Koops, B.J. (2000). *Verdachte en ontsleutelplicht: hoe ver reikt nemo tenetur? Verschenen in: ITeR, 31.* Deventer: Kluwer, 125 pp.

Verdachte en ontsleutelplicht: hoe ver reikt nemo tenetur?

Koops, B.J. (2000). *Verdachte en ontsleutelplicht: hoe ver reikt nemo tenetur? Verschenen in: ITeR, 31.* Deventer: Kluwer, 125 pp.

Verdachte en ontsleutelplicht: hoe ver reikt nemo tenetur?

Bert-Jaap Koops

Kluwer, Deventer 2000

Koops, B.J. (2000). *Verdachte en ontsleutelplicht: hoe ver reikt nemo tenetur? Verschenen in: ITeR, 31.* Deventer: Kluwer, 125 pp.

Onderzoeksrapporten die recentelijk in de IT*e*R-reeks zijn verschenen (een lijst van alle publicaties van de IT*e*R-reeks staat achterin deze uitgave):

- Knowing the law. Legal information systems as a source of knowledge (IT*e*R nr. 25, 1999)
- Constitutionele convergentie van pers, omroep en telecommunicatie (IT*e*R nr. 26, 2000)
- Verdeling van het spectrum (IT*e*R nr. 27, 2000)
- De universiteitsbibliotheek in het databankenrecht (IT*e*R nr. 28, 2000)
- Het bibliotheekprivilege in de digitale omgeving (IT*e*R nr. 29, 2000)
- De wenselijkheid en mogelijkheid van infiltratie en pseudo-koop op het Internet (IT*e*R nr. 30, 2000)

In de IT*e*R-reeks worden de resultaten van het Nationaal Programma voor Informatietechnologie en Recht gepubliceerd. Meer informatie over IT*e*R en de in het kader van IT*e*R lopende onderzoeksprojecten is te vinden op de weblocatie: <http://www.nwo.nl/iter>.

Redactie: Annemique de Kroon en Aernout Schmidt
Redactieadres: Programmabureau IT*e*R, Postbus 93120, 2509 AC Den Haag, telefoon 070 3151950, fax 070 3832841, e-mail iter@nwo.nl

Het is mogelijk om een abonnement op de IT*e*R-reeks te nemen. IT*e*R-onderzoekers, rechtenstudenten, leden van de NVvIR en van de VMC, alsmede bestuursleden en waarnemers van de stichting JURIX krijgen 50 procent korting op de abonnementsprijs. Abonnementenregistratie: Kluwer/Libresso, Postbus 23, 7400 GA Deventer, e-mail: libresso@kluwer.nl, telefoon 0570 633155, fax 0570 621660.

ISBN 90-268-3655-4
NUGI 697/706

Omslagontwerp: Wim Goedhart

© 2000, Bert-Jaap Koops

Niets uit deze uitgave mag worden verveelvoudigd en/of worden openbaar gemaakt door middel van druk, fotokopie, microfilm of op welke andere wijze dan ook zonder voorafgaande schriftelijke toestemming van de auteur. Het gebruik van tekst als toelichting of ondersteuning bij artikelen, boeken en scripties is toegestaan, mits de bron duidelijk wordt vermeld.

Koops, B.J. (2000). *Verdachte en ontsleutelplicht: hoe ver reikt nemo tenetur? Verschenen in: ITeR, 31.* Deventer: Kluwer, 125 pp.

Voorwoord

Dit deel van de ITeR-reeks onderzoekt of de politie verdachten kan bevelen versleutelde gegevens leesbaar te maken. In opsporingsonderzoeken loopt justitie aan tegen versleutelde telecommunicatie en computerbestanden, waardoor zij geen kennis kan nemen van de inhoud. Een van de weinige mogelijkheden om iets aan dit probleem te doen is om de houder van het versleutelde bestand of de geadresseerde van het versleutelde bericht te bevelen het te ontsleutelen. Een dergelijk bevel mag momenteel niet worden gegeven aan de verdachte – die hoeft immers niet mee te werken aan zijn eigen veroordeling (het nemo-teneturbeginsel). De centrale vraag in dit rapport is of een ontsleutelplicht voor verdachten verenigbaar is met het nemo-teneturbeginsel, gegeven de op het spel staande belangen van misdaadbestrijding en het recht op een eerlijk proces. Daartoe wordt het nemo-teneturbeginsel bestudeerd, door een analyse van de ratio van het beginsel en door een overzicht van de inbreuken die naar huidig recht zijn toegestaan op nemo tenetur. Ook worden de technische kanten van de ontsleutelplicht geanalyseerd, met name de vraag in hoeverre verdachten in staat zijn te ontsleutelen. De juridische en technische analyses worden vervolgens met elkaar in verband gebracht om een aanbeveling te doen voor de wetgever over een ontsleutelplicht voor verdachten.

Dit rapport is het resultaat van een stand-van-zakenonderzoek in het kader van het ITeR-programma. Het Nationaal Programma Informatietechnologie en Recht (ITeR) is een stimuleringsprogramma dat onderzoek naar actuele juridische vraagstukken op het gebied van informatie- en communicatietechnologie stimuleert en financiert. Het programma is een samenwerkingsverband tussen de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO) en de ministeries van Economische Zaken, Binnenlandse Zaken en Koninkrijksrelaties, Justitie, Onderwijs, Cultuur en Wetenschappen, en Verkeer en Waterstaat.

Inleiding

Bij het schrijven van dit rapport heb ik dankbaar gebruik gemaakt van commentaar van Marc Groenhuijsen en Klaas Rozemond op een eerdere versie.

Het onderzoek is uitgevoerd van juli tot en met december 1999.
De studie is afgerond op 5 januari 2000.

Bert-Jaap Koops
Tilburg, januari 2000

Koops, B.J. (2000). *Verdachte en ontsleutelplicht: hoe ver reikt nemo tenetur? Verschenen in: ITeR, 31.* Deventer: Kluwer, 125 pp.

Inhoudsopgave

Voorwoord **iii**

Deel I. Achtergronden **1**

1. Inleiding **3**

2. Context – de cryptocontroverse **7**
2.1 Cryptografie 7
2.2 Problemen voor de opsporing 10
2.3 'Oplossingen' 11
2.4 Wetgeving Nederland 12
2.5 Wetgeving buitenland 13
2.6 Wenselijkheid van een ontsleutelplicht 14

3. De huidige wettelijke status van de ontsleutelplicht **15**
3.1 De ontsleutelplicht in Nederland 15
3.1.1 Computercriminaliteit I 15
3.1.2 Computercriminaliteit II 18
3.2 De ontsleutelplicht in andere landen 21

Deel II. Grenzen van de ontsleutelplicht voor verdachten **25**

4. Het nemo-teneturbeginsel **27**
4.1 Bestaat het nemo-teneturbeginsel? 27
4.1.1 Funke 28
4.1.2 Murray 29
4.1.3 Saunders 30
4.2 Het systeem van de Nederlandse wet 33
4.3 De reikwijdte van nemo tenetur 34

Inleiding
4.3.1 Onafhankelijk materiaal, de wil van de verdachte en het zwijgrecht 35
4.3.2 Controle, opsporing, verdenking, vervolging en bewijs 36
4.3.3 Natuurlijke en rechtspersonen en soort delicten 38
4.3.4 Actieve en passieve medewerking 42
4.4 De ratio van nemo tenetur 44
4.5 Een definitie van het nemo-teneturbeginsel 48
4.6 Maakt een ontsleutelplicht inbreuk? 53

5. Analogieën en precedenten 55
5.1 Analogieën 55
5.1.1 Bevel geheimschrift prijs te geven 55
5.1.2 Bevel te vertalen 57
5.2 Precedenten 58
5.2.1 Plichten te verklaren 58
Meldplichten 58
Inlichtingenplichten 61
Kentekenaansprakelijkheid 62
Zwijgen en omkering van de bewijslast 64
Spreekplicht van getuigen 66
5.2.2 Plichten actief mee te werken 67
5.2.3 Conclusie 70

6. Opties voor een ontsleutelplicht 73

7. Handhaving en technische bezwaren 77
7.1 Opzet of risico-aansprakelijkheid? 77
7.2 In staat zijn te ontsleutelen 79
7.3 Conclusie 88

8. Afweging 89

9. Conclusies en aanbevelingen 99

Summary 101

Bibliografie 115

Afkortingen 121

Auteur 123

Koops, B.J. (2000). *Verdachte en ontsleutelplicht: hoe ver reikt nemo tenetur? Verschenen in: ITeR, 31.* Deventer: Kluwer, 125 pp.

Deel I. Achtergronden

Koops, B.J. (2000). *Verdachte en ontsleutelplicht: hoe ver reikt nemo tenetur? Verschenen in: ITeR, 31.* Deventer: Kluwer, 125 pp.

1. Inleiding

Er is een duidelijke maatschappelijke behoefte om digitale gegevens te beschermen tegen onbevoegde kennisname. De laatste jaren neemt het gebruik van gegevensversleuteling (encryptie) dan ook toe. Ook misdadigers beginnen te ontdekken dat versleutelsystemen (cryptografie) handig zijn om hun verdachte informatiestromen aan het wakend oog van justitie te onttrekken. Hun berichten zien er niet meer zo uit:

> *Kom morgenmiddag naar de haven om de lading van de MS Extaze binnen te halen!*

maar zo:

> *qANQR1DBwU4DoFOjvEqaYQoQCADuZoWNo9hpUCugPFABqjbmsQwElkYgRxH5Dm5Yh7seCQ1CG31AWkacOl/DVpmxpL7Og9nMiBmmucNg5BZn9kkrqT3qJhw7gbzPtwsJ4WgP3KHx3A/Ep7+4BnZFCVc1sNlN4CpE7UiELWliee/*

Waar justitie tegen dergelijke versleuteling aanloopt, heeft zij weliswaar de mogelijkheid om iemand te bevelen te ontsleutelen, maar dit bevel mag niet aan verdachten worden gegeven. En het is meestal alleen de verdachte die de sleutel kent. Daar schiet justitie dus weinig mee op.

Daarom werd in 1998 een ballonnetje opgelaten in het concept-wetsvoorstel Computercriminaliteit II. Onder bepaalde omstandigheden zou de politie een ontsleutelbevel ook aan de verdachte mogen geven. Het ballonnetje werd ijverig doorgeprikt door juridisch Nederland, geschokt over deze inbreuk op het nemo-teneturbeginsel, en de bepaling werd uit het wetsvoorstel geschrapt. Daar schiet justitie dus nóg niet veel mee op.

Een ontsleutelingsplicht voor verdachten is evenwel een van de beste alternatieven – en misschien wel het enige – om iets aan het probleem van cryptogebruik door misdadigers te doen (zie hoofdstuk 2). Daarom is het relevant om te onderzoeken in hoeverre een bevel aan verdachten om te ontsleutelen toch in het Nederlandse strafprocesrecht zou kunnen worden ingevoerd, met inachtneming van de grenzen die het nemo-teneturbeginsel en praktische bezwaren daaraan stellen. Daarbij moet er ook gekeken worden naar

de sanctiemogelijkheden als de verdachte weigert te voldoen aan zo'n bevel – als er geen reële dreiging is van een sanctie, zal het bevel immers krachteloos zijn.
Dit leidt tot de volgende **probleemstelling** van deze studie:

> *In hoeverre is een ontsleutelbevel aan verdachten verenigbaar met het nemo-teneturbeginsel? 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?*

Ik beperk mij in deze studie tot de opsporing. Versleuteling levert ook problemen op voor de bescherming van de nationale veiligheid, maar dat is een andere problematiek, alleen al omdat een ontsleutelbevel moeilijk verenigbaar is met het heimelijke karakter van veiligheidsonderzoeken.[1]
Ook beperk ik mij in dit rapport tot een toetsing van een ontsleutelbevel aan het nemo-teneturbeginsel. Mogelijk maakt een ontsleutelplicht ook inbreuk op de persoonlijke levenssfeer (art. 8 EVRM, art. 10 GW), zodat een zelfstandige toetsing aan dit grondrecht nodig is. Daarvoor is geen plaats binnen het bestek van dit onderzoek. Overigens hoeft deze toets pas te worden uitgevoerd als de resultaten van dit onderzoek zouden aangeven dat een ontsleutelplicht voor verdachten een gerechtvaardigde inbreuk op nemo tenetur zou zijn en daarom invoering zou behoeven.

De **opbouw** van dit rapport is als volgt. De rest van deel I schetst de context van de problematiek: het cryptoprobleem voor justitie en mogelijke oplossingen daarvoor (hoofdstuk 2) en de huidige wetgeving rond de ontsleutelplicht (hoofdstuk 3). Vervolgens wordt in deel II de probleemstelling in drie deelvragen beantwoord.

1. Hoe ziet het nemo-teneturbeginsel eruit (par. 4.1-4.5)?
2. Maakt een ontsleutelplicht daarop inbreuk (par. 4.6)?
3. Is een wettelijke ontsleutelplicht aanvaardbaar en zo ja, onder welke voorwaarden (hoofdstukken 5-8)? Bij de beantwoording van deze derde onderzoeksvraag kijk ik naar analogieën in het huidige recht (hoofdstuk 5), welke vormen een ontsleutelplicht kan aannemen (hoofdstuk 6), technische en praktische grenzen in verband met de handhaafbaarheid (hoofdstuk 7), en argumenten waarmee het opsporingsbelang en de rechten van de verdachte in dit geval kunnen worden afgewogen (hoofdstuk 8).

Ten slotte trek ik conclusies en geef ik aanbevelingen voor de Nederlandse wetgever (hoofdstuk 9).

---

[1] Niettemin stelt het wetsvoorstel voor de Wet op de inlichtingen- en veiligheidsdiensten wel een ontsleutelplicht voor, zie art. 24 lid 3 en art. 25 lid 8. TK 1997-1998, 25 877, nrs. 1-2.

Nog enkele opmerkingen over **terminologie**. Ik gebruik de termen versleuteling en encryptie voor het proces van onleesbaar maken van gegevens, met als synoniem vercijfering; decryptie slaat op het omgekeerde proces – ontsleuteling of ontcijfering, het weer leesbaar maken van de oorspronkelijke gegevens. Cryptografie duidt op geautomatiseerde systemen voor versleuteling.
Ik gebruik in dit rapport verschillende aanduidingen van "de ontsleutelplicht" en "het decryptiebevel": een bevel of gebod om te ontsleutelen, dan wel een bevel of gebod om een sleutel te overhandigen of een wachtwoord te geven dat de sleutel beveiligt. Hoewel er praktische verschillen zijn tussen deze vormen, maakt het voor de vraag naar juridische toelaatbaarheid weinig uit. Het gaat steeds om de vraag of de verdachte door mee te werken aan ontsleuteling meewerkt aan zijn eigen veroordeling en of dit juridisch aanvaardbaar is.

Koops, B.J. (2000). *Verdachte en ontsleutelplicht: hoe ver reikt nemo tenetur? Verschenen in: ITeR, 31.* Deventer: Kluwer, 125 pp.

2. Context – de cryptocontroverse[2]

2.1 Cryptografie

Volgens David Kahn, geschiedschrijver van de cryptografie, ontstaat er in elke taal al vroeg een behoefte aan geheimtaal. Kennelijk is de behoefte aan geheime, vertrouwelijke communicatie net zo oud als de behoefte aan communicatie zelf. Kahn geeft in zijn standaardwerk *The Codebreakers*[3] mooie voorbeelden van geheimtaalsystemen. Julius Caesar ontwierp een systeem waarin elke letter drie plaatsen in het alfabet opschoof; om een geheimtekst te ontcijferen moest men dus elke letter drie plaatsen terugschuiven in het alfabet. De Spartanen gebruikten een "hardware"-systeem: een staaf waar de zender een smalle strook papyrus omwikkelde, waarop de tekst vervolgens in verticale kolommen werd genoteerd: bij het afwikkelen kwamen de letters zodoende door elkaar op de strook te staan. De ontvanger kon de tekst weer lezen door de papyrusstrook rond een staaf van dezelfde dikte te wikkelen.
Door de jaren heen werden de geheimtalen steeds ingewikkelder, maar de principes van Caesar (substitutie: het vervangen van letters door andere) en de Spartanen (transpositie: het door elkaar husselen van letters) bleven basisbeginselen. In de Tweede Wereldoorlog gebruikte men ingenieuze coderingsmachines die een tekst letter voor letter vervingen aan de hand van een veelcijferige begintoestand (die, net als het cijfer 3 bij Caesar, de sleutel vormde tot het ontcijferen).

In de jaren zeventig ontstond de moderne, geautomatiseerde cryptografie.[4] De overheid van de VS koos in 1976 een nieuwe standaard voor het versleutelen

---

2 Voor een uitgebreider overzicht van de context van de ontsleutelplicht voor verdachten verwijs ik naar mijn proefschrift, Koops 1998.

3 Kahn 1967.

4 Voor een overzicht van moderne cryptografie zie Schneier 1996 en Menezes, van Oorschot & Vanstone 1996.

van gevoelige overheidsinformatie, de Data Encryption Standard (DES). Het is een complex algoritme dat een tekst in blokken versleutelt met behulp van een 56-bits-sleutel. Hoewel het dezelfde simpele principes als Caesar en de Spartanen gebruikt (substitutie en transpositie), en het algoritme algemeen bekend is, is het proces van versleuteling dermate complex dat het zelfs tegenwoordig niet makkelijk te kraken is. Voor wie de sleutel niet kent, is de enige manier om een tekst te ontcijferen het uitproberen van alle mogelijke sleutels (2^{56}, ongeveer 72 biljard sleutels), wat zelfs met moderne supercomputers nog een paar uur tijd kost.[5] Voor echt gevoelige informatie gebruikt men tegenwoordig triple-DES, waarbij een tekst drie keer met DES wordt versleuteld – dat geldt in elk geval voor de komende tien jaar als onkraakbaar.
Het nadeel van DES, zoals van alle traditionele crypto-systemen, is echter dat zowel de zender als de ontvanger dezelfde, geheime sleutel moeten hebben: het is een symmetrisch systeem. Die sleutel moet dus op een betrouwbare manier worden overgebracht, wat een ander kanaal vergt dan dat waarover men wil communiceren (dat is immers onveilig, anders hoef je geen cryptografie te gebruiken). Hij moet bijvoorbeeld met de post of met een koerier worden verstuurd in plaats van met e-mail, of je moet hem in persoon overhandigen. Waar dat op kleine schaal goed mogelijk is, is zo'n systeem op grote schaal minder toepasbaar. Als een bedrijf met veel klanten veilig wil communiceren, is het weinig aantrekkelijk om met elke klant afzonderlijk een geheime sleutel in persoon uit te wisselen.

Om het probleem van sleuteluitwisseling op te lossen, is in de jaren zeventig een andere vorm van cryptografie uitgevonden: de asymmetrische cryptografie. Diffie en Hellman ontwikkelden een systeem waarbij Annie en Bob op een openbare manier sleutels kunnen uitwisselen. Diffie-Hellman is gebaseerd op een wiskundige "eenrichtingsfunctie": het is gemakkelijk om in een bepaald wiskundig stelsel te machtsverheffen, maar zeer complex om daarin wortel te trekken (in wiskundige termen: het discrete logaritme te nemen); het is alleen makkelijk als je extra informatie hebt. Kort na Diffie-Hellman ontwikkelden Rivest, Shamir en Adleman een soortgelijk systeem (RSA), gebaseerd op een ander wiskundig probleem, het ontbinden in factoren.
Asymmetrische cryptografie gaat uit van het principe dat elke gebruiker twee sleutels heeft: een openbare en een privésleutel.[6] Elke gebruiker verspreidt haar openbare sleutel onder potentiële communicatiepartners; de privésleutel houdt zij strikt geheim. De privésleutel wordt normaliter opgeslagen op een

5 Zie Blaze 1996 en Lenstra & Verheul 1999.

6 Voor de duidelijkheid reserveer ik de term "geheime sleutel" voor een sleutel in een symmetrisch systeem, zoals DES; de geheime sleutel in asymmetrische systemen duid ik aan met privésleutel.

gegevensdrager (harde schijf of diskette), beveiligd met een wachtwoord (of liever nog een wachtzin). Annie en Bob kunnen nu als volgt veilig communiceren. Bob zoekt Annies openbare sleutel op (bijvoorbeeld in een telefoonboek of een openbaresleutelregister) en versleutelt daarmee een bericht. Hij stuurt het bericht naar Annie, die het vervolgens ontcijfert met haar corresponderende privésleutel. Als Eva (een afluisteraar, naar het Engelse "eavesdropper") Bobs bericht onderschept, kan zij het niet ontcijferen, omdat zij Annies privésleutel niet kent. Het systeem berust op de moeilijkheid om uit de publieke sleutel de privésleutel af te leiden: dat is bij robuuste systemen zoals RSA of Diffie-Hellman praktisch onmogelijk. De sleutellengtes worden dusdanig gekozen dat het iemand die de privésleutel niet kent te veel rekenkracht (dat wil zeggen: tijd en geld) kost om met enige kans van slagen een bericht te proberen te ontcijferen.
Een analogie kan dit verduidelijken. Annie gebruikt vertaling in het Koeterwaals als haar cryptosysteem. Ze heeft een publieke sleutel: het woordenboek Nederlands-Koeterwaals, en een privé-sleutel: het woordenboek Koeterwaals-Nederlands. Bob versleutelt een boodschap aan Annie door met het woordenboek Nederlands-Koeterwaals het bericht in het Koeterwaals te vertalen. Annie kan het vervolgens lezen door het terug te vertalen naar het Nederlands. Omdat zij de enige is met een woordenboek Koeterwaals-Nederlands, blijft de boodschap voor alle anderen Koeterwaals. Iemand kan weliswaar de moeite nemen om bij elk woord Koeterwaals het (openbare) woordenboek Nederlands-Koeterwaals te gebruiken om te kijken bij welk Nederlands woord dit hoort, maar dit is in de praktijk – zeker bij de Dikke Koeterwaals – praktisch onmogelijk.

De voordelen van een asymmetrisch systeem zijn duidelijk: Annie en Bob hoeven niet via een ander, persoonlijk kanaal een sleutel uit te wisselen. Ook hebben zij niet voor elke communicatiepartner een andere sleutel nodig: één sleutelpaar per gebruiker volstaat in principe.
In de praktijk werkt de versleuteling overigens iets anders. Omdat het versleutelen met een asymmetrisch systeem veel meer tijd kost dan met een symmetrisch systeem, versleutelt Annie een bericht met een symmetrisch systeem, bijvoorbeeld IDEA. Vervolgens wisselt zij met Bob de symmetrische sleutel uit met behulp van een asymmetrisch systeem, bijvoorbeeld RSA. Dit doet ze door de IDEA-sleutel te versleutelen met Bobs openbare RSA-sleutel. Ze kan nu in één keer sturen: het bericht versleuteld met IDEA, en de IDEA-sleutel versleuteld met RSA. Bob gebruikt bij ontvangst eerst zijn privé-RSA-sleutel om de IDEA-sleutel te achterhalen, en past deze vervolgens toe op het versleutelde bericht. Via zo'n "hybride" systeem (een combinatie van een

symmetrisch en een asymmetrisch systeem) kan men dus doelmatig vertrouwelijk communiceren.

Cryptografie wordt overigens niet alleen gebruikt voor het waarborgen van vertrouwelijkheid, maar ook voor het waarborgen van integriteit en authenticiteit, en wel in digitale handtekeningen.[7] Hoewel deze toepassing geen problemen oplevert voor de opsporing (digitaal ondertekende berichten zijn gewoon te lezen), is het wel relevant om rekening mee te houden bij een mogelijk decryptiebevel. In diverse systemen, zoals PGP, kan namelijk één en hetzelfde sleutelpaar gebruikt worden voor zowel vertrouwelijkheid (versleutelen) als authenticiteit (digitale handtekening). Wanneer nu een politie-agente de privésleutel van een verdachte zou verkrijgen om onderschepte berichten te kunnen lezen, zou zij ook (verdachte) berichten kunnen (fabriceren en) ondertekenen namens de verdachte. Voor de betrouwbaarheid van het bewijs is het dus noodzakelijk dat de privésleutel die de verdachte gebruikt voor digitale handtekeningen, niet in handen komt van de politie. Een eventueel ontsleutelbevel zal daarmee rekening moeten houden.

2.2 Problemen voor de opsporing

Cryptografie heeft inmiddels een brede toepassing gekregen – het is een essentieel onderdeel van informatiebeveiliging. Het wordt bijvoorbeeld gebruikt voor de beveiliging van telecommunicatie, persoonsgegevens, elektronische betaalsystemen, intellectuele-eigendomsrechten, gevoelige overheids- en bedrijfsinformatie en mensenrechten. Het kan ook misdaad voorkómen, zoals computercriminaliteit en bedrijfsspionage.
Vervelend genoeg heeft cryptografie niet alleen positieve kanten. Misdadigers kunnen het gebruiken om aan oog en oor van de politie te ontsnappen. Onderzoek in computers en telefoontaps hebben weinig zin als de daarmee verkregen gegevens versleuteld blijken. Nu zijn onkraakbare cryptosystemen makkelijk verkrijgbaar (het programma Pretty Good Privacy (PGP) is binnen te halen van diverse locaties op het Internet), en in de praktijk blijken misdadigers daarvan ook al gebruik te maken. Veel gebeurt dat (nog) niet – in de praktijk lijkt het cryptogebruik van misdadigers vooralsnog beperkt te zijn tot enkele (georganiseerde of computerdeskundige) boeven, die het vooral toepassen bij opgeslagen gegevens. Er zijn weinig gevallen bekend van zaken waarin afgetapte telecommunicatie versleuteld bleek.[8] En daarbij bleken de zaken uiteindelijk

7 Zie ITeR-deel 7.

8 Voor een overzicht van opsporingszaken met cryptografie, zie Denning & Baugh 1997 en de actualisering daarvan in Denning & Baugh 1999.

geen obstakel te vormen voor een veroordeling, hetzij omdat er genoeg ander bewijs was, hetzij omdat de misdadiger zo onhandig was geweest om het wachtwoord ergens op te schrijven of om een makkelijk kraakbaar systeem te gebruiken.
De algemene verwachting is echter wel dat de problemen voor de opsporing groter zullen worden. Cryptografie wordt steeds meer ingebouwd in standaardprogramma's, zoals e-post-, webblader-, tekstverwerkings- en besturingsprogrammatuur. Bovendien worden de systemen steeds gebruikers-vriendelijker. Daarmee komen robuuste systemen binnen handbereik van die boeven die momenteel nog niet de moeite nemen om aparte programmatuur binnen te halen. Ook de ontwikkeling van Internettelefonie zal bijdragen tot omvangrijker cryptogebruik bij telecommunicatie – een programma als PGPfone is makkelijker te verkrijgen dan huidige cryptofoons. Binnen justitie en politie bestaat dan ook de vrees dat computeronderzoek en telefoontaps een belangrijk deel van hun waarde voor de opsporing zullen verliezen als er niets aan het cryptogebruik door misdadigers wordt gedaan.[9]

2.3 'Oplossingen'

Maar wat valt er aan het probleem te doen? Domweg verbieden van cryptografie, of het verbinden aan een vergunningstelsel, zoals een louche Nederlands wetsontwerp in 1994 voorstelde, is geen optie – misdadigers zouden zich er niets van aantrekken. Ook het kraken van versleutelde berichten is geen daadwerkelijke optie, omdat de kraakbaarheid afhangt van fouten van de boef – alleen als hij een slecht cryptosysteem gebruikt of zijn sleutels laat slingeren, kan de politie kraken; bij goed gebruik van cryptografie blijven de gegevens ontoegankelijk.[10] Er zijn theoretisch drie mogelijkheden.

1. Het stimuleren van BEDOT-cryptografie (dat wil zeggen: Bevat Een Decryptiemogelijkheid voor OpsporingsToegang). Er zijn systemen met een ingebouwd sleuteldepot- of sleutelherwinningsmechanisme, die ervoor zorgen dat de politie de sleutel kan achterhalen zonder dat de verdachte het merkt. Er kleven diverse bezwaren aan deze optie, waaronder de verminderde veiligheid van dergelijke systemen, en het feit dat een beetje boef geen cryptosysteem zal gebruiken waarvan hij weet dat het hem BEDOT.

---

9 Zie Koops 1998, p. 95.

10 Zie Koops 1998, p. 91-92, over kraakbaarheid van cryptografie door de politie. Hoewel het in de praktijk vaak blijkt te lukken, acht ik dit geen optie, omdat het afhangt van de 'medewerking' van (minder slimme) boeven. Het probleem is nu juist het doordacht cryptogebruik van slimme boeven.

2. Het bevelen van personen om te ontsleutelen. Meestal zal alleen een verdachte in staat zijn te ontsleutelen, en in dat geval stuit een decryptiebevel wellicht op het nemo-teneturbeginsel.
3. Het gebruik van alternatieve opsporingsmethoden. Als cryptosleutels niet beschikbaar zijn (wat het geval is als de eerste twee opties niet gekozen worden), worden computeronderzoek en telefoontaps minder effectief. De politie zal dan andere manieren moeten gebruiken om verdachte communicatie en bewijsmateriaal te achterhalen. Hierbij valt bijvoorbeeld te denken aan direct afluisteren (artt. 126l en 126s Sv), infiltratie of kroongetuigen.

(In mijn proefschrift heb ik een vierde optie verdedigd, namelijk het beleid kiezen om niets aan het probleem te doen. Men kan er echter over twisten of deze optie onder het kopje 'oplossingen' valt.)

2.4 Wetgeving Nederland

Begin jaren '90 van de vorige eeuw, bij de discussie over het wetsvoorstel Computercriminaliteit, werd al onderkend dat de bevoegdheid onderzoek te doen in computers weinig zin had als de daarin opgeslagen gegevens versleuteld zijn. Daarom is bij de Wet computercriminaliteit de bevoegdheid ingevoerd om ontsleuteling te bevelen (art. 125k lid 2 Sv). Nederland is daarmee het eerste (en vooralsnog, voorzover ik weet, enige) land met dergelijke wetgeving. Het bevel mag niet aan de verdachte worden gegeven, een erkenning van het nemo-teneturbeginsel. In het wetsvoorstel Computercriminaliteit II wordt voorgesteld de bevoegdheid uit te breiden. (Zie nader hierover hfd. 3.)

Omdat het ontsleutelbevel aan niet-verdachten bepaald geen ultieme oplossing is voor het cryptoprobleem, heeft de Nederlandse overheid zich beraden op nadere mogelijkheden. In maart 1994 lekte een voorontwerp van wet uit, dat tot strekking had het bezit, gebruik of verhandelen van cryptografie te verbieden. Wie een "legitiem belang" had, kon een vergunning aanvragen, waarbij een van de voorwaarden was het beschikbaar stellen van informatie aan een beheerorgaan. Velen interpreteerden dit als een verplichting om cryptosleutels te deponeren bij het beheerorgaan. Een storm van protesten stak op, en het wetsontwerp werd fluks van tafel gehaald (waar het overigens nooit officieel op was gelegd). Sindsdien staat de Nederlandse regering op het standpunt dat het gebruik van cryptografie vrij is.[11]

Wel heeft de regering overwogen om het gebruik van BEDOT-cryptografie te stimuleren. Daarbij wordt vooral gekeken naar 'Trusted Third Parties' (TTP's), vertrouwde, onafhankelijke partijen die diensten aanbieden die de betrouw-

[11] TK 1997-1998, 25 880 (*Wetgeving voor de elektronische snelweg*), nrs. 1-2, p. 10.

baarheid van elektronische gegevensuitwisseling en gegevensopslag vergroten.[12] Hoewel die diensten (in elk geval in de praktijk) vrijwel alleen digitale handtekeningen faciliteren, denkt de regering dat het handig zou zijn als zij cryptografische privésleutels in beheer zouden houden. Voor digitale handtekeningen is dat niet nodig (integendeel, het is ongewenst), maar voor TTP's die diensten op het gebied van vertrouwelijkheid aanbieden, zou het een optie zijn. Voor zulke TTP's geldt dan de verplichting om de sleutels desgevraagd ter beschikking te stellen aan justitie; er geldt echter geen verplichting dat TTP's privésleutels in bewaring houden. Als evenwel de "partnerschapsbenadering" om met het bedrijfsleven tot een oplossing van het cryptoprobleem te komen, onvoldoende vruchten afwerpt, zou de regering alsnog kunnen overwegen om nadere regelgeving voor BEDOT-cryptografie in te voeren. [13]

2.5 Wetgeving buitenland

Hoewel er in veel landen stevig gediscussieerd en gewetsvoorsteld wordt over het cryptoprobleem, kennen maar weinig landen cryptowetgeving (uitgezonderd exportwetgeving, die los staat van het onderhavige probleem).[14] Hierin vallen vier stromingen te onderkennen.

1. Een verbod en vergunningstelsel op cryptografie. Rusland is het belangrijkste voorbeeld hiervan. Frankrijk had ook een restrictief vergunningstelsel voor cryptogebruik, maar schafte dit goeddeels af in januari 1999.
2. Het stimuleren of verplicht stellen van BEDOT-cryptografie. Diverse landen (vooral de VS en het VK) hebben hiertoe voorstellen gedaan, maar Frankrijk was het enige land dat daadwerkelijk BEDOT-wetgeving had (men kon een vergunning krijgen voor gebruik van sterke cryptografie mits men een sleutel deponeerde bij een sleutelbeheerorgaan). De betreffende wetgeving werd echter begin 1999 afgeschaft.
3. Het invoeren van een ontsleutelplicht. Nederland is vooralsnog het enige land met een wettelijk decryptiebevel, maar in steeds meer landen worden voorstellen gedaan een dergelijke bepaling in te voeren (bijvoorbeeld Australië, België, Canada, Finland, Frankrijk en het VK). Niet altijd wordt daarbij aangegeven of zo'n bevel aan verdachten mag worden gegeven.
4. Het strafbaarstellen of definiëren als strafverzwarende omstandigheid van cryptogebruik "ter bevordering of versluiering van een misdaad" (vaak in

---

12 Zie TTP-dossier 1998.

13 TK 1998-1999, 26 581 (*Nationaal TTP-project*), nr. 1, p. 21-24. Zie voor een kritische beschouwing Koops & De Jong 1998.

14 Zie voor een overzicht van cryptowetgeving in ruim vijftig landen, Koops 1999.

combinatie met het invoeren van een ontsleutelplicht). Dit is bijvoorbeeld voorgesteld in Australië en de VS.

2.6 Wenselijkheid van een ontsleutelplicht

Wie de mogelijke 'oplossingen' (zie par. 2.3) en de 'stromingen' in buitenlandse wetgeving (zie par. 2.5) bestudeert, kan concluderen dat er maar weinig mogelijkheden zijn om het cryptoprobleem aan te pakken, en dat er geen enkele optie is die echt een oplossing biedt. Het verbieden of aan vergunningen onderwerpen van cryptografie is uitgesloten. BEDOT-cryptografie is weinig effectief en onaantrekkelijk. Er valt dan ook een tendens te bespeuren van de BEDOT-rage die vooral van 1995 tot 1998 hoogtij vierde, in de richting van een ontsleutelplicht.[15]
Volgens mij is een decryptiebevel dan ook de enige optie waarvan je kunt zeggen dat die een 'oplossing' biedt voor de opsporingsproblemen veroorzaakt door cryptografie. De derde optie – alternatieve opsporingsmethoden – kan weliswaar aantrekkelijker zijn, maar deze verhelpt de problemen niet echt, omdat andere methoden andere soorten informatie opleveren (nog los van de risico's die met elk van deze methoden gemoeid zijn) en vaak voor andere doeleinden worden ingezet. Een richtmicrofoon of kroongetuige levert andersoortige informatie op dan een telefoontap of computeronderzoek.

Voor een directe aanpak van de problemen van cryptografie voor telefoontaps en computeronderzoek, is een ontsleutelplicht in feite de enige reële optie.[16] Bij gebrek aan BEDOT-mogelijkheden, is een decryptiebevel immers de enige manier om aan cryptosleutels te komen, en zonder toegang tot cryptosleutels krijgt de politie geen toegang tot (goed) versleutelde berichten.

Dit gegeven maakt de ontsleutelplicht uiterst wenselijk om in te voeren, en dat heeft de Nederlandse wetgever dan ook gedaan. Deze worstelt evenwel met de vraag of het decryptiebevel ook aan verdachten moet kunnen worden gegeven.

---

15 Ik beschouw de vierde stroming – het strafbaarstellen van cryptocrimineel gebruik – als heilloos, vanwege het instrumentele karakter, maar vooral omdat het een vicieuze cirkel introduceert: om te bewijzen dat iemand cryptografie gebruikt "om een misdaad te bevorderen of verhullen" zul je die misdaad moeten bewijzen, en dat kon nu juist niet vanwege de cryptografie! Ik laat dit als 'oplossing' buiten beschouwing, omdat het niets oplost.

16 Zo ook Kaspersen: "Het enige zinnige alternatief lijkt mij het opleggen van informatie-verplichtingen op alle bij de communicatie betrokken partijen: (…) te bevelen de inhoud van het geregistreerde verkeer (…) bekend te maken. Een dergelijk bevel zou ook aan de verdachte gegeven moeten kunnen worden." Kaspersen 1997, p. 410.

