

Technische voorzieningen en cryptografie-onderzoek

Ot van Daalen

Technische voorzieningen en cryptografie-onderzoek

Ot van Daalen
Scriptiebegeleider: Prof. mr. E.J. Dommering

Doctoraalscriptie Nederlands Recht 2003
Universiteit van Amsterdam

Copyright © 2003 Ot van Daalen

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License."

Inhoudsopgave

Samenvatting	iii
Voorwoord	v
1 Inleiding	1
1.1 Vraagstelling	1
1.2 Opzet	2
2 Cryptografie	5
2.1 Geschiedenis	5
2.2 Technologie	7
2.3 Gebruik	9
2.4 Full disclosure v. bug secrecy	9
3 Technische voorzieningen in het recht	13
3.1 Het WIPO Auteursrechtverdrag	14
3.2 De Auteursrechtrichtlijn	15
3.3 Het wetsvoorstel	17
3.4 Verslag van de Kamercommissie	18
3.5 Nader verslag van Kamercommissie	18
3.6 Conclusie	19
4 Encryptie in de Verenigde Staten	21
4.1 Regulering	21
4.2 Prélude	22
4.3 De zaak Bernstein	22
4.4 De zaak Karn	25
4.5 De zaak Junger	27
4.6 Conclusie	27
5 Decryptie in de Verenigde Staten	29
5.1 Regulering	29
5.2 De zaak Felten	30
5.3 De zaak 2600	31
5.4 De zaak Elcomsoft	35
5.5 Voorbeelden van zelfcensuur	36
5.6 Conclusie	37

6	Encryptie in Europa en Nederland	39
6.1	Regulering	39
6.2	COCOM en Regeling van Wassenaar	40
6.3	Europa	41
6.3.1	De inhoudelijke regeling	42
6.4	Nederland	45
6.4.1	Nederlandse exportcontrole	46
6.4.2	Het uitgelekte wetsvoorstel	46
6.5	Conclusie	49
7	Decryptie in Nederland	51
7.1	Artikel 32a Auteurswet	51
7.2	Artikel 326c Wetboek van Strafrecht	52
7.3	De vrijheid van meningsuiting en software	54
7.4	Conclusie	56
8	Conclusie	59
	Bronnen	65
	GNU Free Documentation License	73

Samenvatting

Cryptografie is de kunst van de versleuteling en ontcijfering van informatie. In een maatschappij waar informatie een centrale rol speelt is het onderzoek naar technieken om informatie te beveiligen van groot belang.

Op dit moment is in de Tweede Kamer een wetsvoorstel in behandeling dat de verspreiding van omzeilingsmiddelen van technische voorzieningen verbiedt. Technische voorzieningen zijn technologische maatregelen die de exploitatie van, en toegang tot, auteursrechtelijk beschermde werken controleren. Technische voorzieningen worden meestal geïmplementeerd door middel van cryptografische technieken.

De verspreiding van kennis over kwetsbaarheden in cryptografische technieken is een essentieel onderdeel van het cryptografie-onderzoek. De vrijheid om deze kennis te verspreiden wordt echter beperkt door de wettelijke bescherming van technische voorzieningen. Kennis over een kwetsbaarheid in een technische voorziening kan namelijk worden aangemerkt als een omzeilingsmiddel.

De Europese en Nederlandse regelgever erkennen dat het onderzoek naar cryptografie kan worden beperkt door de bescherming van technische voorzieningen. In de parlementaire discussie heeft de Minister aangegeven dat de publicatie van serieus wetenschappelijk onderzoek naar kwetsbaarheden in technische voorzieningen is toegestaan. Tegelijkertijd moet de onderzoeker voorkomen dat anderen gemakkelijk auteursrechtinbreuk kunnen plegen met de resultaten van dat onderzoek.

Deze scriptie tracht beginselen te formuleren die de rechter kan hanteren bij het beslechten van een geschil waar de spanning tussen cryptografie-onderzoek en de bescherming van technische voorzieningen centraal staat. Daarbij wordt gekeken naar de Amerikaanse en Europees-Nederlandse regulering van kennis over cryptografie en kwetsbaarheden in informatiebeveiligingssystemen. De volgende beginselen komen naar voren.

Ten eerste blijkt uit de Amerikaanse jurisprudentie en de Europees-Nederlandse regelgeving dat kennis over cryptografie beschermd wordt door de vrijheid van meningsuiting. Ook als deze kennis is geformuleerd in een programmeertaal is deze beschermd door de vrijheid van meningsuiting.

De vorm waarin cryptografische kennis wordt geformuleerd kan wel een reden zijn om de verspreiding van deze kennis te beperken. Software die auteursrechtinbreuk actief bevordert is minder snel toelaatbaar dan software die slechts bedoeld is om een bepaalde stelling op wetenschappelijk verantwoorde wijze te ondersteunen.

Daarnaast is van belang of een beveiligingsmethode is verwerkt in andere

toepassingen dan technische voorzieningen. Een rechthebbende kan bijvoorbeeld niet voorkomen dat kennis over een kwetsbaarheid in de beveiliging van een financieel systeem wordt verspreid omdat deze kwetsbaarheid ook aanwezig is in een technische voorziening.

Ook speelt het forum waar deze kennis wordt verspreid een rol. Een forum waaraan met name serieuze cryptografie-onderzoekers deelnemen is een minder schadelijke plek voor het publiceren van kennis over kwetsbaarheden dan een forum waar met name auteursrechtinbreukmakers aan deelnemen.

Tot slot speelt de wijze waarop de kennis wordt verspreid een rol bij de beoordeling van de rechtmatigheid van een publicatie. De onderzoeker dient de producent van technische voorzieningen een redelijke termijn te gunnen om zijn systeem te repareren, alvorens de kwetsbaarheid te publiceren. Of een bepaalde termijn redelijk is hangt af van de vraag of de producent binnen die termijn redelijkerwijs de kwetsbaarheid kan repareren. Daarnaast moet de onderzoeker niet actief anderen aanmoedigen tot het plegen van auteursrechtinbreuk. Of dit het geval is zal aan de hand van de context van de publicatie moeten worden beoordeeld.

Voorwoord

Een belangrijk adagium van vrijheidslievende cybernauten is dat informatie vrij moet zijn. Een ander belangrijk adagium van deze gemeenschap is dat cryptografie vrij moet zijn. Deze twee adagia staan op gespannen voet. Sterke cryptografie verpakt informatie immers in onbreekbare schillen. Als sterke cryptografie beschikbaar komt zal het niet lang duren tot alle informatie achter slot en grendel verdwijnt.

De bescherming van technische voorzieningen kan deze ontwikkeling echter vertragen. Deze bescherming is gebaseerd op de veronderstelling dat de beperking van de verspreiding van kennis over kwetsbaarheden de veiligheid van beveiligingsystemen dient. Ik denk dat een dergelijk beleid de ontwikkeling van de beveiligingswetenschap juist remt, en de ontwikkeling van onbreekbare technische voorzieningen vertraagt.

Dit paradoxale beleid is de aanleiding om deze scriptie te schrijven. Toen ik aan mijn scriptie begon, in maart van dit jaar, lag het wetsvoorstel ter implementatie van de Auteursrechtlijn bij de Tweede Kamer. Een passage van dit wetsvoorstel is gewijd aan de verhouding tussen het cryptografie-onderzoek en technische voorzieningen. Het laat echter een aantal vragen over dit onderwerp open. Het was mijn bedoeling om deze vragen in een artikel aan de orde te stellen, zodat de parlementaire discussie hierover helderheid kon verschaffen.

Tegelijkertijd was ik bij Bits of Freedom gaan werken. Bits of Freedom adviseerde op dat moment GroenLinks bij het stellen van kamervragen over de implementatie van de Auteursrechtlijn. Een van de bijzondere aandachtspunten betrof de verhouding tussen cryptografie en technische voorzieningen. Mijn artikel werd een advies aan GroenLinks.

De antwoorden van de Minister bleken niet alle onduidelijkheid over bovenstaande spanning op te heffen. Deze scriptie bouwt voort op de discussie in de Tweede Kamer. Ik hoop dat de conclusie recht doet aan zowel de belangen van de cryptografie-onderzoeker als de belangen van de rechthebbende.

Ik bedank iedereen die tijdens het schrijven van deze scriptie opmerkingen heeft gegeven. In het bijzonder bedank ik Lodewijk Asscher, Rineke van Daalen, Anton Ekker, Bas Levinsohn en Gijs de Waal voor het becommentariëren van eerdere versies van dit document.

De scriptie is geschreven in \LaTeX formaat met behulp van GNU Emacs 21.2.1 op GNU/Linux (de Debian distributie). Het zetwerk is verzorgd door \TeX , het tekstopmaakstelsel van de hand van informatica-hoogleraar Donald Knuth. De scriptie is gezet in een 10-punts Palatino lettertype, ontworpen rond 1949 door Hermann Zapf.

De scriptie is uitgegeven onder de GNU Free Documentation License (GFDL).

Dat betekent, kort gezegd, dat deze scriptie mag worden gewijzigd en verspreid zonder voorafgaande toestemming van de auteur, mits de scriptie beschikbaar wordt gesteld onder de GFDL. Voor de precieze voorwaarden verwijs ik naar de GFDL, die in een bijlage bij deze scriptie is opgenomen.

Deze scriptie is geschreven van maart tot juli 2003. De scriptie is afgesloten op 30 juli 2003.

Amsterdam, 30 juli 2003.

Hoofdstuk 1

Inleiding

Cryptografie, de kunst van de versleuteling en ontcijfering van informatie, is een sleuteltechnologie in de informatiemaatschappij. Op dit moment ligt bij de Tweede Kamer het wetsvoorstel ter implementatie van de Europese Auteursrechtlijn. Een onderdeel van dit wetsvoorstel verbiedt de omzeiling van technische voorzieningen. Het wetsvoorstel scheidt echter geen uitzondering voor het onderzoek naar cryptografie.

Ervaring in de Verenigde Staten wijst erop dat de bescherming van technische voorzieningen het onderzoek naar cryptografie kan hinderen. In de Tweede Kamer zijn dan ook vragen gesteld naar de verhouding tussen de bescherming van technische voorzieningen en het onderzoek naar cryptografie. Hoewel in de parlementaire discussie een gedeelte van de onduidelijkheid over deze spanning is opgeheven behoudt de rechter interpretatieruimte in concrete gevallen.

De Nederlandse rechter zal de spanning tussen technische voorzieningen en cryptografie-onderzoek moeten beslechten aan de hand van een nog niet geformuleerd beslissingskader. Deze scriptie probeert een dergelijk beslissingskader te ontwikkelen, aan de hand van wetgeving en jurisprudentie in Amerika en Europa.

1.1 Vraagstelling

De vraagstelling van deze scriptie luidt:

1. Beperkt de bescherming van technische voorzieningen het onderzoek naar cryptografie?
2. Welke beginselen dient de Nederlandse rechter te hanteren bij de beoordeling van een concreet geschil waarin de spanning tussen de bescherming van technische voorzieningen en het onderzoek naar cryptografie centraal staat?

In het bijzonder komt het publiceren over kwetsbaarheden in cryptografische beveiligingsmechanismen aan bod. De scriptie gaat niet uitvoerig in op het verbod van de omzeilingsdaad.

De scriptie tracht de bovenstaande vraag te beantwoorden aan de hand van de ervaring die in Amerika is opgedaan met de regulering van cryptografie. Ook wordt gebruik gemaakt van de Europese en Nederlandse ervaring op dit gebied.

Overigens is de discussie over de regulering van encryptietechnologie verweven met de discussie over het verplicht ontsleutelen van geëncrypteerde boodschappen. Een dergelijke verplichting lijkt met name strijdig met het *ne-mo tenetur* beginsel, het beginsel dat niemand aan zijn eigen veroordeling hoeft mee te werken. Voor deze scriptie is dit onderwerp niet van belang, en deze scriptie besteedt hier geen aandacht aan.

Deze scriptie bespreekt daarnaast de regulering van cryptografie slechts vanuit het perspectief van de vrijheid van meningsuiting. De verhouding tussen de regulering van cryptografie en het recht op vertrouwelijke communicatie zoals neergelegd in artikel 8 EVRM en artikel 13 Grondwet komt slechts zijdelings aan de orde. Het gaat in dat laatste geval immers met name om een conflict tussen de nationale veiligheid en de privacy, een onderwerp dat slechts indirect raakt aan het onderzoek naar cryptografie in het algemeen.

Overigens kan men stellen dat software die technische voorzieningen omzeilt niet beschermd wordt door de vrijheid van meningsuiting, omdat de vrijheid van meningsuiting het exclusief recht van de auteur niet kán beperken. Hierover kan ik twee dingen zeggen. Het is ten eerste geen uitgemaakte zaak dat de vrijheid van meningsuiting niet een aparte beperking op het auteursrecht vormt. De in de loop van de jaren toegenomen reikwijdte van het auteursrecht zet deze klassieke doctrine onder druk. Maar ook als men aanneemt dat de vrijheid van meningsuiting het auteursrecht niet kan beperken, dan nog betekent dat niet dat de vrijheid van meningsuiting geen beperking vormt van het verbodsrecht ten aanzien van informatie over voorzieningen die auteursrecht *beschermen*. De twee klassieke rechtvaardigingsgronden van het auteursrecht, nut en billijkheid, strekken zich mijns inziens niet uit tot de bescherming van beveiligingstechnologie. Hoe het ook zij, in deze scriptie wordt aangenomen dat de vrijheid van meningsuiting wel een rol speelt bij de beoordeling van verboden om informatie over technische voorzieningen te verspreiden.

1.2 Opzet

Het tweede, volgende, hoofdstuk geeft achtergrondinformatie — de geschiedenis, de technologie en het gebruik van cryptografie komen aan de orde. Ook bespreekt dit hoofdstuk de discussie over de publicatie van kwetsbaarheden in beveiligingssystemen. Deze discussie is in het nadeel van openheid beslist, zo blijkt uit het derde hoofdstuk, dat het juridische kader van technische voorzieningen bespreekt. Hier komt de ontstaansgeschiedenis van artikel 6 van de Auteursrechtrichtlijn, dat technische voorzieningen beschermt, en het Nederlandse wetsvoorstel ter implementatie van dit artikel aan de orde. Vervolgens bespreekt de scriptie de regulering van cryptografie. Hoofdstuk vier bespreekt de Amerikaanse rechtszaken over het exportverbod op encryptiesoftware, en hoofdstuk vijf behandelt de Amerikaanse rechtszaken over de bescherming van technische voorzieningen. Hoofdstuk zes bespreekt de Nederlandse regulering van encryptiesoftware, en hoofdstuk zeven onderzoekt de Nederlandse ervaring met de bescherming van technische voorzieningen. De conclusie, in

hoofdstuk acht, formuleert een aantal beginselen die de rechter dient te hantieren bij het beslechten van concrete geschillen waar de spanning tussen cryptografie en de bescherming van technische voorzieningen centraal staat.

Hoofdstuk 2

Cryptografie

Cryptografie is de kunst en de wetenschap van het beveiligen van informatie.¹ Cryptografie omvat twee activiteiten: encryptie, de versleuteling van informatie, en decryptie, de ontcijfering van informatie. Hieronder wordt kort ingegaan op de geschiedenis, de technologie en het gebruik van cryptografie. Ook volgt een korte beschrijving van de discussie over de publicatie van kwetsbaarheden in beveiligingssystemen.

2.1 Geschiedenis

Cryptografie is zo oud als de menselijke communicatie. Herodotus schrijft dat in 500 voor Christus de verbannen Spartaan Demaratus een geheime boodschap zendt naar zijn oud-landgenoten over de aanstaande invasie van de Perzen.² Uit dezelfde tijd stamt de Spartaanse *σκυταλη*, één van de eerste voorbeelden van cryptografische technologie. Het systeem bestaat uit een stuk papyrus, gewikkeld rond een houten stok, waarop de verzender een boodschap in de lengte schrijft. Uitgerold bevat de strook papyrus een onbegrijpelijke verzameling letters, maar de ontvanger kan met een vergelijkbare stok de boodschap reconstrueren. Deze encryptietechniek is niet onfeilbaar — een verzameling stokken van verschillende dikte is voldoende om de boodschap te onthullen.

De geschiedenis van de cryptografie is een geschiedenis van maken en kraken. Van de Arabische wetenschappers in de achtste eeuw na Christus tot de Engelse geleerden in de 19e eeuw, de encryptie gaat hand in hand met de cryptanalyse, het achterhalen van versleutelde boodschappen. Eerst geschiedde dit nog door menselijk vernuft, maar later met computers en toegepaste wiskunde — een quantumsprong in de voortgang van het cryptografie-onderzoek.

Cryptografie heeft altijd een belangrijke rol gespeeld in de militaire communicatie. De uitkomst van de Eerste en de Tweede Wereldoorlog is voor een deel te danken aan de ontcijferkunsten van inlichtingendiensten. De pogingen van Engelse mathematici in Bletchley Park om de Duitse encryptiemachine Enigma te kraken hebben een belangrijk deel bijgedragen aan de overwinning van

¹Schneier 1996, p. 1.

²Singh 2000, p 4 citeert de *Historiæ* van Herodotus.

de Geallieerden in de Tweede Wereldoorlog.

Overheden houden streng toezicht op de verspreiding van cryptografie-technologie, opdat veiligheids- en inlichtingendiensten de vijand ongehinderd kunnen afluisteren. Die vijand is soms een ander land, en soms een interne dreiging. In Amerika is de National Security Agency (NSA) de belangrijkste luistervink. De NSA, in het geheim opgericht in 1952, houdt zich enerzijds bezig met de beveiliging van overheidsinformatie, en anderzijds met het afluisteren van communicatie. Een groot deel van het werk van de NSA bestaat uit het ontwikkelen, en breken, van cryptografische technologie.

De NSA ontwikkelde tot in de jaren zeventig vrijwel alle encryptietechnologie, met name voor overheidsgebruik. De transformatie naar een post-industriële maatschappij in de jaren zeventig creëerde echter bij private partij en een vraag naar sterke, vrijwel onbreekbare, encryptietechnologie. De NSA kon in deze vraag niet voorzien, omdat dit haar afluistermogelijkheden sterk zou beperken. Een aantal niet-NSA mathematici, bezorgd over het nakend gebrek aan privacy in het informatietijdperk, ontwikkelen rond die tijd geavanceerde encryptietechnieken voor privaat gebruik, dit tot ontsteltenis van de NSA, die haar cryptografiemonopolie ziet afbrokkelen.³

De eerste bres in het bastion van de NSA komt van de wiskundigen Whitfield Diffie en Martin Hellman, die in 1971 het artikel 'New Directions in Cryptography' publiceren. Het artikel introduceert een revolutionair concept in de cryptografie: 'Public Key Cryptography' (PKC). Een verzender en ontvanger kunnen met behulp van PKC een beveiligd communicatiekanaal opzetten via een niet-veilige verbinding. Hoewel het artikel de theorie introduceert komt de praktische implementatie van andere zijde. Die eer valt ten deel aan de wiskundigen Rivest, Shamir en Adelman, die in 1978 het algoritme RSA introduceren, vernoemd naar de beginletters van hun achternamen.

De Amerikaanse overheid, getuige van bovenstaande ontwikkelingen, tracht daarom sinds de jaren zeventig de ontwikkeling en verspreiding van cryptografische technologie en kennis te beperken. Zij verbiedt de export van encryptiesoftware, en ontmoedigt het cryptografie-onderzoek dat buiten de NSA plaatsvindt.

Deze pogingen hebben weinig succes. De derde bres in het bastion van de NSA komt van Phil Zimmerman, autodidact cryptograaf. Phil Zimmerman heeft een missie: de verspreiding van cryptografie. Zimmerman ontwikkelt aan de hand van het RSA-algoritme het encryptieprogramma Pretty Good Privacy (PGP). Rond die tijd ligt bij het Amerikaanse parlement een wetsvoorstel, S. 266, dat niet alleen de export van sterke cryptografie zou verbieden, maar ook het gebruik daarvan.⁴

Het zou slechts zijn toegestaan om informatie te versleutelen met cryptografische algoritmes die een achterdeur bevatten, zodat de Amerikaanse overheid met een universele sleutel toegang zou hebben tot de informatie die haar burgers versleutelen. Zimmerman verspreidt PGP via USENET over de hele wereld in een poging om krachtige cryptografie te redden zolang het gebruik hiervan nog is toegestaan. Binnen een dag krijgt hij enthousiaste brieven van PGP-gebruikers in andere landen. Zijn plan is gelukt, maar de Amerikaanse overheid is minder tevreden.

³Zie hierover Levy 2001.

⁴Levy 2001, p. 195.

Het vergunningstelsel dat aan bovenstaand exportverbod ten grondslag ligt is in het begin van de jaren negentig onderwerp geweest van drie rechtszaken, die in afdeling 4 worden besproken.

2.2 Technologie

Encryptie versleutelt informatie zodat derden de informatie niet kunnen lezen. Een leesbare boodschap kan door encryptie onleesbaar worden gemaakt — ‘hallo’ wordt ‘s73h@!jd.’ Hieronder wordt kort ingegaan op de werking van encryptie, waarbij de uitleg beperkt blijft tot de hoofdlijnen.

Encryptie kent twee verschillende technieken: symmetrische en asymmetrische encryptie. Symmetrische encryptie maakt gebruik van één sleutel, zowel voor de versleuteling en de ontcijfering. Asymmetrische encryptie kent twee verschillende sleutels; één om de informatie te versleutelen, en één om de informatie te ontcijferen.

Personen die niet beschikken over de ontcijfersleutel kunnen geëncrypteerde informatie op twee manieren proberen te achterhalen. Men kan alle mogelijke sleutels uitproberen; een *brute force attack*. Dit kan veel tijd kosten. Hoe langer de sleutel, hoe groter de mogelijkheden, en hoe meer tijd het kost om de juiste sleutel te achterhalen. Het is eleganter om aan de hand van ontwerp- of implementatiefouten een encryptiealgoritme te kraken. Dergelijke technieken bieden een kortere route naar de ontcijferde informatie.

Voor een goed begrip van de hieronder besproken rechtszaken is algemene kennis van de werking van computerprogramma's noodzakelijk. Daarom wordt hieronder kort ingegaan op de kernbegrippen die in de rechtszaken aan de orde komen.

Algoritmes Encryptie vindt plaats aan de hand van een algoritme, een verzameling instructies die informatie transformeert. Een algoritme dat de letters in een boodschap substitueert heet een *cipher*. Hieronder volgt een voorbeeld van een dergelijk algoritme, het zogenaamde *Caesar cipher*, vernoemd naar het Romeinse staatshoofd die zijn eerste gebruiker schijnt te zijn geweest.

voer op alle letters de volgende opdracht uit:
 verwissel de letter met de letter die zich
 drie plaatsen verder in het alfabet bevindt.

Dit algoritme kan ook in een wiskundige formule zijn opgeschreven, bijvoorbeeld:

$$G : \mathbb{N}/25\mathbb{N} \rightarrow \mathbb{N}/25\mathbb{N} \quad (2.1)$$

$$: n \mapsto n + 3 \quad (2.2)$$

Of het kan worden geschreven in een programmeertaal, zoals Perl:

```
#!/usr/bin/perl -p
y/A-Za-z/E-ZA-De-za-d/;
```

Algoritmes, waaronder cryptografische algoritmes, worden tegenwoordig meestal beschreven in een hogere-orde programmeertaal. Een hogere-orde programmeertaal abstraheert de werking van een programma van de beschrijving van dit programma, en maakt het ontwikkelingsproces van software overzichtelijker. Perl, C++ en Java zijn voorbeelden van dit soort programmeertalen, ieder met hun eigen lexicon en grammatica.

Broncode en objectcode De rechtszaken die in de volgende hoofdstukken aan de orde komen gaan gedeeltelijk over de vraag of algoritmes, in de vorm van een computerprogramma, beschermd zijn door de vrijheid van meningsuiting. De rechter maakt bij zijn analyse onderscheid tussen broncode en objectcode. Daarom wordt hieronder ingegaan op de verschillende verschijningsvormen van een computerprogramma.

