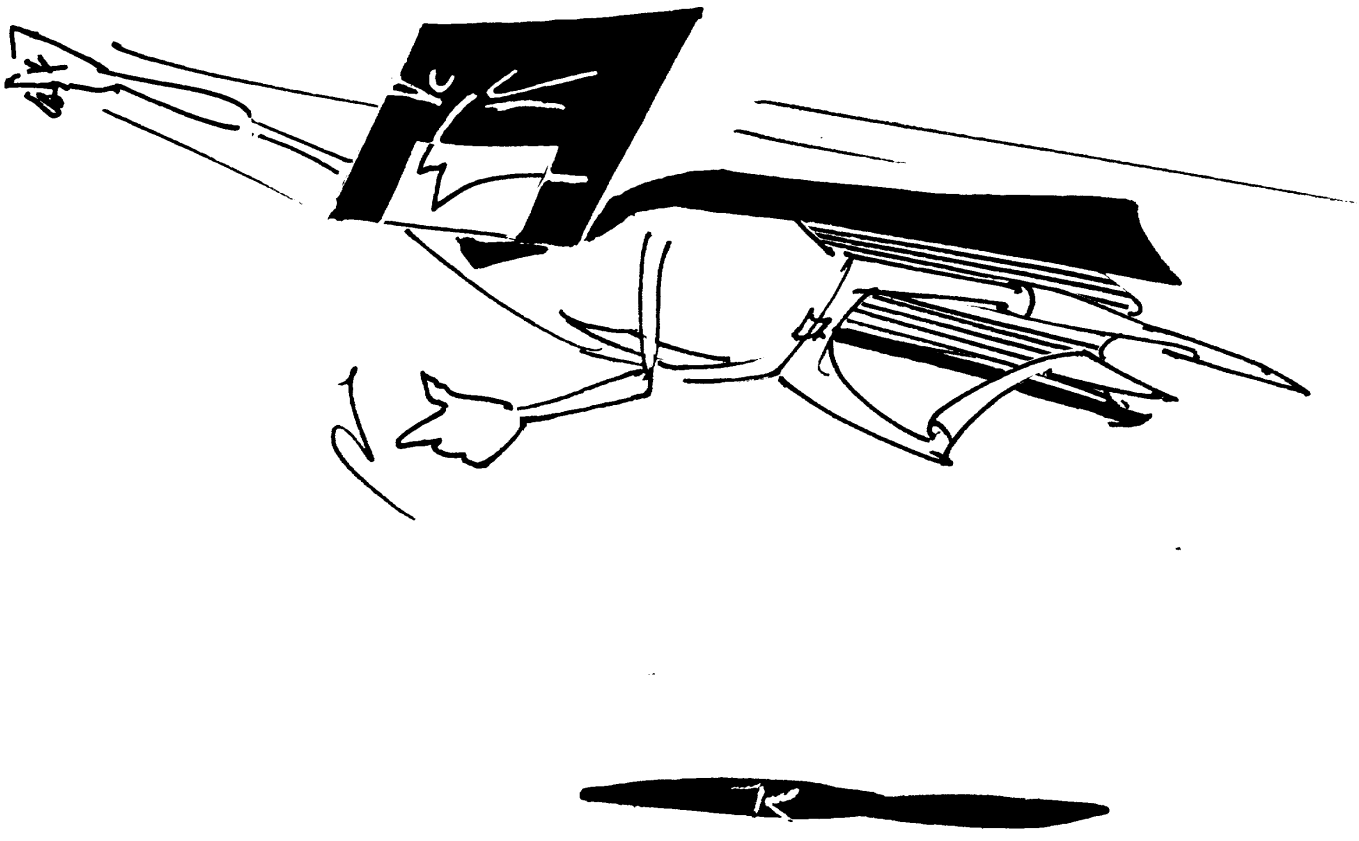
Rechtsvragen over informatietechnologie

ONTWIKKELING, STAND VAN ZAKEN EN BETEKENIS
VAN HET INFORMATICARECHT



P. KLEVE

Rechtsvragen over informatietechnologie

Rechtsvragen over informatietechnologie

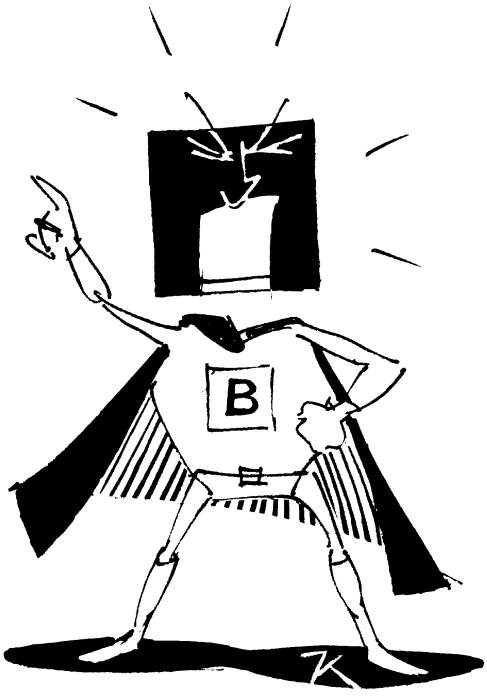
ONTWIKKELING, STAND VAN ZAKEN EN BETEKENIS VAN HET INFORMATICARECHT

P. KLEVE

KONINKLIJKE VERMANDE BV
LELYSTAD - 1996

ISBN 90 5458 400 9 / CIP
NUGI 697

Illustraties: Karel Kindermans, Rotterdam



Inhoudsopgave

Voorwoord XI

Afkortingen XIII

1 Recht en informatietechnologie 1
1.1 Juridische aspecten van informatietechnologie 2
1.2 Informatietechnologie voor juristen 3
1.3 Rechtswetenschappelijk onderzoek en informatietechnologie 4
1.4 Recht binnen de informatiemaatschappij 5
1.5 'Noord-Zuid' verhouding 9
1.6 Perceptie invloed informatietechnologie 10

2 Informaticarecht 12
2.1 Termen en begrippen 13
2.2 'Eigendomsbegrippen' 16
2.3 De juridische kwalificatie van software 17
2.4 Informatica en recht 21
2.4.1 Juridische informatica 21
2.4.2 Informaticarecht 22
2.4.3 Informatierecht 23

2.5 Informaticarecht 24
2.6 Een zelfstandige discipline? 26
2.7 Jurisprudentie 27
2.8 Literatuur 27

3 Inleiding intellectuele rechten 29
3.1 Auteursrecht 31
3.1.1 Werk van letterkunde, wetenschap of kunst 31
3.1.2 Maker 34
3.1.3 Beschermingsomvang 36
3.1.4 Rechtverkrijgenden 38
3.1.5 Beperkingen van het auteursrecht 39
3.2 Octrooirecht 39
3.2.1 Uitvinding 40
3.2.2 Uitvinder 41
3.2.3 Beschermingsomvang 41
3.2.4 Rechtverkrijgenden 42
3.2.5 Beperkingen van het octrooirecht 42
3.3 Chipsrecht 43
3.3.1 Topografie 44
3.3.2 Rechthebbende 44
3.3.3 Beschermingsomvang 45
3.3.4 Beperkingen van het chipsrecht 45
3.4 Literatuur 45

4 Juridische bescherming van software 47
4.1 Beschermingsmogelijkheden 48
4.2 De ontwikkeling van software: stadia en verschijningsvormen 49
4.3 Auteursrechtelijke bescherming van software 52
4.3.1 De hoofdlijnen van de richtlijn 52
4.3.2 Decompilatie 57
4.3.3 Prestatiebescherming 59
4.3.4 Interoperabiliteit en standaardisatie 61
4.3.5 Geschriftenbescherming 61
4.3.6 Overige aandachtspunten 62
4.4 Octrooirechtelijke bescherming van software 64
4.4.1 Werkwijze-octrooien en software 65
4.4.2 Software en het voortbrengsel-octrooi 66
4.5 Jurisprudentie 67
4.6 Literatuur 70

5 Auteursrechtelijke aspecten van databanken en multimedia 71
5.1 Multimedia 72

5.1.1 Digitale informatie 72
5.1.2 Logistieke c.q. distributieproblemen 75
5.1.3 Cumulatie van regimes 75
5.2 Databanken....77
5.2.1 Bulletin board systemen 78
5.2.2 Internet 79
5.2.3 Afbakening....80
5.3 De aanleg van databanken 81
5.3.1 Toestemming....83
5.3.2 Invoer / opslag....84
5.3.3 Uitvoer / raadpleging 86
5.4 De exploitatie van databanken....87
5.5 Jurisprudentie 91
5.6 Literatuur....93

6 Detachering van IT-deskundigen 94
6.1 Automatiseringsovereenkomsten 95
6.2 De bodyshopovereenkomst 97
6.3 De Arbeidsvoorzieningswet 100
6.3.1 Toepasselijkheid Arbvowet 101
6.3.2 De vergunning.... 102
6.4 Inlenersaansprakelijkheid.... 104
6.5 Jurisprudentie 106
6.6 Literatuur.... 107

7 Computercontracten en aansprakelijkheid 108
7.1 Karakteristieken van automatiseringsprojecten 109
7.1.1 Ongelijkheid tussen partijen 109
7.1.2 Produkt van samenwerking 109
7.1.3 Vitaal belang 110
7.1.4 Langdurig 110
7.2 Traject.... 111
7.2.1 Precontractuele fase.... 111
7.2.2 Tot stand koming.... 112
7.2.3 Uitvoering 113
7.2.4 Garantie/onderhoud 113
7.3 Aansprakelijkheid uit wanprestatie.... 114
7.3.1 Toerekenbare tekortkoming? 115
7.3.2 Opties 117
7.3.3 Conclusies 118
7.4 Systematische contractsindeling.... 119
7.4.1 Considerans 120
7.4.2 Definities.... 120

7.4.3 Primaire prestatie-verplichtingen ... 121
7.4.4 Secundaire prestatie-verplichtingen ... 121
7.4.5 Procedures ... 122
7.4.6 Afsluitende juridische bepalingen ... 124
7.4.7 Algemene voorwaarden ... 125
7.5 Jurisprudentie ... 125
7.6 Literatuur ... 125

8 Zelfregulering in de automatiseringsbranche ... 127
8.1 Softwarecertificatie ... 128
8.1.1 Certificatie ... 128
8.1.2 Object van certificatie ... 129
8.1.3 Gevolgen van certificatie voor aansprakelijkheid ... 130
8.2 Beroepscode voor informatici ... 131
8.2.1 Verenigingen van informatici ... 131
8.2.2 Redenen voor een beroepscode ... 132
8.2.3 Gevolgen van gedragscodes ... 133
8.3 Geschillenbeslechting in de automatisering ... 134
8.3.1 Minitrial ... 135
8.3.2 Criteria bij forumkeuze ... 136
8.4 Jurisprudentie ... 139
8.5 Literatuur ... 140

9 EDI elektronisch handelsverkeer ... 141
9.1 Waarom EDI? ... 142
9.2 Rechtsgeldigheid van EDI-transacties ... 145
9.2.1 Vormvereisten ... 145
9.2.2 Wilsovereenstemming ... 146
9.2.3 Overige vereisten ... 147
9.3 Interchange agreement ... 148
9.3.1 Identificatie ... 149
9.3.2 Vertegenwoordigingsbevoegdheid ... 149
9.3.3 Beveiliging ... 150
9.3.4 Gebreken en procedures ... 150
9.3.5 Aansprakelijkheid ... 151
9.3.6 Bewijs ... 152
9.3.7 Bewaring ... 152
9.4 Conflictbeslechting ... 153
9.4.1 Recht versus techniek ... 154
9.4.2 EDI-beheerder als conflictbeslechter ... 155
9.4.3 Een rechtstoekomstig perspectief ... 156
9.5 Jurisprudentie ... 156
9.6 Literatuur ... 157

10 Elektronisch betalingsverkeer 158
10.1 Misbruik 159
10.1.1 Authenticiteit 159
10.1.2 Aansprakelijkheid en bewijs 160
10.2 Privacy 161
10.3 Juridische of technische oplossingen? 163
10.4 Zelfregulering en conflictbeslechting 165
10.5 Jurisprudentie 166
10.6 Literatuur 167

11 Bescherming van persoonsgegevens 168
11.1 Plaatsbepaling 169
11.1.1 Historische achtergrond 171
11.1.2 Europese dimensie 174
11.2 De Wet Persoonsregistraties 177
11.2.1 Materiële normen 179
11.2.2 Zelfregulering 180
11.2.3 Belangen van geregistreerden 182
11.3 Privacy en de overheid 184
11.3.1 Koppeling van bestanden en het sofinummer 185
11.3.2 Beperkte legitimatieplicht 186
11.3.3 Koppeling en fraudebestrijding 187
11.3.4 Aanwending van overheidsautomatisering: een nieuwe richting 189
11.4 Jurisprudentie 191
11.5 Literatuur 191

12 Grensoverschrijdend gegevensverkeer 193
12.1 Aard en omvang van grensoverschrijdend gegevensverkeer 194
12.1.1 Algemene aspecten 195
12.1.2 Belangen 197
12.2 Gegevensbescherming 198
12.2.1 De Wet Persoonsregistraties 200
12.2.2 Te trage groei 200
12.3 Free flow of information 201
12.4 Literatuur 202

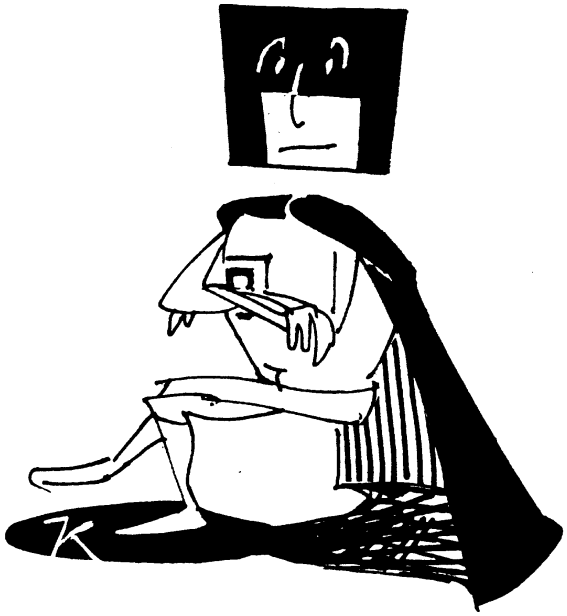
13 Computercriminaliteit 204
13.1 Computercriminaliteit - probleem van definitie 205
13.1.1 Probleem met definitie 205
13.1.2 Juridische overwegingen 209
13.2 Rol van de overheid 210
13.2.1 Wetgeving 210
13.2.2 Wetshandhaving 214

13.2.3 Overige en verklaring 214
13.3 Consequenties voor bedrijven 216
13.4 Strafrecht en internet 216
13.5 Jurisprudentie 218
13.6 Literatuur 221

14 Internetrecht? 222
14.1 Internet 223
14.2 Omgaan met technologie 224
14.3 Prestatiebescherming 225
14.4 Internationale dimensie 226
14.5 Mogelijkheden van integrale toegankelijkheid van rechtsbronnen .. 228
14.6 Noodzakelijke kwantificering en verwetenschappelijking van recht .. 230
14.7 Literatuur 232

Rechtspraakregister 235

Trefwoordenregister 239



Voorwoord

Dit boek is het resultaat van vijf jaar studie. ‘Juridische aspecten van automatisering’ was een deelproject van het onderzoekprojekt van het Centrum voor Informatica en Recht van de Erasmus Universiteit Rotterdam. Het werd voor een belangrijk deel gefinancierd door het Sanders Instituut, het onderzoeksinstituut van de Faculteit der Rechtsgeleerdheid.

Het doel van het project was in de eerste plaats inventariserend en integrerend van aard. Enerzijds wordt het recht beïnvloed door de maatschappelijke ontwikkelingen in brede zin en hierbij speelt informatietechnologie een vooraanstaande rol. Anderzijds beinvloedt informatietechnologie het recht ook rechtstreeks, doordat het gebruik van de nieuwe instrumenten tot juridische problemen leidt. Tenslotte zal het recht een gedaanteverwisseling ondergaan als gevolg van het gebruik van informatietechnologie door de juristen zelf. Na het gesproken, het geschreven en het gedrukte recht is ‘vierde generatie recht’, dus recht in de vorm van geautomatiseerde informatiesystemen allang geen toekomstig verschijnsel meer. Wij ondervinden dagelijks de gevolgen daarvan. De meeste de burgers betreffende beschikkingen van het openbaar bestuur, met name die van de ministeries, worden met behulp van computers genomen. Studenten bijvoorbeeld, die klachten hebben over beslissingen van de Informatiseringsbank met betrekking tot hun studiekostenvergoeding, worden systematisch gewezen op het schier onfeil-

bare karakter van de door de computer genomen beslissing. Internet heeft tot de meest recente golf van juridische belangstelling geleid en de tijd is nog ver dat de juristen weer op rustig vaarwater mogen rekenen.

In dit boek worden de belangrijkste juridische problemen met informatietechnologie behandeld, gewoonlijk op een manier die het boek ook lezenswaardig maakt voor niet-juristen en juristen in de dop.

Pieter Kleve neemt steeds een zelfstandige positie in bij de analyse, en dikwijls ook bij het aandragen van oplossingen voor de geïndentificeerde problemen. Het domein kent voortdurende, vaak zelfs turbulente veranderingen en aan zijn op de feiten gebaseerde, doch creatieve benadering is maatschappelijk en juridisch gezien zeker behoefte. Ik hoop dan ook dat wij ons op frequente herziene herdrukken van dit boek mogen verheugen.

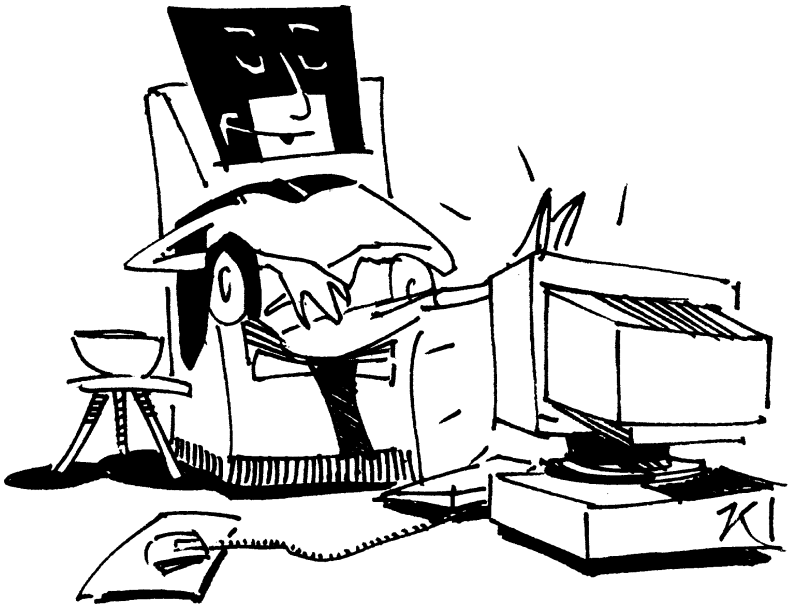
Een studie als deze komt alleen tot stand met behulp van vele personen binnen en buiten de direkte werkomgeving van de schrijver. Onder de velen komt vooral Mr P.C. van Schelven, sinds dit jaar verbonden als advocaat aan het kantoor Derks • Star Busmann • Hanotiau, dank toe voor zijn ondersteuning en voor zijn concrete suggesties.

R.V. De Mulder.

Afkortingen

ADR	Alternative Dispute Resolution
AMR	Auteursrecht, tijdschrift voor auteurs- en mediarecht
Arbvowet	Arbeidsvoorzieningswet
Aw	Auteurswet 1912
BBS	Bulletin Board System
BGH	Bundes Gerichtshof
BIE	Bijblad Industriële Eigendom (tijdschrift)
BSA	Business Software Alliance
BuPo	Internationaal verdrag inzake Burgerrechten en politieke rechten
BW	Burgerlijk Wetboek
Cr	Computerrecht (tijdschrift)
CSV	Coördinatiewet Sociale Verzekeringen
EC	Europese Commissie
EDI	Electronic Data Interchange
EDP	Electronic Data Processing
EU	Europese Unie
EVRM	Europees Verdrag tot bescherming van de Rechten van de Mens en de fundamentele vrijheden
FENIT	Federatie Nederlandse IT-bedrijven

GATT	General Agreement on Tariffs and Trade
GBA	Gemeentelijke Basis Administratie
GRUR	Gewerblicher Rechtsschutz und Urheberrecht (tijdschrift)
GW	Grondwet
HR	Hoge Raad
ICIT	Instituut voor Certificatie van Informatietechnologie
IER	Intellectuele Eigendom en Reclamerecht (tijdschrift)
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
IT	informatietechnologie
JURICAS	Juridische Computeradviessystemen
NGI	Nederlands Genootschap voor Informatici
NJ	Nederlandse Jurisprudentie
NOREA	Nederlandse Orde van Register EDP-Auditors
NVBI	Nederlandse Vereniging van Beëdigde Informatica-deskundigen
OESO	Organisatie voor Economische Samenwerking en Ontwikkeling
Pb	Publikatieblad van de Europese Gemeenschappen
PC	Personal Computer
RI	Register Informaticus
RvdW	Rechtspraak van de Week
ROW	Rijksoctrooiwet 1995
Sr	Wetboek van Strafrecht
Sv	Wetboek van Strafvordering
TRIPs	Trade-Related Aspects of Intellectual Property Rights
VANS	Value Added Network Services
VRI	Vereniging van Register Informatici
WIPO	World Intellectual Property Organization
WPR	Wet Persoonsregistraties
WTO	World Trade Organisation
WWW	World Wide Web



1 Recht en informatietechnologie

De term ‘informaticarecht’ roept bij menigeen die niet zo thuis is in dit vakgebied associaties op met ‘whizz kids’, ‘computerkrakers’ en ‘computerfreaks’. Mensen - in dit geval juristen - met een waarschijnlijk zonderling gedrag, die in bedompte zolderkamers hun tijd onledig achter flikkerende beeldschermen doorbrengen. Daarbij bedienen zij zich van een jargon waardoor betekenisvolle discussies op voorhand uitgesloten lijken. Dit beeld staat in schril contrast met de stereotypering van de traditionele jurist: conservatief dan wel liberaal, erudiet gezeten achter een bureau van ebben- of mahoniehout, omringd door wandkasten gevuld met de pennevruchten van rechtsgeleerde schrijvers. Hoe onjuist zijn beide beelden!

Echter, waar de traditionele jurist meewarig het hoofd kan schudden over de beeldvorming van hemzelf onder buitenstaanders, zo hardnekkig schijnt hij op zijn beurt te volharden in zijn perceptie van de informatica-vakbroeder. Net zo, echter, als de beoefenaar van bijvoorbeeld het zeerecht niet altijd in een bootje zit, zo zit de informaticajurist niet steeds achter de computer. Anders echter dan bij zeerecht kan men bij ‘informaticarecht’ niet louter spreken over een specialisatie. Daarvoor is de invloed van (informatie)-technologie op maatschappelijke ontwikkelingen - en dientengevolge de betekenis daarvan voor recht en rechtsontwikkeling - te algemeen. Dit hoofd-

stuk schetst de samenhang tussen recht en technologie en geeft enkele van die ontwikkelingen aan.

1.1 Juridische aspecten van informatietechnologie

Het ontstaan van het vakgebied informaticarecht zou men kunnen plaatsen in de jaren ‘70, met de opkomst van het fenomeen kantoorautomatisering. Juristen kregen op verschillende manieren te maken met vraagstukken die voortvloeiden uit automatiseringsactiviteiten. Nadat automatisering aanvankelijk was aangewend ten behoeve van technische produktieprocessen werd vervolgens de automatisering van administratieve bedrijfsprocessen gezien als een belangrijke factor voor kostenbeheersing en -besparing. Aan kantoorautomatisering werden ongekende mogelijkheden toegedicht en automatisering was vooral voor computerleveranciers een lucratieve aangelegenheid. De vraag was groot, de techniek voorhanden, de verwachtingen hoog gespannen. Slechts geleidelijk aan groeide het besef - bij afnemers zowel als leveranciers - dat in de euforie omtrent de technologische ontwikkeling onvoldoende was onderkend dat succesvolle automatisering vooral ook te maken heeft met organisatorische aspecten en invoeringsbegeleiding. En zo konden juristen zich gaan buigen over de eerste gevallen van ‘mislukte automatisering’. Opgeschrikt door de alarmerende berichtgeving of door schade en schande wijs geworden, wendden de ondernemers zich vervolgens tot de juristen voor de contractsonderhandelingen, alles onder het ook door de advocatuur uitgedragen motto ‘voorkomen is beter dan genezen’. Niet alleen de computerleveranciers maar ook de advocatuur spinde garen bij de automatiseringshausse.

Een volgende tendens lag in de verschuiving van functionaliteit van apparatuur naar programmatuur, van hardware naar software. In het kielzog van de grote computerfabrikanten kwam een geheel nieuwe industrie tot bloei, die van de makers van toepassingsprogramma’s. Aanvankelijk kleine bedrijven, soms zelfs eenmansbureau’s, zagen hun kans schoon om onafhankelijk van de computerleveranciers toepassingsprogramma’s te ontwikkelen zoals boekhouding, tekstverwerking e.d., en deze aan te bieden op de markt van geïnstalleerde systemen. De investeringen in deze programmeerarbeid moesten worden veilig gesteld en juristen konden zich buigen over het vraagstuk softwarebescherming.

Dat computers niet alleen tot heil van de mensheid konden dienen, maar ook tot inspiratie van het criminele gilde, werd duidelijk door het bekend worden van allerlei systeemmanipulaties, zoals het invoeren van gefingeerde facturen, het naar de eigen bankrekening afboeken van afrondingsverschillen en wat dies meer zij. Tamelijk vervelend daarbij was dat deze manipulaties nogal gemakkelijk verdoezeld konden worden; gegevensbestanden werden

nadien gewijzigd of gewist, de computer liet geen sporen na. Computercriminaliteit werd voer voor strafrechtjuristen en een plaag voor opsporingsambtenaren.

Als slot van dit indicatieve overzicht zij nog vermeld de toenemende zorg omtrent het beheer van privacy-gevoelige gegevensbestanden. De commotie rond de volkstelling van 1970 was nog niet gestild, of allerwegen werden bij de overheid en in het bedrijfsleven persoonsregistraties aangelegd, gekoppeld of uitgewisseld. En wederom was het aan juristen deze dataparadijzen te beteugelen en de angst voor het 'big brother is watching you' effect weg te nemen. Dat zal zo rond 1984 geweest zijn.

De hier genoemde juridische aspecten van automatisering - aansprakelijkheid bij mislukte automatisering, computercontracten, softwarebescherming, computercriminaliteit en bescherming van persoonsgegevens - worden tot het computerrecht of *informaticarecht* gerekend (zie verder hoofdstuk twee).

1.2 Informatietechnologie voor juristen

Automatisering heeft juristen evenwel ook op een andere manier niet onberoerd gelaten. In de juridische beroepsbeoefening oriënteerde men zich op de toepassing van automatisering ten behoeve van het eigen kantoor. Het spreekt voor zich dat automatisering van de financiële administratie net zo goed voor advocatenkantoren nuttig is. Maar ook meer aan de advocatuur eigen applicaties als dossieradministratie en roladministratie werden ontwikkeld. Het belangrijkste aandachtspunt echter binnen deze juridische informatica - waarvoor ook de benaming *rechtsinformatica* wordt gehanteerd - zijn teksten. Het recht wordt immers vorm gegeven in teksten, juristen lezen teksten, juristen produceren teksten. De verreweg meest gangbare toepassing van automatisering in het recht is dan ook tekstverwerking. Maar waar de toepassing van tekstverwerkers - overigens uiterst nuttig - beperkt blijft tot het invoeren, opslaan, aanpassen en reproduceren van teksten, reiken de aspiraties van de beoefenaars van de rechtsinformatica verder, namelijk tot de automatisering van primaire juridische processen.

Allereerst denken we dan aan het toegankelijk maken van teksten. Van steeds meer teksten. De computer blijkt een zo goed als feilloos hulpmiddel voor het snel en doeltreffend vinden van teksten. Er verschijnen steeds meer juridische databanken, zowel op het gebied van wetgeving, jurisprudentie als dogmatiek, en menig advocatenkantoor beheert een eigen kennisdatabank. En deze ontwikkeling staat pas aan het begin. Een handicap van databanken is thans vaak nog de zoekmethode. Een enkel trefwoord kan tot een schier eindeloze hoeveelheid van - ook niet-relevante - teksten leiden, terwijl juist sommige wel relevante er niet bij hoeven te zitten. Een trefwoord is tenslotte

niet meer dan een letterpatroon. Om de praktische bruikbaarheid van databanken te vergroten is de ontwikkeling van conceptuele zoekmethoden nodig.

Ook voor de fase tussen het zoeken van teksten en het (re)produceren daarvan, die wel wordt aangeduid als het juridisch inhoudelijke terrein, worden computers steeds belangrijker. Juridische computer adviessystemen (zoals JURICAS) ondersteunen juristen bij het nemen van beslissingen. Deze systemen zijn van belang bij het vastleggen van juridisch relevante transacties ter ondersteuning van beslissingen en sinds enkele jaren in toenemende mate ook als geprogrammeerd beslissingensysteem, dus zelfs als plaatsvervanger van de beslisser (de toekenning van studiefinanciering bijvoorbeeld). De uitvoering van sommige wetten is heden ten dage niet meer mogelijk zonder zulke systemen. Men denke bijvoorbeeld aan de fiscus, de reeds genoemde studiefinanciering en het bekeurings-afhandelingssysteem (BAS).

Door de toegenomen complexiteit van regelgeving, vooral in combinatie met de uitvoering daarvan, zien we op verschillende departementen dat zelfs de opstelling van regels steeds vaker ondersteund wordt door computermodellen, en dat soms zelfs bepalend is voor de inhoud van de wettelijke regeling de mate waarin de uitvoering daarvan met behulp van computersystemen kan worden gerealiseerd. Een tendens die de overgang markeert naar '4e-generatie' wetgeving: van het gesproken recht, het geschreven recht en het gedrukte recht naar het gedigitaliseerde recht. Zoals dat met iedere fase het geval is geweest, zal ook nu de macht van de centrale overheid weer kunnen toenemen, door de verspreiding via computers van regelgeving waarvan zowel de opstelling als de uitvoering centraal kan worden beheerst.

1.3 Rechtswetenschappelijk onderzoek en informatietechnologie

Naast de juridische aspecten en de juridische toepassingen van automatisering gaat er van de computer een belangrijke impuls uit naar de wetenschappelijke beoefening van recht en de rechtstheoretische ontwikkeling. Als object van wetenschap, gedefinieerd als het vermeerderen van kennis, heeft recht in de academische wereld altijd een wat bijzondere plaats ingenomen. De beoefening van de rechtswetenschap is bij gebreke van voldoende kwantitatief empirische kennis omtrent de werking van recht toch vooral een beoefening van een 'kunde' gebleven, waarvan de beperking ook in de benaming *rechtsgeleerdheid* tot uitdrukking komt.

Dankzij de computer is het nu mogelijk omvangrijke tekstbestanden - in de orde van grootte van bijvoorbeeld de gepubliceerde Nederlandse Jurisprudentie - te onderzoeken. Uitkomsten van dergelijk onderzoek zijn bijvoorbeeld welke factoren een rol gespeeld hebben bij het tot stand komen van bepaalde beslissingen. Indien vervat in een model, moet het mogelijk worden op grond daarvan voorspellingen te doen. Statistische analyses

kunnen behulpzaam zijn bij het met grotere mate van zekerheid doen van voorspellingen, bijvoorbeeld omtrent de kans dat een aan te vangen rechtsgeding tot een gunstige beslissing zal leiden.

Door sommigen wordt reeds de mogelijkheid voorzien om in de toekomst uitspraken te doen over de effectiviteit van voorgenomen wetgeving, een belangrijk onderdeel van de opportuniteitsvraag. Ter aanduiding van deze empirische tak van de rechtswetenschap, die steunt op het gebruik van kwantitatief wiskundige modellen, wordt wel de term *jurimetrie* gehanteerd.

1.4 Recht binnen de informatiemaatschappij

De aanvankelijke opvatting van velen dat de raakvlakken van recht en informatica beperkt zouden blijven tot de twee nieuwe specialisaties informaticarecht en rechtsinformatica, begint zich af te tekenen als een grove onderschatting van de 'impact' van informatietechnologie binnen onze samenleving, en dus binnen het recht. Waar eertijds nog werd verondersteld dat deze juridische aspecten op termijn herleid zouden worden naar traditionele disciplines, zoals het contractenrecht en het intellectuele eigendomsrecht, blijkt zich thans een geheel eigen perspectief te hebben ontwikkeld. Gezaghebbende juristen als Pitlo en Scholten hebben altijd gewezen op de maatschappelijke functie van recht. Wil recht daadwerkelijk een neerslag zijn van gerechtvaardigde behoeften, dan dient het de samenleving te bestuderen en veranderingen daarin te onderkennen. Het recht beoogt die veranderingen te normeren, te reguleren en waar gewenst te stimuleren. Zonder overdrijving kan gesteld worden dat in de huidige samenleving iedere verandering van enige importantie voortkomt uit of samenhangt met ontwikkelingen op het gebied van (informatie)technologie. De hedendaagse juridische beroepsuitoefening is niet meer denkbaar zonder kennis van die ontwikkelingen. Het rapport van de 'tweede commissie Franken' biedt een uitvoerige analyse van deze verschijnselen.

De informatiemaatschappij wordt inmiddels van fictie tot werkelijkheid. In de jaren '80 hebben we gezien dat personal computers automatiseringstoepassingen binnen ieders (hand)bereik hebben gebracht. De positie van de computergiganten die voorheen deze markt domineerden met hun minicomputers en mainframes is drastisch gewijzigd. Het mainframe lijkt vrijwel verdrongen door die kleine, goedkopere computers, die steeds krachtiger worden en eenvoudiger te bedienen. Reuzen op technologiegebied zijn er op stuk gelopen of hebben de bakens moeten verzetten. Illustratief is wel de machtsverschuiving van de fabrikanten van computer hardware naar de ontwerpers van operatingsystemen (besturingssoftware) en andere essentiële software. Waar eens IBM de markt dicteerde, is het nu Microsoft als leverancier van een besturingssysteem waar alle softwareontwikkelaars hun pro-

gramma's op afstemmen. De strijd om de standaarden is in alle hevigheid losgebarsten. De jaren '90 voegen hier weer een dimensie aan toe die de samenleving ingrijpend zal beïnvloeden: draadloze, mobiele communicatie. De combinatie van computersystemen en telecommunicatie, ook wel telematica genoemd, vormt de technologische conditie waaronder de informatiemaatschappij nu eerst tot volle wasdom zal komen. De 'hobbel' van de infrastructuur zal in de jaren '90 genomen worden. Vanwege de voortschrijding van ISDN (Integrated Services Digital Network, de integratie van spraak, data, beeld en tekst over één kabel) zal grootschalig gebruik van internet en multimedia niet langer gehinderd worden door ontoereikende infrastructurele voorzieningen. Satellietcommunicatie zal bovendien het belang van kabelverbindingen doen verminderen. Hoewel de strijd binnen de wereld van de hardware en de software bij lange na nog niet gestreden is, kunnen we ons reeds opmaken voor die van het object van de informatica: de beschikbaarheid en bescherming van de *data* zelf.

Personal computers, netwerken, multimedia en draadloze communicatie hebben niet alleen als object betekenis voor het recht. Ook zijn zij van strategisch belang voor ondernemingen en overheden voor het eigen functioneren. Maar vooral zullen zij grote verschuivingen in bestaande machtsstructuren tot gevolg hebben. Tenminste drie terreinen zijn hierin aan te duiden:

1. De met de informatietechnologie samenhangende globalisering heeft invloed op de machtsverhoudingen tussen staten en op die tussen staten en het internationaal opererende bedrijfsleven;
2. Er is een veranderende machtsverhouding tussen de overheid en burgers, tussen overheden onderling en tussen wetgevende, rechterlijke en uitvoerende macht;
3. Er treden verschuivingen op in de economische orde en in de rechtsorde tengevolge van drastische wijzigingen in de produktie van goederen en diensten en het handels- en geldverkeer.

Ad 1. Van daadwerkelijke soevereiniteit van staten, in de zin van zelfbeschikkingsrecht van autonome entiteiten, is tegenwoordig steeds minder sprake. Het wetgevend handelen en ook het overig optreden van nationale overheden is reeds verregaand ingeperkt door internationale verdragen - zoals ten onzent vooral het EU-verdrag het kader afbakent van de nationale bevoegdheden - en supranationale organisaties. In dit verband kan de commotie rondom 'Maastricht' dan ook nauwelijks anders begrepen worden dan dat burgers zich kennelijk eerst nu bewust worden van deze inperkingen. Maar ook overigens is de wederzijdse afhankelijkheid van staten onderling - men denke maar aan de koppeling van de waarde van de Nederlandse Gulden aan die van de Duitse Mark - een de facto beperking van soeverein optreden. Ondanks de huidige destabilisering in sommige delen van Europa en het hier en daar

oplevend nationalisme mag men verwachten dat deze tendens van onderlinge afhankelijkheid en integratie zich alleen maar zal voortzetten.