3. De huidige wettelijke status van de ontsleutelplicht

3.1 De ontsleutelplicht in Nederland

3.1.1 Computercriminaliteit I[17]

De Nederlandse wetgever realiseerde zich al in een – zeker internationaal gezien – vroeg stadium dat versleuteling problemen oplevert voor justitie. In de discussie over het wetsvoorstel Computercriminaliteit I stelde de vaste Commissie voor justitie in de Tweede Kamer voor om het wetsvoorstel "aan te vullen met een beperking in de trant van artikel 125 k [het bevel tot toegangsverschaffing tot een computer bij huiszoeking], waarbij een bevel tot decryptie gegeven kan worden."[18] Dit bevel zou niet aan de verdachte mogen worden gegeven. Bij tweede nota van wijziging nam de minister dit voorstel over. Aan het voorgestelde artikel 125k Sv werd een tweede lid toegevoegd, luidende:

> *2. Het eerste lid is van overeenkomstige toepassing indien in een geautomatiseerd werk versleutelde gegevens worden aangetroffen. Het bevel richt zich tot degeen van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de wijze van versleuteling van deze gegevens.*

De toelichting merkte hierbij op: "Met toegang tot een geautomatiseerd werk of een deel daarvan waarin niet-ontsluierbare gegevens zijn vastgelegd, is de waarheidsvinding immers niet gediend."[19] Het bevel zou overeenkomstig het voorgestelde artikel 125m Sv niet aan de verdachte mogen worden gericht. De

---

17 Eigenlijk heetten het wetsvoorstel en de wet 'Computercriminaliteit', maar nu een vervolg is verschenen, 'Computercriminaliteit II' genaamd, lijkt het raadzaam om de oorspronkelijke wet *ex post facto* te herdopen tot Computercriminaliteit I.

18 TK 1991-1992, 21 551, nr. 10, p. 12-13.

19 TK 1991-1992, 21 551, nr. 12, p. 3 en p. 6.

voorgestelde tekst werd aangenomen, en het ontsleutelbevel aan niet-verdachten was in Nederland per 1 maart 1993 een feit.[20]

Hoe de tekst moet worden gelezen, is overigens niet glashelder. Het eerste lid van artikel 125k Sv bepaalt:

> *1. Voor zover het belang van het onderzoek dit bepaaldelijk vordert, kan bij een doorzoeking[21] of bij toepassing van artikel 125j [een netwerkzoeking tijdens een doorzoeking] tot degeen van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de wijze van beveiliging van een geautomatiseerd werk, het bevel worden gericht toegang te verschaffen tot de aanwezige geautomatiseerde werken of delen daarvan. Degeen tot wie het bevel is gericht, dient desgevraagd hieraan gevolg te geven door de kennis omtrent de beveiliging ter beschikking te stellen.*

De 'overeenkomstige toepassing' suggereert dat een bevel kan worden gegeven tot het verschaffen van toegang tot versleutelde gegevens door de 'kennis omtrent' de versleuteling ter beschikking te stellen.[22] Ik neem aan dat de 'overeenkomst' betekent dat niet *fysieke* toegang tot de versleutelde gegevens wordt geboden (die is er immers al door het bevel van het eerste lid), maar *hermeneutische* toegang, dat wil zeggen tot de klare tekst. Het doel van het bevel is immers de klare tekst van de gegevens te achterhalen. Wat moet dan ter beschikking worden gesteld? De toelichting in de wetsgeschiedenis zegt hierover dat "de sleutel tot ontsluiering ter beschikking [moet] worden gesteld".[23] Volgens Kaspersen hoort daar ook het algoritme bij – wat naar zijn smaak onvoldoende wordt gedekt door de tekst.[24] Dat laatste zal volgens mij meestal niet nodig zijn – het gebruikte cryptoprogramma zal vaak op dezelfde harde schijf staan als de gegevens, zodat de politie het programma gewoon kan copiëren. Als de sleutel beveiligd is opgeslagen, zal de te verschaffen kennis (ook) het wachtwoord omvatten waarmee de sleutel is beveiligd.

Het bevel tot toegangsverschaffing uit het eerste lid kan echter op twee manieren worden opgevolgd: door zelf de toegang te verschaffen (lees: het wachtwoord in te tikken) of door ("desgevraagd") kennis ter beschikking te stellen (lees: het wachtwoord aan de politie te geven). Analoog hieraan zou de adressant van een decryptiebevel of zelf kunnen ontsleutelen, of de sleutel (met

---

20 Stb. 1993, 33 (Wet computercriminaliteit).

21 De oorspronkelijke term 'huiszoeking' is gewijzigd in 'doorzoeking' bij de Wet herziening van het gerechtelijk vooronderzoek, Stb. 1999, 243.

22 Dit is een incorrecte formulering, aangezien beoogd is om kennis omtrent *ont*sleuteling beschikbaar te stellen. Bij asymmetrische cryptografie is het een wereld van verschil of je kennis hebt van de openbare sleutel (de wijze van *ver*sleuteling) of van de privésleutel (de wijze van *ont*sleuteling). We zullen maar aannemen dat een teleologische interpretatie hier geoorloofd is.

23 TK 1991-1992, 21 551, nr. 12, p. 6.

24 Kaspersen 1993, p. 142.

wachtwoord) kunnen afgeven, maar dit wordt niet gedekt door de Memorie van Toelichting. Strikt genomen zou iemand dan ook alleen door het afgeven van de sleutel aan het bevel kunnen voldoen. Als toch de eerste mogelijkheid wordt toegestaan, zal de politie wel over de schouder willen meekijken om te controleren dat ook daadwerkelijk de cijfertekst ontsleuteld wordt, en niet een onschuldig tekstje ergens vandaan wordt getoverd.

Het ontsleutelbevel in de huidige vorm kent nogal wat beperkingen. Tot wie de politie het bevel kan richten, is geregeld in de zinsnede "degeen van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de wijze van versleuteling". Aan wie de wetgever daarbij heeft gedacht, is mij niet geheel duidelijk. Bij het eerste lid – toegang verschaffen tot een beveiligde computer – is expliciet gedacht aan de systeembeheerder of een gemeenschappelijke gebruiker van de computer. Dergelijke personen hebben echter meestal geen kennis van de versleuteling die iemand aanbrengt op zijn computer (die is immers juist bedoeld om anderen te verhinderen de gegevens te lezen!). Systeembeheerders kunnen toegang verschaffen tot computers, maar kennen zelden cryptosleutels van gebruikers. In de meeste gevallen zal alleen de verdachte de benodigde kennis hebben – en tot hem mag het bevel niet worden gericht.
Een andere complicatie is dat het bevel slechts kan worden gegeven 'bij een doorzoeking'. Dit suggereert dat de politie alleen *tijdens* de doorzoeking het bevel kan geven.[25] In de praktijk wordt meestal de volledige harde schijf gecopieerd en op het bureau onderzocht – dat is dan te laat om nog een ontsleutelbevel te kunnen geven.
Tot slot geldt nog de kanttekening dat de bevoegdheid van een decryptiebevel beperkt is tot situaties van een doorzoeking (ook de netzoeking van 125j Sv mag immers alleen tijdens een doorzoeking plaatsvinden). Er zijn echter meer situaties waarin de politie opgeslagen versleutelde gegevens kan aantreffen, zoals bij inbeslagneming van een schootcomputer buiten de huiszoeking – dat kan bijvoorbeeld bij aanhouden of staande houden (art. 95 Sv), bij ontdekking op heterdaad (art. 96 Sv), en tijdens een gvo (art. 104 Sv). In die gevallen biedt 125k Sv dus geen soelaas.

Al met al blijkt het ontsleutelbevel van art. 125k lid 2 Sv een innovatieve bevoegdheid, maar wel één die in de praktijk nauwelijks waarde heeft. De grootste belemmering zie ik in de beperking tot niet-verdachten.[26]

---

25 Anders Van Dijk & Keltjens 1995, p. 249.

26 Een interessante vraag lijkt mij overigens wel of een decryptiebevel mag worden gegeven aan een crypto-expert, met name aan een deskundige in het kraken van versleutelde boodschappen. Zo is er een Amerikaans bedrijf, AccessData, dat bedrijfsmatig versleutelde

3.1.2 Computercriminaliteit II

De Wet computercriminaliteit I is inmiddels bijna zeven jaar oud en aan actualisering toe. In januari 1998 circuleerde daartoe een concept-wetsvoorstel Computercriminaliteit II, dat ter consultatie aan diverse instanties en personen werd toegestuurd. Het duurde even voor alle kritiek verwerkt was en de Raad van State zich over het wetsvoorstel had gebogen. Het wetsvoorstel Computercriminaliteit II werd op 8 juli 1999 aan de Tweede Kamer aangeboden.[27] Een van de spannendste onderdelen hierin is de uitbreiding van de ontsleutelplicht.
Het wetsvoorstel stelt ten eerste voor om ook bij telecommunicatie een decryptiebevel te kunnen geven (voorgestelde artt. 126m en 126t leden 5-8 Sv). De verplichting tot ontsleuteling geldt alleen voorzover de geadresseerde daartoe in staat is; hij hoeft geen technische voorzieningen aanwezig te hebben om te kunnen ontsleutelen, en hoeft dus niet per se sleutels te bewaren (terwijl juist bij telecommunicatie vaak gebruik wordt gemaakt van eenmalige sessiesleutels, die na afloop van het gesprek of de fax worden weggegooid). Voor de vraagstelling van dit onderzoek maakt het overigens weinig verschil of het decryptiebevel slaat op opgeslagen of bij telecommunicatie onderschepte gegevens, al zal in het laatste geval de doeltreffendheid (nog) kleiner zijn.[28]
De (vermoedelijke) beperking van het bevel tot de doorzoeking zelf wordt opgeheven door de woorden 'bij een doorzoeking' te vervangen door 'bij of terstond na een doorzoeking'.[29] De woorden 'terstond na' sluiten aan bij de definitie van heterdaad (art. 128 Sv); de concrete duur hangt af van de omstandigheden van het geval, maar het gaat erom dat de opsporingsambtenaren "onverwijld overgaan tot het onderzoek van het bij een doorzoeking vergaarde materiaal en daarmee niet nodeloos wachten". (Mij lijkt dat laatste een rijkelijk ruimer begrip dan het 'terstond' van de heterdaad, maar dat terzijde.) De gevallen waarin versleutelde gegevens buiten een huiszoeking worden aangetroffen, blijven helaas buiten beeld in het wetsvoorstel.

---

bestanden kraakt (meestal voor wanhopige werknemers die de sleutel kwijt zijn). Men kan beargumenteren dat zo iemand voldoende "kennis draagt van de wijze van versleuteling" om hem op te dragen zijn kraakkunsten (en zijn supercomputers) los te laten op de gewraakte cijfertekst. De vraag is of dat via 125k Sv moet – maar bij meer onwillige burgers (denk aan de Electronic Frontier Foundation uit de VS, die een speciale DES-kraakcomputer heeft gebouwd) zou het misschien een aardige optie kunnen zijn?

27 Wijziging van het Wetboek van Strafrecht, het Wetboek van Strafvordering en de Telecommunicatiewet in verband met nieuwe ontwikkelingen in de informatietechnologie (computercriminaliteit II), TK 1998-1999, 26 671, nrs. 1-2.

28 Voor een kritische bespreking van dit voorstel, zie Koops & Schellekens 1999.

29 TK 1998-1999, 26 671, nr. 3, p. 50.

Wat het voorstel vooral interessant maakt, is dat het concept uit januari 1998 voorstelde om het bevel ook aan de verdachte te kunnen geven. De desbetreffende tekst van het artikel 125m lid 1 Sv zou komen te luiden:

> *Een bevel als bedoeld in artikel 125k kan slechts aan de verdachte worden gegeven indien uit feiten en omstandigheden blijkt van ernstige bezwaren tegen de verdachte en indien het onderzoek dringend noodzakelijk is voor het aan de dag brengen van de waarheid.*

Het bevel bij telecommunicatie in de voorgestelde artikelen 126m en 126t Sv kende een soortgelijke bepaling.[30]
Volgens de Memorie van Toelichting achtte de minister het onder omstandigheden gerechtvaardigd om een bevel tot de verdachte te richten. "Het blijkt namelijk in de praktijk dat het bij het toenemend gebruik door criminelen van informatietechnologie voor de politie soms zeer moeilijk, zo niet onmogelijk is om het overtuigend bewijs van het strafbaar feit te leveren, aangezien dit letterlijk ligt 'opgesloten' in een computer." De minister vond deze benadering "in overeenstemming met de eisen die uit art. 6 EVRM volgen." Er is immers "geen sprake van een verplichting om in eigen bewoordingen een oorspronkelijke weergave van bepaalde feiten of gebeurtenissen te geven".[31] Bij de voorwaarden – ernstige bezwaren en dringende noodzakelijkheid – sloot de minister aan bij de regeling voor DNA-onderzoek (art. 195d lid 3 Sv).

Het verrassende voorstel bleek al snel controversieel. De reacties in de consultatie en in de literatuur waren verdeeld, met een meerderheid tegen het voorstel. De minister kreeg steun van Buruma, die (overigens niet in directe reactie op het wetsontwerp) in zijn pre-advies voor de NJV-jaarvergadering van 1998 de regeling van artikel 125m Sv een "rijkelijk vergaande erkenning van het nemo teneturbeginsel" had genoemd.[32] Deze uitspraak leverde genoeg stof voor discussie op tijdens de jaarvergadering. Kuitenbrouwer bestempelde dit in zijn interventie als een "onaanvaardbare overschrijding (…) van de grens tussen passieve en actieve medewerking van de verdachte die de kern uitmaakt van het *nemo tenetur*beginsel."[33] Ook De Roos vond dat hier "een principiële grens overschreden [werd], namelijk die van passieve naar actieve medewerkingsverplichting voor de verdachte."[34]

---

30 *Computercriminaliteit II. Voorstel van wet en Memorie van Toelichting*. Concept, januari 1998.

31 *Ibid.*

32 Buruma 1998, p. 179.

33 NJV 1999, p. 36.

34 NJV 1999, p. 40. Zo ook Drion 1998, p. 1187. Ook Patijn, hoofd wetgevingszaken op het Ministerie van Justitie, deelde de kritiek (Klaver 1998). Kaspersen 1998 en Corstens 1998 onthielden zich van een oordeel in dezen, maar Kaspersen heeft eerder opgemerkt dat een

Buruma pareerde echter de aanval. Hij besefte uiteraard dat hij zich "op de rand van het nemo-teneturbeginsel" bewoog door te vinden dat een verdachte "verplicht kan worden gegevens omtrent die programma's of die passwords te verschaffen." Buruma achtte het evenwel "een rechtspolitieke vraag van interpretatie" – en in de (rechts)politieke keuze zou hij liever inbreuk maken op het nemo-teneturbeginsel dan dat de overheid zou kiezen voor een systeem van verplichte sleuteldeponering (waar Buruma kennelijk bang voor was). Oftewel, waar Kuitenbrouwer en De Roos vanuit het rechtssysteem keken en het voorgestelde ontsleutelbevel aan verdachten onaanvaardbaar achtten, vond Buruma veeleer dat er een politieke keuze gemaakt moet worden, waarbij het voorstel het voordeel van de twijfel kreeg.

Los van de discussie binnen de NJV, gaven nog enkele instanties hun mening over het wetsontwerp. De Nederlandse Orde van Advocaten was – weinig verrassend – faliekant tegen het voorstel. "Juist deze voorgestelde dwang tot [actief] meewerken maakt dat de grens van het uitoefenen van toelaatbare dwang wordt overschreden. Bovendien bestaat zelfs onder de huidige wet geen medewerkingsverplichting voor de verdachte tot het ontsleutelen van op schrift gestelde versleutelde informatie. Door introductie van een medewerkingsplicht van de verdachte wordt een kritische grens gepasseerd".[35] De Registratiekamer toonde zich vooralsnog niet overtuigd: "Anders dan het dronken rijden is het gebruik van encryptie op zichzelf niet gevaarzettend. Daarnaast is het maar de vraag of (…) met een ontsleutelingsverplichting voor de verdachte het daarmee beoogde resultaat kan worden bereikt."[36] Niettemin toonde de Registratiekamer zich wel gevoelig voor de justitiële druk om het cryptoprobleem op te lossen, en in dat kader gaf hij aan een ontsleutelingsplicht verreweg te prefereren boven een (BEDOT-)deponeringsplicht. Hoewel dat niet expliciet gezegd wordt, zou de Registratiekamer daarom mogelijk eerder kunnen instemmen met een ontsleutelingsbevel aan de verdachte dan met "verdergaande" maatregelen.[37]

Samenvattend concludeer ik dat het voorstel vooral kritiek kreeg van degenen die het op zichzelf beschouwden, met name omdat het de grens van passieve naar actieve medewerking van de verdachte zou overschrijden (De Roos, Kuitenbrouwer, Drion, NOVA), maar dat het acceptabeler was voor diegenen die het in de bredere context van het cryptoprobleem voor justitie plaatsten, met name wanneer het afgezet wordt tegen BEDOT-achtige maatregelen (Buruma, Kaspersen, mogelijk ook Registratiekamer).

"dergelijk bevel (…) ook aan de verdachte gegeven [zou] moeten kunnen worden." Kaspersen 1997, p. 410.

35 NOVA 1998.

36 Registratiekamer 1998a.

37 Registratiekamer 1998b.

De minister toonde zich evenwel gevoelig voor de kritiek. In het wetsvoorstel dat in juli 1999 aan de Tweede Kamer werd aangeboden, was de medewerkingsplicht voor de verdachte geschrapt. "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."[38] Het valt niet te verwachten dat de Tweede Kamer alsnog zal proberen de medewerkingsplicht voor de verdachte in te voeren, en daarmee lijkt voorlopig in Nederland een ontsleutelverplichting voor de verdachte van de baan.

3.2 De ontsleutelplicht in andere landen[39]

De discussie over het decryptiebevel aan verdachten wordt in meer landen gevoerd. Sinds een jaar of drie worden in allerlei landen suggesties gedaan een dergelijke bevoegdheid in te voeren, waarbij opvallend genoeg niet altijd aandacht wordt besteed aan de vraag of een ontsleutelplicht voor verdachten mogelijk inbreuk maakt op het nemo-teneturbeginsel. In deze paragraaf geef ik een overzicht van voorstellen in andere landen, waarbij ik waar mogelijk tekstvoorstellen citeer die inspiratie kunnen bieden voor een mogelijke Nederlandse regeling. Overigens heeft, ondanks de discussies, nog geen land daadwerkelijk een ontsleutelplicht ingevoerd.

In *België* stelden parlementsleden Bribosia en Maximus in juni 1996 voor om een vage Belgische BEDOT-wet af te schaffen en in plaats daarvan de onderzoeksrechter de bevoegdheid te geven "in uitzonderlijke gevallen, wanneer het onderzoek zulks vereist, voor het ontcijferen van een bericht de hulp [te] vorderen van ieder die daartoe in staat is", onder voorwaarden van subsidiariteit en proportionaliteit. Er werd geen uitzondering voor verdachten voorgesteld. Bij weigering zou de onderzoeksrechter de gedagvaarde kunnen dwingen – desnoods met lichamelijk geweld (!?) – om hulp te bieden bij ontsleuteling. Voorts zou een weigering gestraft kunnen worden met een gevangenisstraf van één tot vijf jaar en een geldboete van honderd tot vijfduizend frank. Omdat de gewraakte BEDOT-wet in december 1997 werd aangepast, is dit wetsvoorstel – voorzover ik weet – verder niet behandeld.
Canada publiceerde in oktober 1998 een cryptobeleid, waarin wetgeving werd voorgesteld die duidelijk zou maken dat bestaande huiszoekingsbevelen en medewerkingsverplichtingen ook van toepassing zijn op situaties waarin

38 TK 1998-1999, 26 671, nr. 3, p. 26.

39 De bronnen waarop deze paragraaf is gebaseerd, zijn toegankelijk via mijn *Crypto Law Survey*, Koops 1999. Ik zie hier af van expliciete vermelding van elk document.

versleuteling aan de orde is, zodat opsporingsambtenaren toegang zouden hebben tot materiaal of sleutels voor ontsleuteling. Hoe de wetgeving er precies uit zou zien, werd in het beleidsdocument niet geëxpliciteerd.
Ook het *Finse* cryptobeleid, zoals in oktober 1998 gepubliceerd, bevatte het voorstel om van dienstaanbieders medewerking te eisen bij ontsleuteling; een verdachte zou evenwel niet hoeven mee te werken aan ontsleuteling.
In *Ierland* stelde de regering in juni 1998 een raamwerk op voor cryptobeleid. Eén van de principes daarin is het voorstel om wetgeving in te voeren die cryptogebruikers verplicht om klare tekst over te dragen (mits die verifieerbaar hoort bij de cijfertekst) of algoritmes en sleutels af te geven. Een weigering zou worden bestraft met 'adequate' sancties. In een consultatiedocument uit augustus 1999 is dit principe echter verlaten; er wordt nog slechts een algemene bevoegdheid tot huiszoeking en inbeslagname van materiaal voorgesteld.

Na diverse eerdere beleidsvoorstellen en langdurige discussies, lanceerde de overheid van het *Verenigd Koninkrijk* in juli 1999 een ontwerp voor een *Electronic Communications Bill*, waarin onder andere wordt voorgesteld een ontsleutelbevel in te voeren. In een voorafgaand consultatiedocument uit maart 1999 constateerde het verantwoordelijke ministerie, het Department of Trade and Industry (DTI), dat de inbeslagnemingsbevoegdheid van artikel 20 Police and Criminal Evidence Act 1984 (PACE) impliceert dat een opsporingsambtenaar kan bevelen gegevens uit te leveren in zichtbare en leesbare vorm, hetgeen uitlevering van klare tekst suggereert. Dit betekent echter nog niet een bevoegdheid om sleuteluitlevering te vragen, terwijl ook bij versleutelde telecommunicatie geen bevoegdheid bestaat om ontsleuteling te bevelen. Daarom stelde de ontwerp-wet voor dat in gevallen waarin politie rechtmatig versleutelde gegevens in handen krijgen, deze een sleuteluitleveringsbevel kunnen geven aan degene die naar het lijkt in het bezit is van de sleutel. Voor een dergelijk bevel is een "written notice" nodig, en het mag niet gericht zijn op sleutels die bedoeld zijn om alleen elektronische handtekeningen te genereren en die niet daadwerkelijk voor andere doeleinden zijn gebruikt. De geadresseerde mag altijd zelf ontsleutelen in plaats van de sleutel af te geven, tenzij de bevelgever uitdrukkelijk stelt dat alleen sleuteluitlevering voldoet. Een weigering wordt strafbaar gesteld met maximaal twee jaar gevangenisstraf en/of een geldboete, tenzij de geadresseerde aantoont dat hij de sleutel niet bezat, maar wel alle informatie had gegeven aan de bevelgever die deze nodig heeft om in het bezit van de sleutel te komen, of als hij aantoont dat zulks niet redelijkerwijs uitvoerbaar voor hem was. Volgens de toelichting bij het eerdere consultatiedocument, gelooft de regering niet dat de voorstellen inbreuk maken op het nemo-teneturbeginsel. Het gaat immers om het begrijpelijk maken van bewijs dat al in handen is van de opsporingsinstanties, niet om een verdachte te

bevelen om bewijs te onthullen.[40] Vanwege de vele kritiek op dit voorstel, werd het uit dit wetsvoorstel gehaald met de bedoeling het terug te laten komen in een wetsvoorstel over onder andere de telefoontap, de *Regulation of Investigatory Powers bill*. Op het moment van schrijven is dit wetsvoorstel nog niet beschikbaar.

Naast deze voorstellen van overheden, hebben ook adviseurs en wetenschappers suggesties gedaan voor een ontsleutelbevel aan verdachten.[41] De twee belangrijkste voorstellen komen van Gerald Walsh, die een grondige studie van het cryptoprobleem en advies voor een Australisch cryptobeleid schreef, en de Deense wetenschappers Andersen en Landrock. Walsh geeft de overheid in overweging om de politie de bevoegdheid te geven om te bevelen informatie of materiaal uit te leveren waarmee inbeslaggenomen versleutelde gegevens begrijpelijk kunnen worden gemaakt. Volgens Walsh zou er voldoende steun zijn voor zo'n bevoegdheid, als er geen zicht op is dat een onafhankelijke autoriteit de sleutel zou kunnen achterhalen, en als er aanwijzingen zijn (circumstantial evidence) dat de versleutelde gegevens in relatie staan tot een ernstig strafbaar feit.[42]
Andersen en Landrock hebben in Denemarken voorgesteld om bij versleutelde gegevens die mogelijk bewijs verbergen, de bewijslast om te keren. De rechter zou dit kunnen doen als voldaan is aan drie voorwaarden: er zijn aanwijzingen (circumstantial evidence) dat iemand een strafbaar feit heeft gepleegd, het is waarschijnlijk (substantial likelihood) dat de verdachte versleutelde gegevens heeft die bewijs van zijn schuld kunnen leveren, en de verdachte is in staat te ontsleutelen maar weigert om dat te doen.[43]

Uit dit overzicht blijkt dat de discussie over een ontsleutelbevel aan verdachten in diverse landen wordt gevoerd. De vraag naar verenigbaarheid met het nemo-teneturbeginsel wordt daarbij niet altijd grondig beantwoord; soms komt deze helemaal niet aan de orde. Niettemin geven de diverse voorstellen voldoende bouwstenen om de problematiek te analyseren. Relevante aspecten zijn bijvoorbeeld welke voorwaarden gelden voor de bevoegdheid, met name welke mate van bewijs er moet zijn dat de cijfertekst verdacht is en dat de verdachte in staat is te ontsleutelen, of een verdachte zelf mag ontsleutelen of dat hij de sleutel moet afgeven, of sleutels voor digitale handtekeningen uitgeleverd mogen

---

40 DTI 1999, p. 30.

41 Opvallend genoeg besteedt het lijvige en gedegen rapport van de Amerikaanse National Research Council (NRC 1996) geen woord aan een mogelijk decryptiebevel aan verdachten; het concentreert zich voornamelijk op exportwetgeving en BEDOT-aspecten.

42 Walsh 1996, par. 1.2.29 en 3.7.11.

43 Andersen & Landrock 1996, p. 348.

worden, en welke sanctie er staat op niet-naleving van het bevel. In de Nederlandse discussie heeft vooral de vraag centraal gestaan of een bevel aan verdachten verenigbaar is met het nemo-teneturbeginsel, in zoverre er *actieve* medewerking van de verdachte wordt geëist. In het tweede deel van deze studie zal ik deze aspecten gebruiken voor de beantwoording van de onderzoeksvraag.

Deel II. Grenzen van de ontsleutelplicht voor verdachten

4. Het nemo-teneturbeginsel

4.1 Bestaat het nemo-teneturbeginsel?

Het lijkt misschien een domme vraag: bestaat er een nemo-teneturbeginsel? Verdachten kunnen immers niet worden gedwongen zelf hun hoofd in de strop van justitie te steken. Het adagium "Nemo tenetur prodere se ipsum"[44] (Niemand is gehouden zichzelf te belasten) lijkt een fundamenteel, zij het ongeschreven, uitgangspunt van onze strafrechtspleging.
Maar is het dat ook? Ansmink kwam in 1981 na een uitvoerige studie van de geschiedenis van nemo tenetur tot de conclusie dat er geen eenstemmigheid heerst over het gelden van het nemo-teneturprincipe voor ons strafproces. Aan de ene kant staan diverse ontkenningen van het bestaan van het beginsel:

- "de regel dat de verdachte niet – op straffe – verplicht kan worden mee te werken aan zijn eigen veroordeling [geldt] niet als een (ongeschreven) regel voor ons strafproces";[45]
- "In het Nederlandse recht is niet verankerd een onvoorwaardelijk recht of beginsel dat een verdachte op generlei wijze kan worden verplicht tot het verlenen van medewerking aan het verkrijgen van voor hem mogelijk bezwarend bewijsmateriaal", zoals de Hoge Raad sinds 1977 meermalen als een mantra heeft uitgesproken;[46]
- "een analyse van het Nederlandse procesrecht [levert] niet een beginsel tot niet meewerken met uitzonderingen [op] maar een beginsel van wel meewerken, met zekere restricties."[47]

Daartegenover staan vele meningen dat er wél een nemo-teneturbeginsel bestaat in het Nederlandse recht, zoals:

---

44 Alternatieve formulering zijn "Nemo tenetur edere contra se" (niemand is gehouden tegen zichzelf te getuigen) en "Nemo tenetur se accusare" (niemand is gehouden zichzelf te beschuldigen).

45 Ansmink 1981, p. 444.

46 HR 15 februari 1977, NJ 1977, 557. Zo ook recentelijk bijvoorbeeld HR 23 juni 1998, *Njb* 1998, p. 1363 en HR 22 juni 1999, NJ 1999, 648.

47 Van Veen 1979, p. 688.

- "de grondgedachte dat niemand gedwongen mag worden bewijsmateriaal tegen zichzelf te verschaffen en aan zijn eigen veroordeling mee te werken";[48]
- "dat de verdachte dan op straffe zou worden verplicht tot zijn eigen veroordeling mee te werken, hetgeen met de geest van het nieuwe Wetboek van Strafvordering kwalijk zou stroken" (de Hoge Raad in 1928);[49]
- "Inmiddels zijn er zo veel uitzonderingen, dat met recht de vraag is opgeworpen of het door de Hoge Raad ontwaarde beginsel nog wel geldt, en de verdachte niet veeleer, behoudens uitzonderingen, tot medewerking *verplicht* is. Een ontkennend antwoord lijkt mij – omdat ik hecht aan de mollenvangersdoctrine – nog altijd het juiste, maar dat inmiddels vooral op historische gronden";[50]
- "Maar wel kan het bestaan van een beginsel worden aangenomen, dat niemand gedwongen mag worden zichzelf in het strafrechtelijk onderzoek te bezwaren, tenzij de *wet* daarop een uitzondering maakt."[51]

Het Europees Verdrag voor de Rechten van de Mens noemt nemo tenetur niet expliciet, maar het Europees Hof heeft het beginsel ingelezen in artikel 6 lid 1 EVRM:

> *There can be no doubt that the right to remain silent under police questioning and the privilege against self-incrimination are generally recognised international standards which lie at the heart of the notion of a fair procedure under Article 6 (…). By providing the accused with protection against improper compulsion by the authorities these immunities contribute to avoiding miscarriages of justice and to securing the aims of Article 6.*[52]

De strekking van het beginsel heeft het Hof in de arresten *Funke*, *Murray* en *Saunders* nader bepaald.[53]

4.1.1 Funke[54]

De Duitse vertegenwoordiger Funke, woonachtig te Frankrijk, werd verdacht van overtreding van de regels voor financiële transacties met het buitenland.

---

48 Myjer 1978, p. 22.
49 HR 16 januari 1928, NJ 1928, p. 233 (*Mollenvanger*).
50 Reijntjes 1996b, p. 11.
51 De Roos 1990, p. 117.
52 EHRM 8 februari 1996, NJ 1996, 725 m.nt. Kn. (*Murray*).
53 Zie Rozemond 1998, p. 314-330, voor een uitvoeriger beschrijving en analyse van deze zaken.
54 EHRM 25 februari 1993, NJ 1993, 485 m.nt. Kn. (*Funke*).

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. Hoger beroep en cassatie waren vergeefs voor Funke. Het Europees Hof concludeerde echter dat artikel 6 lid 1 EVRM 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 Art. 6, to remain silent and not to contribute to incriminating himself.*

Een van de kernpunten van dit arrest is het feit dat de douane niet zeker wist dat Funke de gevraagde documenten in zijn bezit had ("they were not certain of the fact"). Een uitleveringsbevel waarvan niet-naleving gesanctioneerd is, is alleen rechtvaardig als men zeker weet dat de geadresseerde eraan kan voldoen.[55]

4.1.2 Murray[56]

L. werd door de IRA gegijzeld op verdenking een informant van de politie te zijn. Bij de inval in het huis waar L. gevangen werd gehouden, kwam John Murray de trap aflopen; hij had zojuist tegen L. gezegd, die Murray zonder blinddoek herkende, dat er politie was en dat hij beneden TV moest gaan kijken. Bij het verhoor werd Murray herhaaldelijk gewezen op een bepaling uit de Prevention of Terrorism Act 1989, op grond waarvan het nalaten ontlastende feiten te vermelden als een ondersteuning van het bewijsmateriaal kan worden gebruikt. Murray antwoordde steeds dat hij niets te zeggen had. Zijn weigering uit te leggen waarom hij zich bevond in het huis waar L. werd vastgehouden, werd vervolgens door de rechter gebruikt als ondersteunend bewijs dat hij schuldig was; volgens de wet kon de rechter met zo'n weigering rekening houden in de mate waarin hij dat behoorlijk acht.
Het Europees Hof overwoog dat het zwijgrecht en het nemo-teneturbeginsel bij de kern liggen van het recht op een eerlijk proces, maar dat deze immuniteiten niet absoluut zijn:

---

55 Koops 1998, p. 175; Rozemond 1998, p. 316; Hieltjes 1998, p. 98; Jörg 1998, p. 73.
56 EHRM 8 februari 1996, NJ 1996, 725 m.nt. Kn. (*Murray*).

> *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.*

In casu vond het Hof dat er geen onbehoorlijke druk was uitgeoefend, omdat Murray zijn zwijgen had weten te bewaren. Het proces werd niet gevoerd voor een jury, maar voor een ervaren rechter, en de regeling van bewijsgebruik was omkleed 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, "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" – dat is in feite voldoende bewijs voor veroordeling[57];
3. de rechter heeft een discretionaire bevoegdheid om aan het zwijgen al dan niet conclusies te verbinden, en deze beslissing is onderworpen aan herziening door de appelrechter;
4. de rechter moet het gebruik van zwijgen en het gewicht dat hij daaraan toekent motiveren.

Onder de omstandigheden was het gebruik van Murrays zwijgen niet in strijd met zijn recht op een eerlijk proces: aan de voorwaarden was voldaan in de regeling en bij het gebruik van zijn zwijgen door de rechter. Er was immers een "formidable case" tegen de verdachte waarin de omstandigheden om een verklaring van de verdachte "riepen"; met gezond verstand kon men daaruit concluderen dat er geen ontlastende verklaring was en dat de verdachte schuldig was.

Wel was er sprake van een oneerlijk proces omdat Murray geen toegang had gehad tot een raadsman in het beginstadium van politieverhoor, juist omdat in dat stadium de verdachte moest kiezen tussen zwijgen, waaraan conclusies kunnen worden verbonden, en spreken, hetgeen zijn mogelijkheden voor verdediging kon beïnvloeden.

4.1.3 Saunders[58]

De hoofddirecteur van drank- en voedingsmiddelenconcern Guinness wordt gehoord in een serie hoorgesprekken in het kader van een administratief onderzoek naar mogelijke beursfraude. Hij is verplicht mee te werken aan het

57 Jörg 1998, p. 181.

58 EHRM 17 december 1996, NJ 1997, 699 m.nt. Kn. (*Saunders*).

onderzoek op grond van de Companies Act 1985, en hij voert in de loop van zes maanden negen gesprekken. Halverwege deze periode wordt Saunders beschouwd als verdachte in een strafrechtelijk onderzoek naar de zaak. In een mini-proces over de vraag of de processen-verbaal van de gesprekken met Saunders als bewijs tegen hem mochten worden gebruikt, oordeelt de rechter, op grond van de Police and Criminal Evidence Act 1984, dat de gesprekken vóór de verdenking toelaatbaar zijn als bewijs (de Companies Act bepaalt onder meer dat bij een onderzoek elk antwoord als bewijs kan worden gebruikt tegen de ondervraagde). De PACE laat het gebruik van bekentenissen toe, tenzij aangevoerd wordt dat de bekentenis is verkregen als gevolg van een optreden dat de bekentenis onder de gegeven omstandigheden onbetrouwbaar maakt. In de hoofdzaak worden de verklaringen ter zitting aan de jury voorgelezen, om tegenstrijdigheid aan te tonen met Saunders' verklaring dat hij onschuldig is. Hij werd schuldig bevonden en tot vijf jaar veroordeeld.

Het Europees Hof merkt op dat het in deze zaak alleen gaat om het *gebruik* van de verklaringen in de strafzaak, niet om het afdwingen van de verklaringen als zodanig. Het Hof geeft vervolgens een uitleg van het nemo-teneturbeginsel: dat

> *is primarily concerned, however, with respecting the will of an accused to remain silent. (…) it 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.*

Dan stelt het Hof vast dat de verklaringen in de administratieve fase onder dwang zijn afgelegd, omdat weigeren te antwoorden strafbaar was met twee jaar gevangenisstraf en de betrokkene zich niet kon beroepen op een zwijgrecht bij belastende verklaringen. De verklaringen in casu waren ook belastend, omdat zij toegaven 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 het Openbaar Ministerie voor de jury, hetgeen een extra druk op de verdachte legde tijdens de rechtszitting om een verklaring af te leggen en zich niet op zijn zwijgrecht te beroepen. De niet-deskundige jury kreeg immers allicht een uiterst negatieve indruk van Saunders door de manier waarop de verklaringen werden voorgelezen. 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.*

Op grond hiervan concludeerde het Hof dat het recht zichzelf niet te hoeven beschuldigen geschonden was.

