebevel?

In 2000 waren er geen landen met een ontsleutelplicht voor verdachten en er waren ook geen directe aanwijzingen dat landen een dergelijke plicht zouden gaan invoeren. Inmiddels is de internationale context echter substantieel gewijzigd. Van de ons omringende landen heeft België een decryptiebevel ingevoerd dat niet aan verdachten mag worden gegeven. Frankrijk en het Verenigd Koninkrijk kennen inmiddels wel een ontsleutelplicht voor verdachten. Het VK heeft een uitgebreide wettelijke regeling getroffen voor de uitvoering en sanctionering van de ontsleutelplicht. In Frankrijk beperkt de wettelijke regeling zich tot de sanctionering van een weigering te ontsleutelen, met een zelfstandige strafbaarstelling en strafverhoging. Australië heeft een wettelijk decryptiebevel ingevoerd dat zich specifiek tot verdachten richt, terwijl in de VS zich een ontsleutelplicht voor verdachten uitkristalliseert in de rechtspraak, die onder bepaalde voorwaarden verenigbaar wordt geacht met het 'privilege against self-incrimination' (dat veel gelijkenissen heeft met het Europese nemo-teneturbeginsel).

Hieruit blijkt dat wetgevers en rechters in het VK, de VS, Australië en Frankrijk een strafrechtelijk gesanctioneerde ontsleutelplicht voor verdachten onder bepaalde voorwaarden aanvaardbaar achten. Uit de Britse en vooral Amerikaanse (lagere) rechtspraak komt naar voren dat de handeling van het afgeven van de sleutel of het zelf ontsleutelen een 'testimonial' karakter heeft, omdat het impliciet de band van verdachte met het versleutelde materiaal erkent, waardoor het decryptiebevel inbreuk maakt op nemo tenetur. Die inbreuk is volgens Amerikaanse rechtspraak gerechtvaardigd a) als het een uitgemaakte zaak is om wat voor bestanden het gaat en dat de verdachte de sleutel kent, of b) als er bewijsuitsluiting wordt beloofd voor het resulterende (belastende) materiaal. In de enige beschikbare uitspraak in het VK werd de inbreuk van het decryptiebevel op nemo tenetur aanvaardbaar geacht, mede vanwege de vele *checks and balances* die de Britse regeling kent en vanwege het feit dat de zittingsrechter altijd de mogelijkheid heeft om afgedwongen bewijs, als dat belastend blijkt, terzijde te leggen.

Hoewel de rechtspraak in de landen met een ontsleutelplicht voor verdachten nog in ontwikkeling is, kan in elk geval wel worden geconcludeerd dat de vraag naar verenigbaarheid met het nemo-teneturbeginsel in deze landen niet a priori negatief wordt beantwoord, maar in de rechtspraak casuïstisch

wordt beantwoord, waarbij het afdwingen van medewerking soms wel en soms niet aanvaardbaar wordt geacht.
Dit betekent voor Nederland dat, anders dan in 2000, de wetgever serieus de mogelijkheid kan overwegen om een ontsleutelplicht voor verdachten mogelijk te maken. Weliswaar wekken de buitenlandse ervaringen niet de verwachting dat een decryptiebevel in grote aantallen kan worden toegepast – daarvoor zijn de omstandigheden waarin het redelijk is een verdachte tot ontsleuteling te dwingen, te specifiek – maar het biedt een mogelijkheid die verschillende andere landen in elk geval in hun opsporingsarsenaal willen hebben.
Daarbij moet wel worden aangetekend dat in deze landen een hoge mate van dwang wordt ingezet (een hoge straf op decryptieweigering) die wordt gecompenseerd door vergaande waarborgen, waaronder de mogelijkheid van bewijsuitsluiting als de zittingsrechter de afgedwongen medewerking in strijd acht met het nemo-teneturbeginsel. De Britse regeling – die de meeste aanknopingspunten biedt voor de Nederlandse beleidsvorming – past enerzijds in de Britse tendens van een *surveillance*-maatschappij (die Nederland niet op alle onderdelen volgt) maar kent anderzijds ook waarborgen die Nederland niet kent, zoals een onafhankelijke toezichthouder. De wetgever zal dus goed moeten nadenken of en hoe het Britse voorbeeld in de Nederlandse context navolging kan verdienen, met inachtneming van alle *checks and balances* die in de Britse regeling zijn ingebouwd.

4 Wat valt er te zeggen over de verwachte effectiviteit en handhaafbaarheid van een decryptiebevel?

De studie van 2000 legde veel nadruk op handhaving en technische bezwaren. De inschatting was dat verdachten makkelijk zouden kunnen betogen dat zij graag zouden meewerken maar helaas de sleutel of het wachtwoord niet (meer) hadden. Een hoge sanctie op niet-medewerking zou dan alleen zin hebben als justitie onomstotelijk zou kunnen aantonen dat de verdachte toch in staat is te ontsleutelen, wat vermoedelijk zelden zou voorkomen. Daarom zou een ontsleutelplicht voor verdachten in de praktijk weinig effectief zijn.
Inmiddels heeft justitie echter ruimere mogelijkheden dan in 2000 het geval leek, om te betogen dat een verdachte mogelijk belastend materiaal (zoals binnengehaalde kinderporno) op zijn computer heeft staan en in staat is te ontsleutelen, bijvoorbeeld met aanwijzingen uit een tap of verkeersgegevens. Bovendien geeft de ontwikkeling van de rechtspraak over negatieve conclusies aan dat het niet nodig is dat justitie onomstotelijk aantoont dat de verdachte belastend materiaal heeft dat hij kan ontsleutelen, maar dat het voldoende is om dit aannemelijk te maken, waarna het aan de verdachte is om een enigszins plausibele verklaring te geven voor de versleutelde bestanden. Ook de Britse en Amerikaanse rechtspraak tonen aan dat er diverse gevallen

mogelijk zijn waarin de verdachte 'iets uit te leggen heeft' als hij niet wil ontsleutelen.
Daartegenover staat dat er 'antiforensische' programma's ontwikkeld zijn, dat wil zeggen cryptoprogramma's om niet alleen bestanden te versleutelen maar ook om het bestaan van de versleutelde bestanden 'aannemelijk ontkenbaar' te maken, waardoor het moeilijk wordt voor justitie om voldoende hard te maken dat de verdachte mogelijk bewijsmateriaal aan het verbergen is.
Deze twee tendensen heffen elkaar niet op, maar betekenen eerder dat het sterk van de omstandigheden zal afhangen of een decryptiebevel handhaafbaar is. Anders dan in 2000, vormt de handhaafbaarheid daarom een minder zwaarwegend argument voor een categorische afwijzing van een ontsleutelplicht voor verdachten. Vanuit beleidsoogpunt moet de wetgever zich echter wel realiseren dat de ontsleutelplicht vermoedelijk weinig effectief zal zijn bij zware en berekenende misdadigers en dat vooral de kleinere of minder slimme misdadigers zullen gaan meewerken (of bestraft kunnen worden voor decryptieweigering). Ook moet de wetgever meewegen dat het invoeren van een gesanctioneerde ontsleutelplicht zou kunnen leiden tot een toename in de ontwikkeling en het gebruik van 'antiforensische' programmatuur, wat een averechts effect zou hebben op de opsporing.

5 Gegeven de bevindingen uit de vorige deelvragen, in hoeverre is een decryptiebevel verenigbaar met het nemo-teneturbeginsel?

Uit bovenstaande bevindingen blijkt dat een decryptiebevel aan verdachten niet onverenigbaar is met het nemo-teneturbeginsel. Het hangt ervan af hoe het wettelijk wordt vormgegeven (bijvoorbeeld welke soort en mate van dwang kan worden gebruikt) en hoe het in een concreet geval wordt toegepast, of het recht op een eerlijk proces van de verdachte wordt geschonden. Die constatering wijkt als zodanig niet af van de studie uit 2000. Wel kan nu een andere conclusie worden verbonden aan deze constatering ten aanzien van de vervolgvraag of een ontsleutelplicht voor verdachten in Nederland zinvol en haalbaar zou zijn. De studie uit 2000 concludeerde dat Nederland geen ontsleutelplicht voor verdachten zou moeten invoeren, omdat die alleen effectief zou zijn bij een sterke mate van dwang maar daarmee een onaanvaardbare inbreuk op het nemo-teneturbeginsel zou opleveren. Inmiddels is de situatie bij twee factoren die aanzienlijk gewicht hadden in de afweging in 2000, substantieel veranderd. Ten eerste hebben sinds 2000 verschillende landen een ontsleutelplicht voor verdachten ingevoerd, waarbij op de weigering om mee te werken een substantiële straf staat. In de landen waar blijkens rechtspraak en rapportages de sanctionering daadwerkelijk wordt toegepast – het VK en de VS – wordt het ontsleutelbevel onder bepaalde voorwaarden als een aanvaardbare inbreuk op het nemo-teneturbeginsel gezien. Weliswaar heeft de hoogste rechter zich in deze landen nog niet over de verenigbaarheid met nemo tenetur uitgelaten, maar er zijn geen

aanwijzingen dat het decryptiebevel in deze landen als zeer problematisch wordt gezien. Het functioneert als een bevoegdheid die, in een beperkt aantal gevallen en met de nodige waarborgen omkleed, in de praktijk kan worden ingezet als justitie geen andere mogelijkheden heeft om versleuteld materiaal te ontsluiten. Ten tweede ligt ook het vraagstuk van de handhaafbaarheid anders, omdat het in voorkomende gevallen goed mogelijk is dat justitie voldoende aannemelijk kan maken dat de verdachte mogelijk belastend bewijsmateriaal aan het verbergen is. Een decryptiebevel hoeft dus niet bij voorbaat als niet effectief te worden afgewezen; eerder zou door de rechtspraak nader kunnen worden ingekleurd onder welke omstandigheden het redelijk is aan te nemen dat een verdachte wel of niet in staat is te ontsleutelen, zoals in de Verenigde Staten gebeurt. Beide factoren tezamen suggereren dat de inbreuk van een ontsleutelplicht voor verdachten op het nemo-teneturbeginsel aanvaardbaar zou kunnen zijn als de wettelijke regeling en uitvoering met voldoende waarborgen zijn omkleed.
Dat roept de vraag op welke modaliteit een ontsleutelplicht zou kunnen aannemen. In dit rapport zijn vijf opties geanalyseerd:
A: een decryptieregeling conform de regeling van het verhoor;
B: een decryptiebevel met bewijsuitsluiting;
C1: een decryptiebevel met strafbaarstelling van weigering;
C2: een decryptiebevel met belastende gevolgtrekkingen bij weigering;
C3: een decryptiebevel met strafverzwaring.
Opties A en B maken weinig inbreuk op nemo tenetur, omdat daar weinig dwang wordt uitgeoefend op verdachten om mogelijk zelfbelastend materiaal te ontsluiten. Optie A betekent dat de ontsleutelplicht aansluit op de regeling van het verhoor in plaats van (zoals in de huidige wetgeving) op de regeling van uitlevering van voorwerpen. Dit is een geschikte optie die verenigbaar is met het nemo-teneturbeginsel. Het is weliswaar niet per se effectiever dan de huidige situatie waarin al om vrijwillige medewerking kan worden gevraagd, maar het past beter binnen het systeem van de Nederlandse wet dan de huidige bepaling. Optie B kan interessant zijn in zaken waarin het versleuteld materiaal belangrijk zou kunnen zijn voor de vervolging van anderen dan de verdachte zelf of voor het vaststellen (of uitsluiten) van slachtoffers, wat in kinderpornozaken een belangrijk aspect kan zijn. Deze optie kan echter alleen ingezet worden in gevallen waarin het gezochte materiaal op geen enkele andere wijze kan worden achterhaald (dus als laatste redmiddel), of in gevallen waarin er al het nodige andere bewijsmateriaal voorhanden is voor een veroordeling met substantiële straf.
Bij de opties onder C is die dwang groter, met name bij optie C1 waarbij een directe dwang wordt uitgeoefend in de vorm van een straf op niet-meewerken. Als daarbij een strafmaximum van 2-3 jaar wordt gehanteerd, wat in de meeste landen het geval is, is dit een zware dwang die alleen aanvaardbaar is voor het Europees Hof als deze in sterke mate wordt gecompenseerd door andere waarborgen: aantoonbaar ernstige gevallen, een uitgebreid en afge-

wogen stelsel van procedurele waarborgen en terughoudendheid bij het daadwerkelijk opleggen van straf voor weigering of het daadwerkelijk gebruiken van ontsleuteld materiaal als bewijs. Dat zijn zware voorwaarden waardoor het aantal gevallen waarin een gesanctioneerd decryptiebevel feitelijk effect heeft, vermoedelijk beperkt is. Dat blijkt ook wel uit het VK, waar in vier jaar tijd 23 verdachten meewerkten aan een bevel en 35 verdachten weigerden; van de laatsten zijn zes veroordeeld voor decryptieweigering.
De opties C2 en C3 oefenen ook dwang uit op de verdachte om mee te werken, maar deze is indirect en minder groot dan bij strafbaarstelling van weigering. Niettemin verbindt het Europees Hof strenge eisen aan het trekken van negatieve conclusies (optie C2): er moet een behoorlijk 'formidabele' zaak tegen de verdachte zijn en de belastende omstandigheid moet echt vragen om een verklaring die van de verdachte kan worden verlangd. Deze optie zal daarom evenmin als de vorige in veel gevallen kunnen worden toegepast, maar heeft wel als voordeel dat de wet niet hoeft te worden aangepast en dat er meer ruimte is in de rechtspraak om de grenzen af te tasten. Het verbinden van negatieve conclusies zal daarom vermoedelijk in meer zaken gebruikt kunnen worden (met een beperkt maar niet te verwaarlozen effect op de bewijsconstructie in de hoofdzaak) dan het bestraffen van decryptieweigering. Voor optie C3 geldt een soortgelijke overweging: het gebruiken van een decryptieweigering bij de strafoplegging is een interessante mogelijkheid om enige druk uit te oefenen op verdachten om mee te werken, waarbij vergelijkbare eisen gelden als bij het trekken van negatieve conclusies voor het bewijs. Ook dit is mogelijk binnen de bestaande wettelijke kaders; daarnaast zou de wetgever kunnen overwegen om voor bepaalde delicten een strafverzwarende omstandigheid in te voeren (bijvoorbeeld bij kinderpornobezit als de verdachte weigert versleuteld materiaal te ontsluiten), maar het is de vraag of dat veel meerwaarde heeft.
Wanneer de opties in samenhang worden bekeken, kan worden geconcludeerd dat er grofweg drie mogelijkheden zijn voor de Nederlandse wetgever ten aanzien van de ontsleutelplicht voor verdachten.