Men ontwikkelt computerprogramma's meestal in *source code*, broncode. De broncode bevat opdrachten aan de computer om bepaalde handelingen uit te voeren. Men kan in de broncode ook commentaar verwerken, zodat anderen de werking van het programma beter begrijpen. Hieronder volgt de broncode van een simpel programma in C:

```
#include <stdio.h>
int main(void) {
    printf("hello world");
    return 0;
    /* dit is commentaar */
}
```

Het computerprogramma kan pas worden uitgevoerd op een computer als de broncode is gecompileerd. Compileren is het omzetten van de broncode in code die kan worden uitgevoerd op een specifiek besturingssysteem. De gecompileerde broncode noemt men objectcode. Objectcode is vrijwel onbegrijpelijk voor mensen. Een gedeelte van het bovenstaande programma ziet er in gecompileerde vorm als volgt uit:

```
double:t(0,18)=r(0,18);
24;0;__builtin_va_list:
t(0,19)=*(0,20)=(0,20).
./include/libc-symbols.
h../sysdeps/unix/sysv/l
inux/_G_config.h../sysd
eps/unix/sysv/linux/bit
```

Wetenschappers in de cryptografie beschrijven cryptografische algoritmes dus meestal in broncode.

Overigens is het onderscheid tussen broncode en objectcode een erfenis uit het verleden, toen de meeste computerprogramma's werden geschreven in programmeertalen die compilatie vereisten om te functioneren. Inmiddels bestaan er geavanceerde *scripting languages*, zoals Perl en PHP. Deze talen functioneren met behulp van een *interpreter*, die de opdrachten die in de scriptingtaal zijn geschreven direct uitvoert. Programma's die in een dergelijke taal zijn geschreven zijn dus direct uitvoerbaar, en toch leesbaar voor mensen. Dit in

tegenstelling tot objectcode, die weliswaar direct uitvoerbaar is, maar niet leesbaar is voor mensen, en broncode, die weliswaar leesbaar is, maar niet direct uitvoerbaar.

2.3 Gebruik

Cryptografie is een sleuteltechnologie in het informatietijdperk. Of, zoals de regering het uitdrukt in de Nota Wetgeving voor de Elektronische Snelweg: "cryptografische technieken spelen een belangrijke rol bij verschillende vormen van betrouwbaarheid."⁵

Cryptografie kent in ieder geval vier toepassingen. Ten eerste gebruikt men cryptografie ter afscherming van informatie, zoals computerbestanden, e-mail en spraaktelefonie. Een tweede toepassing, hieraan verwant, is de afscherming van communicatiekanalen, zoals draadloze netwerken en lease-lijnen. Cryptografie wordt ten derde gebruikt om de integriteit van informatie te verzekeren, opdat men zeker is dat informatie niet is gewijzigd. Tot slot kan cryptografie worden gebruikt ter identificatie.

In het dagelijks leven speelt cryptografie een belangrijke rol. Banken zijn afhankelijk van cryptografie om hun pinautomaten te beveiligen. Gebruikers van mobiele telefoons versleutelen hun communicatie met behulp van cryptografie. Mensenrechtenactivisten die leven onder repressieve regimes communiceren met behulp van cryptografie. Wachtwoorden zijn versleuteld met behulp van cryptografie. Op het Internet verzekert men de integriteit van bestanden met cryptografie. De rode telefoonlijn tussen Moskou en Washington is beveiligd met cryptografie.

De beveiliging van informatie vereist een paranoïde instelling. Zo is mijn webserver de laatste tien dagen 45 keer aangevallen. Dagelijks berichten softwarebedrijven over tientallen belangrijke en minder belangrijke gaten in computersystemen. Als een kwaadwillend persoon zich toegang verschafft tot mijn computer is het een geruststellend idee dat belangrijke informatie met behulp van sterke cryptografie is versleuteld. Cryptografie is niet een panacee voor deze gaten in de computerbeveiliging, maar het is wel een extra drempel voor de potentiële informatiedief of -dievegge.

Voor alle cryptografische toepassingen is het daarom van groot belang dat een encryptiealgoritme veilig is. Men moet er zeker van zijn dat het algoritme niet gemakkelijk kan worden gekraakt, anders heeft het gebruik van het algoritme immers geen nut.

Een informatiemaatschappij kan simpelweg niet zonder sterke cryptografie.

2.4 Full disclosure v. bug secrecy

Deze scriptie bespreekt onder meer de juridische status van informatie die beschrijft hoe men beveiligingsmechanismen kan omzeilen. De discussie over de publicatie van kwetsbaarheden in computersystemen is niet nieuw. Sinds het

⁵Kamerstukken II 1997/98, 25 880, nrs. 1-2, p. 47.

ontstaan van de wetenschap van de computerbeveiliging is reeds een discussie gaande over de gewenste methode van publicatie van kwetsbaarheden.⁶ De argumenten voor en tegen openheid over softwarefouten zijn door Schneier en Vidstrom samengevat.⁷ De discussie kan worden verdeeld in twee standpunten.

Aan de ene kant vindt men de optimisten, die geloven dat het mogelijk is om vrijwel veilige systemen te ontwikkelen. Het verzwijgen van kwetsbaarheden is voor optimisten ook een vorm van beveiliging, omdat zij ervan uitgaan dat anderen de kwetsbaarheden niet zullen ontdekken. Deze methode van beveiliging noemt men *'security through obscurity,'* of, duidelijker, *'bug secrecy.'*

Aan de andere kant ligt het kamp van de cynici, die geloven dat geen enkel systeem 'echt' veilig is. Als een systeem kan worden gebroken wordt het systeem gebroken. Optimale veiligheid ontstaat slechts bij de gratie van volledige openheid over de kwetsbaarheid van systemen — *full disclosure.*

Het debat komt, aldus Schneier, hierop neer: "Is the benefit of publicizing an attack worth the increased threat of the enemy learning about it?" Volgens Schneier is dit het geval. Full disclosure is een prikkel voor softwareproducenten om hun producten zo veilig mogelijk te maken, en te houden. Full disclosure voorkomt daarnaast de onwenselijke situatie dat slechts een beperkt groepje kwaadwillende krakers en beveiligingsexperts op de hoogte zijn van een kwetsbaarheid.

Maar hoewel openheid over kwetsbaarheden de softwareproducent prikkels geeft om zijn producten te beveiligen, stelt het kwaadwillende krakers ook in staat om deze informatie te misbruiken. Tegenstanders van full disclosure stellen daarom dat het veiliger is om de publicatie van informatie over kwetsbaarheden te beperken. Voorstanders van openheid brengen daartegen weer in, dat deze opvatting is gebaseerd op de veronderstelling dat degene die de kwetsbaarheid openbaart de eerste is die de kwetsbaarheid heeft ontdekt. Dat is niet altijd het geval, aldus Schneier. Soms weten bepaalde groepen al veel langer over het bestaan van een kwetsbaarheid, maar hebben zij deze informatie niet gepubliceerd.

De informatie die beschikbaar wordt gesteld, moet volgens Schneier zeer gedetailleerd zijn, omdat de producent anders kan volhouden dat de kwetsbaarheid niet bestaat, en omdat dit de stand van de beveiligingswetenschap kan bevorderen:

The only way to make vendors sit up and take notice is to publish details: both in human- and computer-readable form. [...] This free information flow, of both description and proof-of-concept code, is also vital for security research. [...] Full disclosure is essential if we are to continue to improve the security of our computers and networks.

Niet elke vorm van publicatie is echter acceptabel, aldus Schneier. Zo dient de onderzoeker de producent van tevoren op de hoogte te stellen over het bestaan van een kwetsbaarheid. De onderzoeker dient de producent een redelijke termijn te gunnen om een reparatiekit, een *patch*, voor de kwetsbaarheid beschikbaar te stellen. Daarnaast is het volgens Schneier niet juist om informatie

⁶Zie Zweers 2003.

⁷Schneier 2001 en Vidstrom 2003.

te publiceren in een vorm dat deze direct aangewend kan worden door onervaren kwaadwillende computergebruikers. Informatie in dergelijke vorm maakt systemen slechts kwetsbaarder, en bevordert de stand van de wetenschap niet.

Het idee dat slechts volledige openheid de stand van de beveiligingswetenschap kan bevorderen klinkt ook door in de oratie van Bart Jacobs van 16 mei 2003.⁸ Jacobs heeft deze rede uitgesproken in het kader van zijn aanvaarding van het ambt van hoogleraar Beveiliging en correctheid van programmatuur. Hij stelt dat wetenschappelijk onderzoek naar beveiliging van computersystemen er inherent op is gericht om fouten te vinden. Een verbod op de publicatie van dergelijk onderzoek leidt tot een verslechtering van beveiligingsmechanismen, aldus Jacobs.

Zoals in de volgende hoofdstukken zal blijken is de spanning tussen het cryptografie-onderzoek en de bescherming van technische voorzieningen een gevolg van de tegengestelde opvattingen die bestaan over het bereiken van optimale informatiebeveiliging.

⁸Jacobs 2003, p. 23.

Hoofdstuk 3

Technische voorzieningen in het recht

Rechthebbenden verspreiden auteursrechtelijk beschermde werken steeds vaker in digitale vorm. Muziek staat niet meer op vinyl, maar op CD. Films staan niet meer op video, maar op DVD. Een muzikliefhebber met een computer, een Internetaansluiting en een CD- of DVD-brander kan deze informatie zonder moeite lezen, kopiëren en wereldwijd distribueren. Rechthebbenden, die vrezen om de controle over hun 'content' te verliezen, beschermen hun informatie daarom met zogenaamde technische voorzieningen.

Technische voorzieningen die informatie beschermen zijn niet nieuw. Bladmuziek is sinds lang beschermd door onzichtbare inkt die strepen trekt door de kopieën. Omdat de reproductie en distributie van digitale informatie zo weinig kost is het kopiëren van informatie echter toegenomen. Om deze ontwikkelingen tegen te gaan is ook de toepassing van technische voorzieningen de laatste tijd toegenomen.

Men onderscheidt twee vormen van technische voorzieningen.¹ De eerste vorm is toegangscontrole: de rechthebbende controleert de *toegang* tot zijn werk met behulp van technische voorzieningen. De tweede vorm is exploitatiecontrole: de rechthebbende controleert de *exploitatiehandelingen* die de gebruiker kan verrichten met zijn werk. Landen verschillen met betrekking tot de exploitatiehandelingen die zij aan de rechthebbende toekennen. In Nederland omvat het auteursrecht de openbaarmaking en de verveelvoudiging van een werk.² In de Verenigde Staten omvat het auteursrecht onder meer het exclusief recht op de reproductie, distributie, publicatie en uitvoering van een werk.³

De implementatie van een systeem van toegangscontrole is betrekkelijk eenvoudig: de rechthebbende dient de toegang tot de informatie beperken. Dit gebeurt met name door encryptie. De rechthebbende versleutelt zijn informatie, en geeft de gebruiker de toegangssleutel.

In vergelijking daarmee is de implementatie van een systeem van exploitatiecontrole meer gecompliceerd. Hiertoe dient de rechthebbende immers elk middel te controleren dat een exploitatiehandeling mogelijk maakt. Een sys-

¹Zie bijvoorbeeld Koelman 2003.

²Art. 1 Aw.

³17 U.S.C. § 106.

teem van exploitatiecontrole van CD-muziek zou in ieder geval CD-spelers en CD-branders omvatten; CD-spelers maken openbaar, en CD-branders kunnen verveelvoudigen. Een systeem van exploitatiecontrole maakt noodzakelijkerwijs gebruik van een systeem van toegangscontrole. De rechthebbende versleutelt zijn informatie, en geeft de producent van geautoriseerde exploitatiemiddelen de toegangssleutel. De producent verwerkt de toegangssleutel vervolgens in geautoriseerde apparatuur.

3.1 Het WIPO Auteursrechtverdrag

De World Intellectual Property Organization (WIPO) tracht sinds de jaren negentig het auteursrecht in een digitaal jasje te steken. Deze pogingen mondden uit in het WIPO Auteursrechtverdrag (Wav) van 1996.⁴ Het WIPO onderkent in dit verdrag de rol die technische voorzieningen spelen in het digitale tijdperk.

Artikel 11 van het Wav beschermt technische voorzieningen. Het verplicht Verdragsluitende partijen tot “het voorzien in een adequate rechtsbescherming tegen het onwerkzaam maken van doeltreffende technische maatregelen die door auteurs worden gebruikt teneinde te beletten dat met betrekking tot hun werken niet-toegestane handelingen worden verricht.” Artikel 18 van het WIPO Verdrag inzake uitvoeringen en fonogrammen (Wuf) bevat een gelijklopende formulering.⁵ Het Cybercrime verdrag kan, als dit van kracht wordt, ook van belang zijn. Artikel 6 van dit verdrag stelt de distributie strafbaar van middelen waarmee, kort gezegd, computercriminaliteit kan worden bedreven.⁶ Ook de onlangs door de Europese Commissie voorgestelde IE richtlijn kan in de toekomst van belang worden.⁷ Artikel 21 van deze richtlijn zou, kort gezegd, de invoer, distributie en het gebruik van “onwettige technische middelen” verbieden. Elk technisch middel dat bedoeld is om technologie die is bedoeld om originele goederen te produceren te omzeilen zou onwettig zijn. Deze scriptie gaat verder niet in op het Cybercrime verdrag en de IE richtlijn.

Overigens beschermen beide verdragen daarnaast Digital Rights Management (DRM) systemen — systemen voor het beheer van rechten. Hoewel DRM systemen ook worden geïmplementeerd met behulp van cryptografische technieken komen de bepalingen hierover verder niet aan de orde in deze scriptie. De problematiek die speelt bij de bescherming van DRM systemen is echter vergelijkbaar met de problematiek ten aanzien van technische voorzieningen, en de conclusies van deze scriptie zijn daarom deels van toepassing binnen de context van DRM systemen.

Het Wav is op 6 maart 2002 in werking getreden door toetreding van Gabon. Het Wuf is op 20 maart 2002 in werking getreden door aansluiting van Honduras. Ingezetenen van verdragsluitende partijen kunnen zich sinds die datum in andere verdragsluitende landen beroepen op de bescherming van het Wav en het Wuf.

De Europese Gemeenschap en de Verenigde Staten hebben allebei het Wav ondertekend en implementatiestappen ondernomen. In de Verenigde Staten is

⁴*Trb.* 1997, 318 (de Engelse en Franse tekst), en *Trb.* 1998, 247 (de Nederlandse tekst).

⁵*Trb.* 1997, 319 (de Engelse en Franse tekst), en *Trb.* 1998, 243 (de Nederlandse tekst).

⁶*Trb.* 2002, 18.

⁷COM(2003)46 def.

artikel 11 van het Wav geïmplementeerd in afdeling 1201 van de Digital Millennium Copyright Act. Deze bepaling komt in afdeling 5 aan de orde. De Europese Gemeenschap heeft artikel 11 van het Wav omgezet in artikel 6 van de Auteursrechtlijn. Dit artikel, en de Nederlandse implementatie van dit artikel, komen hieronder aan de orde.

3.2 De Auteursrechtlijn

De geboorte van de Auteursrechtlijn is elders al uitgebreid besproken — hier wordt slechts kort ingegaan op de ontstaansgeschiedenis van artikel 6 van die richtlijn.⁸

In het Groenboek Auteursrecht in de Informatiemaatschappij vraagt de Europese Commissie aan belanghebbenden advies over een Europese bescherming van technische voorzieningen.⁹ In het vervolg op het Groenboek stelt de Commissie dat een meerderheid van de belanghebbenden een sterke bescherming van technische voorzieningen voorstaat.¹⁰ De Commissie roept marktpartijen op om tot standaardisering van beschermingssystemen te komen, en zij meent dat Europa deze ontwikkeling moet ondersteunen door technische voorzieningen bescherming te bieden.

Het eerste voorstel voor de Auteursrechtlijn, van 10 december 1997, reflecteert deze overwegingen.¹¹ Overweging 30 stelt dat, ten bate van de werking van de interne markt, rechtsbescherming geboden moet worden aan technische voorzieningen — toen nog aangeduid als ‘technologische’ voorzieningen. De Commissie merkt op dat “een dergelijke rechtsbescherming in overeenstemming moet zijn met het evenredigheidsbeginsel en niet mag leiden tot een verbod van inrichtingen of activiteiten die een ander doel of nut van commerciële betekenis dan het onwerkzaam maken van de technische beveiliging hebben.” Artikel 6 van het voorstel werkt deze beginselen uit. Het artikel verbiedt, kort gezegd, de opzettelijke productie en distributie van middelen die systemen van exploitatiecontrole omzeilen, en het opzettelijk verrichten van diensten die deze controle omzeilen. Deze activiteiten moeten, buiten het onwerkzaam maken van bedoelde voorzieningen, slechts een beperkt doel of nut van commerciële betekenis hebben.

Het Economisch en Sociaal Comité stelt in haar advies van 9 september 1998 voor om het verbod van artikel 6 uit te breiden tot de “promotie, reclame en marketing van apparatuur die speciaal dient tot het onwerkzaam maken van technologische voorzieningen.”¹² Het Europees Parlement introduceert op 10 februari 1999 in eerste lezing echter een geheel nieuwe formulering van artikel 6.¹³ Het voorstel van het Parlement verbiedt, kort gezegd, én de omzeilingsdaad, én de productie en distributie van omzeilingsmiddelen en diensten.

Vervolgens, in het gewijzigd voorstel voor een richtlijn van 12 mei 1999, gebruikt de Commissie dit voorstel van het Europees Parlement als uitgangs-

⁸Zie over de geschiedenis van de Auteursrechtlijn in het algemeen bijvoorbeeld Arkenbout 2001. Uitgebreid over de ontstaansgeschiedenis van technische voorzieningen is Koelman 2003.

⁹COM(95)382 def.

¹⁰COM(96)586 def.

¹¹COM(97)628 def., *PbEG* 1998, C 108/6.

¹²*PbEG* 1998, C 407/33.

¹³*PbEG* 1999, C 150/171.

punt.¹⁴ Omwille van de leesbaarheid verwisselt de Commissie overweging 30 in overwegingen 30 en 30bis, en ze introduceert twee relevante wijzigingen. Ten eerste stelt overweging 30bis nu expliciet dat de bescherming van technische voorzieningen met name het onderzoek op het gebied van de cryptografie niet mag hinderen. Uit de beschikbare documenten blijkt niet waarom deze uitzondering is geïntroduceerd. Ten tweede voegt de Commissie aan artikel 6 toe dat omzeiling slechts verboden is “indien deze handeling wordt verricht door een persoon die weet of redelijkerwijs behoort te weten wat het doel van deze handeling is” — zij formuleert een opzetvereiste.

De Raad publiceert op 28 september 2000 haar Gemeenschappelijk standpunt.¹⁵ Zij voegt de overwegingen 30 en 30bis weer samen in overweging 48. De cryptografie-exceptie blijft echter intact. De Commissie accepteert het Gemeenschappelijk standpunt van de Raad.¹⁶ Bij het Europees Parlement worden 200 amendementen ingediend, waarvan uiteindelijk slechts 9 door het Parlement worden aangenomen.¹⁷ Geen van de amendementen betreft het cryptografisch onderzoek of de bescherming van technische voorzieningen. Op 29 maart gaat de Europese Commissie akkoord met dit voorstel van het Parlement.¹⁸ De Auteursrichtlijn wordt gepubliceerd in de lente van 2001.¹⁹

De uiteindelijke richtlijn De Auteursrecht richtlijn wijdt de overwegingen 13 en 47 tot 53 aan de bescherming van technische voorzieningen. In dit verband is overweging 48 het interessantst. De overweging luidt, voor zover van belang:

[De rechtsbescherming van technische voorzieningen] moet in overeenstemming zijn met het evenredigheidsbeginsel en mag niet leiden tot een verbod van inrichtingen of activiteiten die een ander commercieel doel of nut hebben dan het omzeilen van de technische beveiliging. Deze bescherming mag met name het onderzoek op het gebied van de cryptografie niet hinderen.

Zoals hierboven opgemerkt wordt uit de beschikbare documenten niet duidelijk waarom deze cryptografie-exceptie is geïntroduceerd.

De bescherming van technische voorzieningen is uitgewerkt in artikel 6. Dit artikel verplicht de Lidstaten ten eerste om de daad van omzeiling te verbieden, als een persoon weet of redelijkerwijs behoort te weten dat hij aldus handelt. Op het verbod van de omzeilingsdaad wordt verder niet ingegaan.

Ten tweede verbiedt het artikel, kort gezegd, de distributie van-, het bezit voor commerciële doeleinden van middelen die-, en het verrichten van diensten die:

- a. gestimuleerd, aangeprezen of in de handel gebracht worden om de bescherming te omzeilen, of
- b. slechts een commercieel beperkt doel of nut hebben, naast de omzeiling van de bescherming, of

¹⁴COM(99)250 def., *PbEG* 1999, C 180/6.

¹⁵*PbEG* 2000, C 344/1.

¹⁶SEC(2000)1734 def.

¹⁷A5-0043/2001.

¹⁸COM(2001)170 def.

¹⁹Richtlijn 2001/29/EG, *PbEG* 2001, L 167/10.

- c. in het bijzonder ontworpen, geproduceerd of aangepast zijn met het doel de omzeiling mogelijk of gemakkelijker te maken van doeltreffende technische voorzieningen.

De richtlijn hanteert dus drie aanknopingspunten voor de beoordeling van de rechtmatigheid van omzeilingsmiddelen of -diensten. Diensten of middelen zijn onrechtmatig als ze (1) worden geadverteerd, (2) worden gebruikt of (3) zijn ontworpen als omzeilingsmiddel.

Overigens is het niet duidelijk of software als omzeilingsmiddel of -dienst aangemerkt zou moeten worden. In het vervolg zal worden gesproken van omzeilingsmiddelen.

Overweging 48 waarborgt dat het onderzoek naar cryptografie niet wordt gehinderd door de bescherming van technische voorzieningen. Zoals hieronder blijkt heeft de Nederlandse wetgever deze waarborg niet in het Nederlandse wetsvoorstel opgenomen.

3.3 Het wetsvoorstel

In Nederland is het wetsvoorstel ter implementatie van de Auteursrechtlijn op dit moment in behandeling bij het parlement. De artikelen 29a van de Auteurswet, 19 van de Wet op de Naburige Rechten en 5a van de Databankwet implementeren artikel 6 van de richtlijn.²⁰ De formulering van de bovenstaande bepalingen stemt vrijwel overeen met de tekst van de richtlijn.²¹ Het wetsvoorstel schept geen uitzondering voor het onderzoek naar de cryptografie, en wijdt hieraan verder geen aandacht.

De regering riep belanghebbenden op om reactie te geven op de vragen over het wetsvoorstel.²² Naar mijn weten heeft geen enkele partij de gevolgen van het wetsvoorstel voor het cryptografie-onderzoek aangestipt. Zelfs de Nederlandse Organisatie voor Wetenschappelijk onderzoek wijdt in haar commentaar geen woord aan deze kwestie. Ook het advies van de Raad van State gaat niet in op het cryptografisch onderzoek.²³

Op 9 oktober 2002 sturen twintig verontruste geïnteresseerden daarom een brief naar de leden van de Vaste Kamercommissie van Justitie van de Tweede Kamer.²⁴ Zij vragen aandacht voor de bedreiging die het huidige wetsvoorstel meebrengt voor het wetenschappelijk onderzoek naar computerbeveiliging, omdat deze de publicatie van dergelijk onderzoek onrechtmatig dreigt te verklaren, "terwijl die publicatie nu juist een essentieel onderdeel vormt van het wetenschappelijk discours."