Met deze drie zaken heeft het Europees Hof enig houvast gegeven om het nemo-teneturbeginsel uit te leggen; wel moet men zich realiseren dat de uitspraken van het Hof sterk casuïstisch zijn.

Verder is in enkele internationale verdragen het nemo-teneturbeginsel expliciet vastgelegd. Artikel 14 lid 3 onder g IVBPR zegt dat eenieder die wordt vervolgd het recht heeft om "niet te worden gedwongen tegen zichzelf te getuigen of een bekentenis af te leggen". Het Statuut van het Joegoslavië-Tribunaal heeft dit overgenomen: de verdachte heeft het recht "not to be compelled to testify against himself or to confess guilt" (art. 21 lid 4 sub g ICTYS). Hetzelfde zegt het Statuut van het Rwanda-Tribunaal (art. 20 lid 4 sub g ICTRS). Ook het recente Statuut van het Internationaal Strafhof (Rome Statute of the International Criminal Court, 17 juli 1998) bepaalt dat bij een onderzoek in het kader van het statuut, een persoon "shall not be compelled to incriminate himself or herself or to confess guilt" (art. 55 lid 1 onder a ICCS) (een ruimere formulering dan die van de ad-hoc tribunalen).

Het nemo-teneturbeginsel bestaat dus wel degelijk. Maar er is veel discussie over de vraag welke juridische status het heeft (is het een beginsel, een geloofsartikel,[59] een matigende instructienorm of een "gedramatiseerde fictieve werkelijkheid"[60]?), wat de juiste formulering en dus wat de reikwijdte is, en wat de ratio ervan is. In dit hoofdstuk geef ik een overzicht van de meningen over deze vragen, om tot een definitie te komen van het nemo-teneturbeginsel waaraan de ontsleutelplicht kan worden getoetst. Ik besteed juist uitvoerig aandacht aan deze kwestie, omdat de definitie van nemo tenetur cruciaal is voor de vraag of een wettelijk decryptiebevel daarop inbreuk maakt en of deze inbreuk gerechtvaardigd is. In dit hoofdstuk werk ik toe naar een definitie van het beginsel, die ik pas aan het eind kan geven. Voor die tijd ben ik dus gedwongen een voorlopige omschrijving te hanteren: het beginsel dat een verdachte niet kan worden gedwongen mee te werken aan zijn eigen veroordeling.

---

59 De Roos 1990, p. 117.

60 Hulsman, geciteerd in Baauw 1979, p. 469.

De vraag naar bestaan en strekking van nemo tenetur beantwoord ik als volgt. Eerst kijk ik welke nemo-teneturaspecten uit het systeem van de Nederlandse wet zijn af te leiden (par. 4.2). Vervolgens analyseer ik de reikwijdte van nemo tenetur aan de hand van de vragen: wat, wanneer, wie en hoe (par. 4.3). Voor een definitief antwoord op deze vragen, zal ook de waarom-vraag relevant blijken (par. 4.4). Ten slotte kan ik een definitie geven van het beginsel (par. 4.5). Aansluitend bekijk ik of een ontsleutelingsplicht voor verdachten inbreuk maakt op dit beginsel (par. 4.6).

4.2 Het systeem van de Nederlandse wet

In de Nederlandse wetgeving is het nemo-teneturbeginsel niet expliciet verwoord. Maar wie het Wetboek van Strafvordering erop naslaat, komt diverse bepalingen tegen die een uitdrukking (kunnen) zijn van de nemo-tenetur-gedachte. Zo bepaalt art. 96a lid 2 Sv dat een bevel tot uitlevering van voor inbeslagneming vatbare voorwerpen niet aan de verdachte wordt gegeven. Evenzo stelt artikel 125m lid 1 Sv dat het bevel tot 'uitlevering' van gegevens, het bevel tot toegangsverschaffing tot een beveiligde computer en het bevel tot ontsleuteling niet aan de verdachte mogen worden gegeven. Iemand hoeft de aangifteplicht voor bepaalde misdrijven niet na te komen als hij door aangifte gevaar loopt zelf te worden vervolgd (art. 160 lid 2 Sv, art. 162 lid 3 Sv), terwijl hij het ook niet hoeft te melden als hij weet dat een zeker misdrijf wordt beraamd, als daardoor gevaar zou ontstaan van een strafvervolging tegen hemzelf (art. 137 Sr). Ook is de verdachte niet tot antwoorden verplicht (art. 29 lid 1 Sv).[61]

De enige uitzondering in Sv is artikel 551 (uitlevering bij een aantal delicten), maar dit strekt alleen tot verbeurdverklaring of onttrekking aan het verkeer, niet tot waarheidsvinding (zie par. 5.2.2). Daarmee is dit geen zuivere uitzondering ten opzichte van de genoemde artikelen. Volgens het Wetboek van Strafvordering kan een verdachte derhalve niet worden gedwongen om iets te doen waarbij hij zichzelf mogelijk zou belasten.

Maar hij moet wel veel dulden. Een verdachte moet toestaan dat opsporingsambtenaren hem onderzoeken aan lichaam en kleding (artt. 56, 195 Sv) en voorwerpen inbeslagnemen die hij bij zich voert (art. 95 lid 1 Sv). Hij moet toestaan dat foto's, vingerafdrukken en lichaamsmaten worden genomen (art. 61a Sv) en dat bloed wordt afgenomen voor een DNA-test (art. 195d Sv). Als de

61 Volgens Ansmink is dit evenwel geen uitdrukking van het nemo-teneturbeginsel, maar een zelfstandig recht van de verdachte dat voortgekomen is uit de afschaffing van marteling om een bekentenis af te dwingen. Ansmink 1981, p. 437.

verdachte zich hiertegen verzet, maakt hij zich schuldig aan wederspannigheid (art. 180 Sr, maximaal drie maanden gevangenisstraf).
Het systeem van het Wetboek van Strafvordering suggereert dus dat een verdachte niet kan worden gedwongen om actief mee te werken aan zaken waarbij hij zichzelf zou kunnen beschuldigen, maar dat hij wel passief acties moet dulden die tot zijn veroordeling kunnen bijdragen.

Dit beeld wordt echter genuanceerd in de bijzondere wetgeving. Verdachten kunnen wel degelijk worden gedwongen tot actieve medewerking. Men moet vuurwapens uitleveren, inzage geven in bescheiden, en "alle medewerking verlenen die redelijkerwijs nodig is" (zie par. 5.2.1 en 5.2.2). Het bijzondere is dat de opsporingsbevoegdheden die bijzondere opsporingsambtenaren hebben voor hun controle-activiteiten, ook mogen worden uitgeoefend voor de opsporing als de ambtenaar opsporingsbevoegdheid heeft. De Hoge Raad is van mening "dat het bestaan van een redelijke verdenking dat een bepaalde persoon een strafbaar feit heeft begaan niet in de weg staat aan het uitoefenen van evenbedoelde controlebevoegdheid tegenover die verdachte of tegenover een derde, mits daarbij de aan de verdachte als zodanig toekomende waarborgen in acht worden genomen" (zoals de cautie).[62] De bescherming die de verdachte in het Wetboek van Strafvordering geniet, kan in deze gevallen dus worden overstemd.[63] Als een verdachte weigert te voldoen aan een bevel tot medewerking, is hij strafbaar volgens art. 184 Sr (maximaal drie maanden gevangenisstraf).

Voorzover er een systeem in de wet zit (logisch gezien kan men daaraan twijfelen, maar juridisch gezien is dat het geval), luidt dit dus als volgt: in het commune strafrecht hoeven verdachten niet actief mee te werken aan hun veroordeling, maar moeten zij wel passief bewijs opleverende activiteiten dulden; in het bijzondere strafrecht kunnen zij wel regelmatig worden gedwongen materiaal af te staan dat mee kan werken aan het bewijs. Verdachten worden echter bijna nooit gedwongen tot het afleggen van een verklaring (zie verder par. 5.2.1).

4.3 De reikwijdte van nemo tenetur

Voor ik een definitie geef van het nemo-teneturbeginsel, wil ik kijken naar vier aspecten die de werking van het beginsel afgrenzen. Deze aspecten kunnen

62 HR 26 april 1988, NJ 1989, 390 (*Controle en opsporing*).

63 Hetgeen niet betekent dat de resultaten zonder meer voor het bewijs mogen worden gebruikt, hoewel de Hoge Raad dat wel lijkt te suggereren. Zie *Saunders*.

vervolgens worden verwerkt in de definitie. In deze paragraaf analyseer ik of het beginsel geldt:

- voor materiaal dat onafhankelijk van de wil van de verdachte bestaat (wat);
- in het stadium van een strafrechtelijke aanklacht of ook in de stadia daarvoor (wanneer);
- voor natuurlijke personen of ook voor rechtspersonen (wie);
- voor actieve of ook voor passieve medewerking (hoe).

Bij de bespreking van deze vragen zal blijken dat vooral ook de waarom-vraag van belang is. Ik analyseer daarom de ratio van nemo tenetur in par. 4.4, waarna ik een definitieve definitie kan geven van het beginsel.

Van de "vijf w-vragen" blijft alleen nog over de "waar-vraag", oftewel in welk rechtsgebied het beginsel geldt. Mogelijk is de reikwijdte van nemo tenetur breder dan ik hier schets, omdat het ook in het privaatrecht en het bestuursrecht gelding kan hebben. Vanwege de probleemstelling van dit onderzoek beperk ik me echter tot nemo tenetur in strafzaken.

4.3.1 Onafhankelijk materiaal, de wil van de verdachte en het zwijgrecht

Bij het verschijnen van het arrest *Saunders*, leek het nemo-teneturbeginsel een stuk duidelijker te zijn geworden. Materiaal dat onafhankelijk van de wil van de verdachte bestaat wordt in het arrest in duidelijke termen uitgesloten van bescherming van nemo tenetur:

> *The right not to incriminate oneself (…) 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.*

Het Hof ziet als vooronderstelling van nemo tenetur dat de politie geen dwangmiddelen gebruikt tegen de (verklarings)wil van de verdachte in. "The right not to incriminate oneself is primarily concerned (…) with respecting the will of an accused person to remain silent." Daarmee wordt het beginsel bijna gelijk gesteld met het zwijgrecht, zoals Knigge in zijn noot vaststelt: "Dat zou betekenen dat aan het recht nauwelijks nog zelfstandige betekenis toekomt naast het zwijgrecht."

De Hoge Raad ziet eveneens het nemo-teneturbeginsel in het licht van de aan art. 29 Sv ten grondslag liggende verklaringsvrijheid,[64] terwijl ook in de literatuur beide rechten wel op één hoop worden gegooid.[65]

---

64 Aldus Schalken in zijn noot bij HR 29 oktober 1996, NJ 1997, 232, aantekening 2.

65 T&C Sv 1997, aant. 1 bij art. 29 Sv.

Men kan zich afvragen waarom we dan nog blijven spreken van twee verschillende rechten. Wat is het bestaansrecht van nemo tenetur *naast* het zwijgrecht? Martens merkt in zijn afwijkende mening bij *Saunders* op dat het Hof hier de twee rechten lijkt te vereenzelvigen, terwijl het in *Murray* en *Funke* wel degelijk twee verschillende immuniteiten had onderscheiden. Martens vindt het belangrijk om het onderscheid te blijven maken, omdat het nemo-teneturbeginsel het zwijgrecht weliswaar omvat, maar breder is dan dat. Het vereenzelvigen van nemo tenetur met het beperktere zwijgrecht perkt dus *de facto* de bescherming van verdachten in. Het arrest *Saunders* lijkt hem in twee opzichten te absoluut: nemo tenetur geldt nooit voor materiaal dat onafhankelijk van de wil van de verdachte bestaat, en voor verklaringen geldt het altijd. Martens ziet, zo lees ik zijn mening, liever een genuanceerde benadering, waarbij het nemo-teneturbeginsel in brede zin wordt gelezen (het gaat zowel om verklaringen als om 'onafhankelijk materiaal'), maar waarbij ook plaats is voor een belangenafweging: onder omstandigheden moet het mogelijk zijn inbreuk te maken op het beginsel. Het Hof lijkt voor zo'n afweging de deur dichtgegooid te hebben.[66]
Martens merkt terecht op dat het strikte standpunt van het Hof niet in overeenstemming is met de ratio die het Hof in hetzelfde arrest lijkt aan te dragen voor nemo tenetur. Aan de wil van de verdachte, waar het Hof zo'n nadruk op legt, wordt immers even veel afbreuk gedaan door gedwongen verklaringen als door gedwongen uitlevering van 'onafhankelijk materiaal'. Om te beoordelen of het Hof terecht onafhankelijk materiaal uitsluit van de reikwijdte van nemo tenetur, moet men daarom eerst de ratio van het beginsel bestuderen. Dit zal ik doen na het behandelen van de wanneer-, wie- en hoe-vragen.

4.3.2 Controle, opsporing, verdenking, vervolging en bewijs

Het tweede aspect van de reikwijdte van nemo tenetur betreft de wanneer-vraag. Strafvordering kan worden ingedeeld in de (deels overlappende) fasen: opsporing, verdenking, 'criminal charge', vervolging, berechting en tenuitvoerlegging. Los van strafvordering, maar in bepaalde gevallen daaraan voorafgaand, is de fase van controle: het preventief controleren op naleving van wetten door bijzondere controleambtenaren.
Nu spreken de gebruikelijke formuleringen van nemo tenetur, waaronder die van de Hoge Raad (zie par. 4.1), over een "verdachte", hetgeen suggereert dat het beginsel niet geldt in de fasen voorafgaand aan verdenking. Bij controle en

66 Martens 1996. Ook Ansmink is na bestudering van de geschiedenis van nemo tenetur en het zwijgrecht tot de conclusie gekomen dat beide rechten niet vereenzelvigd kunnen worden; sterker nog, het zijn rechten die zich redelijk autonoom hebben ontwikkeld. Ansmink 1981, p. 437 en 447.

bij opsporingsonderzoek waarbij nog geen sprake is van een verdenking, zou dan medewerking kunnen worden afgedwongen.
Het Europees Hof formuleerde het beginsel aldus:

> *the right of anyone 'charged with a criminal offence', within the autonomous meaning of this expression in Art. 6 (…) not to contribute to incriminating himself.*[67]

Hier gaat het dus om een 'criminal charge' (hierna: strafrechtelijke aanklacht), zoals het EHRM dit begrip interpreteert,[68] en niet zozeer om een verdenking. In het algemeen is de fase van een strafrechtelijke aanklacht beperkter en later dan de fase waarin er een verdachte is – tegen de verdachte hoeft immers niet noodzakelijk een vervolging te worden ingesteld. In de interpretatie van het Europees Hof begint de fase van een 'criminal charge' als iemand (meestal een verdachte) uit handelingen van de overheid in redelijkheid kan afleiden dat tegen hem een strafrechtelijke vervolging is of zal worden ingesteld.
Het lijkt mij zinvol om uit te gaan van de definitie van het Europees Hof. Het beginsel ziet immers op het gebruik van eventueel resulterend bewijsmateriaal in een strafzaak tegen de verdachte. In het geval een verdachte gedwongen wordt tot medewerking, maar noch de resultaten van deze medewerking noch andere omstandigheden tot een vervolging leiden, dan lijkt er geen sprake te zijn van inbreuk op het beginsel dat een verdachte niet aan zijn eigen veroordeling hoeft mee te werken. Er is immers geen mogelijkheid dat hij wordt veroordeeld.
Derhalve geldt nemo tenetur vanaf de fase van een strafrechtelijke aanklacht. In de fasen die daaraan voorafgaan, zoals controle, opsporing en verdenking waarbij nog geen sprake is van een strafrechtelijke aanklacht, kan dus medewerking worden afgedwongen van betrokkenen (en alleen van een verdachte voorzover er nog geen sprake is van strafrechtelijke aanklacht). Dat betekent evenwel niet dat de resultaten van die medewerking zomaar mogen worden gebruikt voor het bewijs als het later alsnog tot vervolging komt. In dat opzicht werpt het beginsel als het ware zijn schaduw vooruit. Zoals het Europees Hof in *Saunders* heeft bepaald, geldt het beginsel niet als er geen sprake is van een strafrechtelijke aanklacht, maar mogen eventuele resultaten niet worden gebruikt voor het bewijs als dat in strijd is met het recht op een eerlijk proces van artikel 6 lid 1 EVRM.[69] Dit geldt ook voor bewijs dat verkregen wordt als rechtstreeks gevolg van de gedwongen medewerking,

---

67 EHRM 25 februari 1993, NJ 1993, 485 (*Funke*).

68 De "autonome betekenis" wil zeggen dat het EHRM zelf bepaalt of een handeling van de overheid een strafrechtelijke aanklacht is. Het EHRM kijkt dus niet naar de eventuele kwalificatie van de overheid zelf, die bijvoorbeeld rechtswaarborgen voor verdachten zou kunnen willen ontlopen door bepaalde handelingen in administratieve in plaats van strafrechtelijke procedures onder te brengen.

69 EHRM 17 december 1996, NJ 1997, 699 (*Saunders*), par. 69.

volgens de leer van de "verboden vruchten": als de boom is vergiftigd, mogen de vruchten niet worden geplukt.
Dit heeft overigens tot gevolg dat de vraag wannéér die medewerking precies heeft plaatsgevonden, niet per se overwegende betekenis heeft voor het gebruik van bewijsmateriaal verkregen door gedwongen medewerking. De fase heeft wel consequenties voor de rechtmatigheid van de dwang als zodanig (in de fase voor een strafrechtelijke aanklacht is dwang geoorloofd, daarna niet, als de dwang in strijd is met nemo tenetur), maar niet altijd voor het gebruik van bewijs: in beide gevallen mag het materiaal niet worden gebruikt als dit gebruik strijdig is met het recht op een eerlijk proces.
De argumentatie van de Hoge Raad in zijn arrest van 29 oktober 1996 kan na *Saunders* dan ook niet worden volgehouden. In dit arrest betoogde de Hoge Raad dat het gebruik voor het bewijs van uitgeleverde bescheiden rechtmatig was, *omdat* er ten tijde van het bevel tot uitlevering nog geen sprake was van een 'criminal charge'.[70] Blijkens *Saunders* is dat als zodanig niet een beslissend argument voor de rechtmatigheid van het bewijs. Het gaat ook om het *gebruik* van het bewijs en de mate van dwang die dat uitoefent op de verdachte ter zitting. Na *Saunders* heeft de Hoge Raad dan ook zijn argumentatie aangepast: het gebruik van bescheiden, verkregen door een bevel tot uitlevering toen er nog geen 'criminal charge' was, voor het bewijs is rechtmatig, omdat het gaat om materiaal dat onafhankelijk van de wil van de verdachte bestaat, zoals het EHRM dat in Saunders heeft gezegd.[71]
Samenvattend: het nemo-teneturbeginsel geldt alleen vanaf de fase van een strafrechtelijke aanklacht. Als er (nog) geen sprake is van een strafrechtelijke aanklacht, is gedwongen medewerking geoorloofd. Het nemo-teneturbeginsel kan echter onder bepaalde omstandigheden wel het gebruik voor het bewijs van de resultaten daarvan verhinderen als het alsnog komt tot een vervolging.

4.3.3 Natuurlijke en rechtspersonen en soort delicten

Geldt nemo tenetur ook voor rechtspersonen? Ik stel bij de beantwoording van deze vraag voorop dat het hierbij uiteindelijk ook om natuurlijke personen zal gaan: *als* rechtspersonen recht hebben op het nemo-teneturbeginsel, dan kunnen natuurlijke personen die onderdeel zijn van die rechtspersoon zich beroepen op een daarvan afgeleid recht om niet mee te werken.[72] De bevolen medewerking

---

70 HR 29 oktober 1996, NJ 1997, 232 m.nt. Sch.
71 HR 21 oktober 1997, NJ 1998, 173.
72 Vgl. Hartmann & De Meijer 1997, die betogen dat het zwijgrecht moet gelden voor die werknemers van een verdachte rechtspersoon, die vallen binnen het kader van de wijze waarop de strafrechtelijke aansprakelijkheid van de betrokken rechtspersoon wordt geconstitueerd.

zal immers altijd door natuurlijke personen moeten worden uitgeoefend – een bevel aan de rechtspersoon als zodanig zal weinig uithalen. Maar de vraag of natuurlijke personen die onderdeel zijn van een rechtspersoon zich op een afgeleid recht om niet mee te hoeven werken aan de veroordeling van de rechtspersoon, staat los van de vraag of zij zich op een zelfstandig recht kunnen beroepen, als zij zelf worden vervolgd. In deze paragraaf gaat het uitsluitend om de vraag of de bescherming van nemo tenetur toekomt aan rechtspersonen die blootstaan aan vervolging.

Uit de jurisprudentie blijkt dat rechtspersonen in beginsel recht hebben op dezelfde waarborgen voor een eerlijk proces als natuurlijke personen. De Hoge Raad heeft uitgesproken dat

> *de in art. 6 EVRM neergelegde waarborgen niet alleen voor natuurlijke personen maar ook voor rechtspersonen als de onderhavige hebben te gelden.*[73]

Ook bij de opname van een aantal grondrechten in de Grondwet 1983 is gesteld dat:

> *de voorgestelde bepalingen beogen ook aan rechtspersonen en aan groepen en aan organisaties zonder rechtspersoonlijkheid rechten en aanspraken te verlenen voor zover dat naar de aard van het betreffende grondrecht zin kan hebben.*[74]

Hoewel in het algemeen rechtspersonen zich dus kunnen beroepen op grondrechten, is het niet vanzelfsprekend dat ook het nemo-teneturbeginsel daaronder valt. Het Europees Hof van Justitie heeft in de zaak *Orkem* bepaald dat een rechtspersoon niet kan worden verplicht antwoorden te geven, waardoor zij het bestaan van de inbreuk [op het mededingingsrecht] zou moeten erkennen, die de Europese Commissie heeft te bewijzen. Dit suggereert welis-waar iets nemo-teneturachtigs, maar in hetzelfde arrest overwoog het Hof dat

> *aangenomen dat een onderneming waartegen een onderzoek op het gebied van het mededingingsrecht is ingesteld, zich op [art. 6 EVRM] kan beroepen, (…) noch uit de tekst ervan noch uit de rechtspraak van het Europese Hof voor de rechten van de mens valt af te leiden, dat die bepaling het recht erkent om niet tegen zichzelf te getuigen.*[75]

Het tweede deel van deze uitspraak valt na *Funke* en *Saunders* niet meer te handhaven, maar het Europese Hof van Justitie hield toch vast aan de ontkenning van nemo tenetur voor ondernemingen in de post-*Funke* zaak *Otto*.[76] Dit kan erop duiden dat het Hof van Justitie rechtspersonen uitsluit van de werking van nemo tenetur. Opvallend is ook dat in de VS, waar de rechtspraak over het Vijfde Amendement veel gelijkenissen vertoont met de Europese rechtspraak

---

73 HR 1 juni 1993, NJ 1994, 52, r.o. 5.4.

74 TK 1975-1976, 13 872, nr. 3, p. 11, geciteerd in Bovens 1998.

75 HvJ 18 oktober 1989, Jur. HvJ 1989, p. 3283ff (*Orkem*).

76 Zie Finaly 1996, p. 110-111.

over nemo tenetur, rechtspersonen ook kategorisch lijken te worden uitgesloten van het nemo-teneturbeginsel:

> *the corporation (…) of course possesses no such privilege.*[77]

Het "of course" in deze uitspraak suggereert dat het vanzelfsprekend is dat rechtspersonen *geen* aanspraak kunnen maken op nemo tenetur.
Zo vanzelfsprekend is dat evenwel niet, getuige de aangehaalde uitspraak van de Hoge Raad. Toch zijn voor de stelling in *Braswell* twee hoofdargumenten aan te voeren. Ten eerste verschillen rechtspersonen vaak van natuurlijke personen in hun machtspositie. Met name grote rechtspersonen hoeven zich tegenover de overheid niet in een ondergeschikte positie te bevinden, integendeel. De rechtsbescherming zou daarom navenant verminderd kunnen worden, aangezien deze veelal is bedoeld om de zwakkere partij in het recht te beschermen. Het verschil in machtsverhouding zou een verschillende behandeling van natuurlijke en rechtspersonen kunnen rechtvaardigen.[78] Finaly, die een warm pleidooi houdt voor het toekennen van nemo tenetur aan rechtspersonen, is het niet eens met dit argument:

> *De m.i. verwerpelijke redenering lijkt zo ongeveer te zijn, dat een vermogend rechtssubject een heel blik advocaten kan opentrekken, en dat het dan wel wat lastig wordt hem (ook nog) aanspraak op art. 6 EVRM, althans op het privilege, toe te kennen.*[79]

Bovens is daarentegen van mening dat een vermindering van waarborgen voor (machtige) rechtspersonen wel gerechtvaardigd kan worden, omdat er geen intrinsieke redenen zijn om grondrechten toe te kennen aan rechtspersonen. Daarvoor zijn alleen consequentialistische redenen aan te voeren, dat wil zeggen dat bescherming van rechtspersonen een ander doel kan dienen, zoals de verhoging van rechtszekerheid en daardoor het bevorderen van de maatschappelijke welvaart. Omdat de bescherming bekeken wordt vanuit de consequenties, kan er een afweging worden gemaakt of in een bepaald geval het toekennen of juist het onthouden van een grondrecht aan een rechtspersoon het beste het maatschappelijke doel dient. Met name bij procedurele rechten, zoals nemo tenetur, kan dit leiden tot een verschil in de rechtsbescherming tussen natuurlijke en rechtspersonen.[80]

---

77 *Braswell* v. *United States*, 487 U.S. 99, 1988.

78 In deze zin Bovens 1998, p. 658: "In het licht van de enorme maatschappelijke machtspositie van die grote rechtspersonen is het echter voorstelbaar dat hun rechten met minder waarborgen worden omgeven".

79 Finaly 1996, p. 114. Vgl. Bovens 1998, p. 658: "eenzame officieren van justitie, arm aan tijd en middelen, moeten het opnemen tegen uitstekend geëquipeerde teams van bedrijfsjuristen en gespecialiseerde advocaten die geen middel onbenut laten."

80 Bovens 1998, p. 657-658.

Een tweede argument voor het onthouden van de bescherming van nemo tenetur is gelegen in de aard van (de opsporing van) het misdrijf. Bij rechtspersonen gaat het veelal om fraude en het ontduiken van bijzondere wetgeving, zoals milieuvoorschriften. De opsporing van dit soort misdrijven is van een andere aard dan de opsporing van, bijvoorbeeld, moord, omdat in het laatste geval meestal het onderzoek begint met de vaststelling *dat* er een misdrijf is gepleegd – er is immers een lijk. Bij ondernemingsmisdrijven is juist het bestaan van een strafbaar feit meestal verborgen; dit komt pas naar voren tijdens een onderzoek, dat daarom vooral in de controlerende fase plaatsvindt. Met andere woorden: zonder medewerking van mogelijke overtreders blijft de overtreding zelf onbekend.[81] Dit onderscheid verklaart waarom in bijzondere wetgeving voor controlebevoegdheden een andere rechtsbescherming bestaat (zie par. 5.2.1): er zijn extra bevoegdheden nodig om het bestaan van het strafbare feit zelf boven water te halen. De specifieke moeilijkheden van dit soort opsporing rechtvaardigen dat in deze gevallen het nemo-teneturbeginsel niet (of minder) moet gelden.[82] Hetzelfde argument kan men hanteren om de bescherming van nemo tenetur aan rechtspersonen in het algemeen te onthouden (of te beperken), omdat het meestal zal gaan om ondernemingsmisdaad die anders moeilijk op te sporen zou zijn.

Ik vind de argumenten voor inperking van nemo tenetur voor rechtspersonen sterk, maar niet overtuigend genoeg om hen het beginsel maar helemaal te onthouden. Er zijn immers ook zwakke rechtspersonen en machtige natuurlijke personen; het eerste argument kan daarom niet zwaar wegen voor de wetgever (wel kan het, lijkt mij, meespelen op het niveau van de toepassing van een bevoegdheid in een concreet geval). Het tweede argument kan meespelen voor de wetgever bij het bepalen of een bepaalde bevoegdheid om medewerking af te dwingen gerechtvaardigd is, gelet op de aard van de strafbare feiten die de bevoegdheid beoogt te voorkomen en op te sporen. Maar dat betekent ook dat men niet in het algemeen kan zeggen dat rechtspersonen uitgesloten moeten zijn van nemo tenetur – dat hangt dan immers samen met de aard van het soort misdaad en van de bijbehorende opsporingsbevoegdheid.

Daarom concludeer ik dat in beginsel rechtspersonen aanspraak kunnen maken op het nemo-teneturbeginsel,[83] maar dat de bescherming (makkelijker) ingeperkt

---

81 Vgl. Buruma 1993, p. 249: "Niet voor niets is het ophelderingspercentage bij bijzondere wetten om en nabij de 100."

82 De Hoge Raad spreekt van "de specifieke eisen en problemen van de waarheidsvinding in zodanige zaken" die de bijzondere wetgever tot medewerkingsplichten nopen. HR 29 oktober 1996, NJ 1997, 232 m.nt. Sch. Zo ook Mäder 1997, p. 321, Martens 1996, par. 25 en Hieltjes 1998, p. 98.

83 Zo ook Lensing & Mulder 1994, p. 68-69, die dit vooral baseren op de overweging dat de rechtspositie van natuurlijke personen zou worden ondermijnd als rechtspersonen zich niet op nemo tenetur kunnen beroepen.

kan worden bij misdaad die naar zijn aard moeilijker op te sporen is doordat het bestaan van strafbare feiten zonder adequate controle- en opsporingsbevoegdheden veelal voor justitie verborgen zal blijven.

4.3.4 Actieve en passieve medewerking

Het systeem van de wet suggereert dat er een duidelijk verschil is tussen actieve en passieve medewerking van de verdachte. Velen hebben dit dan ook als fundamenteel aspect van het nemo-teneturbeginsel aangemerkt (vgl. par. 3.1.2) en het beginsel zou dan ook alleen van toepassing zijn op *actieve* medewerking van de verdachte. Maar dat is wel wat gekunsteld.
Ten eerste heeft het onderscheid tussen (actief) medewerken en (passief) dulden, zoals Meijer heeft opgemerkt, soms veel van een woordspelletje. "Waar de verdachte niet actief mee hoeft te werken, maar wel moet [...] dulden dat fysieke dwang toegepast wordt bestaat het verschil tussen actief meewerken en passief dulden alleen nog in de eigen of andermans spierbeweging."[84] Zo moet iemand een sorteerproef van speurhond Leo dulden, waarbij hij kan worden aangewezen als de drager van dezelfde geur als de vuisthamer die in het overvallen postagentschap werd gevonden. Theoretisch is het mogelijk dat de verdachte daarvoor niets actief hoeft te doen – de politie kan hem dragen naar de rij van personen waaruit Leo moet kiezen, maar waarschijnlijker is het dat de verdachte bevolen zal worden mee te lopen en ergens te gaan staan.[85] Dit geldt te meer voor een Oslo-confrontatie, waarin een getuige de dader uit een rij van op elkaar lijkende personen moet pikken. Denkelijk zal de verdachte daarin toch (actief) zijn plaats in de rij moeten innemen. Ook onderzoeksmethoden als schrijfproeven, stemanalyse en urine-onderzoek kunnen praktisch moeilijk zonder actieve medewerking van de verdachte worden uitgevoerd.[86] Zo duidelijk is het onderscheid tussen actieve medewerking en dulden dus niet. [87]

---

84 Meijer 1991, p. 895. In dezelfde zin Reijntjes 1996b, p. 12. Een mooie illustratie hiervan is de uitspraak van Van Veen: "Dus om het eens op de spits gedreven te zeggen: de verdachte die aan zijn lichaam moet worden onderzocht behoeft niet op het bevel 'doe Uw mond open' te reageren. Hij moet wel gedogen dat, indien hij niet meewerkt, zijn mond wordt opengebroken" (geciteerd in HR 2 juli 1990, NJ 1990, 751 (*Wangslijm*)). Meijer legt liever de nadruk op de dwang die wordt toegepast, niet op de aard van de vereiste medewerking.

85 Jörg 1998, p. 49. Volgens de Hoge Raad valt dit onder een "duldplicht". HR 2 juli 1990, NJ 1990, 751, m.nt. Sch (*Wangslijm*).

86 De Commissie Meijers, die voorstellen heeft gedaan voor de regeling van onderzoek aan het lichaam, schaart deze methoden merkwaardigerwijs onder de kategorie bevoegdheden waarbij de verdachte niets hoeft te doen. Commissie Meijers 1997, p. 17.

87 Jörg 1998, p. 49. Het onderscheid is volgens van Veen "niet te hanteren". Van Veen 1979, p. 688. Het is ook significant dat de Hoge Raad slechts sporadisch de bewoordingen heeft gebruikt dat "een verdachte – behoudens in bij de wet voorziene uitzonderingsgevallen – niet mag worden verplicht *actief* medewerking te verlenen aan hetgeen tot zijn veroordeling kan

Rozemond is het daar niet mee eens. Hij wijst op de samenhang met een principieel onderscheid: moet de verdachte bewijs leveren of moet de staat dat doen? Dit correspondeert immers met de onderscheiden strafbaarstellingen van wederspannigheid ("niet dulden door zich te verzetten", art. 180 Sr) en het niet voldoen aan een ambtelijk bevel ("niet actief meewerken", art. 184 Sr). Het onderscheid volgt volgens hem ook uit het systeem van de wet.[88] Dat is juist, maar dat impliceert niet dat het daarom een cruciaal onderscheid is bij de vraag of een onderzoeksbevoegdheid inbreuk maakt op nemo tenetur. De wetgever moet weliswaar kiezen welke vorm de bevoegdheid moet aannemen: een bevel tot actieve medewerking of een duldplicht, zodat duidelijk is welke strafbaarstelling van toepassing is als de verdachte tegenwerkt. Maar het feit dat bij diverse bevoegdheden actieve medewerking en dulden in de praktijk moeilijk te (onder)scheiden vallen, impliceert dat de wetgever hier een betrekkelijk willekeurige keuze moet maken: materieel komt het immers op hetzelfde neer. Die willekeur betekent dat de keuze voor een actieve medewerking of voor een dulden door de verdachte geen allesoverwegende betekenis toekomt voor de vraag of het nemo-teneturbeginsel in het geding is.
Dat komt mede door een tweede relativering. "Passieve medewerking" kan net zo belastend zijn voor de verdachte als actieve medewerking: voor het bewijs maakt het niet zoveel uit of de verdachte meewerkt aan bloedafname (actieve medewerking) of dat hij duldt dat bloed wordt afgenomen (passieve medewerking). Het hangt er dan maar net van af wat de ratio van het beginsel is of een dergelijke belasting acceptabel is. Als de grondgedachte achter nemo tenetur is dat het inhumaan is een verdachte te dwingen mee te werken aan zijn veroordeling, is dwingen te dulden net zo fout als dwingen te verklaren. De ratio van het beginsel moet dan ook worden vastgesteld voor we kunnen bepalen of nemo tenetur zich al dan niet mede uitstrekt over passieve medewerking – met andere woorden, het antwoord op de waarom-vraag is nodig voor beantwoording van de hoe-vraag.

---

leiden" (HR 1 oktober 1985, NJ 1986, 405 m.nt. ThWvV, mijn cursivering); in latere arresten gebruikt de Raad weer de mantra uit 1977 waarin het onderscheid doen-dulden niet wordt gemaakt (zie par. 4.1).

88 Rozemond 1992, p. 129.

4.4 De ratio van nemo tenetur

In rechtspraak en literatuur zijn vier gronden genoemd voor het nemo-teneturbeginsel, die weliswaar samenhangen maar toch een andere nadruk krijgen.[89]

1. Pressieverbod
In deze visie is het nemo-teneturbeginsel vooral bedoeld als instructienorm voor de overheid om geen ontoelaatbare druk op de verdachte uit te oefenen om zichzelf te beschuldigen. Het komt voort uit het verbod op marteling, waarvan men in de 18e eeuw inzag dat het onmenselijk was, en overigens ook onbetrouwbare verklaringen kon opleveren.[90] In deze visie hangt nemo tenetur sterk samen met het zwijgrecht van de verdachte: het gaat vooral om het voorkomen van fysieke of psychische druk op de verdachte om hem verklaringen te ontlokken. Passieve medewerking valt in deze visie dan ook niet onder nemo tenetur. Een exponent van deze visie is Baauw,[91] en ook Ansmink lijkt dit de meest reële visie te vinden.[92]

2. Menselijke waardigheid
Het spiegelbeeld van de eerste visie legt de nadruk op de menselijke waardigheid van de verdachte. Het hangt samen met de idee van het pressieverbod, maar bekijkt het van de andere kant: de verdachte. Het is inhumaan om iemand te dwingen aan zijn veroordeling mee te werken: hij hoeft niet voor het wrede dilemma te worden geplaatst om zichzelf te beschuldigen (en veroordeeld te worden voor het strafbare feit) of niet mee te werken (en veroordeeld te worden voor meineed, wederspannigheid of het niet opvolgen van een ambtelijk bevel). Anders gezegd: "gaat het er uiteindelijk niet om dat we het inhumaan, en dus ethisch verwerpelijk, vinden om iemand te dwingen aan zijn eigen ongeluk bij te dragen?"[93] In deze visie valt ook passieve medewerking onder het beginsel, omdat het ook onethisch is iemand te onderwerpen aan een onderzoekshandeling waarvan hij weet dat die bewijs tegen hem kan opleveren. De verdachte heeft dan immers nog de keuze tussen het passief ondergaan van de onderzoekshandeling (en veroordeeld te worden voor het feit) of zich met geweld daartegen te verzetten om de handeling te voorkomen (en veroordeeld te

---

89 Ik ga hier voorbij aan gesuggereerde gronden van "equality of arms" (Finaly 1996, p. 112) of "privacy of the mind" (*Pennsylvania* v. *Muniz*, 496 U.S. 582, 1990), daar deze volgens mij geen verklarende waarde hebben.