1 *De huidige situatie handhaven.* Een ontsleutelbevel mag dan niet worden gegeven aan verdachten, maar politie en justitie kunnen verdachten wel verzoeken om vrijwillige medewerking. Afhankelijk van de omstandigheden kan de rechter binnen de bestaande wettelijke kaders tot op zekere hoogte al rekening houden met het feit dat een verdachte niet ontsleutelt, in de bewijsconstructie of bij de strafoplegging (opties C2, C3). In voorkomende gevallen kan justitie een verdachte ook bewijsuitsluiting beloven als het versleutelde materiaal noodzakelijk lijkt voor de vervolging van anderen of voor slachtofferhulp (optie B).
2 *Een decryptieregeling conform de regeling van het verhoor.* De praktijk van het vragen om ontsleuteling wordt geformaliseerd, in de wet of in lagere regelgeving, waarbij het verzoek wordt genormeerd op dezelfde wijze als het verhoor (art. 29 Sv). Dit zal voor de praktijk niet veel verschil maken

ten opzichte van de huidige wettelijke situatie; het past echter beter in het systeem van de wet omdat het meewerken aan ontsleuteling meer lijkt op het afleggen van een verklaring dan op het uitleveren van voorwerpen. Door het formaliseren van de mogelijkheid om een decryptieverzoek te doen en de normering conform de regulering van het verhoor, worden expliciet waarborgen van toepassing, waaronder de toegang tot een advocaat, die een belangrijke rol spelen in de EHRM-rechtspraak. Door de formalisering van deze waarborgen voor het vragen om medewerking kunnen ook de mogelijkheden worden versterkt om negatieve conclusies te trekken (optie C2) of om decryptieweigering te betrekken bij de strafoplegging (optie C3), omdat de inbreuk op het nemo-teneturbeginsel dan duidelijker wordt gecompenseerd door procedurele waarborgen.

3 *Een decryptiebevel aan verdachten met strafbaarstelling van weigering*. De wet wordt aangepast door het schrappen van de huidige bepaling dat het decryptiebevel niet aan verdachten wordt gegeven (optie C1). Niet-meewerken wordt dan strafbaar op basis van artikel 184 Sr (maximaal drie maanden gevangenisstraf). De wetgever kan ook overwegen, in navolging van andere landen die veelal een maximumstraf van 2-3 jaar hanteren, om een hogere straf op decryptieweigering te zetten; dat zou kunnen voor alle delicten, maar vanuit de EHRM-eisen zal een zwaardere straf eerder aanvaardbaar zijn als die zich beperkt tot specifieke delicttypen waarbij versleuteling aantoonbaar een groot maatschappelijk probleem veroorzaakt.

Een dergelijke wetswijziging maakt een grotere inbreuk op het nemo-teneturbeginsel dan de vorige mogelijkheid. Deze inbreuk zal alleen aanvaardbaar zijn in het licht van artikel 6 EVRM als de wettelijke regeling en uitvoering met voldoende waarborgen worden omkleed. Een zorgvuldige regeling met veel *checks and balances*, zoals in de Britse regeling, is dan vereist. De hoofdlijnen daarvan zouden in het Wetboek van Strafvordering moeten worden geregeld; de nadere uitwerking ervan zou bij AMvB, Aanwijzing of Richtlijn kunnen geschieden, zolang de waarborgen maar voldoende kenbaar en afdwingbaar zijn. De wetgever en rechter moeten zich hierbij voorts realiseren dat het Europees Hof ook kijkt naar de manier waarop afgedwongen materiaal wordt gebruikt; een discretionaire bevoegdheid van de rechter om belastend materiaal alsnog uit te sluiten van bewijs (en een zware motiveringsplicht wanneer belastend materiaal wél wordt gebruikt) speelt daarbij een belangrijke rol, zoals ook blijkt uit de Britse en Amerikaanse rechtspraak. Wanneer de wetgever een decryptiebevel onder strafdreiging zou invoeren zal artikel 359a Sv (bewijsuitsluiting bij vormverzuimen) dus de nodige aandacht moeten krijgen in de rechtsontwikkeling. De Memorie van Toelichting zou daarbij richting kunnen geven door nader in te gaan op de rol van bewijsuitsluiting in relatie tot de nemo-teneturjurisprudentie.

Op basis van de analyse van de EHRM-rechtspraak en het systeem van de Nederlandse wet, acht ik een decryptieregeling conform de regeling van het verhoor – net als in 2000 – te prefereren boven de huidige situatie. Anders dan in 2000 sta ik nu echter neutraler ten opzichte van de mogelijkheid van een decryptiebevel met strafbaarstelling. Ik denk dat er enige ruimte is binnen de grenzen van het nemo-teneturbeginsel om een onder strafdreiging afgedwongen ontsleutelplicht voor verdachten in te voeren. De regeling moet dan wel zeer zorgvuldig en afgewogen zijn en rekening houden met alle criteria die het Europees Hof aanlegt. De dwang die van een straf op weigering uitgaat mag niet te groot zijn, wat betekent dat alleen in uitzonderlijke gevallen *de facto* een substantiële straf op decryptieweigering zou kunnen worden opgelegd. De effectiviteit van een strafrechtelijk gesanctioneerd decryptiebevel dat binnen de nemo-teneturgrenzen blijft, zal gezien de zware eisen niet groot zijn maar zou in incidentele gevallen wel aanwezig kunnen zijn. Het is daarom vooral een beleidsafweging of een strafbaarstelling van decryptieweigering – die mogelijk is binnen de grenzen van het nemo-teneturbeginsel als er voldoende waarborgen zijn – te prefereren is boven een decryptieregeling conform de regeling van het verhoor.

8.2 Aanbevelingen

Deze studie heeft geleid tot de conclusie dat onder bepaalde – strenge – voorwaarden een ontsleutelplicht voor verdachten verenigbaar is met het nemo-teneturbeginsel. Aangezien de situatie sinds 2000 veranderd is, met name door ontwikkelingen in het buitenlandse recht en technische ontwikkelingen, verdient het aanbeveling dat de wetgever een hernieuwde afweging maakt of en onder welke omstandigheden een decryptiebevel aan verdachten zou kunnen worden gegeven. De wetgever kan daarbij kiezen tussen 1) het handhaven van de huidige situatie, 2) het formaliseren van de praktijk van het vragen aan verdachten om ontsleuteling, met een regeling conform de normering van het verhoor, en 3) het invoeren van een decryptiebevel aan verdachten met strafbaarstelling van weigering. Vanuit het oogpunt van het systeem van de wet zou de wetgever in elk geval serieus de tweede mogelijkheid moeten overwegen. De keuze tussen de tweede en derde mogelijkheid komt vooral neer op een beleidsafweging.
De belangrijkste vraag die de wetgever zich bij deze beleidsafweging moet stellen is of een lage mate van dwang (via een regeling conform die van het verhoor) of een hoge mate van dwang (via strafbaarstelling van decryptieweigering) de voorkeur verdient. Daarbij moeten enerzijds de eisen die het nemo-teneturbeginsel stelt aan afgedwongen medewerking (die wijzen in de richting van een lichte dwang) en anderzijds de effectiviteit (die wijst in de richting van meer dwang) tegen elkaar worden afgewogen. Het gaat echter niet om een zwart-wit-afweging tussen legitimiteit en effectiviteit; belangrijk

is vooral dat een zorgvuldige combinatie wordt gekozen van uit te oefenen dwang, de manier waarop afgedwongen materiaal wordt gebruikt en de procedurele waarborgen, en dat vanuit het publiek belang zorgvuldig wordt gemotiveerd waarom een gekozen regeling een aanvaardbare inbreuk op het nemo-teneturbeginsel oplevert. Een grotere mate van dwang kan aanvaardbaar zijn naarmate er meer waarborgen worden getroffen, zoals een schriftelijk bevel, toegang tot een advocaat, een cautie, een redelijke bewijsvoeringslast, een discretionaire bevoegdheid voor de rechter om zelfbelastend materiaal alsnog uit te sluiten van bewijs, en toezicht op de praktijk door een onafhankelijk toezichthouder.
Verder verdient het aanbeveling dat de wetgever bij de beleidsafweging ook de volgende overwegingen betrekt:

- binnen de *huidige wettelijke kaders* bestaan al mogelijkheden om enige druk uit te oefenen op verdachten om te ontsleutelen; onder omstandigheden kan een weigering om vrijwillig een wachtwoord af te geven worden gebruikt bij het bewijs of de strafoplegging;
- omdat de proceshouding van verdachten sowieso een rol speelt bij de opsporing en vervolging, hoeft een wettelijke regeling die een zekere mate van medewerking van verdachten eist, niet per se ten koste te gaan van hun rechtsbescherming; een *normering* van de voorwaarden waaronder ontsleuteling van verdachten kan worden geëist, biedt wellicht betere waarborgen voor het voorkómen van afgedwongen zelfbelasting dan een niet-genormeerde praktijk waarin verdachten om vrijwillige medewerking wordt gevraagd;
- een ontsleutelplicht voor verdachten is *geen wondermiddel*; het zal alleen effect sorteren in gevallen waarin een verdachte duidelijk 'iets uit te leggen heeft' en waarin er al het nodige bewijs tegen de verdachte bestaat;
- de *effectiviteit* van een ontsleutelplicht hangt samen met het *doel* dat ermee beoogd wordt;
  - als het doel is om zware (zeden)misdadigers aan te pakken, zal een decryptiebevel waarschijnlijk weinig effectief zijn; een ontsleutelplicht zou hooguit kunnen helpen om de groep verdachten die toch al meewerkt met justitie iets groter te maken; naar verwachting zal een ontsleutelplicht vooral de kleinere of minder slimme misdadigers treffen;
  - als het doel is om materiaal in handen te krijgen dat belangrijk is in het kader van slachtofferhulp (zoals het identificeren of uitsluiten van potentiële slachtoffers van seksueel misbruik), kan justitie overwegen – ook binnen de huidige wettelijke kaders – om de verdachte tot ontsleuteling aan te zetten door een toezegging van bewijsuitsluiting, wat vermoedelijk effectiever is dan een sanctiedreiging;
- een strafbaarstelling van decryptieweigering is een vorm van *instrumentele wetgeving*: de bedoeling van het strafprocesrecht is om misdadigers te straffen voor feiten die zij hebben begaan, niet om verdachten te straffen voor het niet meewerken aan bewijsgaring; de wetgever zou terughou-

dend moeten zijn met instrumentalisering van het strafrecht die leidt tot 'punishment by proxy';
- de invoering van een gesanctioneerde ontsleutelplicht zou een *potentieel averechts effect* kunnen hebben als het leidt tot een verdere ontwikkeling en breder gebruik van 'antiforensische' programmatuur; of zo'n effect zal optreden, is echter moeilijk te zeggen;
- de wenselijkheid van een ontsleutelplicht voor verdachten moet worden afgezet tegen *alternatieve mogelijkheden*, met name tegen de mogelijkheid om Trojaanse paarden in te zetten die wachtwoorden of sleutels heimelijk kunnen onderscheppen; mensen uit de politie- en justitiepraktijk geven de voorkeur aan deze laatste mogelijkheid omdat die effectiever zal zijn. De inzet van Trojaanse politiepaarden is echter een ingrijpende bevoegdheid die meer inbreuk maakt op de privacy van burgers dan een ontsleutelplicht voor verdachten, omdat meer wordt onderschept dan alleen wachtwoorden. De wetgever zou daarom een gemotiveerde belangenafweging moeten maken tussen de huidige situatie, een ontsleutelplicht voor verdachten en een bevoegdheid om Trojaanse politiepaarden te plaatsen;
- de wenselijkheid van een ontsleutelplicht voor verdachten zou ook in samenhang moeten worden bekeken met de *beleidsvorming rond andere technische ontwikkelingen*, zoals door buitenlandse aanbieders versleutelde internettelefonie, het bestaan van 'kogelvrije aanbieders' (die antiforensische ICT-diensten aanbieden) en *cloud computing* (waarbij je niet weet waar gegevens zijn opgeslagen). Enerzijds veroorzaken deze ontwikkelingen mogelijk grotere opsporingsproblemen dan encryptie door verdachten (zodat oplossingen voor andere problemen urgenter zijn), anderzijds kan een medewerkingsplicht voor verdachten ook bijdragen aan de oplossing van die problemen.[293] Daarom is een geïntegreerde beleidsvorming rond de verschillende computercriminaliteitdossiers wenselijk.