Zij roepen op om "een expliciete vrijwaring te creëren in het wetsvoorstel van consumenten- en onderzoeksrechten, conform overweging 48 van de Richtlijn." Deze brief is ook geplaatst in het Financieele Dagblad van 5 februari 2003.²⁵

²⁰Kamerstukken II 2001/02, 28 482, nrs. 1–2.

²¹Zo ook de MvT, Kamerstukken II 2001/02, 28 482, nr. 3, p. 27.

²²Zie de website van het Ministerie van Justitie: <http://www.justitie.nl/themas/wetgeving/dossiers/auteursrecht/>.

²³Kamerstukken II 2001/02, 28 482, nrs. A en B.

²⁴Te vinden op: <http://www.bof.nl/nieuws/021108.html>.

²⁵Huizer e.a. 2003.

3.4 Verslag van de Kamercommissie

De Vaste Kamercommissie van Justitie heeft dit bericht gelezen, zo blijkt uit de vragen die de leden van de verschillende fracties hierover hebben gesteld. In het Verslag stellen zij de eerste vragen.²⁶ De LPF-leden van de Commissie vragen aan de regering om het “ontbreken van voorzieningen voor onderzoek naar beveiliging en versleuteling tot een belemmering van dat onderzoek” te verklaren. De leden van de SGP-fractie formuleren het duidelijker.²⁷ Zij vragen of de publicatie van onderzoek naar de kwetsbaarheid van netwerken en informatietechnieken kan worden gekwalificeerd als een overtreding van artikel 29a Auteurswet. Ook vragen zij hoe artikel 29a zich verhoudt tot overweging 48 van de Richtlijn.

Op 21 maart 2003 heeft Minister Donner deze vragen beantwoord in de Nota naar aanleiding van het Verslag. De Minister ziet geen aanleiding om een expliciete cryptografie-exceptie in de wet op te nemen.²⁸ De Minister stelt enerzijds dat de publicatie van “serieus wetenschappelijk onderzoek” niet door deze richtlijn wordt geraakt, omdat dit niet tot doel heeft om technische voorzieningen te omzeilen. Anderzijds merkt de Minister op dat het handelen in strijd met artikel 29a als onrechtmatige daad moet worden gekwalificeerd. Een rechtvaardigingsgrond kan een dergelijke handeling haar onrechtmatig karakter doen verliezen.

De waarborg die de Minister hier aanstipt voor de publicatie van beveiligingsonderzoek is naar de mening van de Vaste Kamercommissie niet voldoende. Toen zich een nieuwe vragenronde voordeed hebben de leden over dit onderwerp aanvullende vragen gesteld.

3.5 Nader verslag van Kamercommissie

Groenlinks, PVDA en de VVD stellen alledrie vragen over cryptografie in het Nader Verslag van de Vaste Kamercommissie.²⁹ Ten eerste bepleit GroenLinks de opnemng van een *expliciete* uitzondering voor het doen van cryptografisch onderzoek. Het bestaan van een rechtvaardigingsgrond kan, aldus GroenLinks, pas in de rechtszaal worden vastgesteld, en onduidelijkheid hierover zal wetenschappers al bij voorbaat beperken in hun academische vrijheid.

Op advies van de auteur van deze scriptie heeft GroenLinks ook gevraagd of een rechthebbende kan voorkomen dat zwakheden in publiekelijk beschikbare algoritmes die niet zijn ontwikkeld door een rechthebbende worden gepubliceerd. Het publiek belang kan immers gediend zijn bij een open discussie over de zwakheden in beveiligingsmechanismen die een brede toepassing kennen, ook al worden hierdoor de zwakheden in DRM systemen blootgelegd.

Ook de leden van de PVDA-fractie maken zich zorgen over de implicaties van de bescherming van technische voorzieningen voor het onderzoek naar informatiebeveiliging, met name binnen de context van de innovatie en open source software.³⁰ De VVD-fractie merkt in twee zinnen op dat het onderzoek

²⁶ *Kamerstukken II* 2002/03, 28 482, nr. 4.

²⁷ *Kamerstukken II* 2002/03, 28 482, nr. 4, p. 18–19.

²⁸ *Kamerstukken II* 2002/03, 28 482, nr. 5, p. 42.

²⁹ *Kamerstukken II* 2002/03, 28 482, nr. 7, p. 15.

³⁰ *Kamerstukken II* 2002/03, 28 482, nr. 7, p. 12.

naar cryptografie kan worden gehinderd door de bescherming van technische voorzieningen.³¹

Minister Donner beantwoordt de vragen in een korte paragraaf in de Nota naar aanleiding van het nader verslag van 21 mei 2003.³² Hij stelt dat van een wetenschapsbeoefenaar mag worden verwacht dat “hij zorgvuldig handelt en ertegen waakt dat door zijn onderzoek zo veel mogelijk derden op eenvoudige wijze technische beschermingsvoorzieningen kunnen omzeilen.” Hoewel de Minister wel vaststelt dat rechthebbenden geen open source software gebruiken in hun beschermingsmaatregelen, gaat hij niet in op de vraag van GroenLinks of publiekelijk beschikbare algoritmes anders behandeld dienen te worden dan *proprietary* beschermingsmaatregelen. Tot slot zou het leerstuk van de onrechtmatige daad overigens voldoende van toepassing zijn.

3.6 Conclusie

De Europese en Nederlandse wetgever onderkennen dat een spanning bestaat tussen de bescherming van technische voorzieningen en cryptografie-onderzoek. Dit blijkt uit de Auteursrechtlijn, die in overweging 48 een expliciete uitzondering bevat voor het cryptografie-onderzoek. Het blijkt ook uit de discussie tussen de Minister en de kamerleden in de Tweede Kamer over het wetsvoorstel.

Een expliciete cryptografie-exceptie acht de regering echter niet nodig. De Minister geeft wel een aantal aanknopingspunten voor de beoordeling van de rechtmatigheid van een publicatie over zwakheden in een systeem van technische voorzieningen.

Ten eerste zal wetenschappelijk onderzoek naar beveiliging en versleuteling volgens de Minister niet tot doel hebben om technische voorzieningen te omzeilen. Daarom zou het doen van dit onderzoek niet onrechtmatig zijn op grond van artikel 29a. De publicatie van serieus wetenschappelijk onderzoek op dit terrein zou daarnaast niet onder de richtlijn vallen. Dit blijkt uit de Nota naar aanleiding van het verslag.

Ten tweede geeft de Minister aan dat van een wetenschapsbeoefenaar verwacht mag worden dat hij zorgvuldig handelt en tracht te voorkomen dat anderen door zijn onderzoek op eenvoudige wijze technische beschermingsvoorzieningen kunnen omzeilen.

Deze twee opmerkingen lijken betrekkelijk helder, maar leggen tegelijkertijd de kern van het probleem bloot. Immers, een van de voorwaarden van wetenschappelijkheid is reproduceerbaarheid — een artikel dient een herhaalbaar bewijs te leveren, opdat andere wetenschappers de resultaten kunnen verifiëren. Een opmerking in een artikel met de strekking: “wij hebben een gat gevonden, maar we kunnen helaas niet aangeven waar het gat ligt” kan niet als serieus onderzoek worden gekwalificeerd, ook niet in de beveiligingswereld.

Aan de andere kant eist de Minister zorgvuldigheid van de zijde van de wetenschapper. Hij moet trachten te voorkomen dat anderen door zijn onderzoek op eenvoudige wijze technische voorzieningen kunnen omzeilen. Maar als de wetenschapper resultaten publiceert die zijn collega's niet in staat stel-

³¹Kamerstukken II 2002/03, 28 482, nr. 7, p. 12.

³²Kamerstukken II 2002/03, 28 482, nr. 8, p. 18.

len om op eenvoudige wijze technische voorzieningen te omzeilen dan is het onderzoek niet herhaalbaar — en dus niet wetenschappelijk.

De Minister vraagt van wetenschappers het onmogelijke — of niet? Wellicht kunnen andere aanknopingspunten uitkomst bieden. In de volgende hoofdstukken wordt ingegaan op verbodsbepalingen ten aanzien van het publiceren van onderzoek inzake encryptie en decryptie in Amerika en Europa.

Hoofdstuk 4

Encryptie in de Verenigde Staten

Zoals gezegd houdt de Amerikaanse wetgever de ontwikkeling van cryptografische technologie nauwlettend in de gaten. Zij tracht het gebruik, de ontwikkeling en de export van encryptietechnologie te beperken, zodat haar inlichtingendiensten de vijand ongehinderd kunnen afluisteren. In het begin van de jaren negentig zijn over dit beleid drie uitgebreide rechtszaken gevoerd. Deze rechtszaken komen hieronder aan de orde.

4.1 Regulering

De Amerikaanse overheid reguleert encryptietechnologie door middel van een vergunningstelsel. Dit stelsel is de afgelopen jaren een paar keer aangepast, en wordt ook nu nog bij tijd en wijle veranderd.¹

Het vergunningstelsel werkt als volgt. De Arms Export Control Act (AECA) geeft de President de bevoegdheid om de export en import van militaire producten en diensten te controleren.² De President kan producten en diensten met een militair karakter op de United States Munitions List (USML) plaatsen. Voor de import en export van producten en diensten die op de USML staan is een vergunning vereist. De International Traffic in Arms Regulations (ITAR) zijn uitgevaardigd ter implementatie van de AECA. Het Department of State van de Director of the Office of Defense Trade Controls (ODTC) voert de ITAR uit.

De ITAR kennen een zogenaamde 'commodity jurisdiction procedure' (CJ), op grond waarvan de ODTC beslist of een bepaald artikel of een bepaalde dienst door de USML wordt bestreken. Op grond van de ITAR is voor de export van cryptografische software een vergunning nodig. Ook kan informatie over cryptografische technieken onder het exportverbod vallen. De ITAR bevatten uitzonderingen voor 'mass market software' en cryptografische software die wordt gebruikt in pinautomaten.

¹Zie voor een overzicht van de wijzigingen de website van Bert-Jaap Koops, <http://rechten.kub.nl/koops/cryptolaw/>.

²22 U.S.C. § 2778 e.v.

Op 15 november 1996 heeft de overheid de regels inzake de im- en exportcontrole van encryptietechnologie veranderd. Dit deed zij terwijl twee van de drie encryptie-rechtszaken liepen. Cryptografie is nadien gereguleerd op grond van de Export Administration Regulations (EAR), uitgevaardigd door het Department of Commerce. Encryptietechnologie die voorheen werd gekwalificeerd als 'munition' op grond van de USML is nu onder de Commerce Control List (CCL) geplaatst, en het Bureau of Export Affairs (BXA) behandelt vergunningaanvragen. Deze regelingen zijn na 1996 nog een paar keer gewijzigd, maar die wijzigingen zijn voor deze scriptie niet van belang.

In de rechtszaken over dit exportverbod stelden de eisers dat het onduidelijk was welke informatie over cryptografie onder het exportverbod valt, en dat het vergunningstelsel het cryptografisch onderzoek beperkt. Hieronder worden deze rechtszaken besproken, na een korte prélude.

4.2 Prélude

Het beleid van de Amerikaanse overheid richtte zich sinds de jaren zeventig op het beperken en ontmoedigen van onderzoek naar de cryptografie. De overheid was zich terdege bewust dat dit beleid op gespannen voet staat met de vrijheid van meningsuiting. Uit notities van 1978 tot 1984 blijkt dat de Amerikaanse regering over deze spanning een aantal keer advies heeft gevraagd aan haar interne juridische adviseurs. Het antwoord van het Office of Legal Counsel is steeds dat de exportverboden in strijd kunnen zijn met het First Amendment.³ Zo schrijft het Office of Legal Counsel in 1984: "we concluded that the ITAR also presents serious First Amendment problems."

Olie op het vuur van de cryptografen; de rechtszaken kunnen beginnen.

4.3 De zaak Bernstein

De meest invloedrijke rechtszaak over de exportcontrole is *Bernstein*. Daniel Bernstein is een gerenommeerd computerbeveiligingsdeskundige. Zo heeft hij een van de meest veilige mailservers ontwikkeld, `qmail`. Bernstein schrijft ten tijde van de eerste rechtszaken een proefschrift over cryptografie aan de Universiteit van Berkeley in Californië. Tijdens zijn studie ontwikkelt Bernstein een encryptie- en decryptiealgoritme, genaamd 'Snuffle.' Het algoritme, een 'one way hash mechanism,' heeft hij op zo een manier ontworpen dat er onduidelijkheid over bestaat of deze technologie onder het vergunningstelsel valt. Bernstein beschrijft de algoritmes in een wetenschappelijk artikel, genaamd 'The Snuffle Encryption System.' Ook beschrijft hij de algoritmes in broncode, in bestanden die hij 'snuffle.c' en 'unsnuffle.c' noemt. De bestanden hebben de extensie '.c' omdat ze zijn geschreven in de programmeertaal C.

Bernstein verzoekt de overheid op 30 juni 1992 om te bepalen of voor de export van het wetenschappelijk artikel en de beide algoritmes een vergunning nodig is. De brief van Bernstein stelt dat hij deze informatie wil publiceren op een nieuwsgroep genaamd `sci.crypt`, terwille van discussie door de 'worldwide academic community.'

³De brieven zijn te vinden op: <http://cr.yip.to/export/1984/0705-simms.txt> en <http://cr.yip.to/export/1984/0828-olson.txt>.

Na een intensieve briefwisseling tussen Bernstein en de overheid blijkt dat een exportvergunning is vereist voor *snuffle.c* en *unsnuffle.c*.⁴ Bernstein gaat hiertegen in beroep op 22 september 1993. Ondertussen start hij echter ook een rechtszaak waarin hij de constitutionaliteit van de wet *prima facie* betwist. Hij wordt in deze zaak verdedigd door Cindy Cohn en Lee Tien, beiden als *pro bono* advocaten verbonden aan de Electronic Frontier Foundation.

Het District Court Bernstein stelt dat de ITAR in strijd is met de Amerikaanse Constitutie. Hij baseert zich hierbij op een aantal argumenten. Zijn belangrijkste argument is dat een vergunningenstelsel voor het publiceren van informatie over cryptografie in strijd is met de uitingsvrijheid.

De rechtbank behandelt in haar eerste beslissing de vraag in welke mate de resultaten van cryptografisch onderzoek een vorm van 'speech' zijn, en in welke mate deze resultaten dus zijn beschermd door de vrijheid van meningsuiting.⁵ "The paper, an academic writing explaining plaintiff's scientific work in the field of cryptography, is speech of the most protected kind," aldus de rechter. Maar ook broncode is een vorm van speech die is beschermd door het First Amendment:

This court can find no meaningful difference between computer language, particularly high-level languages as defined above, and German or French. [sic, OvD] All participate in a complex system of understood meanings within specific communities.

Dat broncode een functioneel aspect heeft, ze kan immers worden omgezet in een functioneel computerprogramma, doet volgens de rechtbank aan deze vaststelling niet af.

Op 9 december 1996 doet de rechtbank voor de tweede keer uitspraak in de zaak *Bernstein*, ditmaal over de constitutionaliteit van de ITAR en de AECA.⁶ De rechtbank wijdt een groot deel van zijn uitspraak aan de constitutionaliteit van het vergunningenstelsel. Een vergunningenstelsel dat de vrijheid van meningsuiting beperkt dient te voldoen aan drie voorwaarden, aldus de rechtbank. Ten eerste kan een voorafgaande beperking slechts voor een korte periode worden toegepast. Ten tweede moet een snelle rechterlijke toetsing van de beperking beschikbaar zijn, en ten derde rust op de overheid de bewijslast dat het vergunningenstelsel in overeenstemming is met de vrijheid van meningsuiting. De ITAR voldoet aan geen van de voorwaarden, en is daarom in strijd met de Constitutie.

De rechtbank wijdt een aantal overwegingen aan de onbepaaldheid (*vagueness*) van de ITAR. Zo scheidt de ITAR een uitzondering op het exportverbod met betrekking tot "information available to the public through fundamental research in science and engineering." Volgens de rechtbank is deze uitzondering niet voldoende duidelijk toepasbaar:

[T]he uncertainty created in scientists about what speech is subject to regulation under the ITAR is unacceptable. [...] [I]t would be

⁴Zie voor een overzicht van de briefwisseling <http://cr.yip.to/export/docs.html>.

⁵*Bernstein v. U.S. Dept. of State*, 922 F.Supp. 1426 (N.D.Cal. 1996).

⁶*Bernstein v. U.S. Dept. of State*, 945 F.Supp. 1279 (N.D.Cal. 1996). Dit was een verzoek van beide zijden om *summary judgment*.

hard for scientists to discern when their work was a defense article and when it was wholly exempt from the ITAR without going through a CJ determination before any effort at publication. In fields of applied science, what is commonly taught in universities may well overlap with what the government might choose to regulate. In this instance the deterrent effect on protected expression appears both real and substantial. These academic exemptions from the definition of technical data [...] are accordingly void for vagueness. (citaten weggelaten)

Deze overweging is interessant in verband met de Nederlandse regulering van technische voorzieningen. Zoals in afdeling 3.4 is geschreven kent de toelichting bij de implementatiewet van de Auteursrechtlijn een bijzondere status toe aan het serieus wetenschappelijk onderzoek naar technische voorzieningen, maar geeft zij niet duidelijk aan wanneer resultaten de vrucht zijn van wetenschappelijk onderzoek. De bovenstaande overwegingen van het District Court leiden tot de conclusie dat deze onzekerheid over toegestane vormen van onderzoek een beperking van de vrijheid van meningsuiting tot gevolg heeft.

Zoals in afdeling 4.1 is aangegeven wijzigt de overheid in 1996 de regels met betrekking tot de export van encryptietechnologie. Omdat de regels zijn gewijzigd wendt Bernstein zich voor een derde maal tot de rechter. Hij vordert dat de rechtbank ook de nieuwe regels in strijd verklaart met de Constitutie.

Op 25 augustus 1997 oordeelt de rechtbank over de nieuwe regels.⁷ De rechtbank bevestigt haar eerdere bevindingen, en oordeelt dat ook de nieuwe regels in strijd zijn met de Constitutie. De rechtbank verbiedt bij voorlopige voorziening (*preliminary injunction*) de overheid om de regels te handhaven jegens eenieder die het encryptieprogramma van Bernstein gebruikt, bespreekt of publiceert.

Het Court of Appeals De overheid gaat tegen dit oordeel in beroep, en op 6 mei 1999 doet het Court of Appeals for the Ninth Circuit, Californië, uitspraak.⁸ De lijst van *amici curiae* leest als een ware *who's who* van de digitale gemeenschap. Prominente belanghebbenden buigen zich over de zaak, waaronder de organisaties EPIC, ACLU, CDT en PI, maar ook de cryptografiedeskundigen Diffie, Neumann en Rivest dienen een *amicus brief* in.

Het Court of Appeals bevestigt het verbod van de rechtbank in eerste instantie. Zij stelt in krachtige termen dat broncode is beschermd door de vrijheid van meningsuiting, en dat het vergunningstelsel in strijd is met de vrijheid van meningsuiting. Deze overwegingen worden hier verder niet herhaald. Het Court of Appeals doet geen uitspraak over de vraag of objectcode ook voldoende communicatieve waarde heeft om onder de vleugels van het First Amendment te worden geplaatst, omdat deze vraag niet aan de orde is in de rechtszaak. Bernstein's algoritme is immers opgesteld in broncode.

De beroemde eindoverwegingen van het Court of Appeals zijn de moeite waard om te citeren.

⁷Bernstein v. U.S. Dept. of Justice, 974 F. Supp. 1288 (N.D.Cal. 1997).

⁸Bernstein v. U.S. Dept. of Justice, 176 F.3d 1132, (9th Cir. 1999), *MediaForum* 1999/10, m.nt. L.F. Asscher.

[W]e note that insofar as the EAR regulations on encryption software were intended to slow the spread of secure encryption methods to foreign nations, the government is intentionally retarding the progress of the flourishing science of cryptography. To the extent the government's efforts are aimed at interdicting the flow of scientific ideas (whether expressed in source code or otherwise), as distinguished from encryption products, these efforts would appear to strike deep into the heartland of the First Amendment. [...] ¶ [T]he government's efforts to regulate and control the spread of knowledge relating to encryption may implicate more than the First Amendment rights of cryptographers. In this increasingly electronic age, we are all required in our everyday lives to rely on modern technology to communicate with one another. This reliance on electronic communication, however, has brought with it a dramatic diminution in our ability to communicate privately. [...] Whether we are surveilled by our government, by criminals, or by our neighbors, it is fair to say that never has our ability to shield our affairs from prying eyes been at such a low ebb. The availability and use of secure encryption may offer an opportunity to reclaim some portion of the privacy we have lost. [...] [I]t is important to point out that *Bernstein's* is a suit not merely concerning a small group of scientists laboring in an esoteric field, but also touches on the public interest broadly defined.

De overheid vraagt het Court of Appeals om een *rehearing*, een nieuwe behandeling van de zaak. Op 30 september 1999 besluit het Court of Appeals om de zaak *en banc*, met de voltallige kamer, opnieuw te horen.⁹ Op 11 april 2000 verwijst het Court of Appeals de zaak naar het District Court, die ten tijde van dit schrijven nog geen uitspraak heeft gedaan vanwege de continue wijzigingen van het exportbeleid.

Hoe het ook zij, het recente juridische steekspel mist het vuur en de relevantie van de eerdere zaken, en deze scriptie gaat op *Bernstein* verder niet in.¹⁰

4.4 De zaak Karn

De tweede encryptie-rechtszaak, *Karn*, draait om één van de bijbels van de cryptografie, het boek *Applied Cryptography* van Bruce Schneier. Het boek beschrijft onder andere de werking van de meest bekende encryptiealgoritmes. Hoofdstuk vijf bevat een paar van deze algoritmes in broncode. Deze algoritmes zijn ook opgeslagen op twee diskettes. Philip Karn wil het boek en de diskettes exporteren, en hij dient hiertoe op 12 januari 1994 een CJ verzoek in bij de ODTC, met het verzoek om vast stellen of een vergunning is vereist voor de export van het boek en de diskettes.

De ODTC besluit op 2 maart 1994 dat voor de export van het boek geen vergunning nodig is. De twee diskettes mogen echter niet zonder vergunning

⁹*Bernstein v. U.S. Dept. of Justice*, 192 F.3d 1308 (9th Cir. 1999).

¹⁰Zie voor de huidige ontwikkelingen de website van *Bernstein*: <http://cr.yip.to/export/docs.html>.

worden geëxporteerd. Karn gaat tegen deze beslissing in administratief beroep, maar het beroep wordt afgewezen op 7 oktober 1994. Ook het hierop volgend administratief beroep wordt op 13 juni 1995 afgewezen. Op 21 september 1995 maakt Karn daarom een zaak aanhangig bij de rechtbank.¹¹ De zaak *Bernstein* is dan al in volle gang.

Ook Karn stelt, onder andere, dat de afwijzing van de exportvergunning in strijd is met de vrijheid van meningsuiting. De rechtbank van het District of Columbia doet op 22 maart 1996 uitspraak.¹²

Het commentaar in de broncode — niet de programmeerinstructies — is volgens de rechtbank tot op zekere hoogte beschermd door het First Amendment. Een exportverbod op encryptietechnologie beperkt daarom de vrijheid van meningsuiting.

De toelaatbaarheid van deze beperking is echter afhankelijk van de ratio die ten grondslag ligt aan de beperking. Als de beperking ziet op inhoud van de uiting past de rechter *strict scrutiny* toe; een strenge toets. Als de ratio van de beperking niet op de inhoud van de uiting is gebaseerd dan dient de beperking te voldoen aan *intermediate scrutiny*; een mildere toets. De laatste toets, geformuleerd in *O'Brien*, vereist dat de beperking belangrijke overheidsbelangen nastreeft zonder de uitingsvrijheid disproportioneel te belasten.¹³ De rechtbank stelt de vraag welke ratio ten grondslag ligt aan het vergunningstelsel.