90 Ansmink 1981, p. 435. Ansmink ziet dit zelf overigens als verklaring voor het zwijgrecht, maar niet voor nemo tenetur. Europees rechter Martens vindt dat wel het geval: het martelverbod is mede een grond voor het nemo-teneturbeginsel (Martens 1996, par. 8).

91 Baauw 1979, p. 469.

92 Ansmink 1981, p. 445.

93 Reijntjes 1996b, p. 18.

worden voor wederspannigheid) – eenzelfde soort wreed dilemma. Het onderscheid tussen actief en passief verklaart overigens wel waarom de wetgever eerder tot passieve medewerking verplicht: het wrede dilemma is minder pregnant bij dulden dan bij actieve medewerking, omdat het alleen speelt in situaties waarin de verdachte zo zeer een onderzoekshandeling vreest dat hij zich gedwongen kan zien te proberen met geweld de handeling te voorkomen.

3. Procesautonomie

Samenhangend met de menselijke waardigheid, maar met een andere nadruk, is de visie dat nemo tenetur een uitdrukking is van de procesautonomie van de verdachte: hij mag zelf zijn houding bepalen bij het onderzoek en tijdens de terechtzitting. Uit zijn keuze mag geen bewijs worden afgeleid (al kan de houding meespelen bij de strafmaat). Ook deze visie impliceert een brede strekking van het nemo-teneturbeginsel: respect voor een al dan niet meewerkende houding van de verdachte houdt ook in dat gedwongen passieve medewerking in principe ontoelaatbaar is.[94] Een inbreuk is alleen gerechtvaardigd als hogere belangen daartoe noodzaken. In deze visie, onder andere verdedigd door Knigge[95] en Jörg[96], heeft het beginsel een duidelijk raakvlak met het zwijgrecht, de belangrijkste weerslag van de verklaringsvrijheid van de verdachte, maar valt het er niet mee samen.

4. Betrouwbaarheid

Tegenover de procesautonomie, dat het belang van de verdachte vooropstelt, staat de verklaring van nemo tenetur vanuit de betrouwbaarheid van het bewijs – een visie die het belang van de waarheidsvinding vooropstelt. Het nemo-teneturbeginsel beoogt vooral om betrouwbaar bewijs te garanderen: het verbiedt daarom verplichte medewerking van de verdachte bij activiteiten waarbij deze het resulterende bewijs kan beïnvloeden. De gebruikte dwang zou dan immers ten koste (kunnen) gaan van de betrouwbaarheid – denk aan onder marteling afgelegde verklaringen. Deze visie heeft een grote verklarende waarde voor het onderscheid tussen passieve en actieve medewerking: naarmate de verdachte actiever moet meewerken, heeft hij meer gelegenheid het resultaat te manipuleren en is de dwang dus minder gerechtvaardigd, of omgekeerd, naarmate een onderzoeksmethode (zoals DNA-onderzoek) betrouwbaarder bewijs oplevert, neemt de geldingskracht van het nemo-teneturbeginsel af. Deze

---

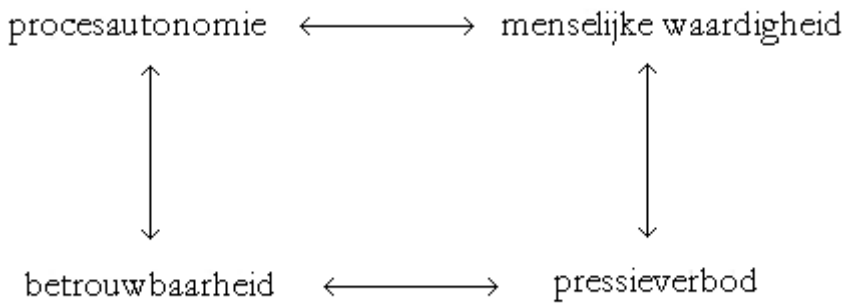
94 Martens 1996, par. 9. Martens leest deze visie in de uitspraak van het Europees Hof in de zaak *Saunders*, waar het Hof opmerkt dat het nemo-teneturbeginsel bijdraagt tot de vervulling van de doelen van art. 6 lid 1 EVRM. Martens zelf vindt dit te absoluut.

95 Annotaties bij EHRM 25 februari 1993, NJ 1993, 485 (*Funke*) en EHRM 17 december 1996, NJ 1997, 699 (*Saunders*).

96 Jörg 1998, p. 49-54.

visie is vooral verdedigd door Schalken,[97] en sluit goed aan bij de uitspraak van het Europees Hof in *Saunders* dat het nemo-teneturbeginsel zich niet uitstrekt over het gebruik van materiaal dat via dwangmiddelen verkregen wordt en dat onafhankelijk van de wil van de verdachte bestaat – een van de gronden van nemo tenetur vindt het Hof immers het voorkomen van rechterlijke dwalingen.[98] Hoewel het Hof het beginsel daarmee feitelijk inperkt tot de verklaringsvrijheid van de verdachte, en het daardoor vrijwel gelijk stelt met het zwijgrecht, is dat geen noodzakelijke interpretatie in deze visie; Schalken ziet een bredere strekking van het beginsel, zij het dat in gebieden van grotere betrouwbaarheid eerder inbreuken geoorloofd zijn.

Men zou nu kunnen vragen of de echte ratio nu wil opstaan. Ik denk dat dat geen zinvolle vraag is. Alle genoemde visies hebben goede argumenten. Het Europees Hof spreekt niet voor niets van "onder andere" bij het noemen van gronden voor nemo tenetur. De waarheid ligt ergens ertussen in. Ik zou de ratio van nemo tenetur dan ook willen weergeven in een schema dat de samenhang tussen de vier verklaringen aangeeft.



Afbeelding 1. De ratio van nemo tenetur

ezelfde medaille. Verticaal is er sprake van een tegenstelling. De bovenste rij legt de nadruk op het belang van de verdachte, de onderste op het belang van de opsporing. De bovenste visies zijn ook meer geneigd om het beginsel breed te interpreteren en ook passieve medewerking eronder te laten vallen. De onderste visies beperken het veeleer tot gedwongen actieve medewerking van de

97 Annotaties bij HR 2 juli 1990, NJ 1990, 751, HR 22 november 1994, NJ 1995, 240 en HR 29 oktober 1996, NJ 1997, 232. Zo ook Koops 1998, p. 179-180.

98 EHRM 17 december 1996, NJ 1997, 699 (*Saunders*), par. 68-69.

verdachte, en zien nemo tenetur ook sneller als instructienorm voor wetgever en politie dan als rechtsbeginsel.

Geen van deze gronden is alomvattend of alverklarend. De vele interpretaties van het kernarrest *Funke* kan men bijvoorbeeld verklaren door de verschillende nadruk die de interpreten leggen: op het pressieverbod (Funke werd op onaanvaardbare wijze tegen zijn wil *gedwongen* tot uitlevering van bankafschriften), op de betrouwbaarheid (Funke werd op onaanvaardbare wijze tegen zijn wil gedwongen tot uitlevering van *bankafschriften*),[99] op de menselijke waardigheid van de verdachte (Funke werd op *onaanvaardbare* wijze tegen zijn wil gedwongen tot uitlevering van bankafschriften) of op de procesautonomie (Funke werd op onaanvaardbare wijze *tegen zijn wil* gedwongen tot uitlevering van bankafschriften).

Ervan uitgaand dat de ratio van nemo tenetur het samenstel is van de vier geschetste verklaringen, kunnen we de reikwijdte van het beginsel nader invullen. Valt het uitleveren van materiaal dat onafhankelijk van de wil van de verdachte bestaat eronder? Is een duldplicht in principe een inbreuk op nemo tenetur? De ratio van betrouwbaarheid pleit voor een beperkte invulling van het beginsel: vormen van medewerking waarbij de medewerking geen invloed kan hebben op de betrouwbaarheid van het bewijs, hoeven niet beschermd te worden. In dat licht valt te verklaren waarom het Europees Hof het uitleveren van materiaal dat onafhankelijk van verdachtes wil bestaat, heeft uitgesloten van de werking van nemo tenetur, en waarom duldplichten vaak niet beschouwd worden als inbreuk.
Maar de ratio's van procesautonomie en menselijke waardigheid suggereren dat het beginsel een bredere strekking moet hebben. Vanuit het uitgangspunt dat een verdachte zelf zijn proceshouding moet kunnen bepalen, valt te beargumenteren dat verdachten ook niet gedwongen zouden mogen worden om onafhankelijke zaken uit te leveren of bezwarende handelingen te dulden.[100] Daar komt bij dat er bij diverse onderzoekshandelingen geen duidelijke, strikte scheidslijn bestaat tussen actieve medewerking en dulden, terwijl ook het kriterium "onafhankelijk van verdachtes wil" in de praktijk moeilijker hanteerbaar is dan het lijkt, omdat niet altijd duidelijk zal zijn of de gevorderde zaken daadwerkelijk bestaan (zie *Funke*). Het bestaan van een grijs grensgebied pleit voor een ruimere interpretatie. Waar in de praktijk een aanzienlijk schemer-

99 Waarbij men dan leest: zijn weigering tot uitlevering was onbetrouwbaar en dus ongeschikt voor het bewijs, omdat de douane-ambtenaren niet zeker wisten dat hij de betreffende bankafschriften had. Zie par. 4.1.

100 Jörg 1998, p. 49, die betoogt dat het verplicht dulden van bloedafname voor DNA-onderzoek een kritische grens heeft overschreden.

gebied bestaat tussen actieve medewerking en dulden door de verdachte, kan het niet zo zijn dat de wetgever bij de keuze voor een bevoegdheid in de vorm van een actieve medewerkingsplicht *wel*, maar in de vorm van een duldplicht *niet* een toets zou moeten uitvoeren aan het nemo-teneturbeginsel. Het past immers niet om rechtsbeginselen in twijfelgevallen eng te interpreteren.
Om deze twee redenen – de ratio's van procesautonomie en menselijke waardigheid, en het bestaan van een onduidelijk grensgebied tussen de soorten medewerking – nopen ertoe om het nemo-teneturbeginsel ruim uit te leggen. In principe vallen daarom ook vormen van dulden en het uitleveren van onafhankelijk materiaal onder de reikwijdte van het beginsel.[101]

4.5 Een definitie van het nemo-teneturbeginsel

Een algemene formulering van het nemo-teneturbeginsel, ingekleurd volgens de hiervoor besproken aspecten en met de nadruk op de uitoefening van bevoegdheden, luidt: "Niemand mag worden gedwongen bewijs tegen zichzelf te leveren." Een ander formulering, met de nadruk op het gebruik voor het bewijs, kan zijn: "Resultaten van onder dwang verkregen medewerking of dulden van iemand, mogen niet worden gebruikt als bewijs tegen hem."
Een formulering die beide aspecten verenigt, luidt:

> *Niemand mag worden gedwongen (actief of passief) bewijs te leveren dat tegen hem wordt of zal worden gebruikt.*

Dit beginsel geldt zowel voor natuurlijke als voor rechtspersonen. Deze formulering weerspiegelt de werking op verschillende niveaus van het beginsel. Voor de *wetgever* bestaat een onderscheid naar het stadium van het onderzoek. In de stadia *voor een strafrechtelijke aanklacht* is de afgedwongen medewerking geen inbreuk op nemo tenetur, omdat de medewerking hier (nog) niet met zich meebrengt dat de resultaten als bewijs tegen de persoon zullen worden gebruikt.[102] Als dat evenwel in een later stadium toch gebeurt, kan dat in strijd zijn met nemo tenetur, afhankelijk van de mate van dwang en het gebruik van het bewijsmateriaal. De eventuele inbreuk vindt dan dus pas plaats als de resultaten ook daadwerkelijk voor het bewijs worden gebruikt.

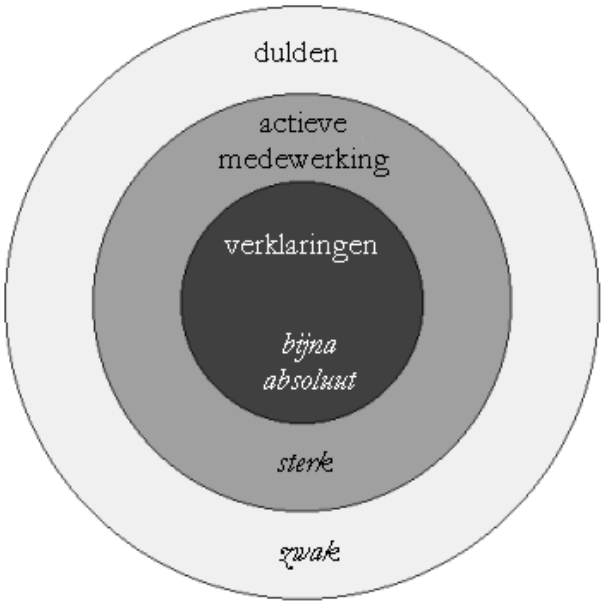
---

101 In deze zin ook Leijten, die bij "medewerking aan zijn eigen veroordeling" denkt aan "wettelijk geeiste actieve daden van de verdachte *of aan het gedogen van actieve ingrepen* in zijn persoon of lichaam" (conclusie bij HR 14 januari 1992, NJ 1992, 360, m.nt. ThWvV; mijn cursivering). Zo ook Lensing & Mulder 1994, p. 78-79, die spreken van de "periferie van het beginsel", en Jörg 1998, p. 49.

102 Een uitzondering is misschien wetgeving die een niet-verdachte tot medewerking verplicht met het (hoofd)oogmerk om de resultaten tegen hem te gebruiken in een strafproces als hij naar aanleiding van de medewerking verdachte wordt – zie de discussie over de meldplicht euthanasie (par. 5.2.1.1).

In het stadium *vanaf een strafrechtelijke aanklacht* is afgedwongen medewerking in principe een inbreuk, omdat de medewerking in dit stadium in beginsel met zich meebrengt dat belastende resultaten als bewijs zullen worden gebruikt. Dit lijdt alleen uitzondering als de regeling expliciet geen bewijsgaring beoogt, zoals de uitleveringsplicht van 551 Sv (zie par. 5.2.2).
Voor de *rechter* staat het gebruik van de resultaten als bewijs voorop. Een onderzoekshandeling die rechtmatig is, kan in een later stadium toch onrechtmatig bewijs opleveren, als het *gebruik* van de resultaten als bewijs, in combinatie met de dwang waaronder ze zijn verkregen, strijd oplevert met het recht op een eerlijk proces.
Nemo tenetur is dus primair een *bewijsregel*. Wel heeft het een reflexwerking op het voorafgaande onderzoek, omdat men daarin natuurlijk rekening moet houden met de bruikbaarheid van de resultaten voor het bewijs. Het kan daarom ook het uitoefenen beletten van te veel dwang om medewerking te verkrijgen, en het kan de wetgever beletten om een bevoegdheid in te voeren die beoogt bewijsmateriaal onder dwang te verkrijgen van strafrechtelijk aangeklaagden.

Op het nemo-teneturbeginsel kan inbreuk worden gemaakt. De algemene formulering kan geen recht doen aan de nuances van deze mogelijke inbreuken. Uit het systeem van de wet en de ratio's van het beginsel volgt immers dat de werking ervan mede afhangt van het stadium, de geadresseerde, de soort medewerking en de manier waarop resultaten voor het bewijs worden gebruikt. Het beginsel is sterker naarmate de gevorderde medewerking actiever is en dichter in de buurt komt bij handelingen die afhankelijk zijn van de wil van de verdachte, met name bij verklaringen. Men kan daarom spreken van een 'sterk nemo-teneturbeginsel' (bij actieve medewerking) en een 'zwak nemo-teneturbeginsel' (bij passieve medewerking). De werking van nemo tenetur valt derhalve als volgt weer te geven.



Afbeelding 2. De reikwijdte van het nemo-teneturbeginsel

Deze afbeelding geeft de reikwijdte van nemo tenetur weer. De harde kern ervan wordt gevormd door het zwijgrecht: dit recht is vrijwel[103] absoluut, en er kan dus vrijwel geen inbreuk op worden gemaakt.[104]
De middelste cirkel betreft gedwongen actieve medewerking. Dit zijn handelingen waarbij de geadresseerde iets moet doen, zoals materiaal uitleveren, een schrijfproef afleggen, of een opdracht schrijven aan de bank om informatie aan justitie te geven. Binnen deze cirkel bestaan natuurlijk gradaties: bepaalde handelingen liggen dicht bij het afleggen van een verklaring (zoals het overhandigen van een moordwapen, waarmee de verdachte toegeeft dat hij wist

103 Na *Murray* kan niet meer worden gezegd dat het zwijgrecht absoluut is (zie par. 5.2.1.4).

104 Men kan erover twisten of deze cirkel strikt genomen tot het nemo-teneturbeginsel behoort, of dat nemo tenetur alleen de buitenste twee cirkels omvat. Volgens Ansmink hebben beide rechten een verschillende achtergrond (zie par. 4.3.1). De meesten zien echter het zwijgrecht als de harde kern van – en dus behorend tot – het nemo-teneturbeginsel. Ik sluit mij hierbij aan, met de kanttekening dat het nodig blijft om het onderscheid tussen de twee te maken, met name vanwege het fundamentele verschil tussen de 'harde kern' van verklaringen (in principe geen inbreuk mogelijk) en de middelste ring van actieve medewerking (in principe inbreuk mogelijk).

waar het moordwapen lag), terwijl andere handelingen dichter liggen bij passieve medewerking, zoals het meewerken aan een confrontatie of een ademtest. In deze ring geldt het 'sterke' nemo-teneturbeginsel: iemand mag alleen worden gedwongen tot actieve medewerking als daar zwaarwegende maatschappelijke belangen tegenover staan en als de afweging tussen nemo tenetur en deze andere belangen doorslaat naar de laatste.

De grootste cirkel betreft tenslotte alle vormen van medewerking, waaronder 'passieve', dat wil zeggen het dulden van handelingen die bewijs kunnen opleveren, zoals een bloedproef. In de buitenste ring geldt het 'zwakke' nemo-teneturbeginsel: iemand mag worden gedwongen tot passieve medewerking als daar maatschappelijke belangen tegenover staan en als de afweging tussen nemo tenetur en deze andere belangen doorslaat naar de laatste. Het nemo-teneturbeginsel weegt hier minder zwaar dan bij actieve vormen van medewerking, zodat de balans sneller zal doorslaan naar de maatschappelijke belangen bij gedwongen medewerking.

Bij de afweging tussen geen gedwongen medewerking (nemo tenetur) en wel gedwongen medewerking (andere maatschappelijke belangen) spelen mijns inziens vooral de volgende overwegingen:

- **subsidiariteit**: een bevoegdheid die iemand dwingt tot medewerking mag eerder worden ingevoerd of toegepast als er geen alternatieven zijn, zoals huiszoeking en inbeslagneming; een uitvloeisel hiervan is dat bij misdrijven die naar hun aard moeilijk zijn op te sporen zonder bevoegdheden die afhankelijk zijn van de medewerking van (mogelijke) verdachten, eerder een inbreuk mag worden gemaakt dan bij andere (zie par. 4.3.3);
- **proportionaliteit**: de dwang die mag worden toegepast moet proportioneel zijn met de noodzaak en het doel van de medewerking; bij grotere noodzaak (zwaardere maatschappelijke belangen) mag dus meer dwang worden toegepast, zoals een hogere straf op niet-medewerking; een uitvloeisel hiervan is dat (machtige) rechtspersonen eerder kunnen worden gedwongen tot medewerking dan natuurlijke personen, gezien de consequentialistische grondslag van de nemo-teneturbescherming voor rechtspersonen (zie par. 4.3.3).

Wat betekent dit nu voor de **wetgever**? Deze mag een bevoegdheid invoeren om:

- verklaringen af te dwingen alléén van (rechts)personen die niet onderworpen zijn aan een strafrechtelijke aanklacht (de resulterende verklaringen (die dus niet in vrijheid zijn afgelegd) mogen niet altijd worden gebruikt als bewijs als het later alsnog komt tot een vervolging);

- actieve medewerking af te dwingen van vervolgde (rechts)personen alleen als er zwaarwegende maatschappelijke belangen zijn die de bevoegdheid noodzakelijk maken, de beginselen van subsidiariteit en proportionaliteit in acht nemend;
- passieve medewerking af te dwingen van vervolgde (rechts)personen alleen als er maatschappelijke belangen zijn die de bevoegdheid noodzakelijk maken, de beginselen van subsidiariteit en proportionaliteit in acht nemend.

Voor de **toepassing** van bevoegdheden betekent dit, dat:
- resultaten van rechtmatig afgedwongen medewerking van (rechts)personen voor het bewijs mogen worden gebruikt als dat, gegeven de mate van dwang en de manier waarop het als bewijs wordt gebruikt, en gegeven de relevante maatschappelijke belangen, opweegt tegen het recht van de verdachte op een eerlijk proces, de beginselen van subsidiariteit en proportionaliteit in acht nemend;
- resultaten van onrechtmatig afgedwongen medewerking van (rechts)personen niet voor het bewijs mogen worden gebruikt.

Het is van belang om deze niveaus goed uit elkaar te houden bij de vraag of afgedwongen medewerking van strafrechtelijk aangeklaagden rechtmatig is. De wetgever moet een afweging maken in abstracto, tussen het nemo-teneturbeginsel en (al dan niet zwaarwegende) maatschappelijke belangen, zoals misdaadbestrijding, de nationale veiligheid en het economisch welzijn. Het subsidiariteitsbeginsel speelt hier een cruciale rol: een bevoegdheid tot afgedwongen medewerking mag alleen worden ingevoerd, als het doel van de bevoegdheid niet kan worden bereikt door andere bevoegdheden die niet of minder inbreuk maken op grondrechten en beginselen. Ook moet de bevoegdheid proportioneel zijn, dat wil zeggen dat de mate van dwang en de strafmaat op niet-medewerking in verhouding moeten staan tot het doel van de bevoegdheid.
De rechter moet een oordeel geven of de toepassing van dwang in concreto gerechtvaardigd was, en of de resultaten van de dwang voor het bewijs mogen worden gebruikt, door het nemo-teneturbeginsel af te wegen tegen de maatschappelijke belangen bij het toepassen van de dwang en bij het gebruik voor het bewijs. Bij deze afweging speelt het subsidiariteitsbeginsel een rol (had de politie ook op een andere manier voldoende bewijs kunnen vergaren?), maar ook het proportionaliteitsbeginsel: is de mate van dwang (vanuit de nemo-teneturratio's van pressieverbod en humaniteit) en het gebruik voor het bewijs (vanuit de nemo-teneturratio van betrouwbaarheid) proportioneel met het te bereiken doel (waarheidsvinding en misdaadbestrijding in dit concrete geval)?

4.6 Maakt een ontsleutelplicht inbreuk?

Gegeven deze omschrijving van het nemo-teneturbeginsel, kan ik nu antwoord geven op de vraag of een ontsleutelplicht voor verdachten inbreuk maakt op het beginsel. Een ontsleutelplicht voor verdachten waarvan de resultaten voor het bewijs worden gebruikt, maakt inbreuk op het beginsel. Het betreft hier een vorm van actieve medewerking: de verdachte moet het wachtwoord geven of zelf ontsleutelen.
Bovendien gaat het om een activiteit die waarschijnlijk afhankelijk is van de wil van de verdachte. Het gaat strikt genomen niet om het afleggen van een verklaring, omdat het wachtwoord geen beschrijving is van feiten of omstandigheden in de woorden van de verdachte. Hij kan het wachtwoord ook niet in zijn geest veranderen. Maar aan de andere kant is het bestaan van het wachtwoord wel afhankelijk van de wil van de verdachte, in de situaties waarin de politie het wachtwoord niet op een briefje naast de computer vindt en een wachtwoordraadprogramma het laat afweten. In die gevallen bestaat het wachtwoord immers in feite alleen in het hoofd van de verdachte en in die zin is het bestaan van het wachtwoord wel degelijk afhankelijk van zijn wil. Bovendien kan het bekendmaken van het wachtwoord een verklarende waarde hebben, omdat de verdachte daardoor blijk geeft kennis te hebben van het wachtwoord: de handeling is dan "testimonial", tenzij de politie door omstandigheden zeker weet dat de verdachte beschikt over het wachtwoord.
Een ontsleutelplicht bevindt zich daarom op het grensvlak van afgedwongen verklaringen en afgedwongen actieve medewerking. Het maakt dus inbreuk op het (sterke) nemo-teneturbeginsel, en onder omstandigheden ook op het zwijgrecht.

5. Analogieën en precedenten

Voor het maken van een afweging of de bevoegdheid van een ontsleutelingsbevel voor verdachten gerechtvaardigd is, gegeven de belangen van nemo tenetur en misdaadbestrijding, moet men de overwegingen kennen die daarbij een rol (moeten) spelen. Die overwegingen zullen concreter moeten zijn dan "het belang van de verdachte" en "het belang van de misdaadbestrijding". In dit hoofdstuk beoog ik een concretisering te geven van de overwegingen die voor wetgever en rechter een rol spelen bij de beoordeling of een bepaalde inbreuk op nemo tenetur is gerechtvaardigd.
Ik zal dit doen door de overwegingen te analyseren die tot nu toe de Nederlandse wetgever en de Nederlandse en Europese rechters hebben gebruikt bij hun oordeel over mogelijke inbreuken op nemo tenetur. Deze analyse zal een beeld geven van de omstandigheden die van invloed zijn op het oordeel over te toelaatbaarheid van een inbreuk.
Naast een analyse van deze precedenten, kunnen enkele analogieën mogelijk ook een licht werpen op de onderzoeksvraag. Ik bespreek daarom eerst twee situaties waarin momenteel een soort "ontsleutelplicht" kan gelden, waarbij ik de overeenkomsten en verschillen met een decryptiebevel aan verdachten analyseer.
Uit de analogieën en momenteel toegestane inbreuken op nemo tenetur zal ik conclusies trekken over de omstandigheden die van invloed zijn op het oordeel of een bepaalde bevoegdheid, in casu een ontsleutelbevel aan verdachten, een gerechtvaardigde inbreuk op het nemo-teneturbeginsel is.

5.1 Analogieën

5.1.1 Bevel geheimschrift prijs te geven

De meest voor de hand liggende analogie is het geheimschrift – de traditionele vorm van encryptie. Er is immers eigenlijk niets nieuws aan versleuteling: al sinds jaar en dag gebruiken misdadigers geheimschrift om niet in handen te vallen van justitie. Digitale versleuteling verschilt niet fundamenteel van geheimschrift op papier. Tot voor kort is er nooit sprake geweest van de

dringende wens bij justitie om een bevoegdheid te hebben verdachten te dwingen hun geheimschrift prijs te geven. De kraakcapaciteit van de politie was kennelijk voldoende om de versleutelde berichten die zij onderschepte toch te kunnen lezen.

Waarom zou dan de opkomst van ICT, en de daarmee gepaard gaande mogelijkheid om berichten digitaal te versleutelen, wel nopen tot het invoeren van een ontsleutelingsplicht? Welke overwegingen kunnen worden aangevoerd om een andere afweging hier te rechtvaardigen? Ik denk dat er voldoende verschillen zijn tussen de situatie van geheimschriften tot ca. 1975 en de situatie van digitale versleuteling sinds het eind van de vorige eeuw, om ruimte te laten voor een andere afweging. De belangrijkste verschillen zijn volgens mij:

- schaalvergroting: geheimschriften werden redelijk beperkt gebruikt en hadden een relatief klein verspreidingsgebied (velen vonden hun eigen geheimschrift uit), terwijl digitale versleuteling in potentie door iedereen die een computer (of digitale telefoon) heeft kan worden gebruikt; de snelle opkomst van communicatienetwerken maakt deze schaalvergroting dusdanig, dat, hoewel er geen *fundamenteel* verschil is, men wel kan spreken van een *enorm gradueel* verschil tussen geheimschrift en digitale versleuteling;
- het gemak van toepassing: een geheimschrift op papier kost tijd, terwijl digitale versleuteling met een paar muisklikken en toetsaanslagen te realiseren is;
- de robuustheid van versleutelingssystemen: geheimschriften, die altijd gebaseerd zijn geweest op talige systemen, zijn altijd relatief goed te kraken geweest, terwijl digitale versleutelingssystemen, die gebaseerd zijn op wiskundige principes (bij goed gebruik en met voldoende lange sleutels) waarschijnlijk onkraakbaar zijn;
- het gemak van sleuteluitwisseling: bij geheimschrift moesten misdadigers onderling afspraken maken over het geheimschrift en eventueel te gebruiken sleutels, en die afspraken moesten in persoon worden gemaakt (om onderschepping te voorkomen), terwijl moderne versleutelingssystemen openbaar zijn en een openbare sleuteluitwisseling kennen;
- de opkomst van de aandacht voor de georganiseerde misdaad: het is niet zo dat misdaad voor 1975 nooit georganiseerd was, maar sinds die tijd is de georganiseerde misdaad een veel belangrijker aandachtspunt voor de politie geworden; georganiseerde misdaad gaat vanzelfsprekend gepaard met communicatie, terwijl ook per definitie middelen worden gezocht om die communicatie aan het oog en oor van de politie te onttrekken.[105] De

[105] Zie de definitie van de Enquêtecommissie opsporingsmethoden: "Van georganiseerde criminaliteit is sprake wanneer groepen van personen (…) in staat zijn deze misdaden op betrekkelijk effectieve wijze af te schermen". Enquêtecommissie opsporingsmethoden 1996, p. 25.

opkomst van een nieuwe "soort" misdaad, die mogelijk alleen afdoende bestreden kan worden met een bepaald arsenaal aan (nieuwe) opsporingsmethoden, kan een reden zijn om een andere afweging te maken;
- de opkomst van de telefoontap als opsporingsmiddel: de telefoontap is in de tweede helft van de vorige eeuw steeds belangrijker geworden als opsporingsmiddel, mede in verband met de opkomst van de georganiseerde misdaad; de politie is derhalve meer afhankelijk geworden van het onderscheppen van communicatie van misdadigers, zodat problemen bij dat onderscheppen, zoals door digitale versleuteling, nu meer de misdaadbestrijding belemmeren dan voorheen, bij geheimschriften.

Al met al zijn er dusdanig grote verschillen tussen traditionele geheimschriften en digitale versleuteling, dat je niet meer van een analogie kunt spreken. Het ontbreken van een bevoegdheid om een geheimschrift prijs te doen geven, kan daarom niet worden gebruikt als argument in de discussie over de invoering van een ontsleutelbevel aan verdachten.

5.1.2 Bevel te vertalen

Geheimschrift wordt soms vergeleken met teksten die zijn geschreven in andere (exotische) talen. Men kan zich daarom afvragen of er ooit een bevel is gegeven aan verdachten die communiceren in onverstaanbare talen, om hun communicatie te vertalen. Bij mijn weten is dat nooit gebeurd. Bij telefoontaps worden veel gesprekken in buitenlandse talen opgenomen, die vervolgens vertaald worden door vertalers (de kosten voor vertalen blijken zo'n 40% uit te maken van de kosten van telefoontaps!).[106]

Een plicht voor verdachten om te vertalen zou ook niet logisch zijn. Als justitie de taal niet kent, heeft zij geen mogelijkheid om te controleren of de vertaling door de verdachte klopt. Alleen al daarom gaat een vergelijking tussen een ontsleutelplicht en een vertaalplicht mank.

Met zou zich nog een hypothetisch geval kunnen voorstellen van opgenomen gesprekken van verdachten die in een uiterst zeldzame taal, zoals het Kwakiutl, hebben gecommuniceerd, waarbij de politie geen vertaler kan vinden. Zou de politie hen kunnen vragen om uitlevering van woordenboeken Kwakiutl-Nederlands? Die kunnen in dit geval immers dienen om de waarheid aan het licht te brengen. Een dergelijk bevel zou waarschijnlijk geen inbreuk zijn op het nemo-teneturbeginsel, omdat het overhandigen van woordenboeken op geen enkele manier incriminerend is. Aan de andere kant is zo'n bevel in de praktijk zinloos, omdat de politie nooit weet of iemand zo'n woordenboek heeft (als het al bestaat, hetgeen bij dergelijke talen op zich al twijfelachtig is). Met andere

106 Reijne 1996, p. 71.

woorden, er kan geen sanctie worden gezet op het niet naleven van zo'n bevel. Uitgaande van verdachten die niet vrijwillig willen meewerken met justitie, is dit daarom geen zinvolle analogie voor een eventuele plicht om sleutels te overhandigen, omdat zo'n plicht in elk geval onder strafbedreiging zal moeten worden gehandhaafd.

5.2 Precedenten

In de laatste decennia hebben wetgever en rechter diverse inbreuken op het nemo-teneturbeginsel toegelaten. Deze precedenten kunnen interessante invalshoeken opleveren voor de beantwoording van de onderzoeksvraag, omdat zij omstandigheden en argumenten definiëren die kennelijk van invloed zijn op de toelaatbaarheid van inbreuken op het beginsel. In deze paragraaf geef ik een uitgebreid, maar niet uitputtend, overzicht van (mogelijke) inbreuken op nemo tenetur die naar huidig Nederlands recht zijn toegestaan. Hierbij ga ik uit van de ruime definitie van het beginsel zoals onder 4.5 beschreven, die de verklaringsvrijheid, actieve medewerking en passieve medewerking omvat. Aangezien de ontsleutelplicht zich bevindt op het grensvlak tussen verklaringen en actieve medewerking, zal ik me op deze twee concentreren en duldplichten buiten beschouwing laten.

5.2.1 Plichten te verklaren

Meldplichten

Ten eerste bestaan er meldplichten die mogelijk een inbreuk zijn op het (brede) nemo-teneturbeginsel. Te denken valt bijvoorbeeld aan het afsluitformulier mestboekhouding, de meldplicht euthanasie, de melding ongebruikelijke transacties en de Bruyninckx-richtlijnen voor advocaten.[107] Bij dergelijke meldplichten wordt van personen verwacht dat zij opgave doen van hun handelen, naar aanleiding waarvan (mede) gecontroleerd kan worden of dat handelen wel legaal is geweest.
Een dergelijke verplichting rust echter op personen die niet verdacht zijn en (nog) niet onderworpen zijn aan een strafrechtelijke aanklacht. Daarom is een dergelijke wettelijke verplichting als zodanig niet in strijd met het nemo-teneturbeginsel, dat immers slechts geldt voor vervolgden (zie 4.3.2).[108]

---

107 Volgens deze richtlijnen moeten advocaten betalingen van meer dan ƒ25.000 in contanten melden – het accepteren van een dergelijke betaling kan in strijd zijn met de zorgvuldigheidsnorm van art. 46 Advocatenwet.

108 Zo bijvoorbeeld HR 22 juni 1999, NJ 1999, 648 over het afsluitformulier mestboekhouding. Anders Wöretshofer, die de meldingsprocedure levensbeëindiging een inbreuk op het

Wel blijft de vraag staan of de informatie die via dergelijke meldplichten is verkregen, gebruikt kan worden als bewijs tegen de melder. Volgens de Hoge Raad is dat in het algemeen het geval, omdat de meldplicht rechtmatig is en de informatie dus rechtmatig verkregen is.[109] Dit is echter te eenvoudig geredeneerd, gezien de opmerking van het Europees Hof in *Saunders*: "Moreover the fact that statements were made by the applicant prior to his being charged does not prevent their later use in criminal proceedings from constituting an infringement of the right." Het Europees Hof toetst het gebruik van het bewijs ook aan andere zaken, zoals de mate van dwang, de soort afgedwongen medewerking, het type rechtspraak (deskundige rechter of een ondeskundige jury) en of het resultaat in de strafzaak wordt gebruik op een manier die erop gericht is de verdachte te beschuldigen.
Aangezien het bij dergelijke meldplichten gaat om verklaringen – die de harde kern van het nemo-teneturbeginsel uitmaken – en er een zekere dwang bestaat om de verklaring af te leggen (weigering van melding wordt meestal gesanctioneerd), kan ik mij voorstellen dat onder omstandigheden het gebruik van meldingen in een strafzaak in strijd is met het nemo-teneturbeginsel, en dat het EHRM een dergelijk gebruik niet zou toestaan (zie vooral de sterke formulering in *Saunders*: "Het algemeen belang kan niet worden ingeroepen ter rechtvaardiging van het gebruik van gedurende een niet-gerechtelijk onderzoek onder dwang verkregen antwoorden, ter beschuldiging van de verdachte tijdens het strafproces"). Zo kan nemo tenetur noodzaken tot uitsluiting van bewijs verkregen uit een euthanasiemeldingsprocedure, als de mate van dwang de inhoud van de overlijdensverklaring en de proceshouding van de arts ter zitting dusdanig heeft beïnvloed, dat hij daardoor geacht kan worden onder dwang verklaringen te hebben afgelegd die tegen hem worden gebruikt om hem te beschuldigen in een strafzaak.[110]

---

beginsel vindt, omdat het – anders dan procedures die ten behoeve van controle werken – een duidelijk strafvorderlijk doel heeft. Wöretshofer 1996, p. 55 en Jörg 1998, p. 85-90. Ook anders Rozemond, die de wettelijke verplichting tot meewerken in een alcoholonderzoek ook voor niet-verdachten een inbreuk acht op nemo tenetur. Rozemond 1998, p. 310.