293 Zie hierover Koops et al. 2012, Colarusso 2011, Engel 2012.

Summary

The Decryption Order and the Privilege Against Self-Incrimination
Do developments since 2000 suggest a need to force suspects to decrypt?

Background and research question

When a criminal encrypts his computer data or communications, it is difficult for criminal investigators to collect this information through computer search and interception. One of the possible solutions to this problem is to force the persons in question to decrypt their data. The Netherlands introduced a decryption obligation in the Computer Crime Act (1993). However, at present, suspects cannot be ordered to decrypt their data. To date the Dutch legislator has proceeded on the assumption that compelled decryption violates the privilege against self-incrimination (known in Dutch as the principle of *nemo tenetur*). According to established case-law of the European Court of Human Rights (ECtHR), the privilege against self-incrimination lies at the heart of the right to a fair trial in article 6 of the European Convention of Human Rights and Fundamental Freedoms (ECHR). The precise scope of the privilege has not yet been properly thought-out and there is acceptance of the necessary exceptions to the privilege in legislation and case-law.
A study carried out in 2000[294] concluded that it is a major breach of the privilege to compel suspects to decrypt their data and that this could not be justified in the interest of criminal investigation. However, since 2000 there have been new developments in the field of technology and case-law on the privilege against self-incrimination. Following the Amsterdam child-abuse case involving Robert M., the Dutch Second Chamber also raised the question whether a decryption order should be newly introduced for suspects. Against this background and in view of developments since 2000, the main question investigated in this report is: to what degree can a decryption order (an order enforcing co-operation to access protected data) be considered compatible with the privilege against self-incrimination? Answers to this question are based on desk research, analysis of legal developments in other countries, and five semi-structured interviews with experts in investigative practice.

The privilege against self-incrimination

The scope of the privilege against self-incrimination has, in the European Court's case-law, not significantly changed since 2000. The essence of the privilege still lies in the freedom to make statements or to remain silent. Sometimes a suspect may be put under a certain amount of pressure to obtain statements, but that pressure should not be excessive and must be controlled by procedural safeguards, such as access to a lawyer and inform-

294 Koops 2000. For an English summary, see Koops, B.J. (2000), 'Commanding Decryption and the Privilege against Self-incrimination. The Dutch perspective', in: C.M. Breur, M.M. Kommer, J.F. Nijboer & J.M. Reijntjes (eds.), *New Trends in Criminal Investigation and Evidence – Volume II*, Antwerpen etc.: Intersentia 2000, p. 431-445.

ing the accused of the consequences his attitude could have on the course of the proceedings. In other forms of compelled co-operation than making statements, the privilege implies that the more the suspect has to actively participate in the investigation, especially if he has to make an intellectual effort, the more likely this obligation to collaborate will be in conflict with the privilege against self-incrimination. A decryption order comes very close to making a statement, because the password resides in the head of the accused and it cannot be obtained without his (intellectual) effort. This is why, just like the 2000 study concluded, a decryption order for suspects infringes the privilege against self-incrimination.
This infringement may, however, be justified, because there are possible exceptions to the privilege. The European Court considers four factors, which together determine whether or not compelled co-operation is acceptable in light of the privilege against self-incrimination:
1 the nature and extent of coercion;
2 the weight of the public interest;
3 the presence of relevant safeguards in the procedure;
4 the way in which the compelled material is used.
As the amount of pressure to co-operate increases and compelled material plays a greater role as evidence, the public interest of compelled co-operation will have to be higher and more safeguards for legal protection will have to be present. In case of a lower level of coercion or a subordinate role of the compelled material as evidence, a decryption order will sooner stand the test of article 6 ECHR.
In Dutch law, the role of the privilege against self-incrimination has largely remained the same since 2000. A decryption order for suspects would still not fit well in the system of Dutch criminal law to the extent that a refusal to co-operate would be punishable. Case-law does indicate that it is possible to request decryption from suspects if they can excuse themselves, comparable to an interrogation when an accused may claim the right to remain silent. In this case, the suspect takes a certain procedural risk if he does not co-operate, because under certain circumstances, if the presence of protected files clearly raises questions, the judge might use his refusal to decrypt in the construction of evidence, in sentencing, or in other decisions to the detriment of the accused.

Developments abroad

In 2000, no country had introduced a decryption order for suspects, but things have changed substantially since then. The decryption order introduced in Belgium may not be issued to suspects, but France and the United Kingdom have introduced a decryption duty for suspects. The UK has extensive legislation with various legal safeguards as to when and how a decryption order may be given. In France, legislation is limited to criminalising the

refusal to decrypt. In addition, Australia has introduced a statutory decryption order that specifically targets suspects, whereas in the United States, case-law is gradually shaping the conditions under which a decryption order for suspects is deemed consistent with the (American) privilege against self-incrimination (which has many similarities with the ECHR version of the privilege).
British and American case law suggest that co-operating with a decryption command is similar to making a statement, as it implicitly acknowledges the connection between the suspect and the encrypted material. This infringes the privilege against self-incrimination. However, according to US case-law, this can be justified either if the existence and location of the files and the suspect's ability to decrypt are a foregone conclusion, or if immunity is provided for the act of decryption and for the (incriminating) material that emerges after decryption. In the United Kingdom, the decryption order's infringement of the privilege against self-incrimination has been considered acceptable because of the many checks and balances in the British system and because of the court's discretionary power during trial to exclude compelled incriminating evidence. Although the case-law in these countries is still developing, it appears that a decryption order for suspects is considered acceptable under certain conditions, which can be shaped and further developed by the courts. British legislation thus provides points of reference for Dutch policy. The regulatory framework cannot be directly transferred, however; the United Kingdom has opted for a high degree of coercion (2 to 5 years' imprisonment for failure to co-operate), which can only be justified by extensive safeguards, including the possibility to exclude evidence, but also including some safeguards unknown to the Netherlands, such as an independent supervisory authority to oversee investigation powers.

Enforceability and developments in technology

The use of cryptography by suspects, particularly to encrypt stored data, has notably increased since 2000. For the time being, strong encryption seems to be used mainly in certain child pornography networks (which are often early adapters of advanced hiding technologies), but other groups of criminals could follow. An important development is the rise of 'anti-forensic' programs, i.e., crypto programs that do not only encrypt files but also make it possible to conceal the existence of encrypted files with 'plausible deniability'. These programs make it difficult for the judiciary to prove that there are any encrypted data on the hard disk.
On the other hand, the prosecution now appears to have greater opportunities than seemed the case in 2000 to argue that a suspect has possibly incriminating evidence (such as downloaded child pornography) on his computer and that he is able to decrypt, e.g., using indications from intercepted communications or traffic data. British and American case-law also show that

there are several possible cases in which the accused 'has something to explain' if he does not want to decrypt.
These two developments do not neutralise each other, but rather imply that much will depend on the circumstances whether a decryption order is enforceable. Therefore, unlike the 2000 study concluded, the difficulty of enforcement does not necessarily imply that a decryption order for suspects should be categorically rejected. Instead, it can be an option to have a statutory power that the judiciary may or may not apply depending on the circumstances. A decryption order will probably have little effect on serious and calculating criminals who do not co-operate with the police anyway, and is likely to affect rather the minor or less smart criminals. Experience in the United Kingdom indicates that a decryption order is imposed in only a limited number of cases, in which less than half of the addressees co-operate; in the past four years, only six refusers have been sentenced for not co-operating.

Conclusions and recommendations

The above findings show that a decryption order for suspects is not incompatible with the privilege against self-incrimination. It depends on how the law is structured (e.g. the type and degree of coercion used) and how it is applied in specific cases. Where the 2000 study concluded that the Netherlands should not adopt a decryption order for suspects because this would only be effective through a high level of coercion and this would yield an unacceptable infringement of the privilege against self-incrimination, the situation is somewhat different now. Developments abroad and in technology suggest that a decryption order for suspects could be compatible with the privilege against self-incrimination and – albeit in a limited number of cases – effective, provided the legislation and implementation are based on adequate safeguards.
Should the legislator, as in the UK, opt for a decryption order with a high level of coercion, then significant safeguards must be taken, such as a written order, access to a lawyer, a fair burden of proof, a discretionary power for the court to exclude self-incriminating evidence, and oversight of the practice by an independent supervising authority. It is also conceivable to choose less coercion, that is, not to criminalise the refusal to decrypt, but to allow the court to draw adverse inferences from a decryption refusal in constructing the evidence or in sentencing. Furthermore, the judiciary can, in some cases, also consider providing a suspect with immunity if he will decrypt. The decrypted material can then not be used against the suspect but it can be used against others or, for example, to identify (or exclude) victims, which in child pornography cases can be an important aspect.
Viewed together, there are three options for the Dutch legislator regarding the decryption order for suspects.

1 *Maintain the status quo.* An order to decrypt may not be issued to suspects, but the police and judiciary may request suspects to co-operate voluntarily. Under certain circumstances, current law allows the court to use the fact that a suspect has not decrypted in the construction of evidence or when sentencing.
2 *A decryption regulation in accordance with the regulation of interrogation.* Current practice to request decryption is formalised, in a statute or lower regulations, in order to regulate the decryption request in the same way as interrogation is regulated (art. 29 Dutch Code of Criminal Procedure). This will not make much difference in practice, but it fits better in the legal system because co-operating with decryption is more similar to making statements than to delivering physical evidence. Regulating decryption requests according to the rules for interrogation has the advantage that appropriate safeguards are present, such as access to a lawyer and informing the suspect beforehand of the right to remain silent. This could increase the possibilities of drawing adverse inferences from the suspect's decision not to co-operate.
3 *A decryption command to suspects with criminalization of non-co-operation.* Failure to co-operate with a decryption order is penalised under Article 184 of the Dutch Criminal Code (the general provision on not complying with a legal order, carrying up to three months' imprisonment) or under a separate provision that carries a higher maximum punishment. The ECHR requirements imply that a heavier penalty will be more acceptable if it is restricted to specific types of offences that demonstrably cause a major social problem. Criminalising the refusal to decrypt infringes the privilege against self-incrimination more seriously than the previous option; it must therefore have many safeguards and its need should be carefully substantiated. In order not to deprive the privilege against self-incrimination of its meaning, in any case, the court should always have the legal possibility to exclude compelled decrypted data from the evidence.

Analysis of the ECtHR case-law and the Dutch legal system shows that the second option is preferable to the first one. Unlike in 2000, the third option does not have to be rejected outrightly. There is some scope within the limits of the privilege against self-incrimination to issue, under threat of a criminal sanction, a decryption order to suspects. In view of the strong requirements, it will not be very effective in general, but it may be in specific cases. It is therefore ultimately a question of public policy whether penalising the refusal to decrypt – which can be done within the boundaries of the privilege against self-incrimination if sufficient safeguards apply – is preferable over regulating decryption requests in accordance with the regulation of interrogation.

In view of this conclusion, it is recommended that the legislator renews its consideration whether and under what conditions a decryption order could

be issued to suspects. The legislator should in any case seriously consider the second option. The choice between the second and third option (i.e., between little or much coercion) rather boils down to a decision of criminal policy. This does not imply a zero-sum trade-off between legitimacy and effectiveness. It is especially important for a decryption order for suspects, that a well-considered combination is chosen of the coercion to be applied, the way in which compelled material is used, and procedural safeguards, as well as that the legislator carefully motivates on the basis of public interest why the chosen regulatory framework yields an acceptable infringement of the privilege against self-incrimination.

It is important for policy-makers not to expect miracles from a decryption order. It will only be effective in a limited number of cases where a defendant clearly 'has something to explain' and where already much evidence is available against the suspect. Moreover, the legislator should show reserve in the instrumental use of criminal law: the objective is to punish criminals for offences they have committed, and not to punish defendants for failure to cooperate in gathering evidence. Furthermore, in respect of the policy concerning the decryption order, it is recommended to look at the broader perspective of problems encountered in digital investigation (e.g. cloud computing) and to consider alternative ways of addressing the problem of encryption, such as police Trojans that can secretly intercept passwords or keys.

Literatuur

Administrative Office of the United States Courts (2001)
Administrative Office of the United States Courts, *2000 Wiretap Report*, Washington, DC.: U.S. Courts, April 2001 (<www.uscourts.gov/uscourts/Statistics/WiretapReports/2000/2000wttxt.pdf>).

Akdeniz et al. (2001)
Y. Akdeniz, N. Taylor & C. Walker, 'BigBrother.gov.uk: State surveillance in the age of information and rights', *Criminal Law Review* 2001-februari, p. 73-90.

Behr (2008)
D.J. Behr, 'Anti-Forensics: What it is, what it does and why you need to know', *New Jersey Lawyer, the Magazine* (255) 2008, p. 9-13.

Brenner (2002)
S.W. Brenner, 'The privacy privilege. Law enforcement, technology, and the constitution', *Journal of Technology Law & Policy* (7) 2002, p. 123-194.