Volgens de rechtbank is de beperking in onderhavig geval inhoudsonafhankelijk. De overheid reguleert de export van de diskette niet vanwege de inhoud van het commentaar bij de broncode, maar om te voorkomen dat functionele encryptietechnologie in de handen komt van buitenlandse veiligheidsdiensten. Dit ontlokt aan de eisers de cynische opmerking: “they think terrorists can’t type?” Immers, het maakt voor de beschikbaarheid van de algoritmes vrijwel geen verschil of de broncode in een boek is gedrukt of is opgeslagen op een diskette. De rechtbank laat echter beleidsmatige beslissingen aangaande de nationale veiligheid over aan de wetgever, en hij wijst de vordering af.

Philip Karn gaat in beroep. Inmiddels voegen zich ook in deze rechtszaak de ACLU en de EPIC als *amici curiae*. Nadat de partijen hun stukken hebben uitgewisseld, maar voordat de rechtbank uitspraak heeft gedaan, brengt de overheid de eerder vermelde veranderingen aan in haar exportbeleid. Het Court of Appeals verwijst de zaak daarom op 21 januari 1997 weer naar het District Court.¹⁴

De lagere rechtbank gebiedt Karn om zijn verzoek voor een vergunning opnieuw in te dienen. Karn doet dat, maar de overheid wijst het verzoek opnieuw af. Ook het administratief beroep slaagt niet. Uiteindelijk wendt Karn zich weer tot de rechtbank. Op 14 januari 2000 wijzigt de overheid haar exportbepalingen echter opnieuw; voor de export van publiek beschikbare encryptiebroncode, waaronder de software van Karn, is geen vergunning meer nodig. Karn besluit daarom om de zaak te laten rusten, en de rechtszaak sterft

¹¹Zie de website van Phil Karn: <http://people.qualcomm.com/karn/export/index.html>.

¹²Karn v. U.S. Dept. of State, 925 F.Supp. 1 (D.D.C. 1996).

¹³United States v. O'Brien, 391 U.S. 367, 377 (1968) (“a governmental regulation subject to intermediate scrutiny will be upheld if it advances important governmental interests unrelated to the suppression of free speech and does not burden substantially more speech than necessary to further those interests.”)

¹⁴Karn v. U.S. Dept. of State, 107 F.3d 923 (D.C.Cir. 1997).

een stille dood.

4.5 De zaak Junger

Junger v. Daley is aanhangig gemaakt in 1996, nadat de overheid de nieuwe exportregels heeft uitgevaardigd. Junger, hoogleraar in de rechten, onderwijst het vak 'Computers and the Law' aan de Case Western Reserve University Law School in Cleveland, Ohio. Hij wil op zijn website informatie over encryptie-software publiceren. Hij verzoekt daarom de rechtbank te verklaren dat het vergunningstelsel in strijd is met de vrijheid van meningsuiting. Ook verzoekt hij de rechtbank om de overheid te verbieden het exportverbod op hem toe te passen.

Op 2 juli 1998 doet de rechtbank van het Northern District of Ohio uitspraak.¹⁵ De rechtbank meent dat de export van encryptiesoftware niet is beschermd door de vrijheid van meningsuiting. De broncode van encryptiesoftware bezit daarvoor niet voldoende communicatieve waarde.

Junger gaat tegen deze uitspraak in beroep, en op 4 april 2000 vernietigt het Court of Appeals for the Sixth Circuit de beslissing van de rechtbank.¹⁶ 'Because computer source code is an expressive means for the exchange of information and ideas about computer programming, we hold that it is protected by the First Amendment,' aldus het Court of Appeals. Ook in deze zaak wijst het Court of Appeals de zaak terug naar de rechtbank vanwege de recente wijzigingen in de encryptieregulering. Het District Court heeft echter nooit uitspraak gedaan.

4.6 Conclusie

Cryptografiedeskundigen communiceren over de cryptografie met behulp van algoritmes, geformuleerd in programmeertalen. De Amerikaanse rechter heeft in drie zaken erkend dat dit soort algoritmes, geschreven in broncode, vanwege hun communicatieve waarde zijn beschermd door het First Amendment.

De Amerikaanse overheid tracht de verspreiding van cryptografische technologie te beperken. Zij bemoeilijkt het onderzoek naar cryptografie, en zij verbiedt de export van bepaalde cryptografische technologie. Cryptografische technologie is tegenwoordig echter niet meer mechanisch van aard; boutjes en bouten zijn vervangen door bits en bytes. Daarom is een exportverbod op cryptografische technologie in het digitale tijdperk noodzakelijkerwijs een exportverbod op algoritmes, geformuleerd in computertalen. Omdat algoritmes een communicatieve waarde bezitten achtte de rechter tot drie maal toe het vergunningstelsel een beperking van de uitingsvrijheid, omdat cryptografen de ideeën over hun vakgebied niet met de wereld kunnen delen.

In *Bernstein*, de meest uitgebreide zaak, achtte de rechter het vergunningstelsel zelfs ontoelaatbaar. Zelfs het zwaarwegend belang van de nationale veiligheid rechtvaardigt niet dat de vrijheid van meningsuiting zo drastisch wordt beperkt, aldus het Court of Appeals.

¹⁵Junger v. Daley, 8 F.Supp.2d 708 (N.D. Ohio 1998).

¹⁶Junger v. Daley, 209 F.3d 481 (6th Cir. 2000).

De rechtszaken luidden het einde in de van de *crypto-wars*, de oorlog tussen de cryptografen en de overheid. Tegelijkertijd gaven de rechtszaken legitimiteit aan het private onderzoek naar cryptografische technologie.

De vrijheid van het cryptografisch onderzoek ligt echter opnieuw onder vuur. De bescherming van technische voorzieningen, geïntroduceerd in 1998, leidt ook tot beperkingen van de vrijheid van cryptografie-onderzoek. Ditmaal betreft het niet een verbod op encryptie, maar een verbod op decryptie. De rechtszaken over dit verbod worden in het volgende hoofdstuk besproken.

Hoofdstuk 5

Decryptie in de Verenigde Staten

In het vorige hoofdstuk is de regulering van de resultaten van encryptie-onderzoek aan de orde gekomen. In drie zaken heeft de rechter uitgemaakt dat exportverboden een beperking van de vrijheid van meningsuiting vormen. Hieronder komen de Amerikaanse maatregelen die het onderzoek naar decryptietechnologie kunnen beperken aan de orde.

5.1 Regulering

Het Congres, de Amerikaanse federale wetgever, heeft op 28 oktober 1998 de Digital Millennium Copyright Act (DMCA) aangenomen.¹ De DMCA implementeert onder andere het WIPO Auteursrechtverdrag, dat in afdeling 3 is besproken. Afdeling 1201 van de DMCA ziet op de bescherming van technische voorzieningen.²

Afdeling 1201 is een gecompliceerd artikel. De bepaling telt meer dan 4000 woorden, is vier leden diep en meer dan 125 leden lang. Het artikel komt, kort gezegd, op het volgende neer. De *omzeiling* van toegangscontrole-systemen is verboden op grond van afdeling 1201(a)(1)(A). *Middelen* die deze *toegangscontrole* omzeilen zijn verboden op grond van afdeling 1201(a)(2). Afdeling 1201(b) verbiedt *middelen* die *exploitatiecontrolerende* systemen omzeilen. Omdat veel objecten aan te merken zijn als omzeilingsmiddelen geven de afdelingen 1201(a)(2) en 1201(b)(1) aan welke middelen gekwalificeerd kunnen worden als omzeilingsmiddelen. Een omzeilingsmiddel is verboden dat:

1. met name is ontworpen of gemaakt met de bedoeling om een toegangscontrole te omzeilen, of
2. enkel een beperkt commercieel significante toepassing of gebruik kent, anders dan het omzeilen van die toegangscontrole, of
3. wordt aanbevolen ter omzeiling van toegangscontrole.

¹Pub.L.No. 105-304 (1998).

²17 U.S.C. § 1201.

De DMCA hanteert dus, evenals de Europese wetgever, het ontwerp, het gebruik en de advertentie als aanknopingspunt voor de onrechtmatigheid van omzeilingsmiddelen.

Voor deze scriptie is één uitzondering op het omzeilingsverbod van belang: de cryptografie-exceptie van 1201(g). Deze exceptie komt in de zaak *2600*, in afdeling 71 aan de orde. Een andere uitzondering, de reverse-engineering-exceptie van 1201(f), hangt met de cryptografie-exceptie samen. Reverse engineering is het achterhalen van de logische werking van een computerprogramma aan de hand van zijn functionele kenmerken. Mijns inziens is de reverse-engineering-exceptie echter met name bedoeld ter bevordering van compatibiliteit en interoperabiliteit, en deze scriptie gaat verder niet in op het reverse-engineering verweer.

Afdeling 1201 is de afgelopen jaren in de rechtszaal een aantal keer gebruikt.³ Commentatoren op de rechtszaken besteden met name aandacht aan de effecten die de voorzieningenbescherming heeft op de mededinging en de toegang tot informatie. Slechts twee korte artikelen zijn tot nu toe gewijd aan de effecten die afdeling 1201 heeft op het cryptografie-onderzoek.⁴

De meest relevante zaken in dit verband gaan over het kraken van watermerken, het kraken van DVD-kopieerbescherming en het kraken van eBooks. Deze drie zaken worden hieronder besproken.⁵

5.2 De zaak Felten

De zaak van Edward Felten is het meest illustratief voor de gevaren die de bescherming van technische voorzieningen meebrengt voor het cryptografie-onderzoek. Edward Felten is een computerbeveiligings-onderzoeker aan Princeton University. Daarnaast is hij deskundige geweest bij een van de mededingingszaken tegen Microsoft en bij de zaak *2600*, die hieronder volgt.

De muziekindustrie ontwikkelt rond 2000 een kopieerbeveiligingssysteem voor digitaal opgeslagen muziek. Een aantal grote distributielabels richten hiertoe het Secure Digital Music Initiative op, dat een standaard tracht te ontwikkelen voor de veilige distributie van muziek. Op 6 september 2000 schrijft de SDMI op het Internet een open brief aan de digitale gemeenschap waarin ze beveiligingsdeskundigen uitnodigt om de ontwikkelde kopieerbeveiliging te kraken door bepaalde digitale watermerken te verwijderen.⁶ Zij hopen op deze manier kwetsbaarheden in hun systeem te ontdekken voordat ze het systeem in gebruik nemen.

Een groep onderzoekers, onder leiding van Felten, gaat in op de uitnodiging van het SDMI, en slaagt erin om de beveiliging te kraken. De SDMI heeft

³De 1201-zaken die niet het First Amendment en de vrijheid van cryptografie onderzoek bespreken zijn: *Sony Computer Entertainment America, Inc. v. Gamemasters*, 87 F.Supp.2d 976 (N.D.Cal. 1999); *RealNetworks, Inc. v. Streambox, Inc.*, 1999 WL 1448173 (W.D.Wash. 1999), 2000 WL 127311 (W.D.Wash. 2000) en 2000 WL 141196 (W.D.Wash. 2000); *Lexmark International, Inc. v. Static Controls, Inc.*, niet gepubliceerd (E.D.Ky. 2003), te vinden op: http://www.eff.org/IP/DMCA/Lexmark_v_Static_Controls/20030303-finding-of-facts.pdf. Die uitspraken worden hier verder niet besproken.

⁴Imfeld 2003 en Samuelson 2001.

⁵Het artikel van Fred von Lohmann, advocaat van de Electronic Frontier Foundation, biedt een goed overzicht van de ervaring die in de Verenigde Staten is opgedaan met afdeling 1201: Von Lohmann 2003.

⁶De uitnodiging is te vinden op: http://www.sdmi.org/pr/OL_Sept_6_2000.htm.

echter bezwaren tegen het voornemen van Felten om zijn resultaten te publiceren op de Fourth International Information Hiding Workshop in Pittsburgh, omdat het systeem inmiddels in gebruik is genomen. De SDMI en haar leden dreigen met een rechtszaak op grond van afdeling 1201 van de DMCA als Felten zijn resultaten zou publiceren. De publicatie van informatie over de verwijdering van de watermerken zou namelijk zijn aan te merken als distributie van omzeilingsmiddelen.

Hoewel de SDMI deze bedreigingen later terugneemt maakt Felten als reactie een rechtszaak aanhangig. Hij verzoekt de rechtbank om vast te stellen dat hij de vrijheid heeft om zijn resultaten te publiceren. Ook deze rechtszaak heeft de aandacht van vooraanstaande informatiebeveiligingsdeskundigen, waaronder Bruce Schneier en Niels Ferguson, die beiden een verklaring afleggen.⁷ De rechtbank wijst de vordering echter af omdat zij meent dat Felten geen belang heeft bij de vordering — de SDMI heeft immers toegezegd dat zij Felten niet aansprakelijk zal houden als hij de resultaten van het onderzoek publiceert.⁸ De rechtbank komt dus helaas niet aan een inhoudelijke behandeling van de zaak toe. Daardoor weet Felten niet met volledige zekerheid of hij aansprakelijk kan worden gehouden voor het publiceren van zijn resultaten onder afdeling 1201.

5.3 De zaak 2600

De zaak 2600 speelt zich af rond 2000, tegelijkertijd met de zaak *Felten*. Zij is de meest uitgebreide Amerikaanse zaak over de omzeiling van technische voorzieningen. De rechter, met name in de 78-pagina's lange opinie van het District Court, gaat in op de belangrijkste aspecten van afdeling 1201, op het hyperlinken naar decryptiesoftware en op de merites van het reverse-engineering verweer. Binnen deze context is echter van belang dat een gedeelte van de zaak is gewijd aan de relatie tussen afdeling 1201 en de vrijheid van meningsuiting. Ook komt de reikwijdte van de cryptografie-onderzoeksexceptie in deze paragraaf aan de orde.

Achtergrond De Digital Versatile Disc (DVD) is vanwege zijn grote opslagcapaciteit in het begin van de jaren negentig door de filmindustrie aangemerkt als de meestbelovende opvolger van de video. In tegenstelling tot de video zijn films op DVD in digitale vorm opgeslagen. De filmindustrie ontwikkelt daarom, in samenwerking met technologie-industrie, een beveiligingssysteem dat piraterij moet voorkomen, genaamd het Content Scramble System (CSS). CSS bestaat uit een encryptiealgoritme, een decryptiealgoritme, en 400 digitale sleutels.⁹ Om de informatie te ontcijferen heeft men het decryptie-algoritme nodig, en een van de 400 decryptiesleutels. De DVD Copy Control Association (DVD-CCA) beheert de technologie. Zij licentieert het decryptiealgoritme en de sleutels aan honderden producenten van DVD-spelers, zodat de spelers versleutelde DVD's kunnen lezen.

In september 1999 ontwikkelt de 15-jarige Noorse Jon Johansen, samen met twee andere computerprogrammeurs, het computerprogramma DeCSS.

⁷Zie het archief van de EFF: http://www.eff.org/Legal/Cases/Felten_v_RIAA/.

⁸Felten v. RIAA, No. CV-01-2669, 6 juni 2001 (D.N.J. 2001).

⁹Guadamuz González 2003.

DeCSS ontcijfert de versleutelde DVD's van de eisers; het is een variant op het decryptiealgoritme dat de DVD-CCA licentieert. Het programma is ontwikkeld door de werking van de gelicentieerde technologie te bestuderen en deze technologie na te bouwen, het zogenaamde reverse-engineering. Johansen plaatst het computerprogramma op het Internet, waarna het programma zich snel verspreidt op websites over de hele wereld. Het programma telt ongeveer 200 lijnen en is geschreven in de programmeertaal C.

De uitgevers van het tijdschrift 2600, een Amerikaans onafhankelijk tijdschrift dat onder andere gaat over informatiebeveiling, publiceren DeCSS op het Internet in 2000. Zijn redacteur Eric Corley — beter bekend als Emmanuel Goldstein — wordt tezamen met de uitgevers van 2600 voor de rechter gedaagd.

De rechtbank verbiedt hen op 20 januari 2000 bij voorlopige voorziening, een *preliminary injunction*, om DeCSS te publiceren.¹⁰ Op 2 februari 2000 publiceert de rechtbank een meer uitgebreide motivering van het verbod.¹¹ In reactie op het publicatieverbod roepen de verweerders anderen op om het programma te publiceren. Zij publiceren zelf een link naar de websites die DeCSS publiceren.

Beide partijen verzoeken om een behandeling van de zaak in een bodemprocedure zonder jury, een *non-jury trial*. De eisers vorderen nu niet alleen een publicatieverbod, maar ook een verbod om te linken naar websites die DeCSS publiceren. De verweerders vragen om het publicatieverbod op te heffen.

Eerst volgen een paar juridische schijnmanoeuvres. De eisers proberen de advocaat van de wederpartij wegens belangenverstrengeling van de zaak te krijgen. De rechtbank gaat hier niet op in.¹² De verweerders proberen een van de rechters te wraken omdat hij een oud-partner is van een betrokken advocatenkantoor. Dit verzoek wijst de rechtbank ook af.¹³ Na een uitgebreid proces publiceert de rechtbank van het Southern District of New York haar *finding of facts and law* op 17 augustus 2000.¹⁴ Het verbod volgt op 19 augustus 2000.¹⁵

De *finding of facts and law* van 17 augustus 2000 is het meest uitgebreid. De rechtbank gaat eerst in op de vraag of DeCSS een verboden omzeilingsmiddel is op grond van afdeling 1201 — dat is het geval. Vervolgens stelt de rechtbank de vraag of de publicatie van DeCSS een verboden distributievorm van de omzeilingsmiddelen is. Ook dat is het geval. Pas daarna gaat de rechtbank in op de verweren. Hieronder volgen de gedeelten van de opinie die gaan over het cryptografie-onderzoek en de vrijheid van meningsuiting.

De cryptografie-exceptie Zoals eerder besproken schept afdeling 1201(g) een exceptie op het omzeilingsverbod ten bate van het onderzoek naar encryptie. In het kader van encryptieonderzoek te goeder trouw mag men middelen om beschermingsmaatregelen te omzeilen ontwikkelen, bespreken, en gebruiken. De rechter dient op grond van artikel 1201(g)(3) rekening te houden met drie factoren bij de beoordeling van deze goeder trouw. Ten eerste dient de rechtbank te beoordelen of de resultaten van het encryptieonderzoek worden ge-

¹⁰Universal City Studios, Inc. v. Reimerdes, 2000 WL 48514 (S.D.N.Y. 2000).

¹¹Universal City Studios, Inc. v. Reimerdes, 82 F.Supp.2d 211 (S.D.N.Y. 2000).

¹²Universal City Studios, Inc. v. Reimerdes, 98 F.Supp.2d 449 (S.D.N.Y. 2000).

¹³Universal City Studios, Inc. v. Reimerdes, 104 F.Supp.2d 334 (S.D.N.Y. 2000).

¹⁴Universal City Studios, Inc. v. Reimerdes, 111 F.Supp.2d 294 (S.D.N.Y. 2000).

¹⁵Universal City Studios, Inc. v. Reimerdes, 111 F.Supp.2d 346 (S.D.N.Y. 2000).

bruikt om de kennis over encryptietechnologie te verbeteren, of dat deze daarentegen worden gebruikt om auteursrechtinbreuk te vergemakkelijken. Ten tweede dient de rechtbank te onderzoeken of de decryptieactiviteiten onderdeel zijn van legitiem werk of studie. Ten derde dient de rechtbank te onderzoeken of de resultaten van dit onderzoek prompt worden meegegeeld aan de rechthebbende.

In de onderhavige zaak ontbreekt de goeder trouw volgens de rechtbank. De resultaten van het cryptografie-onderzoek zijn niet doorgegeven aan de rechthebbende, maar DeCSS is daarentegen direct op het Internet gepubliceerd. Deze vaststelling kan problematisch zijn voor het onderzoek naar cryptografie, dat zich veelal afspeelt in publieke fora. De uitwisseling van informatie over encryptietechnologie tussen onderzoekers wordt hierdoor belemmerd, nu deze informatie eerst moet worden doorgegeven aan de rechthebbende, wil men vallen onder de cryptografie-exceptie. De rechter besteedt aan deze problematiek echter geen aandacht.

Het First Amendment De rechtbank behandelt ook de relatie tussen afdeling 1201 en het First Amendment. Enerzijds stellen de verweerders dat het First Amendment computercode beschermt. Het verbod op het verspreiden van DeCSS is daarom in strijd met de vrijheid van meningsuiting. Anderzijds stellen zij dat afdeling 1201 een te breed toepassingsbereik heeft — zij is *overbroad* — omdat het verbod op de verspreiding van decryptietechnologie aan derden de mogelijkheid ontnemt om gebruik te maken van hun *fair use* rechten. Het recht van *fair use* is een open beperking op het exclusief recht van de auteur.¹⁶ Voor deze scriptie is dit argument niet van belang, omdat deze scriptie de beperking van cryptografie-onderzoek bespreekt, niet de reikwijdte van het exclusief recht van de auteur.

Het eerste argument is daarentegen wel van belang. De rechtbank overweegt hierover:

It cannot seriously be argued that any form of computer code may be regulated without reference to First Amendment doctrine. The path from idea to human language to source code to object code is a continuum. As one moves from one to the other, the levels of precision and, arguably, abstraction increase, as does the level of training necessary to discern the idea from the expression. Not everyone can understand each of these forms. [...] But each form expresses the same idea, albeit in different ways.

Omdat broncode een vorm van ‘speech’ is, en afdeling 1201 het aanbieden van bepaalde broncode beperkt, beperkt afdeling 1201 dus de vrijheid van meningsuiting. Ook ditmaal, net zoals in de eerder besproken rechtszaken over encryptietechnologie, is het de vraag welke toets de rechter moet toepassen op deze beperking van de vrijheid van meningsuiting.

De rechtbank overweegt ook hier dat de ratio van de overheid om de uiting te beperken niet is gelegen in de inhoud van de uiting. De wetgever reguleert met behulp van afdeling 1201 in dit geval de functionele aspecten van de informatie; het feit dat de software versleutelde informatie kan ontcijferen. De

¹⁶17 U.S.C. § 107.

rechtbank past daarom de in afdeling 52 genoemde *O'Brien* test toe — de regeling dient belangrijke overheidsbelangen na te streven zonder de uitingsvrijheid disproportioneel te belasten. Afdeling 1201 passeert deze toets. Afdeling 1201 beschermt een zwaarwegend belang; de bescherming van auteursrechtelijk beschermde werken tegen het toegenomen risico van piraterij in het digitale tijdperk. De bescherming gaat volgens de rechtbank niet verder dan nodig is.

Na dit te hebben vastgesteld geeft de rechtbank nog een kleine toegift, vergelijkbaar met, maar toch anders dan, de vaststelling van het Court of Appeals in *Bernstein*.

Society increasingly depends upon technological means of controlling access to digital files and systems, whether they are military computers, bank records, academic records, copyrighted works or something else entirely. There are far too many who, given any opportunity, will bypass those security measures, some for the sheer joy of doing it, some for innocuous reasons, and others for more malevolent purposes. Given the virtually instantaneous and worldwide dissemination widely available via the Internet, the only rational assumption is that once a computer program capable of bypassing such an access control system is disseminated, it will be used.

Afdeling 1201 van de DMCA is niet in strijd met de Constitutie.

In beroep De verweerders gaan in beroep en op 18 november 2001 doet het Court of Appeals for the Second Circuit, New York, uitspraak.¹⁷ Het beroepshof bevestigt de beslissing van het District Court. De beperkte interpretaties van afdeling 1201 die de appellanten voorstaan accepteert het Court of Appeals niet. De rechtbank wijdt een belangrijk gedeelte van haar beslissing aan de vraag of computercode beschermd is door het First Amendment. Dit is het geval.