De nieuwe ordening zal echter een inbreuk op de nationale soevereiniteit te zien geven vanuit een heel andere hoek, die vanuit het bedrijfsleven, waarvan de reikwijdte nauwelijks te voorspellen valt. Van telematica zal een enorme stimulans uitgaan op de wereldhandel. Het belang van vestigingsplaatsen van internationaal opererende concerns zal nog verder afnemen, aangezien het als gevolg van de moderne telecommunicatie geen verschil meer maakt voor het besturen van een onderneming en voor het sluiten van transacties of dit vanuit hetzelfde gebouw, dan wel vanuit een ander werelddeel geschiedt. En waar bij het verplaatsen van produktiefaciliteiten nog rekening gehouden diende te worden met de daarmee gepaard gaande logistieke rompslomp, speelt dit met betrekking tot de data-industrie geen enkele rol van betekenis meer, vanwege het ontbreken van iedere fysieke belemmering. Het is aannemelijk te veronderstellen dat er in de nabije toekomst meer dan thans een (economische) machtsfactor tot stand komt *naast* de staatsmacht. Ondernemingen die in dit circuit participeren, zullen, evenals multinationals, optreden als werkelijk autonoom opererende entiteiten, voor wie de huidige staatsorganisaties nog alleen een belemmering vormen. Voor overheden zal dit betekenen dat zij zich moeten heroriënteren op hun functioneren, waarbij het evident is dat zij - gelijk een marktpartij - een aandeel in de informatievoorziening zullen trachten te verwerven.

Ad 2. Het gebruik van talloze databestanden door de overheid en de koppeling daartussen bevorderen de ‘transparantie’ van burgers. Het is een ontwikkeling die op gespannen voet staat met grondrechten zoals het recht op privacy, met rechtsbeginselen en waarborgen bijvoorbeeld ten aanzien van de ‘verdachte’ en meer algemeen met beginselen van rechtstaat en democratie. Het huidige tijdsbeeld bijvoorbeeld wordt gekenmerkt door de opvatting dat zo goed als ieder gedrag dat strekt tot vermindering van fraude gelegitimeerd is, met name fraude in de belastingen en de sociale voorzieningen. Los van de vraag in hoeverre deze tijdgeest door de overheid wordt aangegrepen om haar positie te versterken, zal dit overheidsgedrag niet zelden inbreuk maken op de hier genoemde rechtsnormen. De informatiemaatschappij zal voorts van invloed zijn op de democratische verhoudingen tussen overheden en burgers. Hierbij zijn zowel ontwikkelingen denkbaar die deze verhoudingen positief kunnen beïnvloeden als negatief. Ook meer algemeen zullen we een verandering zien in de omgang tussen overheden en burgers. Het is in dit verband zeer wel denkbaar dat individuele burgers de overheid steeds minder ‘partij’ kunnen geven. Tenslotte, zoals we hierboven reeds signaleerden, zal de ontwikkeling van 4e-generatie wetgeving een versterkte centralistische tendens bewerkstelligen.

Belangwekkend hierin vanuit juridisch oogpunt is dat al deze maatschappelijke veranderingen zich schijnen te voltrekken zonder dat daaraan enige ideologie dan wel politieke denkbeelden ten grondslag liggen. Wat in het voormalig Oostblok op basis van ideologie niet is gelukt - een door de overheid gecontroleerde samenleving - lijkt in het Westen realiteit te worden op basis van implementatie van informatietechnologie. Anders dan in het voormalig Oostblok, is de toenemende machtsconcentratie bij de centrale overheid geen bewuste (politieke) strategie, maar eerder een (toevallig) gevolg van technologische ontwikkelingen, dat zich tot heden buiten het blikveld van betrokkenen (burgers) lijkt af te spelen. Dit zet toch aan het denken over Oost-Europese schijnbare onvrijheid ten opzichte van Westerse schijnvrijheid. Een belangrijke taak derhalve voor juristen om de hiermee verband houdende normatieve vraagstukken voor het voetlicht en in de maatschappelijke belangstelling te brengen. Overigens zien we dat het hierboven gehanteerde onderscheid tussen informaticarecht en rechtsinformatica zowel in de praktijk als in de theorievorming steeds meer is gaan vervagen. Waar het informaticarecht zich ten doel stelt normatieve vragen met betrekking tot de invoering van informatietechnologie te beantwoorden, is het juist de rechtsinformatica die deze vragen oproept.

Ad 3. Een synthese die ten grondslag ligt aan te verwachten verschuivingen in de economische orde is die tussen het elektronisch handelsverkeer en het elektronisch geldverkeer. Onder invloed van EDI (electronic data interchange) zal de manier van zaken doen drastisch wijzigen. Ten aanzien van het handelsverkeer in een bedrijfskolom zal de traditionele marketing inspanning, gericht op afnemersselectie, aanbod, overeenkomst en financiële afwikkeling, geleidelijk overgaan in het participeren in (besloten) netwerken. Voor wat betreft incidentele transacties zullen vraag en aanbod, alsmede het sluiten van de overeenkomst steeds meer plaats vinden door middel van open computernetwerken zoals internet. Voorts zal EDI voor veel ondernemingen de mogelijkheid tot ‘global sourcing’ realiseren. Dit veranderend handelsverkeer stelt eisen aan aanbieders in de zakelijke en financiële dienstverlening. Vanuit de gedachte dat er al een netwerk functioneert dat de transacties registreert, is het nog maar een kleine stap om datzelfde netwerk te benutten voor de registratie van rekening-courant-verhoudingen. We betreden hierbij het terrein van de wetgever, de financiële wereld en de geschillenbeslechter.

Nogal eens kan men beluisteren dat de wetgever inspanningen zou moeten verrichten om het elektronisch handelsverkeer te bevorderen. Deze eenzijdige oriëntatie op de juridische aspecten van EDI gaat in feite voorbij aan de realiteit van de alsmaar voortgaande invoering van EDI. In de praktijk is het nu juist zo dat men veel minder blijkt aangewezen op (overheids)regelgeving en dat het bedrijfsleven in toenemende mate een ‘interne’ aangelegenheid wordt waarbinnen interventie vanuit overheids- of supranationale organisaties

steeds minder wenselijk wordt. De participatie die vanuit overheidswege benodigd is, wordt inmiddels gerealiseerd door de mogelijkheden van elektronische inklaring en andere douaneformaliteiten. Speelde de gewone rechter al een marginale rol bij de geschillenbeslechting in het handelsverkeer, het is te verwachten dat internationale arbitrage eveneens aan betekenis zal inboeten. Hier lijkt namelijk een uitgelezen positie weggelegd voor de netwerkbeheerder, de nieuwe intermediaire dienstverlener.

Voor wat betreft de functie van de banken in het geldverkeer zal zich wederom een moderne variant op het verhaal van David en Goliath kunnen aandienen. Evenals de oprichter van het destijds betekenisarme Microsoft de machtspositie van IBM onderuit heeft gehaald, is het hier zo dat in beginsel vanuit iedere zolderkamer waar een PC staat met een enthousiaste ondernemer aan het toetsenbord intermediaire netwerk dienstverlening kan worden aangeboden - waaronder de registratie van rekening couranten - welke in rechtstreekse concurrentie daarmee zal kunnen treden.

1.5 ‘Noord-Zuid’ verhouding

Hierboven hebben we gewag gemaakt van verschuivingen in machtsstructuren, tengevolge van de voortschrijdende informatietechnologie. Omdat door telematica de wereld kleiner wordt, zullen veel van deze verschuivingen een mondiaal karakter hebben. In dat kader past zeker een opmerking over de ‘Noord-Zuid’ verhouding, in feite een vierde terrein waarop verschuivingen tengevolge van de informatietechnologie plaats kunnen hebben.

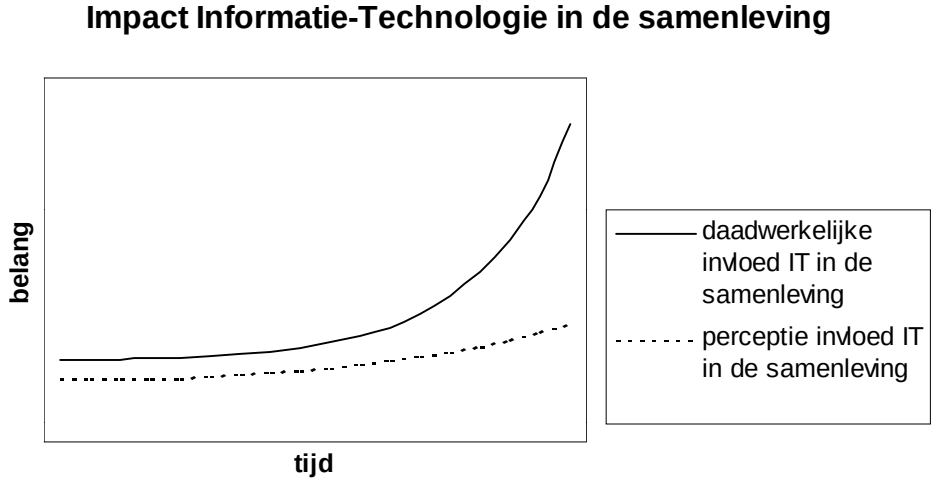
Voorzover ontwikkelingslanden in de internationale afspraken omtrent de frequentieverdeling en toegang tot communicatiesatellieten niet wederom in een achterstandspositie worden gemanoeuvreerd, kan telematica een belangrijke bijdrage leveren aan de aanpak van de ontwikkelingsproblematiek. Een vraagstuk dat in de westerse samenleving steeds meer aan belang toeneemt, getuige de grote toeloop van asielzoekers, die niet alleen uit politieke motieven verklaard kan worden. Was het ontwikkelingsvraagstuk eerst nog een aangelegenheid voor ‘ver weg politiek’, inmiddels hebben de ‘kansarmen’ de mobiliteit ontdekt. En zolang de westerse landen niet een gedeelte van de welvaart wensen weg te brengen, zullen mensen uit de derde wereld naar hier komen voor een aandeel in de welvaart. Bovenop de problemen waarmee de westerse economieën te kampen hebben, zien we nu al het gevaar dat deze toestroom op verschillende plaatsen binnen West-Europa tot ontwrichting van de samenleving kan leiden. Het is een signaal dat niet anders kan worden opgepakt dan dat er nu werkelijk serieus werk van moet worden gemaakt. In een tijd waarin extreem rechts belangrijk aan aanhang wint, er discussies gaande zijn om minimumlonen te verlaten teneinde de concurrentie met lagelonen landen aan te kunnen, wordt het nuttig daadwerkelijk na te denken over

verhoging van de levensstandaard elders, in plaats van aanpassing hier aan daar.

Telematica lijkt daar een antwoord op te kunnen geven. Behoud en verdere ontwikkeling van hoogwaardige kennis van informatietechnologie is voor de westerse landen een prioriteit van de eerste orde, terwijl activiteiten als de verwerking van data en software-ontwikkeling juist bij uitstek geschikt lijken voor economische impulsen in ontwikkelingslanden. Dankzij mobiele, draadloze communicatie is de infrastructurele achterstand in ieder geval veel minder zwaarwegend geworden.

1.6 Perceptie invloed informatietechnologie

Waarom nu kan met zoveel overtuiging dit standpunt over de gevolgen van informatietechnologie naar voren worden gebracht? Voor een deel kan een verklaring worden gevonden in het uitgangspunt dat een verregaande mate van invoering van telematica - een 'technology push' die niet te stuiten is - een enorme reductie van 'informatiekosten' tot gevolg zal hebben. Dit betekent dat er een afnemende noodzaak ontstaat voor traditionele, bekende intermediaire functies. Bij de in 1.4 hierboven onderscheiden drie deelterreinen zijn dat de (nationale) staat (met in haar kielzog de nationale overheidsrechter), de decentrale overheden, respectievelijk bijvoorbeeld het bankwezen en andere zakelijke, intermediaire dienstverleners.



Figuur 1: Onderschatting van de impact van informatietechnologie in de samenleving.

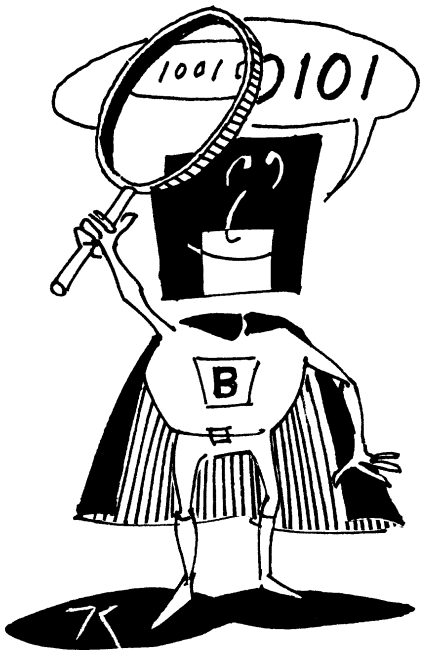
De grafiek in figuur 1. geeft de veronderstelling weer dat de daadwerkelijke invloed van informatietechnologie in de samenleving aanmerkelijk groter is

dan de perceptie daarvan. Bovendien komt hierin het - eveneens veronderstelde - omslagpunt tot uiting, dat de jaren ‘90 markeert als de intrede in de ‘informatiemaatschappij’.

Als redenen voor de veronderstelde explosieve toename van de ‘impact’ van informatietechnologie kunnen worden aangevoerd:

- prijserosie computers, onder toenemende kracht en functionaliteit;
- multimedia en integratie van gebruiksmogelijkheden;
- stijging consumentenaandeel omzet van nul tot meer dan 50% tussen ‘90 en ‘94;
- versterking ontwikkeling en invoering nieuwe technologie onder invloed particulier gebruik (‘technology pull’);
- voortgaande liberalisering telecommunicatiemarkt;
- mobiele, draadloze communicatie;
- breedband netwerken;
- internet.

Illustratief voor de beleving onder studenten van het hier geschetste perspectief mag evenwel zijn de reactie van een student die eens terloops informeerde naar het vak van schrijver dezes. Op het antwoord dat dat informaticarecht was, keerde hij zich om met de opmerking dat hij niet zo geïnteresseerd was in computers. Waarop hij zijn gang vervolgde naar de geldautomaat omdat hij net zijn (geautomatiseerde) beschikking van zijn studiefinanciering had gekregen.



2 Informaticarecht

In het vorige hoofdstuk is geschetst dat er geleidelijk aan een ontwikkeling heeft plaats gevonden die tot een zekere profilering van het ‘vakgebied’ informaticarecht heeft geleid en verder zal leiden. Binnen het informaticarecht treffen we in de eerste plaats onderwerpen aan die raken aan de informatietechnologie zelf, zoals de juridische bescherming van software, chips, databanken en data. In de tweede plaats besteedt informaticarecht aandacht aan aspecten met betrekking tot automatiseringsprojecten, zoals computercontracten, aansprakelijkheid bij (mislukte) automatisering en detachering van automatiseringsdeskundigen. Ten derde beoogt informaticarecht maatschappelijke gevolgen van informatietechnologie in een breder juridisch kader te plaatsen, zoals het elektronisch handels- en betalingsverkeer, privacyvraagstukken en computercriminaliteit. Als zodanig is informaticarecht meer te beschouwen als de *hedendaagse invalshoek* van recht, dan als een vakgebied daarbinnen. En dus een van importantie, niet alleen maatschappelijk, maar ook juridisch.

Een van de verrijkingen van het informaticarecht voor de traditionele rechtsgebieden, zoals privaatrecht en strafrecht, en voor de rechtsontwikkeling is dat het zich vaak begeeft op de grenzen van bestaande juridische dogmatiek. In zoverre is er sprake van verdieping van traditionele juridische

disciplines. Bovendien heeft binnen de invalshoek van het informaticarecht integratie plaats van de verschillende juridische disciplines.

Een belangrijke aanleiding voor het ontstaan van informaticarecht vormt informatie zelf. Nu is informatie zelf niet nieuw, ook niet binnen de juridische wereld. Slechts de toegenomen beheersbaarheid, manipulatie en aanwending van informatie is nieuw, tengevolge van nieuwe technieken. Hier rijst de vraag naar de relatie met een ander nieuw vakgebied: (auteurs-, media- en) informatierecht. Ook dit vakgebied is tot stand gekomen onder invloed van het aanmerkelijk toegenomen belang van informatie. De invalshoek van het informatierecht is die van een verdere uitbouw van bestaande juridische dogmatiek waaronder ook *niet* aan de automatisering gerelateerde aandachtsgebieden vallen. Informaticarecht is vooral gericht op de factor technologie en de daaruit voortvloeiende maatschappelijke consequenties, ook die welke buiten het blikveld van het informatierecht vallen. Informatierecht en informaticarecht zijn dan ook disciplines die met elkaar niet strijden om de voorrang, doch wederzijds bevruchtend zijn.

Voor juristen die zich wensen bezig te houden met informaticarecht is bekendheid met termen en begrippen uit de informatica natuurlijk onontbeerlijk. Informatietechnologie kent een eigen jargon, dat helaas niet altijd eenduidig wordt gehanteerd. Maar bovendien is vooral van belang welke *juridische kwalificatie* aan die begrippen kan worden verbonden. In dit hoofdstuk worden enkele voor het informaticarecht belangrijke termen nader omschreven. Vervolgens wordt ingegaan op de belangrijke vraag van de juridische kwalificatie van software (c.q. gegevens, c.q. informatie) en vindt een nadere, globale afbakening plaats van het informaticarecht.

2.1 Termen en begrippen

Informatica is een relatief jong vakgebied, dat bovendien gekenmerkt wordt door snel op elkaar volgende ontwikkelingen. De in dit vakgebied gehanteerde terminologie is dan ook geenszins eenduidig. In juridische teksten en wetgeving wordt hiermee onvoldoende rekening gehouden.

Zo wordt in de richtlijn softwarebescherming gesproken van ‘interfaces’ (onderdelen van het programma die koppeling en interactie van een systeem verzekeren). De term interface kan betekenen dat gedeelte van een computerprogramma dat verantwoordelijk is voor de interactie met gegevensbestanden en/of andere computerprogramma’s, maar bijvoorbeeld ook de wijze waarop een programma zich presenteert aan de gebruikers. Zelfs kan men beweren dat het toetsenbord een interface is, tussen gebruiker en centrale verwerkingseenheid.

Gezien de gememoreerde snelheid van de technische ontwikkelingen is het niet zinvol in de wet een uitgebreide en per definitie arbitraire begrippenlijst

te hanteren. Ter voorkoming van misverstanden echter, is het wenselijk om vooral te achterhalen wat in een concrete situatie nu met welke term wordt bedoeld.

Mede ten gevolge van de onduidelijkheid van het informatica jargon bestaat er, behalve ten aanzien van de technische termen zelf, ook onduidelijkheid of de bedoelde begrippen te brengen zijn onder de juridische begrippen. Is software een zaak in de juridische betekenis? Dienen we daarbij nog te onderscheiden tussen de privaatrechtelijke en strafrechtelijke dogmatiek? Kunnen gegevens zaken zijn? Is een computerbestand een geschrift? Ter oriëntatie op het informaticarecht is het nuttig om eerst eens stil te staan bij een aantal relevante termen.

INFORMATICA

Informatica is de kunst en wetenschap die de verzameling, opslag, verwerking en distributie van gegevens door middel van geautomatiseerde systemen (computers) bestudeert.

GEGEVENS

Met gegevens (of data) wordt bedoeld patronen die informatie kunnen bevatten. Gegevens zijn representaties van feiten.

INFORMATIE

Een uitspraak bevat informatie als hij antwoord geeft op een vraag van iemand. Informatie vermindert onzekerheid. Informatie is te kwantificeren door de mate waarin onzekerheid wordt weggenomen.

SOFTWARE

Software is een ambigu begrip. Enerzijds wordt software gebruikt in de abstracte betekenis van ‘geestesprodukt’, het ‘werk’ in de zin van de Auteurswet 1912. Anderzijds wordt de term software gehanteerd ter aanduiding van een concreet exemplaar van een computerprogramma. (Soms worden ook de ‘listing’ - de uitdraai van de programmaregels - en de documentatie hiertoe gerekend.) Er bestaat een verschil van opvatting over het karakter van zo’n concreet exemplaar. Sommigen menen dat een exemplaar van een computerprogramma bestaat uit een materiële drager, waarop onstoffelijke gegevens - de software - zijn vastgelegd. Deze opvatting echter is onbegrijpelijk. Juister is het om een exemplaar van een computerprogramma zowel fysisch als juridisch te kwalificeren als een stoffelijk object, een zaak dus (zie hieronder 2.3)

Een invalshoek waarom software niet als zaak zou moeten worden aangemerkt, zou kunnen liggen in de veronderstelling dat met gegevens andere *belangen* in het geding zijn. Gegevens nemen in het informaticarecht een

belangrijke plaats in. Hoewel aan informatie doorgaans meer belang wordt toegekend, zullen we zien dat de bescherming van die belangen veelal verloopt via de bescherming van de patronen waarin die informatie kan zijn vervat. Het is meer hanteerbaar om gegevens te beschermen, aangezien het niet zo hoeft te zijn dat dezelfde gegevens voor iedereen dezelfde informatie opleveren.

De Commissie Computercriminaliteit ('Commissie Franken') onderkende in haar rapport 'Informatietechniek en strafrecht' (1987) de volgende beschermenswaardige belangen aan gegevens: beschikbaarheid, exclusiviteit en integriteit. Deze belangenonderscheiding kan niet worden aangevoerd als een criterium op basis waarvan we gegevens niet als zaken zouden moeten behandelen; ook voor andere zaken geldt immers dat zij beschikbaar moeten zijn, exclusief en integer.

Er bestaat een spanningsveld tussen het belang van de exclusieve beschikking en het belang van wat wel genoemd wordt de 'free flow of information'. Of, met andere woorden, een spanningsveld tussen de opvatting dat op gegevens (eigendoms)rechten kunnen rusten, ten opzichte van de gedachte dat informatie (of, liever gezegd: gegevens) publiekelijk en vrij beschikbaar dient te zijn. Op deze plaats wordt volstaan met de opmerking dat noch het interstatelijk vrije verkeer van gegevens, noch het grondrecht van vrijheid van meningsuiting en informatiegaring aan het hebben van subjectieve rechten ten aanzien van bepaalde gegevens in de weg staan. (Zie verder paragraaf 12.3)

Ook wordt wel aangevoerd dat het *karakter* van gegevens anders zou zijn dan dat van zaken: i) zaken zijn uniek, gegevens daarentegen zijn multiple beschikbaar; ii) zaken zijn een produkt van lichamelijke inspanning, gegevens komen voort uit geestelijke arbeid.

Dat alleen gegevens multiple zouden zijn, en zaken niet, lijkt een eenzijdige opvatting die met een bezoek aan de lopende band bij General Motors is kort te sluiten. Echter, een bepaalde representatie van gegevens, een bepaald exemplaar van een computerprogramma, is net zo uniek als een bepaald exemplaar van een Opel Astra.

Voorts kan een Opel Astra weliswaar als een produkt van (geautomatiseerde) lichamelijke arbeid worden bestempeld, dit neemt niet weg dat het toch vooreerst is voortgekomen uit geestelijke arbeid. Mutatis mutandis moet men stellen dat de vervaardiging van een boek toch ook gepaard gaat met lichamelijke inspanning: de data moeten worden ingevoerd en het boek moet worden gedrukt.

2.2 ‘Eigendomsbegrippen’

Van belang voor de juridische kwalificatie van de begrippen uit de vorige paragraaf is welke juridische begrippenkaders daarvoor in aanmerking komen. We kunnen verschillende juridische invalshoeken onderscheiden, waarbinnen bepaalde rechten op informatie zijn te onderkennen:

ZAKENRECHTELIJKE EIGENDOM

Het goederenrecht in het BW maakt in art. 3:1 een onderscheid tussen zaken en vermogensrechten. Zaken worden in art. 3:2 BW gedefinieerd als de voor menselijke beheersing vatbare stoffelijke objecten. De term ‘eigendom’ (art. 5.1 BW) wordt in het goederenrecht slechts in verband met zaken gebruikt. In verband met vermogensrechten spreekt men van ‘rechthebbende’.

Een zaak, gedefinieerd als een stoffelijk object, kan voorwerp van eigendom zijn. Men kan bijvoorbeeld eigenaar zijn van (een exemplaar van) een auto, een boek of van een exemplaar van een computerprogramma.

INTELLECTUELE RECHTEN

Intellectuele rechten is een met de zakenrechtelijke eigendom verwant begrip voor een vermogensrecht dat men kan hebben op een produkt van de menselijke geest. (In de visie van aanhangers van een onderscheid tussen zaken en gegevens zou dat produkt dan een immaterieel goed moeten zijn, niet zijnde vermogensrecht, maar onstoffelijk object!) Zo kan men rechthebbende zijn op het auteursrecht op een boek of een computerprogramma.

Het spreekt voor zich dat met de verkoop van een exemplaar van een boek niet het auteursrecht op het geestesprodukt in andere handen overgaat, net zo min als bij de overdracht van het auteursrecht de reeds in het verkeer gebrachte exemplaren ineens van eigenaar verwisselen. De zakenrechtelijke eigendom gedraagt zich onafhankelijk van de intellectuele rechten.

PRESTATIEBESCHERMING

Een ander begrip dat *lijkt* op eigendom is prestatiebescherming. Beschermt bijvoorbeeld het auteursrecht alleen geestesprodukten die voldoen aan een bepaalde mate van *oorspronkelijkheid*, het begrip prestatiebescherming duidt op de ontlening van een zeker recht alleen al op de *inspanning* die men zich getroost heeft, bijvoorbeeld om gegevens te verzamelen. Volgens het criterium van de Hoge Raad in het Decca-Holland Nautic arrest (HR 27 juni 1986, NJ 1987, 191, BIE 1986, 71, IER 1986, 29, Cr 1986/3):

> *dat ‘voor een (met een recht van intellectuele eigendom) vergelijkbare bescherming via het recht van de ongeoorloofde mededinging in beginsel tenminste vereist (is) dat wordt geprofiteerd van een prestatie van dien aard dat zij op één lijn valt te stellen met die welke toekenning van een dergelijk recht rechtvaardigt’*

Deze zogenoemde éénlijnsprestatie, heeft vooralsnog veel weg van een gesloten deur waarachter zich een blinde muur bevindt. (Zie voorts: Staat-Den Ouden, HR 20 november 1987, NJ 1988, 311; KNVB-NOS, HR 23 oktober 1987, NJ 1988, 310 en Elvis Presley, HR 24 februari 1989, NJ 1989, 701.)

WET PERSOONSREGISTRATIES

Tenslotte wijzen we hier nog op het bestaan van bepaalde rechten ten aanzien van gegevens de eigen persoon betreffende. In de Wet Persoonsregistraties bijvoorbeeld wordt geregistreerden een inzage- en correctierecht toegekend en soms zelfs het recht om bepaalde, niet voor het doel van de registratie van belang zijnde gegevens te verwijderen.

OVERIGE RECHTEN OP INFORMATIE

Natuurlijk zijn er nog talloze andere rechten denkbaar met betrekking tot informatie, zoals (onder omstandigheden) het recht op rectificatie, het recht van weerwoord en het recht om politieke denkbeelden te mogen ontvangen.

2.3 De juridische kwalificatie van software

Een reden voor de onduidelijkheid met betrekking tot de kwalificatie van software is gelegen in het feit dat het denken over software vooral plaats heeft gehad tegen de achtergrond van de auteursrechtelijke bescherming daarvan, waar het ‘geestesprodukt’ geldt als object van bescherming. Onjuist is het echter deze gedachtengang zodanig door te trekken naar het goederenrecht dat daar de conclusie zou zijn dat een computerprogramma derhalve onstoffelijk is.

Zoals men in dat geval over een computerprogramma spreekt als een drager (de diskette) waarop een geestesprodukt (het auteursrechtelijke ‘werk’) is vastgelegd, zo zou men ook over een Opel Astra kunnen spreken als een drager (de plaat staal) waarop een geestesprodukt (het modellenrechtelijke ‘model’) is vastgelegd. In deze zin is het echter heel ongebruikelijk om over auto’s te spreken.

Dat zaken in de zin van het goederenrecht (voor menselijke beheersing vatbare stoffelijke objecten) daarnaast kunnen worden ‘ingestraald’ vanuit een ander rechtsgebied - in dit geval het intellectuele eigendomsrecht - doet aan de goederenrechtelijke status niet af. (Zie bijvoorbeeld het Barbiepop I arrest, HR 21 februari 1992, NJ 1993, 164; BIE 1993, 65). Aannemelijk is voorts dat met het stoffelijkheidscriterium van zaken eerder is beoogd iets aan te duiden over het karakter van *rechten*, namelijk dat deze *niet* tastbaar zijn.

Een argument tegen de kwalificatie van software als zaak is de opvatting dat software beschouwd zou moeten worden als een *dienst*. Hoewel het juist kan zijn, dat de onderliggende rechtsverhouding bij het vervaardigen van

'maatwerk' software kan zijn het verrichten van diensten in het kader van een overeenkomst van opdracht (art. 7:400 BW), kan men het *resultaat* daarvan, het tot stand gekomen software-exemplaar, toch niet anders kwalificeren als een zaak, evenals dat bij het vervaardigen van een 'stoel op maat' het geval zou zijn. (Dientengevolge zou evenzeer de onderliggende rechtsverhouding er een kunnen zijn van aanneming van werk (art. 7A:1637b BW), de tot stand brenging van een bepaald werk van stoffelijke aard.) Ten overvloede: hieraan staat natuurlijk niet in de weg, dat de maker van dat werk tevens auteursrecht daarop zou kunnen doen gelden.

Een volgende reden is wat men zou kunnen noemen het 'vluchtige karakter' van software. Software is eenvoudig (en perfect) te kopiëren en evenzo eenvoudig te wissen, zonder de drager te beschadigen. Men wijzigt 'slechts' de voor het oog niet zichtbare magnetische patronen.

In een opsomming echter van auto's, boeken, muziekcassettes en software zien we slechts een toename van manipuleerbaarheid, dat wil zeggen een toename van het gemak waarmee nieuwe exemplaren vervaardigd kunnen worden. Niet relevant voor de juridische kwalificatie is de bijkomstigheid dat het muziekwerk op een voorbespeelde cassette beschadigd kan worden zonder de cassette te beschadigen en dat dit niet kan met hetzelfde muziekwerk op een compact disk. (Hier zij overigens opgemerkt dat de magnetische patronen op de cassette wel degelijk zijn 'beschadigd'.)

Voorts is wel aangevoerd dat, omdat 'kopiëren' van gegevens niet zou opleveren 'wegnemen' van een goed in de zin van art. 310 Sr (diefstal), gegevens geen goed kunnen zijn. (Let op: de term 'goed' wordt hier gehanteerd in de strafrechtelijke betekenis. In de terminologie van het BW zouden we de term 'zaak' gebruikt hebben.) De gevolgtrekking dat gegevens geen (strafrechtelijk) goed kunnen zijn, volgt niet logisch uit de redenering dat kopiëren niet zou zijn wegnemen. Daaruit kan niet méér geconcludeerd worden dan dat kopiëren niet als wegnemingshandeling zou zijn aan te merken. Of dàt overigens een juiste opvatting is, is een ander vraagstuk. Hoewel we *gewend* zijn dat bij wegnemen van goederen de oorspronkelijke bezitter het goed niet meer heeft, kan men zich afvragen of daar nu de essentie van wegnemen in ligt besloten. Of gaat het er nu juist om dat de wegnemer het goed nu (ook) heeft? Hoe dit ook zij - de *kopie* is immers wel weggenomen, evenals de exclusiviteit en een gedeelte van de informatiewaarde (zie hoofdstuk 13, Computercriminaliteit) - de beantwoording van dit vraagstuk staat los van de goederenrechtelijke status van gegevens (software).

Voor de keuze of computerprogramma's (c.q. gegevens, c.q. informatie) juridisch al dan niet als 'zaak' gekwalificeerd dienen te worden, mag het fysische karakter niet allesbepalend zijn. Binnen het recht is men immers gewoon met ficties te werken ('rechtspersonen', 'meerderjarigheid' etc.).

Indien echter het vanuit juridisch oogpunt wenselijk zou zijn om software (c.q. gegevens, c.q. informatie) *niet* als zaak aan te merken, zullen daarvoor andere argumenten moeten worden aangedragen, bijvoorbeeld dat de juridische consequenties daarvan niet wenselijk zouden zijn.

De zakenrechtelijke kwalificatie van computerprogramma's impliceert dat de daaraan verbonden rechtsgevolgen in beginsel ook van toepassing zijn op computerprogramma's. Dat betekent bijvoorbeeld dat computerprogramma's voorwerp kunnen zijn van eigendom (art. 5:1 BW), dat zij gerevindiceerd kunnen worden (art. 5:2 BW) en dat zij vatbaar zijn voor toeëigening (art. 5:4 BW), natrekking, vermenging en zaaksvorming (artt. 5:14-16 BW).

Toepassing van bijvoorbeeld de zaaksvormingsregel op computerprogramma's zou kunnen opleveren dat een programmeur *eigenaar* wordt van een door hem nieuw gevormd exemplaar, bestaande uit delen van andere computerprogramma's. Dat wil echter allerminst betekenen dat de programmeur vervolgens ook *rechthebbende* (in de zin van de Auteurswet 1912) op dit programma zou zijn. Bovendien zou, nog afgezien van de vraag of de programmeur niet reeds bij de samenstelling van het programma inbreuk heeft gemaakt op auteursrechten van de rechthebbenden op de door hem gebruikte andere programma's, de 'instraling' vanuit het auteursrecht op deze zaak met zich mede kunnen brengen, dat die rechthebbenden (auteursrechtelijk) beslag op het betreffende exemplaar zouden kunnen leggen. Al met al een systematiek zoals we die kennen voor alle zaken die tevens onderhevig zijn aan een regime van intellectuele rechten.

Is hierboven betoogd, dat een andere kwalificatie van computerprogramma's (c.q. gegevens, c.q. informatie) dan als zaak niet kan steunen op de aanwezigheid van belangen of kenmerken die vreemd zijn aan andere zaken, noch op fysische eigenschappen (het stoffelijkheidscriterium) of de aan die kwalificatie verbonden rechtsgevolgen, is het dan wellicht zo, dat de juridische praktijk daarmee niet overweg zou kunnen? Ook dat blijkt niet het geval. Volgens de opvatting van de Hoge Raad, zoals neergelegd in het elektriciteitsarrest (HR 23 mei 1921, NJ 1921, 564), waarin elektriciteit als een (strafrechtelijk) goed ('zaak' in de terminologie van het BW) werd geoordeeld, gelden de volgende criteria: overdraagbaar, reproduceerbaar, beschikbaar en economisch waardeerbaar.

Deze criteria zijn met betrekking tot computergegevens probleemloos toegepast door het Hof Arnhem (Hof Arnhem, 27 oktober 1983, NJ 1984, 80, Cr 1984/1, verduistering van computergegevens). Ondanks het feit dat dit arrest is omstreden, heeft het Hof zijn opvatting dienaangaande in 1994 nog eens bevestigd (Hof Arnhem, 31 maart 1994, Cr 1994/3).

Een van de consequenties van het zakenrechtelijk karakter van computerprogramma's is dat zij 'gewoon' verkocht kunnen worden. De praktijk is echter

anders. Het lijkt nog steeds gebruikelijk om licentie-overeenkomsten aan te gaan, waarin een gebruiksrecht op het programma wordt verleend. En dat, terwijl een koopovereenkomst evenzo goed zou voldoen maar de rechtsbetrekking bovendien zou verhelderen.

Aspecten die nadelig zijn in de praktijk van licentieverleningen is dat licenties veelal verschillend zijn van elkaar, dat er tal van beperkingen in zijn opgenomen en dat zij doorgaans niet gelezen worden. Voorts kan de vraag aan de orde komen of er sowieso wel een geldige overeenkomst tot stand is gekomen. De licentievoorwaarden die de softwareproducent beoogd 'op te leggen' aan de afnemer van het softwarepakket, en die de rechtsverhouding tussen softwareproducent en afnemer zou moeten beheersen, zijn meestal ingesloten in de verpakking van het pakket. Tussen producent en afnemer bestaat doorgaans geen rechtstreekse relatie, aangezien het pakket wordt betrokken bij de tussenhandel. Het is ten eerste dan nog maar de vraag of de overeenkomst die tussen de afnemer en de leverancier is gesloten, zich tevens uitstrekt over de in het pakket ingesloten licentievoorwaarden. Voorts is het de vraag of er sprake is van een rechtsgeldig tot stand gekomen overeenkomst tussen softwareproducent/softwareleverancier enerzijds en afnemer anderzijds, waar, in veel gevallen, de afnemer niet vooraf kennis heeft genomen van de ingesloten licentievoorwaarden. Indien deze vraag onder bepaalde omstandigheden ontkennend moet worden beantwoord, is de consequentie dat de in de 'licentie-overeenkomst' weergegeven voorwaarden in het geheel geen toepassing zullen vinden. De door de softwareproducent nagestreefde bescherming in diens bedoeling niet meer dan een gebruiksrecht te verlenen, blijkt dan een 'overkill' geworden.

De gegroeide praktijk, die erop neerkomt om zo weinig mogelijk 'uit handen te geven' is overigens wel verklaarbaar, vanuit de zorg aan de zijde van softwareproducenten voor een niet te beteugelen kopieerdrift aan de kant van afnemers. Het medicijn lijkt echter erger dan de kwaal. Daar komt nog bij, dat niet gebleken is dat de - ondoorzichtige - praktijk van licentieverleningen heeft bijgedragen aan een vermindering van het verschijnsel van onrechtmatig kopiëren.

De keuze voor een koopovereenkomst voor computerprogramma's zal hierin evenmin verandering brengen. Wel is het zo, dat betrokken partijen in een overzichtelijke rechtsverhouding tot elkaar komen te staan. Op grond van de koopovereenkomst verkrijgt de afnemer de eigendom op het betreffende exemplaar. Op grond van diens bevoegdheid als auteursrechthebbende, verleent de producent de afnemer de bevoegdheid tot het maken van een verveelvoudiging van het programma ten behoeve van het gebruik (in de huidige praktijk de installatie op diens harddisk in de computer). Denkbaar is evenwel dat deze bevoegdheid reeds voort zou vloeien uit de wet (art. 45j Auteurswet 1912). Zou de afnemer echter besluiten het pakket van de hand te

doen, dan wordt hij niet gehinderd door eventuele beperkingen zoals die thans veelal zijn opgenomen in de 'licentie-overeenkomst'. Een volgende eigendomsoverdracht ontneemt hem echter de status van 'rechtmatige gebruiker', zodat hij op dat moment de (eerder toegestane) verveelvoudiging uit zijn computer dient te verwijderen. Deze laatste bevoegdheid komt dàn immers de nieuwe eigenaar toe.