Brenner (2011)
S.W. Brenner, 'The Fifth Amendment, cell phones and search incident. A response to password protected?', *Iowa Law Review Bulletin* (96) 2011, p. 78-91.

Brunst & Sieber (2010)
P.W. Brunst & U. Sieber, *Cybercrime legislation in Germany / regulating internet crimes – Country report for Germany for the 18th International Congress of the International Academy of Comparative Law, Washington D.C. 2010,* Freiburg i.B.: Max Planck Institute for Foreign and International Criminal Law 2010.

Caprioli (2002)
E.A. Caprioli, 'Sécurité, cryptologie et libertés', *Le Bulletin du Barreau de Nice* 2002-september, p. 10-12.

Chatterjee (2011)
B.B. Chatterjee, 'New but not improved. A critical examination of revisions to the Regulation of Investigatory Powers Act 2000 encryption provisions', *International Journal of Law and Information Technology* (19) 2011, p. 264-284.

Chief Surveillance Commissioner (2009)
Chief Surveillance Commissioner, *Annual report of the Chief Surveillance Commissioner (…) for 2008-2009*, Londen: Office of Surveillance Commissioners 2009 (<http://surveillancecommissioners.independent.gov.uk/docs1/osc_annual_rpt_2008_09.pdf>).

Chief Surveillance Commissioner (2010)
Chief Surveillance Commissioner, *Annual report of the Chief Surveillance Commissioner (…) for 2009-2010*, Londen: Office of Surveillance Commissioners 2010 (<http://surveillancecommissioners.independent.gov.uk/docs1/annualreport20092010.pdf>).

Chief Surveillance Commissioner (2011)

Chief Surveillance Commissioner, *Annual report of the Chief Surveillance Commissioner (…) for 2010-2011*, Londen: Office of Surveillance Commissioners 2011 (<http://surveillancecommissioners.independent.gov.uk/docs1/OSC%20Annual%20Report%202010-11.pdf>).

Chief Surveillance Commissioner (2012)
Chief Surveillance Commissioner, *Annual report of the Chief Surveillance Commissioner (…) for 2011-2012*, Londen: Office of Surveillance Commissioners 2012 (<http://surveillancecommissioners.independent.gov.uk/docs1/OSC-annual-report-2011-12.pdf>).

Clemens (2004)
A.M. Clemens, 'No computer exception to the constitution. The Fifth Amendment protects against compelled production of an encrypted document or private key', *UCLA Journal of Law & Technology* 8(2) 2004, p. 1-27.

Colarusso (2011)
D. Colarusso, 'Heads in the cloud, a coming storm. The interplay of cloud computing, encryption, and the Fifth Amendment's protection against self-incrimination', *Boston University Journal of Science and Technology Law* (17) 2011, p. 69-100.

Corstens & Borgers (2011)
G. Corstens, bewerkt door M.J. Borgers, *Het Nederlands strafprocesrecht*, Deventer: Kluwer 2011.

Department of Trade and Industry (1999)
Department of Trade and Industry, *Building confidence in electronic commerce. A consultation document*, Londen, DTI 1999.

Diehl (2008)
M. Diehl, 'Kryptographiegesetzgebung im Wandel. Vom begrenzten Schlüssellängen zur Schlüsselherausgabe', *Datenschutz und Datensicherheit* 32(4) 2008, p. 243-247.

Engel (2012)
J.A. Engel, 'Rethinking the application of the Fifth Amendment to passwords and encryption in the age of cloud computing', *Whittier Law Review* 33(3) 2012, p. 101-127.

Gerhards (2010)
J. Gerhards, *(Grund-)Recht auf Verschlüsselung?*, Baden-Baden: Nomos Verlagsgesellschaft 2010.

Gershowitz (2011)
A.M. Gershowitz, 'Password protected? Can a password save your cell phone from a search incident to arrest?', *Iowa Law Review* (96) 2011, p. 1125-1175.

Gladman (2000)
B.R. Gladman, *The regulation of investigatory powers bill – The provisions for government access to keys*, Londen, FIPR 2000 (<www.fipr.org/rip/RIP-GAKBG.pdf>).

Home Office (2006)
Home Office, *Investigation of protected electronic information. A public consultation*, Londen: Home Office 2006.
Home Office (2007)
Home Office, *Investigation of protected electronic information. Code of practice pursuant to Section 71 of the Regulation of Investigatory Powers Act 2000*, Londen: TSO 2007.
House of Commons Home Affairs Committee (2008)
House of Commons Home Affairs Committee, *A surveillance society?*, Londen: House of Commons 20 mei 2008.
James (2004)
N.J. James, 'Handing over the keys. Contingency, power and resistance in the context of s 3LA of the Australian Crimes Act 1914', *University of Queensland Law Journal* 23(1) 2004, p. 7-21.
Kaspersen (1993)
H.W.K. Kaspersen, 'De Wet Computercriminaliteit is er, nu de boeven nog', *Computerrecht* 1993, p. 134-145.
Koops (1999)
B.J. Koops, *The crypto controversy. A key conflict in the information society*, Den Haag etc.: Kluwer Law International 1999.
Koops (2000)
B.J. Koops, *Verdachte en ontsleutelplicht. Hoe ver reikt nemo tenetur?*, Deventer: Kluwer 2000.
Koops & Stevens (2003)
B.J. Koops & L. Stevens, 'J.B. versus Saunders. De groeiende duisternis rond nemo tenetur', *Delikt & Delinkwent* 2003, p. 281-294.
Koops (2007)
B.J. Koops (red.), *Strafrecht en ICT*, Den Haag: Sdu 2007.
Koops et al. (2012)
B.J. Koops, R. Leenes, P. de Hert & S. Olislaegers, *Misdaad en opsporing in de wolken. Knelpunten en kansen van cloud computing voor de Nederlandse opsporing* Tilburg / Den Haag: TILT / WODC (te verschijnen).
Merckx (2001)
D. Merckx, *Cryptografie en wetshandhaving*, Antwerpen: Kluwer 2001.
Ministère de l'Économie des Finances et de l'Industrie (1999)
Ministère de l'Économie des Finances et de l'Industrie, *Policy paper on the adaptation of the legal framework to the information society*, oktober 1999 (<www.minefe.gouv.fr/fonds_documentaire/societe_information>).
Ministerie van Veiligheid en Justitie (2011)
Ministerie van Veiligheid en Justitie, *Verslag op hoofdpunten van de bijeenkomst van 24 augustus 2011 in Londen, over de ervaringen in het Verenigd Koninkrijk met de wetgeving over de verplichting tot het ontsleutelen van versleutelde informatie*, ongepubliceerd.
Murakami Wood (2006)

D. Murakami Wood (red.), *A report on the surveillance society. For the information commissioner by the surveillance studies network*, s.l. (<www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf>).

Myers Morrison (2012)
C. Myers Morrison, 'Passwords, profiles, and the privilege against self-incrimination. Facebook and the Fifth Amendment', *Arkansas Law Reviev* (65) 2012, p. 133-162.

Nationaal Rapporteur Mensenhandel (2011)
Nationaal Rapporteur Mensenhandel, *Kinderpornografie. Eerste rapportage van de Nationaal Rapporteur*, Den Haag: BNRM 2011.

Odinot et al. (2012)
G. Odinot, D. de Jong, J.B.J. van der Leij, et al., *Het gebruik van de telefoon- en internettap in de opsporing* (Onderzoek en beleid 304), Den Haag: Boom Lemma 2012.

Oerlemans (2011)
J.J. Oerlemans, 'Hacken als opsporingsbevoegdheid', *Delikt en Delinkwent* (8) 2011, p. 888-908.

Palfreyman (2009)
B.M. Palfreyman, 'Lessons from the British and American Approaches to Compelled Decryption', *Brooklyn Law Review* (75) 2009, p. 345ff.

Pardo (2008)
M.S. Pardo (2008), 'Self-Incrimination and the Epistemology of Testimony', *Cardozo Law Review* 30(3) 2008, p. 1023-1046.

Paredes (2009)
L.M. Paredes, 'The Travelers' Privacy Protection Act. Be reasonable with my private information and expensive equipment', *Criminal Law Bulletin* 45(1) 2009, Art. 1.

Quéméner & Charpenel (2010)
M. Quéméner & Y. Charpenel, *Cybercriminalité. Droit pénal appliqué*, Parijs: Economica 2010.

Roberts (2009)
A.J. Roberts, 'Case comment. Evidence: privilege against self-incrimination – key to encrypted material', *Criminal Law Review* (3) 2009, p. 191-193.

Stevens (2005)
L. Stevens , *Het nemo-teneturbeginsel in strafzaken. Van zwijgrecht naar containerbegrip* (diss. Tilburg), Nijmegen: Wolf Legal Publishers 2005.

Stevens (2007)
L. Stevens, 'De reikwijdte van het nemo-teneturbeginsel buiten de verklaringsvrijheid. Noot bij Hoge Raad 19-09-2006', *NJCM-bulletin* (5) 2007, p. 625-634.

Stevens (2008)

L. Stevens, 'Het nemo-teneturbeginsel en de onschuldpresumptie. Commentaar op artikel 271 Sv', in: A.L. Melai & M.S. Groenhuijsen (red.), *Wetboek van Strafvordering*. Deventer: Kluwer 2008, p. 271/1ff.

Van Toor (2011)

D. van Toor, 'Natuur in de mens; het "schuldige" geheugen', *Nederlands Juristenblad* 86(42) 2011, p. 2843-2849.

Ungberg (2009)

A.J. Ungberg, 'Protecting Privacy Through a Responsible Decryption Policy', *Harvard Journal of Law & Technology* (22) 2009, p. 537-558.

Verloop (2012)

P.C. Verloop, 'Jurisprudentiële ontwikkelingen ten aanzien van witwassen', in: C.A. Wielenga et al. (red.), *Jaarboek compliance 2012*, Nederlands Compliance Instituut 2012, p. 167-178.

Walsh (1996)

G. Walsh , *Review of Policy relating to Encryption Technologies*, Barton Act: Attorney-General's Department, 10 oktober 1996 (<www.efa.org.au/Issues/Crypto/Walsh/walsh.htm>).

Warusfel (2002)

B. Warusfel, 'Procédure pénale et technologie de l'information. De la Convention sur la Cybercriminalité à la Loi sur la sécurité quotidienne', *Droit & Défense* (1) 2002, p. 17-22.

Wiemans (2004)

F.P.E. Wiemans , *Onderzoek van gegevens in geautomatiseerde werken* (diss. Tilburg), Nijmegen: Wolf Legal Publishers 2004.

Bijlage 1 Samenstelling begeleidingscommissie

Prof.em. H.W.K. Kaspersen (voorzitter)	Vrije Universiteit
Mr. E.C. van Ginkel	Ministerie van Veiligheid en Justitie / WODC
Dhr. L.P. Mol Lous	Ministerie van Veiligheid en Justitie / DW
Mr. M. van der Staak	Radboud Universiteit Nijmegen

Bijlage 2 Britse wetgeving

[Oorspronkelijke versie (2000)]

Regulation of Investigatory Powers Act 2000

Part III
Investigation of electronic data protected by encryption etc.

Power to require disclosure
49.- [*Notices requiring disclosure*]
(1) This section applies where any protected information—
(a) has come into the possession of any person by means of the exercise of a statutory power to seize, detain, inspect, search or otherwise to interfere with documents or other property, or is likely to do so;
(b) has come into the possession of any person by means of the exercise of any statutory power to intercept communications, or is likely to do so;
(c) has come into the possession of any person by means of the exercise of any power conferred by an authorisation under section 22(3) or under Part II, or as a result of the giving of a notice under section 22(4) , or is likely to do so;
(d) has come into the possession of any person as a result of having been provided or disclosed in pursuance of any statutory duty (whether or not one arising as a result of a request for information) , or is likely to do so; or
(e) has, by any other lawful means not involving the exercise of statutory powers, come into the possession of any of the intelligence services, the police or the customs and excise, or is likely so to come into the possession of any of those services, the police or the customs and excise.
(2) If any person with the appropriate permission under Schedule 2 believes, on reasonable grounds—
(a) that a key to the protected information is in the possession of any person,
(b) that the imposition of a disclosure requirement in respect of the protected information is—
(i) necessary on grounds falling within subsection (3), or
(ii) necessary for the purpose of securing the effective exercise or proper performance by any public authority of any statutory power or statutory duty,
(c) that the imposition of such a requirement is proportionate to what is sought to be achieved by its imposition, and
(d) that it is not reasonably practicable for the person with the appropriate permission to obtain possession of the protected information in an intelligible form without the giving of a notice under this section,
the person with that permission may, by notice to the person whom he believes to have possession of the key, impose a disclosure requirement in respect of the protected information.
(3) A disclosure requirement in respect of any protected information is necessary on grounds falling within this subsection if it is necessary—

(a) in the interests of national security;
(b) for the purpose of preventing or detecting crime; or
(c) in the interests of the economic well-being of the United Kingdom.
(4) A notice under this section imposing a disclosure requirement in respect of any protected information—
(a) must be given in writing or (if not in writing) must be given in a manner that produces a record of its having been given;
(b) must describe the protected information to which the notice relates;
(c) must specify the matters falling within subsection (2) (b) (i) or (ii) by reference to which the notice is given;
(d) must specify the office, rank or position held by the person giving it;
(e) must specify the office, rank or position of the person who for the purposes of Schedule 2 granted permission for the giving of the notice or (if the person giving the notice was entitled to give it without another person's permission) must set out the circumstances in which that entitlement arose;
(f) must specify the time by which the notice is to be complied with; and
(g) must set out the disclosure that is required by the notice and the form and manner in which it is to be made;
and the time specified for the purposes of paragraph (f) must allow a period for compliance which is reasonable in all the circumstances.
(5) Where it appears to a person with the appropriate permission—
(a) that more than one person is in possession of the key to any protected information,
(b) that any of those persons is in possession of that key in his capacity as an officer or employee of any body corporate, and
(c) that another of those persons is the body corporate itself or another officer or employee of the body corporate,
a notice under this section shall not be given, by reference to his possession of the key, to any officer or employee of the body corporate unless he is a senior officer of the body corporate or it appears to the person giving the notice that there is no senior officer of the body corporate and (in the case of an employee) no more senior employee of the body corporate to whom it is reasonably practicable to give the notice.
(6) Where it appears to a person with the appropriate permission—
(a) that more than one person is in possession of the key to any protected information,
(b) that any of those persons is in possession of that key in his capacity as an employee of a firm, and
(c) that another of those persons is the firm itself or a partner of the firm,
a notice under this section shall not be given, by reference to his possession of the key, to any employee of the firm unless it appears to the person giving the notice that there is neither a partner of the firm nor a more senior employee of the firm to whom it is reasonably practicable to give the notice.