Instructions such as computer code, which are intended to be executable by a computer, will often convey information capable of comprehension and assessment by a human being. A programmer reading a program learns information about instructing a computer, and might use this information to improve personal programming skills and perhaps the craft of programming. Moreover, programmers communicating ideas to one another almost inevitably communicate in code, much as musicians use notes. Limiting First Amendment protection of programmers to descriptions of computer code (but not the code itself) would impede discourse among computer scholars, just as limiting protection for musicians to descriptions of musical scores (but not sequences of notes) would impede their exchange of ideas and expression. Instructions that communicate information comprehensible to a human qualify as speech whether the instructions are designed for execution by a computer or a human (or both).

¹⁷Universal City Studios, Inc. v. Reimerdes, 273 F.3d 429 (2nd Cir. 2001).

Computercode is ‘speech,’ en afdeling 1201 beperkt die speech. Het feit dat computercode ook een functionele component kent is echter van belang voor de vraag welke toets moet worden toegepast op afdeling 1201 van de DMCA.

[C]omputer code can instantly cause a computer to accomplish tasks and instantly render the results of those tasks available throughout the world via the Internet. The only human action required to achieve these results can be as limited and instantaneous as a single click of a mouse. These realities of what code is and what its normal functions are require a First Amendment analysis that treats code as combining nonspeech and speech elements, i.e., functional and expressive elements.

De beperking is daarom inhoudsonafhankelijk (*content neutral*), en wordt getoetst met *intermediate scrutiny*, de toetsingsmaatstaf die in afdeling 4.4 is besproken. De beperking voldoet aan deze toets, en het Court of Appeals hanteert hiervoor dezelfde argumenten als het District Court. Zij wijst de vorderingen van de appellanten af. De verweerders zijn tegen dit oordeel niet in beroep gegaan.

De zaak heeft trouwens nog een staartje. Op verzoek van de filmindustrie dagvaardt het Openbaar Ministerie van Noorwegen op 9 januari 2002 Jon Johansen, één van de ontwikkelaars van DeCSS. Johansen zou een wet op de computercriminaliteit hebben overtreden. De rechtbank in eerste aanleg spreekt Johansen een jaar later vrij, op 9 januari 2003. Het Openbaar Ministerie is hiertegen in beroep gegaan, maar de beroepsrechter heeft nog geen uitspraak gedaan.

5.4 De zaak Elcomsoft

Elcomsoft is de meest recente afdeling 1201-rechtszaak. Het is ook de eerste keer dat afdeling 1201 via het strafrecht wordt gehandhaafd. Adobe ontwikkelt een computerprogramma, de *eBook reader*, dat digitale boeken leest. Een eBook bevat informatie over het toegestane gebruik; zo kan de rechthebbende aangeven dat het boek niet mag worden gekopieerd, of niet mag worden geprint. De eBooks zijn opgeslagen in versleutelde vorm, en de eBook lezer ontcijfert deze versleuteling en erkent de gebruiksbeperkingen die de rechthebbende heeft aangebracht. Zo kan het digitale boek bijvoorbeeld aangeven dat het boek slechts dertig dagen mag worden gelezen. Daarna zal de eBook-lezer het boek niet meer ontcijferen. Het eBook systeem is dus, net zoals CSS, een systeem van exploitatiecontrole.

Het Russische softwarebedrijf Elcomsoft ontwikkelt ‘the Advanced eBook Processor (AEBPR).’ Dit computerprogramma laat de gebruiker de gebruiksbeperkingen van eBooks verwijderen, zodat een boek toch kan worden gekopieerd, of toch kan worden geprint. De gebruiker kan hierdoor wettelijk toegestane handelingen verrichten, zoals het maken van een kopie voor privé gebruik, maar hij kan hierdoor ook onrechtmatige handelingen verrichten, zoals het commercieel verspreiden van het eBook.

Dmitry Sklyarov, Russisch programmeur, werkt bij Elcomsoft. Sklyarov is uitgenodigd om op DefCon, een conferentie van computerdeskundigen, de

technologie achter de AEBPR te beschrijven. Na zijn landing in de Verenigde Staten wordt Sklyarov op 16 juli 2001 door de FBI in Las Vegas opgepakt. Het Openbaar Ministerie stelt op 28 augustus 2001 een aanklacht (*indictment*) in tegen Elcomsoft en Sklyarov.¹⁸ Sklyarov zou het omzeilingsverbod van afdeling 1201 hebben overtreden door de AEBPR te ontwikkelen. Het Openbaar Ministerie klaagt Elcomsoft, zijn werkgever, ook aan.

In afwachting van zijn rechtszaak draait Sklyarov de gevangenis in. De Verenigde Staten staat echter toe dat Sklyarov in december 2001 terugkeert naar Rusland tegen een borg van 50.000 dollar. Elcomsoft en Sklyarov vorderen bij de rechtbank van het Northern District of California om de aanklacht te vernietigen. Op 8 mei 2002 wijst de rechtbank de vordering af.¹⁹ De verweerders hanteren in hun verzoek verschillende argumenten, waaronder de stelling dat de aanklacht in strijd is met het First Amendment.

De rechtbank erkent dat het computerprogramma een vorm van speech is, zelfs als dit programma in objectcode is gepubliceerd. Objectcode is immers 'merely one additional translation of speech into a new, and different, language.' Net zoals in de eerdere rechtszaken meent de rechtbank dat afdeling 1201 een inhoudsonafhankelijke beperking van de vrijheid van meningsuiting is. De beperking dient daarom te worden onderworpen aan de hiervoor besproken *O'Brien* toets.

Afdeling 1201 streeft volgens de rechtbank twee belangen na; het voorkomen van onbevoegd kopiëren van beschermde werken, en het bevorderen van de elektronische handel. Dit zijn zwaarwegende belangen, en aan de eerste stap van de toets is dus voldaan. De wet beperkt de uitingsvrijheid niet disproportioneel, en aan de tweede stap is ook voldaan. Zij wijst de vordering af.

Ook deze zaak heeft een staartje. Op 17 december 2002 beslist de jury in San Jose dat alle onderdelen van de tenlastelegging niet zijn bewezen (*not guilty on all counts*). Het Openbaar Ministerie heeft geen beroep ingesteld.

5.5 Voorbeelden van zelfcensuur

De effecten van afdeling 1201 zijn niet altijd in de rechtszaal merkbaar. Soms leidt reeds de dreiging van afdeling 1201 tot zelfcensuur.²⁰

Von Lohmann meldt dat discussies over kopieerbeschermingsystemen op Internetfora worden gecensureerd, uit vrees voor aansprakelijkheid op grond van afdeling 1201. Ook meldt hij dat computerprogrammeurs security-programma's en details over security-protocols hebben verwijderd van hun website. Richard Clarke, de computerbeveiligingsdeskundige van het Witte Huis, vraagt op een bijeenkomst bij het MIT aandacht voor de effecten die afdeling 1201 heeft op het cryptografie-onderzoek: 'I think a lot of people didn't realize that it would have this potential chilling effect on vulnerability research.'²¹

De Nederlandse cryptografie-deskundige Niels Ferguson heeft afgezien van

¹⁸De aanklacht is te vinden op: http://www.eff.org/IP/DMCA/US_v_Elcomsoft/20010828_sklyarov_elcomsoft_indictment.html.

¹⁹U.S. v. Elcom Ltd., 203 F.Supp.2d 1111 (N.D.Cal. 2002).

²⁰Deze voorbeelden zijn te vinden in het artikel van Von Lohmann 2003.

²¹Bray 2002.

publicatie van een fout in het High-bandwidth Digital Content Protection (HDCP) systeem van Intel.²² Hij stelt:

I have written a paper detailing security weaknesses in the HDCP content protection system. I have decided to censor myself and not publish this paper for fear of prosecution and/or liability under the US DMCA law.

Hij wil niet het risico van aansprakelijkheid lopen. Een duidelijk voorbeeld van zelfcensuur.

Hewlett-Packard (HP) dreigde met afdeling 1201 toen onderzoekers een gat in de beveiliging van het Tru64 UNIX besturingssysteem wilden publiceren.²³ Uiteindelijk heeft HP deze dreiging teruggenomen, maar zo een voorval heeft een 'chilling effect.' Zo hebben twee veiligheidsdeskundigen informatie van hun website verwijderd na de aanklacht van Sklyarov, ook uit vrees voor aansprakelijkheid.²⁴

De Institute of Electrical and Electronics Engineers (IEEE), dat 30 procent van alle bladen over de computerwetenschap publiceert, wijzigde naar aanleiding van deze voorvallen in november 2001 haar publicatiebeleid. Nadien hield zij auteurs volledig aansprakelijk voor rechtszaken op grond van afdeling 1201 van de DMCA. Omdat leden van de IEEE hierover hun onvrede uiten heeft de IEEE dit beleid herzien. Bill Hagen, manager van de IEEE, zegt hierover:²⁵

'The Digital Millennium Copyright Act has become a very sensitive subject among our authors. It's intended to protect digital content, but its application in some specific cases appears to have alienated large segments of the research community.'

Er zijn dus aanwijzingen dat afdeling 1201 leidt tot zelfcensuur met betrekking tot de resultaten van cryptografie-onderzoek.

5.6 Conclusie

Rechthebbenden implementeren technische voorzieningen tegenwoordig met name door middel van een combinatie van hard- en softwaresystemen. Encryptie bewaakt de toegang tot de informatie, en kopieerbeveiliging bewaakt de exploitatie van de informatie. Decryptie van de informatie vindt plaats met behulp van sleutels en een decryptie-algoritme, een algoritme dat functioneel weinig verschilt van de algoritmes die in de encryptie-rechtszaken aan de orde zijn gekomen. Niet geautoriseerde decryptie-algoritmes, of methodes om dergelijke algoritmes te ontwerpen zijn door de rechter aangemerkt als omzeilingsmiddelen.

Maar tegelijkertijd zijn dit soort algoritmes vormen van speech, en zij worden beschermd door het First Amendment. In *Elcomsoft* en *2600* erkent de rechter dan ook dat de bescherming van technische voorzieningen de vrijheid van

²²Ferguson 2001.

²³McCullagh 2002.

²⁴Lemos 2001.

²⁵IEEE 2002.

meningsuiting beperkt. Het beperkt immers de vrije uitwisseling van ideeën over cryptografische technologie. In die twee zaken is de rechter van mening dat de beperking een voldoende zwaarwegend belang beschermt om de constitutionele toetsing te doorstaan.

Er is een opvallend verschil tussen de aanpak van de Amerikaanse rechter in de zaken over encryptieregulering en de zaken over technische voorzieningen. De rechter acht de *nationale veiligheid* niet voldoende zwaarwegend om een exportverbod van encryptiesoftware te rechtvaardigen. Maar het belang van de *elektronische handel en de bescherming van het auteursrecht* weegt wel voldoende zwaar om een verbod op ongeautoriseerde decryptietechnologie te rechtvaardigen.

Er is in ieder geval één verklaring voor dit contrast. De encryptie-rechtszaken betroffen directe overheids censuur — de Verenigde Staten voerden een actief ontmoedigingsbeleid ten aanzien van het onderzoek naar cryptografie. De decryptie-rechtszaken gaan over indirecte overheids censuur — private partijen kunnen middels een civiele actie een publicatieverbod vorderen ten aanzien van informatie met cryptografische relevantie. De rechter heeft dit onderscheid echter niet aangestipt in zijn beslissingen over afdeling 1201.

Hoe het ook zij, deze rechtszaken hebben geleid tot vormen van zelfcensuur in de wetenschappelijke gemeenschap. Omdat het onzeker is in welke gevallen een wetenschapper informatie kan publiceren over cryptografische technieken zullen onderzoekers terughoudend zijn in hun publicaties over onderzoek naar informatiebeveiliging. Dat heeft gevolgen voor het cryptografieonderzoek, dat meer velden bestrijkt dan technische voorzieningen die auteursrechtelijk beschermde werken beschermen.

Daar komt bij dat nagenoeg alle informatie auteursrechtelijk beschermd is. De maatstaf voor auteursrechtelijke bescherming, oorspronkelijkheid, is immers betrekkelijk laag. Hoewel deze scriptie verder niet ingaat op de reikwijdte van het begrip ‘technische voorziening’ is het waarschijnlijk dat veel systemen van informatiebeveiliging kunnen worden aangemerkt als technische voorzieningen. In ieder geval leidt ook deze onduidelijkheid over wat onder het begrip ‘technische voorziening’ moet worden verstaan tot een beperking van het cryptografieonderzoek.

De afgevaardigde van het House of Representatives Rick Boucher heeft daarom op 7 januari 2003 voorgesteld om een uitzondering te scheppen op het distributieverbod met betrekking tot omzeilingsmiddelen. De distributie van omzeilingsmiddelen zou niet zijn verboden als ‘the person is acting solely in furtherance of scientific research into technological protection measures.’²⁶ Deze exceptie is met name relevant voor de publicatie van gaten in beveiligingstechnologie — een dergelijke publicatie kan immers door de rechter worden geïnterpreteerd als een vorm van distributie van omzeilingsmiddelen.

In het afgelopen hoofdstuk is vastgesteld dat de bescherming van technische voorzieningen tot op zekere hoogte de mogelijkheid beperkt om de resultaten van cryptografie-onderzoek te publiceren. In het volgende hoofdstuk komt het Europees-Nederlandse stelsel van encryptieregulering aan bod.

²⁶Digital Media Consumers’ Rights Act of 2003, H.R. 107 (2003), te vinden op <http://thomas.loc.gov/cgi-bin/query/z?c108:H.R.107:>

Hoofdstuk 6

Encryptie in Europa en Nederland

Hoewel ook Nederland een exportverbod op cryptografie kent, hebben zich hierover nog geen rechtszaken voorgedaan. De analyse van de juridische aspecten van cryptografie in Nederland begint en eindigt daarom bij de wetgever. Hieronder worden de regels onderzocht die de verspreiding van cryptografie in en uit Nederland beheersen.

Zoals op veel gebieden is de Nederlandse wetgever ook ten aanzien van cryptografie gedeeltelijk gebonden aan Europese en internationale regels, en die komen hieronder tevens aan de orde.

Overigens is voor deze scriptie niet zozeer interessant wát de huidige regelingen zijn, maar wáárom deze regelingen bepaalde uitzonderingen kennen voor het gebruik van cryptografie. Helaas kent de Regeling van Wassenaar, het belangrijkste regelgevend instrument, geen *travaux préparatoires*. Daarom beperkt deze scriptie zich tot de letter van de regels, en tracht ze aan de hand daarvan hun strekking te achterhalen. Ook wordt verwezen naar de veranderingen die in de loop van de jaren zijn aangebracht.

6.1 Regulering

Cryptografie kent zowel civiele als militaire toepassingen. Cryptografie-technologie wordt daarom aangemerkt als een zogenaamd 'product voor tweërlei gebruik,' een *dual use good*. Producten voor tweërlei gebruik en militaire goederen noemt men 'strategische goederen.' Strategische goederen vallen onder een verscherpt export- en doorvoerregime dat is gecoördineerd vanuit internationale fora. Doordat cryptografie is gereguleerd vanuit drie fora — internationaal, Europees en Nederlands — verliest de rechtzoekende zich snel in een gecompliceerd spinnweb van regels.¹

Sinds 1996 is de export van strategische goederen op internationaal niveau gecoördineerd door de Regeling van Wassenaar (RvW), beter bekend als de

¹De verwijzingen naar de relevante documenten zijn met name opgedaan bij de *Crypto Law Survey* van Bert-Jaap Koops, zie: <http://rechten.kub.nl/koops/cryptolaw/>. De auteur bedankt ook Maurice Wessling voor het sturen van zijn notitie over dit onderwerp.

Wassenaar Agreement. De Europese Unie heeft deze regeling geïmplementeerd in een verordening, waarop hieronder in afdeling 6.3 wordt ingegaan. Daarnaast kent Nederland een eigen export- en doorvoerbeleid voor strategische goederen, dat grotendeels is gemodelleerd naar de internationale verplichtingen die op dit vlak bestaan. Ook dit exportbeleid komt hieronder aan de orde. Tot slot bespreekt deze scriptie een uitgelekt Nederlands wetsvoorstel dat het gebruik van cryptografie zonder vergunning in Nederland wilde verbieden.

6.2 COCOM en Regeling van Wassenaar

COCOM Op internationaal niveau coördineerde het Coordinating Committee for Multilateral Export Controls (COCOM) tot 1994 de export van strategische goederen. Het COCOM, een informele organisatie van 17 Westerse landen waaronder Nederland, stelde zich tot doel om de export van strategische goederen en technische data naar communistische landen te beperken. Het COCOM onderhield daartoe een lijst van goederen waarvoor een exportvergunning vereist was, de *International Industrial List and the International Munitions List*. Cryptografische technologie maakte deel uit van deze lijst, zij het met een *status aparte* — sinds 1990 is bepaalde *mass-market* cryptografiesoftware van deze lijst uitgesloten.²

Het COCOM is opgericht tegen de achtergrond van de Koude Oorlog. Toen de politieke spanningen tussen Oost en West wegsmolten concludeerden de deelnemende landen dat behoefte bestond aan een nieuwe organisatie die aan de veranderde dreigingen het hoofd kon bieden. Op 31 maart 1994 hieven de deelnemende landen het COCOM op.³

Regeling van Wassenaar Nadat de oud-leden het COCOM hadden opgeheven kondigden zij op 19 december 1995 de geboorte van een vervangende regeling aan, de *‘Wassenaar Arrangement on export controls for conventional arms and dual-use goods and technologies.’* Deze Regeling van Wassenaar, vernoemd naar de plaats waar de oprichtingsonderhandelingen hebben plaatsgevonden, is in de loop van 1996 tot stand gekomen.

De RvW bestaat uit twee componenten. Aan de ene kant voorziet de regeling in procedures die de uitwisseling van informatie over de export van strategische goederen tussen de deelnemende landen bevorderen. Deelnemende landen zijn bijvoorbeeld op grond van artikel V lid 1 verplicht om elkaar op de hoogte te stellen van geweigerde vergunningen aan niet-deelnemende landen.

Aan de andere kant beschrijft een bijlage bij de regeling de goederen waarvan de deelnemers de export dienen te controleren. Hoewel de RvW haar deelnemers verplicht tot het instellen van een export-controleregime behouden de individuele landen volle discretie over het wel of niet verschaffen van vergunningen.

Artikel III verplicht deelnemende landen tot het implementeren van de verplichtingen in hun nationale wetgeving. Een bijlage van de RvW geeft aan voor welke goederen een exportvergunning is vereist. Afdeling 2 van categorie 5 gaat over producten voor informatiebeveiliging, waaronder cryptografie. De

²Aldus Koops in zijn *Crypto Law Survey*.

³Zie de website van het RvW: <http://www.wassenaar.org/docs/History.html>.

inhoudelijke aspecten van deze afdeling komen verder aan de orde in afdeling 6.3.1.

Op 30 november en 1 december 2000 zijn de deelnemende landen in Bratislava bijeen gekomen in het kader van de zesde plenaire vergadering. De deelnemers erkennen in een *public statement* dat: "it is important to continue deepening Wassenaar Arrangement understanding of how and how much to control intangible transfers."⁴ Hierbij doelden zij met name op cryptografische software, en tijdens deze vergadering zijn belangrijke veranderingen aangebracht in de status van cryptografie binnen de RvW.

Ten eerste is *mass market* cryptografie technologie geheel uitgesloten van exportbeperkingen. Voorheen vereiste het RvW dat cryptografische algoritmes niet meer dan 64-bits sleutels gebruikten. Ten tweede zijn een aantal uitzonderingen opgenomen voor bepaalde vormen van cryptografie, zoals het gebruik van cryptografie in beschermingsmaatregelen voor de intellectuele eigendom. Hiermee is de export van technische voorzieningen dus aanzienlijk vergemakkelijkt. Dit betekent dat rechthebbenden na die datum sterke cryptografie in hun beschermingssystemen kunnen implementeren.

6.3 Europa

Verordening 3381/94 van 19 december 1994 riep voor het eerst een exportregime voor strategische goederen op Europees niveau in leven.⁵ Deze verordening is nadien een paar keer gewijzigd en op 22 juni 2000 vervangen door verordening 1334/2000.⁶ Verordening 1334/2000 bevat de huidige Europese exportregels voor strategische goederen.

Verordening 1334/2000, de geldende exportverordening, bestaat uit 8 pagina's regelgeving en een bijlage van meer dan 200 pagina's. Deze bijlage beschrijft de goederen waarvoor een exportvergunning is vereist. Deze bijlage is 'een technische implementatie van internationaal overeengekomen vergunningsregelingen voor goederen voor tweërlei gebruik, waaronder het Wassenaar Arrangement, het "Missile Technology Control Regime", de Groep van nucleaire exportlanden, de Australiëgroep en het Verdrag inzake chemische wapens,' aldus de verordening. Zoals eerder opgemerkt zijn de regels over cryptografie afkomstig uit de RvW.

Deelnemende landen komen binnen internationale fora geregeld bijeen om de lijsten van strategische goederen aan te passen. Om deze wijzigingen in internationale exportafspraken te verwerken is verordening 1334/2000 sinds haar ontstaan driemaal gewijzigd. De eerste wijziging, die plaatsvond bij verordening 458/2001 van 6 maart 2001, heeft de 64-bit eis uit de cryptografie-noot verwijderd naar aanleiding van de wijzigingen in de RvW, besproken in afdeling 85.⁷ Vervolgens is de verordening gewijzigd door verordening 2432/2001 van 20 november 2001.⁸ Deze nieuwe verordening bevat een volledig herziene bijlage van de lijst met strategische goederen, maar de afdeling over cryptogra-

⁴Public Statement of the Sixth Plenary of the Wassenaar Arrangement, te vinden op: http://www.wassenaar.org/docs/press_5.html.

⁵PbEG 1993, L 367/1.

⁶PbEG 2000, L 159/1, gerectificeerd in PbEG 2000, L 176/52.

⁷PbEG 2001, L 65/19.

⁸PbEG 2001, L 338/1.

fiettechnologie is ongewijzigd. Ook de meest recente wijziging, bij verordening 149/2003 van 27 januari 2003, wijzigt de regels over cryptografietechnologie niet.⁹

Overigens heeft de Europese Gemeenschap een verlichte visie over het gebruik van cryptografie in de samenleving, vergeleken met de Verenigde Staten. Zo benadrukt de Europese Commissie in een beleidsdocument uit 1997 het belang van cryptografie voor de bescherming van de informatiemaatschappij.¹⁰ Zij stelt dat het wenselijk is om een interne markt voor cryptografieproducten tot stand te brengen. Daarnaast staat de Commissie een geleidelijke deregulering van cryptografieproducten op het niveau van de RvW voor. Naar aanleiding van de onrust die is ontstaan over het internationaal afluisternetwerk Echelon raadt het Europees Parlement de burger zelfs aan om zijn communicatie met sterke cryptografie te beveiligen.¹¹ Op dit beleidsmatige standpunt gaat deze scriptie verder niet in.

Omdat Europese verordeningen rechtstreekse werking hebben, en de Nederlandse exportcontroleregelingen daarnaast verwijzen naar de Europese verordeningen, komt hieronder de inhoud van de Europese exportregels aan de orde, voor zover relevant.

6.3.1 De inhoudelijke regeling

De bijlage bij verordening 1334/2000 beschrijft de lijst met producten waarvoor een exportvergunning is vereist. De lijst bestaat uit een algemeen deel, dat definities en algemene uitzonderingen bevat, en negen afdelingen die de verschillende categorieën goederen beschrijven waarvoor een exportvergunning is vereist. Deel 2 van afdeling 5 beschrijft de goederen die worden gebruikt voor 'informatiebeveiling.' Zoals gezegd valt cryptografie onder deze categorie.

Voor deze scriptie zijn twee algemene uitzonderingen op het exportverbod van belang: de Algemene Technolgieenoot en de Algemene Programmatuurnoot. Beiden komen hieronder aan de orde, evenals de afdeling van de bijlage die gaat over cryptografie.