109 Volgens dezelfde redenering als het toelaten van bewijs uit controlebevoegdheden voor de opsporing (HR 26 april 1988, NJ 1989, 390 (*Controle en opsporing*)) en als in HR 29 oktober 1996, NJ 1997, 232 m.nt. Sch.

110 Zo ook Schalken in zijn annotatie bij HR 29 oktober 1996, NJ 1997, 232. Hoewel het niet-melden van euthanasie niet wordt gesanctioneerd, bevindt de arts zich wel in een belastende dwangpositie. Zie de arts die na euthanasie een valse verklaring van overlijden had afgelegd, omdat hij zich niet tot verdachte wilde bestempelen door een juiste verklaring als in de Meldingsprocedure levensbeëindiging af te leggen. (Hij werd veroordeeld voor het valselijk afleggen van een geneeskundige verklaring, art. 228 lid 1 Sr. HR 30 november 1999, NJ 2000, 216 m.nt. Sch.) Het moeten afleggen van een verklaring omtrent de doodsoorzaak brengt de arts dus in een dwangpositie: geen verklaring omtrent de

Bepaalde omstandigheden kunnen de wetgever nopen om bij voorbaat het gebruik van gemelde gegevens als bewijs tegen de melder uit te sluiten. Financiële dienstverleners zijn verplicht ongebruikelijke transacties te melden (art. 9 Wet MOT). Omdat ze zich bij witwastransacties schuldig kunnen maken aan heling, lopen ze door de melding het risico te worden vervolgd. Om te voorkomen dat instellingen om die reden minder transacties zouden melden, is er een bepaling ingevoerd dat de verstrekte inlichtingen niet kunnen worden gebruikt ter opsporing of als bewijs bij een vervolging van de dienstverlener voor heling (art. 12 Wet MOT). (Ze kunnen bijvoorbeeld wel dienen als bewijs bij een vervolging voor fraude of valsheid in geschrifte.)
De omstandigheden die bij deze clausule een rol spelen zijn het doel van de meldplicht en de "beoogde boef". De Wet MOT is bedoeld om witwassers en daarmee illegale winstmakers op te sporen. De melder is in dit geval een schakel die leidt tot de boef, niet degene die met de regeling beoogd wordt mogelijk aangepakt te worden. Bij de meeste andere meldplichten ligt dat anders: daar is degene die meldt ook degene die primair vervolgd zal kunnen worden: de onzorgvuldig euthanaserende arts, de overbemestende boer, de louche advocaat. Daarom kan de Wet MOT zich ook een nemo-teneturclausule veroorloven, en de andere meldplichten niet.
Wel staan bij dergelijke meldplichten andere belangen dan de repressieve voorop: het zijn primair ordenende en preventieve wetten. Pas in tweede instantie is wetgeving repressief – het strafrecht is hier het sluitstuk van een veelomvattende regelgeving. Daaruit volgt dat bij het oordeel of gemelde gegevens in een strafzaak tegen de melder als bewijs mogen worden gebruikt, de belangen van de wetgeving (zoals medische zorgvuldigheid, integriteit van de rechtspleging, het ordelijk verlopen van de economie, bescherming van het milieu) meegewogen worden tegen het nemo-teneturbelang van de verdachte. Ook zal de subsidiariteit van belang zijn, omdat overtreding van de regelgeving vaak moeilijk of niet kan worden opgespoord zonder de gegevens uit de meldplicht.

Meldplichten zijn overigens niet vergelijkbaar met een ontsleutelplicht; ze lijken meer op een algemene verplichting om cryptosleutels te deponeren. Voor het ontsleutelbevel, dat per definitie achteraf wordt gegeven, zijn hier daarom geen directe aanknopingspunten voor de wetgever te vinden.

---

doodsoorzaak afleggen, liegen of euthanasie melden. Jörg 1998, p. 85-90, noemt dit "een dwangpositie waarin de wetgever niemand behoort te plaatsen".

Inlichtingenplichten

In diverse bijzondere wetten bestaan verplichtingen om inlichtingen te verstrekken. Een algemene medewerkingsplicht is vastgelegd in artikel 5:20 lid 1 Awb: "Een ieder is verplicht aan een toezichthouder binnen de door hem gestelde redelijke termijn alle medewerking te verlenen die deze redelijkerwijs kan vorderen bij de uitoefening van zijn bevoegdheden." Deze bevoegdheden omvatten het vorderen van inlichtingen (art. 5:16 Awb) van een ieder, dus ook van verdachten. De inlichtingenplicht geldt absoluut voor niet-verdachten (behalve voor professionele geheimhouders), maar verdachten kunnen zich beroepen op het zwijgrecht van 29 Sv.[111] De verplichting wordt ook niet specifiek gesanctioneerd, maar valt terug op de strafdreiging van art. 184 Sr.
In de Algemene wet inzake rijksbelastingen geldt een algemene verplichting aan de inspecteur inlichtingen te verstrekken "die van belang kunnen zijn" (art. 47 AWR). Niet voldoen aan deze plicht is strafbaar met ten hoogste zes maanden (art. 68 lid 2 AWR). Echter, iemand wie een boete boven het hoofd hangt is niet verplicht een verklaring af te leggen voor zover het betreft de boete-oplegging (art. 67j AWR) (hij is wel verplicht te antwoorden op vragen die van belang zijn voor het vaststellen van de belastingaanslag).
Ook in de Wet op de economische delicten geldt een plicht alle medewerking te verlenen die de opsporingsambtenaren redelijkerwijs kunnen vorderen (art. 24a WED); opzettelijke weigering is een economisch delict (art. 26 WED). De bepalingen van Sv gelden, voorzover hiervan in de WED (en bepaalde andere bijzondere wetten) niet is afgeweken (art. 25 WED), met name dus het zwijgrecht van 29 Sv.
Het zwijgrecht geldt echter niet voor verdachten die in het kader van de Wet wapens en munitie verplicht zijn inlichtingen te geven (art. 47 lid 3 WWM) – alleen professionele geheimhouders kunnen zich daarvan verschonen (lid 4). Weigering is strafbaar met een geldboete van de derde kategorie (art. 54 WWM). Het betreft hier "alle inlichtingen (…) die redelijkerwijs nodig zijn" opdat de ambtenaren hun taak voor deze wet kunnen uitoefenen. Dit is een ruim geformuleerde verplichting met als enige beperkingen de lage strafbedreiging en het beperkte bereik van de wet; vermoedelijk is deze vergaande bevoegdheid ingegeven door het grote gevaar dat kan uitgaan van het ongelegitimeerd houden van wapens en munitie.

In het algemeen kan men hieruit de conclusie trekken dat personen op grond van bijzondere wetgeving gedwongen kunnen worden alle inlichtingen te verschaffen die redelijkerwijs nodig zijn voor de handhaving van de wet, maar dat zij zich kunnen verschonen als zij bloot staan aan vervolging. De

111 PG Awb, p. 352.

inlichtingenplicht in de WWM is hierop een uitzondering, die wordt beperkt door het kleine, afgebakende terrein en door de relatief lage strafbedreiging (geen vrijheidsstraf).

In hoeverre mag nu resulterend materiaal als bewijs tegen de inlichters worden gebruikt? Hier geldt hetzelfde als bij verklaringen uit meldplichten verkregen: het gebruik kan onder omstandigheden in strijd zijn met nemo tenetur, afhankelijk van het belang dat de wet beschermt, de mate van dwang en de invloed van het gebruik als bewijs op de houding en verklaringsvrijheid ter zitting van de verdachte.

Kentekenaansprakelijkheid

Het wegenverkeersrecht kent een bijzondere constructie: de kentekenaansprakelijkheid. Deze komt voort uit de gedachte dat de houder van een voertuig een zorgplicht heeft om te voorkomen dat zijn voertuig door anderen straffeloos wordt misbruikt in het verkeer, en uit de overweging dat de opsporing van daders in het verkeer bijzonder moeilijk wordt als eigenaars van voertuigen niet zeggen wie het voertuig bij het delict bestuurd heeft. De aansprakelijkheid is verschillend uitgewerkt voor drie soorten gevallen.
Bij *Mulder-feiten* (lichte overtredingen die uit het strafrecht naar het bestuursrecht zijn overgeheveld in de Wet administratiefrechtelijke handhaving verkeersvoorschriften) is de houder van een kenteken van een voertuig aansprakelijk voor de feiten die met dat voertuig zijn gepleegd. Het bekendmaken van de bestuurder helpt niet; de houder moet zelf maar zien op de bestuurder de boete te verhalen. De regeling houdt dus een zuivere risico-aansprakelijkheid in. De Mulder-handhaving is wel onderworpen aan art. 6 EVRM, maar de regeling is volgens de Hoge Raad niet in strijd met het beginsel van de onschuldspresumptie (art. 6 lid 2 EVRM), gezien de moeilijkheid tegen de massale overtredingen te kunnen optreden, de mogelijkheden van de kentekenhouder de boete te verhalen op de bestuurder, en de beperkte omvang van de boetes.[112]
Bij een *misdrijf* uit de Wegenverkeerswet door een onbekend gebleven bestuurder, is de kentekenhouder verplicht op vordering naam en volledig adres van de bestuurder bekend te maken (art. 165 lid 1 WVW 1994). Weigering is strafbaar met ten hoogste twee maanden (art. 177 lid 1 WVW 1994). De verplichting geldt evenwel niet voor kentekenhouders die verdacht worden van het misdrijf: voor hen geldt het zwijgrecht van 29 Sv.[113] Om deze reden adviseert de 'Aanwijzing onbekend gebleven bestuurders' de politie om de kentekenhouder eerst te

112 HR 15 juli 1993, NJ 1994, 177 m.nt. C. Corstens verzet zich in zijn annotatie tegen het opheffen van het beginsel 'geen straf zonder schuld', waaraan de beperktheid der boetes volgens hem niet afdoet.

113 HR 26 oktober 1993, NJ 1994, 629 m.nt. C.

bevelen de naam van de bestuurder bekend te maken, en pas vervolgens te horen als verdachte. [114] Strikt genomen maakt de bepaling dus geen inbreuk op nemo tenetur. Ik vraag mij wel af hoe het Europees Hof over deze fictief aandoende constructie zou oordelen, aangezien de kentekenhouder uit het bevel ex 165 WVW 1994 allicht in redelijkheid de gevolgtrekking kan verbinden dat hij zal worden vervolgd voor het gronddelict.[115] Ten tweede kan men zich afvragen of, als de kentekenhouder op de vordering antwoordt dat hijzelf de bestuurder was, deze verklaring als bewijs tegen hem kan worden gebruikt. De verklaring is immers onder dwang afgelegd (de dreiging van twee maanden gevangenisstraf) en het gebruik als bewijs zal invloed hebben op zijn proceshouding. Het gebruik voor het bewijs kan daarom inbreuk maken op het nemo-teneturbeginsel.
Bij *overtredingen* uit de WVW geldt een andere constructie: daar is de kentekenhouder aansprakelijk voor de overtredingen, tenzij hij naam en adres van de bestuurder bekend maakt of het niet kunnen vaststellen van de bestuurder hem redelijkerwijs niet kan worden verweten (art. 181 WVW 1994). De desbetreffende overtredingen zijn strafbaar met ten hoogste twee maanden (art. 177 WVW 1994). Strikt genomen is de kentekenhouder hier niet een verdachte, omdat artikel 181 slechts stelt dat tegen de kentekenhouder dezelfde straffen kunnen worden uitgesproken, zonder de suggestie dat hij de feiten zou hebben begaan. Niettemin is er wel sprake van een "criminal charge" in de zin van art. 6 EVRM, omdat de kentekenhouder blootstaat aan vervolging in een strafzaak waarin diezelfde straffen kunnen worden uitgesproken. Deze dreiging dwingt hem in feite om de bestuurder bekend te maken, en daarom maakt deze regeling inbreuk op het nemo-teneturbeginsel – er is immers gerede kans dat zijn verklaring tegen hemzelf zal worden gebruikt. Deze inbreuk is kennelijk door de wetgever toegelaten, waarbij een rol hebben gespeeld de overwegingen van de gevaarzetting van het autorijden, het belang van de verkeersveiligheid, de moeilijke bewijsbaarheid als de kentekenhouder volhoudt niet de bestuurder te zijn geweest, en de niet al te grote strafdreiging. Toch mag de regeling uitzonderlijk heten, nu een verklaring wordt afgedwongen met een vrijheidsstraf.

---

114 Stct. 1999, nr. 212, p. 13. Jörg 1998, p. 61, noemde eerder al het gevaar dat de jurisprudentie een zekere onwaarachtigheid in de politiepraktijk zou kunnen bevor-deren, hetgeen nu kennelijk geïnstitutionaliseerd is.

115 Vgl. de overweging van de Hoge Raad dat "mag worden aangenomen dat in het merendeel van de gevallen – zeker bij het 'particuliere' deel van het wegverkeer – de bestuurder van het motorrijtuig tevens de kentekenhouder is" (de HR zegt dit over Mulder-feiten, maar dezelfde redenering valt te maken voor verkeersmisdrijven). HR 15 juli 1993, NJ 1994, 177 m.nt. C.

Zwijgen en omkering van de bewijslast

De kentekenaansprakelijkheid bij WVW-overtredingen is strikt genomen geen omkering van de bewijslast, omdat de kentekenhouder niet veroordeeld wordt als schuldige bestuurder, maar als aansprakelijke kentekenhouder. Het enige bewijs dat daarvoor nodig is, is bewijs van daderschap van het voertuig en bewijs van het kentekenhouderschap, en de last voor die bewijzen ligt bij het OM. Niettemin heeft de regeling toch enigszins de schijn van bewijslast-omkering tegen zich, nu zij spreekt van "de op het feit gestelde straffen" die tegen de houder kunnen worden uitgesproken: op de verdachte komt dat al snel over als een veroordeling voor het feit zelf, waarin zijn weigering de bestuurder te noemen als bewijs is gebruikt dat hijzelf de bestuurder was.

Een omkering van de bewijslast past niet in ons strafrecht – het is in strijd met de onschuldspresumptie, die vrijwel absoluut is. Het zwijgen van de verdachte mag niet tegen hem worden gebruikt bij beantwoording van de schuldvraag. Het mag overigens wel worden gebruikt bij de strafmaat.[116] Ook kan het non-verbale gedrag (waaronder zwijgen) van verdachte als voorwerp van eigen waarneming van de rechter meewerken als bewijs, al mag hij dit niet in de voor het bewijs gebezigde verklaring van de verdachte zelf verwerken (bijvoorbeeld door stil-zwijgen als bevestigend antwoord op een vraag weer te geven).[117] Ook kan de uitspraak van de verdachte "dat hij weigerde te verklaren waar hij zich gedurende de nacht van 25 op 26 maart 1971 heeft bevonden" mogelijk tot bewijs meewerken, zij het niet als verklaring van de verdachte maar als eigen waarneming van de rechter.[118] Daarnaast kan een kennelijk leugenachtige verklaring van de verdachte meewerken aan het bewijs onder de streep[119], waarbij de leugenachtigheid en niet de inhoud van de verklaring wordt gebruikt.[120]

Ook kan verdachtes weigering antwoord te geven worden gebruikt bij de gemotiveerde verwerping van zijn verklaring die aangeeft dat hij het niet heeft gedaan en die verenigbaar is met het beschikbare "bewijs"materiaal[121] ("Ik had het pistool wel in mijn hand, maar dat kwam omdat ik het had opgepakt toen ik toevallig langskwam op weg naar mijn werk"). Recentelijk heeft de Hoge Raad dit verder doorgevoerd door de redenering als het ware om te draaien. Indien "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 redelijk, die

---

116 HR 18 december 1984, NJ 1985, 358.

117 HR 16 maart 1999, *Njb* 1999, nr. 54, p. 739-740.

118 Aldus annotator Van Veen in HR 27 juni 1972, NJ 1972, 492 m.nt. ThWvV.

119 Dat wil zeggen als extra redenering, na de bewijsmiddelen die de rechter de innerlijke overtuiging van schuld hebben gegeven.

120 HR 12 november 1974, NJ 1975, 41 m.nt. ThWvV.

121 HR 19 maart 1996, NJ 1996, 540 m.nt. Sch.

redengevendheid ontzenuwende, verklaring heeft gegeven", kan de rechter zulks "in zijn overwegingen omtrent het gebezigde bewijsmateriaal betrekken".[122] Met andere woorden, als de verdachte *niet* een alternatieve verklaring biedt voor een bezwarende omstandigheid, kan de rechter zijn weigering te verklaren gebruiken als overweging om de omstandigheid als redengevend voor de schuld te bezigen. In casu 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); het zwijgen mocht bij de overwegingen ten aanzien van de bewijsvoering worden betrokken. Daarmee werkt het zwijgen van verdachte indirect mee aan het bewijs.
Hoewel deze rechtspraak misschien niet de grens van het zwijgrecht overschrijdt, wordt deze grens wel erg dicht genaderd. Dit valt ook af te leiden uit recente wetsontwerpen die zich op de grens van het toelaatbare begeven. Zo wijzigt wetsvoorstel EK 2000[123] de strafbaarstelling van openlijke geweldpleging (art. 141 Sr) tot het openlijk 'in vereniging' plegen van geweld, met de bedoeling relschoppers makkelijker strafrechtelijk te kunnen aanpakken. Hierbij wordt de "zwijgzaamheid van de deelnemers na afloop (…) gezien als een element van een welbewust gekozen collectieve opstelling", waardoor de suggestie ontstaat "dat de zwijgzaamheid achteraf mede redengevend zou kunnen zijn voor een strafrechtelijke aansprakelijkheid van de (zwijgzame) deelnemer aan een demonstratie van waaruit [het] openlijke geweld is gepleegd".[124] Ook bij de beoogde strafbaarstelling van witwassen zou het zwijgen van de verdachte over de herkomst van het gewassen geld gebruikt kunnen worden bij de bewezenverklaring, hetgeen een verschuiving van de bewijslast met zich mee zou brengen.[125]

Ook in Europese rechtspraak is omkering van de bewijslast aan de orde gekomen. Amosi Salabiaku, wonend te Parijs, ging naar het vliegveld Roissy om een pakje af te halen, dat Afrikaans eten zou bevatten. De vliegveldbeambte stelde voor dat hij de koffer echter niet zou meenemen, omdat deze verboden goederen zou kunnen bevatten. Niettemin nam Salabiaku de koffer mee, waarna de douane hem aanhield en zijn koffer onderzocht. Er zat tien kilo hasj in.

---

122 HR 3 juni 1997, NJ 1997, 584, herhaald in HR 10 november 1998, *Njb* 1998, nr. 147, p. 2031. In dezelfde zin Lensing & Mulder 1994, p. 71.

123 Pardon, ik bedoel natuurlijk Wetsvoorstel tot wijziging van de strafbaarstelling van openlijke geweldpleging, TK 1998-1999, 26 519, nrs. 1-3.

124 Waling 1999, p. 1557.

125 Aldus Van Duyne & Van der Landen 1999, p. 1687.

(Twee dagen later bleek een pakje met levensmiddelen, geadresseerd aan Salabiaku, per ongeluk in Brussel te zijn bezorgd.) Volgens de Franse Douanewet is de bezitter van goederen die niet bij de douane zijn aangegeven, daarvoor aansprakelijk, tenzij hij overmacht kan aantonen. Salabiaku werd veroordeeld voor drugssmokkel op grond van zijn bezit van de hasj; een beroep op overmacht kwam hem niet toe nu hij de waarschuwing 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.[126]
Ook in *Murray* werd de grens van het zwijgrecht verkend: de weigering van Murray te verklaren waarom hij in het huis van de IRA-gijzelaar was aangetroffen, mocht meewerken tot het bewijs (zie par. 4.1).

Uit de casuïstiek blijkt dat, hoewel het zwijgrecht in het strafprocesrecht als vrijwel absoluut wordt gezien, er zeker enige ruimte is voor de rechter om het zwijgen van verdachten indirect te laten meewerken aan het bewijs. De (bijzondere) wetgever heeft volgens Europese rechtspraak ook enige ruimte om de bewijslast om te keren, mits de regeling met voldoende waarborgen is omkleed en zorgvuldig wordt toegepast door een deskundige rechter. Deze bevinding is relevant bij de beoordeling welke sanctie gezet kan worden op nietnaleving van een eventuele ontsleutelplicht: omkering van de bewijslast komt daarvoor in aanmerking als de waarborgen die het Europees Hof heeft vastgesteld in acht worden genomen.

Spreekplicht van getuigen

Anders dan de verdachte, die niet hoeft te antwoorden (art. 29 lid 1 Sv), heeft de getuige in strafzaken wel een plicht om te antwoorden. Als hij weigert, kan hij in gijzeling worden genomen, totdat hij alsnog aan zijn plicht voldoet of totdat zijn getuigenis niet meer nodig is (artt. 221 en 294 Sv). De getuige kan zich echter verschonen van het antwoorden op bepaalde vragen, indien hij door te antwoorden zichzelf aan het gevaar van een strafrechtelijke veroordeling zou blootstellen (art. 219 Sv). Ook in civiele zaken is de getuige verplicht getuigenis af te leggen, maar hij kan zich verschonen als hij zich zou blootstellen aan het

126 EHRM 7 oktober 1988, NJ 1991, 351 (*Salabiaku v. Frankrijk*).

gevaar van een strafrechtelijke veroordeling ter zake van een misdrijf (art. 191 lid 4 Rv).
Een absolute verplichting te antwoorden bestaat wel in de Wet op de Parlementaire Enquête, ook als getuigen zichzelf daardoor zouden beschuldigen. Er bestaat een verschoningsrecht voor professionele geheimhouders (art. 19 WPE), maar niet voor hen die door te antwoorden zichzelf zouden beschuldigen. Van weigering te antwoorden wordt proces-verbaal opgemaakt (art. 15 lid 2 WPE), dat in handen van het Openbaar Ministerie kan worden gesteld (art. 16 WPE), die de weigerachtige getuige kan vervolgen bij de burgerlijke rechter (art. 10 WPE). Tegenover de antwoordplicht staat wel een nemo-teneturmaatregel van bewijsuitsluiting voor afgelegde verklaringen: behoudens bij vervolging voor meineed of omkoping van getuigen, kunnen verklaringen voor een parlementaire commissie niet "als bewijs in rechte gelden, hetzij tegen degene door wie zij afgelegd zijn, hetzij tegen derden" (art. 24 WPE).
Bij de diverse spreekplichten bestaat dus een verschil in uitwerking van het nemo-teneturbeginsel. De verdachte hoeft nooit te antwoorden, terwijl de getuige in strafzaken alleen op bepaalde vragen niet hoeft te antwoorden als het antwoord zou kunnen leiden tot een vervolging tegen hem; de getuige voor een parlementaire enquêtecommissie moet altijd antwoorden, maar zijn antwoorden kunnen niet als bewijs worden gebruikt. Dit niveauverschil laat zich mogelijk verklaren door het verschil in context: bij de verdachte staat voorop dat zijn antwoorden gebruikt worden voor de schuldvraag tegen hemzelf (alles wat hij zegt kan (en zal) tegen hem worden gebruikt), terwijl bij de getuige in strafzaken voorop staat dat zijn antwoorden tegen iemand anders worden gebruikt – alleen secundair zou men zijn antwoorden ook tegen hemzelf kunnen willen gebruiken. Bij getuigen in parlementaire enquêtes staat vervolging hoe dan ook niet voorop, het gaat vooral om het naar boven halen van de waarheid; voor dat doel moet in dit geval de vervolgingsmogelijkheid wijken. Parallel aan het vervolgingsrisico van de spreker loopt dus de nemo-teneturbescherming: hoe hoger het vervolgingsrisico, hoe meer bescherming tegen beschuldiging van zichzelf hij heeft.

5.2.2 Plichten actief mee te werken

Naast de inlichtingenplichten kennen de bijzondere wetten uiteenlopende verplichtingen om actief mee te werken, bijvoorbeeld door inzage in stukken te geven en door zaken uit te leveren. De algemene medewerkingsplicht van artikel 5:20 lid 1 Awb (zie par. 5.2.1) betreft mede het voldoen aan vorderingen tot inzage van zakelijke gegevens en bescheiden (art. 5:17 lid 1 Awb).
De AWR kent een algemene verplichting gegevens en inlichtingen te verstrekken aan de inspecteur, en boeken, bescheiden en andere informatie-dragers (of

de inhoud daarvan) ter beschikking te stellen (art. 47 AWR), terwijl ambtenaren uitlevering van voor inbeslagneming vatbare voorwerpen kunnen vorderen (art. 81 AWR). Er zijn nauwelijks restricties aan verbonden: de inlichtingen en gegevens moeten "van belang kunnen zijn", terwijl inbeslagname "te allen tijde" mogelijk is. De administratie moet ook dusdanig zijn ingericht, dat controle binnen een redelijke termijn mogelijk is; de administratieplichtige verleent de benodigde medewerking, inclusief het verschaffen van het benodigde inzicht in de opzet en werking van de administratie (art. 52 lid 6 AWR). Niet voldoen aan deze plichten is strafbaar met ten hoogste zes maanden (art. 68 lid 2 AWR). De uitzondering voor vervolgden om niet te hoeven verklaren (art. 67j AWR) kent geen pendant bij deze actieve medewerkingsplichten, hoewel dat in de oorspronkelijke versie van het wets-voorstel wel werd voorgesteld: de geadresseerde was "niet gehouden tot het mondeling of *schriftelijk verstrekken van gegevens of inlichtingen*" (mijn cursivering). Wegens bezwaren van de Eerste Kamer hiertegen is de uitzondering in de uiteindelijke wet beperkt tot het afleggen van verklaringen.[127]
Ook in de Wet op de economische delicten gelden medewerkings- (art. 24a WED), inzage- (art. 19 lid 1 WED) en uitleveringsplichten (art. 18 WED); weigering is een economisch delict (art. 26 WED). Er geldt daarbij de voorwaarde dat de medewerking "redelijkerwijs nodig is voor de vervulling van de taak" van de opsporingsambtenaren. Ook gelden de bepalingen van Sv, voorzover hiervan in de WED of in bepaalde bijzondere wetten niet is afgeweken (art. 25 WED). Aangezien er andere voorwaarden gelden voor het uitleveringsbevel van art. 18 WED (in belang van de opsporing voorzover redelijkerwijs nodig) dan voor het commune uitleveringsbevel van art. 96a lid 1 Sv (het moet gaan om een voorlopige-hechtenismisdrijf), is er sprake van een afwijking van Sv, en geldt dus niet de bepaling van art. 96a lid 2 Sv dat het bevel niet aan de verdachte wordt gegeven. Ook de medewerkings- en inzageplichten zijn afwijkingen van Sv, en mogen dus van verdachten worden gevorderd.
Hetzelfde geldt voor de plicht inzage van wapens- en munitie-gerelateerde bescheiden te geven (art. 47 lid 3 WWM): verdachten kunnen zich hier niet van verschonen. Weigering is strafbaar met een geldboete van de derde kategorie (art. 54 WWM).
Bij verdenking van alcoholmisbruik in het verkeer, kan de verdachte worden bevolen mee te werken aan een blaastest of bloedafname. Hij is verplicht hieraan mee te werken (art. 163 WVW 1994); dit is als een vorm van actieve medewerking geformuleerd: de verdachte "is verplicht ademlucht te blazen" (lid 2) of "zijn medewerking te verlenen" aan een bloedonderzoek (lid 6). Weigering is strafbaar met dezelfde straf als alcoholmisbruik: drie maanden (art. 176 lid 3 WVW 1994) of, bij letsel of dood, drie jaar respectievelijk negen jaar (art. 175 lid

127 Zie over de curieuze wetsgeschiedenis Hieltjes 1998.

2 WVW 1994). Door deze strafbaarstelling wordt er dwang uitgeoefend op de verdachte om mee te werken, hetgeen een inbreuk op nemo tenetur is. De belangrijkste reden voor deze inbreuk is dat er vrijwel geen afdoende alternatieven zijn om bewijs van alcoholmisbruik te verkrijgen als de verdachte niet meewerkt aan een adem-, bloed- of urineonderzoek. De wetgever had er ook voor kunnen kiezen om de bloedafname met geweld afdwingbaar te maken, zodat er geen bijzondere strafbaarstelling van weigering had hoeven plaatsvinden; kennelijk werd de inbreuk op nemo tenetur bij de actieve medewerking in dit geval minder zwaar bevonden dan de inbreuk op de lichamelijke integriteit bij een duldplicht tot gedwongen bloedafname.[128]

In het commune strafrecht geldt de verplichting voor eenieder tot uitlevering van voorwerpen bij bepaalde delicten (art. 551 Sv). Wie kijkt naar de catalogus van delicten waar het hier om gaat, valt op dat het allemaal delicten zijn waarbij er een object van het delict is waarvan het raadzaam kan zijn om dat in beslag te nemen ter onttrekking aan het verkeer, zoals een mishandeld dier, kinderporno, een uiting die de koning beledigt. Met de wet tot herziening van het gvo is dit artikel dan ook komen te luiden dat de inbeslagneming alleen kan plaatsvinden "voor zover de vordering tot uitlevering ertoe strekt om hun verbeurdverklaring of onttrekking aan het verkeer mogelijk te maken". Uitlevering ten behoeve van de waarheidsvinding is dus niet geoorloofd. Wel kan men zich afvragen of eenmaal uitgeleverde voorwerpen die verbeurd zijn verklaard of aan het verkeer zijn onttrokken niet ook voor het bewijs kunnen worden gebruikt. De formulering van de bevoegdheid staat dat niet in de weg. Verder bestaan er in het commune strafrecht geen actieve medewerkingsplichten voor verdachten.

In het algemeen kan men hieruit de conclusie trekken dat aan verdachten op grond van bijzondere wetgeving vorderingen kunnen worden gegeven tot actief meewerken, het verschaffen van inzage in stukken en het uitleveren van voorwerpen. Zij kunnen zich niet verschonen als zij bloot staan aan vervolging. De resultaten van de medewerking kunnen in principe tegen hen worden gebruikt als bewijs. De bevoegdheden en de medewerkingsplichten zijn in het algemeen ruim geformuleerd, met veelal als enige beperking dat de medewerking "redelijkerwijs nodig" is voor de taakvervulling van de handhavers van de bijzondere wetgeving. De beperking zit hem dan vooral in het afgebakende terrein van de wet, dat slechts een klein domein van de maatschappelijke activiteit beslaat. Het commune strafrecht kent geen actieve meewerkingsplichten voor verdachten.

128 Vgl. Rozemond 1998, p. 92 en 310.

5.2.3 Conclusie

Uit deze inventarisatie volgt dat de *wetgever* bij medewerkingsplichten onderscheid maakt naar de persoon (verdacht of niet), de aard van de wet (commuun of bijzonder) en de aard van de medewerking (verklaring of actieve medewerking).
Voor niet-verdachten gelden allerlei verklaringsplichten, zoals meldplichten, inlichtingenplichten en getuigplichten. In meldplichten vindt men soms een bewijsuitsluitingsclausule, maar meestal zijn gemelde gegevens volgens de wet toelaatbaar als bewijs. De inlichtingen- en spreekplichten voor niet-verdachten kennen meestal verschoningsrechten als de spreker zichzelf zou blootstellen aan vervolging; soms bestaat geen verschoningsrecht maar geldt er een bewijsuitsluitingsregel.
Voor verdachten gelden zelden verklaringsplichten. Wel zijn in bijzondere wetgeving diverse medewerkingsplichten voor verdachten toegestaan, zolang zij de verklaringsvrijheid niet raken. Deze wettelijke medewerkingplichten maken wel inbreuk op het nemo-teneturbeginsel, maar die inbreuk is toegestaan door de wetgever, vooral op grond van de aard van de delicten (die anders moeilijk op te sporen zijn, zie par. 4.3.3), de beperkte reikwijdte van de bijzondere wetgeving en de relatief lage strafbedreiging. Uitzonderlijk zware regelingen in dit verband zijn de kentekenaansprakelijkheid voor verkeersovertredingen (en mogelijk ook verkeersmisdrijven), waarbij een verklaring wordt afgedwongen onder strafbedreiging van twee maanden, en de relatief hoge straf van zes maanden in de actieve medewerkingsplichten van de AWR.

In hoeverre mag nu de *rechter* resulterend materiaal als bewijs tegen de medewerkers gebruiken? Als het onafhankelijk van verdachtes wil bestaat, altijd, aldus *Saunders* en de Hoge Raad.[129] Dat ligt echter genuanceerder, omdat ook materiaal dat onafhankelijk van verdachtes wil bestaat onder de werking van nemo tenetur valt (zie par. 4.4). Het gebruik daarvan als bewijs kan onder omstandigheden in strijd zijn met nemo tenetur, net zoals het Europees Hof in *Saunders* vaststelde voor het gebruik van Saunders' verklaringen. Niettemin zal dit in Nederland niet snel het geval zijn, gezien de specifieke omstandigheden bij *Saunders*, zoals juryrechtspraak.

Omstandigheden

---

129 Zie bijvoorbeeld HR 21 oktober 1997, NJ 1998, 173 over inzage in bescheiden op grond van art. 19 WED, en HR 30 september 1998, NJ 1998, 104, over het gebruik van stukken die overhandigd zijn op grond van art. 50a lid 3 Organisatiewet sociale verzekering.

Analogieën en precedenten

Op grond van de beschreven gevallen, blijken wetgever en rechter[130] bij de beoordeling van de toelaatbaarheid van afgedwongen medewerking als bewijs de volgende omstandigheden in acht te nemen.

- Het **doel van de wetgeving**: welk belang beschermt de wet?
- De **aard en het bereik van de wetgeving**: is er sprake van commuun strafrecht, bijzonder strafrecht of bestuursrecht? Tot welke groep richt de wetgeving zich? Beslaat de wetgeving een klein of juist een relatief groot gedeelte van de maatschappelijke activiteit?
- Het **doel van de medewerkingsverplichting**: is deze primair ordenend (in het kader van toezicht op een zorgvuldige uitoefening van een maatschappelijke activiteit) of primair repressief (in het kader van bewijsgaring om daders van strafbare feiten te kunnen vervolgen)?
- De **mate van dwang**: wat is de strafbedreiging voor niet-medewerking? De mate van dwang hangt ook samen met het doel van de medewerkingsverplichting: bij ordenende wetgeving (zoals mestboekhouding) bestaat minder dwang dan bij repressieve wetgeving (zoals een uitleveringsplicht voor verdachten van belastingfraude).
- De **aard van de medewerking**: hoe betrouwbaar zijn de resultaten van de medewerking? Kan de medewerker invloed uitoefenen op het resultaat?
- **Subsidiariteit**: zijn er minder ingrijpende alternatieven om het doel van de medewerkingsplicht te bereiken? Valt het strafbare feit nog wel op te sporen zonder deze medewerkingsplicht?
- **Proportionaliteit**: zijn er voldoende waarborgen om de inbreuk tot een minimum te beperken? Zijn de voorwaarden voor de medewerkingsplicht voldoende strikt geformuleerd? Is er in het concrete geval niet te veel dwang uitgeoefend?
- De **invloed** van het gebruik van het bewijsmateriaal **op de proceshouding** van de verdachte: worden de resultaten van de medewerking dusdanig gebruikt dat de verdachte in het strafproces niet meer in vrijheid zijn proceshouding kan bepalen?

130 De rechter toetst het concrete geval, niet de wetgeving zelf, maar hij houdt in zijn toetsing van het concrete geval natuurlijk wel rekening met de omstandigheden die de wetgever ertoe hebben aangezet de medewerkingsplicht in te voeren.

6. Opties voor een ontsleutelplicht

Zoals de precedenten laten zien, zijn er verschillende manieren om meewerkingsplichten wettelijk vorm te geven, met een meer of minder vergaande inbreuk op nemo tenetur. In dit hoofdstuk geef ik een overzicht van de mogelijkheden om een wettelijke ontsleutelplicht in te voeren, waarbij ik aangeef welke variabelen binnen de opties afhangen van welke omstandigheden. Ik presenteer de opties in toenemende mate van inbreuk op nemo tenetur.