(7) Subsections (5) and (6) shall not apply to the extent that there are special circumstances of the case that mean that the purposes for which the notice is given would be defeated, in whole or in part, if the notice were given to the person to whom it would otherwise be required to be given by those subsections.
(8) A notice under this section shall not require the making of any disclosure to any person other than—
(a) the person giving the notice; or
(b) such other person as may be specified in or otherwise identified by, or in accordance with, the provisions of the notice.
(9) A notice under this section shall not require the disclosure of any key which—
(a) is intended to be used for the purpose only of generating electronic signatures; and
(b) has not in fact been used for any other purpose.
(10) In this section 'senior officer', in relation to a body corporate, means a director, manager, secretary or other similar officer of the body corporate; and for this purpose 'director', in relation to a body corporate whose affairs are managed by its members, means a member of the body corporate.
(11) Schedule 2 (definition of the appropriate permission) shall have effect.

50.- [*Effect of notice imposing disclosure requirement*]
(1) Subject to the following provisions of this section, the effect of a section 49 notice imposing a disclosure requirement in respect of any protected information on a person who is in possession at a relevant time of both the protected information and a means of obtaining access to the information and of disclosing it in an intelligible form is that he—
(a) shall be entitled to use any key in his possession to obtain access to the information or to put it into an intelligible form; and
(b) shall be required, in accordance with the notice imposing the requirement, to make a disclosure of the information in an intelligible form.
(2) A person subject to a requirement under subsection (1) (b) to make a disclosure of any information in an intelligible form shall be taken to have complied with that requirement if—
(a) he makes, instead, a disclosure of any key to the protected information that is in his possession; and
(b) that disclosure is made, in accordance with the notice imposing the requirement, to the person to whom, and by the time by which, he was required to provide the information in that form.
(3) Where, in a case in which a disclosure requirement in respect of any protected information is imposed on any person by a section 49 notice—
(a) that person is not in possession of the information,

(b) that person is incapable, without the use of a key that is not in his possession, of obtaining access to the information and of disclosing it in an intelligible form, or
(c) the notice states, in pursuance of a direction under section 51, that it can be complied with only by the disclosure of a key to the information,
the effect of imposing that disclosure requirement on that person is that he shall be required, in accordance with the notice imposing the requirement, to make a disclosure of any key to the protected information that is in his possession at a relevant time.
(4) Subsections (5) to (7) apply where a person ('the person given notice') —
(a) is entitled or obliged to disclose a key to protected information for the purpose of complying with any disclosure requirement imposed by a section 49 notice; and
(b) is in possession of more than one key to that information.
(5) It shall not be necessary, for the purpose of complying with the requirement, for the person given notice to make a disclosure of any keys in addition to those the disclosure of which is, alone, sufficient to enable the person to whom they are disclosed to obtain access to the information and to put it into an intelligible form.
(6) Where—
(a) subsection (5) allows the person given notice to comply with a requirement without disclosing all of the keys in his possession, and
(b) there are different keys, or combinations of keys, in the possession of that person the disclosure of which would, under that subsection, constitute compliance,
the person given notice may select which of the keys, or combination of keys, to disclose for the purpose of complying with that requirement in accordance with that subsection.
(7) Subject to subsections (5) and (6) , the person given notice shall not be taken to have complied with the disclosure requirement by the disclosure of a key unless he has disclosed every key to the protected information that is in his possession at a relevant time.
(8) Where, in a case in which a disclosure requirement in respect of any protected information is imposed on any person by a section 49 notice—
(a) that person has been in possession of the key to that information but is no longer in possession of it,
(b) if he had continued to have the key in his possession, he would have been required by virtue of the giving of the notice to disclose it, and
(c) he is in possession, at a relevant time, of information to which subsection (9) applies,
the effect of imposing that disclosure requirement on that person is that he shall be required, in accordance with the notice imposing the requirement, to disclose all such information to which subsection (9) applies as is in his pos-

session and as he may be required, in accordance with that notice, to disclose by the person to whom he would have been required to disclose the key.
(9) This subsection applies to any information that would facilitate the obtaining or discovery of the key or the putting of the protected information into an intelligible form.
(10) In this section 'relevant time', in relation to a disclosure requirement imposed by a section 49 notice, means the time of the giving of the notice or any subsequent time before the time by which the requirement falls to be complied with.

51.- [*Cases in which key required*]
(1) A section 49 notice imposing a disclosure requirement in respect of any protected information shall not contain a statement for the purposes of section 50(3) (c) unless—
(a) the person who for the purposes of Schedule 2 granted the permission for the giving of the notice in relation to that information, or
(b) any person whose permission for the giving of a such a notice in relation to that information would constitute the appropriate permission under that Schedule,
has given a direction that the requirement can be complied with only by the disclosure of the key itself.
(2) A direction for the purposes of subsection (1) by the police, the customs and excise or a member of Her Majesty's forces shall not be given—
(a) in the case of a direction by the police or by a member of Her Majesty's forces who is a member of a police force, except by or with the permission of a chief officer of police;
(b) in the case of a direction by the customs and excise, except by or with the permission of the Commissioners of Customs and Excise; or
(c) in the case of a direction by a member of Her Majesty's forces who is not a member of a police force, except by or with the permission of a person of or above the rank of brigadier or its equivalent.
(3) A permission given for the purposes of subsection (2) by a chief officer of police, the Commissioners of Customs and Excise or a person of or above any such rank as is mentioned in paragraph (c) of that subsection must be given expressly in relation to the direction in question.
(4) A person shall not give a direction for the purposes of subsection (1) unless he believes—
(a) that there are special circumstances of the case which mean that the purposes for which it was believed necessary to impose the requirement in question would be defeated, in whole or in part, if the direction were not given; and
(b) that the giving of the direction is proportionate to what is sought to be achieved by prohibiting any compliance with the requirement in question otherwise than by the disclosure of the key itself.

(5) The matters to be taken into account in considering whether the requirement of subsection (4) (b) is satisfied in the case of any direction shall include—
(a) the extent and nature of any protected information, in addition to the protected information in respect of which the disclosure requirement is imposed, to which the key is also a key; and
(b) any adverse effect that the giving of the direction might have on a business carried on by the person on whom the disclosure requirement is imposed.
(6) Where a direction for the purposes of subsection (1) is given by a chief officer of police, by the Commissioners of Customs and Excise or by a member of Her Majesty's forces, the person giving the direction shall give a notification that he has done so—
(a) in a case where the direction is given—
(i) by a member of Her Majesty's forces who is not a member of a police force, and
(ii) otherwise than in connection with activities of members of Her Majesty's forces in Northern Ireland,
to the Intelligences Services Commissioner; and
(b) in any other case, to the Chief Surveillance Commissioner.
(7) A notification under subsection (6) —
(a) must be given not more than seven days after the day of the giving of the direction to which it relates; and
(b) may be given either in writing or by being transmitted to the Commissioner in question by electronic means.

Contributions to costs
52.- [*Arrangements for payments for disclosure*]
(1) It shall be the duty of the Secretary of State to ensure that such arrangements are in force as he thinks appropriate for requiring or authorising, in such cases as he thinks fit, the making to persons to whom section 49 notices are given of appropriate contributions towards the costs incurred by them in complying with such notices.
(2) For the purpose of complying with his duty under this section, the Secretary of State may make arrangements for payments to be made out of money provided by Parliament.

Offences
53.- [*Failure to comply with a notice*]
(1) A person to whom a section 49 notice has been given is guilty of an offence if he knowingly fails, in accordance with the notice, to make the disclosure required by virtue of the giving of the notice.
(2) In proceedings against any person for an offence under this section, if it is shown that that person was in possession of a key to any protected informa-

tion at any time before the time of the giving of the section 49 notice, that person shall be taken for the purposes of those proceedings to have continued to be in possession of that key at all subsequent times, unless it is shown that the key was not in his possession after the giving of the notice and before the time by which he was required to disclose it.
(3) For the purposes of this section a person shall be taken to have shown that he was not in possession of a key to protected information at a particular time if—
(a) sufficient evidence of that fact is adduced to raise an issue with respect to it; and
(b) the contrary is not proved beyond a reasonable doubt.
(4) In proceedings against any person for an offence under this section it shall be a defence for that person to show—
(a) that it was not reasonably practicable for him to make the disclosure required by virtue of the giving of the section 49 notice before the time by which he was required, in accordance with that notice, to make it; but
(b) that he did make that disclosure as soon after that time as it was reasonably practicable for him to do so.
(5) A person guilty of an offence under this section shall be liable—
(a) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine, or to both;
(b) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum, or to both.

54.- [*Tipping-off*]
(1) This section applies where a section 49 notice contains a provision requiring—
(a) the person to whom the notice is given, and
(b) every other person who becomes aware of it or of its contents,
to keep secret the giving of the notice, its contents and the things done in pursuance of it.
(2) A requirement to keep anything secret shall not be included in a section 49 notice except where—
(a) it is included with the consent of the person who for the purposes of Schedule 2 granted the permission for the giving of the notice; or
(b) the person who gives the notice is himself a person whose permission for the giving of such a notice in relation to the information in question would have constituted appropriate permission under that Schedule.
(3) A section 49 notice shall not contain a requirement to keep anything secret except where the protected information to which it relates—
(a) has come into the possession of the police, the customs and excise or any of the intelligence services, or
(b) is likely to come into the possession of the police, the customs and excise or any of the intelligence services,

by means which it is reasonable, in order to maintain the effectiveness of any investigation or operation or of investigatory techniques generally, or in the interests of the safety or well-being of any person, to keep secret from a particular person.
(4) A person who makes a disclosure to any other person of anything that he is required by a section 49 notice to keep secret shall be guilty of an offence and liable—
(a) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine, or to both;
(b) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum, or to both.
(5) In proceedings against any person for an offence under this section in respect of any disclosure, it shall be a defence for that person to show that—
(a) the disclosure was effected entirely by the operation of software designed to indicate when a key to protected information has ceased to be secure; and
(b) that person could not reasonably have been expected to take steps, after being given the notice or (as the case may be) becoming aware of it or of its contents, to prevent the disclosure.
(6) In proceedings against any person for an offence under this section in respect of any disclosure, it shall be a defence for that person to show that—
(a) the disclosure was made by or to a professional legal adviser in connection with the giving, by the adviser to any client of his, of advice about the effect of provisions of this Part; and
(b) the person to whom or, as the case may be, by whom it was made was the client or a representative of the client.
(7) In proceedings against any person for an offence under this section in respect of any disclosure, it shall be a defence for that person to show that the disclosure was made by a legal adviser—
(a) in contemplation of, or in connection with, any legal proceedings; and
(b) for the purposes of those proceedings.
(8) Neither subsection (6) nor subsection (7) applies in the case of a disclosure made with a view to furthering any criminal purpose.
(9) In proceedings against any person for an offence under this section in respect of any disclosure, it shall be a defence for that person to show that the disclosure was confined to a disclosure made to a relevant Commissioner or authorised—
(a) by such a Commissioner;
(b) by the terms of the notice;
(c) by or on behalf of the person who gave the notice; or
(d) by or on behalf of a person who—
(i) is in lawful possession of the protected information to which the notice relates; and
(ii) came into possession of that information as mentioned in section 49(1).

(10) In proceedings for an offence under this section against a person other than the person to whom the notice was given, it shall be a defence for the person against whom the proceedings are brought to show that he neither knew nor had reasonable grounds for suspecting that the notice contained a requirement to keep secret what was disclosed.
(11) In this section 'relevant Commissioner' means the Interception of Communications Commissioner, the Intelligence Services Commissioner or any Surveillance Commissioner or Assistant Surveillance Commissioner.