Algemene Technolgieenoot In het algemeen deel is de de Algemene Technolgieenoot (Atn) opgenomen. De Atn, die letterlijk is overgenomen uit de RvW, beschrijft de toepassing van de exportcontrole-regels op technologie. Het volgende onderdeel van de noot is in dit verband van belang:

Vergunningsregelingen voor overdracht van "technologie" zijn niet van toepassing op informatie die "voor iedereen beschikbaar" is, op "fundamenteel wetenschappelijk onderzoek" en op de voor octrooiaanvragen noodzakelijke minimuminformatie.

Technologie is gedefinieerd als "specifieke informatie, onder meer in de vorm van technische gegevens, die nodig is voor de 'ontwikkeling', de 'productie' of het 'gebruik' van een product." Fundamenteel wetenschappelijk onderzoek is gedefinieerd als:

⁹PbEG 2003, L 30/1, gerectificeerd in PbEG 2003, L 52/11.

¹⁰COM(1997) 503 def.

¹¹A5-0264/2001 2001/2098(INI), 11 juli 2001, paragraaf 11.6.

experimenteel of theoretisch werk dat hoofdzakelijk wordt gedaan om nieuwe kennis te verkrijgen over de fundamentele beginselen van verschijnselen of waarneembare feiten, en dat in eerste instantie niet is gericht op een bepaald praktisch doel of oogmerk.

Deze uitzondering plaatst de internationale gegevensoverdracht van informatie, zoals technische gegevens, buiten het vergunningbeleid als deze informatie toegepast wordt in fundamenteel onderzoek. Omdat het onderzoek naar cryptografie zich over het algemeen wél richt op een bepaald praktisch doel of oogmerk, schept de Atn mijns inziens geen uitzondering voor de export van cryptografie-broncode. Daarnaast geldt voor cryptografiesoftware een *lex specialis*, de Algemene Programmatuurnoot, die hieronder verder wordt besproken.

Het is in dit verband echter interessant dat het wetenschappelijk onderzoek een voorkeurspositie krijgt toebedeeld in het systeem van exportcontrole. Het is niet duidelijk wat de regelgever heeft bewogen om deze uitzondering te scheppen. Waarschijnlijk is deze uitzondering opgenomen ten bate van de vrijheid van meningsuiting en de wetenschappelijke vooruitgang.

De Atn schept ook een uitzondering voor de overdracht van technologie die voor iedereen beschikbaar is. Dat is het geval, aldus de definitie in de bijlage, voor:

“technologie” of “programmatuur” die zonder beperkingen aan de verdere verspreiding daarvan beschikbaar zijn gesteld. (Auteursrechtelijke beperkingen hebben niet tot gevolg dat “technologie” of “programmatuur” niet langer “voor iedereen beschikbaar” is.)

De ratio van deze uitzondering blijkt niet uit de regeling zelf. Het is mogelijk dat de bepaling is opgenomen op grond van pragmatische overwegingen — dweilen met een open kraan is onbegonnen werk.

Het is ook mogelijk dat de bepaling is opgenomen op grond van principiële overwegingen. Wellicht achtten de opstellers het niet wenselijk om het publiek domein te verschrompelen, zelfs niet omwille van de staatsveiligheid. ‘De burger’ heeft al jaren toegang tot bepaalde informatie en functionaliteit, en dit gewekte vertrouwen weegt zwaarder dan de nationale veiligheid. Zo een interpretatie is meer gebaseerd op principiële overwegingen.

De uitzondering voor publiekelijk beschikbare cryptografie wordt hieronder uitgebreider besproken in het kader van de Algemene Programmatuurnoot.

Algemene Programmatuurnoot De RvW kent behalve de Atn nog een uitzondering die voor deze scriptie relevant is: de Algemene Programmatuurnoot. Lid a van deze noot, die een uitzondering schept voor zogenaamde *mass market* computersoftware, is niet van toepassing op cryptografiesoftware. Lid b van deze noot zondert programmatuur uit die ‘voor iedereen beschikbaar’ is. De Engelse versie spreekt van software in ‘the public domain.’

Dit lid is voor deze scriptie belangrijker. Veel cryptografiesoftware is immers voor iedereen beschikbaar. Het is interessant om de ratio van deze bepaling te achterhalen. Zoals hierboven al is opgemerkt kan een dergelijke uitzondering zijn opgenomen op grond van zowel pragmatische als principiële

overwegingen. Misschien is de uitzondering opgenomen met het oog op cryptografiesoftware. Het programma PGP van Phil Zimmerman was ten tijde van het opstellen van deze regelingen wijdverspreid, en het zou weinig zin hebben om deze software aan exportcontrole te onderwerpen. Een dergelijke pragmatische overweging zegt echter weinig over het juridisch kader dat cryptografiesoftware beheerst.

Zoals hierboven is opgemerkt kan deze uitzondering ook zijn geschapen uit meer principiële overwegingen. Op grond van het vertrouwensbeginsel zou men het publiek domein niet mogen 'onteigenen' in het kader van de bescherming van de staatsveiligheid. Een dergelijke ratio zou wellicht kunnen dienen als aanknopingspunt bij het formuleren van een rechterlijk beslissingskader om geschillen tussen informatiebeveiliging en technische voorzieningen te beslechten.

Cryptografienoot Naast de Atn en de Apn is in afdeling 5 deel 2, dat ziet op de producten voor informatiebeveiliging, een algemene clausule opgenomen die gaat over cryptografie, de zogenoemde cryptografienoot. De cryptografienoot stelt dat cryptografie is uitgezonderd van het exportverbod wanneer zij aan de volgende kenmerken voldoet:

- a. de goederen zijn algemeen voor het publiek verkrijgbaar doordat ze zonder beperkingen via de detailhandel uit voorraad wordt verkocht via:
 1. winkelverkoop;
 2. postorderverkoop;
 3. elektronische verkoop; of
 4. telefonische verkoop;
- b. de cryptografische werking kan niet eenvoudig door de gebruiker worden veranderd;
- c. de goederen zijn ontworpen voor installatie door de gebruiker zonder wezenlijke ondersteuning van de leverancier; en
- d. zo nodig zijn er over deze goederen nadere gegevens beschikbaar, die op verzoek worden verstrekt aan de bevoegde autoriteiten van de lidstaat waarin de exporteur gevestigd is, zodat kan worden vastgesteld of aan de onder a. tot en met c. beschreven voorwaarden wordt voldaan.

Ook hier betreft het de verkoop van 'mass market' cryptografie-technologie, net zoals bij lid a van de Apn. Lid b van de cryptografienoot eist dat de cryptografische werking niet eenvoudig door de gebruiker kan worden veranderd. Cryptografie-software in broncode is makkelijk aan te passen door de gebruiker die verstand heeft van programmeren. Het is de vraag of 'de gebruiker' in de zin van de cryptografienoot verstand heeft van programmeren. Het lijkt mij, gezien de context van deze bepaling, moeilijk te verdedigen dat cryptografiesoftware in broncode-vorm onder deze uitzondering valt. Immers, lid a van deze bepaling richt zich met name op mass-market software, software die niet eerst gecompileerd moet worden voordat hij kan worden gebruikt. Parvainen

meent daarentegen dat de gemiddelde gebruiker broncode niet eenvoudig kan veranderen.¹²

Het is niet direct duidelijk wat de ratio is van de bepaling. Misschien is de uitzondering opgenomen onder druk van de software-industrie wiens handel in software ernstig is beperkt door intransparante exportregimes. Zo is de verkoop van Lotus Notes, een communicatiesysteem voor de kantooromgeving, met een aantal jaren vertraagd door de verschillen in exportregulering tussen de Verenigde Staten en Europa.¹³ Dat deze noot met name lijkt gericht op het wegnemen van beperkingen van de handel in software blijkt ook uit de handelingen die op grond van deze noot uitgezonderd worden: de verkoop van cryptografie-technologie *over the counter*, zowel fysiek als virtueel.

Overwegingen van vrijheid van meningsuiting lijken bij het opstellen van de cryptografienoot geen rol te hebben gespeeld. Dit blijkt met name uit het feit dat broncode waarschijnlijk niet valt onder deze uitzondering. Omdat er geen ontstaansgeschiedenis bestaat die de interpretatie van de bovenstaande bepaling kan ondersteunen gaat deze scriptie verder niet op haar in.

Vergunningsplichtige software Een vergunning is vereist voor, kort gezegd, systemen van informatiebeveiliging die zijn ontworpen of aangepast voor het hanteren van 'cryptografie.' Het betreft cryptografische systemen, zo blijkt uit afdeling 5A002 van de verordening, die gebruik maken van:

- a. een "symmetrisch algoritme" met een sleutellengte van meer dan 56 bits; of
- b. een "asymmetrisch algoritme" waarvan de beveiliging wordt gewaarborgd door:
 1. ontbinding van gehele getallen van meer dan 512 bits (bv. RSA);
 2. berekening van discrete logaritmen in een groep van een eindig veld met een grootte van meer dan 512 bits (bv. Diffie-Hellman over Z/pZ); of
 3. discrete logaritmen in een andere dan de in 5A002.a.1.b.2 genoemde groepen van meer dan 112 bits (bv. Diffie-Hellman over een elliptische curve);

Wat ook zij van deze technische beschrijvingen, voor deze scriptie is van belang dat de export van sommige cryptografie-software, ook in de vorm van broncode, onderworpen is aan een vergunning voor de export op grond van verordening 1334/2000. Hierbij maakt het niet uit via welk kanaal de overdracht plaatsvindt, zo blijkt uit de *Statement of Understanding* bij de RvW. Overigens schept de regeling zoals gezegd wel een uitzondering voor cryptografie in systemen van kopieerbeveiliging of toegangscontrole.

6.4 Nederland

Nederland is grotendeels gebonden aan de afspraken die op internationale fora zijn gemaakt over de export van cryptografie. Omdat het inhoudelijke deel

¹²Parviainen 2000, p. 21.

¹³Levy 2001, p. 155 e.v.

van de exportregels hierboven al aan de orde is geweest wordt hier slechts kort ingegaan op het Nederlandse bestel dat cryptografie-export controleert. Daarnaast komt een uitgelekt wetsvoorstel aan de orde dat het ongeautoriseerd gebruik van cryptografie strafbaar wilde stellen.

6.4.1 Nederlandse exportcontrole

De export- en doorvoercontrole valt onder de Centrale Dienst voor In- en Uitvoer (CDIU), onderdeel van de Belastingdienst/Douane van het Ministerie van Financiën.¹⁴ De CDIU, die onder beleidstoezicht staat van het Ministerie van Economische Zaken, geeft het Handboek Strategische Goederen uit, dat de inhoudelijke en procedurele kanten van de Nederlandse exportcontrole van strategische goederen beschrijft.

De In- en uitvoerwet vormt de wettelijke basis voor de andere besluiten.¹⁵ Op grond van artikel 19 ligt de toezichthoudende taak bij de Economische Controle Dienst (ECD). Op grond hiervan is het In- en uitvoerbesluit strategische goederen genomen.¹⁶ Dit besluit verbiedt de uitvoer zonder vergunning van militaire goederen die zijn genoemd in de bijlage van het besluit. Ook verbiedt het besluit de export en doorvoer van de goederen die genoemd zijn in verordening 1334/2000.

Exportvergunningen zijn vereist voor militaire goederen en goederen voor tweërlei gebruik. De lijst van militaire goederen ziet niet op cryptografie. De lijst van goederen voor tweërlei gebruik is een letterlijke kopie van verordening 1334/2000, die in afdeling 6.3.1 is besproken. Voor cryptografiesoftware die in de bijlage bij verordening 1334/2000 voorkomt is dus een vergunning vereist. Omdat de Nederlandse lijst een letterlijke kopie van de verordening wordt verder niet ingegaan op de Nederlandse lijst.

6.4.2 Het uitgelekte wetsvoorstel

Op dit moment is slechts de *export* van bepaalde cryptografie verboden. In 1994 leek echter ook het *gebruik* van cryptografie beperkt te worden. Rond die tijd hebben de Ministers van Verkeer en Waterstaat, Justitie, Binnenlandse Zaken en Defensie gezamenlijke stappen ondernomen om het gebruik van cryptografie drastisch in te perken. Het Voorontwerp van een wet inzake de cryptografie, die de Wet op de telecommunicatievoorzieningen (WTV) zou wijzigen, lekte echter uit en is vervolgens in de MediaForum gepubliceerd.¹⁷ Alexander Patijn, ambtenaar bij het Ministerie van Justitie, schrijft een begeleidende inleiding in dezelfde MediaForum.¹⁸ De publicatie van dit wetsvoorstel leidde tot verontwaardigde reacties en heeft het parlement niet bereikt.¹⁹ De kritiek richtte zich met name op de gevaren die een dergelijk voorstel zou meebrengen voor de privacy.

¹⁴Zie de website van het Ministerie van Economische Zaken, <http://www.exportcontrole.ez.nl>.

¹⁵*Stb.* 1962, 295.

¹⁶*Stb.* 1999, 516.

¹⁷*MediaForum* Bijlage 1994 [6]6, p. B49–B55.

¹⁸Patijn 1994a.

¹⁹Zie bijvoorbeeld Van den Hoven van Genderen 1994 voor een inhoudelijke bespreking.

De Memorie van Toelichting van dit wetsvoorstel geeft aan waarom behoefte is aan een algemeen verbod op het bezit, het gebruik en de distributie van cryptografie:

Waar particulieren, en daarmee criminelen, over dezelfde middelen gaan beschikken als voorheen mogelijk vijandige mogendheden, ligt het in de rede de regelgeving met betrekking tot de strijdmiddelen die particulieren worden toegestaan, meer in overeenstemming te brengen met die welke vanouds voor vijandige mogendheden bestaat.

Een haviksredenering voor een draconische wet. De eerder genoemde Alexander Patijn merkt in een begeleidend artikel op dat:²⁰

het strafbaarstellen van crypto zou, voor zover het daarbij gaat om een immateriële zaak, een nieuw informatiedelict zijn. Het past daarmee in een bonte verzameling van bepalingen [zoals] racistische propaganda, kinderpornografie en belediging.

De heer Patijn merkt niets op over de spanning tussen de vrijheid van meningsuiting en een verbod op de cryptografie. De Memorie van Toelichting lijkt met deze spanning echter toch rekening te houden, zoals hieronder zal blijken.

Cryptografie Een nieuw lid 1 van artikel 1 Wtv definieert de term 'cryptografie.' Cryptografie is:

een verzameling opdrachten kennelijk bestemd om gegevens automatisch te bewerken zodanig dat deze in geval van overdracht via telecommunicatie niet meer direct begrijpelijk of bruikbaar zijn, of, indien zij eerder zijn bewerkt, weer direct begrijpelijk of bruikbaar worden, voor zover deze opdrachten ter beschikking worden gesteld of zijn vastgelegd in een vorm dat zij voor onmiddellijk gebruik kunnen worden aangewend.

Interessant is dat het hier slechts gaat om cryptografische algoritmes die in een zodanige vorm zijn vastgelegd dat zij voor onmiddellijk gebruik kunnen worden aangewend. Het is waarschijnlijk dat cryptografische algoritmes die compilatie vereisen voordat ze kunnen worden gebruikt niet voor onmiddellijk gebruik kunnen worden aangewend. In zoverre vallen algoritmes in niet-gecompileerde broncode dus buiten de regeling. Blijkens de MvT is het verder niet noodzakelijk:

dat de serie opdrachten is vastgelegd in computerprogrammatuur. De bewerkingen kunnen bijvoorbeeld ook mechanisch worden uitgevoerd. Handmatige vercijfering valt niet onder de definitie. ¶ De woorden 'verzameling van opdrachten' maken duidelijk dat cryptografie niet een materieel voorwerp betreft dat op een bepaalde plaats, uniek aanwezig is, doch immateriële gegevens die, soms op

²⁰Patijn 1994b.

een gegevensdrager, bij voorbeeld op een floppy, een schijf, een chip of papier, zijn vastgelegd, soms via telecommunicatie worden overgedragen. [...] [D]e definitie omvat slechts opdrachten in objectcode (bruikbaar voor een computer of een ander geautomatiseerd werk) en geen opdrachten in broncode (tekst op papier), zodat bij voorbeeld niet een wetenschappelijke publicatie over dit onderwerp onder de definitie valt.

Dit uitgangspunt is vergelijkbaar met het beleid van de Amerikaanse overheid dat in de cryptografie-rechtszaken aan de orde is gekomen. Aan de ene kant mag men een boek met broncode van cryptografische software wel exporteren, maar een diskette met cryptografische software in objectcode niet.

Het is interessant om te zien dat een wetenschappelijke publicatie over cryptografische technieken expliciet niet wordt aangemerkt als cryptografie in de zin van de wet. Deze uitzondering is wellicht opgenomen ter bescherming van de academische vrijheid en de vrijheid van meningsuiting, maar dat blijkt niet uit de Memorie van Toelichting.

Het gebruik van cryptografie Het nieuwe artikel 30a van de Wtv zou het *bezit en gebruik* van cryptografie strafbaar stellen. Dit verbod zou niet van toepassing zijn op personen die van de Minister een machtiging hebben verkregen, en het is ook niet van toepassing op cryptografie die de Minister heeft toegelaten. Om het onrechtmatig gebruik van cryptografie op te sporen zou het wetsvoorstel 20 bijzondere opsporingsambtenaren inzetten.

Het nieuwe artikel 30b zou het *aanbieden* van cryptografie aan derden strafbaar stellen. Dit verbod zou niet van toepassing zijn op personen die van de Minister verlof hebben gekregen, en op cryptografie waarvan het gebruik is toegestaan. De MvT geeft aan dat dit verbod ook ziet op het aanbod van 'cryptografie die in de vorm van een dienst over de telecommunicatie-infrastructuur aan het publiek kan worden aangeboden.'

Het huidige standpunt Sinds 1997 heeft de regering het standpunt ingenomen dat het gebruik van cryptografie niet moet worden beperkt.²¹ De Commissie Franken neemt in haar eindrapport over de wijziging van de Grondwet het standpunt in dat een *grondrecht* op het gebruik van cryptografie echter niet gewenst is.²² In het kabinetsstandpunt over de Grondwetwijziging van 16 oktober 2000 ontbreekt ook een grondrecht op encryptie.²³ In de Kamervragen over het kabinetsstandpunt wordt dit standpunt gehandhaafd.²⁴ Een verbod op het gebruik van sterke cryptografie is op dat moment nog niet aan de orde.

Sinds de twee gebouwen van het World Trade Center op 11 september 2001 door een terroristische aanslag zijn vernietigd is de opvatting van de regering veranderd. In het naar aanleiding van de aanvallen in New York opgestelde Actieplan Terrorismebestrijding van 5 oktober 2001 stelt de regering in actiepunten 16 dat gestreefd moet worden naar regulering van krachtige cryptogra-

²¹Zie b.v. *Kamerstukken II 1997/98*, 25 880, nr. 1, p. 158, 162 en *Kamerstukken II 1998/99*, 25 880, nr. 3, p. 2, *Kamerstukken II 1999/00*, 25 880, nr. 10, p. 20.

²²Franken e.a. 2000, p. 161. De auteur bedankt Lodewijk Asscher voor deze en hieropvolgende suggesties.

²³*Kamerstukken II 2000/01*, 27 460, nr. 1.

²⁴*Kamerstukken II 2000/01*, 27 460, nr. 2, p. 52.

fie voor publiek gebruik.²⁵ Op 27 juni 2003 biedt Minister Donner de zesde voortgangsrapportage van het Actieplan Terrorismebestrijding aan de kamer aan.²⁶ Daarin meldt hij dat van invoering van een zelfreguleringsmechanisme voor rechtmatige toegang moet worden afgezien. Hij verwijst hierbij naar de eindrapportage van het project Rechtmatige Toegang, dat naar aanleiding van actiepunt 16 was opgericht.²⁷ De eindconclusie in deze rapportage is dat het voorlopig niet opportuun is om rechtmatige toegang wettelijk te verplichten.

Voorlopig is het gebruik van sterke cryptografie in Nederland dus nog toegestaan. Het is opvallend dat de discussie volledig in het teken staat van de functie van cryptografie ter bescherming van de vertrouwelijke communicatie en de privacy in het algemeen. De vrijheid van meningsuiting speelt geen rol bij de beoordeling van de toelaatbaarheid van distributie van cryptografische technologie.

6.5 Conclusie

De export van encryptiesoftware is in Europa, en ook in Nederland, aan controle onderhevig. Eerst in het kader van de COCOM, toen in het kader van de RvW, en inmiddels is de Europese verordening 1334/2000 het belangrijkste reguleringsinstrument. Verordening 1334/2000 stelt weliswaar beperkingen aan de export van cryptografie, maar die beperkingen kennen uitzonderingen die voor deze scriptie interessant zijn.

Ten eerste is de overdracht van gegevens uitgezonderd van de exportcontrole als dit gebeurt in het kader van het fundamenteel wetenschappelijk onderzoek. Hoewel deze bepaling van weinig praktische waarde is voor de export van encryptiesoftware kan men hieruit in ieder geval opmaken dat wetenschappelijke kennis binnen het RvW een *status aparte* krijgt toebedeeld.

Ten tweede scheppen de Apn en de cryptografienoot beiden een uitzondering voor *mass-market* software die wordt verkocht in de retailhandel en niet kan worden aangepast. Daarnaast scheppen beiden noten een uitzondering voor software die 'voor iedereen beschikbaar' is. De mass-market uitzondering is waarschijnlijk niet relevant voor deze scriptie, omdat de belangrijkste cryptografie-software door middel van broncode wordt verspreid, en broncode gemakkelijk kan worden aangepast.

De uitzondering voor publiek-domein software is meer relevant. Het is helaas niet duidelijk of deze uitzondering is opgenomen om principiële of pragmatische redenen. Wat de ratio van dit onderscheid ook moge zijn, als software in het publiek domein is gevallen dan valt zij tevens buiten de encryptieregelingen.

Ook het uitgelekte wetsvoorstel dat het gebruik van cryptografie in Nederland wilde verbieden is informatief voor deze scriptie. Ten eerste vindt men in dit voorstel overwegingen die in de Amerikaanse crypto-zaken hebben gespeeld. Zo zou de wetgever wetenschappelijke publicaties uitgezonderd hebben van de definitie van 'cryptografie' — waarschijnlijk op grond van de academische vrijheid en de vrijheid van meningsuiting. Daarnaast knoopte de wetgever met name aan bij de functionaliteit van het object dat men tracht te

²⁵Kamerstukken II 2001/02, 27 925, nr. 10, p. 11.

²⁶Kamerstukken II 2002/03, 27 925, nr. 96, p. 15

²⁷Kamerstukken II 2002/03, 26 581, nr. 2.

verbieden. Software in objectcode op een diskette is wel verboden, maar software in broncode in een boek niet. Ook hier lijken overwegingen mee te spelen die raken aan de vrijheid van meningsuiting.

De discussie over het reguleren van sterke cryptografie heeft in Nederland een nieuwe impuls gekregen door de terroristische aanvallen van 11 september 2001. In deze discussie wordt echter geen aandacht besteedt aan de relatie tussen de vrijheid van meningsuiting en de regulering van cryptografische algoritmes.

Samenvattend kan men stellen dat ook in de Europese en Nederlandse regulering van cryptografie overwegingen spelen die in de Amerikaanse discussie over de export van software naar voren zijn gekomen. Het is de vraag of dergelijke overwegingen ook bestaan bij de Nederlandse bescherming van technische voorzieningen vóór implementatie van de Auteursrechtlijn. Het volgende hoofdstuk gaat daarop in.

Hoofdstuk 7

Decryptie in Nederland

Ook vóór de implementatie van de Auteursrechtlijn beschermde de Nederlandse wetgever al een beperkte groep technische voorzieningen. Ten eerste verbiedt artikel 7 van de Softwarerichtlijn sinds 1991 “het in het verkeer brengen of het bezit voor commerciële doeleinden van middelen die uitsluitend bestemd zijn om de ongeoorloofde verwijdering of ontwijking van enigerlei technische voorziening te vergemakkelijken die voor de bescherming van een programma getroffen mocht zijn.”¹ Deze bepaling is geïmplementeerd in artikel 32a van de Auteurswet. Ten tweede introduceert artikel 4 van de Voorwaardelijke Toegangsrichtlijn sinds 1998 de bescherming van systemen van voorwaardelijke toegang.² Systemen van voorwaardelijke toegang zijn ook beschermd door middel van technische voorzieningen. De bepaling is geïmplementeerd in artikel 326c van het Wetboek van Strafrecht.