Dit - eenvoudige - systeem vloeit 'zomaar' voort uit de koopovereenkomst in combinatie met het auteursrecht. Of de vorige eigenaar de verveelvoudiging ook daadwerkelijk uit zijn computer zal verwijderen, blijft in het ongewisse. Maar dat was reeds het geval onder de huidige praktijk. Wat ook hetzelfde blijft, zijn de bevoegdheden van de auteursrechthebbende om daartegen op te treden. De 'winst' zit hem echter in de doorzichtigheid van het systeem en de zekerheid dat tussen leverancier en afnemer overeengekomen leveringsvoorwaarden in beginsel van toepassing zijn. Het staat de producent overigens vrij om bij wijze van voorlichting een op de vroegere 'licentie-overeenkomst' gelijkende bijsluiter in het pakket te doen, waarin deze de op het auteursrecht gebaseerde bevoegdheden en beperkingen ten opzichte van de afnemer nog eens uit de doeken doet. (Zie over software en koop uitgebreid Hoeren.)

2.4 Informatica en recht

Informatica en recht omvat twee deelgebieden: de rechtsinformatica, ook wel juridische informatica genoemd (paragraaf 2.4.1), en het informaticarecht, de juridische aspecten van informatietechnologie (paragraaf 2.4.2). Een met het informaticarecht verwant vakgebied is het *informatie*recht (paragraaf 2.4.3). In paragraaf 2.5 wordt aangegeven welke thema's gebruikelijk tot het informaticarecht worden gerekend, waarna in paragraaf 2.6 nog wordt stil gestaan bij de vraag of het informaticarecht wel als zelfstandige discipline kan worden beschouwd.

2.4.1 Juridische informatica

Juridische informatica richt zich op de mogelijkheden die informatica en computers bieden aan rechtspraktijk en rechtswetenschap. Dit is te vergelijken met de meer bekende medische informatica. Computers worden hier gebruikt als hulpmiddel. De volgende thema's vallen onder meer onder de juridische informatica:

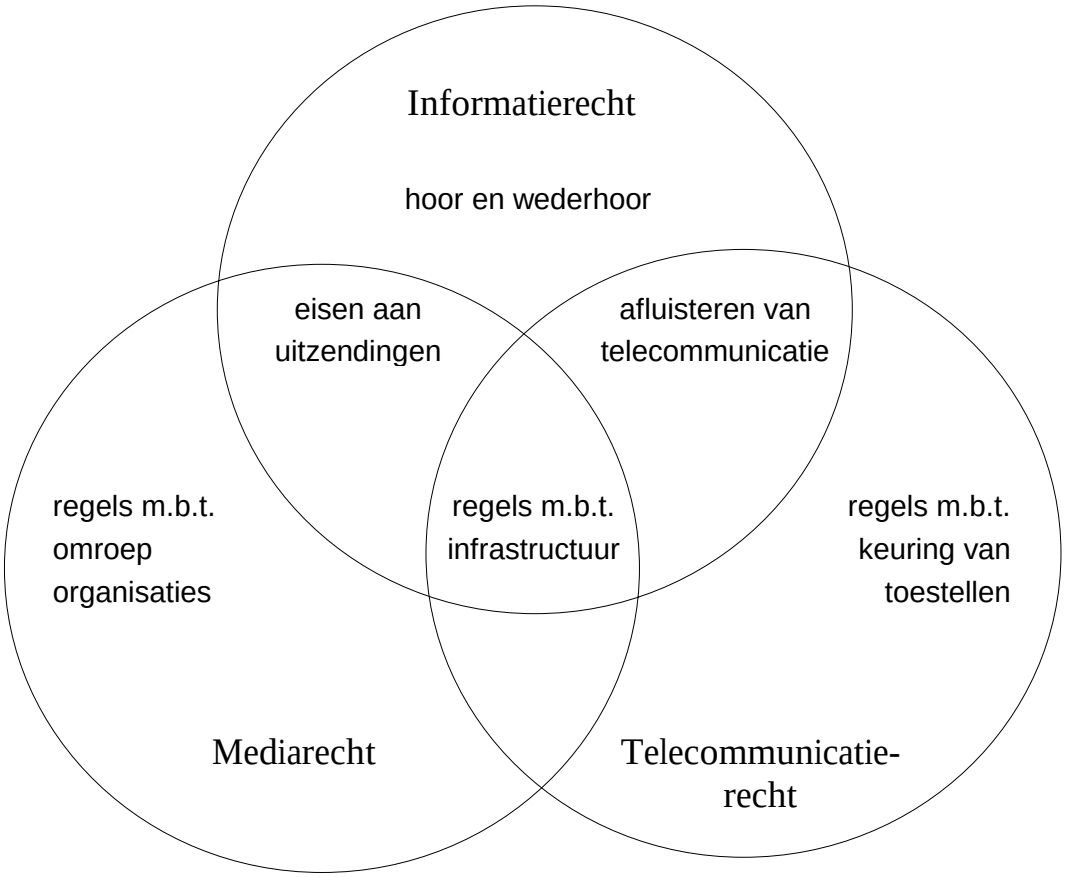
- juridische en fiscale documentatie in databanken;
- tekstverwerking (contracten, vonnissen);
- management information systems (bewaking contracten, termijnen);

- computeradviessystemen (bijvoorbeeld JURICAS);
- fiscale, kadastrale en politieregisters;
- statistische verwerking van gegevensbestanden (taalanalyse, analyse van rechterlijke uitspraken).

2.4.2 Informaticarecht

Informaticarecht is het rechtsgebied dat betrekking heeft op de toepassing van informatietechnologie. Met andere woorden, het gaat om juridisch-normatieve vraagstukken, opgeworpen door computergebruik. Tegen de term informaticarecht bestaan bezwaren. Het object van dit rechtsgebied is immers niet de wetenschap informatica, maar het object van de informatica, dat wil zeggen gegevensverwerking, automatisering e.d. Men spreekt wel van de 'praktische informatica'.

In plaats van informaticarecht worden ook wel de benamingen 'juridische aspecten van automatisering', 'computerrecht' en 'computerlaw' gehanteerd. Aan informaticarecht verwante vakgebieden zijn (auteurs-, media- en) informatierecht, mediarecht en telecommunicatierecht.



Figuur 2: Schema dat de raakvlakken van de vakgebieden illustreert.

2.4.3 Informatierecht

We bevinden ons momenteel in een ontwikkeling van een industriële maatschappij naar een informatiemaatschappij. Er komen steeds meer informatiebronnen, die bovendien steeds gemakkelijker te raadplegen zijn. Op zichzelf is informatie niet nieuw. Informatierecht is weliswaar ontstaan onder invloed van de computertechnologie, maar ziet ook op aspecten buiten de techniek.

Bing onderscheidt de volgende gebieden in 'information law':
1. Recht met betrekking tot data:
   Auteursrecht beschermt de gekozen vorm van een geestesprodukt. De Wet Persoonsregistraties geeft regels voor de opslag en verwerking van persoonsgegevens.
2. Recht met betrekking tot informatie:
   Wetgeving met betrekking tot laster, rassendiscriminatie, handels- of staatsgeheimen (de betekenis van data).
3. Recht met betrekking tot communicatiekanalen:
   Regulering van communicatiekanalen impliceert controle over de informatie. Traditionele media worden soms heel streng gecontroleerd, zoals de omroepen en soms nauwelijks, zoals de krant.

Bull heeft het over het 'recht der informatiebetrekkingen' en onderscheidt:
1. Tegengestelde belangen
   kennisneming - afscherming
   verspreiding - monopolisering
2. Informatie op personen - informatie op zaken
3. Individuele communicatie - massacommunicatie

Dommering heeft het over de 'informatie-driehoek':
1. De auteur, op het hoekpunt van de opdracht en zijn eigen interpretatie van de werkelijkheid;
2. De afgebeelde, het informatie-object;
3. De waarnemer van de gereproduceerde werkelijkheid (vroeger de rijke opdrachtgever).

De informatie-driehoek is een sociale driehoek, omdat zij beoogt juridische gezagsrelaties in een communicatieproces te beschrijven. Elementen die hierbij aan de orde komen, zijn intellectuele eigendom, telecommunicatie, media, privacy.

2.5 Informaticarecht

Informaticarecht houdt zich bezig met dat gedeelte van het informatierecht waar het de geautomatiseerde verwerking van gegevens betreft. Bovendien wordt er aandacht geschonken aan andere juridische onderwerpen waar het gebruik van computers een rol speelt, bijvoorbeeld computercriminaliteit, teleforensing etc. Vanwege de raakvlakken kunnen ook het mediarecht en het telecommunicatierecht voor een gedeelte tot het informaticarecht worden gerekend. Wat niet tot uitdrukking komt in het schema zijn de raakvlakken met verschillende andere gebieden, zoals dat van het mededingingsrecht.

Vanwege het belang dat gegevens en informatie innemen in de automatisering, zullen we vaak aandacht besteden aan deze entiteiten. Zij zijn vanzelfsprekend niet nieuw. Alleen de toegenomen manipulatie, verspreiding en beschikbaarheid door middel van computers verklaren de toegenomen belangstelling hiervoor.

Het informaticarecht omvat een groot aantal verschillende juridische thema's zoals:

- softwarebescherming;
- chipsbescherming;
- databanken (data, privacy, auteursrecht);
- overeenkomsten (licentieovereenkomsten, onderhoudsovereenkomsten);
- aansprakelijkheid (mislukte automatiseringsprojecten, produktaansprakelijkheid, aansprakelijkheid wegens het gebruik van de computer of wegens niet gebruiken van de computer);
- beroepscode informatici;
- elektronisch geld- en handelsverkeer;
- bewijsrecht (output als bewijsmiddel, bewaarverplichting);
- privacybescherming (persoonsregistraties);
- grensoverschrijdend gegevensverkeer;
- computercriminaliteit;
- ergonomische voorschriften;
- belastingrecht (invoerrechten, afschrijving);

In het algemeen gaat de aandacht uit naar een *probleemgeoriënteerde* benadering, hetgeen ook voor de hand ligt, gezien de maatschappelijke functie van recht. Recht bestaat immers niet op zichzelf, maar in interactie met de maatschappelijke vraagstukken die het beoogt te normeren en te reguleren. Pitlo: recht heeft een dienende functie.

Pas wanneer nieuwe technologische kennis geassimileerd is in de samenleving zullen sommige onderwerpen uit het informaticarecht een plaats krijgen in de traditionele rechtsgebieden (computercriminaliteit bij strafrecht, automatiseringsovereenkomsten bij verbintenissenrecht, softwarebescherming

bij handelsrecht etc.). Vanwege het door elkaar lopen van verschillende juridische disciplines gaat de voorkeur vooralsnog uit naar een integrale behandeling.

In het informaticarecht gaat het om de volgende vragen:
- Welke nieuwe vraagstukken worden opgeroepen?
- Welke rechtsgebieden zijn van toepassing? Hoe kunnen deze vraagstukken juridisch worden gekwalificeerd?
- Zijn daarbij interpretatieproblemen?
- Is bestaande wetgeving toereikend, of zijn er aanpassingen, dan wel nieuwe regels nodig? De vraag naar de wenselijkheid van nieuwe wetgeving laat zich vervolgens nog onderscheiden in:
  - Is de huidige regelgeving nog voldoende actueel ter regulering van maatschappelijke ontwikkelingen tengevolge van de informatietechnologie?
  - Dient nieuwe wetgeving tot stand te komen ter stimulering van de toepassing van informatietechnologie?

De *Europese dimensie* van het informaticarecht komt tot uiting in het grote aantal EU-richtlijnen dat specifiek met het oog op informatietechnologie wordt uitgevaardigd. Zo is er een richtlijn chipsbescherming, een richtlijn softwarebescherming, een richtlijn voor de bescherming van databanken en een richtlijn voor de bescherming van persoonsgegevens. Privacy en computercriminaliteit zijn voorts onderwerpen die ook in de belangstelling staan van de Raad van Europa en van de Organisatie voor Economische Samenwerking en Ontwikkeling. Het terrein van de telecommunicatie en dat van de omroep tenslotte worden eveneens bestreken door verschillende richtlijnen.

De grenzen van het informaticarecht zijn vaak niet scherp te trekken. Er zijn juridische kwesties die de informatica rechtstreeks raken, bijvoorbeeld de bescherming van software, er zijn verder verwijderde maatschappelijke gevolgen van automatisering, zoals de relatie tot privacybescherming, en er worden geheel nieuwe juridische vragen opgeroepen.

Een voorbeeld daarvan is *teleforensing*. Met de term ‘telematica’ (een samentrekking van telecommunicatie en informatica) wordt de integratie van telecommunicatie en computers aangeduid. Zo kennen we tegenwoordig het verschijnsel tele-arbeid, waarbij thuis wordt gewerkt en de informatie via telefoonlijnen wordt doorgegeven. Voor het burgerlijk wetboek en de sociale verzekeringen is het van belang om te weten of we in zo’n geval nog wel kunnen spreken van werknemers, ondergeschiktheid, onvervangbaarheid van de persoon etc.

Een ander voorbeeld is EDI, electronic data interchange: met behulp van computers tot stand gekomen handelstransacties. In het BW zien we dat met het oog op de geldigheidsduur daarvan een onderscheid wordt gemaakt

tussen een mondeling of schriftelijk uitgebracht aanbod. Het *elektronisch* uitgebrachte EDI-aanbod roept de vraag op naar de kwalificatie daarvan.

Er is een aantal raakvlakken tussen informaticarecht en juridische informatica. Het informaticarecht behandelt immers normatieve vraagstukken die voor een deel ook door de juridische informatica worden opgeworpen.

Het gebruik van computers door de overheid, bijvoorbeeld voor het nemen van beschikkingen, voor het opstellen van wetgeving of voor rechterlijke uitspraken, is een terrein waarop het informaticarecht en de rechtsinformatica in elkaar overgaan.

Een ander terrein is het gebruik van persoonsgegevensbestanden door verschillende overheidsinstanties en de mogelijke koppelingen daartussen.

Denkbaar is voorts dat het niet raadplegen door advocaten van recente databanken kan leiden tot een claim op grond van beroepsaansprakelijkheid. Indien daardoor (belangrijke) jurisprudentie (of andere informatie) is gemist, die eenvoudig verkrijgbaar was, zou dit verzuim zijn aan te merken als een vorm van onzorgvuldigheid.

2.6 Een zelfstandige discipline?

De vraag wordt wel eens gesteld of informaticarecht een zelfstandige juridische discipline is. Elementen die aan deze vraagstelling ten grondslag liggen:

- geen homogeen vakgebied;
- veel onderwerpen die niet met elkaar verband houden;
- geen samenhangend juridisch deelterrein;
- geen autonome begripsontwikkeling;
- speculatief.

Het vakgebied informaticarecht staat de laatste jaren in een toenemende belangstelling en lijkt zich te hebben gevestigd. Desalniettemin blijft een kritische beschouwing zinvol. Wat mogen juristen verwachten van dit vak?

Ongeacht welke beroepsuitoefening, krijgen juristen te maken met automatisering (intellectuele eigendomsvraagstukken, contracten, geschillen, criminaliteit, handelsverkeer, toepassingen). De vraagstukken uit het informaticarecht zorgen doorgaans voor een verdieping en een verrijking van de bestaande dogmatiek.

In het informaticarecht wordt kennis van automatisering samengebracht met de kennis en kunde uit de verschillende juridische disciplines. Als zodanig zou informaticarecht als een *specialisatie* kunnen worden aangemerkt. Vanwege de relevantie van technologie en automatisering in vrijwel alle maatschappelijke facetten, is informaticarecht echter vooral de *implementatie* van recht in de hedendaagse informatiemaatschappij. Bestudering van recht is in feite niet

meer zinvol mogelijk zonder bestudering van de ‘impact’ van informatietechnologie.

Informaticarecht steunt bij uitstek op technologische ontwikkelingen. Het is een zeer praktijkgeoriënteerd vakgebied. Een pragmatische benadering gaat gepaard met theorievorming. Onbekendheid met technologische ontwikkelingen heeft onduidelijkheid op juridisch terrein tot gevolg. In de volgende hoofdstukken zullen we aan de hand van een beschrijving van de belangrijkste deelgebieden nagaan hoe vanuit het recht wordt omgegaan met informatietechnologie, hier en daar voorzien van een kritische beschouwing ten aanzien van motieven, noodzaak en effectiviteit.

2.7 Jurisprudentie

HOF DEN HAAG, 4 JUNI 1992, CR 1993/6, NT R.J.J. WESTERDIJK
Het wissen, dat wil zeggen het aantasten van de gaafheid van de eenheid van de op de harde schijf respectievelijk de diskette(s) tezamen met de daarop aangebrachte en aanwezige ‘bits’ (magnetische veldjes) met als gevolg functieverlies, vormt, in de zin van de polis, in een geval als het onderhavige beschadiging van een stoffelijk goed. (Zie ook onder computercriminaliteit.)

2.8 Literatuur

- Berkvens, J.M.A., ‘Congestie op data-highways’, Kluwer, Deventer, 1991.
- Bing, J., ‘Information law: a brief introduction’, in: Journal of Media Law and Practice, 1984, pp. 134-140.
- Bull, H.P., ‘De fundamentele problemen van het informatierecht’, W.E.J. Tjeenk Willink, Zwolle, 1985.
- Computerrecht, tijdschrift voor informatica en recht, Kluwer, Deventer.
- Dommering, E.J., ‘De informatiedriehoek’, Kluwer, Deventer, 1989.
- Engelen, Th.C.J.A. van, ‘Prestatiebescherming en ongeschreven intellectuele eigendomsrechten’, (diss.), W.E.J. Tjeenk Willink, Zwolle, 1994.
- Franken, H. (voorz.), ‘Informatietechnologie en recht’, Vermande, Lelystad, 1991.
- Franken, H., H.W.K. Kaspersen en A.H. de Wild, (red.), ‘Recht en computer’, Kluwer, Deventer, 1992.
- Graaf, F. de en J.M.A. Berkvens, (red.), ‘Hoofdstukken informaticarecht’, Samsom H.D. Tjeenk Willink, Alphen aan den Rijn, 1991.
- IT & Recht, tijdschrift, Samsom Bedrijfswetenschappen.

- Klaauw-Koops, F.A.M. van der en S.F.M. Corvers, ‘Praktisch Informatica-recht voor het Hoger Beroepsonderwijs’, W.E.J. Tjeenk Willink, Zwolle, 1995.
- Kleve, P. en R.V. De Mulder, ‘De juridische status van software’, in: Nederlands Juristenblad 1989 nr. 37.
- Koers, A.W., ‘Rechtsstaat, informatisering en juridische informatologie’, in: Computerrecht 1993/5.
- Mulder, R.V. De, ‘Een model voor juridische informatica’, (diss.), Vermande, Lelystad, 1984.
- Mulder, R.V. De en C. van Noortwijk, ‘Computergebruik voor juristen’, Vermande, Lelystad, 1996.
- Nederlandse Vereniging voor Informatica en Recht, ‘10 Jaar IT en recht: verleden, heden en toekomst’, Samsom, Alphen aan den Rijn, 1996.
- Oskamp, A., ‘Het ontwikkelen van juridische expertsystemen’, (diss.), Kluwer, Deventer, 1990.
- Prins, J.E.J., ‘Overtollig recht inzake informatietechnologie’, Kluwer, Deventer, 1995
- Thole, E.P.M., ‘Software, een ‘novum’ in het vermogensrecht’, (diss.), Kluwer, Antwerpen/Deventer, 1991.
- Wees, J.G.L. van der en W.G. Renden, ‘Internet voor juristen, Kluwer, Deventer, 1995.

3 Inleiding intellectuele rechten

Een van de voor het informaticarecht belangrijke rechtsgebieden is het intellectueel eigendomsrecht. Informatiemaatschappij en intellectuele rechten staan in symbiotische relatie tot elkaar. Voor de efficiency van de produktie en distributie van informatie is de juridische inbedding in een systeem zoals dat van intellectuele rechten essentieel. Daar tegenover kan men stellen, dat het belang van en de aandacht voor het rechtsgebied van de intellectuele eigendom enorm is toegenomen onder invloed van de informatiemaatschappij.

Zo heeft de juridische bescherming van software vooral vorm gekregen binnen het auteursrecht en, in mindere mate, het octrooirecht. Ook voor andere produkten van informatietechnologie, zoals computercomponenten en databanken, wordt bescherming gevonden onder het regime van een van de intellectuele rechten. Is daartoe, in beginsel, nog vereist dat er sprake moet zijn van een intellectuele en creatieve prestatie, tegenwoordig zien we zelfs dat dit criterium ten aanzien van het object van informatietechnologie - de informatie of de data zelf - steeds minder van belang wordt gevonden. Louter op grond van de met de inspanning gepaard gaande investering, tegenover het gemak waarmee anderen daarvan kunnen profiteren, wordt voor bepaalde informatieverstrekking wel een vorm van bescherming gerechtvaardigd geacht, zelfs indien de data zelf zulk een bescherming zouden ontberen.

Met uitzondering van het juridisch regime voor chips (topografieën van halfgeleiderprodukten), waarvoor een afzonderlijke wettelijke regeling in het leven is geroepen, wijkt de bescherming van computercomponenten in principe niet af van die van andere (technische) produkten, en behoeft derhalve geen separate aandacht. Ter globale oriëntatie op de voor de bescherming van informatietechnologie belangrijkste intellectuele rechten, zullen in dit hoofdstuk de hoofdlijnen van het auteursrecht, het octrooirecht en het chipsrecht worden behandeld. In hoofdstuk vier zal het vraagstuk van de juridische bescherming van software door middel van het auteursrecht en het octrooirecht worden besproken. De juridische bescherming van databanken, en de daarin opgeslagen data, heeft vooral auteursrechtelijke aspecten, en zal worden behandeld in hoofdstuk vijf.

De rechten van intellectuele eigendom zoals neergelegd in de nationale wetgeving, worden voor een belangrijk deel supranationaal bepaald. Ten aanzien van het auteursrecht kennen we internationale verdragen, zoals de Berner Conventie (WIPO, 1886) en de Universele Auteursrecht Conventie (Unesco, 1952), beide herzien in Parijs in 1971. Naburige rechten, rechten van uitvoerende kunstenaars, van producenten van fonogrammen en van omroeporganisaties zijn onderhevig aan de Conventie van Rome (1961) en de Conventie van Genève (1971).

Zowel het verdrag van Bern als dat van Rome, wordt deels weer omsloten door de Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPs) van de World Trade Organisation (WTO). Dit verdrag - uitvloeisel van de GATT (General Agreement on Tariffs and Trade), het multilaterale verdrag inzake vergaande liberalisatie van de wereldhandel - is een zeer omvattend verdrag dat wereldwijd van grote betekenis is. TRIPs strekt zich uit over auteursrecht en naburige rechten, rechten van industriële eigendom en bescherming van know how. Het bevat, naast bepalingen van materieelrechtelijke aard, regels met betrekking tot de handhaving van intellectuele eigendom, het beschermingsniveau en geschillenbeslechting. Voor de geïndustrialiseerde landen, zoals Nederland, is TRIPs bindend geworden per 1 januari 1996.

Ook in EU-verband wordt de invloed van internationale regulering steeds groter, o.m. blijkens de EU-richtlijnen betreffende de rechtsbescherming van topografieën van halfgeleiderprodukten (87/54/EG, Pb. L24/36), betreffende de rechtsbescherming van computerprogramma's (91/250/EG, Pb. L 122/42), betreffende het verhuurrecht, het uitleenrecht en bepaalde, met het auteursrecht verwante rechten op het gebied van intellectuele eigendom (92/100/EG, Pb. L 346/61) en, recent, betreffende de rechtsbescherming van databanken (96/9/EG, Pb. L 77/20). De tendens binnen de EU, tot harmonisatie van specifieke deelgebieden van het recht van intellectuele eigendom, en de veelvuldige keuzen voor sui generis bescherming, vormen echter steeds

vaker een complicerende factor in de implementatie in de nationale wetgeving.

De intellectuele rechten worden wel onderscheiden in
- het auteursrecht en de naburige rechten (Auteurswet 1912, Wet op de naburige rechten)
  en de
- industriële rechten:
  - octrooirecht (Rijksoctrooiwet 1995, Europees Octrooiverdrag);
  - chipsrecht (Wet bescherming topografieën van halfgeleiderprodukten);
  - modellenrecht (Beneluxwet inzake tekeningen of modellen);
  - kwekersrecht (Zaaizaad- en Plantgoedwet);
  - merkenrecht (Benelux Merkenwet);
  - handelsnaamrecht (Handelsnaamwet).

Vanwege het belang voor de bescherming van software (zie hoofdstuk 4) en databanken (zie hoofdstuk 5), zullen in deze inleiding kort worden behandeld het auteursrecht (3.1) en het octrooirecht (3.2). De sui generis regeling van het chipsrecht wordt besproken in paragraaf 3.3.

3.1 Auteursrecht

Intellectuele rechten beschermen immateriële voortbrengselen van de menselijke geest. Art. 1 van de Auteurswet 1912 (Aw) bevat in feite een definitie van het auteursrecht:

> *'Het auteursrecht is het uitsluitend recht van de maker van een werk van letterkunde, wetenschap of kunst, of van diens rechtverkrijgenden, om dit openbaar te maken en te verveelvoudigen, behoudens beperkingen bij de wet gesteld'*

Het auteursrecht is een uitsluitend recht. Dat wil zeggen dat het te handhaven is tegenover een ieder (absoluut recht). Als zodanig is het recht vergelijkbaar met eigendom. Bronnen van het auteursrecht zijn o.m. de Auteurswet 1912, de Berner Conventie en de Universele Auteursrecht Conventie.

3.1.1 Werk van letterkunde, wetenschap of kunst

Het object van het auteursrecht wordt gevormd door werken van letterkunde, wetenschap en kunst. Het 'werk' begrip wordt in de wet niet nader uitgewerkt maar wel in de jurisprudentie en de literatuur. Een werk is een voortbrengsel van de menselijke geest met een eigen persoonlijk karakter. Het auteursrecht

beschermt de ‘geestelijke schepping’, die doorgaans in een stoffelijk voorwerp is belichaamd. (Anders: de voordracht of de toneeluitvoering.) Maar voor het auteursrecht is de materiële verschijningsvorm niet het essentiële object. We kunnen (in gedachte) onderscheid maken tussen het *corpus mysticum* (het immateriële geestesprodukt dat beschermd wordt) en het *corpus mechanicum* (de materiële drager, het stoffelijk exemplaar waarin het corpus mysticum tot uiting komt).

Voorbeelden van objecten van auteursrecht zijn: boeken, tijdschriften, tekeningen, foto’s en schilderijen, toneel, bankbiljetten, voordrachten en lezingen, titels van boeken, muziek, opera en computerprogramma’s. Art. 10 lid 1 Aw geeft een opsomming van een aantal categorieën werken. Deze opsomming is niet limitatief en de genoemde voorbeelden zijn niet altijd beschermd. Het artikel heeft als zodanig dan ook weinig waarde. Aan voortbrengselen van de menselijke geest worden voor bescherming door het auteursrecht twee eisen gesteld:

1. oorspronkelijkheid/originaliteit en
2. waarneembaarheid.

Voor de beoordeling of een voortbrengsel onder het auteursrechtelijk werkbegrip valt, zijn met name deze twee voorwaarden van belang. Zo staan bijvoorbeeld fotografische werken in het artikel genoemd. Er is echter een groot verschil tussen een kunstfoto en een pasfoto gemaakt in een hokje op het station. Deze laatste foto is niet oorspronkelijk en wordt dus niet beschermd. Art. 10 besluit met een voor software belangrijk element: ‘op welke wijze of in welke vorm dan ook’. (Zie hierna paragraaf 4.2.)

AD 1. OORSPRONKELIJKHEID

Oorspronkelijkheid of originaliteit kent een positieve en een negatieve dimensie. De positieve dimensie houdt in dat het werk het persoonlijk stempel draagt van de maker. Met ‘persoonlijk stempel’ wordt niet bedoeld dat men aan het werk de maker zou moeten herkennen. De Hoge Raad spreekt van een ‘eigen, persoonlijk karakter’. Evenmin dient het originaliteitsvereiste aldus te worden opgevat dat hierin sprake zou zijn van een kwalitatieve beoordeling van het creatieve of kunstzinnige gehalte van het werk. Voldoende is dat de auteur tenminste enige keuzevrijheid heeft gekend.

Niet alle werken zullen in gelijke mate een persoonlijk stempel van de maker dragen. Zo zal een auteur bij het schrijven van een roman meer keuzevrijheid hebben dan bij het schrijven van een leerboek economie voor het eindexamen VWO. Niettemin is bij beide voorbeelden eigen inbreng mogelijk. Aan de originaliteit worden geen hoge eisen gesteld. De Van Dale woordenlijst der Nederlandse taal (zonder omschrijvingen) is, als samenstel van keuzen, oorspronkelijk geacht en auteursrechtelijk beschermd (Hof Den Haag, 1 april 1993, Romme - Van Dale, NJ 1994, 58, IER 1993, 16, Cr 1993/4,

nt P.B. Hugenholtz). Zij is dus niet het eigendom van alle Nederlanders. De negatieve dimensie houdt in dat het werk niet ontleend mag zijn aan het werk van een ander.

Art. 10 lid 1 onder 1 besluit met 'alle andere geschriften'. Ook *niet-oorspronkelijke* geschriften - geschriften zonder eigen, persoonlijk karakter - worden in zekere mate beschermd. Dit heeft een historische achtergrond die teruggaat tot het 19e eeuwse 'kopijregt'. Onder het kopijrecht, dat voornamelijk ten doel had de investeringen van drukkers en uitgevers te beschermen, vielen alle gedrukte werken, zowel oorspronkelijke als niet-oorspronkelijke. De Hoge Raad heeft de omvang van de bescherming van geschriften zonder eigen, persoonlijk karakter enigszins beperkt (Radioprogramma's-arresten I, II en III). Enkele kenmerken van de niet-oorspronkelijke geschriftenbescherming, ook wel *pseudo-auteursrecht* genoemd:

- bescherming louter op grond van opschriftstelling;
- niet beperkt tot in druk verschenen geschriften (telex, handgeschreven);
- alleen bescherming tegen rechtstreekse ontlening aan het betreffende geschrift. Het onafhankelijk vervaardigen van een overeenstemmend geschrift vormt geen inbreuk op het auteursrecht;
- voor bescherming van niet-oorspronkelijke geschriften is vereist dat zij zijn openbaar gemaakt, of bestemd zijn om te worden openbaar gemaakt. Openbaarmaking buiten Nederland is in dit verband voldoende.

Zo worden de omroepprogrammagegevens van de radio- en televisie-uitzendingen beschermd, hoewel deze niet oorspronkelijk zijn. Hetzelfde geldt voor top-40 lijsten, logaritmentafels e.d. Het pseudo-auteursrecht wordt wel de hoeksteen van het publieke omroepbestel genoemd. Niet alleen zijn de omroepen voor een deel aangewezen op de opbrengst van de omroepbladen, maar vooral voor het ledental van de omroepen - op basis waarvan de zendtijd wordt verkregen - nemen de omroepbladen een belangrijke plaats in.

AD 2. WAARNEEMBAARHEID

De ratio van dit vereiste is dat het object de geest verlaten moet hebben. We onderscheiden directe waarneembaarheid, bijvoorbeeld parfum dat je kunt ruiken, een muziekconcert dat je kunt horen, en indirecte waarneembaarheid, bijvoorbeeld de muziek op een compact disk, die alleen door middel van een CD-speler te horen is, of een computerprogramma, dat door middel van het beeldscherm of een print out waarneembaar te maken is.

Het auteursrecht is niet bedoeld voor bescherming van een bepaalde stijl, methode of systeem. Of, met andere woorden: de 'plot' van een roman wordt niet beschermd, wel de door de auteur gekozen uitvoering daarvan. In het Van Gelder/Van Rijn arrest (HR 28 juni 1946, NJ 1946, 712) overwoog de Hoge Raad:

'dat alleen de vormgeving, die de uiting is van datgene, wat de maker tot zijn arbeid heeft bewogen, de bescherming van het auteursrecht geniet;'

Uiting hoeft niet te betekenen dat een werk ook door derden waarneembaar moet zijn. Een foto bijvoorbeeld ontstaat op het moment van het nemen. Het werk is vanaf dat moment, mits oorspronkelijk, auteursrechtelijk beschermd, terwijl het publiek pas na de ontwikkeling van het resultaat kan kennis nemen.

3.1.2 Maker

Onder maker wordt verstaan de 'geestelijke vader' van het werk. Meestal is de maker ook de auteursrechthebbende. Na het overlijden van de maker echter gaat het auteursrecht op het werk over op diens erfgenamen, als regel voor de duur van 70 jaar. Voorts is het auteursrecht vatbaar voor gehele of gedeeltelijke overdracht, in welk geval ook een ander dan de auteur/maker auteursrechthebbende wordt. De auteurswet bevat drie ficties waarbij anderen dan de auteur niet alleen als auteursrechthebbende, maar zelfs als maker worden bestempeld. Dit is het geval indien:

1. het werk wordt vervaardigd naar het ontwerp van een ander en onder diens leiding en toezicht (art. 6);
2. het werk in dienstverband is gemaakt (art. 7);
3. het werk voor het eerst wordt openbaar gemaakt door een rechtspersoon of een vennootschap, zonder vermelding van de naam van de auteur (art. 8).

AD 1. VERVAARDIGER

De maker van het werk behoeft niet dezelfde te zijn als degene die het werk feitelijk vervaardigt. Beslissend voor het makerschap is niet wie het materiële exemplaar vervaardigt, maar wie de geestelijke creatie heeft verricht, de 'auctor intellectualis'. Niet de drukker van het boek is de maker maar de schrijver. Evenzo is niet de uitvoerend kunstenaar de maker van een muziekwerk maar de componist, en de architect ten opzichte van de aannemer. Ook bij werken die tot stand zijn gebracht naar het ontwerp van een ander en onder diens leiding en toezicht (art. 6) is de persoon van de maker en die van de vervaardiger(s) verschillend.

AD 2. IN DIENSTVERBAND VERVAARDIGDE WERKEN

Als het werk in dienstverband is vervaardigd is de werkgever de maker van het werk, tenzij met de werknemer anders is overeengekomen. Bepalend is voorts dat de arbeidstaak (mede) bestaat uit het maken van bepaalde werken, dan wel dat het werk het gevolg is van een concrete opdracht van de werkgever die door de werknemer is aanvaard. Een netwerkbeheerder bijvoor-

beeld, die thuis in zijn vrije tijd een computerprogramma heeft geschreven, is de rechthebbende op het auteursrecht daarop. Een aan deze netwerkbeheerder op incidentele basis gegeven opdracht tot het maken van een computerprogramma kan onder omstandigheden weer wel de toepassing van art. 7 met zich mee brengen.

De term 'dienstverband' heeft een materiële betekenis, zodat de criteria voor de arbeidsovereenkomst als leidraad genomen kunnen worden. Naast loon en de onvervangbaarheid van de persoon, veronderstelt dit een *gezagsverhouding*. Art. 7 wordt dan ook niet van toepassing geoordeeld bij een overeenkomst van opdracht (art. 7:400 BW).

In het geval een organisatie een medewerker van een softwarehuis inhuurt om als projectleider de ontwikkeling van een computerprogramma tot stand te brengen, kan er een ondoorzichtige situatie ontstaan wie als maker/ auteursrechthebbende op het computerprogramma moet worden aangemerkt. Onder meer de volgende situaties zijn denkbaar:

1. De organisatie is de maker, omdat het programma door haar automatiseringsafdeling wordt gemaakt. Vervaardiging van het programma vindt weliswaar plaats onder leiding en toezicht van de projectleider, maar niet naar diens ontwerp.
2. De organisatie is de maker, omdat het programma door de automatiseringsafdeling van die organisatie wordt gemaakt. Vervaardiging van het programma vindt weliswaar plaats naar het ontwerp van de projectleider, maar in de uitvoering heeft de automatiseringsafdeling van de organisatie een grote mate van zelfstandigheid.
3. Het softwarehuis is de maker, omdat het programma onder leiding en toezicht en naar het ontwerp van de projectleider wordt gemaakt en de projectleider een arbeidsverhouding heeft met het softwarehuis.
4. De organisatie is de maker. Weliswaar wordt het programma onder leiding en toezicht en naar het ontwerp van de projectleider vervaardigd en heeft deze een formele arbeidsverhouding met het softwarehuis, de term 'dienstverband' dient materieel te worden uitgelegd, zodat de projectleider feitelijk onderhevig is aan een gezagsverhouding met de directie van de inhurende organisatie.

Uit deze opsomming blijkt wel dat het belangrijk is om zorgvuldig na te gaan hoe de feitelijke inbreng van de betrokkenen ligt. Doorgaans zal men er verstandig aan doen de gewenste rechtsgevolgen in de uitleenovereenkomst te regelen. Men dient daarbij te bedenken dat art. 7 (in dienstverband vervaardigde werken) van regelend recht is, waarvan bij overeenkomst mag worden afgeweken. Indien echter art. 6 (leiding, toezicht en ontwerp van een ander) van toepassing is, kan niet bij overeenkomst worden bepaald wie de maker zal

zijn; wel zal in de overeenkomst kunnen worden opgenomen dat de auteursrechten op het werk zullen worden overgedragen.