1. Een ontsleutelplicht voor niet-verdachten

Een bevel tot ontsleuteling kan aan een ieder worden gegeven, maar niet aan verdachten. Dit is de huidige situatie van art. 125 k lid 2 Sv. Voor vormen van actieve medewerking is dit in het commune strafrecht de regel.

2. Een ontsleutelplicht met verschoningsrecht[131]

Een ontsleutelbevel kan worden gericht tot een ieder (inclusief verdachten), maar de geadresseerde kan zich verschonen als hij zich door ontsleuteling zou blootstellen aan het gevaar van een strafrechtelijke veroordeling. Dit is de vorm van veel verklaringsplichten in het commune en bijzondere strafrecht, zoals het zwijgrecht van art. 29 Sv, de aangifteplicht bij bepaalde delicten, de spreekplicht voor getuigen in straf- en civiele zaken, de boete-gerelateerde verklaringsplicht in de AWR, en de plicht de onbekend gebleven bestuurder terzake van verkeersmisdrijven te noemen.

3. Een ontsleutelplicht met opsporingsingsuitsluitingsregel

Een ontsleutelplicht geldt voor eenieder, maar de resultaten mogen niet worden gebruikt voor de opsporing of vervolging van de geadresseerde. Deze constructie is alleen zinvol voor gevallen waarin de informatie nodig is voor de

131 In zeker opzicht is dit een "grotere inbreuk" op nemo tenetur dan de eerste optie, omdat het bevel aan verdachte kan worden gegeven. Aan de andere kant is dit een "kleinere inbreuk", omdat ook niet-verdachten zich kunnen verschonen, wat ze bij de eerste optie niet kunnen. Vanuit de verdachte bezien is vooral het eerste relevant, vandaar dat ik deze volgorde aanhoud.

opsporing en vervolging van anderen maar waarbij het gevaar bestaat dat de geadresseerd zich bloot zou stellen aan vervolging van een minder ernstig misdrijf. Dit is het geval bij de meldplicht ongebruikelijke transacties voor heling.

4. Een ontsleutelplicht met bewijsuitsluitingsregel

Een ontsleutelplicht geldt voor eenieder, maar de resultaten zijn niet toelaatbaar als bewijs in een strafzaak (of, algemener, in een zaak die valt onder het begrip "criminal charge" van art. 6 EVRM). Deze constructie is gebruikt bij de getuigplicht bij parlementaire enquêtes. Met enige fantasie zou men dit ook kunnen inlezen in de regeling van 551 Sv, de uitleverplicht ter verbeurdverklaring of onttrekking aan het verkeer, waaraan de waarheidsvinding expliciet is onttrokken. In het commune en bijzondere strafrecht is deze constructie echter ongebruikelijk, omdat daarbij meestal de waarheidsvinding en de vervolgingsmogelijkheid voorop staan.

5. Een ontsleutelplicht met bewijsuitsluiting onder voorwaarden

Een wettelijke regeling kan ook voorwaarden stellen waaronder ontsleutelde resultaten niet mogen meewerken aan het bewijs, bijvoorbeeld als een procedure die de betrouwbaarheid van de ontsleuteling moet waarborgen niet is gevolgd. (De verplichte bloedproef in het verkeer lijkt hierop, maar deze regeling bevat geen expliciete bewijsuitsluitingsregel ten aanzien van het onderzoek.) Omgekeerd kan een regeling ook voorwaarden stellen waaronder de resultaten *wel* toelaatbaar zijn, bijvoorbeeld als uit feiten en omstandigheden blijkt dat de geadresseerde beschikt over de kennis die nodig is voor ontsleuteling.[132]

6. Een ontsleutelplicht zonder bewijsbeperkingen

De meest vergaande regeling is een ontsleutelplicht zonder beperkingen ten aanzien van de geadresseerde of de toelaatbaarheid voor het bewijs. Dergelijke medewerkingsplicht zijn te vinden in bijzondere wetten: de bloedproef in het verkeer, de inlichtingen- en inzageplichten in de WWM en de medewerkings- en uitleverplichten in de AWR en de WED. Men zou ook de kentekenaansprakelijkheid voor verkeersovertredingen kunnen zien als een medewerkingsverplichting voor (mogelijk verdachte) kentekenhouders, waarbij het antwoord op de vraag wie bestuurde kan worden gebruikt tegen de

132 Een dergelijke voorwaarde zou tegemoet komen aan de eis van zekere uitvoerbaarheid, die uit *Funke* kan worden afgeleid.

kentekenhouder als hij toegeeft zelf te hebben bestuurd.[133] In het commune strafrecht komt deze constructie alleen voor bij duldplichten.

Binnen deze opties zijn er mogelijkheden om het *bereik* van de ontsleutelplicht te variëren.

A. Een ontsleutelplicht in het commune strafrecht

Een plicht kan ingevoerd worden in het commune strafrecht, zodat in het kader van elk strafrechtelijk onderzoek iemand bevolen kan worden te ontsleutelen. Dit ligt voor de hand bij onderzoeksbevoegdheden die bij veel soorten strafrechtelijk onderzoek nuttig of nodig kunnen zijn, zoals inbeslagneming, stelselmatige observatie of onderzoek aan lichaam of kleding. Naarmate de bevoegdheid zwaarder ingrijpt in fundamentele rechten van betrokkenen, moeten zwaardere voorwaarden voor de toepasbaarheid worden gesteld.

B. Een ontsleutelplicht in bijzondere wetgeving

Als een bevoegdheid slechts voor bepaalde soorten onderzoeken relevant is, of als deze nodig is in het kader van controle van bijzondere wetgeving, kan een medewerkingsplicht alleen in bepaalde bijzondere wetten worden opgenomen. Een voorbeeld hiervan is de blaas- en bloedproef in het verkeer. Een andere reden om een bevoegdheid in een bijzondere wet te regelen, is dat de voorwaarden voor uitoefening van die bevoegdheid in het commune strafrecht dermate streng zijn dat ze de goede handhaving van een bijzondere wet belemmeren. De bijzondere wet stelt dan minder zwaren voorwaarden voor uitoefening van een bevoegdheid die ook in het commune strafrecht voorkomt. Voorbeelden hiervan zijn de uitleveringsbevoegdheden in de AWR, WED en Opiumwet.

Een andere variabele is de manier waarop de plicht afgedwongen wordt: welk *handhavingsmechanisme* moet de wetgever kiezen?

i. Niet voldoen is strafbaar op grond van art. 184 Sr

Dit is het algemene vangnet om medewerkingsplichten te handhaven: wie opzettelijk niet voldoet aan een bevoegd gegeven ambtelijk bevel, is strafbaar op grond van art. 184 Sr met ten hoogste drie maanden.

ii. Niet voldoen is een zelfstandig strafbaar feit

133 Dit is strikt genomen geen medewerkingsplicht, maar een aansprakelijkheids-uitsluitingsgrond. Materieel komt het evenwel neer op een medewerkingsplicht voor kentekenhouders.

Een medewerkingsplicht kan ook worden gehandhaafd door een zelfstandige strafbaarstelling van niet-medewerking. Dit gebeurt met name als de strafbedreiging van 184 Sr als te gering ervaren wordt, zoals bij de medewerkingsverplichtingen in de AWR (zes maanden), of als deze juist te zwaar is, zoals bij het weigeren de onbekende bestuurder bij verkeersmisdrijven bekend te maken (twee maanden) of bij de verklaringsplicht voor verdachten in de WWM (alleen een geldboete).
Verder wordt een zelfstandige strafbaarstelling ook gebruikt om de straf te verbinden met het gronddelict dat onderzocht wordt. Dit kan door de delicten (gronddelict en weigering van medewerking) naast elkaar op te nemen in een strafbepaling, zoals bij de weigering van de bloedproef in het verkeer. Het kan ook in een bepaling die omstandigheden definieert waaronder de op het feit gestelde straffen uitgesproken kunnen worden tegen de medewerkingsweigeraar, zoals min of meer bij de kentekenaansprakelijkheid bij overtredingen het geval is.
Ten slotte zou een zelfstandige strafbaarstelling ook gebruikt kunnen worden om de opzeteis van art. 184 Sr te omzeilen, door (ook niet-opzettelijke) weigering strafbaar te stellen. Dit creëert een risico-aansprakelijkheid voor degenen die zich in situaties bevinden waarin een medewerkingsbevel zou kunnen worden opgelegd.

iii. Niet voldoen wordt meegewogen als bewijs in de hoofdzaak
Een weigering te voldoen aan een ontsleutelbevel kan door de rechter meegewogen worden in het bewijs. Er is in het Nederlandse strafrecht geen wettelijke regeling die iets dergelijks stipuleert, maar tot op zekere, zeer beperkte, hoogte kan de rechter de opstelling van de verdachte gebruiken in bewijsoverwegingen (zie 5.2.1.4). De wetgever kan overwegen een novum in te voeren door bijvoorbeeld een richtlijn uit te vaardigen dat de weigering te ontsleutelen (zoals blijkend uit een proces-verbaal) onder bepaalde voorwaarden door een rechter kan worden opgevat als een indicatie dat het versleutelde bestand belastende informatie bevat.

Gegeven deze drie dimensies, zijn er 6 x 2 x 3 = 36 varianten voor een wettelijke ontsleutelplicht, waarbij er natuurlijk voor combinaties kan worden gekozen (bijvoorbeeld een ontsleutelplicht met verschoningsrecht in het commune strafrecht en een zwaardere ontsleutelplicht in de AWR en WED). Elke variant kan nader worden ingeperkt door beperkende voorwaarden, zoals de mate van verdenking, de zwaarte van de vermoedelijk gepleegde strafbare feiten, de mate van benodigdheid voor het onderzoek, en de mate van waarschijnlijkheid dat de verdachte in staat is te ontsleutelen.

7. Handhaving en technische bezwaren

Om te bepalen welke variant het meest geschikt is gegeven de op het spel staande belangen, is een analyse nodig van de omstandigheden die nopen tot een ontsleutelplicht. Voordat ik zo'n analyse geef, zal ik echter eerst aandacht besteden aan de handhavingsmogelijkheden in relatie tot het (technische) realiteitsgehalte van een ontsleutelplicht. De technische beperkingen van ontsleuteling hebben namelijk consequenties voor de handhaafbaarheid, en het is daarom beter eerst in te schatten welk handhavingsmechanisme geschikt is voor een eventuele ontsleutelplicht, waardoor de nodige varianten kunnen afvallen als onrealistisch.

7.1 Opzet of risico-aansprakelijkheid?

Moet het niet voldoen aan een ontsleutelbevel alleen worden bestraft als iemand opzettelijk niet meewerkt, of moet dat zonder meer gebeuren? Met andere woorden: is het nodig opzet te vereisen voor de strafbaarstelling of voor het verbinden van belastende conclusies aan de weigering mee te werken? Dat is wel gebruikelijk in het strafrecht, en met reden. Medewerkingsplichten zijn altijd instrumenteel, en niet medewerken is dus niet *inherent* strafwaardig. Waar niet-medewerken een dermate negatieve invloed heeft op de mogelijkheid van de overheid om, bijvoorbeeld, strafbare feiten te vervolgen, is het wel redelijk om daaraan sancties te verbinden. Die sancties mogen echter in principe niet zover gaan dat ook onopzettelijk niet-meewerken bestraft wordt. De verantwoordelijkheid voor de opsporing van strafbare feiten ligt immers bij de overheid, dus als burgers niet kunnen meewerken, kan hun dat niet worden aangerekend.
Alleen in een enkel uitzonderingsgeval kan ook een niet-opzettelijke weigering om mee te werken worden bestraft. Dan rust er een risico-aansprakelijkheid op de aangesprokene: als hij zich in een situatie bevindt of begeeft waarin hij geadresseerde kan worden van een bevel tot medewerken, rust op hem de

verplichting om dat te doen, ongeacht of hij dat kan of niet. Als hij niet kan meewerken, had hij zich maar niet in zo'n situatie moeten begeven.
Een van de zeldzame voorbeelden van een dergelijke risico-aansprakelijkheid is de kentekenaansprakelijkheid bij Mulder-feiten (zie par. 5.2.1.3): de kentekenhouder wordt beboet, ongeacht of hij zou willen meewerken met justitie om de naam van de bestuurder bekend te maken.[134] De kentekenhouder moet hierbij zelf maar zien of en hoe hij de boete verhaalt op de bestuurder. Als hij het risico niet wil lopen om beboet te worden voor Mulder-overtredingen zonder dat hij de boete kan verhalen op de bestuurder van zijn auto, moet hij maar geen auto kopen, of moet hij er maar strikt op toezien dat zijn auto niet door personen wordt gebruikt waarop hij een verhaalsrecht niet zou kunnen uitoefenen. Dit is een vorm van risico-aansprakelijkheid, die volgens de Hoge Raad, blijkens een arrest uit 1993, is geoorloofd vanwege de bijzonderheden van het verkeer en de geringe dwang van de regeling: de massaliteit van de overtredingen, de beperkte mogelijkheden tot staandehouding om de bestuurder ter plekke te betrappen, het belang om wel tegen verkeersovertredingen te kunnen optreden, het feit dat meestal de kentekenhouder zelf de bestuurder was, naast de verhaalsmogelijkheden van de kentekenhouder en de beperkte omvang van de financiële sanctie.[135]
Dit zijn op zich valide argumenten, maar toch kleeft er een bezwaar van onrechtvaardigheid aan een dergelijke regeling: het beginsel "geen straf zonder schuld" wordt losgelaten, zoals Corstens in zijn annotatie bij dit arrest de Hoge Raad verwijt. Kennelijk acht de Hoge Raad in dit geval de noodzaak om verkeersovertredingen te kunnen bestraffen belangrijker dan het feit dat hiermee een geringe inbreuk op het fundamentele beginsel wordt gemaakt.
Analoog daaraan, zou men kunnen redeneren dat ook voor encryptie een risico-aansprakelijkheid ingevoerd zou kunnen worden. Wie cryptografie gebruikt en ooit in aanraking komt met justitie, zal ervoor moeten zorgen dat hij in staat is te ontsleutelen op bevel, als hij niet het risico wil lopen gestraft te worden voor decryptieweigering. Stel dat iemand regelmatig berichten stuurt naar een nieuwsgroep waarin ook kinderporno wordt uitgewisseld. Dan kan de verdenking ontstaan dat deze persoon kinderporno bezit. Worden vervolgens bij een huiszoeking op zijn harde schijf versleutelde gegevens aangetroffen die de persoon niet kan ontsleutelen, dan heeft justitie geen mogelijkheden meer om aan te tonen dat de verdachte kinderporno bezit. De redenering, analoog aan de kentekenaansprakelijkheid, zou dan kunnen luiden: kinderporno moet worden bestreden, het is moeilijk tot onmogelijk aan te tonen dat iemand kinderporno bezit als hij cryptografie gebruikt, wie versleutelde bestanden op de harde schijf

134 Ondanks de overheveling van deze feiten naar het bestuursrecht, is er bij deze boeten nog steeds sprake van een straf.
135 HR 15 juli 1993, NJ 1994, 177 m.nt. C.

opslaat zal in het algemeen in staat zijn die te ontsleutelen, dus als een verdachte van kinderpornobezit op zijn harde schijf een versleuteld bestand heeft dat hij weigert te ontsleutelen, moet hij maar worden gestraft voor de decryptie-weigering.
Om vele redenen gaat de vergelijking met de Mulder-aansprakelijkheid niet op. De argumenten van de Hoge Raad voor de toelaatbaarheid van art. 5 WAHV zijn nauwelijks van toepassing op cryptografie, zelfs niet als de risico-aansprakelijkheid voor de opsporing van een beperkt aantal specifieke delicten zou gelden. Men kan niet volhouden dat zonder de crypto-risico-aansprakelijkheid nauwelijks tegen strafbare feiten zou kunnen worden opgetreden, terwijl er in dit geval geen verhaalsmogelijkheden zijn voor de cryptogebruiker om de straf op iemand anders af te wentelen, en het bovendien niet om een kleine boete gaat, maar om een (mogelijk forse) gevangenisstraf. Met andere woorden: een risico-aansprakelijkheid voor cryptogebruik past niet in het systeem van de huidige wetgeving.
Er zijn ook geen argumenten om in dit geval te breken met het systeem en een vergaande inbreuk op het beginsel "geen straf zonder schuld" toe te laten. Cryptografie is immers op geen enkele manier in zichzelf gevaarzettend – anders dan bij auto's, waarvan men nog wel kan volhouden dat het besturen als zodanig enig risico voor de maatschappij met zich meebrengt (namelijk gevaar voor het leven van weggebruikers). Van een kentekenhouder kan men daarom nog wel beweren dat hij een zekere zorgplicht heeft om te voorkomen dat hij zijn auto uitleent aan personen die daarmee de verkeersveiligheid in gevaar kunnen brengen; van cryptografiegebruikers kan men evenwel niet beweren dat die op enige manier als zodanig een risico voor de maatschappij opleveren. Een risico-aansprakelijkheid voor cryptografie moet daarom van de hand worden gewezen.

Deze conclusie heeft tot gevolg dat alleen het opzettelijk niet-meewerken aan een ontsleutelbevel bestraft zou kunnen worden.

7.2 In staat zijn te ontsleutelen

Wil een ontsleutelweigering bestraft worden, dan zal het OM dus in elk geval opzet moeten bewijzen.[136] Iets opzettelijk niet doen vereist dat er in elk geval de mogelijkheid bestaat om het wél te doen. De verdachte kan dus alleen opzettelijk weigeren als hij op het moment van het bevel in staat is te ontsleutelen.

136 Bij de derde soort sanctie, gebruik van de weigering als bewijs in de hoofdzaak, hoeft dat strikt genomen niet, maar wil de rechter de weigering meewegen, dan zal hij wel overtuigd moeten zijn dat de verdachte opzettelijk weigerde.

Daarom zal het OM moeten hardmaken dat de verdachte in staat was te ontsleutelen.[137]

Het bewijs daarvan zal komen van enkele algemene regels en van concrete omstandigheden. De *algemene ervaringsregels* vóór de mogelijkheid te ontsleutelen zijn de volgende.

- Men slaat alleen iets versleuteld op zijn harde schijf op, als men het in de toekomst nog kan ontsleutelen. Een cryptobestand dat niet kan worden ontsleuteld neemt alleen maar zinloze ruimte in.
- Men verstuurt alleen versleutelde berichten als die ontsleuteld kunnen worden. Het heen en weer sturen van onleesbare gegevens legt alleen maar zinloos beslag op de netwerkcapaciteit.
- De eigenaar van een versleuteld bestand en de ontvanger van een versleuteld bericht kunnen dat in de regel ontsleutelen.

Daarnaast zullen in een concreet geval bepaalde *omstandigheden* op de mogelijkheid te ontsleutelen kunnen wijzen.

- De verdachte is een geoefend gebruiker van cryptografie.
- De verdachte is een professioneel gebruiker van cryptografie.
- De sleutel om te ontsleutelen is onlangs aangemaakt.
- De verdachte heeft de sleutel die nodig is om te ontsleutelen nog onlangs gebruikt.
- De verdachte gaat in zijn dagelijkse leven zorgvuldig om met informatiestromen.
- De verdachte is, bijvoorbeeld door de systeembeheerder, gewaarschuwd voor de gevaren van het verlies van de decryptiesleutel of het vergeten van het wachtwoord.
- De verdachte heeft een uitstekend geheugen.
- De verdachte heeft op zijn werk nog nooit zijn wachtwoord vergeten.
- De verdachte gebruikt al jaren lang hetzelfde sleutelpaar.

Tegenover deze argumenten die het OM kan aanvoeren, staan de verdachte diverse verklaringen ter beschikking voor het niet kunnen ontsleutelen. *Algemene ervaringsregels* tégen de mogelijkheid te ontsleutelen zijn bijvoorbeeld de volgende.

- Mensen nemen niet de moeite verouderde of onbruikbare bestanden van hun harde schijf te wissen. De opslagcapaciteit neemt dermate snel toe, dat gebruikers gegevens van oude harde schijven copiëren naar nieuwe harde schijven zonder acht te slaan op de bruikbaarheid van oude bestanden.
- Vanuit beveiligingsoogpunt moet men een moeilijk te raden wachtwoord kiezen en mag men dat wachtwoord niet ergens opschrijven.

---

137 Dit is dezelfde eis als het centrale criterium uit *Funke* dat de politie zeker moet weten dat uit te leveren goederen bestaan. Zie par. 4.1.

- Moeilijk te raden wachtwoorden zijn moeilijk te onthouden.
- Hoe meer wachtwoorden iemand gebruikt, hoe moeilijker het is deze allemaal te onthouden.
- Hoe minder men een wachtwoord actief gebruikt, hoe sneller men dit vergeet.
- Mensen krijgen via het Internet allerlei handelsreclame toegestuurd van onbekenden, waarbij soms bijlagen zijn bijgevoegd die men gevraagd wordt te lezen.

Verder kan een verdachte diverse *omstandigheden* aanvoeren die verklaren waarom hij niet kan ontsleutelen. Zulke omstandigheden worden steeds aangevoerd door mensen die skeptisch zijn over de effectiviteit van een ontsleutelplicht. In de vele discussies die ik gevoerd heb over dit onderwerp, ben ik steeds gestuit op allerlei tegenwerpingen die beargumenteren waarom het OM in het algemeen niet in staat zal zijn de ontsleutelmogelijkheid van verdachte hard te maken. Wil het OM iemand laten veroordelen voor decryptieweigering, dan zal het in elk geval deze tegenwerpingen moeten ontkrachten. Ik ga daarom in deze paragraaf uitvoerig in op de tegenwerpingen en mogelijke ontkrachtingen daarvan.

1. Ik ben mijn wachtwoord vergeten!

Dit is de meest voor de hand liggende tegenwerping. De bal ligt dan weer bij het OM, die omstandigheden zal moeten aanvoeren waarom de verdachte zich toch het wachtwoord zou herinneren; het OM kan daarbij de bovengenoemde ervaringsregels en concrete omstandigheden in stelling brengen. Als het OM hierdoor aannemelijk maakt dat deze persoon in dit geval zijn wachtwoord nog zou moeten kennen, is de verdachte weer aan zet. Hij kan dan, mede op basis van de ervaringsregels, bijvoorbeeld zeggen:

- Ik gebruik zoveel wachtwoorden (voor de toegang op mijn werk, voor toegang thuis, voor mijn schermbeveiliger, voor mijn tekstverwerkingsprogramma enzovoorts), terwijl ik niet zo vaak cryptografie gebruik.
- Ik had, zoals het programma PGP mij aangeraden had, een heel moeilijk wachtwoord van 16 karakters gekozen. Ik dacht toch echt dat het "ekj(2kd&,##ioaz!" was, of was het nou "ekj2)kd&,##ioza?"? Ik had een ezelsbruggetje verzonnen, maar wat was dat ook maar weer?
- Ik ben net terug van vijf weken vacantie.
- Tsja, ik ben nogal vergeetachtig.

Ik vermoed dat, tenzij er sprake is van een professionele, zorgvuldige cryptogebruiker en er aanwijzingen zijn dat de sleutel nog onlangs is gebruikt, het OM deze strijd gaat verliezen.

2. Ik gebruik al lang een ander sleutelpaar!

Als de verdachte aangeeft in de loop der tijd diverse sleutelparen te hebben gebruikt, en dat hij nooit de moeite heeft genomen oude bestanden die hij niet meer nodig had te wissen van de harde schijf, zal het OM aannemelijk moeten maken dat het versleutelde bestand versleuteld is met een paar dat nog in gebruik is. Een programma als PGP geeft in principe aan met welk sleutelpaar een bericht is versleuteld, maar niet altijd valt aan een versleuteld bestand af te lezen welke sleutel is gebruikt. Het OM wint dit alleen als er technisch bewijs is dat het bewuste bestand versleuteld is met een recent gebruikt sleutelpaar, hetgeen mij slechts in zeldzame gevallen mogelijk lijkt.

3. Ik heb dat nooit kunnen ontsleutelen!

De verdachte kan bijvoorbeeld beweren:

- Iemand heeft mij dat bericht gestuurd, maar ik kon het niet ontsleutelen met mijn programma. Misschien heeft de zender het met de verkeerde sleutel versleuteld, of is er tijdens het transport over het Internet mee geknoeid.
- Dat is een bestand dat ik volgens mij ooit heb gekregen bij een e-bericht met handelsreclame. Het ging om een methode om snel rijk te worden. Ik heb het bestand toen opgeslagen op mijn harde schijf, maar ik snapte er niks van. Ik wilde toen aan mijn zoon vragen of hij het bestand leesbaar kon maken, maar daar ben ik nooit aan toegekomen.
- Dat bericht dat u heeft afgetapt komt van iemand die een wrok tegen mij koestert. Hij stuurt mij af en toe gekke bestanden op, in de hoop dat ik ooit veroordeeld word voor een decryptieweigering.[138]

Dergelijke tegenwerpingen klinken misschien niet aannemelijk, maar de verdachte komt wel het voordeel van de twijfel toe. Het OM zal dus minstens aannemelijk moeten maken dat het bestand niet op deze manier in het bezit van verdachte kwam. Dat zal een technische aangelegenheid zijn.

4. Ik heb net de sleutel vernietigd!

De aanval is de beste verdediging.

---

138 Iets soortgelijks overkwam de Britse Minister van Binnenlandse Zaken Jack Straw bij een protestactie tegen de Electronic Communications Bill (ECB, zie par. 3.2). Straw kreeg van de organisatie Stand een brief toegestuurd die een bekentenis van een misdaad zou bevatten, versleuteld met een sleutelpaar dat Stand op Straws naam had aangemaakt. Stand had vervolgens hun exemplaar van het sleutelpaar vernietigd, en de Metropolitan Police bericht dat Straw in het bezit was van strafrechtelijk relevante informatie. Onder de omstreden voorgestelde regeling van section 10 van de ECB zou Straw nu twee jaar de bak in kunnen draaien, omdat hij nooit zou kunnen bewijzen dat hij de sleutel tot de bekentenis niet had – wie weet had Stand hem die wel afzonderlijk toegestuurd. Met deze actie protesteerde Stand tegen de vergaande regeling, met name tegen de omkering van de bewijslast van het al dan niet in staat zijn te ontsleutelen. Stand 1999.

- Ik heb de sleutel net vernietigd toen ik jullie politiewagen zag aankomen en het geklop op de deur hoorde. Hij stond op dit schijfje, dat ik net geformatteerd heb.
- Nadat jullie een huiszoeking gedaan hadden, diskettes in beslag hadden genomen en mijn harde schijf hadden gecopieerd voor bestudering op het bureau, heb ik de sleutel vernietigd – die stond op een diskette die ik aan de buren in bewaring had gegeven. (Gnuif.)

Het vernietigen van een sleutel uit vrees voor de politie is natuurlijk verdacht, maar de verdachte was toch al verdacht, dus meer dan een extra verdenking zal dit niet opleveren (in elk geval niet voldoende om de sprong van bijna genoeg naar genoeg bewijsmateriaal te kunnen maken, als omkering van de bewijslast al in aanmerking zou komen). Immers, op de vraag waarom hij de sleutel vernietigde, kan de verdachte in een drugszaak bijvoorbeeld antwoorden:

- Ik was bang dat jullie mijn versleutelde dagboek zouden lezen; er staan nogal expliciete erotische passages in. In paniek heb ik daarom de sleutel vernietigd toen ik jullie zag aankomen.
- Ik had een paar versleutelde pornoplaatjes op de computer, waarvan sommige van jongens van een jaar of zestien. Ik wilde niet het risico lopen vervolgd te worden voor kinderporno.
- Ik beken: ik ben een racist. Ik heb *Mein Kampf* versleuteld op mijn computer staan.[139]

Dit lijken mij legitieme verklaringen voor de aanwezigheid van versleutelde bestanden op de computer en voor het vernietigen van een sleutel. Een veroordeling voor decryptieweigering op grond van *culpa in causa* lijkt mij daarom in deze gevallen te ver gaan, tenzij er sterke aanwijzingen zijn dat de versleutelde bestanden geen erotische dagboeken, dubieuze plaatjes of racistische teksten zijn, maar belastende informatie bevatten over het drugsdelict. Dat lijkt mij vrijwel onmogelijk aannemelijk te maken.

Voorwaarde voor dit verweer is wel dat de verdachte anticipeert op de huiszoeking en zijn sleutel op een apart schijfje of bijvoorbeeld een *remote server* opslaat, en alert genoeg is om de sleutel tijdig te vernietigen.

---

139 De verdachte loopt met deze bekentenis natuurlijk wel het risico van veroordeling voor het in voorraad hebben van een racistisch geschrift (art. 137e Sr), maar neemt die lagere strafdreiging op de koop toe, zeker vanwege de minimumbewijsregel dat alleen een bekentenis niet volstaat (art. 341 lid 4 Sv).

Als een verdachte dit verweer zou voeren zónder eerst de sleutel te hebben vernietigd, zal justitie hem vragen zijn bewering te staven door het bestand toch te ontsleutelen, desnoods na een toezegging van niet-vervolging voor racisme. Verweren in de zin van "Maar dit bestand is helemaal niet relevant voor uw onderzoek!" zullen daarom niet slagen.

5. *De sleutel ligt in vijftien stukjes opgeslagen over de hele wereld. Hier heeft u de (e-post)adressen van de houders.*

Er zijn crypto-systemen met een drempelschema: de sleutel wordt in stukjes geknipt en over verscheidene mensen verspreid; voor reconstructie van de sleutel is een minimum-aantal van deze stukjes nodig. Een verdachte kan bijvoorbeeld kiezen voor een 9-uit-15-drempelsysteem (vijftien stukjes, waarvan negen nodig zijn voor reconstructie). Niet praktisch in het gebruik, maar wel zo veilig. Als een verdachte dit verweer voert en vijftien adressen geeft, zullen vele rechtshulpverzoeken nodig zijn. De politie zal de sleuteldeeltjes uit de Kaaimaneilanden, Puka-Puka en Irak wel kunnen vergeten, zodat ze moeten hopen dat van de twaalf overgeblevenen minstens negen personen niet verhuisd zijn, hun wachtwoorden niet vergeten hebben én willen meewerken. En wat als vijf adressen niet blijken te kloppen? De verdachte leunt ondertussen rustig achterover.

6. *Maar natuurlijk wil ik dat ontsleutelen. Ziet u maar!*

De politie ziet de verdachte ontsleutelen en krijgt een erotisch dagboek, een dubieus plaatje van een net-niet minderjarige of een hoofdstuk uit *Mein Kampf* te zien. Interessant, maar niet wat de politie zocht.

Er bestaat een mogelijkheid voor de verdachte om een versleuteld bestand te "ontsleutelen" naar een andere tekst dan de oorspronkelijke. Hij moet dat voorbereid hebben door een bepaald cryptosysteem te gebruiken (het One Time Pad) en door een sleutel te hebben gegenereerd die het versleutelde bestand "ontsleutelt" naar het drogbestand.[140] Het gebruik van dit systeem is ongebruikelijk, dus de verdachte zal misschien moeten uitleggen waarom hij zo'n systeem gebruikt en hoe hij aan de sleutel is gekomen. Maar met een beetje geluk treft hij een argeloze politie-agent, die de mogelijkheid ontgaat dat hij beduveld wordt – zeker als het resultaat van de ontsleuteling lichtelijk belastend is voor een relatief onschuldig delict.

Naast de tegenwerpingen over het niet in staat zijn te ontsleutelen, kan de verdachte aanvechten dat het hier om versleutelde gegevens gaat.

7. *Wie zegt dat dit versleutelde gegevens zijn?*

Een cijfertekst is meestal ingebed in andere, wel leesbare informatie (*header-informatie*), om het crypto-programma en de crypto-gebruiker houvast te geven.

Zo beginnen PGP-berichten standaard met:

---

140 Zie Koops 1998, p. 47, voor een voorbeeld.

-----BEGIN PGP MESSAGE-----
*Version: PGP for Personal Privacy *.**

Nu kan een gebruiker dergelijke *header*-informatie weggehaald hebben, waardoor aan de tekst niet meer te zien valt of en zo ja met welk programma de tekst versleuteld is. Het OM zal dan moeten aantonen dat het wel om versleutelde gegevens gaat. Als elke vorm van *header*-informatie ontbreekt, is het technisch niet mogelijk te bewijzen dat het een cryptografische cijfertekst is,[141] al kan het misschien door externe factoren wel aannemelijk gemaakt worden (de aanwezigheid van een crypto-programma op de harde schijf, van crypto-handboeken in de boekenkast, de aanwezigheid van andere, wel evident versleutelde bestanden, een bericht van iemand "Heb je dat versleutelde bericht van mij van gisteren nog gelezen?"). Dit verweer van verdachte zal volgens mij vaak slagen, maar een voorwaarde is wel dat de verdachte vooraf de moeite heeft genomen alle *header*-informatie te verwijderen. Dat is onpraktisch en vergt enige technische kennis, maar het is voor een vastberaden, achterdochtige en slimme misdadiger niet ondenkbeeldig.

8. Maar dit zijn random *gegevens!*

Versleutelde gegevens, mits ze met een goed crypto-programma zijn versleuteld, hebben dezelfde eigenschappen als willekeurige (*random*) gegevens. Dit komt omdat een aanvaller, als een cijfertekst *niet* willekeurig zou zijn, de patronen die erin zitten kan gebruiken om de tekst te kraken. De cijfertekst zelf ziet er dus uit als willekeurige gegevens. Dit verweer vereist wel dat de *header*-informatie verwijderd is (zie verweer 7); het zou een aanvullend verweer kunnen zijn als het OM door externe factoren (crypto-handboeken en andere versleutelde bestanden op de harde schijf) aannemelijk zou maken dat hier cryptografie is gebruikt.

Als een verdachte dit verweer voert, zal hij wel de redelijke vraag moeten beantwoorden: "Maar waarom heb je willekeurige gegevens op je harde schrijf staan?", of: "Waarom stuur je willekeurige gegevens over het Internet?" De verdachte kan daarop bijvoorbeeld het volgende zeggen.

- Ik ben erg geïnteresseerd in cryptografie en crypto-analyse (kijk maar naar mijn boekenkast), en in dat kader bestudeer ik de eigenschappen van *random* getalreeksen.

---

141 De enige manier om dat te bewijzen is om door het invoeren van de (cijfer?)tekst in een cryptoprogramma met een bepaalde sleutel een begrijpelijke, zinvolle tekst te voorschijn te toveren; de kans dat een reeks willekeurige karakters in een crypto-systeem ontsleutelt naar een zinvolle tekst is dermate klein, dat de enige mogelijkheid is dat de onleesbare gegevens de versleuteling waren van die zinvolle tekst. Als het OM dit echter lukt, ontvalt de reden voor een veroordeling voor decryptieweigering, omdat het doel daarvan juist was de klare tekst te achterhalen.

- Ik ben misschien wat paranoïde, maar ik gebruik een vergaande vorm van beveiliging om te voorkomen dat mijn concurrent Connie weet wanneer ik berichten stuur aan Anton, mijn aandelenbeheerder. Elke dag stuur ik een bericht met willekeurige gegevens naar Anton; alleen als ik een opdracht wil doorgeven, stuur ik hem een versleuteld bericht. Connie kan aan de gegevens niet zien of ze willekeurig of versleuteld zijn, dus ze weet nooit wanneer ik opdrachten geef om aandelen te verhandelen.
- Als ik bestanden wis van mijn harde schijf, doe ik dat extra goed, zoals beveiligingsexperts aanraden. De computer wist normaliter een bestand door het etiket weg te halen, maar daarmee blijft het bestand nog wel achter op de harde schijf. Om zeker te weten dat de bestanden weg zijn, overschrijf ik ze daarom met reeksen willekeurige getallen.

Dit zijn weliswaar in het algemeen geen sterke argumenten, maar slimme misdadigers kunnen hun voorzorgsmaatregelen treffen om deze verweren aannemelijker te maken.