De twee artikelen zijn sinds 2000 een paar keer in de rechtszaal gebruikt. Die uitspraken zijn slechts gedeeltelijk relevant voor deze scriptie, omdat ze met name de distributie van fysieke omzeilingsmiddelen betreffen. De verspreiding van software, die in meerdere mate door de vrijheid van meningsuiting is beschermd, is nog niet aan de orde geweest. Om een indruk te krijgen van de aanpak van de Nederlandse rechter worden de relevante aspecten van deze zaken hieronder besproken. Ook wordt ingegaan op de rechtsliteratuur over de bescherming van software door artikel 10 EVRM.

7.1 Artikel 32a Auteurswet

Artikel 32a Auteurswet is de eerste bepaling die voorziet in de bescherming van technische voorzieningen. De bepaling, die stamt uit de Softwarerichtlijn, beoogt kopieerbeveiliging van software te beschermen. De bepaling is tot nu toe twee keer toegepast.

De eerste zaak betreft het ombouwen van Playstations, zodat deze geschikt worden gemaakt voor het lezen van illegaal gekopieerde Playstation-spellen. Dit gaf aanleiding tot een civiele actie van de Stichting BREIN, en een strafrechtelijke actie van het Openbaar Ministerie. Het Openbaar Ministerie legt de verdachte een overtreding van artikel 32a Aw ten laste.

¹Richtlijn 91/250/EEG, *PbEG* 1991, L 122/42.

²Richtlijn 98/84/EG, *PbEG* 1998, L 320/54.

De strafkamer van de Rechtbank Alkmaar acht in haar mager gemotiveerde vonnis van 30 november 2000 bewezen dat de verdachte in strijd heeft gehandeld met dit artikel.³ De verdachte houdt zich immers bezig met het ombouwen van Sony Playstations, opdat deze ook geschikt zijn voor het spelen van illegaal gekopieerde Playstation-spellen. Ook biedt de verdachte onderdelen aan die benodigd zijn voor het ombouwen van de Playstation, waaronder zogenaamde *mod chips*. De vrijheid van cryptografisch onderzoek komt niet ter sprake.

Ook in de civiele evenknie, *Stichting BREIN/X*, komt deze vrijheid niet aan de orde.⁴ De rechter loopt in deze beslissing vooruit op de implementatie van de Auteursrechtlijn. Hij beslist aan de hand van de Auteursrechtlijn dat omzeilingsmiddelen niet mogen worden verhandeld als deze slechts een commercieel beperkt doel of nut hebben. De onderhavige *modchips* hebben slechts een beperkt commercieel doel of nut, anders dan omzeiling. Interessant is in dit verband dat de eisers vorderen dat de rechter niet alleen de distributie van de omzeilingsmiddelen verbiedt, maar ook de distributie van de “instructies omtrent de wijze waarop modchips moeten worden ingebouwd en geprogrammeerd.” Instructies zijn een vorm van informatie, en die worden dus tot op zekere hoogte door de informatievrijheid beschermd. De rechter wijst echter ook deze vordering toe, en hij gaat niet in op de vrijheid van meningsuiting.

7.2 Artikel 326c Wetboek van Strafrecht

De vrijheid van meningsuiting komt wel aan de orde in de zaak *VNU/Canal+*, die in dit verband het meest relevant is.⁵ Deze zaak is gebaseerd op artikel 326c van het Wetboek van Strafrecht, dat, zoals gezegd, artikel 4 van de Voorwaardelijke toegangsrichtlijn implementeert. Artikel 326c lid 2 verbiedt de productie, het bezit, en de distributie van een voorwerp dat kennelijk is bestemd om zonder te betalen gebruik te maken van een voorwaardelijke toegangsdiens. Betaaltelevisie en andere interactieve diensten zijn voorbeelden van voorwaardelijke toegangsdiens.

VNU v. Canal+ VNU publiceert op 13 juli 2000 het vijftiende nummer van het tijdschrift *Computer Idee*. Het tijdschrift beschrijft hoe men zonder abonnement de diens van Canal+ kan ontvangen. Dit kan met een televisiekaart en een computerprogramma dat het Canal+ signaal ontcijfert, de zogenaamde *cable crypt decoder*. Het artikel beschrijft waar dit programma op het Internet te vinden is. Canal+ stelt dat deze publicatie onrechtmatig is jegens haar. De president geeft op 14 juli 2000 een terugroepgebod en gelast op 18 juli 2000 een rectificatie.

Hiertegen gaat VNU in beroep. VNU beroept zich met name op de vrijheid van meningsuiting. Het Hof Amsterdam overweegt:

Dat het een blad als *Computer Idee* — gericht op personen die een

³Rb. Alkmaar 30 november 2000, *Computerrecht* 2001/3, p. 157–159, m.nt. K.J. Koelman.

⁴Vzr. Breda 24 april 2002, *AMI/Informatierecht* 2002/4, p. 137–143, m.nt. Jacqueline Seignette (*Stichting BREIN/X*).

⁵Pres. Rb. Haarlem 28 juli 2000, Zaak nr. 66855/KG ZA 00-388 en Hof Amsterdam 21 februari 2002, *MediaForum* 2002/4, p. 119–120 (*VNU/Canal+*).

bijzondere belangstelling hebben voor computers — vrijstaat maatschappelijke ontwikkelingen als de onderhavige te beschrijven en dat exploitanten als Canal+ zich dit op grond van de vrijheid van pers dienen te laten welgevalen is op zichzelf niet in het geding. ¶ Ook het enkele feit dat wordt verwezen naar een website waar (naar het hof verstaat al vrij lang) een programma kon worden geladen via internet waarmede ontcijfering (decoding) van een gecodeerde zender via de tv-kaart van de personal computer kon worden bewerkstelligd valt onder diezelfde vrijheid.

Dat echter een volledige technische handleiding wordt gepubliceerd gaat het Hof te ver.

[VNU] heeft dan ook, door in Computer Idee lezers actief aan te moedigen tot het kraken van de codering, en hen, door publicatie van het stappenplan, daartoe instructies te geven, de grenzen van de ten opzichte van Canal+ in acht te nemen zorgvuldigheid overschreden. Dit wordt in casu niet gerechtvaardigd door een beroep op de persvrijheid. Daarbij wordt het volgende in aanmerking genomen. ¶ De wetgever heeft ter bescherming van een bepaald commercieel belang gedragingen als de onderhavige van privépersonen vrij recentelijk als misdrijf strafbaar gesteld [Art. 326c WvSr, OvD]. Dit feit is een belangrijke aanwijzing voor de rechter dat bij de hiervoor bedoelde noodzakelijke afweging van persvrijheid enerzijds en een commercieel belang zoals dat van Canal+ anderzijds, laatstgenoemd belang de doorslag moet krijgen indien lezers op de hiervoor vermelde wijze van voldoende technische kennis worden voorzien om stelselmatig het abonnementsstelsel van Canal+ te ontduiken.

Het Hof geeft duidelijk aan dat de publicatie van een technische handleiding over het kraken van technische voorzieningen kan worden verboden. De vrijheid van meningsuiting staat hieraan niet in de weg. Deze uitkomst is vergelijkbaar met de in afdeling 5 besproken rechtszaken over de bescherming van technische voorzieningen. Ook daar oordeelde de rechter dat een ieder de vrijheid toekomt om over omzetting te publiceren, maar tegelijkertijd kent deze vrijheid een grens. Overigens gaat de Nederlandse rechter niet in op de vrijheid van cryptografie-onderzoek.

Canal+ v. Xtra Sat De tweede artikel 326c-zaak betreft weer de diensten van Canal+. Canal+ verspreidt haar diensten met behulp van decoders, die voor ontvangst de installatie van een smartcard vereisen. De firma Xtra Sat verkoopt ten tijde van de dagvaarding illegale en blanco smartcards. Illegale smartcards zijn smartcards die zijn geprogrammeerd om de diensten van Canal+ te ontvangen zonder toestemming van Canal+. Blanco smartcards kunnen worden geprogrammeerd om de diensten van Canal+ te ontvangen, maar zijn hier niet voor geprogrammeerd.

Canal+ vordert bij de rechter dat Xtra Sat de distributie van illegale en blanco smartcards staakt. De rechter wijst het verkoopverbod ten aanzien van ille-

gale smartcards toe.⁶ De rechter overweegt echter dat blanco smartcards niet zijn ontworpen of aangepast om ongeautoriseerd toegang te verkrijgen tot een voorwaardelijke toegangsdienst. Ook de onrechtmatigheid van de overige ondersteunende programmatuur en apparatuur is niet voldoende vast komen te staan.

Overigens heeft de rechter ook een paar keer het distribueren van decodeermiddelen gekwalificeerd als onrechtmatig handelen.⁷ Deze rechtszaken speelden zich af toen de Voorwaardelijke toegangsrichtlijn nog niet bestond en zijn daarom voor de hedendaagse praktijk minder van belang. Hierop wordt verder niet ingegaan.

7.3 De vrijheid van meningsuiting en software

De jurisprudentie die in dit hoofdstuk is besproken geeft geen antwoord op de vraag of software, en informatie over kwetsbaarheden in omzeilingsmechanismen, naar Nederlands recht wordt beschermd door de vrijheid van meningsuiting. Bij gebreke van Nederlandse jurisprudentie gaat de volgende paragraaf in op de jurisprudentie van het Europees Hof voor de Rechten van de Mens (EHRM) en de Nederlandse literatuur over dit onderwerp.

Artikel 10 van het Europees Verdrag voor de Rechten van de Mens (EVRM) beschermt het recht op vrijheid van meningsuiting.⁸ Artikel 7 van de Nederlandse Grondwet beschermt dit recht ook.⁹ De laatste jaren past de Nederlandse rechter artikel 7 Grondwet meestal toe in combinatie met artikel 10 EVRM. Omdat artikel 10 EVRM een hogere rechtsbron is dan artikel 7 Grondwet besprekt deze paragraaf de vrijheid van meningsuiting binnen het kader van artikel 10 EVRM.

Jurisprudentie Het EHRM heeft zich nog niet uitgesproken over de vraag of software, en informatie over kwetsbaarheden in beveiligingssystemen, door artikel 10 EVRM wordt beschermd. Het recht op vrijheid van meningsuiting omvat, blijkens artikel 10 EVRM, niet alleen het recht om een mening te koesteren, maar ook om inlichtingen of denkbeelden te verstrekken en ontvangen. De uitspraak van het EHRM in *Handyside* is nog steeds het uitgangspunt voor de vraag welke informatie de bescherming van artikel 10 EVRM geniet:¹⁰

[Article 10] is applicable not only to “information” or “ideas” that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population.

⁶Pres. Rb. Den Bosch 12 maart 2001, *AMI/Informatierecht* 2001/4, p. 92–97, m.nt. M. de Cock Buning (*Canal+/Xtra Sat*). Zie voor een vergelijkbare zaak Pres. Rb. Middelburg 26 juli 2001, *MediaForum* 2001/9, p. 265 (*Canal+/M-Sat*).

⁷Pres. Rb. 20 januari 1986, KG 1986/92 (*Filmnet I*), Pres. Rb. Amsterdam 22 november 1990, *MediaForum* bijlage 1991/3, p. 27 en Hof Amsterdam 22 mei 1991, *MediaForum* 1991/9, p. 94 e.v., m.nt. Th.C.J.A. van Engelen (*Esselte/Ten-Electronics*).

⁸*Trb.* 1951, 154.

⁹Zie ook artikel 19 van de Universele Verklaring van de Rechten van de Mens, dat geen afdwingbare verplichtingen in het leven roept, *Trb.* 1969, 99, en artikel 19 van het Internationaal Verdrag inzake Burgerrechten en Politieke Rechten (IVBPR), dat wel rechtstreekse werking heeft, *Trb.* 1969, 99 en *Trb.* 1978, 177 (Nederlandse vertaling).

¹⁰EHRM 7 december 1972, NJ 1978, 236 (*Handyside/Verenigd Koninkrijk*)

Dat wil niet zeggen dat iedere informatie, en iedere vorm van informatie, evenveel bescherming verdient. Zo genieten mededelingen over zaken van openbaar belang een voorkeurspositie.¹¹ Maar beperkingen van mededelingen met een commercieel karakter toetst het Hof minder streng.¹² En ook artistieke expressie valt binnen het kader van artikel 10.¹³

Literatuur In de literatuur neemt men daarom aan dat de bescherming van artikel 10 zich uitstrekt tot alle soorten informatie.¹⁴ Ook informatie die een politieke boodschap ontbeert, zoals bijvoorbeeld productinformatie, zou onder deze bescherming vallen.¹⁵

In Nederland heeft Hins twee regels gewijd aan de vraag of software beschermd is onder artikel 10 EVRM.¹⁶ Hins stelt dat het uitwisselen van computerprogramma's en videospelletjes geen activiteit is die wordt beschermd door artikel 7 Grondwet of artikel 10 EVRM, uitzonderingen daargelaten. Een videospel dat uitdrukking geeft aan een politieke overtuiging of computerprogramma's die tot doel hebben informatie toegankelijk te maken zijn voorbeelden van dergelijke uitzonderingen. Hins verwijst daarbij naar de uitspraak van het EHRM in *Autronic*, waarin ook het communicatiemiddel onder de bescherming van artikel 10 EVRM is gebracht.¹⁷

Asscher suggereert in zijn noot bij *Bernstein* aan de hand van de redenering van Hins dat ook programma's die informatie ontoegankelijk maken in sommige gevallen beschermd zullen zijn.¹⁸

Beide opvattingen klinken door in het antwoord van Minister Donner op de vragen van het kamerlid van der Ham van D66. Deze vroeg of de Minister het computerspel 'Postal 2' ging verbieden omdat de hoofdpersoon van het spel kan schieten op junks, dikke mensen en homo's. De Minister zag daartoe geen mogelijkheden, omdat artikel 7 Grondwet preventief toezicht op de inhoud van computerspellen verbiedt.¹⁹ Overigens achtte de Minister repressief ingrijpen wel mogelijk, maar dat laat de Minister over aan het Openbaar Ministerie.

Of software een meningsuiting is speelt overigens ook bij de discussie over intellectuele eigendomsrechten op software. Zo schrijven Spoor en Verkade dat computerprogrammatuur door deskundigen "gelezen, begrepen, ja zelfs gewaardeerd" kan worden, dit naar aanleiding van een opmerking van Vandenberghe dat pas van een werk kan worden gesproken als het voortbrengsel is gericht op communicatie met de mens.²⁰ Deze scriptie gaat verder niet in op overwegingen over de vrijheid van meningsuiting in het kader van de bescherming van software door het auteurs- of octrooirecht.

Afgezien van deze terloopse opmerkingen zijn mij geen bronnen bekend die de verhouding tussen artikel 10 EVRM en software, of mededelingen over

¹¹Zie bijvoorbeeld EHRM 26 april 1979, NJ 1980, 146, m.nt. E.A. Alkema (*Sunday Times*).

¹²EHRM 20 november 1989, NJ 1991, 738, m.nt. E.A. Alkema (*Markt intern Verlag*).

¹³EHRM 24 mei 1988, NJ 1991, 685 (*Müller v. Zwitserland*).

¹⁴Harris/O'Boyle/Warbrick 1995, p. 377-378 en de Meij 1996, p. 110.

¹⁵Vroom-Cramer 1998, p. 54.

¹⁶Hins 1995, p. 31-32.

¹⁷EHRM 22 mei 1990, NJ 1991, 740, m.nt. E.A. Alkema (*Autronic*).

¹⁸Bernstein v. U.S. Dept. of Justice, 176 F.3d 1132, (9th Cir. 1999), *MediaForum* 1999/10, m.nt. L.F. Asscher.

¹⁹*Aanhangsel Handelingen II* 2002/03, nr. 889, vermeldt in *MediaForum* 2003/4, p. 134.

²⁰Spoor & Verkade 1993, p. 66.

informatiebeveiliging, bespreken.

De academische vrijheid Zoals eerder is besproken zijn veel van de publicaties die kwetsbaarheden in beveiligingssysteem blootleggen de vrucht van wetenschappelijk onderzoek. Er bestaan twee uitspraken van het EHRM waarin het Hof de academische vrijheid expliciet behandelt.²¹

Uit de eerste zaak, *Hertel v. Zwitserland*, komen twee beginselen naar voren. Ten eerste betreft het EHRM het forum waarin een mededeling is gedaan bij de beoordeling van de rechtmatigheid van een beperking van de uitingsvrijheid, zoals ook door Dommering in zijn noot is opgemerkt. Ten tweede acht het EHRM het niet noodzakelijk in een democratische samenleving om het publiceren van onderzoek te verbieden, terwijl men het *doen* van onderzoek toestaat. Het doen van onderzoek impliceert het publiceren van onderzoek, aldus het EHRM.

Ook intellectuele eigendoms wetten kennen een bijzondere positie toe aan het wetenschappelijk onderzoek. Zo stelt lid 3 van artikel 53 van de Rijsoctrooiwet 1995 dat het uitsluitend recht van de octrooihouder zich, kort gezegd, niet uitstrekt tot handelingen die uitsluitend dienen tot onderzoek van het ge-octrooieerde. Artikel 45l van de Auteurswet stelt dat degene die bevoegd is tot het vervoelvoudigen van een computerprogramma tevens bevoegd is om de werking van dit programma waar te nemen, te bestuderen en te testen om de ideeën en beginselen die daaraan ten grondslag liggen te achterhalen.

7.4 Conclusie

Er bestaat weinig Nederlandse jurisprudentie over de bescherming van technische voorzieningen. De weinige uitspraken die ons ter beschikking staan hebben voor dit onderzoek beperkte relevantie, omdat hierin de handel in fysieke omzeilingsmiddelen centraal staat.

Slechts in Canal+/VNU is de relatie tussen de bescherming van technische voorzieningen en de vrijheid van meningsuiting meer nadrukkelijk aan de orde gekomen. Het ging in deze zaak echter niet om de publicatie van decryptie-algoritmen of technische informatie over encryptiesystemen, maar om een technische handleiding over het ontvangen van Canal+ zonder abonnement. Het Hof achtte in deze zaak de vrijheid van meningsuiting ondergeschikt aan de belangen van Canal+. Lezers actief aanmoedigen tot het kraken van de codering, en hen, door publicatie van het stappenplan, daartoe instructies te geven, is onzorgvuldig jegens Canal+, aldus de rechter. Daarbij speelt een rol of lezers van voldoende technische kennis worden voorzien om stelselmatig het abonnementssysteem van Canal+ te ontduiken.

Men kan dus in ieder geval concluderen dat het actief aanmoedigen van het omzeilen van technische voorzieningen de publicatie van de kwetsbaarheden in een systeem eerder onrechtmatig maakt.

Ook in de jurisprudentie van het EHRM is de publicatie van software, of kwetsbaarheden in beveiligingssystemen, niet aan de orde gekomen. In de

²¹EHRM 25 augustus 1998, NJ 1999, 712 m.nt. EJD (*Hertel*) en EHRM 8 juli 1999, NJ 2001, 62, m.nt. EJD (*Baskaya & Okçuoglu v. Turkije*). Nederlandse zaken die raken aan de academische vrijheid, zijn: Rb. Den Haag 31 oktober 1990, IER 1990/6, p. 139–140 (*BAT/Stivoro*), en Rb. Arnhem 1 april 1999, *MediaForum* 1995/5, p. 154–158, m.nt. Aernout Nieuwenhuis (*X v. Van de Bunt*).

literatuur wordt aangenomen dat artikel 10 EVRM vele soorten informatie beschermt. Asscher en Hins menen in ieder geval dat software die informatie toegankelijk of ontoegankelijk maakt door dit artikel wordt beschermd.

Daarnaast blijkt dat de publicatie van wetenschappelijk onderzoek onder de reikwijdte van dit artikel valt. Het toestaan van het doen van onderzoek impliceert het publiceren van dit onderzoek, aldus het EHRM.

Hoofdstuk 8

Conclusie

Software is kennis, geformuleerd in een programmeertaal. Een omzeilingsmiddel is kennis over een kwetsbaarheid in een beveiligingssysteem, mogelijk geformuleerd in een programmeertaal. Een verbod op de verspreiding van omzeilingsmiddelen beperkt daarom de verspreiding van kennis, en dus de vrijheid van meningsuiting.

Een van de grondslagen van de vrijheid van meningsuiting is het belang bij een ongehinderde uitwisseling van ideeën. De ongehinderde uitwisseling van ideeën bevordert het vinden van de waarheid. Cryptografie-onderzoekers benadrukken dit belang voor hun onderzoek. Zoals Schneier zegt: “This free information flow, of both description and proof-of-concept code, is [...] vital for security research.” Tegelijkertijd bevordert ongehinderde distributie van kennis over omzeilingstechnieken het plegen van auteursrechtinbreuk.

De Europese en Nederlandse wetgever erkennen deze spanning. De Minister geeft in zijn bespreking van de implementatiewet aan dat de publicatie van serieus wetenschappelijk onderzoek naar cryptografie niet door het wetsvoorstel wordt verboden. Maar de onderzoeker moet wel trachten te voorkomen dat anderen op eenvoudige wijze technische beschermingsvoorzieningen kunnen omzeilen.

De uitdaging is, kort gezegd, hoe onrechtmatige auteursrechtinbreuk door het omzeilen van technische voorzieningen te voorkomen, en tegelijkertijd het onderzoek naar cryptografie zo min mogelijk te beperken. De voorgaande hoofdstukken bieden een aantal aanknopingspunten voor het beslechten van deze spanning.

De vorm Ten eerste is de vorm waarin kennis wordt verspreid van belang. Kwetsbaarheden kunnen worden gepresenteerd in de vorm van een handleiding in natuurlijke taal die precies beschrijft welke stappen men moet uitvoeren om een kwetsbaarheid bloot te leggen. Het is ook mogelijk om een kwetsbaarheid te beschrijven in de vorm van software, in bron- of objectcode, die deze stappen uitvoert — een zogenaamde *exploit*. Het is tot slot mogelijk om de software zo te schrijven, dat deze kant-en-klaar toegepast kan worden door een onervaren computergebruiker.

Deze drie vormen bevatten dezelfde kennis, en zijn mijns inziens alle drie beschermd door de vrijheid van meningsuiting. Natuurlijke taal is in ieder geval beschermd door de vrijheid van meningsuiting. In de Amerikaanse recht-

spraak is echter vastgesteld dat onderzoekers hun ideeën onder meer uitwisselen in de vorm van software, en dat deze software daarom ook beschermd is door de vrijheid van meningsuiting. Dat doen onderzoekers ook in Europa, en er bestaat mijns inziens geen reden om aan te nemen dat software niet is beschermd door artikel 10 EVRM. Artikel 10 EVRM beschermt immers ideeën, en software is een idee, geformuleerd in een programmeertaal.

Zelfs software in objectcode geniet mijns inziens de bescherming van artikel 10 EVRM. Immers, zoals het Court of Appeals in Bernstein opmerkt: “the path from idea to human language to source code to object code is a continuum.” Objectcode bevat dezelfde informatie als broncode, maar in een andere vorm. Het feit dat objectcode direct uitvoerbaar is ontnemt deze software niet de bescherming van artikel 10.

De functionaliteit kan wel grond zijn voor het toestaan van een beperking van de vrijheid van meningsuiting, omdat deze functie auteursrechtinbreuk bevordert, en dus schade veroorzaakt.