GEMEENSCHAPPELIJK AUTEURSRECHT

Voor de beoordeling of er sprake is van een gemeenschappelijk auteursrecht is het van belang allereerst een onderscheid te maken tussen een gemeenschappelijk werk en een combinatie van twee afzonderlijke werken. Als meerdere auteurs ieder een deel van een boek schrijven en in het voorwoord of de inhoudsopgave wordt vermeld welk deel van welke schrijver is, dan is er geen sprake van een gemeenschappelijk auteursrecht. Wordt het boek als geheel gepresenteerd en zijn de afzonderlijke bijdragen van de auteurs niet scheidbaar, dan is er sprake van één auteursrecht dat aan de auteurs gezamenlijk toekomt. Het auteursrecht kan door hen dan slechts gezamenlijk worden geëxploiteerd en bij inbreuk door derden door ieder van hen afzonderlijk worden uitgeoefend. Een film en de daarop afgestemde muziek vormen een combinatie van twee afzonderlijke werken waarbij de filmmaker het auteursrecht op de film toekomt en de componist dat op de muziek.

VERZAMELWERKEN

Art. 10 lid 2 beschermt verzamelwerken als zelfstandige werken, onverminderd het eventuele auteursrecht op de oorspronkelijke werken. Maker is volgens art. 5 lid 1 degene onder wiens leiding en toezicht het werk tot stand is gebracht, dan wel degene die de verschillende werken verzameld heeft. Voorbeelden zijn encyclopedieën, bloemlezingen, readers en databanken. Voor opname in een verzamelwerk behoeft de verzamelaar toestemming van de rechthebbende op het oorspronkelijke werk. (zie hierover hoofdstuk 5, Auteursrechtelijke aspecten van databanken en multimedia).

3.1.3 Beschermingsomvang

Auteursrecht ontstaat van rechtswege, door de enkele creatie van het werk. Voor bescherming door de Auteurswet 1912 zijn geen formaliteiten vereist. Het ‘copyright statement’ (©) heeft daarom voor Nederland vooral een psychologische functie. Auteursrecht is te onderscheiden in de volgende rechten:

1. exploitatierechten (vermogensrechtelijk deel):
2. persoonlijkheidsrechten (morele rechten / droit morale).

AD 1. EXPLOITATIERECHTEN

De exploitatierechten worden opgesomd in art. 1 Aw: *openbaarmaking* en *verveelvoudiging*.

De term openbaarmaking wordt gebruikt volgens de normale taalkundige betekenis. Openbaar maken ziet op een aantal handelingen die ten doel hebben het werk op de een of andere manier aan een publiek ter beschikking te stellen. Er is een uitbreiding van dit begrip via art. 12 naar de openbaarmaking van een verveelvoudiging van het geheel of een gedeelte van een werk.

De eerste verspreiding van een werk is een vorm van openbaarmaking waarvoor de toestemming van de rechthebbende benodigd is. De in het leesportefeuille-arrest (HR 25 januari 1952, NJ 1952, 95) vorm gekregen uitputtingsleer houdt in dat de auteursrechthebbende zich niet kan verzetten tegen verdere verspreiding van eenmaal met zijn toestemming in het verkeer gebrachte exemplaren van het werk. Het Poortvliet-arrest (HR 19 januari 1979, NJ 1979, 412) maakt duidelijk dat verdere verspreiding niet geoorloofd is indien het betreffende exemplaar in een andere hoedanigheid wordt verspreid (in casu uit een kalender uitgeknipte afbeeldingen die vervolgens opgeplakt op spaanplaat als reprodukties werden verkocht).

Voortgezette verspreiding dienen we te onderscheiden van ‘secundaire openbaarmaking’. In het Caféradio-arrest (HR 6 mei 1938, NJ 1938, 635) oordeelde de Hoge Raad dat de door de auteursrechthebbende gegeven toestemming om het werk via de radio uit te zenden, geen toestemming impliceerde aan de exploitant van een café om het werk vervolgens door middel van de radio in het openbaar ten gehore brengen.

De term verveelvoudiging wordt in de Auteurswet 1912 gebruikt in twee betekenissen: *reproduktie*, het vastleggen van het werk in een drager (op dit terrein werkt de STEMRA, de Stichting tot exploitatie van mechanische reproduktietechnieken) en *transformatie*, het vertalen, bewerken of wijzigen van de vorm van het werk.

Een transformatie kan oorspronkelijk zijn, zoals de verfilming van een boek of de vertaling van een roman. Op zo’n verfilming of vertaling rusten dan een ‘dubbel’ auteursrecht: één van de vertaler en één van de auteur van het vertaalde werk. Voor de exploitatie van de vertaling behoeft de vertaler derhalve toestemming van de auteursrechthebbende op het oorspronkelijke werk. Soms is een transformatie niet origineel, zoals het omzetten van een muziekstuk in een andere toonaard.

AD 2. PERSOONLIJKHEIDSRECHTEN

De rechtsgrond voor de persoonlijkheidsrechten kan gevonden worden in de erkenning van de persoonlijke band tussen de maker en zijn geestelijke schepping. De positie die deze rechten innemen in de wetgeving is heel verschillend. In Frankrijk staan ze vooraan in de wetgeving, in Engeland en Amerika is er niets geregeld en in Nederland staan regels soms verspreid over

diverse artikelen in de Auteurswet 1912 (art. 2 lid 3; art. 9, art. 25 en art. 45*e*). Het gaat daarbij voornamelijk om de volgende aanspraken:

- droit de divulgation:
  recht om te beslissen of een nog niet eerder geopenbaard werk al dan niet in de openbaarheid wordt gebracht, bijvoorbeeld in het geval van beslag of faillissement;
- droit à la paternité:
  recht om het 'vaderschap' van het werk te eisen;
- droit au respect:
  bescherming tegen de aantasting of wijziging van het werk;
- droit de repentir:
  recht tot het aanbrengen van wijzigingen of tot het terughalen uit de openbaarheid.

Persoonlijkheidsrechten zijn niet overdraagbaar. Evenmin zijn zij vatbaar voor beslag. Afstand van deze rechten is beperkt mogelijk. Persoonlijkheidsrechten vererven niet. De maker kan evenwel iemand aanwijzen om na zijn dood de in art. 25 erkende belangen te behartigen.

3.1.4 Rechtverkrijgenden

Men kan recht verkrijgen door erfopvolging of overdracht. Voor overdracht is een (authentieke of onderhandse) akte vereist. Er kan sprake zijn van gehele of gedeeltelijke overdracht.

Overdracht is niet hetzelfde als licentie. 'Licentia' betekent vergunning. Door middel van een auteurslicentie worden aan een derde, al dan niet tegen vergoeding en/of andere voorwaarden, een of meerdere bevoegdheden die uit het auteursrecht voortvloeien, toegekend.

De licentiehouder is niet de auteursrechthebbende. Op grond van art. 27a lid 2 kan een licentiehouder, mits hij deze bevoegdheid van de auteursrechthebbende heeft verkregen, zelfstandig een vordering instellen indien inbreuk wordt gemaakt op zijn licentie.

Licenties kennen veelal tal van beperkingen, zoals:

- vertalen (= verveelvoudigen) van een roman uitsluitend in de overeengekomen taal;
- uitgeven (= openbaar maken) van een roman in een bepaalde oplage;
- beperkingen in verspreidingsgebied, duur en/of frequentie.

Licentie-overeenkomsten komen we veel tegen in de automatiseringsbranche. Een licentie kan exclusief of niet-exclusief worden verleend en overdraagbaar of niet-overdraagbaar. De licentievergoeding kan bestaan uit een bedrag

ineens, uit een deel van de opbrengst of uit een vergoeding per periode. De licentieverlening is vormvrij.

Een zogenoemde 'wettelijke licentie' bevat de Auteurswet 1912 in art. 45j, waarin de rechtmatige verkrijger van een exemplaar van een computerprogramma het recht wordt toegekend het werk te verveelvoudigen in het kader van het met dat werk beoogde gebruik, het laden, het in beeld brengen of het verbeteren van fouten. Dit verveelvoudigingsrecht kan niet bij overeenkomst worden verboden.

3.1.5 Beperkingen van het auteursrecht

Auteursrechten kunnen aan verschillende beperkingen onderhevig zijn, zoals:

- tijdelijke duur van het auteursrecht (artt. 37-42). In beginsel vervalt het recht 70 jaar na de dood van de maker;
- werken waarop geen auteursrecht rust: wetten en vonnissen (art. 11);
- de inhoud van het auteursrecht kan zijn afgebakend (bijvoorbeeld art. 12.3);
- bevoegdheden van derden, bijvoorbeeld om te kopiëren voor eigen oefening, studie of gebruik (art. 16b);
- uitputtingsleer ten aanzien van verdere verspreiding van een werk;
- uitputtingsleer ten aanzien van openbaarmaking en verveelvoudiging van de afbeelding van een verpakt produkt ten behoeve van de verhandeling daarvan (Dior-Evora arrest, HR 20 november 1995, IER 1995/41);
- persoonlijkheidsrechten zijn niet overdraagbaar.

3.2 Octrooirecht

Octrooirecht (of 'patent') is het recht dat een uitvinder kan verkrijgen op een uitvinding. Evenals auteursrecht is octrooirecht een uitsluitend recht en dus te handhaven tegenover een ieder.

Aan het bestaan van octrooirecht liggen twee gedachten ten grondslag. De eerste steunt op een billijkheidsargument, het belonen van de uitvinder voor de verrijking van de samenleving met zijn uitvinding. De tweede gedachte steunt op een doelmatigheidsargument: octrooiverlening zou zowel het doen uitvinden als het publiceren daarvan stimuleren.

Een octrooi-aanvraag moet aan een aantal materiële en formele eisen voldoen. Hieronder worden kort enkele materiële eisen besproken.

3.2.1 Uitvinding

Vatbaar voor octrooi zijn ingevolge art. 2 lid 1 Rijksoctrooiwet 1995 (ROW) uitvindingen die nieuw zijn, op uitvinderswerkzaamheid berusten en toegepast kunnen worden op het gebied van de nijverheid.

Niet als uitvinding in de zin van art. 2 lid 1 worden o.m. beschouwd wiskundige methoden, presentaties van gegevens en computerprogramma's (art. 2 lid 2), alleen voor zover het betreft de genoemde onderwerpen of werkzaamheden *als zodanig* (art. 2 lid 3). Op grond van dit laatste criterium is een computerprogramma, gezien als een abstracte presentatie van een oplossing van een probleem, niet vatbaar voor octrooiering. Wil een computerprogramma voor octrooiverlening in aanmerking komen, dan dient het programma concreet te zijn vorm gegeven in machine leesbare code en te zijn vastgelegd in een door een computer te verwerken medium (e.e.a. onverlet de overige vereisten). Volgens de Memorie van Toelichting kan in principe octrooi worden verleend voor inrichtingen en werkwijzen waarbij computerprogramma's worden toegepast. Hiermee wordt aansluiting gezocht bij de thans geldende rechtsontwikkeling, zoals vorm gekregen in de jurisprudentie van de Octrooiraad (zie paragraaf 4.4 hierna).

Planten- of dierenrassen, alsmede uitvindingen waarvan de openbaarmaking of toepassing in strijd zou zijn met de openbare orde of goede zeden zijn niet vatbaar voor octrooi (art 3).

Een uitvinding kan zijn een voortbrengsel of een werkwijze, welk verschil van belang is voor de omvang en de wijze van bescherming die het octrooi biedt, neergelegd in art. 53 ROW. Men spreekt van een voortbrengsel als aanwending van natuurkrachten leidt tot een nieuw produkt; een lichamelijke zaak met tot dan toe onbekende eigenschappen.

De Hoge Raad (Hr 20 januari 1950, NJ 1950, 274) heeft bepaald dat sprake is van een werkwijze in het geval van een menselijk handelen, waardoor enige verandering in de natuur wordt gebracht. Dit betekent niet dat daarbij geen gebruik mag worden gemaakt van machines. Evenmin hoeft de werkwijze te leiden tot een nieuw voortbrengsel.

NIEUW

Volgens art. 4 lid 1 ROW wordt een uitvinding als nieuw beschouwd indien zij geen deel uitmaakt van de stand van de techniek. Wat moet worden verstaan onder de stand van de techniek is te lezen in lid 2 t/m 5 van hetzelfde artikel.

RESULTAAT VAN UITVINDERSWERKZAAMHEID

Een uitvinding wordt als het resultaat van uitvinderswerkzaamheid aangemerkt, indien zij voor een deskundige niet op een voor de hand liggende wijze voortvloeit uit de stand van de techniek (art. 6).

De Hoge Raad heeft in het suikerrietplantage-arrest (HR 5 december 1930, NJ 1931, 270) destijds 'uitkomst' gedefinieerd als 'het praktisch resultaat dat bereikt wordt doordat de nieuwe gedachte waarom het bij de uitvinding gaat tot werkelijkheid wordt gemaakt'. Er moet sprake zijn van een bruikbaar produkt of effect; de uitvinding moet werken, moet nuttig zijn.

TOEPASSING OP HET GEBIED VAN DE NIJVERHEID

Een uitvinding wordt als vatbaar voor toepassing op het gebied van de nijverheid aangemerkt, indien het onderwerp daarvan kan worden vervaardigd of toegepast op enig gebied van de nijverheid, de landbouw daaronder begrepen (art. 7).

Het begrip 'nijverheid' wordt ruim geïnterpreteerd. De Hoge Raad heeft bijvoorbeeld octrooieerbaar geacht 'de werkwijze strekkende tot het teweegbrengen van vormverandering van het menselijk haar' (HR 28 juni 1957, NJ 1958, 457).

3.2.2 Uitvinder

Als uitvinder, en uit dien hoofde als degene die aanspraak heeft op het octrooi, wordt de (eerste) aanvrager beschouwd.

Als de uitvinding in dienstverband is gedaan kan de werkgever aanspraak maken op octrooi. Dit is echter alleen mogelijk als de aard van de dienstbetrekking met zich meebrengt dat de uitvinder zijn bijzondere kennis aanwendt tot het doen van uitvindingen van de soort waarop de aanvraag betrekking heeft (art. 12 lid 1). Wel heeft de uitvinder in dergelijke gevallen het recht om als uitvinder te worden vermeld (art. 14).

Is de uitvinding gedaan door verscheidene personen, die volgens afspraak tezamen hebben gewerkt, dan hebben zij gezamenlijk aanspraak op octrooi (art. 13).

3.2.3 Beschermingsomvang

Anders dan bij auteursrecht, moet men om een octrooi te verkrijgen, te behouden en/of te handhaven een aantal formaliteiten afhandelen. Voor octrooiverlening is vereist dat de aanvraag in het octrooiregister wordt ingeschreven (art. 33 lid 1 ROW). Voorafgaand aan de octrooiverlening, kan de aanvrager het Bureau voor de industriële eigendom verzoeken een onderzoek

te doen naar de stand van de techniek met betrekking tot het onderwerp van de octrooiaanvrage (art. 32 lid 1). Hoewel niet nodig voor de verlening van een octrooi., is het onderzoek wel vereist voor de handhaving van het octrooi. Zonder een dergelijk onderzoek is de houder van het octrooi niet ontvankelijk in zijn rechtsvordering (art. 70 lid 2).

In de zogenoemde octrooiconclusies staat beschreven wat de rechten zijn van de houder van het octrooi. Aan de hand daarvan kan men bepalen welke gedragingen de houder kan verbieden. De tekst van deze conclusies wordt echter niet altijd letterlijk genomen. Men gaat veelal op zoek naar het 'wezen van de uitvinding' om te kunnen bepalen of er sprake is van een te verbieden handeling.

De houder van een voortbrengsel-octrooi heeft het uitsluitend recht het voortbrengsel in of voor zijn bedrijf te vervaardigen, te gebruiken, in het verkeer te brengen of verder te verhandelen. Een werkwijze-octrooi geeft de octrooihouder het recht de werkwijze in of voor zijn bedrijf toe te passen, of het rechtstreeks tengevolge daarvan verkregen voortbrengsel in of voor zijn bedrijf te gebruiken, in het verkeer te brengen of te verhandelen (art. 53).

3.2.4 Rechtverkrijgenden

Octrooi, of de aanspraak op octrooi, kan worden overgedragen en is vatbaar voor verpanding en beslag. Overdracht van octrooi, alsmede van het recht voortvloeiende uit een octrooiaanvraag, geschiedt bij een akte. In deze akte verklaart de rechthebbende dat hij zijn recht overdraagt en de ontvanger dat hij het aanneemt. De akte moet bovendien in het octrooiregister worden ingeschreven. Is dit laatste niet gebeurd, dan kan op de overgang ten opzichte van derden geen beroep worden gedaan.

Ook pandrecht wordt gevestigd door middel van een akte en inschrijving in de daartoe bestemde registers van het Bureau. Ook het proces-verbaal van inbeslagname moet worden ingeschreven. Nadien op het octrooi gevestigde rechten kunnen dan niet meer tegen de inbeslagnemer worden ingeroepen.

3.2.5 Beperkingen van het octrooirecht

Enkele beperkingen aan octrooirecht zijn:

- territoriale werking.
  Nederlandse octrooien gelden alleen binnen het Koninkrijk (Nederland, de Antillen en Aruba). Voor ons land verleende Europese octrooien gelden alleen in Nederland.

- chronologische werking.
  Het octrooi blijft van kracht tot het verstrijken van een termijn van zes jaren indien met betrekking tot het onderwerp geen onderzoek naar de stand der techniek is uitgevoerd, respectievelijk twintig jaren indien het onderzoek wel heeft plaats gevonden, te rekenen van de dag van indiening van de aanvraag die tot het octrooi heeft geleid (art. 33 lid 5, c.q. 36 lid 5).
- functionele beperking.
  De octrooihouder kan slechts bedrijfsmatige handelingen verbieden.
- systeem van dwanglicenties
  De Minister van Economische Zaken kan, indien het algemeen belang dit naar zijn oordeel vordert, onder een octrooi een licentie aan een door hem aangewezen persoon verlenen (art. 57).

3.3 Chipsrecht

Met ‘chips’ worden bedoeld: geïntegreerde schakelingen (IC’s of integrated circuits). Een chip is opgebouwd uit dunne ‘plakjes’ geleidend materiaal, waarop het patroon van schakelingen (functioneel vergelijkbaar met printplaten met transistors, weerstanden, dioden en andere elektrische componenten) is aangebracht. Dit tweedimensionale patroon wordt ook wel masker genoemd. Object van bescherming voor het chipsrecht is de topografie van de chip, dat wil zeggen de driedimensionale opbouw van de chip, de opeenstapeling van de verschillende maskers. De in de Nederlandse wet gehanteerde benaming voor chip is ‘halfgeleiderprodukt’. De laatste jaren is het aantal schakelingen dat in een IC kan worden verwerkt steeds groter geworden. Men spreekt wel van VLSI (Very Large Scale Integration). Chips worden tegenwoordig toegepast in allerlei elektronische apparaten; ze worden gebruikt als microprocessors (rekenchips) en geheugenchips.

In de Verenigde Staten is in 1984 de Semiconductor Chip Protection Act ingevoerd (SCPA). Deze wet biedt een sui generis bescherming voor chips en niet, zoals destijds in Nederland wel is voorgesteld, een bescherming onder auteurs- of octrooirecht. De bescherming strekt zich uit tot de maskers, indien en voor zover er chips mee zijn gemaakt en tot de chips die daarmee zijn gemaakt. De bescherming vóór het masker-stadium is niet federaal geregeld, maar wel toegestaan. Ook wetgeving in het kader van bescherming van bedrijfsgeheimen is hier van belang.

Een belangrijke reden voor de VS om chips buiten het bereik van het auteursrecht te brengen, is geweest dat internationale auteursrechtverdragen (de Berner Conventie en de Universele Auteursrecht Conventie bijvoorbeeld) het zogenoemde assimilatiebeginsel hanteren (gelijke bescherming aan ingezetenen en aan niet-ingezetenen). Teneinde het namaken van chips in

sommige landen in met name Zuidoost Azië effectiever te kunnen bestrijden, en zodoende ter bescherming van de eigen chipsindustrie, heeft de Amerikaanse overheid in de SCPA gekozen voor het reciprociteitsbeginsel (slechts bescherming aan niet-ingezetenen indien in het land van herkomst gelijksoortige bescherming wordt geboden aan chips van Amerikaanse oorsprong). Dit heeft in veel landen een hausse aan (met de Amerikaanse wet vergelijkbare) chipswetgeving teweeg gebracht. In de EU is daartoe in 1986 een richtlijn verschenen (87/54/EG, Pb. L24/36),

3.3.1 Topografie

De Nederlandse chipswet, de Wet bescherming van oorspronkelijke topografieën van halfgeleiderprodukten, is 7 november 1987 in werking getreden en is gebaseerd op de EU-richtlijn chipsbescherming, in navolging van de SCPA. In de artt. 1 a en b worden de begrippen halfgeleiderprodukt en topografie nader omschreven. Ingevolge art. 2 heeft de maker van een oorspronkelijke topografie van een halfgeleiderprodukt een uitsluitend recht op deze topografie.

Niet door de chipswet beschermd worden in de topografie belichaamde concepten, processen, systemen, technieken of gecodeerde informatie. Is bijvoorbeeld een computerprogramma in de chip vastgelegd, dan is nog steeds slechts de topografie van de chip beschermd onder de chipswet. Dit neemt niet weg dat het computerprogramma beschermd kan zijn door het auteursrecht.

Net als auteursrecht en octrooirecht is ook chipsrecht een uitsluitend recht. Het criterium voor bescherming onder de chipswet is dat de topografie ‘oorspronkelijk’ moet zijn.

3.3.2 Rechthebbende

De rechthebbende op de topografie is de maker daarvan. Is de arbeid in dienst van een ander verricht, dan is de werkgever de maker, tenzij anders is overeengekomen (art. 3).

In de situatie dat een chip nog niet elders in de wereld is geëxploiteerd, komt ingevolge art. 4 het recht toe aan degene die de chip, met toestemming van de maker, voor het eerst binnen de EU exploiteert.

3.3.3 Beschermingsomvang

Evenals bij auteursrecht ontstaat recht op een topografie door de schepping daarvan. Om bescherming door het chipsrecht ten opzichte van derden te kunnen inroepen, is echter een depot vereist (art. 5 lid 2). Dit depotvereiste is wel aangewezen als de oorzaak voor het geringe aantal depots in Nederland.

Inmiddels is bij wetswijziging van 3 oktober 1991 vastgesteld dat derden naast de inzage geen recht meer hebben op afschriften van de op de inschrijving betrekking hebbende stukken. Bovendien kan de deposant aangeven welke delen van bedrijfsgeheimen bevatten, en niet ter kennis van derden kunnen worden gebracht (art. 8 lid 2).

Het uitsluitende recht op een topografie houdt volgens art. 5 lid 1 in de bevoegdheid
a) om de topografie te verveelvoudigen,
b) een halfgeleiderprodukt te vervaardigen waarin de topografie is vervat en
c) exemplaren van de topografie of van het halfgeleiderprodukt te exploiteren.

3.3.4 Beperkingen van het chipsrecht

Het recht eindigt 10 jaar na depot, dan wel na eerste exploitatie (art. 13 lid 1). De ontwikkelaar wordt dan geacht zijn kosten te hebben terugverdiend. Is een topografie of een halfgeleiderprodukt eenmaal met zijn toestemming in het verkeer gebracht, dan is daarmee het exploitatierecht van de rechthebbende ten aanzien van dat exemplaar uitgeput. Voorts kent de chipswet een regeling ter bescherming van de verkrijger te goeder trouw. Art. 15 lid 1 tenslotte bepaalt dat verveelvoudigingen voor onderwijsdoeleinden of voor analyses van de chip niet als inbreuken op het recht beschouwd kunnen worden. ‘Reverse engineering’ is in de chipswet, evenals in het octrooirecht, toegestaan.

3.4 Literatuur

- Cohen Jehoram, H., ‘Auteursrecht in TRIPs’, in: Informatierecht/AMI 1995/7.
- Dorhout Mees, T.J., ‘Nederlands handels- en faillissementsrecht, deel II, Industriële eigendom en mededingingsrecht’, Gouda Quint, Arnhem, 1989.
- Frensel, G., Chipsbescherming, W.E.J. Tjeenk Willink, Zwolle, 1988.
- Gerbrandy, S., ‘Kort commentaar op de Auteurswet 1912’, Arnhem, 1988.

- Lingen, N. van, ‘Auteursrecht in hoofdlijnen’, Samsom H.D. Tjeenk Willink, Alphen aan den Rijn, 1990.
- Oven, A. van, ‘Handelsrecht/mededingingsrecht’, W.E.J. Tjeenk Willink, Zwolle, 1991.
- Spoor, J.H. en D.W.F. Verkade, ‘Auteursrecht’, Kluwer, Deventer, 1993.

4 Juridische bescherming van software

Het ontwikkelen van computerprogramma's vereist aanzienlijke investeringen. Als zodanig vertegenwoordigt het eindprodukt voor de software-ontwikkelaar een vermogensobject van belang. Het vervaardigen van nieuwe exemplaren op basis van reeds tot stand gekomen produkten is echter uitermate eenvoudig en vraagt een te verwaarlozen investering. Zo kan simpelweg in een gebruiksomgeving al een nieuw exemplaar worden gemaakt, door de computer de magnetische patronen op de programmadiskette te laten aftasten en vervolgens de magnetische patronen op een willekeurig andere diskette dienovereenkomstig te laten rangschikken. Dit wordt wel het 'kopiëren van programma's' genoemd, tegen welke terminologie geen bezwaar bestaat, zolang we ons maar realiseren dat met de term 'kopiëren' i.c. niets anders wordt bedoeld dan 'fabriceren', vervaardigen.

Voorts is het mogelijk door het wijzigen van slechts enkele programmaregels de beeldschermpresentatie dusdanig te veranderen dat het lijkt alsof er sprake is van een volledig ander programma. Hoewel deze activiteit meer kennis van zaken vereist en meer tijd kost dan in het vorige voorbeeld, spreken we nog steeds van slechts een fractie van de oorspronkelijke inspanning. Dit maakt het voor software-ontwikkelaars niet eenvoudig de geïnvesteerde tijd, kennis en mankracht terug te verdienen en verder te exploiteren.

Volgens schattingen van BSA (Business Software Alliance, een samenwerkingsverband van enkele grote softwareproducenten met als doelstelling de bestrijding van softwarepiraterij) beloopt het omzetverlies in Nederland vanwege het kopiëren van software jaarlijks tientallen miljoenen guldens. Het bedrag is moeilijk bepaalbaar, onder meer omdat niet in alle gevallen men anders ook daadwerkelijk tot aanschaf zou zijn overgegaan. Wel is duidelijk dat in Nederland ten opzichte van de ons omringende landen en met name ten opzichte van de VS gesproken kan worden van een lage kopieermoraal. Naast het kopiëren voor eigen gebruik (dat zowel geschiedt binnen organisaties als door particulieren) onderscheiden we nog tussen piraterij, het botweg kopiëren en bedrijfsmatig verhandelen, en plagiaat, het voortborduren op bestaande programma's. De juridische benadering van de beschermingsproblematiek verloopt via twee, elkaar niet uitsluitende, methodieken:
1. Voortborduren op het huidige recht;
2. Uitgaan van de behoeften aan bescherming.

4.1 Beschermingsmogelijkheden

De vraag naar de juridische bescherming van software is in het licht van het voorafgaande op te vatten als de vraag naar investeringsbescherming en eventuele renderende aanwending daarvan. Juridische mogelijkheden vormen daar een onderdeel van. Daarnaast staan de software-ondernemer nog technische, organisatorische en commerciële beschermingsmogelijkheden ter beschikking.

TECHNISCHE BESCHERMINGSMOGELIJKHEDEN

Het meest effectief ter voorkoming van het kopiëren van software is wel het aanbrengen van technische voorzieningen. Hierdoor kan het kopiëren van software enigszins aan banden worden gelegd, aangezien dan tenminste over enige computerkennis en speciale hulpmiddelen beschikt moet worden. Een nadeel hiervan kan zijn dat ook in beginsel toelaatbare handelingen - zoals het maken van reservekopieën - wordt bemoeilijkt.

ORGANISATORISCHE BESCHERMINGSMOGELIJKHEDEN

Hiermee wordt gedoeld op organisatorische en veiligheidsmaatregelen binnen de eigen organisatie, ten opzichte van werknemers, afnemers en derden, ter bescherming van bijvoorbeeld de toegang tot programmatuur en meer algemeen tot de daarin vervatte kennis.

COMMERCIËLE BESCHERMINGSMOGELIJKHEDEN

Onder commerciële beschermingsmogelijkheden wordt bijvoorbeeld verstaan het meer aantrekkelijk maken van het betrekken van software bij de leveran-

cier, door de dienstverlening te verhogen. Voorbeelden daarvan zijn uitgebreide - en duidelijker - handleidingen, opleidingen en invoeringsbegeleiding. Voorts kan het de gebruiker aantrekkelijk gemaakt worden zich te laten registreren, omdat men dan geïnformeerd wordt over nieuwe versies van de programmatuur (updates), deze goedkoper kan worden verkregen en ingeval van problemen een beroep mag worden gedaan op de (telefonische) ondersteuning van de leverancier (helpdesk).

JURIDISCHE BESCHERMINGSMOGELIJKHEDEN

Als belangrijkste juridische beschermingsmogelijkheden voor software worden wel onderscheiden:

- Intellectuele rechten, met name:
  - auteursrecht,
  - octrooirecht,
  - merkenrecht;
  - handelsnaamrecht.
- Onrechtmatige daadsrecht, met name de leerstukken van de:
  - slaafse nabootsing;
  - prestatiebescherming.
- Contractenrecht, in de relatie met:
  - afnemers,
  - distributeurs en dealers, en
  - werknemers.
- Strafrecht:
  Naast de strafrechtelijke bepalingen in bijzondere wetten, met name die van de Auteurswet 1912 (art. 31 e.v.), kunnen ook bepalingen uit het Wetboek van Strafrecht van toepassing zijn, zoals schending van bedrijfsgeheimen (art. 273 Sr), diefstal (art. 310 Sr) en verduistering (art. 321 Sr).

Na een inleiding over de ontwikkelingsstadia en verschijningsvormen van software (4.2) zullen in dit hoofdstuk de auteursrechtelijke (4.3) en de octrooirechtelijke bescherming van software (4.4) worden besproken.

4.2 De ontwikkeling van software: stadia en verschijningsvormen

Voor een beter begrip van de problematiek van de juridische bescherming van software is het nuttig om na te gaan hoe de ontwikkeling van een computerprogramma tot stand komt. De hieronder weergegeven methode is ontleend aan SDM II, system development methodology, doch de verschillende varianten van ontwikkelingsmethoden kennen ongeveer dezelfde fasen:

- basisontwerp (of functioneel ontwerp);
- detailontwerp (of technisch ontwerp);

- programmeren;
- testen;
- implementeren.

De programmeerfase bestaat uit:
- flow chart (stroomdiagram);
- algoritme;
- sourcecode (broncode);
- objectcode (machinecode).

Op basis van een probleemstelling, bijvoorbeeld voorraadbeheer en logistiek in een handelsonderneming, wordt een informatiemodel opgezet: wie dient op welk moment over welke informatie te kunnen beschikken. Het functioneel ontwerp is een beschrijving van de hoedanigheid van het programma in termen van functionaliteit: welke functies zijn nodig om het programma de gewenste taken te laten uitvoeren. Uit het functioneel ontwerp volgt een technisch ontwerp: het opstellen van de technische programmaspecificaties, zoals de bestandsstructuur. Hoewel de fasen in dit overzicht strikt gescheiden zijn weergegeven, is er in de praktijk sprake van een zekere overlap.

Hetzelfde kan gezegd worden over de programmeerfase. Alvorens tot het programmeren over te gaan, zal de programmeur het detailontwerp van de analist logisch willen ordenen en schematiseren in een stroomdiagram. Vervolgens worden voor de verschillende onderdelen van het ontwerp algoritmen opgesteld die stapsgewijs uitdrukken op welke wijze de probleemstellingen worden opgelost. Een algoritme is een stapsgewijze oplossing van een probleem, bijvoorbeeld de stapsgewijze weergave van de manier waarop een willekeurig gegevensbestand alfabetisch kan worden gerangschikt. Computers kunnen deze instructies uitvoeren indien zij zijn weergegeven in binaire vorm, in binaire code, doorgaans nullen en enen, ofwel geen stroom en wel stroom. De vorm waarin de gebruiker het programma ter beschikking krijgt is in deze binaire code, die ook wel objectcode, machinecode of executable code wordt genoemd (het object is de machine). Het vastleggen van deze instructies rechtstreeks in ‘machinetaal’ is echter een lastige opgave. Men kan zich voorstellen dat een aaneengesloten reeks van nullen en enen nu niet bepaald verhelderend werkt voor de programmeur om inzicht te behouden op welke plaats in het programma hij precies bezig is. Daarom zijn er programmeertalen ontwikkeld op een hoger niveau dan machinetaal, talen die meer aansluiten bij menselijk taalgebruik. De syntax, de regels die ten grondslag liggen aan de structuur van een taal, is strikt geformuleerd. De instructies van een computerprogramma dat in een hogere programmeertaal is geschreven, moeten dan uiteraard nog wel worden omgezet in machinetaal. Dit omzettingsproces, dat compileren wordt genoemd, geschiedt met behulp van een daarvoor geschreven computerprogramma, het zogenoemde compileer-

programma. Voorbeelden van hogere programmeertalen zijn COBOL, FORTRAN, ALGOL, PASCAL en C. Er zijn dus ook PASCAL-compilers, C-compilers enz. Een ander voordeel van het schrijven in een hogere programmeertaal is dat veel zogenaamde 'subroutines' (bijvoorbeeld de hier genoemde sorteerroutine) niet meer telkens opnieuw geprogrammeerd behoeven te worden. Dergelijke standaardroutines zijn reeds opgenomen in het compileerprogramma en worden tijdens het compileerproces 'meegekopieerd'.

Een vraag die in dit verband van belang is, is wanneer we nu over een computerprogramma kunnen spreken. Het spreekt voor zich dat het programma in de hogere programmeertaal (de sourcecode, of source) beschouwd kan worden als een representatie van het 'geestesprodukt', het 'werk' in de zin van het auteursrecht. Hetzelfde geldt (inmiddels) ook voor de vorm waarin de gebruiker het programma ontvangt, de binaire machinecode of object code. 'Inmiddels', omdat aanvankelijk wel werd beweerd dat het omzettingsproces zonder enige menselijke tussenkomst geschiedt, zodat er geen sprake zou zijn van een 'geestesprodukt'. Vanuit auteursrechtelijke optiek is deze opvatting onjuist. Onder geestesprodukt dienen we immers te verstaan het corpus mysticum, de abstracte notie van het werk, welke evenzeer tot uitdrukking wordt gebracht in machinecode. Lastiger wordt deze vraag met betrekking tot flow charts en algoritmen. Terecht kan men zich afvragen in hoeverre een flow chart en een algoritme (of een verzameling algoritmen) op eenduidige wijze dit corpus mysticum representeren. Dit zal sterk afhankelijk zijn van de mate van gedetailleerdheid. Dezelfde argumenten gelden voor het functioneel en technisch ontwerp. (De vraag of functioneel ontwerp, technisch ontwerp, flow chart en/of algoritmen (soms) beschouwd kunnen worden als representatie van het werk, en dientengevolge als verschijningsvorm van een computerprogramma beschermd zijn, staat overigens los van de mogelijkheid dat dit materiaal beschermd kan zijn als 'voorbereidend materiaal' (art. 10 lid 1 sub 12 Aw), of, indien oorspronkelijk, als zelfstandig werk.)

Naast de vorm of uitdrukkingswijze van een programma kunnen we ook nog onderscheiden naar de fysieke verschijningsvormen. Een computerprogramma kan zijn vastgelegd op diskette of tape, maar het is ook beschikbaar in de vorm van 'print outs', de uitgeprinte programmaregels op papier, ook wel 'listings' genoemd. Ook zien we steeds vaker dat software permanent en onuitwisbaar is vastgelegd in bepaalde produkten (wasmachines, magnetrons, elektronische apparatuur; zogenoemde 'embedded software'). Vanuit auteursrechtelijke optiek is dit onderscheid wederom niet relevant voor de beschermbaarheid, aangezien voor de vaststelling van het 'werk' niet van belang is het corpus mechanicum, het medium waarin het corpus mysticum is vormgegeven. (De beschermings*omvang* kan evenwel per type drager verschillen.)

Een extra moeilijkheid is nog de vorm waarin het programma zich via het beeldscherm aan de gebruiker presenteert, de zogenoemde 'look and feel

doctrine'. Zoals het mogelijk was om met enkele wijzigingen in de programmaregels van een bestaand programma (in de source) net te doen alsof een geheel nieuw programma is gemaakt, zo is het omgekeerde ook mogelijk: een geheel nieuw programma schrijven, dat zich op het beeldscherm echter op gelijke wijze presenteert als een bestaand programma.

4.3 Auteursrechtelijke bescherming van software

Op 14 mei 1991 is de Richtlijn betreffende de rechtsbescherming van computerprogramma's aangenomen. De richtlijn is in 1994 in de Auteurswet 1912 geïmplementeerd. Bij de tot stand koming van de richtlijn is vanuit met name drie verschillende groeperingen een lobby-circuit actief geweest: de Amerikaanse leveranciers, de Europese leveranciers en de gebruikers van software. Enkele belangrijke overwegingen die aan de richtlijn ten grondslag liggen zijn:

- software zou niet in alle lidstaten duidelijk en in gelijke mate beschermd zijn;
- de ontwikkeling van software gaat gepaard met een enorm menselijk en technisch potentieel, waarvan het eindresultaat eenvoudig is te kopiëren;
- computertechnologie is van belang voor de industriële ontwikkeling van de EU;
- met de richtlijn wordt beoogd internationale standaardisatie te bevorderen.