Van alle genoemde verweren, is het eerste (wachtwoord vergeten) aannemelijk en kansrijk, terwijl het tweede (sleutelpaar niet meer in gebruik) ook overtuigend kan zijn. De overige verweren zijn onwaarschijnlijker, maar kunnen in omstandigheden slagen, vooral als de geadresseerde voorzorgsmaatregelen heeft getroffen.
En dat is het punt. Misdadigers die cryptografie gebruiken, zullen die voorzorgsmaatregelen gaan treffen. Een ontsleutelplicht met een sanctie op niet-naleving beoogt vooral berekenende misdadigers aan te pakken. Als die de moeite nemen om belastende gegevens te ontsleutelen, dan doen zij dat om zich aan oog en oor van justitie te onttrekken. Ze zijn er bewust mee bezig. Aannemend dat zij weten dat een ontsleutelplicht gesanctioneerd wordt (iedereen wordt immers geacht de wet te kennen), zullen zij vaak ook bewust proberen om aan een mogelijk toekomstig ontsleutelbevel te ontkomen. Ze zullen veel wachtwoorden gebruiken, regelmatig sleutelparen verversen en vijf weken op vacantie gaan, versleutelde bestanden en berichten antedateren tot vijf jaar eerder, sleutels op diskettes bij de buren opslaan, interesse gaan kweken voor de wiskundige eigenschappen van willekeurige getalreeksen en wat niet al.
Bovendien zal er een markt ontstaan voor cryptografieproducten waarbij het achteraf ontsleutelen onmogelijk of onaannemelijk is. Nu al wordt in de cryptografische wereld hard gewerkt aan dergelijke systemen voor *perfect forward secrecy*. Bij een wettelijk gesanctioneerde ontsleutelplicht zal de roep om "anti-ontsleutelbevel"-cryptografie aanzienlijk toenemen.[142] Hulpmiddelen die auto-

[142] Een voorbeeld is de introductie van "chaffing and winnowing", een methode die Ron Rivest in 1998 introduceerde om decryptiebevelen onderuit te halen. Dit is een systeem waarin Annie en Bob ondertekende berichten ('koren') uitwisselen vermengd met 'kaf' (wille-

matisch cijferteksten van *header*-informatie ontdoen, zullen via het Internet hun weg vinden. Systemen zullen worden ontwikkeld die automatisch ontsleuteling onmogelijk maken enkele dagen na verzending van een bericht. Cryptosystemen met drempelschema's zullen gemeengoed worden, met netwerken over de hele wereld om elkaars sleutels te bewaren. Niet alle misdadigers zullen de moeite nemen om zich in deze circuits en technieken te verdiepen, maar hoe zwaarder de straf op decryptieweigering, hoe meer misdadigers voorzorgsmaatregelen zullen treffen.

Voor wie is een ontsleutelplicht met straf op weigering dan nodig én nuttig? De slimme, georganiseerde en zorgvuldige misdadiger die bewust cryptografie gebruikt om de politie dwars te zitten, zal waarschijnlijk afdoende voorzorgsmaatregelen treffen om zijn weigering te ontsleutelen aannemelijk te kunnen maken.[143] De iets minder slimme of voorzichtige, maar wel berekenende misdadiger zal niet anticiperen, maar zal bij een ontsleutelbevel al snel uitroepen "Wachtwoord vergeten!". Blijven over de minst slimme, onvoorzichtige en onberekenende misdadigers. Dergelijke boeven gebruiken (nog?) niet zo snel cryptografie, maar als ze dat wel doen, zal een ontsleutelbevel met zware strafdreiging zeker niet het laatste redmiddel zijn voor de politie. Ze zullen een makkelijk raadbaar wachtwoord hebben gekozen, hun wachtwoord hebben opgeschreven, of slechte cryptografie hebben gebruikt.[144] Als dat niet zo is, dan zullen ze zich wellicht makkelijker laten ompraten bij een verhoor om toch maar het wachtwoord te geven, of ze kunnen ten prooi vallen aan één van de trucs van de doorgewinterde opspoorder: de "four o'clock knock" (bel midden in de nacht aan en vraag de slaperige deuropener op de man af wat zijn wachtwoord is). En als ze desondanks volharden in een vergeet-verweer, dan zal de rechter ze wel moeten laten gaan: niet zo slimme boeven hebben immers meestal ook niet zo'n goed geheugen.

---

keurige gegevens). Hun berichten worden dus niet versleuteld met een sleutel, maar vermengd met willekeurige, niet-ondertekende gegevens. Annie en Bob gebruiken een gemeenschappelijke, geheime authenticatie-sleutel waarmee zij zelf het kaf van het koren kunnen scheiden. Aangezien politie-agente Paulien niet mag vragen om uitlevering van handtekening-sleutels (anders zou zij berichten van Annie of Bob kunnen namaken), kan ze alleen maar vragen aan Annie of Bob om het kaf van het koren te scheiden. Ze heeft echter geen mogelijkheid om te controleren of ze kaf of koren krijgt. Zie Rivest 1998.

143 Boeven uit deze kategorie gebruiken vooralsnog weinig cryptografie, omdat er andere middelen zijn om de politie te dwarsbomen: vele mobiele telefoons uit het buitenland met vooruitbetaalde kaarten tegen telefoontaps, en zo weinig mogelijk belastende informatie opslaan tegen computeronderzoek.

144 Volgens het overzicht van Denning & Baugh 1999 vallen vooralsnog de meeste cryptoboeven in deze kategorie.

7.3 Conclusie

Ik concludeer dat de handhaving van een ontsleutelplicht problematisch is. Of er nu gekozen wordt voor een (al dan niet zelfstandige) strafbaarstelling van decryptieweigering of voor omkering van de bewijslast (die ik ook maar aanduid als "straf op decryptieweigering"), in beide gevallen is opzet een vereiste. Voor dat opzet zal het OM moeten aantonen dat er versleutelde gegevens zijn en dat de verdachte in staat is te ontsleutelen. Berekenende misdadigers hebben legio mogelijkheden om voorzorgsmaatregelen te treffen waardoor zij bij een ontsleutelbevel voldoende aannemelijk kunnen maken dat zij niet in staat zijn het bevel op te volgen. Minder berekenende misdadigers kunnen ter plekke uitroepen dat ze het wachtwoord vergeten zijn, hetgeen een zware bewijslast op het OM legt om aannemelijk te maken dat dat niet zo is. Bovendien zijn er bij minder berekenende misdadigers ook alternatieven om toch de klare tekst te achterhalen.

Dit betekent dat, als een ontsleutelplicht gesanctioneerd moet worden, er geen hoge straf kan staan op niet-naleving. Een hoge straf zal immers een des te zwaardere bewijslast bij het OM leggen om aan te tonen dat de verdachte toch in staat is te ontsleutelen, terwijl het tegelijk berekenende misdadigers er des te meer toe zal aanzetten om technieken te ontwikkelen en gebruiken die aannemelijk maken dat zij niet kunnen ontsleutelen. Voor de niet-berekenende, minder slimme misdadigers is een hoge straf disproportioneel, omdat er bij hen andere middelen zijn om het wachtwoord te achterhalen of anderszins voldoende bewijs te vergaren; ook zij zullen zich makkelijk kunnen verschuilen achter een vergeet-verweer.

Op grond hiervan concludeer ik dat een omkering van de bewijslast niet in aanmerking kan komen als nalevingsmiddel, en dat, als er al een zelfstandige straf gesteld zou moeten worden op een decryptieweigering, deze straf niet hoger zou moeten zijn dan de strafdreiging van 184 Sr: drie maanden. Dit zal in het algemeen geen serieuze strafdreiging zijn: de vergaarde versleutelde informatie is vaak verkregen door toepassing van dwangmiddelen die alleen bij voorlopige-hechtenismisdrijven mogen worden toegepast: misdrijven met een veel hogere straf dan drie maanden.

8. Afweging

Ik heb tot nu toe diverse lijnen uitgezet, die moeten meespelen in de afweging van de wetgever om al dan niet een ontsleutelplicht voor verdachten in te voeren. Deze lijnen zijn:

- de context van de bevoegdheid: het cryptoprobleem (hfd. 2);
- de internationale context: de bevoegdheid in andere landen (par. 3.2);
- de reikwijdte van de huidige bevoegdheden: hoe effectief is de huidige ontsleutelplicht voor niet-verdachten (par. 3.1), en kan de politie versleutelde berichten niet gewoon kraken?;
- de reikwijdte en achtergrond van het nemo-teneturbeginsel (hfd. 4);
- het systeem van de wet: welke inbreuken zijn tot nu toe toegelaten op het nemo-teneturbeginsel en welke omstandigheden hebben daarbij een rol gespeeld? (hfd. 5);
- handhavingsperikelen: hoe en in hoeverre zou een ontsleutelplicht te handhaven zijn? (hfd. 7);
- opties voor een ontsleutelplicht: hoe kan zo'n plicht eruit zien? (hfd. 6).

In dit hoofdstuk vat ik de bevindingen uit deze lijnen samen en breng ik de resultaten met elkaar in verband. Daarbij geef ik nog enkele aanvullende overwegingen die de wetgever in zijn afweging moet betrekken.

1. De context

De vraag of een ontsleutelplicht voor verdachten moet worden ingevoerd maakt deel uit van het "crypto-probleem": 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). Het is te beperkt om de ontsleutelplicht alleen te zien in het licht van het nemo-teneturbeginsel, omdat bij de andere oplossingsrichtingen ook andere grondrechten (met name privacy) op het spel staan. Daarom moet meer waarde worden gehecht aan de argumenten van degenen die de ontsleutelplicht in de brede context van de cryptocontroverse hebben gezien, dan aan degenen die de

ontsleutelplicht sec tegen het nemo-teneturbeginsel hebben bekritiseerd (zie par. 3.1).

Twee aandachtspunten in deze brede context zijn de volgende.

- Hoe **ernstig** is het probleem? Op **welke manieren** hindert cryptografie precies de opsporing? Welk **soort misdrijven** en welk **soort verdachten** komt de politie vooral tegen? De feitelijke mate en aard van hinder zijn belangrijke factoren voor de wetgever in de afweging. Openbare gegevens ontbreken voor Nederland om hierop in de context van dit onderzoek afdoende antwoord te geven. Mijn indruk, gebaseerd op openbare bronnen en enkele gesprekken met mensen uit de opsporingspraktijk, is dat het probleem vooralsnog niet ernstig is. Cryptografie hindert tot nu toe slechts weinig opsporingsonderzoeken, laat staan dat in concrete zaken de vervolging van misdaden erdoor definitief geblokkeerd wordt. Maar men moet wel rekening houden met de technische ontwikkelingen: cryptografie wordt binnenkort ingebouwd in diverse algemeen beschikbare computer-programma's, zodat het cryptogebruik door misdadigers waarschijnlijk aanzienlijk zal toenemen.
  Het is wenselijk dat de wetgever eerst deze vraag beantwoordt, alvorens een besluit te nemen over een ontsleutelplicht voor verdachten. De argumenten die de wetgever tot nu toe heeft gehanteerd over de cryptocontroverse vinden onvoldoende onderbouwing in de praktijk – het zijn veeleer theoretische argumenten (áls misdadigers cryptografie gebrui-ken, kan dat een groot probleem zijn) of een drogreden (iedereen roept dat het een probleem is, dús het is een probleem). De wetgever zou daarom, bijvoorbeeld het WODC, opdracht moeten geven een studie uit te voeren naar het vóórkomen van cryptografie in de opsporingspraktijk.
- In hoeverre is dit een **uitzonderlijk probleem** dat om een specifieke bevoegdheid vraagt? Waarin verschilt cryptografiegebruik van geheimschriften die al eeuwen voorkomen, of van kluizen waarin misdadigers geheimen kunnen opbergen? Cryptografie is op zich niets nieuws, maar verschilt wel in de schaal van het probleem. Cryptografie is makkelijker en breder bruikbaar dan geheimschrift (zie par. 5.1.1), terwijl het bij goed gebruik niet te kraken valt, in tegenstelling tot brandkasten en kluizen. Om die reden kan het cryptoprobleem wel degelijk roepen om een specifieke bevoegdheid.

De bevindingen van de context suggereren 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 zijn, maar dat de ernst en aard

van het probleem vooralsnog geen gewichtige redenen lijken te vormen voor een inbreuk op een rechtsbeginsel. Die ernst en aard van het probleem zouden eerst beter in kaart moeten worden gebracht.

2. De internationale context

De internationale context laat zien dat de cryptocontroverse in vele landen speelt, waarbij een ontwikkeling gaande is van sleuteldepotmechanismen naar een ontsleutelplicht, al dan niet voor verdachten. Tot dusver zijn er echter geen landen die een ontsleutelplicht voor verdachten hebben ingevoerd. Wel is in het VK een voorstel gedaan daarvoor, dat echter sterke weerstand heeft opgeroepen.

De internationale context suggereert dat een ontsleutelplicht voor verdachten – vooralsnog – een bevoegdheid is die men in het buitenland niet kent. Dit geeft voor de wetgever in elk geval geen aanleiding om zich af te vragen waarom Nederland nog niet zo'n bevoegdheid heeft.

3. De reikwijdte van de huidige 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 zijn hier relevant.

- De **ontsleutelplicht voor niet-verdachten**. Deze is, zoals uiteengezet in par. 3.1.1, nauwelijks effectief in het *commune* strafrecht. Waar er een titel bestaat om informatie te vergaren, betreft dat meestal dwangmiddelen die worden toegepast in opsporingsonderzoeken, zoals de telefoontap en computeronderzoek, waarbij de personen op wie de bevoegdheid is gericht relevante informatie kunnen geven. Als deze personen cryptografie gebruiken, kunnen zij bevolen worden te ontsleutelen (momenteel bij een doorzoeking; naar het wetsvoorstel Computercriminaliteit II ook bij telefoontaps). In de meeste gevallen zullen de personen die kunnen ontsleutelen echter verdachte zijn; dat geldt zowel bij telefoontaps als bij computeronderzoek.
  In het *bijzondere* strafrecht bestaan echter meer mogelijkheden voor een ontsleutelbevel. Bijzondere medewerkingsverplichtingen, zoals de inzage in de administratie (AWR) en de verplichting alle medewerking te geven die redelijkerwijs nodig is (WED), omvatten als zodanig een verplichting om klare tekst aan te leveren. De bevoegdheid van 125k lid 2 Sv is in die gevallen niet nodig, omdat de ruime specifieke bevoegdheid al volstaat. In gevallen waarin de controlebevoegdheden niet meer kunnen worden

uitgeoefend, omdat er een verdenking bestaat, zou onder omstandigheden wel het commune ontsleutelbevel ex 125k lid 2 Sv kunnen worden ingeroepen: in bedrijfsmatige omgevingen bestaat meer kans dat anderen dan de versleutelende verdachte bestanden of berichten kunnen ontsleutelen. Bedrijven hebben er immers zelf belang bij informatie van hun werknemers in beginsel te kunnen lezen, zodat zij een systeem kunnen hanteren waarbij (bijvoorbeeld) een systeembeheerder de sleutel kan achterhalen. Vooralsnog wordt echter weinig van deze techniek gebruik gemaakt.

- 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 zijn makkelijk kraakbaar, terwijl bij robuuste programma's ook korte sleutels goed te kraken zijn. Er zijn echter genoeg cryptoprogramma's beschikbaar via het Internet, zoals PGP, waarmee de gebruiker lange sleutels kan genereren die pas in honderden jaren te kraken vallen. De politie kan weliswaar supercomputers aanschaffen, of een schermbeveiliger maken met een kraakprogrammaatje dat op alle werkeloze computers van justitie draait, maar hiermee zullen alleen de belangrijkste berichten aangepakt kunnen worden. De politie moet dan sterk vermoeden dat een bepaald bestand al die rekencapaciteit waard is. Mij lijkt dit een mogelijkheid voor een geval waarin veel aanwijzingen zijn dat ultiem bewijsmateriaal is te vinden in een bepaald bestand in een zaak die anders vastloopt; voor de meeste opsporingszaken is dit echter geen optie. Merk op dat een feitelijk onderzoek naar de manieren waarop cryptografie de opsporingspraktijk hindert, hiermee in verband gebracht moet worden: zit het probleem vooral in enkele unieke zaken die stuiten op een enkel versleuteld bestand, of schuilt het probleem veeleer in het verkrijgen van voldoende informatie in veel zaken om de opsporing op gang te brengen of te houden?

  De meeste kans heeft de politie echter niet om het versleuteld bestand zelf te kraken, maar om het *wachtwoord* te vinden (neergeschreven op een geheugensteunpapiertje) of te *raden*. Er zijn programma's die automatisch veelgebruikte wachtwoorden uitproberen, waarmee het grootste deel van de wachtwoorden in enkele minuten in de praktijk te achterhalen blijkt. Men kan zich voorstellen dat berekenende misdadigers in het algemeen betere – moeilijker te raden – wachtwoorden kiezen, maar ik weet niet of dit in de praktijk steun vindt. Ook hier geldt dat een studie naar de cryptoproblemen in de praktijk een indicatie zal moeten geven.
- **Alternatieve opsporingsmethoden**. Bij de Wet Bijzondere opsporingsbevoegdheden is het arsenaal aan niet-traditionele opsporingsmethoden gesystematiseerd en ook uitgebreid. Dit omvat bevoegdheden die niet door cryptografie worden gehinderd, zoals direct afluisteren (artt. 126l en 126s

Sv) en infiltratie (artt. 126h en 126p Sv).[145] Dergelijke bevoegdheden kunnen tot op zekere hoogte een alternatief bieden voor de telefoontap en computeronderzoek als die door cryptogebruik geblokkeerd worden, maar ze zijn aanzienlijk minder praktisch en ze leveren veelal andersoortige informatie op. Een volwaardig alternatief voor telefoontap en computer-onderzoek kunnen ze dan ook niet bieden, al kunnen ze een deel van de pijn wegnemen. In welke mate dit het geval is, zal moeten blijken, nu de bevoegdheid van direct afluisteren pas sinds februari 2000 rechtmatig ingezet kan worden. Ook dit punt hangt overigens samen met de aard en omvang van de huidige cryptoproblemen: bij welk soort onderzoeken loopt justitie tegen crypto op, en hadden in die specifieke onderzoeken ook andere bevoegdheden ingezet kunnen worden om de benodigde informatie te verkrijgen?

De huidige opsporingsbevoegdheden suggereren dat de politie tot op zekere hoogte methoden heeft om cryptoproblemen aan te pakken. Wélke hoogte is moeilijk te zeggen, zonder inzicht in de aard en omvang van de crypto-problemen in de praktijk.

4. De reikwijdte en achtergrond van nemo tenetur

Het nemo-teneturbeginsel is een complex beginsel dat door velen verschillend wordt ingevuld. Men kan zich het beginsel voorstellen als drie concentrische cirkels: de harde kern ervan is de verklaringsvrijheid, waar het een bijna absolute werking heeft; de middelste schil ervan betreft afgedwongen vormen van actieve medewerking, waar het beginsel een sterke werking heeft; en de buitenste schil ziet op afgedwongen duldplichten, waar het beginsel een zwakke werking heeft.
De buitenste schil – duldplichten – is wel onderworpen aan nemo tenetur, ten eerste omdat de scheidslijn tussen actieve medewerking en dulden soms dermate vaag is dat het een kunstmatig onderscheid is – en kunstmatige onderscheiden mogen niet ten koste gaan van de uitleg van grondrechten. Ten tweede is dit het geval, omdat de ratio van nemo tenetur ook elementen omvat waarbij het onderscheid tussen actieve medewerking en dulden niet of minder van belang is. De procesautonomie en de menselijke waardigheid, die een deel van nemo tenetur verklaren, benadrukken dat de verdachte als autonome procespartij zijn eigen houding moet kunnen bepalen; daarbij past het in beginsel niet de verdachte als onderzoeksvoorwerp te zien, wat hij is bij een duldplicht.
Naast deze aspecten, omvat de ratio van nemo tenetur ook het pressieverbod en de betrouwbaarheid van resulterend bewijsmateriaal. Deze aspecten verklaren waarom nemo tenetur sterker werkt bij afgedwongen actieve medewerking en

145 Zie voor een analyse van crypto-onafhankelijke opsporingsmethoden Koops 1998, pp. 203-232.

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 heeft dit tot gevolg dat de wetgever in de afweging om een ontsleutelplicht voor verdachten in te voeren een zwaar gewicht moet 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, zal een ontsleutelplicht meestal de verklaringsvrijheid raken. De wetgever moet daarom zeer zwaarwegende belangen aanvoeren om toch een ontsleutelplicht voor verdachten in te voeren.

5. Het systeem van de wet en huidige inbreuken

Het commune strafrecht kent 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 bestaan meer inbreuken op de kern van het nemo-teneturbeginsel: in bepaalde gevallen worden ook verdachten gedwongen actief mee te werken of zelfs te verklaren. Het gaat dan vrijwel steeds om situaties waarin er geen of nauwelijks alternatieven zijn om de noodzakelijke gegevens te verkrijgen, om wetten met een beperkt bereik (van personen en situaties) en om een beperkte sanctiedreiging (bijna nooit hoger dan drie maanden gevangenisstraf). Alleen in het geval van de verplichting mee te werken aan een adem- of bloedonderzoek bij een verkeersdelict dat letsel of de dood tot gevolg heeft, staat er een zware vrijheidsstraf op niet-medewerking.

Het systeem van de wet suggereert 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 moet dus zeer zwaarwichtige redenen hebben om zo'n bevoegdheid in te voeren. In bijzondere wetgeving past een ontsleutelplicht voor verdachten mogelijk beter. De wetgever kan daar per gebied bekijken of een ontsleutelplicht past bij de bestaande medewerkings-

plichten, waarbij overwegingen voor een ontsleutelplicht kunnen zijn: gebrek aan alternatieven, een lage sanctiedreiging en een ordenend (niet primair repressief) doel van de wetgeving. Maar ook daar moet de wetgever terughoudend zijn: medewerkingsplichten, en zeker verklaringsplichten, zijn uitzonderingen, ook in het bijzondere strafrecht.

6. Handhavingsperikelen

Een wettelijke ontsleutelplicht voor verdachten is alleen zinvol als er enige druk bestaat om mee te werken – anders kan de politie het ook gewoon vriendelijk vragen, waarbij de verdachte vriendelijk aan het verzoek gevolg kan geven of het kan negeren. Er moet dus een sanctie staan op niet-medewerking. Dit gaat echter alleen op voor opzettelijke weigering mee te werken; anders zou er een risico-aansprakelijkheid op cryptogebruik worden gezet, hetgeen onaanvaardbaar is vanwege het belang van cryptografie in de informatiemaatschappij en het ontbreken van een gevaarzetting bij cryptogebruik.

Voor de oplegging van een sanctie op opzettelijke niet-medewerking, zal het Openbaar Ministerie aannemelijk moeten maken dat de verdachte in staat was te ontsleutelen – anders was zijn weigering immers niet opzettelijk. Hier nu zullen 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 zullen moeilijk te weerleggen zijn. Bovendien kunnen berekenende misdadigers voorzorgsmaatregelen treffen die hun verweer ondersteunen. Bij niet-berekenende misdadigers zal een vergeetverweer ("Oeps, wachtwoord vergeten…!") vaak slagen, terwijl bij berekenende misdadigers allerlei verweren kansrijk zijn. Er zal dus weinig dreiging uitgaan van een sanctie op niet-medewerking. Dit kan 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 zal worden voor het OM iemand voor decryptieweigering te veroordelen.

De handhavingsperikelen suggereren dat een ontsleutelplicht voor verdachten in de praktijk weinig effectief zal zijn. Een hoge sanctie op niet-medewerking, laat staan een omkering van de bewijslast in de hoofdzaak, moet worden afgewezen, en een lage sanctie heeft minder kans het beoogde effect – daadwerkelijke ontsleuteling van verdachte bestanden – te bereiken.

7. Opties voor een ontsleutelplicht

Afweging

Als we nu opnieuw kijken naar de mogelijke opties voor een ontsleutelplicht (zie hfd. 6), van een bevel tot alleen niet-verdachten via verschonings- of bewijsuitsluitingsregels tot een gesanctioneerde ontsleutelplicht voor verdachten, in het commune of het bijzondere strafrecht, met een algemene of een specifieke straf op decryptieweigering, dan blijken de meeste opties niet realistisch.
De uitgezette lijnen tonen aan dat de verdergaande opties voor een ontsleutelplicht voor verdachten (opties 5 en 6, waarbij het resultaat voor het bewijs kan worden gebruikt) een ernstige inbreuk op het nemo-teneturbeginsel maken, en dat er zeer zwaarwichtige redenen moeten zijn om zo'n inbreuk te rechtvaardigen. Die redenen kunnen alleen worden gevonden in de bijzonder-heid en de ernst en omvang van de problematiek.
De bijzonderheid van het probleem legt 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 zijn vanwege zware inbreuk op andere grondrechten. Maar de aard en omvang van het probleem zouden zeer ernstig moeten zijn, willen zij opwegen tegen de inbreuk op de kern van nemo tenetur en het systeem van de wet, en er zijn geen afdoende gegevens dat het cryptoprobleem voor de opsporing ook maar in de buurt komt 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, zal die medewerkingsplicht in elk geval effectief moeten zijn om het probleem daadwerkelijk (in hoge mate) op te lossen. Bij cryptografie is die effectiviteit twijfelachtig, en daar zal – bij de huidige stand van de techniek en cryptogebruik – niets aan te doen zijn. Het valt ook niet te verwachten dat dat in de toekomst anders zal zijn. Als er al een ontwikkeling zal plaatsvinden dat cryptogebruikers waarschijnlijker dan nu in staat zullen zijn te ontsleutelen, zullen er tegelijkertijd meer cryptosystemen worden ontwikkeld waarbij de gebruiker juist waarschijnlijk niet in staat zal zijn te ontsleutelen op bevel – een ontwikkeling die men nu reeds kan waarnemen. De vergaande opties 5 en 6 komen daarom niet in aanmerking.

De opties 3 en 4, een ontsleutelplicht voor verdachten met opsporings- of bewijsuitsluitingsregels, komen ook niet in aanmerking. Weliswaar maken ze niet of weinig inbreuk op nemo tenetur (de onder dwang geleverde informatie wordt immers niet voor het bewijs gebruikt), maar ze zijn ook niet effectief. De ontsleutelplicht beoogt juist om op te sporen en bewijs te vergaren tegen de

verdachte. De enige zin van deze opties is dat resulterende informatie tegen anderen dan de verdachte kan worden gebruikt. Maar daarvoor is geen nieuwe bevoegdheid nodig: de politie kan nu ook de verdachte als getuige horen in een zaak tegen de andere verdachte waarin hij zelf geen verdachte is (waardoor art. 125k lid 2 Sv van toepassing is – als de politie tenminste onverwijld handelt), of de politie kan een afspraak met hem maken om te ontsleutelen in ruil voor de toezegging de resultaten niet tegen hem als bewijs te zullen gebruiken. Met andere woorden, opties 3 en 4 hebben geen meerwaarde.

De conclusie moet zijn dat in het commune strafrecht voor een afgedwongen ontsleutelplicht voor verdachten geen plaats is. De enige optie die nemo tenetur open laat is om de huidige bepaling van art. 125m lid 1 Sv, dat het ontsleutelbevel niet aan de verdachte wordt gegeven, te wijzigen in een verschoningsrecht, met bijpassende cautie, voor verdachten. Valt dit te prefereren boven de huidige situatie? Het voordeel is dat een bevel wel aan verdachten kan worden gericht. Aangezien hier geen dwang achter zit, heeft dat weinig meerwaarde boven de mogelijkheid voor de politie om vriendelijk om ontsleuteling te verzoeken, hetgeen momenteel al kan. Toch past bij een ontsleutelplicht een verschoningsrecht wellicht beter dan een regel dat het bevel niet aan de verdachte wordt gegeven. Het ontsleutelen komt immers vaak dichter in de buurt bij het afleggen van een verklaring dan bij het uitleveren van voorwerpen. De rechtsbescherming zou daarop kunnen worden afgestemd: het zwijgrecht en de cautieplicht passen mogelijk beter bij het ontsleutelbevel dan de bepalingen dat verdachten niet kunnen worden gedwongen actief mee te werken. In de praktijk zal het evenwel weinig uitmaken, ook al kan dit misschien het systeem van de wet verhogen.

In het bijzondere strafrecht heeft de wetgever iets meer speelruimte in een belangenafweging om een zwaardere optie te kiezen, maar ook daar gaat een afgedwongen ontsleutelplicht voor verdachten waarschijnlijk mank aan gebrek aan effectiviteit. De bijzondere wetgever kan daarom beter terugvallen op de algemene medewerkingsplichten die de bijzondere wetgeving nu kent (die soms al een ontsleutelplicht impliceren), en de specifieke ontsleutelplicht uit het commune strafrecht.

9. Conclusies en aanbevelingen

Een onder strafdreiging afgedwongen ontsleutelplicht voor verdachten maakt inbreuk op het nemo-teneturbeginsel. Voor een dergelijke inbreuk zijn onvoldoende rechtvaardigingsgronden aan te voeren (zie de analyse in hfd. 8). Er zijn zwaarwegende argumenten tegen een ontsleutelplicht voor verdachten: een dergelijke plicht raakt de kern van het nemo-teneturbeginsel (hfd. 4), er zijn geen precedenten in de huidige wetgeving die een dergelijke inbreuk rechtvaardigen (hfd. 5), terwijl de plicht weinig effectief zal zijn vanwege handhavingsproblemen (hfd. 6). Voor de ontsleutelplicht pleiten alleen de specifieke aard van het probleem en de overweging dat andere manieren om dit aan te pakken nóg erger zijn (hfd. 2, 8), terwijl ook de aard en ernst van de problemen voor justitie gewicht in de schaal kunnen leggen. In dit laatste bestaat echter onvoldoende inzicht. Maar zelfs al zou blijken dat de cryptoproblemen een groot en ernstig probleem voor de opsporing opleveren, dan blijft het gebrek aan effectiviteit van een ontsleutelplicht een belangrijke overweging tegen een gesanctioneerde bevoegdheid.

Daarom is de huidige situatie – een ontsleutelbevel wordt niet gegeven aan verdachten – bevredigend. De wetgever kan overwegen deze bepaling, art. 125m lid 1 Sv, aan te passen naar analogie met het zwijgrecht en de cautie van art. 29 Sv, omdat dit wellicht meer past bij de aard van de bevoegdheid: het achterhalen van een wachtwoord dat in verdachtes geest zit zal vaak meer lijken op het afleggen van een verklaring dan op het uitleveren van voorwerpen. Voor de praktijk zal dat echter geen verschil maken.

Ook in bijzondere wetgeving is invoering van een afgedwongen ontsleutelplicht onwenselijk. Weliswaar is er in bijzondere wetgeving meer ruimte voor inbreuk op nemo tenetur, maar de gebrekkige effectiviteit is een sterk argument tegen een verdergaande ontsleutelplicht. De bijzondere wetgever zal genoegen moeten nemen met de huidige algemene medewerkingsplichten.

Afweging

De aanbeveling voor de wetgever is daarom om geen ontsleutelplicht voor verdachten in te voeren.[146] 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 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.
Om die afweging te kunnen maken, is in elk geval vereist dat de wetgever beschikt over inzicht in de aard, ernst en omvang van het cryptoprobleem voor justitie. De overheid zou er daarom goed aan doen om in kaart te brengen op welke manieren de opsporing en vervolging van welke soorten en hoeveel misdrijven door welk soort cryptogebruik door welk soort misdadigers worden belemmerd. De resultaten daarvan en de systematiek die ik in deze studie gevolgd heb zullen de wetgever dan in staat stellen om een gedegen afweging te maken als bij de lancering van het wetsvoorstel Computercriminaliteit III (rond 2006) opnieuw de roep om een ontsleutelplicht voor verdachten wordt gehoord.

146 Wel behoeft de huidige bepaling van art. 125k lid 2 Sv om andere redenen aanpassing, zie Koops & Schellekens 1999.

Summary

Suspects and Decryption Orders: the Scope of the Privilege Against Self-Incrimination

Introduction

Suppose you are a police officer on the brink of finding out who committed the murder you are investigating. You have probable cause to suspect someone, and you have his phone wiretapped. Unfortunately, when you listen to the taped conversations, you only hear gibberish. Did you intercept a fax message? No, it turns out that the suspect regularly scrambles his wire communications: he uses encryption to keep his conversations and computer messages secret. This, then, does not lead you any further.

Therefore, you decide to do a search at the suspect's place. There is no incriminating evidence readily at hand, but you have reason to believe that in the computer, incriminating messages may be stored, and perhaps also a diary. You browse eagerly in his computer, but when you click on the file diary.doc, the computer asks for your password for decryption. The file turns out to be encrypted – it looks like this:

qANQR1DBwU4DoFOjvEqaYQoQCADuZoWNo9hpUCugPFABqjb
msQwElkYgRxH5Dm5Yh7seCQ1CG31AWkacOl/DVpmxpL7Og9nMi
BmmucNg5BZn9kkrqT3qJhw7gbzPtwsJ4WgP3KHx3A/Ep7+4BnZF
CVc1sNlN4CpE7UiELWliee/R450+E+2y32lC/nKdgHbzDw/HGL2l

So, what do you do? The only way to get that last bit of information you need to finalise the evidence, is to command the suspect to decrypt the scrambled files or to give you his password. But would this not force him to provide evidence against himself?

It is likely that a power to demand decryption is an infringement of the privilege against self-incrimination. Since this privilege is not absolute, the legislature could, in principle, decide to enact such a power. Is this justified? To what extent does the privilege against self-incrimination stretch? In this research, I

deal with these questions, and suggest a way for the Dutch legislature to answer them.[147]

The crypto controversy

Cryptography (secret writing), or crypto for short, is a means to hide data from unauthorised people. Since the 1970s, robust and reliable automated crypto systems provide efficient and generally uncrackable protection of communications and stored data. Since the mid-1990s, crypto programs have become user-friendlier and more widespread, and you can download several good programs from the Internet, such as Pretty Good Privacy.

To encrypt data, you need a crypto program and a key. For *de*crypting the data, you need the decryption key, which is the same as the *en*cryption key in "symmetric" cryptography (such as DES), or a *different* one in "asymmetric" or "public-key" cryptography (such as PGP). The decryption key (which is indeed key to keeping the data secret) must be kept secret, and is generally stored safely on a diskette or a hard disk, protected by a password.

More and more people are starting to use cryptography, and it is being built in in programs and the information infrastructure, because it is one of the best ways to provide information security – a requisite for electronic commerce. Since the middle of the 1990s, cryptography has proved itself an essential tool in the information society.

However, cryptography is not only used to safeguard e-commerce. Criminals are increasingly becoming aware of its potential to shield their incriminating information traffic from eavesdropping and computer-searching police. This has caused governments to think of ways to promote the good uses of cryptography and at the same time of preventing criminals from using it to thwart the police. This has turned out to be impossible. Whatever governments have come up with, such as requirements to store keys with third parties, has proved ineffective and unacceptable to the large majority of information citizens. My research into this issue has led me to the conclusion that the only way to really do something about the crypto problems for law enforcement, is to enact a power for the police to require suspects to decrypt.[148] Whether that is acceptable, in the light of the privilege against self-incrimination, is a complex issue, which requires careful study of the background of the privilege and of the pros and cons of such a power. So far, governments have been wary with infringing the privilege against self-incrimination for this purpose.

Current legal status of the decryption command

147 For an analysis of the situation in US law, see Reitinger 1996 and Sergienko 1996.

148 See my thesis, Koops 1998, in particular Chapter 8.

During the Dutch parliamentary discussions over the Computer Crime Act (CCA), in 1992, the legislature became aware of the potential problems cryptography poses to law enforcement. They decided to introduce a power for the police to command someone to decrypt during a search. They respected, however, the privilege against self-incrimination, and so this command cannot be given to suspects (art. 125m DCCP). Then, in January 1998, a follow-up to the CCA was proposed, the Computer Crime Act II. This contained the power to demand people to decrypt data collected during a search or in a wiretap, and this time, the act proposed to also give this command to suspects, if there is grave evidence ("ernstige bezwaren") against the suspect and if this is urgently necessary for finding the truth. Several protests from the legal community were raised, and the Minister decided to withdraw the provision in the draft law that was submitted to Parliament in July 1999,[149] thus – again – respecting the privilege against self-incrimination.

The privilege against self-incrimination

To be able to judge whether and to what extent a decryption command infringes the privilege against self-incrimination, and whether such an infringement is acceptable given the interests at stake, one must study the way the privilege has been interpreted and what infringements have been allowed to date. I will therefore first analyse the privilege, and subsequently give an overview of infringements that have been allowed in Dutch law.

The privilege against self-incrimination is a fundamental legal principle that is part of the right to a fair trial. It says that a suspect cannot be forced to incriminate himself or to yield evidence against himself. The privilege is recognised in most countries, either explicitly in the constitution or implicitly through case law. It is included explicitly in several international treaties, such as the International Covenant on Civil and Political Rights (article 14 para. 3 sub g: everyone charged with a criminal offence has the right not to be compelled to testify against himself or to confess guilt) and the Statute for the International Criminal Court (article 55 para 1 sub a: a person shall not be compelled to incriminate himself or herself or to confess guilt).
Moreover, the privilege is enshrined in article 6 of the European Convention of Human Rights, as interpreted by the European Court. The right to a fair trial incorporates "the right of anyone 'charged with a criminal offence', within the autonomous meaning of this expression in Art. 6,[150] to remain silent and not to

149 TK 1998-1999, 26 671, nrs. 1-3.

150 The "autonomous meaning" of the term "criminal charge" means that the European Court does not only look at the classification of the alleged offence in a nation's law (criminal or otherwise), but also at the nature of the offence and the nature of the penalty threatened.

contribute to incriminating himself."[151] In three cases,[152] the European Court has laid down the basis for determining the meaning of the privilege against self-incrimination, but at the same time, it has caused considerable confusion over this meaning. The *Saunders* case seems to give the most definitive statement about the privilege. The privilege

> *is primarily concerned, however, with respecting the will of an accused person to remain silent. (...) it 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.*

There is not a general definition of the privilege against self-incrimination in Dutch law. The Constitution and the Dutch Code of Criminal Procedure (DCCP) do not mention it. The DCCP does contain several articles that reflect the privilege; for instance, a command to hand over goods or a command to provide access to a protected computer cannot be given to a suspect (art. 107 and art. 125m para. 1 DCCP).