Een publicatie in natuurlijke taal moet eerst worden omgezet in computercode om te werken. De schade die ontstaat door het ongeautoriseerd omzeilen van een technische voorziening is daarom niet aan de orde bij publicatie in deze vorm. Software die geschreven is in een programmeertaal die compilatie vereist, en dus niet direct uitvoerbaar is, zal deze schade ook niet tot gevolg hebben. Software die direct uitvoerbaar is zal deze schade sneller tot gevolg hebben. En software die kant-en-klaar, gebruiksvriendelijk, een technische voorziening omzeilt leidt het snelst tot schade.

De publicatie van een kwetsbaarheid in een technische voorziening in natuurlijke taal, zelfs in gedetailleerde vorm, is daarom mijns inziens toegestaan. Een kwetsbaarheid in de vorm van een programmeertaal die compilatie vereist, en dus niet direct uitvoerbaar is, is mijns inziens ook toegestaan. Een publicatie van een kwetsbaarheid in direct uitvoerbare software is mijns inziens ook toegestaan, maar deze moet het omzeilen van technische voorzieningen niet actief bevorderen. Of sprake is van actief bevorderen kan worden beoordeeld aan de hand van omstandigheden zoals of de software gebruiksvriendelijk is en of deze een handleiding heeft. Ook kan een rol spelen of de software het mogelijk maakt om stelselmatig technische voorzieningen te omzeilen.

Openbaar belang Het EHRM kent een voorkeurspositie toe aan mededelingen van openbaar belang. Niet alle kennis over omzeilingsmiddelen is echter in gelijke mate een mededeling over een zaak van openbaar belang.

Informatie over encryptietechnieken bevat bij uitstek mededelingen over zaken van openbaar belang. Immers, de mededeling “zo en zo kan een boodschap hermetisch worden versleuteld” is van grote maatschappelijke relevantie in een samenleving waar de bescherming van informatie een centrale rol speelt. Dit lijkt op de redenering van Asscher, die stelt dat artikel 10 EVRM software beschermt die informatie ontoegankelijk maakt. Het lijkt ook op de overweging van de rechter in Bernstein: “Bernstein’s is a suit not merely concerning a small group of scientists laboring in an esoteric field, but also touches on the public interest broadly defined.”

Tegelijkertijd zijn mededelingen over *kwetsbaarheden* in systemen van informatiebeveiliging van grote maatschappelijke relevantie. Een gat in de bescherming van, bijvoorbeeld, financiële software kan ernstige maatschappelij-

ke gevolgen hebben. Ook de mededeling “zo en zo kan een boodschap zonder toestemming worden ontsleuteld” is dus van openbaar belang.

GroenLinks heeft daarom in het Nader Verslag de vraag gesteld of rechthebbers de publicatie kunnen voorkomen van kwetsbaarheden in algemeen toegepaste informatiebeveiligingsmaatregelen, als deze ook zijn geïmplementeerd in technische voorzieningen. De Minister is op deze vraag niet ingegaan. Mijns inziens kan echter op grond van bovenstaande redenering worden gesteld dat de breedte van de toepassing van beschermingsmaatregelen een rol speelt bij de beoordeling of een publicatie toelaatbaar is.

Als een kwetsbaarheid wordt ontdekt in een breed toegepast cryptografisch algoritme is informatie over deze kwetsbaarheid van openbaar belang. Een rechthebbende zal publicatie van die kwetsbaarheid niet kunnen voorkomen. Als een kwetsbaarheid is ontdekt in een beveiligingssysteem dat enkel in een technische voorziening is verwerkt is publicatie daarvan minder snel toelaatbaar.

Het medium In de voorgaande hoofdstukken maken de rechter en de regelgever onderscheid tussen publicatie van kennis in boeken en op diskette. De ratio van deze bepaling is dat informatie in boekvorm minder snel in functionele software kan worden omgezet dan informatie in digitale vorm. Een dergelijk onderscheid tussen verschillende media is mijns inziens niet wenselijk.

Ten eerste beperkt dit onderscheid technologie-neutrale toepassing. Ten tweede wordt kennis tegenwoordig met name in digitale vorm uitgewisseld en het zou onwenselijk zijn om publicatie slechts toelaatbaar te achten als deze plaatsvindt in papieren vorm. De gemeenschap van beveiligingswetenschappers communiceert al lang niet meer via fysieke tijdschriften, maar met name door middel van nieuwsgroepen en mailinglists. Ook publicatie van kwetsbaarheden op het internet is daarom volgens mij toegestaan.

Het forum Dat neemt niet weg dat het forum waarin bepaalde informatie wordt gepubliceerd mee kan spelen bij de rechtmatigheid van de publicatie. De vraag is hier hoe groot de kans is dat het publiek de resultaten van het onderzoek zal gebruiken om auteursrechtinbreuk te plegen. Als de kans vrijwel honderd procent is dat de informatie zal worden gebruikt voor auteursrechtinbreuk is publicatie waarschijnlijk niet toelaatbaar. Als deze kans bestaat maar betrekkelijk klein is, dan is publicatie eerder toelaatbaar.

Zo is de publicatie in een nieuwsgroep of mailinglist waar gewoonlijk de resultaten van serieus onderzoek worden gepubliceerd eerder toelaatbaar dan publicatie op een website die is gewijd aan het plegen van auteursrechtinbreuk. Ook het publiek dat kennis neemt van het forum kan een rol spelen bij deze beoordeling. Als het forum slechts toegankelijk is voor een beperkte groep beveiligingsdeskundigen dan is dit eerder toelaatbaar dan als deelnemers aan het forum zich met name richten op het plegen van auteursrechtinbreuk.

De wijze De kans dat schade ontstaat kan ook worden verminderd door de wijze van publicatie. Ten eerste moet de producent een redelijke termijn worden gegund waarbinnen hij een reparatiekit voor zijn software beschikbaar kan stellen. Dat de onderzoeker eerst de producent op de hoogte moet stellen alvorens de kwetsbaarheid te publiceren is terug te vinden in de cryptografie-

exceptie van 1201(g) van de DMCA. Het is ook terug te vinden in de discussie in de beveiligingswereld over full disclosure.

Of een termijn redelijk is, hangt af van de vraag hoe makkelijk de producent een reparatiekit kan uitbrengen. Een kwetsbaarheid in hardwarematige kopieerbeveiliging is minder gemakkelijk te repareren omdat men hiertoe de hardware moet aanpassen. Het repareren van een kwetsbaarheid in softwarematige beschermingssystemen is makkelijker omdat men software makkelijker kan aanpassen.

Tot slot moet de cryptografie-onderzoeker niet aanzetten tot omzeiling. Of hiervan sprake is, kan worden beoordeeld aan de hand van de context van de publicatie. Als de publicatie tevens adviseert hoe men een kwetsbaarheid kan toepassen voor het plegen van auteursrechtinbreuk zal dit niet snel toelaatbaar zijn. Als de publicatie daarentegen slechts de kwetsbaarheid beschrijft is dit eerder toelaatbaar.

Bronnen

Literatuur

- Arkenbout 2001** E.J. Arkenbout, 'Richtlijn auteursrecht en naburige rechten in de informatiemaatschappij: naar een Europees auteursrecht,' *Computerrecht* 2001/3, p. 126–130.
- Bray 2002** Hiawatha Bray, 'Cyber Chief Speaks on Data Network Security,' *The Boston Globe* 17 oktober 2002, te vinden op: <http://www.boston.com/globe/search/>.
- Ferguson 2001** Niels Ferguson, 'Censorship in action: why I don't publish my HDCP results,' 15 augustus 2001, te vinden op: <http://www.macfergus.com/niels/dmca/cia.html>
- Guadamuz González 2003** Andrés Guadamuz González, 'Trouble with prime numbers: DeCSS, DVD and the protection of proprietary encryption tools,' *Jour. Inf. L. and Tech.* 2002/3, te vinden op: <http://elj.warwick.ac.uk/jilt/02-3/guadamuz.html>.
- Harris/O'Boyle/Warbrick 1995** David J. Harris, Michael O'Boyle & Chris Warbrick, *Law of the European Convention on Human Rights*, London: Butterworths 1995.
- Hins 1995** A.W. Hins, 'Gedachten en gevoelens over de digitale snelweg' in: J.W. Kalkman, A.W. Hins & E.C.M. Jurgens, *Communicatie- en informatie-vrijheid in het digitale tijdperk*, Zwolle: W.E.J. Tjeenk Willink 1995.
- Huizer e.a. 2003** E. Huizer, S. Nas, Chr. Alberdingk Thijm, M. Wessling, 'Nieuwe auteursrecht bedreigt innovatie culturele uitingen,' *Financieele Dagblad* 5 februari 2003.
- IEEE 2002** IEEE, "IEEE to Revise New Copyright Form to Address Author Concerns," 22 april 2002, te vinden op: <http://www.ieee.org/newsinfo/dmca.html>.
- Imfeld 2003** Cassandra Imfeld, 'Playing with fair use? The Digital Millenium Copyright Act's impact on encryption researchers and academicians,' *8 Comm. L. & Pol'y* 2003, p. 111–144.
- Jacobs 2003** B. Jacobs, *De computer de wet gesteld* (oratie Nijmegen) 16 mei 2003, te vinden op: <http://www.cs.kun.nl/~bart/>.

- Koelman 2003** Kamiel J. Koelman, *Auteursrecht en technische voorzieningen: juridische en rechtseconomische aspecten van de bescherming van technische voorzieningen* (diss. Amsterdam UvA), Den Haag: Sdu 2003.
- Koops 1999** Bert-Jaap Koops, *The Crypto Controversy: A Key Conflict in the Information Society*, Den Haag: Kluwer 1999.
- Lemos 2001** Robert Lemos, 'Security Workers: Copyright Law Stifles,' *CNET News* 6 september 2001, te vinden op: <http://news.com.com/2100-1001-272716.html>.
- Levy 2001** Steven Levy, *Crypto: how the code rebels beat the government saving privacy in the digital age*, USA: Penguin 2001.
- McCullagh 2002** Declan McCullagh, 'Security Warning Draws DMCA Threat,' *CNET News* 30 juli 2002, te vinden op: <http://news.com.com/2100-1023-947325.html>.
- De Meij 1996** J.M. de Meij, *Uitingsvrijheid: de vrije informatiestroom in grondwettelijk perspectief*, Amsterdam: Cramwinckel 1996.
- Patijn 1994a** A. Patijn, 'Plannen voor wetgeving inzake cryptografie,' *MF* 1994/6, p. 65.
- Patijn 1994b** A. Patijn, 'Crypto: een zegen of bedreiging,' *Computerrecht* 1994/4, p. 144-150.
- Parviainen 2000** Simo-Pekka Parviainen, *Cryptographic software export controls in the EU* (doctoraalscriptie Universiteit van Helsinki 2000), te vinden op: <http://ethesis.helsinki.fi/julkaisut/oik/julki/pg/parviainen/>.
- Reardon 2003** M. Reardon, 'Routers Rebuff Hacker Attacks,' *Light Reading* 21 juli 2003, te vinden op: http://www.lightreading.com/document.asp?site=lightreading&doc_id=37295.
- Samuelson 2001** Pamela Samuelson, 'Anticircumvention Rules: Threat to Science,' *Science* 2001, p. 2028-2031.
- Schneier 1996** Bruce Schneier, *Applied Cryptography*, New York: Wiley 1996.
- Schneier 2001** B. Schneier, 'Full disclosure,' *Crypto-Gram* 15 november 2001, te vinden op: <http://www.counterpane.com/crypto-gram-0111.html>.
- Singh 2000** Simon Singh, *The code book*, USA: Anchor Books 2000.
- Spoor & Verkade 1993** J.H. Spoor & D.W.F. Verkade, *Auteursrecht*, Deventer: Kluwer 1993.
- Van den Hoven van Genderen 1994** R. van den Hoven van Genderen, 'Het voorlopig voorontwerp tot verbod van de cryptografie. De horror vacui van de ondoorbreekbare beveiliging,' *Computerrecht* 1994/4, p. 157-163.

- Vidstrom 2003** A. Vidstrom, 'Full Disclosure of Vulnerabilities — pros/cons and fake arguments,' te vinden op: <http://ntsecurity.nu/papers/disclosure/>.
- Von Lohmann 2003** F. von Lohmann, 'Unintended consequences: four years under the DMCA,' te vinden op http://www.eff.org/IP/DMCA/20030102_dmca_unintended_consequences.html.
- Vroom-Cramer 1998** B. Vroom-Cramer, *Productinformatie over levensmiddelen*, Lelystad: Koninklijke Vermande 1998.
- Zweers 2003** W. Zweers, 'Minder openheid over softwarefouten?,' *Netkwesties* 63, 12 juni 2003, te vinden op: <http://www.netkwesties.nl/editie63/artikel13.html>.

Regelgeving

Verdragen

- Europees Verdrag voor de Rechten van de Mens, *Trb.* 1951, 154.
- Internationaal Verdrag inzake Burgerrechten en Politieke Rechten, *Trb.* 1969, 99 en *Trb.* 1978, 177 (Nederlandse vertaling).
- Universele Verklaring van de Rechten van de Mens, *Trb.* 1969, 99.
- WIPO Auteursrechtverdrag, *Trb.* 1997, 318 (de Engelse en Franse tekst), en *Trb.* 1998, 247 (de Nederlandse tekst).
- WIPO Verdrag inzake uitvoeringen en fonogrammen, *Trb.* 1997, 319 (de Engelse en Franse tekst), en *Trb.* 1998, 243 (de Nederlandse tekst).
- Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken (Cybercrimeverdrag), *Trb.* 2002, 18.

Verordeningen

- Verordening (EG) 3381/94 van de Raad van 19 december 1994 tot instelling van een communautaire regeling voor exportcontrole op goederen voor tweëerlei gebruik, *PbEG* 1993, L 367/1.
- Verordening (EG) 1334/2000 van de Raad van 22 juni 2000 tot instelling van een communautaire regeling voor controle op de uitvoer van producten en technologie voor tweëerlei gebruik, *PbEG* 2000, L 159/1, gerectificeerd in *PbEG* 2000, L 176/52.
- Verordening (EG) 458/2001 van de Raad van 6 maart 2001 tot wijziging van Verordening (EG) nr. 1334/2000 voor wat betreft de lijst van gecontroleerde producten en technologie voor tweëerlei gebruik bij uitvoer, *PbEG* 2001, L 65/19.
- Verordening (EG) 2432/2001 van de Raad van 20 november 2001 tot wijziging en tot bijwerking van Verordening (EG) nr. 1334/2000 tot instelling van een

communautaire regeling voor controle op de uitvoer van producten en technologie voor tweemaal gebruik, *PbEG* 2001, L 338/1.

Verordening (EG) 149/2003 van de Raad van 27 januari 2003 tot wijziging en tot bijwerking van Verordening (EG) nr. 1334/2000 tot instelling van een communautaire regeling voor controle op de uitvoer van producten en technologie voor tweemaal gebruik, *PbEG* 2003, L 30/1, gerecificeerd in *PbEG* 2003, L 52/11.

Richtlijnen

Richtlijn 91/250/EEG van de Raad van 14 mei 1991 betreffende de rechtsbescherming van computerprogramma's, *PbEG* 1991, L 122/42.

Richtlijn 98/84/EG van het Europees Parlement en de Raad van 20 november 1998 betreffende de rechtsbescherming van diensten gebaseerd op of bestaande uit voorwaardelijke toegang, *PbEG* 1998, L 320/54.

Richtlijn 2001/29/EG van het Europees Parlement en de Raad van 22 mei 2001 betreffende de harmonisatie van bepaalde aspecten van het auteursrecht en de naburige rechten in de informatiemaatschappij, *PbEG* 2001, L 167/10.

Vorbereidende stukken Auteursrechtrichtlijn

Groenboek Auteursrecht in de Informatiemaatschappij, COM(95)382 def.

Vervolg op het Groenboek Auteursrecht in de Informatiemaatschappij, COM(96)586 def.

Voorstel van de Commissie, COM(97)628 def., *PbEG* 1998, C 108/6.

Advies van het Economisch en Sociaal Comité, *PbEG* 1998, C 407/30.

Advies in eerste lezing van het Europees Parlement, *PbEG* 1999, C 150/171.

Gewijzigd voorstel van de Commissie, COM(99)250 def., *PbEG* 1999, C 180/6.

Gemeenschappelijk standpunt van de Raad, *PbEG* 2000, C 344/1.

Aanneming gemeenschappelijk standpunt, SEC(2000)1734 def.

Amendementen in tweede lezing van het Europees Parlement, A5-0043/2001.

Gewijzigd voorstel van de Commissie, COM(2001)170 def.

Overige voorbereidende stukken

Zorgen voor veiligheid van en vertrouwen in elektronische communicatie, naar een Europees kader voor digitale handtekeningen en encryptie, COM(1997)503 def.

Resolutie van het Europees Parlement van 5 september 2001 betreffende het bestaan van een wereldwijd netwerk voor de interceptie van private en commerciële communicatie (Echelon interceptie systeem), A5-0264/2001 - 2001/2098(INI).

Voorstel voor een richtlijn betreffende de maatregelen en procedures om de handhaving van intellectuele eigendomsrechten te waarborgen, COM(2003)46 def.

Verenigde Staten

Digital Millenium Copyright Act, Pub.L.No. 105-304 (1998).

Digital Media Consumers' Rights Act of 2003, H.R. 107 (2003).

Nederland

Parlementaire stukken

Kamerstukken II 1997/98, 25 880, nr. 1.

Kamerstukken II 1998/99, 25 880, nr. 3.

Kamerstukken II 1999/00, 25 880, nr. 10.

Kamerstukken II 2000/01, 27 460, nr. 1.

Kamerstukken II 2000/01, 27 460, nr. 2.

Kamerstukken II 2001/02, 27 925, nr. 10.

Kamerstukken II 2001/02, 28 482, nrs. A en B.

Kamerstukken II 2001/02, 28 482, nrs. 1–2.

Kamerstukken II 2001/02, 28 482, nr. 3.

Kamerstukken II 2002/03, 27 925, nr. 96.

Kamerstukken II 2002/03, 26 581, nr. 2.

Kamerstukken II 2002/03, 28 482, nr. 4.

Kamerstukken II 2002/03, 28 482, nr. 5.

Kamerstukken II 2002/03, 28 482, nr. 7.

Kamerstukken II 2002/03, 28 482, nr. 8.

Aanhangsel Handelingen II 2002/03, nr. 889.

Jurisprudentie

EHRM

EHRM 7 december 1972, NJ 1978, 236 (*Handyside/Verenigd Koninkrijk*).

EHRM 26 april 1979, NJ 1980, 146, m.nt. E.A. Alkema (*Sunday Times*).

EHRM 24 mei 1988, NJ 1991, 685 (*Müller v. Zwitserland*).

EHRM 20 november 1989, *NJ* 1991, 738, m.nt. E.A. Alkema (*Markt intern Verlag*).

EHRM 22 mei 1990, *NJ* 1991, 740, m.nt. E.A. Alkema (*Autronic*).

EHRM 25 augustus 1998, *NJ* 1999, 712 m.nt. EJD (*Hertel*).

EHRM 8 juli 1999, *NJ* 2001, 62, m.nt. EJD (*Baskaya & Okçuoglu v. Turkije*).

Hof

Hof Amsterdam 22 mei 1991, *MediaForum* 1991/9, p. 94 e.v., m.nt. Th.C.J.A. van Engelen (*Esselte/Ten-Electronics*).

Hof Amsterdam 21 februari 2002, *MediaForum* 2002/4, p. 119–120 (*VNU/Canal+*).

Kantonrechter

Pres. Rb. 20 januari 1986, *KG* 1986/92 (*Filmnet I*).

Rb. Den Haag 31 oktober 1990, *IER* 1990/6, p. 139–140 (*BAT/Stivoro*).

Pres. Rb. Amsterdam 22 november 1990, *MediaForum* bijlage 1991/3, p. 27

Rb. Arnhem 1 april 1999, *MediaForum* 1995/5, p. 154–158, m.nt. Aernout Nieuwenhuis (*X v. Van de Bunt*).

Pres. Rb. Haarlem 28 juli 2000, Zaak nr. 66855/KG ZA 00-388.

Rb. Alkmaar 30 november 2000, *Computerrecht* 2001/3, p. 157–159, m.nt. K.J. Koelman.

Pres. Rb. Den Bosch 12 maart 2001, *AMI/Informatierecht* 2001/4, p. 92–97, m.nt. M. de Cock Buning (*Canal+/Xtra Sat*).

Pres. Rb. Middelburg 26 juli 2001, *MediaForum* 2001/9, p. 265 (*Canal+/M-Sat*).

Vzr. Breda 24 april 2002, *AMI/Informatierecht* 2002/4, p. 137–143, m.nt. Jacqueline Seignette (*Stichting BREIN/X*).

Supreme Court

United States v. O'Brien, 391 U.S. 367 (1968).

Court of Appeals

Karn v. U.S. Dept. of State, 107 F.3d 923 (D.C.Cir. 1997).

Bernstein v. U.S. Dept. of Justice, 176 F.3d 1132, (9th Cir. 1999), *MediaForum* 1999/10, m.nt. L.F. Asscher.

Bernstein v. U.S. Dept. of Justice, 192 F.3d 1308 (9th Cir. 1999).

Universal City Studios, Inc. v. Reimerdes, 273 F.3d 429 (2nd Cir. 2001).

Junger v. Daley, 209 F.3d 481 (6th Cir. 2000).

District Court

Karn v. U.S. Dept. of State, 925 F.Supp. 1 (D.D.C. 1996).

Bernstein v. U.S. Dept. of State, 922 F.Supp. 1426 (N.D.Cal. 1996).

Bernstein v. U.S. Dept. of State, 945 F.Supp. 1279 (N.D.Cal. 1996).

Bernstein v. U.S. Dept. of Justice, 974 F. Supp. 1288 (N.D.Cal. 1997).

Junger v. Daley, 8 F.Supp.2d 708 (N.D.Ohio 1998).

Sony Computer Entertainment America, Inc. v. Gamemasters, 87 F.Supp.2d 976 (N.D.Cal. 1999)

RealNetworks, Inc. v. Streambox, Inc., 1999 WL 1448173 (W.D.Wash. 1999).

RealNetworks, Inc. v. Streambox, Inc., 2000 WL 127311 (W.D.Wash. 2000).

RealNetworks, Inc. v. Streambox, Inc., en 2000 WL 141196 (W.D.Wash. 2000)

Universal City Studios, Inc. v. Reimerdes, 2000 WL 48514 (S.D.N.Y. 2000).

Universal City Studios, Inc. v. Reimerdes, 82 F.Supp.2d 211 (S.D.N.Y. 2000).

Universal City Studios, Inc. v. Reimerdes, 98 F.Supp.2d 449 (S.D.N.Y. 2000).

Universal City Studios, Inc. v. Reimerdes, 104 F.Supp.2d 334 (S.D.N.Y. 2000).

Universal City Studios, Inc. v. Reimerdes, 111 F.Supp.2d 294 (S.D.N.Y. 2000).

Universal City Studios, Inc. v. Reimerdes, 111 F.Supp.2d 346 (S.D.N.Y. 2000).

Felten v. RIAA No. CV-01-2669, 6 juni 2001 (D.N.J. 2001).

U.S. v. Elcom Ltd., 203 F.Supp.2d 1111 (N.D.Cal. 2002).

Lexmark International, Inc. v. Static Controls, Inc., niet gepubliceerd (E.D.Ky. 2003), te vinden op: http://www.eff.org/IP/DMCA/Lexmark_v_Static_Controls/20030303-finding-of-facts.pdf.

GNU Free Documentation License

Version 1.2, November 2002

Copyright (C) 2000,2001,2002 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondly, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical

connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough

number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

- A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
- B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
- C. State on the Title page the name of the publisher of the Modified Version, as the publisher.
- D. Preserve all the copyright notices of the Document.
- E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

- F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
- G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
- H. Include an unaltered copy of this License.
- I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
- J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
- K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
- L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
- M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.
- N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.
- O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements."

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements",

"Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See <http://www.gnu.org/copyleft/>.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.