4.3.1 De hoofdlijnen van de richtlijn

In de richtlijn is ervoor gekozen de in de praktijk reeds vorm gekregen auteursrechtelijke bescherming van software te continueren. Software zal daarin worden aangemerkt als een werk van letterkunde (art. 1 lid 1). Deze nadere aanduiding is voor ons land van weinig betekenis, doch in het auteursrecht van andere lidstaten gelden soms verschillende bepalingen voor letterkunde, wetenschap of kunst. De verplichte regeling volgens het auteursrecht laat volgens de richtlijn andere juridische beschermingsmogelijkheden onverlet (art. 9 lid 1). Zo zal het mogelijk blijven octrooirechtelijke bescherming voor software in te roepen, uiteraard voor zover aan de daarvoor gestelde vereisten wordt voldaan.

OBJECT VAN BESCHERMING

De uitdrukkingswijze van software wordt beschermd 'in welke vorm dan ook' (art. 1 lid 2), inclusief het voorbereidend materiaal indien dit van dien aard is dat het later tot zulk een programma kan leiden. De zinsnede 'in gelijk welke vorm' is natuurlijk geheel in overeenstemming met de geldende opvattingen binnen het auteursrecht omtrent het corpus mysticum als object van be-

scherming. Het lijkt erop dat deze toevoeging vooral is bedoeld om een einde te maken aan mogelijke onzekerheid over de vraag of bijvoorbeeld de object-code ook beschermd geacht kan worden. Niettemin is de formulering nog dermate cryptisch dat bijvoorbeeld de grenzen van de 'look and feel' bescherming daarmee niet zijn aangegeven.

Alleen de uitdrukkingswijze van een programma wordt beschermd. Ook dit is in overeenstemming met het hiervoor (paragraaf 3.1.1) neergelegde criterium van de Hoge Raad. Niet beschermd worden ideeën en beginselen die aan enig element van een computerprogramma ten grondslag liggen (art 1 lid 2). Hoewel een onderscheid als hier bedoeld op zichzelf binnen de auteursrechtelijke systematiek als juist beoordeeld kan worden, wreekt zich hier de onduidelijkheid van terminologie en de 'onbalans' tussen considerans en tekst van de richtlijn. Enerzijds wordt gesteld dat voorbereidend materiaal onder de bescherming valt, terwijl anderzijds, in de considerans, algoritmen (en logica en programmeertalen) weer worden uitgesloten. Een enkel algoritme, losgemaakt uit het verband met andere algoritmen, zal terecht geen bescherming mogen genieten. Dit wordt mogelijk anders als we te maken hebben met een combinatie van algoritmen die tezamen een representatie van het programma vormen.

Resteert nog de beoordeling van het stroomdiagram en van de functionele en technische ontwerpen. Ten aanzien van deze 'ontwikkelingsfasen' zullen we het moeten stellen met de vraag of dit als voorbereidend materiaal mag worden aangemerkt dat 'tot zulk een programma' kan leiden.

De uitsluiting van computertalen is in het licht van hetgeen hierover is vermeld vanzelfsprekend. De taal zelf is immers niets meer dan een conventie, een afspraak voor een bepaalde notatie, voor een bepaalde syntax. Anders echter ligt dit voor de compilers, de computerprogramma's die de hogere programmeertaal omzetten in machinetaal. Valt PASCAL niet onder de bescherming van de richtlijn, de PASCAL-compiler van een bepaalde leverancier wel. In feite betekent dit ook dat het zogenoemde 'meekopiëren' van subroutines tijdens het compileren als een auteursrechtelijk relevante verveelvoudiging gezien moet worden. Het is om deze reden dat leveranciers van compilerprogrammatuur dan ook in hun licentievoorwaarden opnemen dat ten aanzien van dit soort kopiëren het auteursrecht niet zal worden uitgeoefend. (Dus wèl als de compiler in zijn geheel wordt gekopieerd!).

CRITERIUM

Als enig criterium voor de beoordeling of een programma als een 'werk' is aan te merken, geldt het oorspronkelijkheidscriterium. Hieraan wordt al voldaan zodra er sprake is van een 'eigen schepping van de maker' (art. 1 lid 3). Er mogen geen nadere esthetische of kwalitatieve eisen worden gesteld. Een laag oorspronkelijkheidscriterium derhalve, dat bedoeld is om het beschermingsniveau van de verschillende lidstaten te harmoniseren. De

Duitse Inkasso-uitspraak, waarin een boekhoudprogramma vanwege een te geringe oorspronkelijkheid auteursrechtelijke bescherming werd onthouden, is op basis van het huidige criterium niet meer mogelijk (BGH, 9 mei 1985, GRUR 1985, blz. 109).

Dit criterium is evenwel aldus uitgelegd dat niet-oorspronkelijke computerprogramma's bescherming op grond van het auteursrecht moeten ontberen, dus ook die van de 'geschriftenbescherming'. Dit lijkt echter een te enge interpretatie. Het is aannemelijk dat de EC met het bedoelde criterium slechts een bovengrens heeft willen aangeven: er mag niet méér worden geëist. Dat de Nederlandse wetgever computerprogramma's - al dan niet oorspronkelijk - van de geschriftenbescherming heeft uitgesloten, kan dan ook niet worden onderbouwd met een verwijzing naar de richtlijn. De overige beschermingsvormen blijven immers onverlet (art. 9 lid 1). Weinig consistent lijkt voorts de systematiek dat voorbereidend materiaal, zo mogelijk zelfs de 'print out' van een computerprogramma, wel zelfstandig bescherming geniet onder de geschriftenbescherming.

RECHTEN MAKER

De rechten die de maker toekomen op grond van de richtlijn (art. 4) worden onderscheiden in:

- reproduktie
- vertalen
  bewerken, wijzigen } transformatie
  omzetten codevorm
- distributie

} verveelvoudigen
'openbaarmaken'

} exploitatie-rechten

Zoals uit bovenstaand schema blijkt, kan de terminologie uit de richtlijn moeiteloos worden ondergebracht onder de bestaande auteursrechtelijke terminologie met betrekking tot de exploitatierechten. Het recht van de rechthebbende zich te verzetten tegen wijzigingen van het werk wordt echter ruimer geacht dan tegen de achtergrond van het verveelvoudigingsrecht. Ook wijzigingen in het betreffende exemplaar zelf (dus ook niet gepaard met een verveelvoudiging) worden onder dit recht begrepen, voorzover het wijzigen niet betreft een toegelaten handeling zoals het verbeteren van fouten (art. 5 lid 1).

Onder *maker* kunnen zowel natuurlijke personen als rechtspersonen worden begrepen (art. 2 lid 1). Ingeval van in dienstverband vervaardigde software is de werkgever bij uitsluiting bevoegd de 'economische rechten' met betrekking tot de software uit te oefenen, tenzij bij overeenkomst anders is bepaald (art. 2 lid 3). Vanwege deze omschrijving blijft in het midden of de werknemer wellicht aanspraak zou mogen maken op de persoonlijkheidsrechten, of dat dit naar de werking van het nationale auteursrecht van een lidstaat moet worden bepaald. Evenmin biedt deze omschrijving uitsluitsel

over wie als auteursrechthebbende moet worden aangemerkt als het programma is gemaakt door werknemers in dienst van een softwarehuis, maar werken onder leiding en toezicht van een 'inlenend' bedrijf. Uit de voorgeschiedenis van de richtlijn kan wel worden opgemaakt dat de systematiek van onder meer het Nederlandse auteursrecht is gevolgd voor wat betreft de ontwikkeling van maatsoftware, van in opdracht gemaakte software. In die situatie is niet de opdrachtgever/betaler auteursrechthebbende, maar de daadwerkelijke maker. Dit zou - op grond van Nederlands recht - slechts anders worden indien de software naar het ontwerp van een ander is gemaakt en onder diens leiding en toezicht (art. 6 Aw).

RECHTEN GEBRUIKER

De richtlijn onderscheidt voor de rechtmatige verkrijger c.q. gebruiker de volgende rechten:

1. Het 'laden' van het programma in het werkgeheugen van de computer en
2. het verbeteren van fouten in het programma (art. 5 lid 1);
3. Het maken van een reservekopie (art. 5 lid 2);
4. De observering, bestudering en het testen van de werking van het programma ten einde vast te stellen welke ideeën en beginselen aan het programma ten grondslag liggen, tijdens het rechtmatig gebruik van het programma (art 5 lid 3).

Bezien we deze vastgelegde rechten nader, dan blijkt dat de positie van de gebruiker op geen enkele wijze verbeterd is ten opzichte van de gangbare praktijk.

Ad 1. Het spreekt voor zich dat een rechtmatige verkrijger c.q. gebruiker van een programma dit programma moet kunnen gebruiken. Daartoe is het technisch noodzakelijk dat het programma in het geheugen van de computer wordt ingevoerd. Licenties voorzien daar al in, maar ook zonder expliciete toestemming in licenties zal men toch mogen aannemen dat in de verstrekking van het programma toestemming tot gebruik ligt besloten. En voorts zou men het inlezen van het programma in het werkgeheugen toch eerder als een gebruikshandeling moeten aanmerken dan als een nieuwe, auteursrechtelijk relevante verveelvoudiging. Hoewel op grond van art. 4 lid 1 in beginsel de toestemming is vereist van de rechthebbende voor het laden, het in beeld brengen of de uitvoering van het programma, geldt dit ingevolge art. 5 lid 1 niet ten aanzien van de rechtmatige verkrijger.

Ad 2. Het verbeteren van fouten zal eerst werkelijk meerwaarde krijgen indien dit recht ook de bevoegdheid tot het opeisen van de broncode met zich mee zou brengen. Dit laatste is iets dat softwareontwikkelaars - begrijpelijk - nu juist niet willen. Het Hof Den Bosch (7 februari 1994, NJ 1994, 616, Cr

1994/2) oordeelde, in een situatie waarin de curator van een softwareleverancier de broncode slechts tegen een vergoeding wilde verstrekken, dat de prijs voor een gebruiksrecht in beginsel niet mede omvat het gebruiksrecht op de broncode, doch dat dit anders kan zijn wanneer het gaat om programmatuur die speciaal ten behoeve van een bepaalde afnemer is ontwikkeld ('maatwerkprogrammatuur'), door deze is gefinancierd, en, gezien de unieke inzetbaarheid daarvan, geen commerciële waarde zal hebben. In een andere uitspraak met betrekking tot maatwerk software oordeelde het Hof Den Bosch (24 april 1995, NJ 1995, 151, Cr 1996/5, bevestigd door de Hoge Raad in het arrest van 21 juni 1996, RvdW 1996, 145, Cr 1996/5) dat op grond van de tussen partijen gesloten overeenkomst de maatwerk programmatuur volledig eigendom van de afnemer werd, mede omvattende het gebruiksrecht op de daarmee samenhangende documentatie en de broncode. Het eventueel door derden aanbrengen van wijzigingen in de programmatuur was niet in strijd met het auteursrecht.

Volgens de considerans van de richtlijn mag het verbeteren van fouten - evenmin als het laden, het in beeld brengen en de uitvoering van het programma - niet bij overeenkomst worden verboden. Dit verbod sluit niet uit dat het gebruiksrecht mag worden beperkt, of dat aan het verbeteren van fouten voorwaarden worden gesteld. Zo is aannemelijk dat de rechtmatige verkrijger bij overeenkomst een eventueel recht op de broncode expliciet mag worden onthouden. De thans in beginsel geschapen mogelijkheid, om ongedocumenteerd, op het niveau van machinetaal fouten te verbeteren, zal waarschijnlijk nauwelijks een wijziging veroorzaken ten opzichte van de vroegere praktijk waar in de licentie-overeenkomsten het verbeteren van fouten veelal niet werd toegestaan.

De term 'fouten' heeft niet slechts betrekking op de situatie dat het programma niet werkt of niet correct werkt, doch ook op onvolkomenheden in het programma waardoor het niet (meer) voor het daarmee beoogde doel kan worden gebruikt.

Ad 3. Het maken van een reservekopie mag niet bij overeenkomst worden verhinderd. Hier ligt hoegenaamd geen belang. In de eerste plaats wordt een bevoegdheid als deze doorgaans juist expliciet opgenomen in de licentiebepalingen. In de tweede plaats laat de praktijk van het computergebruik zien dat het verkregen programma eerst moet worden gekopieerd op de harddisk van de computer (moet worden geïnstalleerd), waarna het oorspronkelijk geleverde exemplaar dienst gaat doen als reservekopie.

Ad 4. De vierde bevoegdheid tenslotte is het bespreken eigenlijk niet waard. Zij kan getypeerd worden als een optische concessie aan de gebruikerslobby. Is het niet te gek voor woorden dat de afnemer bevoegd is om de werking van een programma te begrijpen indien hij het gebruikt waarvoor het is

ontworpen? Tegenover deze 'bevoegdheid' van de rechtmatige gebruiker, treffen we in art. 6 echter een veel ingrijpender beperking aan in de introductie van een verbod tot decompilatie. Dat dit 'verbod' is verwoord aan de introductie van een beperking van mededingingsrechtelijke aard wordt echter in art. 6 een beperking geformuleerd Van meer belang in deze zijn de in art. 6 geformuleerde beperkingen die nadere bestudering van computerprogramma's in de weg staan. Tegenover deze 'bevoegdheid' van art. 5 treffen we echter de veel ingrijpender decompilatiebepaling aan van art. 6, waarin aan nader onderzoek aan een computerprogramma verstrekkende beperkingen worden opgelegd.

4.3.2 Decompilatie

De-compileren, het herleiden van de broncode van een computerprogramma op basis van de machinecode, is een handeling die onder de bredere noemer te brengen valt van *reverse engineering*. Als *engineering* omschreven kan worden als het vervaardigen van praktische toepassingen op basis van theoretische modellen, betekent *reverse* engineering het (re)construeren van het theoretische model aan de hand van de praktische toepassing. Het doel hiervan is het opdoen van inzicht in de werking van de toepassing, veelal met het oogmerk de verworven kennis vervolgens toe te passen in een eigen ontwikkeling.

Men kan de systematiek van een computerprogramma achterhalen door bijvoorbeeld de gedragingen te bestuderen, de manier waarop het programma zich manifesteert op het beeldscherm, het resultaat van de gegevensverwerking, of de handleiding. Meer in het bijzonder spitst de problematiek van reverse engineering van software zich toe op het decompileren en het disassembleren, hoewel het begrip hiermee niet synoniem is. De omzetting van de machinecode leidt naar de huidige stand van de techniek bovendien niet zonder meer tot een bruikbare broncode.

Hierboven is de curieuze bevoegdheid uit art. 5 lid 3 vermeld, op basis waarvan de rechtmatige gebruiker zonder toestemming van de rechthebbende gemachtigd is 'de werking van het programma te observeren, te bestuderen en uit te testen, ten einde vast te stellen welke ideeën en beginselen aan een element van het programma ten grondslag liggen, indien hij dit doet bij het rechtmatig laden of in beeld brengen, de uitvoering, transmissie of opslag van het programma', tijdens het normale gebruik derhalve.

In art. 6 wordt de rechtmatige gebruiker voorts de bevoegdheid toegekend zonder toestemming van de rechthebbende de machinecode om te zetten in broncode (decompileren) indien dit onmisbaar is om informatie te verkrijgen die nodig is om interoperabiliteit met een onafhankelijk gecreëerd computerprogramma tot stand te brengen. Decompilatie dient daarbij te worden

beperkt tot die onderdelen van het oorspronkelijke programma die voor het tot stand brengen van de interoperabiliteit noodzakelijk zijn, de interfaces. De verkregen informatie mag niet worden gebruikt voor de vervaardiging van een 'qua uitdrukkingswijze in grote lijnen gelijk programma' (art. 6 lid 2 sub c).

De introductie hier van een verbod op het toepassen van verkregen inzichten is hoogst opmerkelijk. De toevoeging dat het een programma betreft dat qua uitdrukkingswijze in grote lijnen lijkt op het bestudeerde programma werpt hierop geen ander licht. Het auteursrecht als zodanig is nu juist *bedoeld* om het vervaardigen van zo'n programma als onrechtmatig te mogen kwalificeren. En zo belanden we op het fundamentele criterium waartegen we het vraagstuk van decompilatie op auteursrechtelijke systematiek en dogmatiek zouden dienen te beoordelen.

De regeling van art. 6 geeft nogal aanleiding tot enige onduidelijkheid. Wat dienen we bijvoorbeeld te verstaan onder interoperabiliteit en interfaces? Is bijvoorbeeld de wijze waarop het programma zich via het beeldscherm manifesteert aan de gebruiker, soms ook wel gebruikersinterface genoemd, niet ook een onderdeel van de 'interoperabiliteit' tussen computerprogramma's? Hoe verhoudt deze vorm van 'interoperabiliteit' zich tot de 'look and feel doctrine'? Maakt deze vorm van 'interoperabiliteit' inbreuk op de 'in grote lijnen gelijke uitdrukkingswijze' van art. 6 lid 2 sub c? En in hoeverre zou dit geoorloofd zijn met het oog op de bij het publiek aanwezige behoefte tot standaardisering (Tomado-kleerhanger-arrest, HR 12 juni 1970, NJ 1970, 434)? Duidelijk is wel dat het verbod op decompilatie, met het oog op het achterhalen van achterliggende ideeën en beginselen anders dan die van de interfaces, een extreem krachtige mededingingsbeperkende regeling verankert in het auteursrecht.

Om het mogelijk te maken decompileren voor andere doeleinden dan interoperabiliteit te verbieden, wordt dankbaar gebruik gemaakt van de *toevalligheid* dat dit gepaard gaat met het maken van kopieën. Omdat het verveelvoudigingsbegrip zo aan techniek wordt opgehangen, is het vervolgens steeds nodig uitzonderingen op te nemen, zoals geen toestemming nodig voor het laden van het programma, of voor het maken van reservekopiëen. Men kan zich echter afvragen of het auteursrechtelijke begrip van de term verveelvoudigen wel samenvalt met het technische begrip van de term kopiëren. Daarvoor dienen we eens nader stil te staan bij doel en strekking van het auteursrecht in relatie tot het hier te beschermen belang.

RECHTSGRONDEN VAN HET AUTEURSRECHT

Spoor en Verkade (Auteursrecht) merken op dat voor het auteursrecht niet slechts één rechtsgrond is aan te wijzen: 'Zowel overwegingen van rechtvaardigheid als van maatschappelijk nut spelen een rol.' Ook Van Lingen (Auteursrecht in hoofdlijnen) meent dat de vraag naar de grondslagen van het

auteursrecht niet eenduidig is te beantwoorden: ‘De vraagstelling is echter van meer dan theoretisch belang, omdat de evoluerende opvattingen ter zake bepalend zijn voor rechtsvorming en rechtsvinding door wetgever en rechter, en daarmee voor de (actuele) rechtsposities der betrokkenen. In het algemeen, kan men zeggen, is de wettelijke erkenning van het recht van de auteur gegrond op overwegingen van billijkheid en van utiliteit.’ In relatie tot de decompilatiebepaling zou dit tot de volgende overwegingen kunnen leiden:

1. De introductie in de Auteurswet 1912 van beperkingen aan de bevoegdheid tot decompileren (art. 45m), maakt het de facto moeilijker om de ideeën die aan het computerprogramma ten grondslag liggen te achterhalen. Dit heeft een verstoring tot gevolg van de hierboven geschetste balans tussen het individuele belang en het maatschappelijk belang. Een dergelijke beperking is derhalve niet in overeenstemming met het doel van het auteursrecht.
2. Van groter belang dan de vraag of het kopiëren ingevolge decompilatie een inbreuk vormt op het verveelvoudigingsrecht, is de vraag of een dergelijke verveelvoudiging een schending oplevert van de norm die het auteursrecht door middel van dat verveelvoudigingsrecht beoogt te beschermen. Deze opvatting impliceert de noodzaak tot een beoordeling of de verveelvoudiging ‘auteursrechtelijk relevant’ is.
3. De uitsluitende rechten tot openbaarmaking en verveelvoudiging worden wel samen gebracht onder de noemer ‘exploitatierechten’. De ratio van deze rechten is dat de rechthebbende aldus de exploitatie van het werk kan beheersen. Het ‘verbod’ op openbaarmaking en het ‘verbod’ op verveelvoudiging zijn in zoverre complementair, dat zij beide dienen ter voorkoming van het zonder de toestemming van de maker verspreiden van het werk. De met decompileren gepaard gaande verveelvoudiging is op zichzelf niet gericht op de verspreiding van het werk, en is derhalve geen handeling waarvoor de exploitatierechten bedoeld zijn om te voorkomen.

De systematiek en achterliggende ratio van het auteursrecht biedt eigenlijk helemaal geen basis voor zulke beperkingen aan decompilatie, aangezien hier tenslotte niet de *exploitatie* van het werk - in oorspronkelijke dan wel gewijzigde vorm - in het geding is, doch uitsluitend nog de *inspanning* die aan het maken van het werk ten grondslag heeft gelegen. Er ligt immers geen verbod op het uiteindelijke nieuwe resultaat (voorzover dit resultaat tenminste niet zelfstandig inbreuk maakt op auteursrechten), doch slechts op de wijze waarop de voorbereidingen van dit resultaat hebben plaats gevonden.

4.3.3 Prestatiebescherming

Het tegengaan van decompileren met een beroep op het auteursrecht, leidt tot een verdergaande bescherming van de prestatie van de maker dan waarvoor

het auteursrecht is bedoeld. Los van de vraag naar de wenselijkheid van het tegengaan van reverse engineering is het ook helemaal niet nodig om hierin in het auteursrecht te voorzien. Nu blijkt dat de kern van een verbod op reverse engineering niet gelegen is in de bescherming van de originele vorm van het werk, doch slechts op de daarbij komende inspanning, lijken de leerstukken van slaafse nabootsing en van prestatiebescherming een meer geëigend kader voor een onrechtmatig aanleunen tegen de prestatie van een ander.

Ondanks dat de verwachtingen van de door de Hoge Raad geboden opening in het Decca/Holland Nautic-arrest (HR 27 juni 1986, NJ 1987, 191) door de vervolgarresten enigszins getemperd zijn, lijkt het zinvoller en dogmatisch meer juist deze problematiek in de rechtsontwikkeling van 6:162 BW, de onrechtmatige daad, te laten plaats vinden. Gelet op de hierboven uiteen gezette begripsmatige onduidelijkheid, inherent aan technologie die zo in ontwikkeling is, en de diversiteit aan handelingen en mogelijke doeleinden, zal een beoordeling van deze omstandigheden per geval tot een zorgvuldiger afweging van de in het geding zijnde belangen leiden dan een generiek auteursrechtelijk verbod.

De beoordeling of er onrechtmatig handelen heeft plaats gevonden komt op deze wijze ook helder te liggen, en wel aan de hand van het (nieuwe) eindprodukt. Is het nieuwe programma in meer of mindere mate een kopie van een bestaand programma, dan is er - met of zonder decompilatie - sprake van inbreuk op auteursrechten. Is dat niet het geval, dan resteert de beoordeling of er sprake is van een ‘eenlijnsprestatie’, of dat bij de ontwikkeling van het nieuwe programma op ongeoorloofde wijze is aangeleund tegen het andere programma. Ook zou hierdoor het door de richtlijn geschapen probleem omtrent de handhaving worden vermeden. Indien uit het eindprodukt zelf niet blijkt van enige inbreuk op auteursrechten, lijkt het welhaast ondoenlijk om bewijs aan te dragen van mogelijke decompilatie van een ander programma.

Bovendien ligt het fenomeen decompileren sowieso meer op het terrein van de ongeoorloofde mededinging. Niettemin lijkt het ook in het mededingingsrecht ongebruikelijk decompileren te verbieden. Het is toch ondenkbaar dat nieuwe, hoogwaardige technologieprodukten niet ook door concurrenten zullen worden afgenomen om deze vervolgens uit elkaar te halen tot de laatste weerstand verdwenen is. Indien we voorts een vergelijking maken met de industriële tak van het intellectueel eigendomsrecht, dan zien we dat de verlening van een exclusief recht op grond van het octrooirecht of het chipsrecht nu juist geschiedt onder de conditie dat door publikatie van het werk reverse engineering mogelijk wordt. De decompilatieregeling zorgt dus niet alleen voor een interne inconsistentie binnen het auteursrecht (zie paragraaf 4.3.2 hiervoor), doch ook met andere intellectuele rechten, waarbij het de vraag is of een zodanig beoogde belemmering in de toekomst niet als onrechtmatig zal worden geoordeeld.

4.3.4 Interoperabiliteit en standaardisatie

De andere belangrijke vraag waarvan de beantwoording nog open staat, is die van het gebruik van interfaces. Decompilatie ter verkrijging van informatie omtrent interoperabiliteit, betekent niet vanzelf dat bepaalde onderdelen van computerprogramma's die inmiddels tot marktstandaarden zijn geworden, zullen mogen worden geïncorporeerd in andere programma's. De richtlijn gaat mank voor wat betreft de pretentie hieromtrent meer duidelijkheid te verschaffen. Wat wel duidelijk naar voren komt, is de compromisachtige wijze waarop de softwarelobby's zijn beslecht. Op de volkomen bescherming van computerprogramma's heeft de krachtigste softwarelobby - die van de producenten verenigd in de Software Action Group for Europe (SAGE) - slechts de beperkte uitzondering moeten toestaan voor het analyseren van interfaces. De werkelijke bedreiging voor de industriële ontwikkeling binnen de EU wordt gevormd door de facto marktstandaarden zonder aandeel voor de Europese industrie, zoals wel bepleit door de lobby van Europese producenten, verenigd in ECIS (European Committee for Interoperable Systems). Ook het antwoord hierop ligt besloten in het EU-mededingingsrecht. Op basis daarvan zullen marktleiders wellicht moeten accepteren dat de onder het publiek aanwezige behoefte aan standaardisatie dergelijke 'inbreuken' op het auteursrecht rechtvaardigt.

Behalve tegen de achtergrond van rechtszekerheid, is de roep om expliciete regeling van softwarebescherming in het auteursrecht ook ondersteund door de wens om de verschillende regimes binnen de EU te harmoniseren. Dit op zichzelf te waarderen uitgangspunt krijgt met de huidige regeling echter het karakter van het paard achter de wagen spannen. Niet valt in te zien immers waarom deze wenselijke harmonisatie alleen zou gelden voor computersoftware en zich niet tevens zou dienen uit te strekken over de overige werken onder het auteursrecht. Een EU-richtlijn strekkende tot harmonisatie van het auteursrecht is daartoe een zinvoller - doch zonder twijfel complexer - instrument. De thans gevolgde procedures, het aanpassen van nationaal auteursrecht naar aanleiding van EU-richtlijnen betreffende specifieke onderwerpen, blijkt echter allerminst bevorderlijk voor de interne consistentie.

4.3.5 Geschriftenbescherming

Het leerstuk van de geschriftenbescherming is, vanwege de uitbreidende werking daarvan naar ook niet-oorspronkelijke geschriften, in auteursrechtkringen steeds veel besproken. Bij de implementatie van de softwarerichtlijn in de Auteurswet 1912, heeft de wetgever er voor gekozen computerprogramma's niet aan te merken als geschriften (art. 10 lid 1 sub 12). Afgezien van de opvatting dat in het algemeen terughoudend zou moeten worden

omgegaan met geschriftenbescherming, spitste de kritiek *tegen* het onderbrengen van computerprogrammatuur onder de geschriftenbescherming zich toe op het bezwaar dat auteursrecht op triviale programmatuur zou leiden tot een monopolie op techniek. Dit lijkt een irreëel bezwaar. Gezien de reikwijdte van de geschriftenbescherming - bescherming tegen rechtstreekse ontlening aan het geschrift - wordt alleen voorkomen dat geschriften min of meer letterlijk worden overgenomen. Het staat software-ontwikkelaars niet in de weg *zelfstandig* tot een zelfde programma te komen. Mede gelet op het lage originaliteitsvereiste, zullen programma's die het niveau van bijvoorbeeld een eenvoudige sorteerroutine te boven gaan bovendien al gauw als oorspronkelijke werken beschouwd kunnen worden. Het is zeer wel verdedigbaar dat onderdelen van computerprogramma's waarbij slechts een gering aantal programmeringsmogelijkheden voor handen is, zo zij niet reeds tot het publieke domein behoren, op talloze plaatsen onafhankelijk van elkaar zijn ontwikkeld.

Belangrijker dan het aspect van de bescherming van triviale computerprogramma's is echter dat ook *oorspronkelijke* computerprogramma's onder de geschriftenbescherming zouden vallen. Computerprogramma's die enige (commerciële) betekenis hebben, zouden aldus zwaarder worden beschermd, omdat zowel kopiëren voor eigen oefening, studie of gebruik (art. 16b lid 1), als kopiëren ten behoeve van een onderneming, organisatie of instelling (art. 17 lid 1) beperkt moet blijven tot *een klein gedeelte* van het werk. Een consequentie die met het oog op de lage 'kopieermoraal' hier te lande allerminst zonder belang kan worden geacht. Omdat computerprogramma's echter niet (meer) als geschriften worden beschouwd, is deze beperking niet (meer) van toepassing. Om dan toch het kopiëren voor eigen gebruik of binnen organisaties tegen te gaan, is een extra artikel nodig geworden in de vorm van 45n, waarin wordt bepaald dat de artikelen 16b lid 1 en 17 lid 1 Aw niet van toepassing zijn op computerprogramma's. De keuze in art. 10 lid 1 sub 12 Aw (computerprogramma's zijn geen geschriften) maakt vanuit dit perspectief de implementatie van de richtlijn niet alleen nodeloos complex. Ook draagt deze 'status aparte' weer bij aan een verdere inconsistentie in het auteursrecht en een tot verwarring leidend begrippenkader.

4.3.6 Overige aandachtspunten

Ter afsluiting van de auteursrechtelijke bescherming van software worden in deze paragraaf nog kort enige afzonderlijke aandachtspunten besproken.

DE BESCHERMING VAN MET SOFTWARETOOLS GEMAAKTE APPLICATIES

Onder softwaretools wordt hier verstaan computerprogramma's zoals database-programma's en spreadsheet-programma's ('rekenbladen') met

behulp waarvan (ook) meer algemeen toepasbare applicaties kunnen worden vervaardigd. De beantwoording van dit vraagstuk heeft veel overeenkomsten met die van de bescherming van compilers. Een belangrijk verschil is echter dat de softwaretool-leverancier wèl het auteursrecht op iedere mee te leveren applicatie zal wensen uit te oefenen. Met andere woorden: voor een applicatie geschreven met behulp van een softwaretool zal zowel voor de applicatie als voor de tool een gebruiksrecht moeten worden verkregen.

CASETOOLS, PROGRAMMAGENERATOREN EN MIDDELS COMPUTERS GEMAAKTE WERKEN.

In dit laatste geval handelt het bijvoorbeeld om computerkunst, zoals poëzie, schilderijen, animaties en tekenfilms, die tegenwoordig voor een deel door computers worden gemaakt. Het probleem bij deze vraagstukken is wie de geestelijke vader van het werk is. Is dat de computerprogrammeur of degene die de computer gebruikt? (Nee, natuurlijk niet de computer zelf. Computers zijn immers geen rechtssubjecten). In het algemeen kunnen deze werken wel auteursrechtelijk beschermd zijn, waarbij de gebruiker van het programma doorgaans als de maker moet worden aangemerkt.

DE AUTEURSRECHTELIJKE BESCHERMING VAN BEELDSCHERMSPELLETJES.

Naast de bescherming van het computerprogramma kan ook de output van een beeldschermspelletje beschermd zijn. Het Hof Amsterdam heeft in een zaak tussen Philips en Atari uitgemaakt dat de bescherming van de output van een computerspelletje overeenkomt met de bescherming van een filmwerk (vergelijk art. 10 lid 1 sub g Aw). Atari vroeg om bescherming van ‘Pac-Man’ tegen het daarop gelijkende ‘Happelaar’ van Philips en werd door het Hof in het gelijk gesteld (Hof Amsterdam, 31 maart 1983, AMR 1983, p. 56). In Duitsland kreeg Philips overigens gelijk. Een derde aspect van beeldscherm-spelletjes is de bescherming van de figuren die over het scherm gaan bij het spelen. Bij stripverhalen heeft de Hoge Raad uitgemaakt dat figuren een afzonderlijke bescherming hebben, los van het verloop van het verhaal (Suske en Wiske-arrest, HR 13 april 1984, NJ 1984, 524)). Men zou zich nog kunnen afvragen wat de betrokkenheid is van de speler met betrekking tot de output. De speler stuurt het programma, maar is daarbij niet creatief bezig. Hij kan dan ook niet als de maker van de output gezien worden. Dat blijft de programmeur.

‘CONTRIBUTORY INFRINGEMENT’ (=MEDEPLICHTIGHEID AAN INBREUK)

Hierbij gaat het om een bijdrage aan infringement door derden. In januari 1984 besliste het USA Supreme Court in een zaak tussen Walt Disney en Sony (de zogenoemde. Betamax case). Burgers kopieerden films met gebruik-making van Sony recorders. Het verschaffen van de apparatuur was contri-butory infringement volgens Disney. Het Supreme Court maakte uit dat het thuis kopiëren geen infringement is. Een enigszins vergelijkbare zaak over

computersoftware speelde in West-Duitsland. Met het oog hierop is in de richtlijn de bepaling van art. 7 lid 1 onder c opgenomen, dat passende sancties voorschrijft voor het in het verkeer brengen van middelen die uitsluitend bestemd zijn voor bijvoorbeeld het doorbreken van softwarebeveiligingen.

PUBLIC DOMAIN SOFTWARE EN SHAREWARE

Onder public domain software wordt software verstaan die de makers zonder kosten ter beschikking stellen aan eenieder die het programma maar wenst te hebben. Sommige hobbyisten geeft het feit dat anderen hun (thuis gemaakte) software ook gebruiken reeds genoeg voldoening. Ten onrechte wordt wel gedacht dat op deze software geen auteursrecht rust. Het is alleen zo, dat de auteur *sommige* rechten niet zal uitoefenen. (Doorgaans zal de hobbyist die het om eeuwige roem te doen is, zich wel wensen te verzetten tegen het verwijderen van zijn naam uit het programma.)

Shareware zegt meer over de wijze van *distributie* van software. Een geïnteresseerde is vrij om het programma bijvoorbeeld van een bulletin board te downloaden, om te bezien of hij het zou willen gebruiken. Besluit hij inderdaad dat het programma wat voor hem is, dan wordt op (het fatsoen van) de gebruiker een beroep gedaan om alsnog een (meestal bescheiden) vergoeding over te maken. Om het aantrekkelijk te maken fatsoenlijk te zijn, wordt veelal de toezending van een nuttige handleiding in het vooruitzicht gesteld.

COMPUTERVIRUSSEN

Computervirussen zijn programma's die i) de instructie bevatten zichzelf in andere computerprogramma's te kopiëren zodra zulk ander programma wordt geladen en ii) veelal een vervelende tot zelfs zeer schadelijke activiteit uitvoeren. Dat kan variëren van bijvoorbeeld het spontaan op het scherm weergeven van een stuiterend pingpong balletje tot het wissen van de harddisk. Vanzelfsprekend is het aanbrengen van een virus onrechtmatig. Het opsporen van virussen door zogenoemde antivirus-programma's, die bestaan uit stukjes programmacode van het virusprogramma, kan door de virusauteur natuurlijk niet verboden worden met een beroep op het auteursrecht.

4.4 Octrooirechtelijke bescherming van software

In dit onderdeel komt de ontwikkeling aan de orde van de octrooiëring van softwaregerelateerde uitvindingen in Nederland. Het betreft dus Nederlandse octrooien en niet de in ons land geldende Europese octrooien. Uiteraard kan de ontwikkeling in Nederland niet los gezien worden van de Europese, of liever, internationale octrooi-ontwikkelingen.

Ingevolge art. 2 leden 2 sub c en 3 ROW worden computerprogramma's als zodanig niet beschouwd als uitvindingen die vatbaar zijn voor octrooi. Zoals

besproken in paragraaf 3.2.1, betekent dit dat software als abstracte notie, los gedacht van de concrete vormgeving daarvan in machine leesbare code en vastgelegd in een door een computer te verwerken medium, niet voor octrooiëring in aanmerking komt. Wel is het in beginsel mogelijk dat octrooi wordt verleend voor inrichtingen en werkwijzen waarbij computerprogramma's worden toegepast.

Alvorens in te gaan op de octrooirechtelijke bescherming van software wordt in herinnering gebracht dat men octrooi kan krijgen op een uitvinding zijnde een voortbrengsel of een werkwijze. De geschiedenis van het software-werkwijze-octrooi is duidelijk verschillend van de ontwikkelingen op het gebied van software en het voortbrengsel-octrooi.

4.4.1 Werkwijze-octrooien en software

In 1970 deed de Afdeling van Beroep van de Octrooiraad een uitspraak over de octrooieerbaarheid van een computergestuurde telefooncentrale (Octrooiraad 16 december 1970, telefooncentrale, BIE 1971, 10). De centrale bestond uit een hardwaredeel en een softwaredeel. Het geheel was geschikt voor het tot stand brengen van telefoonverbindingen. Voor de computer inclusief het nieuwe programma, ofwel het hardware- én het softwaredeel, werd een werkwijze-octrooi aangevraagd. Octrooi werd niet verleend. De Afdeling van Beroep stelde in haar beschikking dat voor verkrijging van een werkwijze-octrooi sprake zou moeten zijn van *stoffelijkheid* en dat kon met betrekking tot een computergestuurde werkwijze voor het tot stand brengen van telefoonverbindingen niet worden aangenomen. Het onderwerp van een werkwijze moest van stoffelijke aard zijn in de zin van materie. Informatie kon dus niet het onderwerp van een werkwijze zijn, aldus de Afdeling. Zij achtte bijvoorbeeld wel octrooieerbaar werkwijzen die, met behulp van een computer, chemische, fysische of werktuigkundige veranderingen in materie teweeg zouden brengen.