Safeguards
55.- [*General duties of specified authorities*]
(1) This section applies to—
(a) the Secretary of State and every other Minister of the Crown in charge of a government department;
(b) every chief officer of police;
(c) the Commissioners of Customs and Excise; and
(d) every person whose officers or employees include persons with duties that involve the giving of section 49 notices.
(2) It shall be the duty of each of the persons to whom this section applies to ensure that such arrangements are in force, in relation to persons under his control who by virtue of this Part obtain possession of keys to protected information, as he considers necessary for securing—
(a) that a key disclosed in pursuance of a section 49 notice is used for obtaining access to, or putting into an intelligible form, only protected information in relation to which power to give such a notice was exercised or could have been exercised if the key had not already been disclosed;
(b) that the uses to which a key so disclosed is put are reasonable having regard both to the uses to which the person using the key is entitled to put any protected information to which it relates and to the other circumstances of the case;
(c) that, having regard to those matters, the use and any retention of the key are proportionate to what is sought to be achieved by its use or retention;
(d) that the requirements of subsection (3) are satisfied in relation to any key disclosed in pursuance of a section 49 notice;
(e) that, for the purpose of ensuring that those requirements are satisfied, any key so disclosed is stored, for so long as it is retained, in a secure manner;
(f) that all records of a key so disclosed (if not destroyed earlier) are destroyed as soon as the key is no longer needed for the purpose of enabling protected information to be put into an intelligible form.
(3) The requirements of this subsection are satisfied in relation to any key disclosed in pursuance of a section 49 notice if—
(a) the number of persons to whom the key is disclosed or otherwise made available, and
(b) the number of copies made of the key,

are each limited to the minimum that is necessary for the purpose of enabling protected information to be put into an intelligible form.
(4) Subject to subsection (5) , where any relevant person incurs any loss or damage in consequence of—
(a) any breach by a person to whom this section applies of the duty imposed on him by subsection (2) , or
(b) any contravention by any person whatever of arrangements made in pursuance of that subsection in relation to persons under the control of a person to whom this section applies,
the breach or contravention shall be actionable against the person to whom this section applies at the suit or instance of the relevant person.
(5) A person is a relevant person for the purposes of subsection (4) if he is—
(a) a person who has made a disclosure in pursuance of a section 49 notice; or
(b) a person whose protected information or key has been disclosed in pursuance of such a notice;
and loss or damage shall be taken into account for the purposes of that subsection to the extent only that it relates to the disclosure of particular protected information or a particular key which, in the case of a person falling with paragraph (b) , must be his information or key.
(6) For the purposes of subsection (5) —
(a) information belongs to a person if he has any right that would be infringed by an unauthorised disclosure of the information; and
(b) a key belongs to a person if it is a key to information that belongs to him or he has any right that would be infringed by an unauthorised disclosure of the key.
(7) In any proceedings brought by virtue of subsection (4) , it shall be the duty of the court to have regard to any opinion with respect to the matters to which the proceedings relate that is or has been given by a relevant Commissioner.
(8) In this section 'relevant Commissioner' means the Interception of Communications Commissioner, the Intelligence Services Commissioner, the Investigatory Powers Commissioner for Northern Ireland or any Surveillance Commissioner or Assistant Surveillance Commissioner.

Interpretation of Part III
56.- [*Interpretation of Part III*]
(1) In this Part—
'chief officer of police' means any of the following—
(a) the chief constable of a police force maintained under or by virtue of section 2 of the [1996 c. 16.] Police Act 1996 or section 1 of the [1967 c. 77.] Police (Scotland) Act 1967;
(b) the Commissioner of Police of the Metropolis;
(c) the Commissioner of Police for the City of London;

(d) the Chief Constable of the Royal Ulster Constabulary;
(e) the Chief Constable of the Ministry of Defence Police;
(f) the Provost Marshal of the Royal Navy Regulating Branch;
(g) the Provost Marshal of the Royal Military Police;
(h) the Provost Marshal of the Royal Air Force Police;
(i) the Chief Constable of the British Transport Police;
(j) the Director General of the National Criminal Intelligence Service;
(k) the Director General of the National Crime Squad;
'the customs and excise' means the Commissioners of Customs and Excise or any customs officer;
'electronic signature' means anything in electronic form which—
(a) is incorporated into, or otherwise logically associated with, any electronic communication or other electronic data;
(b) is generated by the signatory or other source of the communication or data; and
(c) is used for the purpose of facilitating, by means of a link between the signatory or other source and the communication or data, the establishment of the authenticity of the communication or data, the establishment of its integrity, or both;
'key', in relation to any electronic data, means any key, code, password, algorithm or other data the use of which (with or without other keys) —
(a) allows access to the electronic data, or
(b) facilitates the putting of the data into an intelligible form;
'the police' means—
(a) any constable;
(b) the Commissioner of Police of the Metropolis or any Assistant Commissioner of Police of the Metropolis; or
(c) the Commissioner of Police for the City of London;
'protected information' means any electronic data which, without the key to the data—
(a) cannot, or cannot readily, be accessed, or
(b) cannot, or cannot readily, be put into an intelligible form;
'section 49 notice' means a notice under section 49;
'warrant' includes any authorisation, notice or other instrument (however described) conferring a power of the same description as may, in other cases, be conferred by a warrant.
(2) References in this Part to a person's having information (including a key to protected information) in his possession include references—
(a) to its being in the possession of a person who is under his control so far as that information is concerned;
(b) to his having an immediate right of access to it, or an immediate right to have it transmitted or otherwise supplied to him; and

(c) to its being, or being contained in, anything which he or a person under his control is entitled, in exercise of any statutory power and without otherwise taking possession of it, to detain, inspect or search.
(3) References in this Part to something's being intelligible or being put into an intelligible form include references to its being in the condition in which it was before an encryption or similar process was applied to it or, as the case may be, to its being restored to that condition.
(4) In this section—
(a) references to the authenticity of any communication or data are references to any one or more of the following—
(i) whether the communication or data comes from a particular person or other source;
(ii) whether it is accurately timed and dated;
(iii) whether it is intended to have legal effect;
and
(b) references to the integrity of any communication or data are references to whether there has been any tampering with or other modification of the communication or data.

SCHEDULE 2

Persons having the appropriate permission
Requirement that appropriate permission is granted by a judge
1(1) Subject to the following provisions of this Schedule, a person has the appropriate permission in relation to any protected information if, and only if, written permission for the giving of section 49 notices in relation to that information has been granted—
(a) in England and Wales, by a Circuit judge;
(b) in Scotland, by a sheriff; or
(c) in Northern Ireland, by a county court judge.
(2) Nothing in paragraphs 2 to 5 of this Schedule providing for the manner in which a person may be granted the appropriate permission in relation to any protected information without a grant under this paragraph shall be construed as requiring any further permission to be obtained in a case in which permission has been granted under this paragraph.

Data obtained under warrant etc.
2(1) This paragraph applies in the case of protected information falling within section 49(1) (a) , (b) or (c) where the statutory power in question is one exercised, or to be exercised, in accordance with—
(a) a warrant issued by the Secretary of State or a person holding judicial office; or

(b) an authorisation under Part III of the [1997 c. 50.] Police Act 1997 (authorisation of otherwise unlawful action in respect of property).
(2) Subject to sub-paragraphs (3) to (5) and paragraph 6(1) , a person has the appropriate permission in relation to that protected information (without any grant of permission under paragraph 1) if—
(a) the warrant or, as the case may be, the authorisation contained the relevant authority's permission for the giving of section 49 notices in relation to protected information to be obtained under the warrant or authorisation; or
(b) since the issue of the warrant or authorisation, written permission has been granted by the relevant authority for the giving of such notices in relation to protected information obtained under the warrant or authorisation.
(3) Only persons holding office under the Crown, the police and customs and excise shall be capable of having the appropriate permission in relation to protected information obtained, or to be obtained, under a warrant issued by the Secretary of State.
(4) Only a person who—
(a) was entitled to exercise the power conferred by the warrant, or
(b) is of the description of persons on whom the power conferred by the warrant was, or could have been, conferred,
shall be capable of having the appropriate permission in relation to protected information obtained, or to be obtained, under a warrant issued by a person holding judicial office.
(5) Only the police and the customs and excise shall be capable of having the appropriate permission in relation to protected information obtained, or to be obtained, under an authorisation under Part III of the [1997 c. 50.] Police Act 1997.
(6) In this paragraph 'the relevant authority'—
(a) in relation to a warrant issued by the Secretary of State, means the Secretary of State;
(b) in relation to a warrant issued by a person holding judicial office, means any person holding any judicial office that would have entitled him to issue the warrant; and
(c) in relation to protected information obtained under an authorisation under Part III of the [1997 c. 50.] Police Act 1997, means (subject to sub-paragraph (7)) an authorising officer within the meaning of section 93 of that Act.
(7) Section 94 of the [1997 c. 50.] Police Act 1997 (power of other persons to grant authorisations in urgent cases) shall apply in relation to—
(a) an application for permission for the giving of section 49 notices in relation to protected information obtained, or to be obtained, under an authorisation under Part III of that Act, and
(b) the powers of any authorising officer (within the meaning of section 93 of that Act) to grant such a permission,
as it applies in relation to an application for an authorisation under section 93 of that Act and the powers of such an officer under that section.

(8) References in this paragraph to a person holding judicial office are references to—
(a) any judge of the Crown Court or of the High Court of Justiciary;
(b) any sheriff;
(c) any justice of the peace;
(d) any resident magistrate in Northern Ireland; or
(e) any person holding any such judicial office as entitles him to exercise the jurisdiction of a judge of the Crown Court or of a justice of the peace.
(9) Protected information that comes into a person's possession by means of the exercise of any statutory power which—
(a) is exercisable without a warrant, but
(b) is so exercisable in the course of, or in connection with, the exercise of another statutory power for which a warrant is required,
shall not be taken, by reason only of the warrant required for the exercise of the power mentioned in paragraph (b) , to be information in the case of which this paragraph applies.

Data obtained by the intelligence services under statute but without a warrant
(...)

Data obtained under statute by other persons but without a warrant
4(1) This paragraph applies—
(a) in the case of protected information falling within section 49(1) (a) , (b) or (c) which is not information in the case of which paragraph 2 or 3 applies; and
(b) in the case of protected information falling within section 49(1) (d) which is not information also falling within section 49(1) (a) , (b) or (c) in the case of which paragraph 3 applies.
(2) Subject to paragraph 6, where—
(a) the statutory power was exercised, or is likely to be exercised, by the police, the customs and excise or a member of Her Majesty's forces, or
(b) the information was provided or disclosed, or is likely to be provided or disclosed, to the police, the customs and excise or a member of Her Majesty's forces, or
(c) the information is in the possession of, or is likely to come into the possession of, the police, the customs and excise or a member of Her Majesty's forces,
the police, the customs and excise or, as the case may be, members of Her Majesty's forces have the appropriate permission in relation to the protected information, without any grant of permission under paragraph 1.
(3) In any other case a person shall not have the appropriate permission by virtue of a grant of permission under paragraph 1 unless he is a person falling within sub-paragraph (4) .
(4) A person falls within this sub-paragraph if, as the case may be—

(a) he is the person who exercised the statutory power or is of the description of persons who would have been entitled to exercise it;
(b) he is the person to whom the protected information was provided or disclosed, or is of a description of person the provision or disclosure of the information to whom would have discharged the statutory duty; or
(c) he is a person who is likely to be a person falling within paragraph (a) or (b) when the power is exercised or the protected information provided or disclosed.

Data obtained without the exercise of statutory powers
5(1) This paragraph applies in the case of protected information falling within section 49(1) (e).
(2) Subject to paragraph 6, a person has the appropriate permission in relation to that protected information (without any grant of permission under paragraph 1) if—
(a) the information is in the possession of any of the intelligence services, or is likely to come into the possession of any of those services; and
(b) written permission for the giving of section 49 notices in relation to that information has been granted by the Secretary of State.
(3) Sub-paragraph (2) applies where the protected information is in the possession, or (as the case may be) is likely to come into the possession, of both—
(a) one or more of the intelligence services, and
(b) the police or the customs and excise,
as if a grant of permission under paragraph 1 were unnecessary only where the application to the Secretary of State for permission under that sub-paragraph is made by or on behalf of a member of one of the intelligence services.

General requirements relating to the appropriate permission
6(1) A person does not have the appropriate permission in relation to any protected information unless he is either—
(a) a person who has the protected information in his possession or is likely to obtain possession of it; or
(b) a person who is authorised (apart from this Act) to act on behalf of such a person.
(2) Subject to sub-paragraph (3) , a constable does not by virtue of paragraph 1, 4 or 5 have the appropriate permission in relation to any protected information unless—
(a) he is of or above the rank of superintendent; or
(b) permission to give a section 49 notice in relation to that information has been granted by a person holding the rank of superintendent, or any higher rank.
(3) In the case of protected information that has come into the police's possession by means of the exercise of powers conferred by—

(a) section 44 of the [2000 c. 11.] Terrorism Act 2000 (power to stop and search) , or
(b) section 13A or 13B of the [1989 c. 4.] Prevention of Terrorism (Temporary Provisions) Act 1989 (which had effect for similar purposes before the coming into force of section 44 of the Terrorism Act 2000) ,
the permission required by sub-paragraph (2) shall not be granted by any person below the rank mentioned in section 44(4) of that Act of 2000 or, as the case may be, section 13A(1) of that Act of 1989.
(4) A person commissioned by the Commissioners of Customs and Excise does not by virtue of paragraph 1, 4 or 5 have the appropriate permission in relation to any protected information unless permission to give a section 49 notice in relation to that information has been granted—
(a) by those Commissioners themselves; or
(b) by an officer of their department of or above such level as they may designate for the purposes of this sub-paragraph.
(5) A member of Her Majesty's forces does not by virtue of paragraph 1, 4 or 5 have the appropriate permission in relation to any protected information unless—
(a) he is of or above the rank of lieutenant colonel or its equivalent; or
(b) permission to give a section 49 notice in relation to that information has been granted by a person holding the rank of lieutenant colonel or its equivalent, or by a person holding a rank higher than lieutenant colonel or its equivalent.