The Dutch Supreme Court has initially said that "it would ill be in keeping with the spirit of the DCCP" if "the suspect would be compelled to contribute to his own conviction under threat of punishment",[153] but since 1977, it has often repeated the magic formula: "there is no unconditional right or principle that a suspect can not in any way be obliged to cooperate in the obtaining of possibly incriminating evidence".[154] The system of Dutch law indicates that, in general, suspects cannot be required to actively cooperate, but they do have to suffer acts that can incriminate them, such as the taking of blood samples. In special laws, dealing, e.g., with environment and tax crime, there are more compulsory powers for the police to require active cooperation from people, including suspects, such as handing over documents. An important reason for the difference between general and special criminal law is that, in the latter, cooperation requirements are considered necessary to find evidence at all that a crime as such has been committed. If people would be able to refuse to give tax documents to tax officials, tax crimes would not be discovered anymore, let alone prosecuted – so the argument goes.

---

151 ECHR 25 February 1993 (*Funke v. France*).

152 ECHR 25 February 1993 (*Funke v. France*), ECHR 17 December 1996 (*Saunders v. United Kingdom*) and ECHR 8 February 1996 (*Murray v. United Kingdom*).

153 HR 16 January 1928, NJ 1928 p. 233.

154 HR 15 February 1977, NJ 1977, 557 m.nt. GEM.

Summary

From the European and Dutch interpretations of the privilege, one can conclude that although the privilege against self-incrimination is usually defined quite broadly ("not contribute to incriminating one-self"), the scope of the privilege is rather limited. It is a strong barrier to the compelled rendering of *testimonial* evidence, implying a suspect's act or statement which somehow or other involves the use of his mind, but it is only a weak barrier to other means of compelled cooperation, such as suffering blood samples or handing over tax documents. In my understanding, the privilege does stretch to these kinds of "cooperation" as well (contrary to what the European Court in *Saunders* suggested) because the suspect cooperates in incriminating himself, but the privilege has a weaker impact on this kind of cooperation.

To understand why this is so, one should try to distil the rationale of the privilege from its history. People have suggested various reasons for the privilege.

1. Humanity: it is not humane to force someone to contribute to his own misfortune.
2. Autonomy: a suspect is free to choose an attitude in criminal proceedings, he can decide whether he wants to cooperate or not.
3. Reliability: evidence must be reliable.
4. Prohibition of pressure: the privilege is a safeguard against the police using (too much) pressure to force a suspect to cooperate.

The third option has great explicative value. The disclosure of things which exist "outside of the will of the suspect" provides reliable evidence, whereas testimonial statements generally do not (you do not know whether the suspect tells the truth). Thus, the privilege contributes to truth-finding and shields the judiciary from "miscarriages of justice", as the European Court stated in *Murray*. However, I think it is impossible (and unnecessary) to pinpoint a single rationale: all of the above grounds have something to say for them and explain different aspects of the privilege.

One must realise that the privilege works on different levels. First, it is a principle the legislature has to take into account when introducing investigation powers. They cannot enact a power that unduly forces a suspect to incriminate himself. Here, the reliability rationale plays an important part: the more reliable evidence a power yields (such as breathalyser tests for drunk driving), the less strongly does the privilege work. And conversely, the less reliable a power is (such as requiring a suspect to make a statement on his involvement with the crime), the more strongly the privilege works.[155]

Second, the privilege has influence on the implementation of investigation powers. Here, it prevents the police from putting too much pressure on a

[155] See Schalken's annotation of HR 29 October 1996, NJ 1997, 232.

suspect to cooperate when they use compulsory powers; this is the rationale of prohibition of pressure.
Third, the privilege plays a part in court. The court must decide whether information obtained through pressure on a suspect to cooperate is admissible as evidence. This is not a simple deduction from the wording of the law that allows investigation powers. Even if the police have the power to compel cooperation, such as handing over documents in a tax investigation, it does not follow automatically that the resulting data can be used as evidence. This can be illustrated by the *Saunders* case. The law that compels people to make statements is acceptable in light of the privilege – it targets people not charged with a criminal offence. However, in Saunders' case, the statements could not be used as evidence, because they had been used in the criminal proceedings in a way incompatible with the privilege. The privilege-infringing use of the statements was mainly caused by the influence the use of the documents had had on Saunders' attitude in court, particularly given the negative impression it created with the jury. Thus, the autonomy of the suspect and the prohibition of pressure are paramount in colouring the privilege as used in court, besides the reliability of the evidence.

Does a decryption command infringe the privilege?
From the definition of the privilege, it is clear that a decryption command is an infringement. Whether the suspect decrypts himself or whether he hands over a key and tells the password, in all cases, he actively cooperates in an activity that results directly in possibly incriminating evidence. Moreover, in most cases, the suspect will have to show or use the contents of his mind, because the password protecting the key is stored there. If the password is written down somewhere, the police can seize the paper or copy the password themselves; the decryption command is targeted precisely at cases in which the password is not readily available to the police.
One can argue over the question to what extent telling a password is testimonial (in Dutch, a "verklaring"). On the one hand, it is not a statement concerning facts or circumstances – it is more like a physical key in that it either works or does not work. In that respect, the password is independent of the will of the suspect, because he cannot alter it with his will power. On the other hand, since the password exists in the mind (assuming the password is not written down somewhere), the suspect must operate his mind to reveal it. In that respect, the password has an existence which does depend upon his will, because if he refuses to give it (e.g., because he has forgotten it), the password, to all practical purposes, does not exist anymore. This means that, even if the password itself is not testimonial, the act of giving it will usually be testimonial: it reveals knowledge of the suspect. Only if it is a foregone conclusion that the suspect

knows the password, can one hold that revealing the password is not testimonial.
This seems exactly the criterion that was pivotal to the *Funke* case, which the European Court decided in 1993. Funke was forced by French custom officials to hand over bank account documents "which they believed must exist, although they were not certain of the fact". Although the court decision is an obscure one, which has triggered divergent interpretations, I believe that this question whether the government knew or not that Funke had the power to comply was a crucial factor in deciding there had been an infringement of the privilege against self-incrimination. Because the officials were *not* sure that Funke had the documents, their forcing him to hand them over was incompatible with the privilege. After all, his refusal to comply could not lead to any conclusion: it may have been caused by unwillingness, but also by inability.[156]

In consequence, a decryption command is in all cases an infringement of the privilege against self-incrimination that prevents incriminating oneself, and it is also an infringement of the strong privilege that prevents providing testimonial evidence, if it is not a foregone conclusion that the suspect knows the password.

Precedents for infringing the privilege in Dutch law

Now, we are to decide whether a power to require suspects to decrypt is acceptable given the privilege and the other interests at stake. This primarily concerns the first level on which the privilege operates: that of the legislature. In balancing the interests at stake, the legislature must bear in mind the system of the law and the arguments one can use to infringe fundamental rights. Therefore, one must analyse what laws the legislature has passed until now to allow infringements.
First, several laws require people to make testimonial statements. There are reporting requirements: e.g., doctors carrying out euthanasia, farmers dealing with manure, and financial institutions accepting unusual amounts of money all have to file reports. These can lead the Public Prosecutor to start an investigation, if the report suggests that rules have not been complied with. Generally, the information contained in the reports can be used as evidence in a criminal trial, because the reporting law addresses non-suspects in regulatory, not criminal, affairs. In certain laws, however, an exception has been made: the law requiring the reporting of unusual financial transactions stipulates that the

156 For this interpretation of *Funke* and the related case of *Fisher v. United States*, see Koops 1998, p. 175, Jörg 1998, p. 73, and Rozemond 1998, p. 316. See also the recent certiorari granted by the Supreme Court in *United States v. Hubbell* (D.C. Cir., 167 F.3d 552): the Fifth Amendment protects the production of business and financial records, unless the government can show its prior knowledge of the information.

information cannot be used in a prosecution of financial institutions for receiving ("heling"). This is because the law is targeted at catching money-laundering criminals, not the reporting financial institutions.
Then, in several special laws, there are requirements to provide information, e.g., in supervisory activities concerning taxes, drugs, or weapons. Usually, the supervisory officials can require people to provide information, but if the addressee is a suspect, he can refuse to testify. This is not so in the Law on Weapons and Munitions: if a suspect does not comply with an order to provide information, he can be fined. This exception may be explained by the importance of controlling the risk of weapons, the restricted scope of the law, and the low punishment, leading to the infringement of the privilege against self-incrimination to be acceptable to the legislature.
Then, witnesses usually are obliged to speak. In criminal cases, however, they can refuse to answer a question if in answering they would incriminate themselves. In parliamentary inquests, they cannot refuse to speak, but a special provision forbids using their answers as evidence in criminal cases. Thus, there are different levels of self-incrimination protection: suspects never have to answer, witnesses in criminal cases can only refuse to answer certain questions, and witnesses in parliamentary inquests always have to answer, but resulting evidence is inadmissible.
A special case is car registration-number liability. The holder of a registration number is liable for certain offences committed with the car, unless he tells the police who was the driver. If he fails to indicate the driver, the registration-number holder can be sentenced to the same punishment as can be given for the offence at issue. Thus, in fact, people are forced to give information, and a refusal is penalised. This infringement of the privilege against self-incrimination should be explained by the special circumstances of the Road Traffic Act, where car owners are considered to have a responsibility to prevent others to use their cars to endanger road safety with impunity. Still, it is the only case in Dutch law where suspects can be forced to make a statement (the name and full address of the driver) while a refusal to comply is punishable with a prison sentence. As such, it hardly fits in with the way Dutch law has incorporated the privilege against self-incrimination.
The general conclusion must be that suspects can, in principle, never be forced to make statements. People who are not a suspect, however, can be forced to give testimonial evidence, although they can usually refuse to comply if they would incriminate themselves. Generally, resulting evidence may not be used against them in court. It is only in very few, restricted areas (weapons, traffic) that compelled statements may be admissible as evidence.

Second, there are requirements to force suspects to actively cooperate with the police – a broader class of cooperation, and less contentious than providing testimonial evidence because the right to silence need not be at stake. One can think of the many requirements in special laws to hand over documents or things that may be helpful for uncovering the truth. Also, in traffic law, people suspected of drunk driving have to actively cooperate with a blood or breath test. If suspects refuse to cooperate, they can be punished with a prison sentence (in tax law), or with the same punishment as can be given for drunk driving (in traffic law). Here, therefore, we see that the privilege is infringed, but that the legislature has allowed this infringement after a balancing of the interests at stake. In these cases, the privilege against self-incrimination has less weight because it concerns material independent of the will of the accused. Thus, the necessities of enforcing special laws (regulating specific kinds of economic activities) can be considered to outweigh the privilege. Further arguments for this balance are the relatively low punishments (in the special laws) and the subsidiarity principle, which holds that a compulsory power which breaches fundamental rights is more acceptable if there are no other powers available to achieve the goals of the legislation (which is a particularly valid argument in the traffic law, because drunk driving can hardly be proved otherwise).

This overview leads to the conclusion that, in general criminal law, suspects do not have to cooperate. In special laws, they often have to actively cooperate, but they usually cannot be forced to give testimonial evidence. Infringements of the privilege against self-incrimination are allowed more easily in special laws, largely because of the principle of subsidiarity (it is harder to prosecute crime in economic-activity regulating areas, because the crime is usually more covert) and because of the principle of proportionality (the more restricted the scope of the law, the less an infringement forced cooperation is).
Furthermore, the laws show different ways of incorporating the privilege against self-incrimination: sometimes, people cannot be forced to cooperate; sometimes, they can be addressed with a cooperation command but they can refuse to comply; sometimes, they are obliged to comply, but resulting data cannot be used as evidence against them at all; and sometimes, people are obliged to cooperate, but resulting evidence is inadmissible in court under certain circumstances. Only laws of the last category concern true infringements of the privilege against self-incrimination.

Options for commanding decryption

Now, if we look at the issue at hand, the analysis of precedents suggests various ways of enacting a decryption command within – and outside of – the limits of

the privilege against self-incrimination. I present these in order of increasing infringement of the privilege against self-incrimination.

1. A decryption command that cannot be given to suspects.
2. A decryption command to all persons. People can refuse if by complying they would incriminate themselves.
3. A decryption command to all persons. Suspects have to comply. Resulting data cannot be used for investigation.
4. A decryption command to all persons. Suspects have to comply. Resulting data cannot be used as evidence.
5. A decryption command to all persons. Suspects have to comply. Resulting data
   - *can* be used as evidence only if certain conditions apply; or
   - *cannot* be used as evidence only if certain conditions apply.
6. A decryption command to all persons. Suspects have to comply. Resulting data can be used as evidence.

Moreover, these options can be chosen for

A. criminal law in general (the Code of Criminal Procedure), or

B. only specific laws (such as tax law, environment law, or drugs law).

To ensure effectiveness, one can choose various enforcement options. A refusal to comply with a decryption command:

i. is punishable as not complying with a legal order (like art. 184 DCC, maximum three months' imprisonment);

ii. is punishable in its own right, with a specific maximum punishment that
   - is the same for all crimes; or
   - is somehow tied to the crime being investigated;

iii. can be used as evidence by drawing an adverse inference in the case against the addressee.

In all options, variables can be added to limit the scope of the power (and the consequent infringement), such as restricting the power to serious crimes, a requirement of probable cause ("redelijke verdenking") or of grave evidence ("ernstige bezwaren"), and requirements of urgency and necessity.

As Dutch law currently stands, A1i is the case.[157] The issue in the Netherlands, then, is to what extent a "heavier" law can and should be established, where A6 is the most far-reaching.

[157] In various special laws, requirements to cooperate can be interpreted as including a command to decrypt, like the requirement in tax law to show books, which must be presented in an understandable format; these could be seen as decryption commands of the type B2ii and B3ii (and B6ii in the case of the munitions law requirement to cooperate).

Enforcement and ability to decrypt

One of the major factors in the decision to introduce a decryption-order law targeted at suspect is enforcement. After all, if the order is to be effective, there must be a threat of punishment for not complying. Such a punishment can only be given to people who *wilfully* do not comply. Otherwise, a risk liability would be introduced for encryption use: if you ever find yourself in front of the police asking you to decrypt, you have to comply, whether or not you are able to. That is unacceptable, given the importance of cryptography in the information society and the fact that using encryption is in no way of itself a dangerous activity. Therefore, if someone is to be punished for not decrypting, the police will have to show that he was able to decrypt.

Here, problems emerge. Addressees can generally easily hide unwillingness to cooperate under retorts of "I forgot my password", "These random data must have been copied to my computer when I downloaded something from the Internet – I've no idea what they are", and "I haven't used that decryption key for over a year". Especially the retort that the addressee forgot his password is difficult to refute. The police can argue why someone should be able to remember his password (e.g., because he is a professional crypto user who has never forgotten his password at the office), but there are too many arguments the suspect can give to make this unlikely (e.g., "I used a particularly difficult password, as my crypto consultant advised me, which I was not allowed to write down – and I haven't used it that often").

Moreover, calculating criminals have plenty of opportunities to anticipate a decryption order. For instance, they can remove all header information so that one cannot see whether the file is encrypted or just consists of random data, they can often change key pairs, and they can antedate files in their computers so that they can argue that they no longer remember the key with which it was encrypted long ago. Also, the crypto community will devise robust schemes for "perfect forward secrecy", in which it is not possible for the user to decrypt the data after a certain period.

As a result, a decryption order will be particularly powerless against calculating criminals, while less-calculating criminals can benefit from an I-forgot-my-password retort. Therefore, it will hardly be useful to put a significant punishment on not complying with a decryption order – the prosecution will have too hard a task to show that someone wilfully did not comply.

Choosing an option

To introduce a decryption command that balances the interests of crime-fighting and the right to a fair trial, the legislature must analyse the following.

1. What is the **scope of the privilege** against self-incrimination in their law system? I have indicated this for the Dutch situation above.
2. What **kind of crimes** is at stake in which the investigation is hampered by encryption? Are these numerous, more general crimes, or mainly certain specific crimes? How serious are these crimes? This analysis should be based on empirical studies of investigation practice.[158] My current impression is that cryptography has truly obstructed investigation in only very few cases to date, although this may change significantly if cryptography is built in in mass-market software, such as operating systems and mail programs.
3. **How** does cryptography hamper investigation? Does it mainly hamper the (initial stages of) investigation (notably in wiretaps), making it more difficult to find out who may be involved in the crime, or does it obstruct the stage of prosecution, making it difficult to finalise the evidence (notably in computer searches)?
4. What **alternatives** are there to investigate and gather sufficient evidence? Does this depend on the kind of crime and investigation involved? E.g., it may be the case that in general investigation, there are sufficient other alternatives (such as infiltration, or using directional microphones and bugs), whereas in specific supervision procedures and investigations (such as tax and environment law), there are far less viable alternatives. Here, one must also assess the extent to which the alternatives infringe fundamental rights, such as the right to privacy and the right to a fair trial, in order to assess what is the least burdensome power.
5. If a power to demand decryption is found necessary, what **safeguards** should be in place to make it as little infringing as possible within the limits of effectiveness? Here, one must choose conditions of the seriousness of the crimes for which the power can be exerted, the amount of suspicion against the addressee, the likelihood of the encrypted data at issue to be useful or necessary for the investigation, and the like. The legislature should look at comparable investigation powers to make the decryption command neatly fit in with the system of the law. Moreover, a safeguard should be built-in to prevent keys used for digital signatures to be handed over.
6. What kind of **enforcement** is required? Here, the legislature must choose between the general penalisation of not complying with a legal order, a specific penalisation for not complying with this order – with an appropriate and just maximum punishment, and a provision that allows the judge to draw an adverse inference from a refusal to comply (effectively reversing the

158 Denning & Baugh 1997 and 1999 have initiated such empirical studies, but these were rather rough and ad hoc. No data avail for the Netherlands. Governments should stimulate studies of the extent to which investigation is hampered by cryptography, rather than roughly indicate the theoretical problems.

burden of proof for the incriminating nature of the encrypted data). Generally, the enforcement will not be effective given the ease with which addressees can claim not to be able to comply. This is a strong argument against a severe infringement of the privilege against self-incrimination.

Conclusion

Cryptography is a potential problem for law enforcement, hampering wiretaps and computer searches. The only way to really solve this problem would be to force suspects to decrypt, but this infringes the privilege against self-incrimination. Governments can decide to introduce a power to command suspects to decrypt, if a full analysis of the problems in practice and the system of the law lead them to account more weight to the necessity of fighting crime than to the privilege against self-incrimination in this particular respect. It is likely, however, that such a power will not be very effective if targeted at suspects. As a result, there should be the most serious and compelling arguments to introduce a decryption power to suspects nonetheless – such as the fact that cryptography is definitively blocking a large number of prosecutions of serious crimes, in which there is no alternative but to get the key to decrypt possibly incriminating evidence. At present, this is far from the case, and it is unlikely that such will ever be the case.

Therefore, an infringement of the privilege against self-incrimination is not warranted. The current Dutch provision that a decryption order can not be given to suspects is a sound one.

Bibliografie

Andersen & Landrock 1996
Mads Bryde Andersen, Peter Landrock, 'Encryption and Interception', *The Computer Law and Security Report* 1996 (November-December), p. 342-348

Ansmink 1981
A.A. Ansmink, 'Het meewerken van de verdachte aan zijn veroordeling en art. 29 Sv', *RM Themis* 1981, p. 426-448

Baauw 1979
P.J. Baauw, Bespreking van Mr. Egbert Myjer, Van duimschroef naar bloedproef, *Nederlands juristenblad* 1979, p. 468-469

Blaze 1996
M. Blaze, W. Diffie e.a., *Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security*, januari 1996, WWW <ftp://ftp.research.att.com/dist/mab/keylength.txt>

Bovens 1998
Mark Bovens, 'Hebben rechtspersonen morele plichten en fundamentele rechten?', *Ars Aequi* 1998, p. 651-659

Buruma 1993
Y. Buruma, *De strafrechtelijke handhaving van bestuurswetten*, Arnhem: Gouda Quint 1993

Buruma 1998
Y. Buruma, 'Internet en strafrecht', preadvies *Nederlandse Juristen-Vereniging 1998-I*, Deventer: Tjeenk Willink 1998, p. 119-195

Commissie Meijers 1997
Rapport van de Commissie onderzoek aan het lichaam, s.l., februari 1997

Corstens 1998
G.J.M. Corstens, 'Internet en strafrecht', *Nederlands juristenblad* 1998, p. 1032-1035

Denning & Baugh 1997

Dorothy Denning, William Baugh, *Cases involving encryption in crime and terrorism*, versie 10 oktober 1997, WWW <http://www.cs.georgetown.edu/~denning/crypto/cases.html>

Denning & Baugh 1999
Dorothy Denning & William Baugh, *Hiding Crimes in Cyberspace*, juli 1999, WWW <http://cryptome.org/hiding-db.htm> en <http://www.cs.georgetown.edu/~denning/crypto/hiding1.doc>

Drion 1998
Coen Drion, 'Van de mazen en het Net', *Nederlands juristenblad* 1998, p. 1185-1188

Van Duyne & Van der Landen 1999
Petrus van Duyne & Dirk van der Landen, 'De "kennelijke" oorsprong van Sneeuwwitje. De nieuwe witwaswet en het "goede verhaal"', *Nederlands juristenblad* 1999, p. 1683-1688

Enquêtecommissie opsporingsmethoden 1996
Enquêtecommissie opsporingsmethoden, *Inzake opsporing*, Den Haag: Sdu 1996

Finaly 1996
R.A.R.S. Finaly, 'Nemo tenetur … niet voor rechtspersonen?', *De naamloze vennootschap* 1996, p. 109-114

Hartmann & De Meijer 1997
A.R. Hartmann & M.E. de Meijer, 'Naschrift' bij 'Zwijgrecht en cautie' van Ronald Verdaas, *Nederlands juristenblad* 1997, p. 343-344

Hieltjes 1998
H.B. Hieltjes, 'Het nieuwe fiscale boeterecht', *MBB: Maandblad belastingbeschouwingen* 1998, p. 91-103

Jörg 1998
N. Jörg, 'Artikel 29', in: A.L. Melai c.s., *Het Wetboek van Strafvordering*, Arnhem z.j., maart 1998

Kahn 1967
David Kahn, *The Codebreakers. The Story of Secret Writing*, New York: MacMillan 1967

Kaspersen 1993
H.W.K. Kaspersen, 'De Wet computercriminaliteit is er – nu de boeven nog', *Computerrecht* 1993 nr. 4, p. 134-145

Kaspersen 1997
H.W.K. Kaspersen, 'Opsporingsonderzoek in computernetwerken', in: H. Franken, H.W.K. Kaspersen & A.H. de Wild, *Recht en computer*, Deventer: Kluwer 1997, derde druk

Kaspersen 1998

H.W.K. Kaspersen, 'Internet en strafrecht, preadvies van Y. Buruma', *Computerrecht* 1998 nr. 3, p. 119-123

Klaver 1998
Marie-José Klaver, 'Verdachten hoeven niet mee te werken', *NRC Handelsblad*, 15 oktober 1998

Koops 1998
Bert-Jaap Koops, *The Crypto Controversy. A Key Conflict in the Information Society*, The Hague: Kluwer Law International 1998

Koops 1999
Bert-Jaap Koops, *Crypto Law Survey*, versie 16.1, oktober 1999, <http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm>

Koops & De Jong 1998
Bert-Jaap Koops & Huub de Jong, 'De risico's van data recovery voor overheid en gebruikers', *Computerrecht* 1998 nr. 5, p. 222-227

Koops & Schellekens 1999
B.J. Koops & M.H.M. Schellekens, 'Computercriminaliteit II: de boeven zijn er – nu de wet weer', *Nederlands juristenblad* 1999, p. 1764-1772

Lensing & Mulder 1994
J.A.W. Lensing & G.E. Mulder, *Hoofdbeginselen van strafprocesrecht*, Zwolle: Tjeenk Willink 1994

Lenstra & Verheul 1999
Arjen K. Lenstra & Eric R. Verheul, *Selecting Cryptographic Key Sizes*, 24 november 1999, WWW <http://www.cryptosavvy.com/cryptosizes.pdf>

Mäder 1997
Detlef Mäder, *Betriebliche Offenbarungspflichten und Schutz vor Selbstbelastung. Zum Spannungsfeld von Umweltrecht und nemo tenetur-Grundsatz*, diss. Freiburg, Freiburg im Breisgau: edition iuscrim 1997

Martens 1996
Martens, afwijkende mening bij EHRM 17 december 1996, NJ 1997, 699 m.nt. Kn. (*Saunders*)

Meijer 1991
Angela Meijer, 'De werking van het nemo tenetur-beginsel in het Nederlandse strafrecht', *Delikt en Delinkwent* 1991, p. 890-896

Menezes, van Oorschot & Vanstone 1996
Alfred J. Menezes, Paul C. van Oorschot & Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC Press 1996

Myjer 1978

Egbert Myjer, *Van duimschroef naar bloedproef. Beschouwingen over de regel dat niemand gedwongen mag worden zichzelf te belasten.* Preadvies Nederlandse Vereniging voor Rechtsvergelijking, Deventer: Kluwer 1978

NJV 1999
Handelingen Nederlandse Juristen-Vereniging 1998-II, Deventer: Tjeenk Willink 1999

NOVA 1998
Nederlandse Orde van Advocaten, Adviescommissie Strafrecht, *Computercriminaliteit II*, 27 februari 1998, te verkrijgen via WWW <http://Ordedata.balienet.nl/NOVA>

NRC 1996
Kenneth W. Dam, Herbert S. Lin (eds.), National Research Council, *Cryptography's Role In Securing the Information Society*, Washington, D.C.: National Academy Press 1996, WWW <http://www.nap.edu/readingroom/books/crisis/>

Registratiekamer 1998a
Registratiekamer, *Brief aan de Minister van Justitie*, 9 maart 1998, kenmerk 98.A.089.01

Registratiekamer 1998b
Registratiekamer, *Brief aan de Minister van Binnenlandse Zaken*, 9 april 1998, kenmerk 98.A.294.01

Reijntjes 1996a
J.M. Reijntjes (red.), *Nemo tenetur*, Arnhem: Gouda Quint 1996

Reijntjes 1996b
J.M. Reijntjes, 'Nemo tenetur: een holle leus?', in: Reijntjes 1996a, p. 9-21

Reitinger 1996
Phillip R. Reitinger, 'Compelled Production of Plaintext and Keys', *University of Chicago Legal Forum* 1996, p. 171-206

Rivest 1998
Ronald L. Rivest, *Chaffing and Winnowing: Confidentiality without Encryption*, versie 24 april 1998, <http://theory.lcs.mit.edu/~rivest/chaffing.txt>

De Roos 1990
Th.A. de Roos, 'De doorzichtige verdachte. Onderzoek aan en in het lichaam vanuit het gezichtspunt van de verdediging', in: G.P.M.F. Mols (red.), *Justitieel onderzoek aan en in het lichaam*, Deventer: Kluwer 1990, p. 116ff

Rozemond 1992
K. Rozemond, 'Het DNA-onderzoek in strafzaken en het nemo tenetur-beginsel', *Nederlands juristenblad* 1992, p. 125-132

Rozemond 1998

Klaas Rozemond, *Strafvorderlijke rechtsvinding*, Deventer: Gouda Quint 1998

Schneier 1996
Bruce Schneier, *Applied Cryptography. Protocols, Algorithms, and Source Code in C*, New York etc.: John Wiley & Sons 1996, 2nd edition

Sergienko 1996
Greg Sergienko, 'Self Incrimination and Cryptographic Keys', *Richmond Journal of Law & Technology* 1996 nr. 1, WWW <http://www.urich.edu/~jolt/v2i1/sergienko.html>

Stand 1999
Stand.org.uk, *Letter to Jack Straw, Home Secretary*, WWW <http://www.stand.org.uk/dearjack/> (inzage 24 november 1999)

T&C Sv 1997
C.P.M. Cleiren & J.F. Nijboer (red.), *Tekst en Commentaar Strafvordering*, Deventer: Kluwer 1997[2]

TTP-dossier 1998
'Dossier Trusted Third Parties', *Computerrecht* 1998 nr. 5, p. 206-234, WWW <http://cwis.kub.nl/~frw/people/koops/pub/ttp-dos.htm>

Van Veen 1979
Th.W. van Veen, 'Van plicht tot spreken en recht tot zwijgen: Art. 29 Sv bevat een uitzondering', *Delikt en Delinkwent* 1979, p. 687-693

Waling 1999
Cornélie Waling, 'Kampioenschap moet niet leiden tot paniekvoetbal', *Nederlands juristenblad* 1999, p. 1555-1557

Walsh 1996
Gerard Walsh, *Review of Policy relating to Encryption Technologies*, 10 oktober 1996, WWW <http://www.efa.org.au/Issues/Crypto/Walsh>

Wöretshofer 1996
J. Wöretshofer, 'De meldingsprocedure levensbeëindiging: ongeoorloofd?', in: Reijntjes 1996a, p. 41-56

Afkortingen

Awb	Algemene wet bestuursrecht
AWR	Algemene wet inzake rijksbelastingen
BEDOT	Bevat Een Decryptiemogelijkheid voor OpsporingsToegang
DCC	Dutch Criminal Code
DCCP	Dutch Code of Criminal Procedure
DES	Data Encryption Standard
gvo	gerechtelijk vooronderzoek
IDEA	International Data Encryption Algorithm
MOT	melding ongebruikelijke transacties
NJ	Nederlandse Jurisprudentie
Njb	Nederlands juristenblad
OM	Openbaar Ministerie
PACE	Police and Criminal Evidence Act
PGP	Pretty Good Privacy
RSA	Rivest Shamir Adleman
Sr	Wetboek van Strafrecht
Sv	Wetboek van Strafvordering
TK	Tweede Kamer
TTP	Trusted Third Party
WAHV	Wet administratiefrechtelijke handhaving verkeersvoorschriften
WED	Wet op de economische delicten
WVW	Wegenverkeerswet
WWM	Wet wapens en munitie

Auteur

Dr. B.J. Koops
Bert-Jaap Koops is postdoc bij het Centrum voor Recht, Bestuur en Informatisering van de Katholieke Universiteit Brabant. Zijn onderzoeksgebieden zijn ICT en strafrecht, en juridische aspecten van cryptografie. In 2000 en 2001 onderzoekt hij met een persoonsgerichte subsidie van NWO het grensvlak tussen opsporing en privacy onder invloed van ICT.
Koops studeerde wiskunde en algemene literatuurwetenschap in Groningen, werkte twee jaar als projectmedewerker bij Amnesty International, en werkte van 1994-1998 als assistent in opleiding bij het SamenwerkingsOrgaan Brabantse Universiteiten (KUB en TUE). Hij promoveerde in januari 1999 op een proefschrift over juridische en particuliere belangen bij encryptie.

WWW http://cwis.kub.nl/~frw/people/koops/bertjaap.htm
E-post e.j.koops@kub.nl

Onderzoeksrapporten die in de IT*e*R-reeks zijn verschenen:

- In het licht van de Wet Persoonsregistraties: Zon, maan of ster? (IT*e*R, nr. 1, 1995)
- Persoonsgegevens of niet: dat is de vraag (IT*e*R, nr. 2, 1996)
- De WPR als zon, maan of ster (IT*e*R, nr. 2, 1996)
- Auteursrechtvergoedingen in Europa en de VS (IT*e*R, nr. 2, 1996)
- Regulering van encryptie (IT*e*R, nr. 3, 1996)
- Smaad, laster, discriminatie en porno op het Internet (IT*e*R, nr. 3, 1996)
- De eeuwigdurende telecom-licentie (IT*e*R, nr. 4, 1996)
- Graafrechten voor telecommunicatievoorzieningen (IT*e*R, nr. 4, 1996)
- Veilen van frequenties (IT*e*R, nr. 4, 1996)
- Overheidsinformatie in de etalage (IT*e*R, nr. 5, 1997)
- Vastgoed persoonlijk benaderd (IT*e*R, nr. 5, 1997)
- Digitale manipulatie van beeldmateriaal: grenzen aan de grenzeloosheid (IT*e*R, nr. 6, 1997)
- Overheidstoezicht op bemiddelingsorganisaties in het auteursrecht (IT*e*R, nr. 6, 1997)
- De juridische status van de digitale handtekening (IT*e*R, nr. 7, 1997)
- Geschriften en handtekeningen: een achterhaald concept? (IT*e*R, nr. 7, 1997)
- Betrouwbaarheid van elektronische berichten in het betalingsverkeer (IT*e*R, nr. 7, 1997)
- De digitale handtekening. Juridische en organisatorische aspecten (IT*e*R, nr. 7, 1997)
- Het lichaam als sleutel. Juridische beschouwingen over biometrie (IT*e*R, nr. 8, 1997)
- Wiring government. Integrated public service delivery through ICT (IT*e*R, nr. 8, 1997)
- Interconnection disputes. Sweden, Great Britain and the United States (IT*e*R, nr. 8, 1997)
- Regulering van het Internet (IT*e*R, nr. 9, 1997)
- Naar een multimedia-bestendig auteursrecht (IT*e*R, nr. 10, 1998)
- Multimedialicenties. Enkele juridische en praktische knelpunten (IT*e*R, nr. 10, 1998)
- Exploitatie en clearance van i.e. rechten in een digitale omgeving (IT*e*R, nr. 10, 1998)
- Met recht een TTP! (IT*e*R, nr. 11, 1998)
- Electronic Commerce. Een privaatrechtelijk kader voor multilaterale EDI (IT*e*R, nr. 12, 1998)
- A formal analysis of Incoterms for electronic commerce (IT*e*R, nr. 12, 1998)
- Verschuivend vertrouwen. Methoden voor het waarborgen van betrouwbaarheid in het elektronisch rechtsverkeer (IT*e*R, nr. 12, 1998)
- Strafbare feiten op de elektronische snelweg (IT*e*R, nr. 13, 1998)
- Vertrouwelijkheid van e-mail (IT*e*R, nr. 13, 1998)
- Netwerkzoeking in theorie en praktijk (IT*e*R, nr. 13, 1998)
- Prijsbepaling voor elektronische overheidsinformatie (IT*e*R, nr. 14, 1998)
- Het adres in cyberspace heeft geen plaats (IT*e*R, nr. 15, 1998)
- Mechanismen voor de verdeling van telecommunicatienummers (IT*e*R, nr. 15, 1998)
- Toekenning van servicenummers met alfanumerieke betekenis (IT*e*R, nr. 15, 1998)
- Regulering van informatienummers (IT*e*R, nr. 15, 1998)
- De merken- en handelsnaamrechtelijke aspecten van het Domain Name System (IT*e*R, nr. 15, 1998)
- Wetgeving voor de Elektronische Snelweg (IT*e*R, nr. 16, 1999)
- Aansprakelijkheid voor schade aan apparatuur door mobiele telefoons (IT*e*R, nr. 17, 1999)
- Verhandelbaarheid van vergunningen in de telecomsector (IT*e*R, nr. 17, 1999)
- Regulatory review through new media in Sweden, the UK, and the USA: convergence or divergence of regulation? (IT*e*R, nr. 17, 1999)
- De juridische status van telefoonnummers. Opmerkingen over de plaats van het regio-telefoonnummer in het Nederlandse vermogensrecht (IT*e*R, nr. 17, 1999)
- Vertrouwelijk gegeven: Juridische beschouwingen over de verstrekking en het beheer van bedrijfsgegevens aan de overheid en het beheer daarvan door de overheid (IT*e*R, nr. 18, 1999)
- Politie en Intranet. Normering van netwerkkoppeling en grensoverschrijdend gebruik van multimediale databases op een internationaal politieel intranet (IT*e*R, nr. 19, 1999)
- Aansprakelijkheid, intermediairs en Electronic Data Interchange (IT*e*R, nr. 20, 1999)
- Aansprakelijkheid van de softwareleverancier voor de Millenniumbug (IT*e*R, nr. 20, 1999)
- Contracten van internetproviders: een adequate basis voor zelfregulering? (IT*e*R, nr. 21, 1999)
- ICT en straftoemeting: de conferentie van 23 april 1998 (IT*e*R, nr. 22, 1999)
- ICT en rechtvaardige strafoplegging bij zeden- en opiumzaken (IT*e*R, nr. 22, 1999)
- Electronic Highway of Electronic Subway? Verborgen merkinformatie op het Internet in Amerikaans perspectief (IT*e*R, nr. 23, 1999)
- Toepassing van privacyregels op elektronische berichten. Privacyregels voor Internetberichten (IT*e*R, nr. 24, 1999)
- Toepassing van privacyregels op elektronische berichten. Privacyregels voor EDI-berichten (IT*e*R, nr. 24, 1999)

- Knowing the law. Legal information systems as a source of knowledge (IT*e*R nr. 25, 1999)
- Constitutionele convergentie van pers, omroep en telecommunicatie (IT*e*R nr. 26, 2000)
- Verdeling van het spectrum (IT*e*R nr. 27, 2000)
- De universiteitsbibliotheek in het databankenrecht (IT*e*R nr. 28, 2000)
- Het bibliotheekprivilege in de digitale omgeving (IT*e*R nr. 29, 2000)
- De wenselijkheid en mogelijkheid van infiltratie en pseudo-koop op het Internet (IT*e*R nr. 30, 2000)