Tevens stelde de Afdeling dat door het communicatiestelsel geen verandering in de natuur werd aangebracht, zodat niet gesproken kon worden van een werkwijze in de zin van de Rijksoctrooiwet (1910). De verandering in de natuur had tevoren plaatsgevonden, bij het installeren van de telefooncentrale. De werkwijze zelf vond zij niet anders dan het doen innemen van verschillende werkingstoestanden van de inrichting ter uitvoering van de werkzaamheden waarvoor de inrichting bestemd was.

Jarenlang veranderde er niets in de rechtspraak betreffende octrooirechtelijke bescherming van software. Totdat de Afdeling van Beroep in 1983 een uitspraak moest doen betreffende een octrooiaanvraag voor een tomoscanner (BIE, 1983, 104). Dat is een apparaat dat door middel van een daarbij toegepaste rekenmethode de dichtheidsverdeling in de doorsnede van een

object bepaalt. De werkwijze bracht geen verandering in materie teweeg, maar resulteerde in bepaalde informatie. Toch besloot de Octrooiraad octrooi te verlenen; een duidelijke verruiming ten opzichte van de uitspraak van 1970. Was voordien slechts octrooi mogelijk voor werkwijzen die veranderingen in materie teweeg brachten, sinds 1983 mag ook informatie het resultaat zijn van een werkwijze.

In het Streepjescode-arrest van 11 mei 1987 gaat de Afdeling van Beroep van de Octrooiraad weer een stap verder (Octrooiraad 11 mei 1987, streepjescode, BIE 1987, 42). In dit arrest werd informatie, de streepjescode, door middel van een computer verwerkt tot andere informatie, informatie over een artikel. Deze bewerking van informatie kan volgens de Afdeling leiden tot een verandering in de natuur. Energie namelijk moet, in welke vorm dan ook, tot de natuur gerekend worden. Als er, zoals in het onderhavige geval, informatie van de ene informatiedrager naar de andere wordt gevoerd via een computer, dan veranderen de elektromagnetische golven (energie) in die computer en vindt er dus een verandering in de natuur plaats. Ondanks het feit dat volgens de Afdeling van Beroep de informatie zelf niet tot die natuur behoort, kan, mits aan alle overige voorwaarden is voldaan, de hierboven beschreven werkwijze octrooieerbaar zijn. De opvatting van de Afdeling uit het Telefooncentrale-arrest, dat energie niet tot de natuur gerekend moest worden, kon blijkbaar in 1987 niet gehandhaafd blijven.

Een octrooi voor een computergestuurde werkwijze is dus al geruime tijd mogelijk. In eerste instantie (1970) was het onderwerp van de werkwijze echter nog beperkt tot materie en werd informatie nadrukkelijk uitgesloten. Sinds 1983 mag het onderwerp ook betrekking hebben op informatie.

4.4.2 Software en het voortbrengsel-octrooi

In de hierboven reeds aangehaalde telefooncentrale-beschikking werd tevens een duidelijk standpunt ingenomen over de mogelijkheden tot het verkrijgen van een voortbrengsel-octrooi voor computergestuurde inrichtingen. De Afdeling van Beroep stelde in haar beschikking dat er in casu wel sprake was van een voortbrengsel: een voor verschillende doeleinden te gebruiken computer, ook wel general purpose computer genoemd. Dit voortbrengsel kon echter slechts door de informatie-inhoud - een nieuw computerprogramma - worden onderscheiden van andere (general purpose) computers en was daarom volgens de Afdeling niet te beschouwen als een nieuw voortbrengsel in de zin van de Rijksoctrooiwet (1910). De computergestuurde inrichting werd om die reden niet octrooieerbaar geacht.

Ook deze opvatting blijft lange tijd ongewijzigd. Pas in 1985 komt hierin verandering als de Afdeling van Beroep een beslissing moet nemen over een aanvraag voor een voortbrengsel-octrooi voor een (general purpose) compu-

ter met nieuwe programmatuur geschikt voor de besturing van een schakelnetwerk (Octrooiraad 12 september 1985, schakelnetwerk, BIE 1985, p. 435). De Afdeling besloot in deze zaak dat het inbrengen van een nieuw, direct adresseerbaar programma in het werkgeheugen van de computer betekent dat in technisch opzicht een andere, nieuwe inrichting wordt verschaft, die kan worden beschouwd als een nieuw voortbrengsel in de zin van de Rijksoctrooiwet (1910). Een volledige ommezwaai ten opzichte van de uitspraak van 1970.

De Octrooiraad heeft dus in de loop der jaren de mogelijkheden om software te kunnen octrooieren aanmerkelijk verruimd, zowel voor voortbrengsel- als voor werkwijze-octrooien.

4.5 Jurisprudentie

RB ASSEN, 28 JULI 1981, BARTELS SOFTWARE - KOERHUIS, nj 1982, 74

Om bescherming op grond van de Auteurswet te genieten, is nodig dat het object mede tot stand is gekomen door een (minimum aan) creativiteit, zodat sprake is van een nieuwe en oorspronkelijke schepping. Teneinde te kunnen beoordelen of zulks het geval is zal eiseres in de gelegenheid worden gesteld het desbetreffende programma in het geding te brengen. Daarna zal aan een of meer deskundigen de vraag moeten worden voorgelegd of i.c. sprake is van een ‘schepping’.

RB AMSTERDAM, K.G. 8 OKTOBER 1982, APPLE - cab i, bie 1983, 100

Gedaagde schept nodeloos verwarringsgevaar, zowel met betrekking tot de uiterlijke vormgeving als met betrekking tot de programmatuur en bijbehorende manuals, die getrouwe kopieën vormen van de produkten van eiseressen. Gedaagde handelt derhalve onrechtmatig jegens alle - bij het op de markt brengen van de Apple II betrokken - eiseressen. De omstreden vraag met betrekking tot auteursrecht op de programmatuur behoeft hierbij geen beantwoording; overeenstemming tussen de merken Apolo II en Apple II.

RB AMSTERDAM, K.G. 24 MAART 1983, APPLE - cab ii, bie 1983, 101, CR 1984/3

Alhoewel het bepaald niet onwaarschijnlijk lijkt dat de bodemrechter een computerprogramma, van welk type dan ook en in welke ‘taal’ ook genoteerd, met een voldoende oorspronkelijk karakter zal beschouwen als een werk in de zin van de Auteurswet 1912, zijn Wij van oordeel dat hierop niet in dit kort geding vooruit behoort te worden gelopen.

HOF AMSTERDAM, 13 APRIL 1989, LENSEN - AUTOMATISERINGSBUREAU PALM, CR 1989/4

Het hof acht voorts door geïmiteerden voorshands voldoende aannemelijk gemaakt dat de door hen (naar het hof begrijpt: incidenteel) aangebrachte

correcties in programmatuur telkens uitsluitend ten behoeve en in opdracht van de desbetreffende individuele afnemer van de programmatuur zijn gemaakt, zodat dit corrigeren, zo dit al als een verveelvoudiging valt te kwalificeren - hetgeen het hof nadrukkelijk in het midden laat - in elk geval als een krachtens de Auteurswet toegelaten vorm van verveelvoudiging voor eigen gebruik van de klant-licentiehouder (of in diens opdracht geschied) kan worden gezien. (De in deze uitspraak op art. 16b Aw toelaatbaar geachte 'third-party maintenance' is, met de uitsluiting van dit artikel voor software, thans gewijzigd. In beginsel kan TPM toelaatbaar zijn op grond van art. 45j Aw - het recht om fouten te verbeteren - tenzij dit recht te dien aanzien contractueel zou zijn beperkt.)

RB AMSTERDAM, K.G. 24 FEBRUARI 1992, SCHOTT E.A. - STEMRA E.A., bie 1994, 83
De stelling dat het slechts gaat om zogenaamde sound sampling waarbij geen inbreuk op het auteursrecht zou zijn gemaakt, wordt verworpen; immers het gaat niet om een flits maar om een totale, zij het gewijzigde kopie van het oorspronkelijke muziekwerk.

RB DEN HAAG, 27 MEI 1992, GORTER/DE VRIES - ptt POST, bie 1993, 61, CR 1993/1
Gezien taak van eisers bij gedaagde sub 1, is gedaagde als maker van de definitiestudie en het daarop gebaseerde ontwerp computerprogramma te beschouwen en bezit tevens persoonlijksheidsrechten van de maker.

RB UTRECHT, K.G. 26 NOVEMBER 1992, KOMAR - HIJ MANNENMODE, bie 1994, 75
Indien het werk is ontworpen door personen in dienst van of in opdracht van degene, die het auteursrecht inroept, dan dient de vraag aan wie het auteursrecht toekomt te worden bepaald door het recht dat op de arbeidsverhouding van toepassing is.

HOF DEN BOSCH, 19 MEI 1993, TEXTIELFABRIEK HATEFA - KWANTUM NEDERLAND, bie 1994, 117
Overdracht auteursrecht op kelim-dessin aan Hatefa op grond van brief van ontwerper; op het door Hatefa geopenbaarde bloemendessin heeft Hatefa het auteursrecht; inbreuk aangenomen.

HOF DEN HAAG, VOMAR - BULL, 27 MEI 1993, CR 1993/4
Opzegging van de licentieovereenkomst is reeds gerechtvaardigd nu Vomar in strijd met de overeenkomst de broncode van de programmatuur aan een derde heeft afgegeven ten behoeve van een proefconversie. Art. 85 EG-Verdrag heeft geen betrekking op de verplichting om de broncode geheim te houden en niet aan derden te openbaren.

RB AMSTERDAM, K.G. 18 NOVEMBER 1993, CR 1994/3, NT A.P. MEIJBOOM
De gebruikersinterface van een computerprogramma is voor het auteursrecht geen zelfstandig beschermbaar werk, maar een onlosmakelijk onderdeel van het computerprogramma zelf.

HOF DEN BOSCH, 7 FEBRUARI 1994, nj 1994, 616, bie 1994, 116, CR 1994/2, NT E.P.M. THOLE
De curator is, bij gebreke van andersluidende afspraken, in beginsel niet verplicht het gebruiksrecht op de zgn. broncode gratis aan de afnemers van de programmatuur ter beschikking te stellen. Dit kan anders zijn wanneer het gaat om programmatuur die speciaal ten behoeve van een bepaalde afnemer is ontwikkeld, omdat in zo'n geval de afnemer doorgaans de ontwikkeling volledig zal hebben gefinancierd en de unieke programmatuur geen commerciële waarde zal hebben.

HOF AMSTERDAM, 3 MAART 1994, INFORMATIERECHT/ami 1995/3
Auteursrechtelijke bescherming TV-plot of concept

RB ARNHEM, K.G. 24 JANUARI 1995, CR 1995/2
Het pre-loaden van standaardprogrammatuur op de harde schijf van computers is auteursrechtelijk relevante verveelvoudiging.

RB BREDA, K.G. 20 FEBRUARI 1995, DE WILD - VAN GENK II, CR 1995/2, NT A.P. MEIJBOOM
Afgifte van broncode dient in beginsel te geschieden in digitale, voor de computer leesbare vorm.

HOF DEN HAAG, 2 MAART 1995, CR 1995/4
Converteren van software (i.c. omzetten van financieel softwarepakket van programmacode Basic naar C.) is geen verveelvoudiging die noodzakelijk is voor de met dat werk beoogde gebruik zoals bedoeld in art. 45j Auteurswet. Inbreuk op auteursrechten.

RB 'S-GRAVENHAGE, 7 JUNI 1995, CR 1995/6
Geoordeeld moet derhalve worden dat sedert 1 september 1994 voor computerprogrammatuur een auteursrechtelijk beschermingsregiem van kracht is dat slechts communautaire uitputting kent. Novell kan zich derhalve tegen de parallelimport door America Direct van de door Novell zelf in de VS in het verkeer gebrachte programma's verzetten.

Hr 21 JUNI 1996, DE WILD - VAN GENK, RVDW 1996, 145, CR 1996/5, NT A.P. MEIJBOOM
Bevel tot afgifte van broncode voor maatwerkprogrammatuur die specifiek voor opdrachtgever geschreven is en waarvoor de opdrachtgever de ontwik-

keling volledig betaald heeft. Op grond van de tussen partijen gesloten overeenkomst is de maatwerk programmatuur volledig eigendom van de afnemer. Dit omvat mede het gebruiksrecht op de daarmee samenhangende documentatie en de broncode. Het eventueel door derden aanbrengen van wijzigingen in de programmatuur is niet in strijd met het auteursrecht

4.6 Literatuur

- Flamée, M., 'Octrooieerbaarheid van software', (diss.), Brussel, 1985.
- Hanneman, H.W.A.M., 'The patentability of computer software', (diss.), Utrecht, 1985.
- Hugenholtz, P.B. en J.H. Spoor, 'Auteursrecht op software', Otto Cramwinckel, Amsterdam, 1987.
- Quaedvlieg, A.A., 'Auteursrecht op techniek', (diss.) W.E.J. Tjeenk Willink, Nijmegen / Zwolle, 1987.
- Schelven, P.C. van en H. Struik, 'Softwarerecht', Kluwer, Deventer, 1995.
- Schelven, P.C. van, 'Bescherming van software en chips in juridisch perspectief', Vermande, Lelystad, 1986.
- Vandenberghe, G.P.V., 'Software - Orakels', Kluwer, Deventer, 1985.
- Vandenberghe, G.P.V., 'Bescherming van computersoftware', (diss.), Kluwer, Deventer / Antwerpen, 1984.
- Verkade, D.W.F., 'Juridische bescherming van programmatuur', Samsom, Alphen aan den Rijn / Brussel, 1985.

5 Auteursrechtelijke aspecten van databanken en multimedia

Mutimedia-applicaties staan in een toenemende belangstelling. In het onderwijs, bij bibliotheken, in onderzoek en amusement wordt steeds vaker gebruik gemaakt van CD-ROM en CD-I met een mengeling van tekst, geluid en beeldmateriaal. Op het eerste gezicht lijkt het dat multimedia-applicaties geen bijzondere rechtsvragen in het leven roepen. Tenslotte is juist ter bescherming van dit soort materiaal het auteursrecht gecreëerd. De problematiek ligt dan ook niet in de vraag of in multimedia-applicaties vastgelegd materiaal voor bescherming door het auteursrecht in aanmerking komt, maar komt voort uit de vorm waarin het is vastgelegd. Het uniforme, digitale formaat van computergegevens maakt de band tussen informatietypen en de traditioneel daarmee geassocieerde media en voorwerpen steeds losser, met als gevolg dat regulering van informatie zich steeds minder eenduidig laat formuleren. Daarnaast creëren de tengevolge van dit digitale formaat toegenomen mogelijkheden tot manipulatie van data en tot eenvoudige en perfecte reproduktie, in combinatie met wereldwijde verspreidingsmogelijkheden zoals internet, problemen van logistieke aard en beheersbaarheid.

Omdat we veel verzamelwerken tegenkomen in multimediale vorm, waarbij zich bovendien een aantal gelijksoortige auteursrechtelijke vragen aandienen, worden databanken en multimedia hier samen behandeld.

Hieronder worden achtereenvolgens besproken:
- multimedia (5.1), digitale informatie (5.1.1), logistieke c.q. distributie-problemen (5.1.2) en cumulatie van regimes (5.1.3);
- databanken (5.2), bulletin board systemen (5.2.1) en internet (5.2.2);
- de aanleg van databanken (5.3);
- de exploitatie van databanken (5.4).

5.1 Multimedia

Onder multimedia wordt verstaan de integratie van tekst, geluid en beeld binnen hetzelfde medium. Van Dale definieert de term 'medium' als: "middel, instrument om informatie openbaar te maken (b.v. krant, radio, televisie)". Globaal genomen kan men stellen dat voorheen ieder van deze drie 'informatietypen' gebonden was aan een bepaald medium, met een daaraan eigen - analoge - vorm (waarbij overigens tot op zekere hoogte een parallel valt op te merken met de door Van Dale genoemde *communicatie*media):
- tekst, in de vorm van lettertekens; bijvoorbeeld boek, tijdschrift of krant;
- geluid, bijvoorbeeld in de vorm van elektromagnetische signalen; LP, muziekcassette of radio;
- beeld, in de vorm van punten of beeldlijnen; foto, film of televisie.

Gebruikelijk genoemde media voor multimedia-applicaties zijn CD-ROM (Compact Disk-Read Only Memory) en CD-I (Compact Disk-Interactief).

Een *CD-ROM* is een CD zoals we die kennen van de muziek-CD-speler, maar dan voor gebruik in combinatie met computers. Met 'read only memory' wordt bedoeld dat computers dit extern geheugenmedium - anders dan bij een floppy disk, die zowel 'gelezen' als opnieuw 'beschreven' kan worden - alleen kunnen gebruiken om de daarop vastgelegde data te 'lezen' en niet opnieuw kunnen 'beschrijven' met gewijzigde data. Wel bestaan er CD-schrijvers waarmee data op 'lege' CD's kunnen worden vastgelegd. *CD-I's* worden gebruikt in CD-I-spelers in combinatie met een televisietoestel.

Dat in computers de verschillende informatietypen kunnen samenkomen, komt voort uit het feit dat de *vorm* waarin gegevens in computers worden opgeslagen voor alledrie de typen hetzelfde is, namelijk digitaal.

5.1.1 Digitale informatie

We zijn gewoon dat verschillende 'typen' informatie op verschillende media worden vastgelegd. Een foto drukken we af op papier, een film leggen we vast op celluloid, een schilderij op linnen en een computerprogramma in

magnetische patronen op een floppy disk. Voorts schrijven we het verschil in 'typen' informatie nog toe aan de vorm waarin het is vastgelegd: papier met analoge schrifttekens noemen we een leesboek, een enkel beeld een foto, een aaneenschakeling van beelden een film. En vaak is de kwalificatie van het type informatie ook opgehangen aan het voorwerp waarmee het is vervaardigd: uit een fototoestel komt een (papieren) foto, uit een super 8 camera een (celluloid) film.

We zien ook dat wettelijke regelingen sterk verbonden zijn met de hier genoemde onderscheiden. Zo bevat de Auteurswet 1912 naast algemene bepalingen ook specifieke bepalingen omtrent bijvoorbeeld boeken, muziekwerken, film en foto, software en geschriften. We kennen specifieke bepalingen voor kranten, radio en televisie. Een ander voorbeeld treffen we aan als we kijken naar de omroep- en telecommunicatiewetgeving. Op de informatie omtrent de aankomst- en vertrektijden van Schiphol via teletekst is de Mediawet van toepassing, terwijl dezelfde informatie, geraadpleegd door middel van internet, onderworpen is aan de Wet op de Telecommunicatievoorziening.

Onder invloed van de voortschrijdende technologie, zoals de convergentie van traditionele media en technieken, blijken in wetgeving gehanteerde termen hun onderscheidend karakter te verliezen. We wisten en weten allemaal wat een boek is, maar is het manuscript, vastgelegd op floppy disk, nu ook een boek? We zijn het erover eens dat beide vormen hetzelfde werk in de zin van de Auteurswet 1912 belichamen. De term boek lijkt aan eenduidige (juridisch relevante) betekenis te verliezen.

Ook is een boek een geschrift. Onder geschrift wordt gebruikelijk begrepen: drager van verstaanbare leestekens. Het zou onzinnig zijn om het manuscript op floppy disk een geringere mate van bescherming toe te kennen dan het papieren boek. Bovendien is een floppy disk evenzeer te beschouwen als een drager van verstaanbare leestekens. Dat we daarvoor een computer nodig hebben, doet daar niets aan af. Het gebruik van hulpmiddelen kennen we net zo goed bij foto's, film en muziek. In de jurisprudentie is een ponskaart (zeg maar de voorloper van de floppy disk) als 'geschrift' gekwalificeerd (Hof Amsterdam (Strafkamer), 18 februari 1972, NJ 1972, 210, zij het i.c. niet in de zin van art. 321 Sr (valsheid in geschrifte), omdat de betreffende ponskaart geen bewijsbestemming had). Het manuscript op floppy disk is derhalve te kwalificeren als geschrift.

Computerprogramma's zijn als aparte entiteit inmiddels expliciet opgenomen in de Auteurswet 1912. Evenals boeken, die kunnen zijn vastgelegd in analoge vorm (op papier) en in digitale vorm (op floppy disk), kennen computerprogramma's verschillende verschijningsvormen. Naast de digitale verschijningsvorm kunnen zij worden uitgeprint op papier (in analoge vorm). Vòòr de wijziging van de Auteurswet 1912 werd vrij algemeen verondersteld

dat computerprogramma's - in gelijk welke vorm - te beschouwen zijn als geschriften. Na de wetswijziging zijn computerprogramma's echter uitgesloten van de geschriftenbescherming. Het verschil in beschermingsregime tussen boeken en computerprogramma's kan niet worden verklaard door een verschil in verschijningsvorm. Er is immers in verschijningsvorm geen verschil tussen een papieren versie van een boek en de print out van een computerprogramma, noch tussen de digitale versie van een computerprogramma en die van een manuscript. Als het dan niet het 'uiterlijk' is, de vorm, kan het dan wellicht de functie zijn, de werking.

Qua functie worden computerprogramma's wel gedefinieerd als

> *een verzameling instructies die bestemd zijn om een informatieverwerkende machine een bepaalde functie te laten uitvoeren.*

Dit echter, lijkt een onwerkbaar onderscheid. Zo kennen we informatieverwerkende systemen die data verzamelen. Worden er data van een bepaalde aard, dan wel bepaalde omvang waargenomen (de hoeveelheid smog in het Rijnmondgebied bijvoorbeeld), dan dienen deze data ter instructie aan het informatieverwerkende systeem om de alarmfase in te schakelen. Volgens de hierboven weergegeven definitie zouden bedoelde data dan onderdeel van het computerprogramma zijn (of worden?). De onwerkbaarheid van een dergelijk onderscheid zal de informaticus duidelijker zijn dan de jurist, maar in feite fungeren alle data in een informatieverwerkend systeem als instructie om handelingen te verrichten.

Hetgeen in de vorige alinea's is besproken, dient ter opmaat van de stelling dat van informatietechnologie geen impuls uitgaat tot nadere detaillering van wetgeving. Integendeel, omdat de voorheen zo helder gehanteerde begrippenkaders bij nadere bestudering niet meer zo vanzelfsprekend zijn, ligt het meer in de rede bestaande verbijzonderingen aan een nadere analyse te onderwerpen en wetgeving zo mogelijk te vereenvoudigen. Multimedia-applicaties zouden wel eens de ceasuur kunnen worden in de tot heden gevolgde tendens tot verdere explicitering van entiteiten in wetgeving.

Laten we daarvoor nog eens kijken naar de aard van multimedia-applicaties. De term multimedia doelt op de situatie dat informatietypen - tekst, geluid en beeld - die voorheen op gescheiden media in een daarvoor vereiste vorm waren vastgelegd, tegenwoordig in een en hetzelfde medium verenigd kunnen worden. Dit is mogelijk dankzij de vorm waarin informatietypen op computermedia worden vastgelegd en binnen computers worden verwerkt. Deze vorm, enen en nullen, wel stroom en geen stroom, is nu juist voor alle 'typen' informatie gelijk. In dit verband wordt wel gesproken van 'digitale informatie'. Kenmerkend aan digitale informatie is niet zozeer wat die

informatie representeert, doch veeleer de eenvoud en de snelheid waarmee informatie kan worden samengevoegd, overgenomen, bewerkt en getransporteerd. Hier lijkt dus geen reden tot nadere verbijzondering in wetgeving op grond van de gedachte dat er een *nieuwe categorie* van werken zou zijn ontstaan. Het digitale karakter veroorzaakt andere problemen, die vooral in de sfeer liggen van de beheersbaarheid van informatie.

5.1.2 Logistieke c.q. distributieproblemen

Internet is wel ‘s werelds grootste kopieermachine genoemd. Alhoewel we hebben geconstateerd dat er een juridisch beschermingsregime op multimedia-applicaties van toepassing is, zouden niettemin het auteursrecht, het contractenrecht en licentieverleningen in de praktijk wel eens ontoereikend kunnen blijken voor een daadwerkelijke en effectieve bescherming. De oorzaak hiervan is gelegen in het digitale formaat van de data, waardoor het mogelijk is gegevens perfect, eenvoudig en met weinig kosten te kopiëren en desgewenst te modificeren, in combinatie met wereldwijde verspreidingsmogelijkheden tengevolge van bijvoorbeeld internet.

De logistieke problemen lijken op dit moment het grootste obstakel te vormen voor de gegevensverwerkende industrie. Dit geldt de *samenstelling* van multimedia-applicaties en van databanken - in de zin dat het voor de samensteller vaak ondoenlijk zal blijken de auteursrechthebbende op bepaalde informatie te achterhalen - alswel de *distributie* daarvan, in de zin dat het voor de exploitant haast ondoenlijk lijkt controle over de distributie te behouden. In Wired van maart 1994 merkte Barlow hierover op: ‘If our property can be infinitely reproduced and instaneously distributed all over the planet without cost, without its leaving our possession, how can we protect it?’. In dezelfde zin ook Dommering, in Computerrecht 1994/3: ‘Het auteursrecht spoelt weg door het elektronisch vergiet’. Het is de verwachting dat voor de effectiviteit van bescherming vooral technische maatregelen nodig zullen zijn.

5.1.3 Cumulatie van regimes

Een probleem dat we onder de huidige diversificatie van regelgeving bovendien ontmoeten bij de samenvoeging van verschillende informatietypen binnen hetzelfde medium, is de cumulatie van verschillende beschermingsregimes. Zoals we ons hierboven terecht afvroegen of het wel verstandig was verschil aan te brengen in computerdata, zo zien we dit eens te meer terug keren bij multimedia-applicaties.

De combinatie van verschillende informatietypen binnen een multimedia-applicatie roept een aantal vragen op. Zou een foto, genomen met een digitale

camera, anders behandeld moeten worden dan een traditionele foto. Dient, vervolgens, die 'foto', vastgelegd op CD-ROM, anders behandeld te worden dan een daarop vastgelegde 'video'? Zouden we uit die verzameling microscopisch kleine putjes op de CD, die putjes eruit moeten halen die we qua functionaliteit 'computerprogramma' noemen? Is de toepassing van het op traditionele afbakeningen gebaseerde auteursrecht nog toereikend, waar thans ook rekening moet worden gehouden met het digitale karakter waarin de informatie is opgeslagen; is het beschermingsregime ook daarvoor voldoende? Of zou het beter zijn om onder het 'digitale informatierecht' een beschermingsregime te creëren dat voor alle digitale informatie in een bepaald werk gelijk is, ongeacht wat de digitale informatie representeert?

De huidige diversificatie in het auteursrecht heeft zinvol een functie kunnen vervullen, omdat het technisch medium mede bepalend was voor de beheersbaarheid van het werk. In een omgeving van multimedia en internet verliezen traditioneel gecategoriseerde werken aan beheersbaarheid. Het gevolg is dat een complex systeem van regels resteert, met weinig uitzicht op effectiviteit, dat bovendien als een zware deken de bewegingsvrijheid binnen de informatieproduktie belemmert.

Indien en voor zover multimedia en internet aanleiding geven tot nadere bijstelling in wet- en regelgeving, bijvoorbeeld de Auteurswet 1912, zou dat niet meer (sec) op de techniek gebaseerd moeten worden. Medium, vorm en voorwerp zijn voor de verschillende informatietypen steeds meer inwisselbaar geworden. Een nadere definiëring in termen van functionaliteit van de informatie lijkt evenmin hanteerbaar. Het uitgangspunt zou moeten zijn het verschil in maatschappelijke functie van het informatieprodukt, zoals dat wordt gepresenteerd door de aanbieder daarvan, met de door hem bedoelde, daaraan verbonden functie. Doel van een dergelijke benadering is rechthebbenden juridische bescherming te bieden tegen inbreuken die rechtstreeks raken aan (de exploitatie van) het betreffende informatieprodukt, zonder anderen daarbij onnodig te belemmeren in wenselijk (her)gebruik van delen van het informatieprodukt, voor zover het door deze derden beoogd (her)gebruik gericht is op een andere maatschappelijke functie.

Wat kan men verstaan onder de maatschappelijke functie van het werk? De maatschappelijke functie van een computerprogramma in objectcode bijvoorbeeld is een andere dan die van de listing van datzelfde computerprogramma in een computervakblad. Zo op het oog verzet niets zich ertegen (voor wat betreft de belangen van de maker; anders ligt dat wellicht ten aanzien van de belangen van de uitgever van het tijdschrift) indien deze listing door derden wordt overgenomen (in een ander tijdschrift bijvoorbeeld). Wat die derde echter niet zal mogen doen, is die listing omzetten in binaire code en vervolgens een (nagenoeg) gelijk computerprogramma op de markt brengen.

Evenzo zou de (on)rechtmatigheid van het overnemen van delen van een CD-ROM kunnen worden beoordeeld aan de hand van de vraag of met die overname inbreuk plaats vindt op het als zodanig met die CD-ROM gerepresenteerde werk. Het is voorstelbaar, dat de overname van een plaatje uit een CD-ROM-encyclopedie, bijvoorbeeld met de bedoeling dat plaatje te gebruiken als illustratie bij een artikel, geen inbreuk oplevert op het auteursrecht op de CD-ROM-encyclopedie (en evenmin op een eventueel auteursrecht van een derde, indien het gebruik van het plaatje onder een toegelaten uitzondering zou vallen), maar weer wel indien dat plaatje gebruikt zou worden in een andere encyclopedie.

Een voortzetting van de huidige tendens van een steeds meer omvattend beschermingsregime onder afnemende beheersbaarheidsmogelijkheden, draagt het risico in zich op den duur contra-produktief te worden, niet slechts in relatie tot een meer algemeen maatschappelijk belang, doch uiteindelijk ook ten opzichte van informatieproducenten. De introductie van maatschappelijke functie als criterium ter beoordeling van auteursrecht inbreuken zou voorts zorgen voor een verminderde noodzaak tot verdere verbijzondering binnen het intellectueel eigendomsrecht en voor een evenwichtiger regeling die minder dan thans tegenstrijdigheden zou opwerpen. Nieuw is deze gedachte overigens niet. Immers, aan een groot aantal van de onder het auteursrecht opgenomen handelingen die niet als inbreuk op het auteursrecht worden beschouwd, liggen dit soort opvattingen ten grondslag. In andere auteursrechtstelsels, zoals dat van de VS, kent men een daarmee verwant beginsel, dat van de ‘fair use’. Slechts de gekozen methode, om wenselijk geachte inbreuken niet meer zelfstandig in de wet te regelen doch bij voorkeur onder een meer algemeen toepasbare norm, zou men ten aanzien van het Nederlandse auteursrecht nieuw kunnen noemen.

5.2 Databanken

In de EU-richtlijn van 11 maart 1996 betreffende de rechtsbescherming van databanken wordt in art. 1 lid 2 onder ‘databank’ verstaan:

> *een verzameling van werken, gegevens of andere zelfstandige elementen, systematisch of methodisch geordend, en afzonderlijk met elektronische middelen of anderszins toegankelijk.*

Wat opvalt is, dat deze definitie ook niet-elektronische gegevensbestanden omvat. In een tijd waarin ‘scanners’ (optische lezers die de informatie vastleggen op elektronische informatiedragers) het mogelijk maken met betrekkelijke eenvoud omvangrijke tekstbestanden om te zetten van papier naar digitale vorm, bovendien zodanig dat de informatie als tekst, dan wel als

plaatje te bewerken valt, is een dergelijke keuze goed te begrijpen. In dit hoofdstuk zal steeds worden uitgegaan van die elektronische toegankelijkheid.

Databanken worden aangelegd voor gebruik binnen de eigen organisatie - interne databanken - of voor (mede) gebruik door derden - externe databanken. Raadpleging van openbare databanken geschiedt gratis of tegen een vergoeding, bijvoorbeeld gebaseerd op een abonnement of op de verbruikte tijd.

In Nederland zijn inmiddels enkele honderden externe databanken, aangelegd door Nederlandse organisaties of waaraan door Nederlandse organisaties is meegewerkt, on-line beschikbaar over uiteenlopende onderwerpen. Een willekeurige greep: dienstregelingen en tarieven van luchtvaartmaatschappijen; aanbod van gebruikte auto's; handelsinformatie; beleggingsadviezen; informatie over bladmuziek; bibliothekenbestanden; medische informatie; beursinformatie; scheepsbeschrijvingen; sexcontacten; toeristeninformatie, tropische landbouw; tijdschriftteksten; subsidieregelingen; milieuregelingen; artikelsamenvattingen over biomedisch onderzoek; socio-economische marktsegmentering per gezinstype; encyclopedie.

Bij het communicatieproces door middel van databanken is een aantal partijen betrokken:
1. De maker van de databank;
2. De exploitant van de databank: de databankuitgever of databasepublisher;
3. De auteur van de teksten en andere informatie die in databanken opgeslagen liggen of de auteursrechthebbende daarop;
4. De afnemers van de databank;
5. De leverancier van de communicatieverbindingen tussen databank en afnemer.

Databanken kunnen op verschillende manieren toegankelijk zijn:
- de databankexploitant levert de bestanden op informatiedragers, bijvoorbeeld een encyclopedie op CD-ROM of CD-I (off-line databanken);
- rechtstreeks, door middel van een telefoonverbinding, of via internet, bijvoorbeeld de catalogi van bibliotheken (on-line databanken);
- de gebruiker kan een zoekopdracht opgeven aan de databankexploitant, waarna deze de gevonden gegevens, afgedrukt op papier, vastgelegd op een informatiedrager of via email, naar de gebruiker toezendt (delivery service).

5.2.1 Bulletin board systemen

Een meer bekende vorm van databanken is het bulletin board, een soort 'elektronisch mededelingenbord'. De belangrijkste toepassingen zijn wel

electronic mail (elektronische post of email), discussie platforms en de uitwisseling van software en computerbestanden. In de meest eenvoudige uitvoering bestaat een bulletin board system (BBS) uit een PC die door middel van een modem aan het telefoonnet is verbonden. Met behulp van algemene communicatiesoftware kunnen gebruikers vanaf hun eigen PC (met modem) van de diensten van het BBS gebruik maken.

Bulletin board systems (BBSs) worden zowel door particulieren als door organisaties aangelegd en beheerd. In Nederland zijn er zo'n 400 BBSs; voor de VS wordt het aantal BBSs geschat op circa 150.000. Particuliere BBSs worden veelal aangelegd ten behoeve van idealistische doelstellingen, of voor de lol, rondom een onderwerp waarin de beheerder zelf geïnteresseerd is. Het bedrijfsleven schijnt het BBS ontdekt te hebben als een eenvoudige, doeltreffende en goedkope manier van aanvullende dienstverlening. Zo zien we dat veel computerleveranciers een BBS gebruiken ter ondersteuning van hun software releases, bijvoorbeeld door nieuwe printer drivers beschikbaar te stellen en allerlei tips voor de oplossing van in de praktijk gesignaleerde problemen met de software.

Veel BBSs zijn aangesloten bij een organisatie die het hen mogelijk maakt deel uit te maken van een wereldwijd netwerk van BBSs. Anders dan bij internet zijn dit in het algemeen geen permanente verbindingen. Een BBS maakt periodiek een verbinding met een andere BBS om data uit wisselen, welk BBS op zijn beurt weer een verbinding maakt met een of meer andere BBSs.

Internet is niet zonder gevolgen gebleven voor BBSs. Veel BBS-diensten zijn eveneens beschikbaar via internet. De permanente verbindingen van internet bieden daarbij een groot voordeel. Electronic mail en NetNews (een soort internet bulletin board) zijn sneller; de (internationale) verbindingen vaak goedkoper. De meeste beheerders van BBSs, (ook wel 'system operator' of 'sysop' genoemd) maken hun BBS tegenwoordig eveneens toegankelijk via internet.

5.2.2 Internet

In een overzicht van multimedia wordt veelal ook 'internet' genoemd. Internet is echter geen medium, evenmin als dat het een computersysteem of één computernetwerk is. In oorsprong weliswaar opgezet als een netwerk van computers (ten behoeve van het Amerikaanse Ministerie van Defensie om de kwetsbaarheid van de informatievoorziening te beperken) kan internet in feite beter beschouwd worden als een communicatie-protocol. Op basis van het internet-protocol worden computers met elkaar verbonden, door middel van een 'netwerk' van gewone telefoonlijnen, huurlijnen, glasvezelkabels en satellietverbindingen.

Hoewel er natuurlijk fysiek sprake is van gebruik van kabel- en andere verbindingen, is het toch minder juist om 'het internet' als een fysiek netwerk te beschouwen, gelet op het willekeurige gebruik van deze verbindingen, waarover bovendien nog verschillende andere toepassingen plaats vinden, zoals de gewone telefoon en televisie. De reden waarom internet in dit verband vaak genoemd wordt, is omdat het informatie-aanbod via internet veelal in multimediale vorm is.

Computers die internet-dienstverlening verzorgen staan permanent met elkaar in verbinding. Email en nieuwsgroepen (de internet benaming voor discussie-platforms) zijn sneller, betrouwbaarder en continue internationaal toegankelijk. Dit betekent dat gebruikers via internet op ieder moment en op elk tijdstip boodschappen en bestanden kunnen verzenden of binnenhalen. Voor bedrijven heeft dit als voordeel dat zij niet meer in ieder land een BBS hoeven op te starten. Eén internet site is voldoende.

World Wide Web (WWW) is een software-techniek die het mogelijk maakt in de informatie allerlei verwijzingen naar informatie op andere plaatsen op te nemen. Met een muisklik kan de gebruiker vervolgens van document tot document 'springen'. Dat de betreffende informatie op verschillende computers kan staan, zelfs in verschillende landen, is iets waar de gebruiker niet naar hoeft om te zien.