Duration of permission
7(1) A permission granted by any person under any provision of this Schedule shall not entitle any person to give a section 49 notice at any time after the permission has ceased to have effect.
(2) Such a permission, once granted, shall continue to have effect (notwithstanding the cancellation, expiry or other discharge of any warrant or authorisation in which it is contained or to which it relates) until such time (if any) as it—
(a) expires in accordance with any limitation on its duration that was contained in its terms; or
(b) is withdrawn by the person who granted it or by a person holding any office or other position that would have entitled him to grant it.

(...)

Bijlage 3 Franse wetgeving

[*zoals geldend per juli 2012*]

Code de procédure pénale
Partie législative
Livre Ier : De l'exercice de l'action publique et de l'instruction
Titre IV : Dispositions communes

Chapitre Ier : De la mise au clair des données chiffrées nécessaires à la manifestation de la vérité

Article 230-1
Sans préjudice des dispositions des articles 60, 77-1 et 156, lorsqu'il apparaît que des données saisies ou obtenues au cours de l'enquête ou de l'instruction ont fait l'objet d'opérations de transformation empêchant d'accéder aux informations en clair qu'elles contiennent ou de les comprendre, le procureur de la République, la juridiction d'instruction ou la juridiction de jugement saisie de l'affaire peut désigner toute personne physique ou morale qualifiée, en vue d'effectuer les opérations techniques permettant d'obtenir la version en clair de ces informations ainsi que, dans le cas où un moyen de cryptologie a été utilisé, la convention secrète de déchiffrement, si cela apparaît nécessaire.
Si la personne ainsi désignée est une personne morale, son représentant légal soumet à l'agrément du procureur de la République ou de la juridiction saisie de l'affaire le nom de la ou des personnes physiques qui, au sein de celle-ci et en son nom, effectueront les opérations techniques mentionnées au premier alinéa. Sauf si elles sont inscrites sur une liste prévue à l'article 157, les personnes ainsi désignées prêtent, par écrit, le serment prévu au premier alinéa de l'article 160.
Si la peine encourue est égale ou supérieure à deux ans d'emprisonnement et que les nécessités de l'enquête ou de l'instruction l'exigent, le procureur de la République, la juridiction d'instruction ou la juridiction de jugement saisie de l'affaire peut prescrire le recours aux moyens de l'Etat soumis au secret de la défense nationale selon les formes prévues au présent chapitre.

Article 230-2
Lorsque le procureur de la République, la juridiction d'instruction ou la juridiction de jugement saisie de l'affaire décident d'avoir recours, pour les opérations mentionnées à l'article 230-1, aux moyens de l'Etat couverts par le secret de la défense nationale, la réquisition écrite doit être adressée au service national de police judiciaire chargé de la lutte contre la criminalité liée aux technologies de l'information, avec le support physique contenant les données à mettre au clair ou une copie de celui-ci. Cette réquisition fixe le délai dans lequel les opérations de mise au clair doivent être réalisées. Le

délai peut être prorogé dans les mêmes conditions de forme. A tout moment, l'autorité judiciaire requérante peut ordonner l'interruption des opérations prescrites.
Le service de police judiciaire auquel la réquisition a été adressée transmet sans délai cette dernière ainsi que, le cas échéant, les ordres d'interruption, à un organisme technique soumis au secret de la défense nationale, et désigné par décret. Les données protégées au titre du secret de la défense nationale ne peuvent être communiquées que dans les conditions prévues par la loi n° 98-567 du 8 juillet 1998 instituant une Commission consultative du secret de la défense nationale.

Article 230-3
Dès l'achèvement des opérations ou dès qu'il apparaît que ces opérations sont techniquement impossibles ou à l'expiration du délai prescrit ou à la réception de l'ordre d'interruption émanant de l'autorité judiciaire, les résultats obtenus et les pièces reçues sont retournés par le responsable de l'organisme technique au service de police judiciaire qui lui a transmis la réquisition. Sous réserve des obligations découlant du secret de la défense nationale, les résultats sont accompagnés des indications techniques utiles à la compréhension et à leur exploitation ainsi que d'une attestation visée par le responsable de l'organisme technique certifiant la sincérité des résultats transmis.
Ces pièces sont immédiatement remises à l'autorité judiciaire par le service national de police judiciaire chargé de la lutte contre la criminalité liée aux technologies de l'information.
Les éléments ainsi obtenus font l'objet d'un procès-verbal de réception et sont versés au dossier de la procédure.

Article 230-4
Les décisions judiciaires prises en application du présent chapitre n'ont pas de caractère juridictionnel et ne sont susceptibles d'aucun recours.

Article 230-5
Sans préjudice des obligations découlant du secret de la défense nationale, les agents requis en application des dispositions du présent chapitre sont tenus d'apporter leur concours à la justice.

Code pénal
Partie législative
LIVRE Ier : Dispositions générales
TITRE III : Des peines

CHAPITRE II : Du régime des peines

Section 3 : De la définition de certaines circonstances entraînant l'aggravation, la diminution ou l'exemption des peines

Article 132-79
Lorsqu'un moyen de cryptologie au sens de l'article 29 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique a été utilisé pour préparer ou commettre un crime ou un délit, ou pour en faciliter la préparation ou la commission, le maximum de la peine privative de liberté encourue est relevé ainsi qu'il suit :
1° Il est porté à la réclusion criminelle à perpétuité lorsque l'infraction est punie de trente ans de réclusion criminelle ;
2° Il est porté à trente ans de réclusion criminelle lorsque l'infraction est punie de vingt ans de réclusion criminelle ;
3° Il est porté à vingt ans de réclusion criminelle lorsque l'infraction est punie de quinze ans de réclusion criminelle ;
4° Il est porté à quinze ans de réclusion criminelle lorsque l'infraction est punie de dix ans d'emprisonnement ;
5° Il est porté à dix ans d'emprisonnement lorsque l'infraction est punie de sept ans d'emprisonnement ;
6° Il est porté à sept ans d'emprisonnement lorsque l'infraction est punie de cinq ans d'emprisonnement ;
7° Il est porté au double lorsque l'infraction est punie de trois ans d'emprisonnement au plus.
Les dispositions du présent article ne sont toutefois pas applicables à l'auteur ou au complice de l'infraction qui, à la demande des autorités judiciaires ou administratives, leur a remis la version en clair des messages chiffrés ainsi que les conventions secrètes nécessaires au déchiffrement.

LIVRE IV : Des crimes et délits contre la nation, l'Etat et la paix publique
TITRE III : Des atteintes à l'autorité de l'Etat
CHAPITRE IV : Des atteintes à l'action de justice

Section 2 : Des entraves à l'exercice de la justice

Article 434-15-2
Est puni de trois ans d'emprisonnement et de 45 000 euros d'amende le fait, pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en oeuvre, sur les réqui-

sitions de ces autorités délivrées en application des titres II et III du livre Ier du code de procédure pénale.
Si le refus est opposé alors que la remise ou la mise en oeuvre de la convention aurait permis d'éviter la commission d'un crime ou d'un délit ou d'en limiter les effets, la peine est portée à cinq ans d'emprisonnement et à 75 000 euros d'amende.

Bijlage 4 Lijst geïnterviewde personen

Dhr. F. Bernaards	KLPD, beleidsmedewerker Team High Tech Crime
Dhr. B. Frans	politie Amsterdam-Amstelland, Team Digitale Expertise
Dhr. F. Kolkman	politie Oost-Nederland, hoofd van de High Tech Crime Unit
Dhr. Ph. Van Linthout	onderzoeksrechter bij de Rechtbank van Eerste Aanleg te Mechelen
Mw. M. Spoormaker	Openbaar Ministerie, landelijk officier kinderporno
Dhr. P. Zinn	KLPD, adviseur Team High Tech Crime
Dhr. L. van Zwieten	Openbaar Ministerie, landelijk officier van justitie cybercrime

Bijlage 5 Jurisprudentie Europees Hof voor de Rechten van de Mens

Alle uitspraken van het EHRM zijn beschikbaar op http://hudoc.echr.coe.int.

Allan v. The United Kingdom (Application no. 48539/99) 5 November 2002
Averill v. The United Kingdom (Application no. 36408/97) 6 June 2000
Balitskiy v. Ukraine (Application no. 12793/03) 3 November 2011
Beckles v. The United Kingdom (Application no. 44652/98) 8 October 2002
Brusco c. France (Requête nº 1466/07) 14 octobre 2010
Bykov v. Russia (Application no. 4378/02) 10 March 2009
Condron v. The United Kingdom (Application no. 35718/97) 2 May 2000
Falk v. The Netherlands (Application no. 66273/01) 19 October 2004
Gäfgen v. Germany (Application no. 22978/05), 1 June 2010 (rectified 3 June 2010)
Getiren v. Turkey (Application no. 10301/03) 22 July 2008
Heaney and McGuinness v. Ireland (Application no. 34720/97) 21 December 2000
Jalloh v. Germany (Application no. 54810/00) 11 July 2006
J.B. v. Switzerland (Application no. 31827/96) 3 May 2001
Kansal v. The United Kingdom (Application no. 21413/02) 27 April 2004
Krumpholz v. Austria (Application no. 13201/05) 18 March 2010
Lückhof and Spanner v. Austria (Applications nos. 58452/00 and 61920/00) 10 January 2008
Lutsenko v. Ukraine (Application no. 30663/04) 18 December 2008
Magee v. The United Kingdom (Application no. 28135/95) 6 June 2000
John Murray v. The United Kingdom (Application no. 18731/91) 8 February 1996
Nechiporuk and Yonkalo v. Ukraine (Application no. 42310/04) 21 April 2011
O'Halloran and Francis v. The United Kingdom (Applications nos. 15809/02 and 25624/02) 29 June 2007
Pavlenko v. Russia (Application no. 42371/02) 1 April 2010
P.G. and J.H. v. The United Kingdom (Application no. 44787/98) 25 September 2001
Quinn v. Ireland (Application no. 36887/97) 21 December 2000
Rieg v. Austria (Application no. 63207/00) 24 March 2005
Salduz v. Turkey (Application no. 36391/02) 27 November 2008
Saunders v. The United Kingdom (Application no. 19187/91) 17 December 1996
Shabelnik v. Ukraine (Application no. 16404/03) 19 February 2009
Shannon v. The United Kingdom (Application no. 6563/03) 4 October 2005
Todorov v. Ukraine (Application no. 16717/05) 12 January 2012
Weh v. Austria (Application no. 38544/97) 8 April 2004
Zaichenko v. Russia (Application no. 39660/02) 18 February 2010

Bijlage 6 Over de auteur

Prof. dr. Bert-Jaap Koops is hoogleraar regulering van technologie bij TILT, het Tilburg Institute for Law, Technology, and Society van de Universiteit van Tilburg. Van 2005-2010 was hij lid van De Jonge Akademie, een onderdeel van de Koninklijke Nederlandse Akademie van Wetenschappen.
Koops doet onderzoek naar regulering en technologie, in het bijzonder strafrechtelijke onderwerpen als opsporingsbevoegdheden en privacy, computercriminaliteit, cryptografie en DNA. Hij is ook geïnteresseerd in andere onderwerpen binnen technologieregulering, zoals identificatie, dataprotectie, digitale grondrechten, regulering door techniek, de maakbare mens, en regulering van bio-, nano- en neurotechnologie. Van 2004-2009 leidde hij een VIDI-onderzoeksprogramma over recht, technologie en schuivende machtsverhoudingen.
Koops studeerde wiskunde en algemene literatuurwetenschap in Groningen. Hij promoveerde in 1999 in de rechtswetenschappen op een onderzoek naar regulering van cryptografie. Koops is coredacteur van zes boeken over ICT-regulering, *Emerging Electronic Highways* (1996), *ICT Law and Internationalisation* (2000), *Starting Points for ICT Regulation* (2006), *Cybercrime and Jurisdiction* (2006), *Constitutional Rights and New Technologies* (2008) en *Dimensions of Technology Regulation* (2010). Hij publiceerde diverse boeken en vele artikelen over recht en technologie. Zijn webpublicatie *Crypto Law Survey* wordt wereldwijd beschouwd als een standaardbron over cryptografieregulering.

WODC-rapporten

Om zo veel mogelijk belanghebbenden te informeren over de onderzoeksresultaten van het WODC wordt een beperkte oplage van de rapporten kosteloos verspreid onder functionarissen, werkgroepen en instellingen binnen en buiten het ministerie van Justitie. Dit gebeurt aan de hand van een verzendlijst die afhankelijk van het onderwerp van het rapport opgesteld wordt. De rapporten in de reeks Onderzoek en beleid (O&B) worden uitgegeven door Boom Juridische uitgevers en zijn voor belangstellenden die niet voor een kosteloos rapport in aanmerking komen, te bestellen bij Boom distributiecentrum, Postbus 400, 7940 AK Meppel, tel.: 0522-23 75 55, via e-mail: budh@boomdistributiecentrum.nl.
Een complete lijst van de WODC-rapporten is te vinden op de WODC-site (www.wodc.nl). Daar zijn ook de uitgebreide samenvattingen te vinden van alle vanaf 1997 verschenen WODC-rapporten. Volledige teksten van de rapporten (vanaf 1999) zullen met terugwerkende kracht op de WODC-site beschikbaar komen. Hieronder volgen de titelbeschrijvingen van de vanaf 2007 verschenen rapporten.