5.2.3 Afbakening

Een nauwkeurige afbakening tussen de termen databank, bulletin board en internet is niet eenvoudig, deels omdat het - weliswaar verwante maar - ongelijksoortige grootheden zijn. De term databank kan beschouwd worden als een algemene benaming voor systematisch toegankelijke gegevensbestanden, gegroepeerd rondom een bepaald onderwerp. Ook wordt de term wel in engere zin gehanteerd, namelijk dat de gegevens in databanken volgens een vooraf bepaalde structuur (records en velden) moeten zijn ingedeeld. Een BBS is dan wel een databank in de eerste betekenis, voor zover de data rondom een bepaald onderwerp zijn gegroepeerd, maar niet meer voor wat betreft bijvoorbeeld de email functie. Vanwege de veelal vrijere structuur van een BBS - men kan files in allerlei formaten (bijvoorbeeld WordPerfect-formaat of MS Word for Windows-formaat) downloaden - zou een BBS weer geen databank zijn in de tweede betekenis.

Internet is, zoals gezegd, geen databank, maar veeleer een communicatie-protocol voor de uitwisseling van data via een fysiek niet nader afgebakend 'netwerk'. Voor de toegang tot internet dienen gebruikers een aansluiting te hebben met een van de computers die permanent internetcommunicatie verzorgen. Deze dienstverlening wordt aangeboden door zogenoemde 'access

providers', ondernemingen die hun computer permanent in verbinding houden met die van andere access providers. Vaak verzorgen access providers aanvullende dienstverlening op internet. Zij stellen bijvoorbeeld ruimte ter beschikking op hun computersystemen waar hun klanten, als zij dat willen, zich kunnen presenteren (de zogenoemde 'home page'). In dat geval worden access providers tevens 'service providers', hetgeen wellicht consequenties kan hebben voor hun juridische positie (bijvoorbeeld dat zij ten aanzien van het materiaal van hun klanten eerder verantwoordelijk gehouden kunnen worden voor eventuele inbreuken op auteursrechten, voor kinderpornografische afbeeldingen of voor racistische uitspraken.)

Een relatie tussen internet enerzijds en databanken en BBSs anderzijds is dat de laatste voor de uitwisseling van informatie gebruik (kunnen) maken van internet. Een organisatie die binnen een internetomgeving het beheer voert over een bepaalde dienst is vergelijkbaar met een sysop (system operator) van een BBS. De binnen internet gebezigde term daarvoor is die van system administrator of 'sysadmin'.

De relatie met multimedia tenslotte is dat veel informatie-uitwisseling tegenwoordig een multimediaal karakter heeft, hetgeen door de digitale techniek wordt mogelijk gemaakt.

Databanken bestaan uit computerapparatuur, uit het computerprogramma dat de opslag, zoekstructuur en selectie van gegevens verzorgt en het gegevensbestand. Bij auteursrechtelijke aspecten van databanken gaat het om de volgende vragen:

1. Is er voor opname van gegevens in een databank wellicht toestemming nodig van een rechthebbende op die gegevens? (zie paragraaf 5.3)
2. Is de databank zelf beschermd tegen ongewenste overname door derden? (zie paragraaf 5.4)

In dit verband gaat het niet om de vraag of het computerprogramma van de databank auteursrechtelijk beschermd is. Databank-computerprogramma's onderscheiden zich in dit opzicht niet van andere computerprogramma's. Zoals in hoofdstuk 4 besproken, vallen computerprogramma's onder de werking van het auteursrecht indien zij aan de eisen van het werkbegrip voldoen.

5.3 De aanleg van databanken

Het samenstellen van databanken en multimedia-applicaties kan aan juridische beperkingen onderhevig zijn, namelijk indien bij de samenstelling gebruik wordt gemaakt van informatie afkomstig uit bronnen van derden. In deze paragraaf zal de vraag worden behandeld of voor de opname van

materiaal afkomstig van derden, toestemming van die derden is vereist. Daarbij dienen we erop bedacht te zijn dat in de wet geformuleerde toegelaten inbreuken op auteursrechten verschillend kunnen zijn, al naar gelang het gebruik en de aard van het materiaal (tekst, beeld of geluid).

Ten aanzien van de inhoud van databanken kunnen we onderscheiden tussen:
1. Werken waarop auteursrecht kan rusten;
2. Feitelijke gegevens, bijvoorbeeld handelsinformatie, beurskoersen, olieprijzen.

Ad 1. Boeken, tijdschriftartikelen en in het algemeen publikaties zullen veelal voldoen aan de eisen voor een 'werk van letterkunde, wetenschap of kunst', zodat daarop in de meeste gevallen auteursrechten zullen rusten. Op een verwijzing die aan het werk zelf is ontleend, zoals een door de auteur vervaardigd uittreksel of een samenvatting, kan auteursrecht rusten. Indien het abstract door de uitgever (van een databank bijvoorbeeld) is gemaakt, is er doorgaans geen sprake van inbreuk op auteursrechten van de auteur. Dit is alleen anders indien het abstract het karakter krijgt van een bewerking.

Het auteursrecht geeft aan de maker van het werk het uitsluitende recht tot verveelvoudiging en openbaarmaking, de zogenoemde exploitatierechten. Daarnaast kent het auteursrecht de maker een aantal andere rechten toe, de zogenoemde persoonlijkheidsrechten, zoals het recht op naamsvermelding en het recht zich te verzetten tegen wijzigingen of aantastingen van het werk. Persoonlijkheidsrechten zijn niet overdraagbaar. Een uitgever aan wie het auteursrecht op een werk is overgedragen, heeft op grond van de exploitatierechten de bevoegdheid het werk in een databank op te nemen, doch op grond van de persoonlijkheidsrechten kan de maker zich verzetten tegen opname in gewijzigde vorm.

Ad 2. Feitelijke gegevens zijn in beginsel geen object van het auteursrecht. Gegevens*verzamelingen* echter, genieten over het algemeen bescherming van het auteursrecht, hetzij als verzamelwerken met een eigen, oorspronkelijk karakter, hetzij als 'niet-persoonlijke' geschriften. Voor verzamelwerken geldt de bescherming niet alleen het verzamelwerk als zodanig, maar bovendien de afzonderlijke onderdelen waaruit het verzamelwerk is samengesteld.

Bij de komende implementatie van de EU-richtlijn in de Auteurswet 1912 is het te verwachten dat databanken - evenals dat het geval was met software - van het regime van de geschriftenbescherming worden uitgesloten. Ten aanzien van niet-auteursrechtelijk beschermd materiaal in een overigens wel onder de reikwijdte van de richtlijn vallende databank, wordt een extractierecht geïntroduceerd, zodat overname van data uit een databank (elektronisch zowel als papieren!) in beginsel niet toelaatbaar wordt (zie paragraaf 5.4 hierna). Dit gaat veel weg hebben van een tijger die bezig is in zijn eigen staart

te bijten. Immers, voor veel van de samen te stellen databanken zal gelden dat de informatie moet worden verkregen uit andere databank-achtige bronnen.

Op wetten en op rechterlijke uitspraken bestaat geen auteursrecht (Art. 11 Aw). Opname van full-text jurisprudentie maakt dan ook geen inbreuk op auteursrechten. De *verzameling* van *geselecteerde* uitspraken in een jurisprudentiebundel kan als verzamelwerk beschermd zijn. De 'kopjes' boven de uitspraken kunnen als abstracts aangemerkt worden, waarop auteursrecht van de uitgever rust. Titels van boeken zijn ook auteursrechtelijk beschermd, voornamelijk ter voorkoming van plagiaat. Opname van boektitels in een documentatiesysteem wordt in de literatuur toelaatbaar geacht. In het oorspronkelijk ontwerp van de richtlijn werd de maker van een databank het recht toegekend om zonder toestemming bibliografische gegevens, excerpten of citaten op te nemen. Deze expliciete bevoegdheid is in de definitieve tekst van de richtlijn evenwel vervallen.

5.3.1 Toestemming

Voor de beantwoording van de vraag of voor de opname in een databank van auteursrechtelijk beschermd materiaal toestemming van de rechthebbende is vereist, kunnen we nog onderscheiden naar twee fasen:

1. Invoer / opslag (paragraaf 5.3.2)
   Het aanleggen van het gegevensbestand door de maker/databankexploitant en de vastlegging daarvan in de computer;
2. Uitvoer / raadpleging (paragraaf 5.3.3)
   Het proces van selectie en sortering in het werkgeheugen van de computer dat volgt op de zoekopdracht van de gebruiker, de weergave van het resultaat op het beeldscherm en de eventuele vastlegging daarvan op magnetische informatiedragers of op papier.

In de praktijk kan het voorkomen dat er meer partijen bij dit proces zijn betrokken. Een vraag die zich in dat verband aandient is of bij iedere schakel opnieuw sprake is van (verdere) verveelvoudiging en/of openbaarmaking. Een databankexploitant kan zelfstandig het gegevensbestand aanmaken en beheren, of dit uitbesteden aan een computerservicebedrijf. Krijgt deze het gegevensbestand bijvoorbeeld aangeleverd op tape, dan zal het opnieuw worden ingelezen en opgeslagen in diens computersysteem.

Ten aanzien van de fase van raadpleging en uitvoer kan men zich afvragen of de met het selectie- en sorteringsproces gepaard gaande kopieën in het werkgeheugen van de computer als zelfstandige, auteursrechtelijk relevante verveelvoudigingen zijn aan te merken. Algemeen wordt aangenomen dat voor verveelvoudigen tenminste enige duurzame vastlegging vereist is. Gezien

de zeer kortstondige levensduur voldoen deze kopieën niet aan dit criterium. Niettemin wordt in de richtlijn in art. 5 - handelingen waarvoor toestemming nodig is - sub a gesproken van 'de permanente of tijdelijke reproduktie'. Deze bepaling ziet weliswaar op toepassing in de relatie databankmaker - databankgebruiker, doch waar hierin sprake lijkt te zijn van een sterk op techniek leunend verveelvoudigingsbegrip, zou men dit begrip evenzogoed kunnen doortrekken naar de relatie databankmaker - rechthebbende (op de betreffende data). Dat zou dan betekenen, dat de toestemming van de rechthebbende aan de databankmaker zich mede dient uit te strekken tot het 'gebruik' van de data door de databankafnemer. In het licht van het betoog onder paragraaf 4.3, softwarebescherming, en onder paragraaf 5.1, is het wel jammer dat wederom voor zo'n op techniek gebaseerd criterium lijkt te worden gekozen. Voor gebruikers van on-line databanken is tussen deze fasen eigenlijk geen verschil waarneembaar.

5.3.2 Invoer / opslag

De invoer van het gegevensbestand, het aanmaken van een tape bijvoorbeeld, wordt algemeen beschouwd als een vorm van verveelvoudiging. Toestemming van de auteursrechthebbende is nodig indien deze verveelvoudiging niet onder een van de toelaatbare uitzonderingen valt.

De exceptie van art. 16b Aw, de verveelvoudiging voor eigen oefening, studie of gebruik, zal slechts voor een aantal databanken van toepassing kunnen zijn. De overname van werken als bedoeld bij art. 10 lid 1 sub 1 (boeken, brochures, nieuwsbladen, tijdschriften en alle andere geschriften), dient bovendien beperkt te blijven tot een klein gedeelte van het werk, behalve indien het betreft werken waarvan geen exemplaren meer verschijnen of tot korte artikelen in dag-, nieuws-, of weekbladen en tijdschriften.

Art. 17 kan beschouwd worden als een verruiming van de bevoegdheden van art. 16b voor *organisaties,* tot verveelvoudiging van de in art. 10 lid 1 sub 1 bedoelde werken, voor zover het betreft werken van wetenschap, waarbij de verveelvoudigingen nog steeds beperkt dienen te blijven tot een klein gedeelte, onder de verplichting tot het betalen van een billijke vergoeding en met een beperking aan het aantal exemplaren tot zoveel als binnen de organisatie nodig is.

Hoewel als hoofdregel geldt dat invoer van gegevens een verveelvoudiging is, zal op basis van bovenstaande uitzonderingen voor de aanleg van veel interne databanken geen toestemming van de auteursrechthebbende vereist zijn. In het geval van externe databanken daarentegen zal de - veelal commerciële - exploitatie niet verenigbaar zijn met de eigen gebruik exceptie van art. 16b, noch met die van art. 17 Aw.

Vastlegging van het gegevensbestand in de databankcomputer gaat wederom gepaard met het maken van een verveelvoudiging. Op deze tweede verveelvoudiging is gelijke argumentatie van toepassing als hierboven. Maar met de vastlegging in een *on-line* databankcomputer komt het gegevensbestand bovendien ter beschikking van de gebruikers, zodat hier de vraag rijst of vastlegging tevens als openbaarmaking te beschouwen valt. Alhoewel reeds voor invoer toestemming van de auteursrechthebbende benodigd kan zijn, geeft Hugenholtz (Auteursrecht en information retrieval) als motivering voor een separate bespreking onder meer de mogelijkheid dat invoer van het gegevensbestand een toelaatbare uitzondering op het verveelvoudigingsrecht zou kunnen zijn, doch niettemin als ongeoorloofde openbaarmaking zou zijn aan te merken.

Aan het voor openbaarmaking beslissende criterium 'beschikbaarstelling aan het publiek' lijkt te zijn voldaan bij de vastlegging van gegevens in een on-line databank. Evenmin als dat het geval is bij het spelen van muziek in een leeg café, een tentoonstelling zonder bezoekers of boeken in een boekhandel die niet verkocht worden, is hier van belang of de opgenomen gegevens ooit daadwerkelijk geraadpleegd zullen worden.

Aannemelijk is voorts dat de in het leesportefeuille-arrest vorm gekregen uitputtingstheorie niet van toepassing is op het in de databank opgeslagen gegevensbestand. Op basis van deze theorie zou de auteursrechthebbende zich niet kunnen verzetten tegen verdere openbaarmaking van rechtmatig en met toestemming in het verkeer gebrachte *exemplaren*. Zijn openbaarmakingsrecht is voor wat betreft deze exemplaren 'uitgeput'. Een belangrijke aanwijzing hiervoor vinden we in rechtsoverweging 33 van de databankrichtlijn: "overwegende dat on-line databanken onder het begrip dienstverrichting vallen en er dus geen sprake is van uitputting van het recht van verspreiding". Ook deze overweging ziet in eerste instantie op de relatie databankmaker - databankgebruiker. Toegepast in de relatie met de rechthebbende op het betreffende materiaal, zou deze zich kunnen verzetten tegen opname daarvan in de databank, ook in het geval de verveelvoudiging van het materiaal wel zou zijn toegelaten.

Naast het reeds aangebrachte verschil tussen de vastlegging in on-line en off-line databanken, is hier ook het onderscheid tussen interne en externe databanken van belang. Zoals gesteld, komt met de vastlegging in een on-line databank het werk ter beschikking van de gebruikers. Ten aanzien van externe databanken kan dit beschouwd worden als een ongeoorloofde openbaarmaking. Omdat Spoor (Auteursrechtelijke aspecten van databanken) dit mede baseert op het tentoonstellingsregime van art. 12 lid 2 Aw, komt hij ten aanzien van interne databanken echter tot een andere conclusie dan Hugenholtz. Art. 12 lid 2 bepaalt dat (onder meer) tentoonstellingen ook in besloten kring onder openbaar worden begrepen, tenzij die kring zich beperkt tot familie of vrienden. Het leidt geen twijfel dat gebruikers van een interne

databank niet zijn een daaraan gelijk te stellen kring. Hugenholtz meent echter dat aan art. 12 lid 2 een beperkte toepasselijkheid moet worden toegekend, en niet van toepassing is op databanken. Naar zijn mening dient het 'papieren regime' te worden gevolgd, dat het kopiëren en uitdelen binnen een organisatie onder de voorwaarden van art. 17 toestaat. Als men de bedoeling en de aard van het gebruik van interne databanken in ogenschouw neemt, interne documentatievoorziening, lijkt de zienswijze van Hugenholtz meer voor de hand te liggen dan het tentoonstellingsregime.

5.3.3 Uitvoer / raadpleging

Hierboven is vastgesteld dat invoer en vastlegging van een gegevensbestand in een externe databank die on-line toegankelijk is, gepaard gaat met verveelvoudiging en openbaarmaking, zodat toestemming benodigd is van de auteursrechthebbende.

Bij off-line databanken en delivery services zal openbaarmaking eerst aan de orde komen bij de uitvoer van gegevens. De vraag of bij deze vormen van externe databanken toestemming vereist is van de auteur voor de verveelvoudiging als gevolg van de invoer, is in principe bevestigend beantwoord; het zwaartepunt ligt begrijpelijkerwijze bij de openbaarmaking.

De invoer in interne databanken kan in aanzienlijke mate onder de verschillende regimes van toelaatbare uitzonderingen worden gebracht.

De relevantie van een separate bespreking van de *uitvoer* uit databanken concentreert zich derhalve op de vragen i) of toestemming voor opslag van gegevens in externe on-line-databanken zich tevens dient uit te strekken tot uitvoer, ii) of gegevensverstrekking uit databanken die niet on-line toegankelijk zijn zelfstandig inbreuk maakt op auteursrechten en iii) of ook uitvoer uit interne databanken onder de toelaatbare uitzonderingen zal vallen.

Ad i) Uitvoer op beeldscherm wordt doorgaans niet als verveelvoudiging aangemerkt omdat weergave op het beeldscherm niet als duurzame vastlegging wordt beschouwd. Ten opzichte van uitvoer op diskette of papier, neemt het beeldscherm derhalve een afwijkende positie in. Wat er verder zij van de ratio van dit onderscheid, de met de uitvoer gepaard gaande verveelvoudiging zal meestal onder de toelaatbare uitzonderingen vallen.

Over de vraag of beeldschermweergave dan een daad van openbaarmaking is, wordt verschillend gedacht. Merkwaardig is dat Hugenholtz hier wel de besloten kring van het tentoonstellingsregime 'opvoert', en de mogelijkheid openlaat dat de beeldschermweergave door meer mensen gelijktijdig geconsumeerd kan worden, in welk geval sprake zou kunnen zijn van een ongeoorloofde openbaarmaking. Aan de andere kant is het eveneens merkwaardig dat Spoor het vermoeden dat het niet waarschijnlijk is dat een aantal

mensen tezelfdertijd hetzelfde werk uit de databank raadpleegt, aanvoert ter weerlegging van mogelijke openbaarmaking. Het criterium is immers niet of het werk daadwerkelijk door een aantal mensen wordt geraadpleegd, net zo min als dat het geval was bij de afgespeelde muziek in een café met één bezoeker. Zoals de verspreiding van een enkele fotokopie een daad van (verdere) openbaarmaking kan zijn, zo kan ook de uitvoer op beeldscherm uit een externe on-line-databank opgevat worden als openbaarmaking. Toestemming van de auteursrechthebbende zou zich dan dienen uit te strekken tot en met de uitvoer van de gegevens.

Ad ii) In het geval van delivery service zal de uitvoer van gegevens uit externe databanken zowel een daad van verveelvoudiging als van openbaarmaking betekenen, waarvoor toestemming is vereist van de auteursrechthebbende. Off-line databanken die periodiek het gegevensbestand ter beschikking stellen aan hun abonnees, bijvoorbeeld op CD-ROM, maken vanzelfsprekend verveelvoudigingen. De niet on-line toegankelijke databanken hebben niet alleen toestemming nodig voor de invoer en vastlegging van werken in het gegevensbestand, doch ook voor de reproduktie en verspreiding daarvan.

Ad iii) De uitvoer van gegevens uit interne databanken zal, evenals de invoer en vastlegging daarvan, veelal toelaatbaar zijn op grond van de artt. 16b en 17 Aw. Zoals hierboven (paragraaf 5.3.2) aangevoerd, lijkt het tentoonstellingsregime niet van toepassing op interne databanken, dus ook niet op de uitvoer via het beeldscherm.

5.4 De exploitatie van databanken

In paragraaf 5.3 is de vraag behandeld of de maker van een databank voor de opname daarin van gegevens afkomstig van derden, toestemming nodig heeft van die derden. Voor wat betreft interne databanken lijkt dit niet snel het geval; voor zover er een rechthebbende bestaat op die gegevens, zijn invoer, vastlegging en uitvoer veelal niet als inbreuken op diens exclusieve rechten van verveelvoudiging en/of openbaarmaking aan te merken, maar toelaatbaar te achten op grond van in de wet genoemde excepties.

Ten aanzien van externe databanken blijkt doorgaans toestemming vereist van de rechthebbende. Bij externe *on-line* databanken kan de invoer en vastlegging van de gegevens worden aangemerkt als ongeoorloofde verveelvoudiging, zowel als openbaarmaking. Uitvoer blijkt in dat geval meestal geen inbreuk meer op te leveren, eveneens op grond van de excepties. Bij externe *off-line* databanken kunnen zowel de invoer en vastlegging, als de distributie beschouwd worden als handelingen waarvoor toestemming van de rechthebbende is vereist.

Voor zover het gegevens betreffen die zelf afkomstig zijn uit databankachtige bronnen (elektronische en/of papieren), geldt echter een beperking op grond van de richtlijn databankbescherming: art. 7 lid 1 geeft de databankfabrikant het recht om de opvraging en/of hergebruik van het geheel of een in kwalitatief of kwantitatief opzicht substantieel deel van de inhoud te verbieden.

De databankrichtlijn ziet niet zozeer op de relatie databankmaker - rechthebbenden op daarin opgenomen werken. Volgens art. 2 betreft de auteursrechtelijke bescherming van databanken in deze richtlijn niet de inhoud van die databanken en laat de bestaande rechten op die inhoud onverlet. Het is echter denkbaar, dat een toekomstige nadere invulling van termen uit de richtlijn ('tijdelijke reproduktie', 'uitputting') reflexwerking kunnen hebben.

In deze paragraaf zal de auteursrechtelijke bescherming van de databank zelf tegen ongeoorloofde overname worden besproken. De aanleg van databanken kan aanzienlijke menselijke, technische en financiële inspanningen vergen, terwijl zij kunnen worden gekopieerd of geraadpleegd voor een fractie van de kosten die moeten worden besteed om deze produkten zelfstandig te ontwikkelen. Het zonder toestemming opvragen en/of hergebruiken van een databank is een handeling die ernstige economische en technische gevolgen kan hebben (aldus de rechtsoverwegingen 7 en 8 van de richtlijn databankbescherming). De auteursrechtelijke bescherming waarop rechthebbenden op de inhoud van databanken zich kunnen beroepen, is niet toereikend ten opzichte van de databankmaker. Voor deze geldt een eigen belang om zelfstandig te mogen optreden tegen ongeoorloofde raadpleging en/of hergebruik.

Naar huidig recht kunnen databanken bescherming genieten als verzamelwerk krachtens art. 5 Aw. Volgens het criterium van de Hoge Raad in Romme - Van Dale is daartoe nodig dat de verzameling het resultaat is van een selectie die een persoonlijke visie van de maker tot uitdrukking brengt. Het is, met andere woorden, nodig dat het verzamelwerk voldoet aan de auteursrechtelijke criteria voor werken: oorspronkelijkheid en waarneembaarheid. De 'persoonlijke visie' vertoont overeenstemming met het 'eigen, persoonlijk karakter', uit paragraaf 3.1.1.

Voorzover iedere creativiteit aan een databank zou ontbreken, bijvoorbeeld een alfabetische rangschikking van *alle* zware metalen met hun atoomgetal, valt te verdedigen dat de databank onder het beschermingsregime van geschriften zonder persoonlijk karakter is te plaatsen. Het gegevensbestand uit een databank valt onder het begrip 'geschrift', opgevat als drager van verstaanbare leestekens. Een verschil ten opzichte van een uitgave in druk lijkt overigens niet goed verdedigbaar.

Op 11 maart 1996 is de EU-Richtlijn Betreffende de Rechtsbescherming van Databanken aangenomen (96/9/EG, Pb. L 77/20). De richtlijn brengt als zodanig geen essentiële veranderingen te weeg ten opzichte van de hierboven besproken beschermingsomvang. Art. 3 lid 1 luidt als volgt:

> *Volgens deze richtlijn worden databanken die door de keuze of de rangschikking van de stof een eigen intellectuele schepping van de maker vormen, als zodanig door het auteursrecht beschermd. Er worden geen andere criteria toegepast om te bepalen of ze voor die bescherming in aanmerking komen.*

Databanken worden beschermd door het auteursrecht. Het in dit artikel neergelegde oorspronkelijkheidscriterium heeft veel weg van de omschrijving in art. 1 lid 3 van de softwarerichtlijn, 'eigen schepping van de maker'. Er mogen geen andere criteria worden toegepast, zoals kwalitatieve of esthetische vereisten. Het is een laag criterium, dat minder verstrekkend lijkt te zijn dan de door de Hoge Raad geformuleerde 'persoonlijke visie'.

Evenals we dat gezien hebben bij de implementatie van de softwarerichtlijn is het voorspelbaar dat de wetgever naar aanleiding van dit artikel ook databanken buiten de werking van de geschriftenbescherming zal plaatsen.

Waar de databankmaker zich thans nog met een beroep op de geschriftenbescherming zou kunnen verzetten tegen hergebruik van aan de databank ontleende gegevens die niet zelfstandig voor bescherming als oorspronkelijk werk in aanmerking komen, introduceert de richtlijn een sui generis bescherming, in de vorm van een extractierecht. Art. 7 lid 1 van de richtlijn bepaalt dat de lidstaten moeten voorzien in een recht voor de fabrikant van een databank, waarvan de verkrijging, de controle of de presentatie van de inhoud in kwalitatief of kwantitatief opzicht getuigt van een substantiële investering, de opvraging of het hergebruik van het geheel of een in kwalitatief of kwantitatief opzicht substantieel deel van die inhoud te verbieden. Het is een regeling van mededingingsrechtelijke aard en vertoont verwantschap met de auteursrechtelijke geschriftenbescherming en met het op de ongeoorloofde mededinging gebaseerde leerstuk van prestatiebescherming. Het recht kent ingevolge art. 10 een duur van vijftien jaar gerekend vanaf het moment van voltooiing of eerste publikatie en van elke substantiële wijziging van de databank. Het systeem van auteursrecht en sui generis extractierecht is cumulatief.

De exclusieve rechten van de databankmaker met betrekking tot de voor *auteursrechtelijke* bescherming in aanmerking komende uitdrukkingsvorm van de databank bestaan volgens art. 5 uit:

a) de permanente of tijdelijke reproduktie, geheel of gedeeltelijk, met ieder middel en in iedere vorm;
b) de vertaling, bewerking, schikking en iedere andere verandering;

c) iedere vorm van openbare verspreiding van de databank of van kopieën daarvan (met toepassing van de uitputtingsleer ten aanzien van rechtmatig in het verkeer gebrachte exemplaren van de databank, bijvoorbeeld op CD-ROM);
d) elke mededeling, voorstelling of demonstratie voor het publiek
e) elke reproduktie, verspreiding, mededeling, voorstelling of demonstratie voor het publiek van de onder b. vermelde handelingen.

In art. 6 lid 1 wordt bepaald dat de rechtmatige gebruiker zonder toestemming van de maker alle in art. 5 bedoelde handelingen mag verrichten die noodzakelijk zijn voor de toegang tot en het normale gebruik van de databank.

Uit de bepaling van art. 6 lid 2 valt op te maken, dat de onder het huidige auteursrecht toegelaten excepties niet zonder meer van toepassing geacht mogen worden op databanken: de in art. 5 aan de databankmaker toegekende rechten *kunnen* de lidstaten beperken wanneer het betreft het kopiëren voor eigen gebruik van een niet-elektronische databank (kopiëren voor eigen gebruik van *elektronische* databanken is derhalve niet geoorloofd, tenzij het betreft 'in kwalitatief of kwantitatief opzicht niet-substantiële delen en de overname van die delen geen inbreuk oplevert op auteursrechten op die delen zelf - artt. 7 lid 4 en 8 lid 1), wanneer het betreft gebruik alleen ter illustratie bij onderwijs of voor wetenschappelijk onderzoek, of wanneer het gaat om andere, volgens de nationale wetgeving traditioneel toegestane uitzonderingen.

Onder het extractierecht behoudt de rechtmatige gebruiker de mogelijkheid in kwalitatief of kwantitatief opzicht niet-substantiële delen van de inhoud van een databank op te vragen en/of te hergebruiken, voor welk doel dan ook. Dit recht mag niet worden verboden (art. 8 lid 1). Deze bevoegdheid van de rechtmatige gebruiker mag - begrijpelijkerwijze - weer niet aldus worden aangewend, dat hij 'beetje bij beetje' (systematisch) de gehele databank in 'niet-substantiële' delen overneemt (art. 7 lid 5).

De rechtmatige gebruiker, tenslotte, mag geen handelingen verrichten waardoor ongerechtvaardigde schade wordt toegebracht aan de rechtmatige belangen van de fabrikant van de databank (art. 8 lid 2) of nadeel berokkenen aan de houder van een auteursrecht of een naburig recht op de in die databank vervatte werken of prestaties (art. 8 lid 3).

De richtlijn moet uiterlijk 1 januari 1998 in de nationale wetgeving van de lidstaten zijn verwerkt.

5.5 Jurisprudentie

RB AMSTERDAM, 17 MEI 1989, GRAFISCHE INDUSTRIE HAARLEM - OEDIP NEDERLAND, CR 1990/3

De samenstelling, groepering en indeling van het Compendium, dat bestaat uit voor het merendeel van derden verkregen technische informatie en gegevens, geeft op zichzelf onvoldoende eigen karakter aan het Compendium om aanspraak te kunnen maken op de volle omvang van de bescherming die art. 10 van de Auteurswet 1912 verleent aan werken van letterkunde, wetenschap of kunst. De met de samenstelling, groepering en indeling van de inhoud van het Compendium gemoeide inspanning en zorg rechtvaardigt echter wel de beperkte auteursrechtelijke bescherming tegen ontlening die toekomt aan geschriften zonder persoonlijk karakter.

RB HAARLEM, K.G. 5 DECEMBER 1989, VNU - SPEETS, H & H, CR 1990/3

Het is denkbaar dat twee auteurs onafhankelijk van elkaar tot hetzelfde systeem van ordening van gegevens (i.c. met betrekking tot een n.a.w.-gegevensbestand) zouden komen, zodat de PCM-databank niet als een werk in de zin van art. 1 Auteurswet is te beschouwen. De vraag die vervolgens beantwoord moet worden is of de PCM-databank in aanmerking komt voor bescherming als 'geschrift' op grond van art. 10 van de Auteurswet. Het auteursrecht op geschriften die geen eigen of persoonlijk karakter bezitten, is niet beperkt tot werken die in druk zijn verschenen. Het PCM-databestand voldoet niet aan het vereiste dat het openbaar is gemaakt of bestemd is om te worden openbaar gemaakt. Het staat gedaagden echter niet vrij om met gebruikmaking van de PCM-databank stelselmatig relaties van PCM te benaderen. Deze vorm van concurrentie is ongeoorloofd en onrechtmatig jegens VNU. (Onrechtmatige daad in plaats van bescherming op grond van auteursrecht)

HR 4 JANUARI 1991, ROMME - VAN DALE, NJ 1991, 608, RVDW 1991, 27, IER 1991, 38 NT FWG, CR 1991/2 NT P.B. HUGENHOLTZ

Wil een voortbrengsel kunnen worden beschouwd als een werk als bedoeld in art. 1 in verbinding met art. 10 Auteurswet 1912, dan is vereist dat het een eigen, oorspronkelijk karakter heeft en het persoonlijk stempel van de maker draagt. Een verzameling van woorden (zoals het trefwoordenbestand van Van Dale) die deel uitmaken van de Nederlandse taal, voldoet niet zonder meer aan dit vereiste. Op zich zelf is zulk een verzameling niet meer dan een hoeveelheid feitelijke gegevens die als zodanig voor auteursrechtelijke bescherming niet in aanmerking komt. Dat zou slechts anders zijn indien de verzameling het resultaat zou zijn van een selectie die een persoonlijke visie van de maker tot uitdrukking brengt.

RB ALMELO, 12 NOVEMBER 1991, CR 1993/5, NT E.P.M. THOLE
Het kopiëren en aanbieden van illegale standaardprogrammatuur via bulletin boards is in strijd met de Auteurswet. Boete alsmede verbeurdverklaring van alle in beslag genomen hardware waarmee inbreuk is gepleegd.

HOF DEN HAAG, 1 APRIL 1993, ROMME - VAN DALE, nj 1994, 58, ier 1993, 16, CR 1993/4, NT P.B. HUGENHOLTZ
Bij de selectie van de verzameling woorden van de Nederlandse taal is een samenstel van keuzen gemaakt. De verzameling is derhalve als een oorspronkelijk werk auteursrechtelijk beschermd.

HOF DEN HAAG, 1 DECEMBER 1994, INFORMATIERECHT/ami 1995/3
Vertoning films in privé videocabines videotheek is openbaarmaking.

Hr 27 JANUARI 1995, INFORMATIERECHT/ami (19) 1995/4
Openbaarmaking van een werk beoordelen naar het recht van het land waar de verveelvoudiging is vervaardigd.

RB ROTTERDAM, 24 AUGUSTUS 1995, BRIDGESOFT - LENIOR, CR 1996/5, NT R.V. DE MULDER
Het 'downloaden' (kopiëren van een computerprogramma van het bulletin board system van Lenior) door anderen was kennelijk mogelijk doordat Lenior met betrekking tot de door een derde 'ge-uploade' software een wijziging heeft aangebracht in de Title Allocation Table; door zulks te doen heeft Lenior de software dus openbaar gemaakt en alleen al daardoor inbreuk gemaakt op het auteursrecht van Bridgesoft.

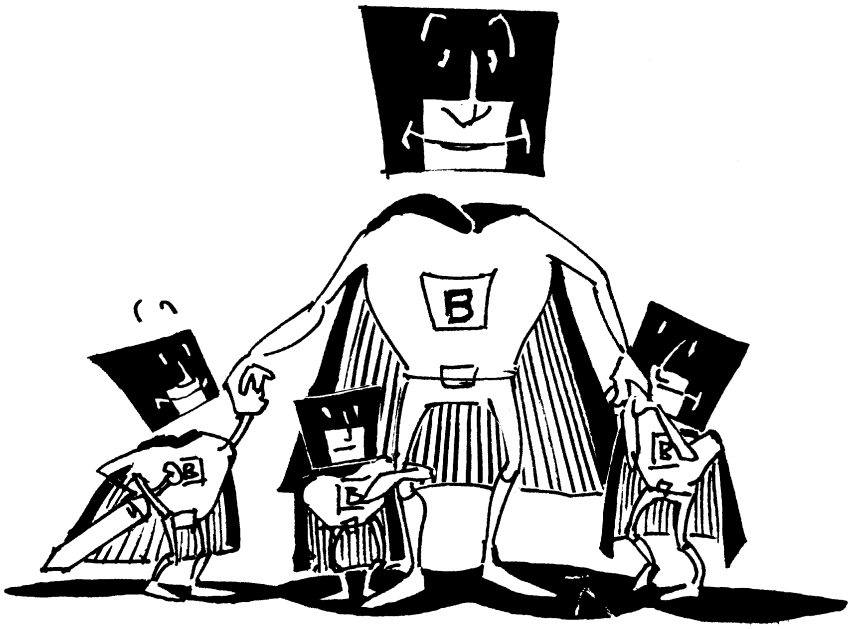
RB DEN HAAG, K.G. 12 MAART 1996, SCIENTOLOGY-CHURCH, CR 1996/2
Internet access providers doen niet meer dan gelegenheid geven tot openbaarmaking en kunnen in beginsel geen invloed uitoefenen of zelfs maar kennis dragen van datgene wat diegenen die via hen toegang tot internet hebben gekregen daarop uitdragen. In beginsel is er daarom geen aanleiding hen aansprakelijk te houden voor onrechtmatige - bijvoorbeeld op auteursrechten van derden inbreuk makende - handelingen van gebruikers. Een aansprakelijkheid zou aangenomen kunnen worden in een situatie waarin onmiskenbaar duidelijk is dat een publikatie van een gebruiker onrechtmatig is en waarin redelijkerwijs mag worden aangenomen dat zulks ook bij de access provider bekend is, bijvoorbeeld doordat deze op een en ander is geattendeerd.

RB HAARLEM, 10 JULI 1996, cd-FOONGIDS OP INTERNET, CR 1996/5, NT P.B. HUGENHOLTZ
Volgens de heersende leer wordt een gegevensbestand dat in een computerleesbare vorm op een elektronisch medium (i.c. een CD-ROM) is vastgelegd als

'geschrift' in de zin van de Auteurswet aangemerkt. Een geschrift, dat geen eigen of persoonlijk karakter heeft, wordt beschermd tegen het door ontlening aan het geschrift zelf overnemen van de inhoud daarvan, indien het geschrift openbaar is gemaakt, of bestemd is om openbaar te worden gemaakt. Dat de gegevens van het databestand openbaar zijn gemaakt is evident, nu de CD-foongids in de handel verkrijgbaar is en tot stand is gekomen met het oog op informatieverstrekking aan derden.

5.6 Literatuur

- Dommering, E.J., 'Het auteursrecht spoelt weg door het elektronisch vergiet', in: Computerrecht 1994/3.
- Hugenholtz, P.B., 'Auteursrecht en information retrieval', Post Scriptum Reeks, 1982.
- Hugenholtz, P.B., 'Auteursrecht op informatie', (diss.), Kluwer, Deventer, 1989.
- Hugenholtz, P.B., 'De Databankrichtlijn eindelijk aanvaard: een zeer kritisch commentaar', Computerrecht 1996/4.
- J.H. Spoor, 'Auteursrechtelijke aspecten van databanken', in: Computerrecht 1984/2.
- Visser, D.J.G., 'Gebruik van CD-ROM's in netwerken en het auteursrecht', in: Computerrecht 1994/5.



6 Detachering van IT-deskundigen

In organisaties wordt voor de uitvoering van automatiseringsprojecten veel gebruik gemaakt van automatiseringsdeskundigen van buiten de eigen organisatie. De vorm waaronder dit geschiedt kan uiteen lopen van enerzijds volledige uitbesteding van het project aan een automatiseringsbedrijf tot anderzijds het volledig in eigen beheer uitvoeren daarvan. In het laatste geval wordt dan gebruik gemaakt van arbeidskrachten van een automatiseringsbedrijf, die in de organisatie werken alsof het 'eigen' personeel is. Een belangrijk verschil tussen deze vormen van uitvoering is natuurlijk de mate waarin een partij verantwoordelijk gehouden kan worden voor het eindresultaat.