Daalder, A.L. (2007). *Prostitutie in Nederland na opheffing van het bordeelverbod.* O&B 249. (*Prostitution in the Netherlands since the lifting of the brothel ban.* O&B 249a.)

Jennissen, R.P.W., & Oudhof, J. (red.) (2007). *Ontwikkelingen in de maatschappelijke participatie van allochtonen.* O&B 250.

Mheen, D. van de, & Gruter, P. (red.) (2007). *Helingpraktijken onder de loep: Impressies van helingcircuits in Nederland.* O&B 251.

Bunt, H.G. van de, & Kleemans, E.R., m.m.v. Poot, C.J. de, Bokhorst, R.J., Huikeshoven, M., Kouwenberg, R.F., Nassou, M. van, & Staring, R. (2007). *Georganiseerde criminaliteit in Nederland: Derde rapportage op basis van de Monitor Georganiseerde Criminaliteit.* O&B 252.

Struiksma, N., Ridder, J. de, & Winter, H.B. (2007). *De effectiviteit van bestuurlijke en strafrechtelijke milieuhandhaving.* O&B 253.

Eshuis, R.J.J. (2007). *Het recht in betere tijden: Over de werking van interventies ter versnelling van civiele procedures.* O&B 254.

Heide, W. van der, & Eggen, A.Th.J. (red.) (2007). *Criminaliteit en rechtshandhaving 2006: Ontwikkelingen en samenhangen.* O&B 255.

Tollenaar, N., Meijer, R.F., Huijbrechts, G.L.A.M., Blom, M., & Harbachi, S. el (2007). *Monitor Veelplegers: Jeugdige en zeer actieve veelplegers in kaart gebracht.* O&B 256.

Dijk, J. van, Kesteren, J. van, & Smit, P. (2007). *Criminal Victimisation in International Perspective: Key findings from the 2004-2005 ICVS en EU ICS.* O&B 257. (*Victimización en la perspectiva internacional: Resultados principales de la ENICRIV y ENECRIS 2004-2005.* O&B 257a.)

Spapens, A.C.M., Bunt, H.G. van de, & Rastovac, L. (2007). *De wereld achter de wietteelt.* O&B 258.

Koeter, M.W.J., & Bakker, M. (2007). *Effectevaluatie van de Strafrechtelijke Opvang Verslaafden (SOV).* O&B 259.

Kunst, M.J.J., Schweizer, S., Bogaerts, S., & Knaap, L.M. van der (2008). *Onderlinge agressie en geweld, posttraumatische stress en arbeidsverzuim in penitentiaire inrichtingen.* O&B 260. (*Aggression and violence, posttraumatic stress, and absenteeism among employees in penitentiaries.* O&B 260a.)

Voert, M.J. ter, & Peters, S.L. (2008). *Trendrapportage advocatuur 2006: Toegankelijkheid, continuïteit en kwaliteit van de dienstverlening.* O&B 261.

Boom, A. ten, & Kuijpers, K.F., m.m.v. Moene, M.H. (2008). *Behoeften van slachtoffers van delicten: Een systematische literatuurstudie naar behoeften zoals door slachtoffers zelf geuit.* O&B 262.

Kogel, C.H. de, & Nagtegaal, M.H. (2008). *Toezichtprogramma's voor delinquenten en forensisch psychiatrische patiënten: Effectiviteit en veronderstelde werkzame mechanismen.* O&B 263.

Hulst, R.C. van der, & Neve, R.J.M. (2008). *High-tech crime, soorten criminaliteit en hun daders: Een literatuurinventarisatie.* O&B 264.

Laclé, Z.D., & Voert, M.J. ter (2008). *Trendrapportage Notariaat 2006: Toegankelijkheid, continuïteit en kwaliteit van de dienstverlening.* O&B 265.

Guiaux, M., Uiters, A.H., Wubs, H., & Beenakkers, E.M.Th. (2008). *Uitgenodigde vluchtelingen.* O&B 266.

Klein Haarhuis, C.M., & Niemeijer, E. (2008). *Wet en werkelijkheid: Bevindingen uit evaluaties van wetten.* O&B 267.

Laan, A.M. van der, Vervoorn, L., Schans, C.A. van der, & Bogaerts, S. (2008). *Ik zit vast: Een exploratieve studie naar emotionele verwerking van justitiële vrijheidsbeneming door jongeren.* O&B 268. (*Being inside: An explorative study into emotional reactions of juvenile offenders to custody.* O&B 268a.)

Teeuw, Wouter B., Vedder, Anton H., Custers, Bart H.M., Dorbeck-Jung, Bärbel R., Faber, Edward C.C., Iacob, Sorin M., Koops, Bert-Jaap, Leenes, Ronald E., Poot, Henk J.G. de, Rip, Arie, & Vudisa, Jacques N. (2008). *Security Applications for Converging Technologies: Impact on the constitutional state and the legal order.* O&B 269.

Kogel, C.H. de (2008). *De hersenen in beeld: Neurobiologisch onderzoek en vraagstukken op het gebied van verklaring, reductie en preventie van criminaliteit.* O&B 270.

Eggen, A.Th.J., & Kalidien, S.N. (red.) (2008). *Criminaliteit en rechtshandhaving 2007: Ontwikkelingen en samenhangen.* O&B 271.

Gestel, B. van, m.m.v. Kouwenberg, R.F., Verhoeven, M.A., & Verkuylen, M.W. (2008). *Vastgoed & fout: Een analyse van twaalf strafrechtelijke opsporingsonderzoeken naar illegale en criminele praktijken in de woningsector.* O&B 272.

Gosselt, J.F., Hoof, J.J. van, Jong, M.D.T. de, Dorbeck-Jung, B., & Steehouder, M.F. (2008). *Horen, zien en verkrijgen? Een onderzoek naar het functioneren van Kijkwijzer en PEGI (Pan European Game Information) ter bescherming van jongeren tegen schadelijke mediabeelden.* O&B 273.

Ridder, J. de, Klein Haarhuis, C.M., & Jongste, W.M. de (2008). *De ceas aan het werk: Bevindingen over het functioneren van de Commissie Evaluatie Afgesloten Strafzaken 2006-2008.* O&B 274.

Wartna, B.S.J. (2009). *In de oude fout: Over het meten van recidive en het vaststellen van het succes van strafrechtelijke interventies.* O&B 275.

Laan, A.M. van der, Schans, A. van der, Bogaerts, S., & Doreleijers, Th.A.H. (2009). *Criminogene en beschermende factoren bij jongeren die een basisraadsonderzoek ondergaan: Een verkennende inventarisatie van de mate van zorg en van risico- en beschermende factoren gesignaleerd door raadsonderzoekers.* O&B 276.

Jennissen, R.P.W. (2009). *Criminaliteit, leeftijd en etniciteit: Over de afwijkende leeftijdsspecifieke criminaliteitscijfers van in Nederland verblijvende Antillianen en Marokkanen.* O&B 277.

Klapwijk, A., & Voert, M. ter (2009). *Evaluatie De Geschillencommissie 2009.* O&B 278.

Kalidien, S.N., & Eggen, A.Th.J. (2009). *Criminaliteit en rechtshandhaving 2008: Ontwikkelingen en samenhangen.* O&B 279.

Jong, P.O. de, & Zijlstra, S.E., m.m.v. Ommeren, F.J. van, Neerhof, A.R., & Lange, F.A. de (2009). *Wikken, wegen en (toch) wetgeven: Een onderzoek naar de hiërarchie en omvang van wetgeving in vijf Europese landen.* O&B 280.

Poot, C.J. de, & Sonnenschein, A., m.m.v. Soudijn, M.R.J., Bijen, J.G.M., & Verkuylen, M.W. (2009). *Jihadistisch terrorisme in Nederland: Een beschrijving op basis van afgesloten opsporingsonderzoeken.* O&B 281.

Kruisbergen, E.W., & Jong, D. de, m.m.v. Kouwenberg, R.F. (2010). *Opsporen onder dekmantel: Regulering, uitvoering en resultaten van undercovertrajecten.* O&B 282.

Velthoven, B.C.J. van, & Klein Haarhuis, C.M. (2010). *Geschilbeslechtingsdelta 2009: Over verloop en afloop van (potentieel) juridische problemen van burgers.* O&B 283.

Diephuis, B.J., Eshuis, R.J.J., & Heer-de Lange, N.E. de (2010). *Rechtspleging Civiel en Bestuur 2008: Ontwikkelingen en samenhangen.* O&B 284.

Killias, M., Aebi, M.F., Aubusson de Cavarlay, B., Barclay, G., Gruszczyńska, B., Harrendorf, S., Heiskanen, M., Hysi, V., Jehle, J.-M., Shostko, O., Smit, P., Þórisdóttir, R., & Jaquier, V. (2010). *European Sourcebook of Crime and Criminal Justice Statistics – 2010.* O&B 285.

Wijkhuijs, L.J.J., & Jennissen, R.P.W. (2010). *Arbeidsmigratie naar Nederland: De invloed van gender en gezin.* O&B 286.

Knaap, L.M. van der, El Idrissi, F., & Bogaerts, S. (2010). *Daders van huiselijk geweld.* O&B 287.

Veen, H.C.J. van der, & Bogaerts, S. (2010). *Huiselijk geweld in Nederland: Overkoepelend syntheserapport van het vangst-hervangst-, slachtoffer- en daderonderzoek 2007-2010.* O&B 288.

Heer-de Lange, N.E. de, & Kalidien, S.N. (2010). *Criminaliteit en rechtshandhaving 2009: Ontwikkelingen en samenhangen.* O&B 289.
Nagtegaal, M.H., Horst, R.P. van der, & Schönberger, H.J.M. (2011). *Inzicht in de verblijfsduur van tbs-gestelden: Cijfers en mogelijke verklaringen.* O&B 290.
Poot, C.J. de, & Sonnenschein, A., m.m.v. Soudijn, M.R.J., Bijen, J.G.M., & Verkuylen, M.W. (2011). *Jihadi terrorism in the Netherlands: A description on closed criminal investigations.* O&B 291. [Engelse vertaling van O&B 281.]
Laan, A.M. van der, & Blom, M. (2011). *Meer jeugdige verdachten, maar waarom? Een studie naar de relatie tussen maatschappelijke ontwikkelingen en de veranderingen in het aantal jeugdige verdachten van een misdrijf in de periode 1997-2007.* O&B 292.
Slotboom, A., Wong, T.M.L., Swier, C., & Broek, T.C. van der (2011). *Delinquente meisjes: Achtergronden, risicofactoren en interventies.* O&B 293.
Molleman, T. (2011). *Benchmarking in het gevangeniswezen: Een onderzoek naar de mogelijkheden van het vergelijken en verbeteren van prestaties.* O&B 294.
Verhoeven, M.A., Gestel, B. van, & Jong, D. de (2011). *Mensenhandel in de Amsterdamse raamprostitutie: Een onderzoek naar aard en opsporing van mensenhandel.* O&B 295.
Voert, M.J. ter, Zwenk, F., & m.m.v. Beenakkers, E.M.Th. (2011). *Kwaliteit in zware tijd: Marktwerking, vraaguitval en notariële dienstverlening.* O&B 296.
Weenink, A.W., Klein Haarhuis, C.M., Bokhorst, R.J., Smit, M. (2011). *De staat van bestuur van Aruba: Een onderzoek naar de deugdelijkheid van bestuur en de rechtshandhaving.* O&B 297.
Kalidien, S.N., & Heer-de Lange, N.E. de, m.m.v. Rosmalen, M.M. van (2011). *Criminaliteit en rechtshandhaving 2010: Ontwikkelingen en samenhangen.* O&B 298.
Jennissen, R.P.W. (red.) (2011). *De Nederlandse migratiekaart: Achtergronden en ontwikkelingen van verschillende internationale migratietypen.* O&B 299.
Eichelsheim, V.I., Laan, A.M. van der (2011). *Jongeren en vrijheidsbeneming: Een studie naar de wijze waarop jongeren in Justitiële Jeugdinrichtingen omgaan met vrijheidsbeneming.* O&B 300.
Eshuis, R.J.J., Heer-de Lange, N.E. de, Diephuis, B.J., & Rosmalen, M.M. van (2011). *Rechtspleging Civiel en Bestuur 2010: Ontwikkelingen en samenhangen.* O&B 301.
Fischer, T.F.C., Captein, W.J.M., & Zwirs, B.W.C. (2012). *Gedragsinterventies voor volwassen justitiabelen.* O&B 302.
Eshuis, R.J.J., Holvast, N.L., Bunt, H.G. van de, Erp, J.G. van, & Pham, N.T. (2012). *Het aansprakelijk stellen van bestuurders: Onderzoek naar de overwegingen die spelen bij het al dan niet intern aansprakelijk stellen van bestuurders en interne toezichthouders.* O&B 303.