Hoewel in het oog springend, is dit echter niet het enige aandachtspunt. Het ter beschikking stellen van arbeidskrachten valt namelijk in beginsel onder de werking van de Arbeidsvoorzieningswet, in welk geval een vergunning is vereist. Aan dit vergunningenstelsel zijn beperkingen verbonden, die zich slecht blijken te verdragen met de praktijk van automatisering. Bovendien is gebruikmaking van ingeleende arbeidskrachten niet zonder risico voor wat betreft de aansprakelijkheid van de inlener jegens de fiscus en de bedrijfsvereniging.

In dit hoofdstuk wordt in paragraaf 6.1 eerst een onderscheid op hoofdlijnen aangebracht tussen de hier genoemde vormen van automatiseringsovereenkomsten. Vervolgens besteden we in paragraaf 6.2 aandacht aan de

redenen waarom we de figuur van detachering zo veelvuldig tegen komen in de automatiseringsbranche, en wat er zoal in een dergelijke overeenkomst geregeld moet worden. In paragraaf 6.3 staan we stil bij de vraag of deze vorm van 'ter beschikking stelling van arbeidskrachten' onder de werking van de Arbeidsvoorzieningswet valt en welke consequenties daaraan moeten worden verbonden. Een belangrijke consequentie, die van de inlenersaansprakelijkheid, wordt besproken in paragraaf 6.4

6.1 Automatiseringsovereenkomsten

Voor de uitvoering van een automatiseringsproject staan er verschillende mogelijkheden open. De ontwikkeling van software kan vorm krijgen in verschillende typen overeenkomsten. Hieronder worden achtereenvolgens besproken de turn key overeenkomst, de software-ontwikkelingsovereenkomst en de detacherings- of bodyshopovereenkomst.

TURN KEY OVEREENKOMST

Onder een turn key-overeenkomst verstaan we een overeenkomst waarin het automatiseringsproject - het geheel van hardware, software en diensten - in zijn totaal wordt uitbesteed aan een opdrachtnemer, bijvoorbeeld een softwarehouse. De opdrachtgever formuleert van tevoren zijn eisen voor het te ontwikkelen systeem, waarna de opdrachtnemer voor de uitvoering zorg draagt. De opdrachtgever behoeft als het ware alleen nog maar de 'sleutel om te draaien' om het systeem in werking te stellen. Voor dit type contract komen we ook wel de benaming SI-contract, system integration-contract, tegen. Hiermee wordt bedoeld dat de opdrachtnemer de functie van 'systeemintegratie' - het zorgen voor een juiste afstemming van de verschillende hardwarecomponenten en programmatuur - uit handen neemt van de opdrachtgever.

Een turn key-overeenkomst bestaat eigenlijk uit een (groot) aantal deelovereenkomsten: i) de koop, huur of lease van hardware, ii) de opdracht tot ontwikkeling van software, of een licentieverlening op software, eventueel de overdracht van intellectuele rechten op software, en iii) de opdracht tot het verrichten van diensten van uiteenlopende aard, zoals implementatie (het werkbaar maken van het systeem in de organisatie van de opdrachtgever) en opleiding. Meestal treffen we een soort 'mantelovereenkomst' aan, waarin het te ontwikkelen systeem in hoofdlijnen wordt gespecificeerd en waarin voorwaarden van algemene aard zijn opgenomen. Daaronder bevindt zich vervolgens een aantal specifieke overeenkomsten van divers karakter.

Het behoeft overigens niet zo te zijn, dat de system integrator alle onderdelen van het automatiseringsproject ook zelf uitvoert. Zo zal een softwarehouse, als opdrachtnemer, de voor het project meest toepasselijke hardware

bestellen bij een hardwareleverancier, en wellicht ook op onderdelen standaardsoftware bij derden betrekken.

SOFTWARE-ONTWIKKELINGSOVEREENKOMST

Bij dit type contract wordt slechts een overeenkomst gesloten met betrekking tot de te ontwikkelen software. De functie van 'system integrator' blijft dus rusten bij de opdrachtgever. Op basis van een pakket van eisen van de opdrachtgever, wordt de software ontwikkeld door de opdrachtnemer. De verantwoordelijkheid voor een juiste interactie van het pakket met andere programma's en met de bestaande hardware, rust in beginsel bij de opdrachtgever. De eisen die deze andere onderdelen aan het computersysteem stellen, zullen meestal wel onderdeel uitmaken van de ontwikkelingsovereenkomst.

Beschouwt men het ontwikkelen van software als het verrichten van arbeid gericht op de tot stand koming van een stoffelijk werk, dan kan de softwareontwikkelingsovereenkomst gekwalificeerd worden als 'aanneming van werk' (art. 7A:1637b BW). In het andere geval is de 'overeenkomst van opdracht' (art. 7:400 BW) van toepassing.

DETACHERINGS- OF BODYSHOPOVEREENKOMST

Anders dan bij de vorige twee typen overeenkomsten, waarbij de softwareontwikkeling werd uitbesteed, kiest men in het geval van een bodyshopovereenkomst voor het in eigen beheer ontwikkelen van de software. In dit laatste geval is er dan geen sprake van de opstelling door de opdrachtgever van een pakket van eisen met betrekking tot het computerprogramma, maar van eisen aan dan wel kwalificaties van medewerkers die door de opdrachtnemer ter beschikking worden gesteld. Zij zullen onder leiding en toezicht van de opdrachtgever en eventueel samen met medewerkers van de opdrachtgever het computerprogramma ontwikkelen.

Hoewel het in alle drie de typen overeenkomsten natuurlijk te doen is om het ontwikkelen van software, is de detachering in zoverre verschillend van de andere twee, dat juridisch gesproken het 'onderwerp van de overeenkomst' niet de software is, maar de personen van het softwarehouse/opdrachtnemer.

Het *juridische* 'werken onder leiding en toezicht' van de opdrachtgever, die bij dit type contract ook wel 'inlener' wordt genoemd, moet men voorts niet gelijk stellen met het *feitelijk* werkzaam zijn binnen de onderneming van de inlener. Ook onder de beide vorige overeenkomsten kan het zo zijn dat de programmeurs van de opdrachtnemer feitelijk werken binnen de organisatie van de opdrachtgever. Zij zijn dan echter niet aan de opdrachtgever verantwoording schuldig, maar aan de projectleider van de opdrachtnemer. Deze is op zijn beurt in de relatie opdrachtnemer - opdrachtgever verantwoording schuldig aan de opdrachtgever. In feite is het zo, dat het voor de werkzaamheden van de programmeurs geen verschil behoeft te maken, of zij nu

werkzaam zijn onder vigeur van een turn key-overeenkomst, een software-ontwikkelingsovereenkomst of een bodyshopovereenkomst.

Met betrekking tot de verantwoordelijkheid voor het eindresultaat, de vraag of de ontwikkelde software ook daadwerkelijk voldoet aan de daaraan gestelde eisen, kunnen we de typen contracten globaal afzetten op een denkbeeldige lijn. Ter linker zijde, bij een turn key-overeenkomst, ligt de verantwoordelijkheid voor de kwaliteit van de software in belangrijke mate bij de opdrachtnemer. Aan de rechter zijde treffen we de bodyshopovereenkomst aan, in welk geval de verantwoordelijkheid voor de kwaliteit van de software voornamelijk ligt bij de opdrachtgever/inlener zelf. De software-ontwikkelingsovereenkomst bevindt zich ergens daartussen, aangezien voor deze overeenkomst doorgaans een grotere interactie plaats vindt tussen opdrachtgever en opdrachtnemer.

Het hier aangebrachte onderscheid is een onderscheid op hoofdlijnen. In de praktijk komen we allerlei mengvormen tegen. Het is dan ook zaak om vooral te letten op de *inhoud* van het contract, meer dan de benaming daarvan. Zo is bij een turn key-overeenkomst van belang of de opdrachtnemer heeft bijgedragen aan de definitie van de projecteisen, of dat deze zijn opgesteld door de opdrachtgever. In het geval van een bodyshopovereenkomst, waar het in eerste instantie om het in/uitlenen van mensen gaat, kunnen niettemin bepalingen zijn opgenomen, bijvoorbeeld met betrekking tot de projectbegeleiding, waardoor de opdrachtnemer/uitlener enige verantwoordelijkheid voor het eindresultaat gaat dragen.

6.2 De bodyshopovereenkomst

Aan een bodyshopovereenkomst gaat de beslissing vooraf om de software in eigen huis te ontwikkelen. Daarvoor zijn verschillende redenen denkbaar:

- De organisatie behoudt een maximale invloed op de tot stand koming van het resultaat;
- Het is niet nodig, en soms ook niet mogelijk, om het gehele project vooraf en detail te specificeren;
- Men behoeft geen - vertrouwelijke - know how naar buiten prijs te geven. De specifieke bedrijfskennis, de interne organisatie en werkwijze, alsmede de strategische betekenis van informatietechnologie blijven exclusief voorbehouden aan de onderneming;
- De organisatie bouwt een maximale kennis op omtrent de inrichting en werkwijze van de programmatuur. Dit kan van belang zijn voor het onderhoud van de software en de integratie daarvan met andere computerprogramma's.

Soms worden ook wel als redenen aangevoerd dat de ontwikkeling in eigen huis minder kosten met zich meebrengt en dat het auteursrecht op de software aan de onderneming toekomt. Wat betreft dit laatste is het niet zonder meer duidelijk dat het auteursrecht vanzelf bij de inlenende organisatie terecht komt. Zoals gesteld in paragraaf 3.1.4, is dit mede afhankelijk van de uitleg die men kan geven aan de in de auteurswet gestelde vereisten dat het werk ofwel 'naar het ontwerp van een ander en onder diens leiding en toezicht' (ex art. 6 Aw), dan wel 'in dienst van een ander' (ex art. 7 Aw) moet zijn vervaardigd. Het is derhalve veelal raadzaam om in de overeenkomst expliciet een bepaling op te nemen waardoor het auteursrecht bij de inlener komt te liggen. En dat kan men evenzo bereiken in een software-ontwikkelingsovereenkomst of bij een turn key contract.

Ook voor wat betreft de kosten kan men niet zonder meer stellen dat ontwikkeling van software in eigen beheer goedkoper is dan uitbesteden. Dit geldt des te sterker waar men besluit om de ontwikkeling in eigen huis uit te voeren met ingeleende werknemers van een softwarehouse. Of men nu de loonsom betaalt als onderdeel van een software-ontwikkelingsovereenkomst of als onderdeel van een bodyshopovereenkomst is in feite om het even.

Om software in eigen huis te kunnen ontwikkelen, dient de organisatie wel aan een aantal voorwaarden te voldoen. Men moet beschikken over:

- voldoende kennis van het betreffende automatiseringsgebied.
  Bepaalde toepassingen kunnen zeer specialistisch zijn, waarvoor de kennis niet standaard en continue voor de organisatie beschikbaar hoeft te zijn;
- voldoende capaciteit.
  De ontwikkelingsactiviteit dient niet een dergelijk groot beslag op de beschikbare capaciteit te leggen, dat de overige werkzaamheden in het gedrang komen;
- voldoende kennis van projectmanagement.

Uit deze voorwaarden volgen de belangrijkste redenen voor organisaties om met ingeleend personeel te werken:

- het opvangen van piekbelasting;
- het inhuren van projectmanagement;
- het inhuren van specialistische kennis;
- niet belast worden met scholings- en opleidingstrajecten;
- directe inzetbaarheid;
- het tijdelijk karakter van de werkzaamheden.

Het argument van het tijdelijk karakter van de werkzaamheden is overigens betrekkelijk. Bij banken, verzekeringsmaatschappijen en de overheid bijvoorbeeld, zijn in feite continue tientallen werknemers op inleenbasis werkzaam. De relatieve schaarste aan automatiseringsdeskundigen speelt hierin een rol,

alsmede de honorering van deze medewerkers, welke soms buiten de in de organisatie gangbare salarisschalen valt.

De redenen voor softwarehuizen om bedrijfsmatig arbeidskrachten uit te lenen onder een detacheringsconstructie zijn tamelijk evident:
- er is vraag naar;
- commercieel eenvoudiger, geen ingewikkelde offertes;
- de aansprakelijkheid voor het eindresultaat wordt geminiseerd.

Ten onrechte wordt uit dit laatste argument wel de opvatting gedestilleerd dat een bodyshopovereenkomst een 'inspanningsverbintenis' oplevert, daar waar de turn key en de software-ontwikkelingsovereenkomst meer het karakter hebben van 'resultaatsverbintenissen'.

Alhoewel het juist is, dat het softwarehouse als uitlener niet of in mindere mate aansprakelijk is voor het resultaat van de software-ontwikkeling, dient het begrip resultaatsverbintenis juridisch in verband te worden gebracht met de vraag of de betreffende partij gehouden mag worden aan het bereiken van een resultaat ingevolge de met hem gesloten overeenkomst.

Aangezien de bodyshopovereenkomst *niet* de software-ontwikkeling zelf tot onderwerp heeft, maar het ter beschikking stellen van mensen, dient men hier dus de vraag te stellen of het softwarehouse gehouden is om op de overeen gekomen tijd en voor de overeen gekomen duur de met name genoemde personen ter beschikking te stellen, of dat het softwarehouse alleen maar zijn best moet doen. Het behoeft geen nader betoog dat de inlener/opdrachtgever slechts gebaat is bij het daadwerkelijk ter beschikking stellen, zodat de bodyshopovereenkomst eveneens het kenmerk heeft van een resultaatsverplichting.

Omdat, zoals gezegd, het onderwerp van een bodyshopovereenkomst is het ter beschikking stellen van arbeidskrachten, ligt het voor de hand dat het contract vooral bepalingen bevat omtrent de hoedanigheden van die arbeidskrachten. Te denken valt aan de volgende, persoons-gerelateerde aspecten: kwaliteit van de medewerkers, opleidingsniveau, ervaring (in soortgelijke projecten), specifieke deskundigheid en sociale vaardigheden.

Het is dan ook gebruikelijk dat opdrachtgever/inlener en softwarehouse/uitlener samen een keuze maken op basis van verschillende CV's en dat de arbeidskrachten bij naam genoemd worden in de bodyshopovereenkomst.

Voorts bevat de overeenkomst bepalingen van meer 'huishoudelijke' aard, zoals een beschrijving van de aard van de te verrichten werkzaamheden, de bevoegdheid van de inlener om aanwijzingen te geven (zie ook art. 7:402 BW), de werktijden en de locatie.

Tenslotte worden bepalingen opgenomen die de nadere verhouding tussen opdrachtgever/inlener en softwarehouse/uitlener regelen:

- de bevoegdheid van de *inlener* om de arbeidskracht te doen vervangen (bij gebleken ongeschiktheid bijvoorbeeld);
- de bevoegdheid van de *uitlener* om de arbeidskracht te vervangen (als die nodig mocht zijn op een ander project);
- de wijze van overleg tussen inlener en uitlener;
- de duur en beëindiging van de ter beschikking stelling;
- eventueel benodigde verlenging van de ter beschikking stelling (waarbij bij voorkeur dezelfde arbeidskrachten betrokken moeten blijven, omdat deze het project kennen en vertrouwd zijn geworden met de overige medewerkers);
- eventueel benodigde extra mankracht gedurende de looptijd van het project;
- wat te doen bij ziekte en vakantie van de arbeidskracht (vervanging);
- een eventueel verbod op 'onderaanneming', op het doorlenen van arbeidskrachten die de uitlener bij een derde heeft betrokken;
- een eventueel verbod op het in dienst nemen van elkaars medewerkers;
- geheimhoudingsbedingen, al dan niet mede ondertekend door de betreffende medewerkers;
- de werkgeversaansprakelijkheid van art. 6:170 BW. (Voorkomen dat naast de inlener, in wiens organisatie de uitgeleende immers werkzaam is en wiens opdrachten hij moet uitvoeren, ook de uitlener aansprakelijk gehouden kan worden);
- verzekeringen;
- bepalingen met betrekking tot de wijze van betaling;
- verantwoordelijkheden van de uitlener en de inlener.

Het is duidelijk dat er een spanningsveld bestaat tussen het leggen van verantwoordelijkheden bij de uitlener voor het eindresultaat en de aanwijzingsbevoegdheid van de inlener.

6.3 De Arbeidsvoorzieningswet

Het detacheren van personeel heeft op het eerste gezicht verwantschap met het werkterrein van uitzendbureaus. Ingevolge de Arbeidsvoorzieningswet (Arbvowet) is dit alleen toegestaan indien de uitzendende onderneming over een vergunning beschikt. Aan de andere kant vertoont deze vorm van dienstverlening ook verwantschap met het werkterrein van de vrije beroepsbeoefenaren, zoals accountants en advocaten. In grote organisaties bevinden zich vrijwel permanent werknemers van het externe accountantskantoor. In paragraaf 6.3.1 wordt stil gestaan bij de vraag of detachering van automatise-

ringspersoneel, zoals dat gebruikelijk geschiedt door softwarehuizen, valt onder de werking van de Arbvowet. In paragraaf 6.3.2 komen vervolgens de vergunningsaspecten aan de orde.

6.3.1 Toepasselijkheid Arbvowet

Per 1 januari 1991 is de Arbvowet in werking getreden, ter vervanging van de Wet op het ter beschikking stellen van arbeidskrachten (WTBA), de Arbeidsbemiddelingswet 1930 en de Wet op de openbare arbeidsbemiddeling.

De WTBA was voornamelijk bedoeld als anti-misbruik wet, ter bescherming van de positie van werknemers op de arbeidsmarkt. Uit de kamerstukken van de Arbvowet blijkt dat deze twee doelstellingen heeft:
1. Bescherming van de rechtspositie van werknemers;
2. Optimale allocatie van arbeidskrachten.

Bezien we de situatie in de automatiseringsbranche, dan kunnen we vast stellen dat de detacheringsconstructie bij uitstek voorziet in de allocatiedoelstelling. Maar ook de positie op de arbeidsmarkt van de hierin werkzame arbeidskrachten is sterk. Automatiseringsmedewerkers zijn doorgaans goed betaalde specialisten, waar veel vraag naar is. Bovendien bestaat er meestal een vast dienstverband met de uitlener (dit kan anders zijn voor de zogenoemde 'poolbedrijven'). Mocht het zo zijn, dat er op enig moment geen werk beschikbaar is, dan worden ze normaal doorbetaald.

Voor de beantwoording van de vraag of op detachering niettemin de Arbvowet van toepassing is, kijken we eerst naar de criteria in de wet. Art. 1.1 onder i definieert het 'ter beschikking stellen van arbeidskrachten' als:
1. het *tegen vergoeding* ter beschikking stellen van arbeidskrachten aan een ander
2. voor het onder diens *leiding en toezicht*,
3. *anders dan* krachtens een met deze gesloten *arbeidsovereenkomst*,
4. verrichten van aldaar *gebruikelijke arbeid*.

Aan het eerste criterium wordt zonder meer voldaan: de inlener betaalt geen loon aan de uitgeleende, maar een vergoeding aan de uitlener voor de aan hem ter beschikking gestelde arbeidskrachten.

Ook het tweede criterium is van toepassing, zij het dat de inlener niet de enige is die in een gezagsverhouding staat tot de arbeidskracht. Ingevolge de tussen de uitlener en de werknemer gesloten arbeidsovereenkomst, is de werknemer ook gehouden aan opdrachten van zijn formele werkgever, bijvoorbeeld de opdracht om zijn werkzaamheden in de organisatie van de inlener te verrichten.

Ten aanzien van het derde criterium kan worden gesteld dat de arbeidskracht weliswaar een arbeidsovereenkomst heeft met de *uitlener*, maar de

onderliggende rechtsverhouding tussen uitlener en uitgeleende is hier niet van belang. De kenmerken van de arbeidsovereenkomst - loon, onvervangbaarheid van de persoon en gezagsverhouding - gaan hier ten opzichte van zijn relatie tot de *inlener* niet op. (Een uitzondering moet soms gemaakt worden voor de situatie waar men zich bedient van de constructie van de zogenoemde 'management B.V.'. Als de uitgeleende als het ware zichzelf uitzendt als werknemer van zijn eigen B.V., en hij voorts slechts voor één opdrachtgever werkzaam is, wordt dit in de rechtspraak en voor de uitvoering van de loonbelasting en sociale verzekeringen wel gezien als een (zogenoemd fictief) dienstverband. Hieraan zijn bepaald risico's verbonden voor de inlener!)

Het vierde criterium, het verrichten van aldaar gebruikelijke arbeid, wordt doorgaans ook van toepassing geacht. 'Gebruikelijke arbeid' dient men niet aldus op te vatten, dat het arbeid zou moeten betreffen met een directe relatie tot de ondernemingsactiviteit. Schoonmaakwerkzaamheden bijvoorbeeld zijn in iedere organisatie gebruikelijk en niet slechts voor schoonmaakbedrijven. Evenzo zijn automatiseringsactiviteiten tegenwoordig voor iedere organisatie wel aan te merken als 'gebruikelijke arbeid'. Dit spreekt des te meer voor organisaties die zelf over een automatiseringsafdeling beschikken, hetgeen veelal het geval blijkt. Dat detachering soms wel geschiedt met het oog op een specifiek project of specialistische kennis, doet hier niet aan af.

De conclusie, dat bodyshopping onder de werking van de Arbvowet valt, lijkt dan ook gerechtvaardigd. Op grond van art. 90 Arbvowet zou het softwarehouse derhalve over een vergunning dienen te beschikken.

6.3.2 De vergunning

We hebben kunnen constateren dat bodyshopping als activiteit niet direct in strijd lijkt te zijn met de doelstellingen van de Arbvowet, zodat speciale aandacht hiervoor van de wetgever niet noodzakelijk lijkt. Desalniettemin hebben we eveneens geconstateerd dat de activiteit wel onder het begrippenkader van de Arbvowet moet worden geplaatst. Softwarehuizen die aan detachering doen, dienen in beginsel dus over een vergunning te beschikken. Aan een vergunning is echter een aantal beperkingen verbonden, waardoor de praktijk van detachering op gespannen voet komt te staan met de wettelijke verplichtingen.

Zo noemt art. 93 lid 1 Arbvowet het verbod om aan de ter beschikking gestelde arbeidskrachten belemmeringen in de weg te leggen om met derden een dienstverband aan te gaan. Op het eerste gezicht lijkt dit een bepaling die een redelijk doel dient, namelijk dat arbeidskrachten die door uitzendbureaus op tijdelijke basis in een organisatie te werk worden gesteld, de mogelijkheid

niet wordt ontnomen om met deze organisatie een dienstverband voor onbepaalde tijd aan te gaan.

Voor de automatiseringsbranche wordt met dit verbod het paard achter de wagen gespannen. Zoals gememoreerd, wordt automatiseringspersoneel veelal ingehuurd om hun specifieke deskundigheid. Gelet op de ontwikkelingen in de automatisering is de kennis van automatiseringsdeskundigen bovendien aan snelle veroudering onderhevig. We zien dan ook, dat softwarehuizen vele tienduizenden guldens investeren in een permanent opleidingstraject voor hun medewerkers. Indien zij deze investering niet kunnen veilig stellen, door het maken van afspraken met inleners om geen personeel over te nemen en het maken van afspraken met hun medewerkers in de sfeer van een concurrentiebeding ex art. 1637x BW of desnoods het terugbetalen van de opleidingskosten, zal de animo om in opleidingen te investeren zeer snel aflopen. Uiteindelijk is daar niemand mee gebaat. De inlener kan geen hoog opgeleid personeel meer inhuren op tijdelijke basis, de werknemers worden niet meer geschoold en de uitlener ziet zijn nering teruglopen. Voor een goed begrip wordt hier nog eens gewezen op de situatie dat dit automatiseringspersoneel, anders dan bijvoorbeeld een via een uitzendbureau uitgezonden secretaresse of een elektrisch lasser, vaak al een arbeidsovereenkomst voor onbepaalde tijd *heeft*, namelijk met de uitlener.

Andere beperkingen treffen we aan in art. 94 lid 2 Arbvowet. Naast een uitgebreide administratieverplichting wordt gesteld dat de beloning en andere vergoedingen die de arbeidskracht geniet in verhouding dienen te staan met die in de inlenende organisatie, en dat de maximale duur van de ter beschikking stelling ten hoogste zes maanden (of 12 maanden indien niet full time) mag bedragen.

Ook deze bepalingen lijken vooral geïnspireerd door de bepalingen uit de vroegere WTBA ter bescherming van werknemers in de traditionele uitzendbranche. De duurbeperking geschiedt met het oog op de ontwijking van regels met betrekking tot de maximale proeftijd en ontslagbescherming, en moet voorkomen dat bedrijven personeel uitsluitend nog zouden aanstellen via uitzendbureaus. Automatiseringsprojecten duren vaak langer dan de hier genoemde termijn, veelal zelfs ‘semi-permanent’, terwijl eerder al is geconstateerd dat het aspect van bescherming van de rechtspositie van automatiseringsdeskundigen niet zo urgent is. Gelet op de relatieve schaarste van automatiseringsdeskundigen en het specialistische karakter, ligt de honorering doorgaans hoger dan in de inlenende organisaties.

Op grond van deze ongewenste neveneffecten is wel een uitzondering bepleit voor bepaalde branches (ook de activiteiten van accountants, van organisatieadviesbureaus, binnen de bouw/metaal of van geprivatiseerde voormalige overheidsdiensten bijvoorbeeld zouden wellicht zijn aan te merken als

detachering), of op basis van algemene kenmerken van een bepaalde vorm van uitlening. Hoewel de wet daartoe de mogelijkheid biedt, meent het Centraal Bestuur van de Arbeidsvoorziening, een tripartiet samengesteld orgaan waarin werkgevers, werknemers en de overheid participeren en dat belast is met de uitvoering van de Arbvowet, nochtans dat de wetgever dan maar in dergelijke uitzonderingen moet voorzien.

Er doet zich overigens de merkwaardige situatie voor, dat aanvragen noch worden afgewezen, noch worden toegekend. Het ziet er naar uit dat van een niet-officieel gedoogbeleid sprake is. 'Boze tongen' beweren dat de reden daarvoor onder meer is gelegen in het feit dat de overheid zelf een van de grootste bodyshoppers is.

Het ter beschikking stellen van arbeidskrachten zonder over de daarvoor vereiste vergunning te beschikken, is niet zonder gevolgen. Zo levert schending van de Arbvowet op een economisch delict in de zin van de Wet op de Economische Delicten. Voorts is in een uitspraak van de Hoge Raad (28 juni 1991, NJ 1991, 787) een uitleenovereenkomst nietig verklaard, wegens het ontbreken van een vergunning.

6.4 Inlenersaansprakelijkheid

Een ander aspect van bodyshopactiviteiten betreft de 'inlenersaansprakelijkheid'. Art. 16a van de Coördinatiewet Sociale Verzekeringen, de Wet op de Loonbelasting 1964 en art. 34 van de Invorderingswet 1990 bepalen dat de inlener hoofdelijk aansprakelijk is voor de afdracht van sociale premies respectievelijk loonbelasting en omzetbelasting die de uitlener verschuldigd is in verband met de werkzaamheden van de uitgeleende arbeidskracht.

Deze bepaling is in het leven geroepen in het kader van de anti-misbruik wetgeving. Evenals in het geval van onderaanneming (waarvoor in art. 16*b* CSV de ketenaansprakelijkheid in het leven is geroepen) beoogt de regeling van de inlenersaansprakelijkheid te voorkomen dat (malafide) bedrijfjes gedurende zekere tijd inkomsten verwerven uit de ter beschikking stelling (c.q. de onderaanneming), over die inkomsten geen afdrachten doen en vervolgens failliet gaan waardoor de fiscus het nakijken heeft. In zo'n situatie kunnen de sociale premies en de loon- en omzetbelasting volledig verhaald worden op de inlener (c.q. de aannemer).

Omdat hiermee grote bedragen gemoeid kunnen zijn, is het voor een inlener van groot belang zich tegen deze aansprakelijkheid in te dekken. Wat natuurlijk *niet* helpt, is deze aansprakelijkheid bij contract met de uitlener uitsluiten. Deze is immers failliet wanneer het op betalen aankomt. En een exoneratie kan men nu eenmaal niet een derde tegen werpen, die geldt slechts tussen

partijen. Bovendien is het de wetgever er nu juist om te doen geweest de inlener er in te betrekken.

Art. 16a lid 2 CSV lijkt de helpende hand te bieden. Dit artikel maakt het de inlener mogelijk zich tegen de hier bedoelde inlenersaansprakelijkheid te vrijwaren, indien hij melding maakt bij de bedrijfsvereniging dat hij gebruik maakt van ter beschikking gestelde arbeidskrachten. Echter, dit artikel is alleen van toepassing indien de terbeschikkingstelling geschiedt met gebruikmaking van een vergunning als bedoeld in art. 90 van de Arbvowet ('zo deze is vereist').

Hierboven hebben we geconstateerd dat softwarehuizen die detachering verzorgen, formeel over een vergunning dienen te beschikken, doch dat tot heden geen vergunningen zijn afgegeven. Zo zien we de merkwaardige paradox dat enerzijds de overheid de inlener een wettelijke mogelijkheid biedt aan zijn inlenersaansprakelijkheid te ontkomen, terwijl dat anderzijds, tengevolge van het gedoogbeleid, weer onmogelijk blijkt. Het wachten is op een faillissement van een softwarehouse dat tevergeefs een vergunningsaanvraag heeft ingediend, opdat de inlener dit gedoogbeleid ter toetsing aan de rechter kan voorleggen.

Nu art. 16a lid 2 niet schijnt te helpen, is het zaak voor inleners zich te bezinnen op andere mogelijkheden om de hieraan verbonden risico's te beperken. In de bouw kennen we het verschijnsel van de zogenoemde 'g-rekening'. Dit is een geblokkeerde rekening waarop de aannemer rechtstreeks ten behoeve van de fiscus de verplichte afdrachten van de onderaannemer stort. Deze optie wordt gecreëerd door art. 16*b* lid 5 CSV. Maar omdat 16b expliciet handelt over *keten*aansprakelijkheid, waar art. 16a handelt over inlenersaansprakelijkheid, wordt deze figuur niet van toepassing geacht op het verschijnsel bodyshopping (en andere uitzendactiviteiten). Wat rest de inlener dan nog wel? Er zijn helaas geen opties met absolute zekerheid, maar hij kan:

- bedingen dat de uitlener alleen eigen werknemers ter beschikking stelt;
- periodiek (ieder kwartaal?) verklaringen eisen van de externe accountant van de uitlener, waaruit blijkt dat deze aan zijn betalingsverplichtingen jegens de fiscus en de bedrijfsvereniging heeft voldaan. (Deze optie laat naheffingen overigens onverlet.);
- zelf de premies en de belastingen inhouden op de faktuur en deze bedragen in de vorm van een derdenbetaling, een betaling namens de uitlener, rechtstreeks overmaken naar de fiscus en de bedrijfsvereniging. (Ook hier zij opgemerkt, dat een dergelijke betaling de inlener geenszins hoeft vrij te pleiten van zijn verplichting op basis van de inlenersaansprakelijkheid.)

Voorts zien we steeds vaker dat contracten zo geredigeerd worden dat ze niet meer uitdrukkelijk onder de Arbvowet vallen. Een voorbeeld hiervan is de Service Level Agreement (SLA), waarin de detacheringsactiviteiten allengs

meer gekoppeld worden aan concrete prestatieverplichtingen met betrekking tot de te ontwikkelen software. Wat de inlener in ieder geval kan doen is uitsluitend in zee gaan met bona fide en solvabele ondernemingen.

Het is de verwachting dat het arbeidsrecht in de komende tijd nog een grondige revisie zal ondergaan. Algemeen wordt de wettelijke ontslagbescherming tegenwoordig als te rigide gezien, hetgeen een nadelig effect zou hebben op de bereidheid van werkgevers om personeel aan te nemen. Inmiddels is het zo dat bij de aanvraag voor een ontslagvergunning bij de directeur van het Regionaal Bureau voor de Arbeidsvoorziening niet meer behoeft te worden gewacht met het ingaan van de opzeggingstermijn tot de ontslagvergunning is verleend.

Andere ontwikkelingen die aan een veranderend arbeidsrecht ten grondslag liggen, zijn de pogingen om het voor werkgevers aantrekkelijker te maken langdurig werklozen in dienst te nemen, verlaging van de kosten van arbeid en vooral ook flexibilisering van de arbeidsmarkt. Een aspect van die flexibilisering is het verschijnsel telewerken. Het is denkbaar dat werknemers in de toekomst meer dan thans als min of meer zelfstandigen hun arbeidskracht aanbieden, waarbij zij hun werkzaamheden thuis achter de computer voor hun verschillende 'werkgevers' kunnen verrichten.

6.5 Jurisprudentie

HR 28 JUNI 1991, VERKERK - BOUWSERVICE DOETINCHEM, nj 1992, 787
Uitleenovereenkomst zonder de daarvoor vereiste vergunning leidt tot de nietigheid van de tussen uitlener en inlener gesloten overeenkomst.

RB UTRECHT, K.G. 14 JUNI 1994, DATATEAM - TAS INFORMATICA, KG 1994, 263
Detachering van computerprogrammeur, in tijdelijke dienst van eiseres, valt onder de werkingssfeer van de Arbeidsvoorzieningswet. Eiseres mocht haar werknemer derhalve niet beperken in zijn mogelijkheden bij gedaagde of bij een andere werkgever in dienst te treden.

CENTRALE RAAD VAN BEROEP, 22 JUNI 1994, AB 1995, 15.
G-rekening alleen van toepassing bij ketenaansprakelijkheid

HOF LEEUWARDEN, 27 SEPTEMBER 1994, ipas 1189-1993
Detachering zonder de vereiste vergunning levert een economisch delict op.

6.6 Literatuur

- Esch, R.E. van, 'Bodyshopping, De Arbeidsvoorzieningswet', in: Computerrecht 1992/1.
- Francovich, S.G. en M.J. Vos, 'De nieuwe Arbeidsvoorzieningswet en het ter beschikking stellen van arbeid', in: Sociaal recht, 1991/5.
- Frielink, K. En H.J. van Straaten, 'Softwarehuizen in wurggreep van vergunning?', in: Sociaal recht, 1990/10.
- Houte, Y.A.E. van, 'Detacheren en ter beschikking stellen; de wetgeving en de realiteit', in: Sociaal recht, 1995/9.
- Schelven, P.C. van en M.C. Paap, 'Detachering in de automatiseringsbranche', in: Sociaal recht, 1995 nr. 9.
- Vries, H.H. de, 'Juridische aspecten van huistelematica: telewerken en consumeren in het informatietijdperk', (diss.), Kluwer, Deventer, 1993.

7 Computercontracten en aansprakelijkheid

Het opstellen van computercontracten is een complexe materie, niet in het minst vanwege de moeilijke beheersbaarheidsgraad van automatiserings-projecten. Juristen - en ook afnemers - tenderen daarom nogal eens tot het zoveel mogelijk fixeren van de verplichtingen van leveranciers in het contract. Termen in dit verband zijn ‘fixed price’, ‘fixed date’, ‘fixed functionality’ en ‘fixed quality’. Voordat hiermee de illusie wordt gewekt dat alles dan ook goed geregeld zal zijn, is het verstandig eerst eens te kijken naar de karakteristieken van automatiseringsprojecten, om te bezien of zij wel op deze wijze beheers-baar zijn (paragraaf 7.1).

Automatiseringsovereenkomsten zijn er voorts in alle ‘soorten en maten’, hetgeen een scala van mogelijke aandachtspunten zou opleveren. Wat echter voor alle automatiseringsprojecten geldt, is dat zij eenzelfde traject doorlopen. In iedere fase van dit traject, van pre-contractuele fase tot en met garantie en onderhoud, zijn verplichtingen te onderkennen (paragraaf 7.2).

Nadat in paragraaf 7.3 (aansprakelijkheid uit wanprestatie) de vermeende effectiviteit van de hierboven weergegeven juridische insteek aan een kritische beschouwing is onderworpen, zal in paragraaf 7.4 een aanzet worden gegeven de verschillende contractuele aandachtspunten als een soort checklist te rangschikken.

7.1 Karakteristieken van automatiseringsprojecten

Als karakteristieken van automatiseringsprojecten onderscheiden we in deze paragraaf achtereenvolgens de ongelijkheid tussen partijen (7.1.1), produkt van samenwerking (7.1.2), vitaal belang (7.1.3) en de lange duur van de samenwerking (7.1.4).

7.1.1 Ongelijkheid tussen partijen

De ongelijkheid van partijen komt onder meer tot uiting in het verschil in kennis, verplichtingen en ervaring.

Leveranciers worden geacht meer deskundig te zijn op het vlak van automatisering dan hun afnemers. Zo dit ten opzichte van grotere afnemers niet in het algemeen zou gelden, gaat dit weer wel op voor de specifiek door de leverancier te ontwikkelen c.q. ter beschikking te stellen applicatie. Afnemers daarentegen zijn weer bij uitstek de partij die kennis draagt van alle ‘ins’ en ‘outs’ rondom de eigen organisatie, werkwijze en gewenste eindtermen, de zogenoemde ‘materiedeskundigheid’.

Bezien we de bepalingen in een automatiseringsovereenkomst goed, dan zal veelal blijken dat het leeuwendeel van de verplichtingen op de schouders rust van de leverancier. Hoewel er wel enige verplichtingen tot meewerken van de zijde van de afnemer bestaan, lijkt diens belangrijkste verplichting toch te zijn die tot betaling. Zonder nadere beperking zouden de risico’s verbonden aan de uitvoering van het project derhalve voor een belangrijk deel worden afgewenteld op de leverancier.

Automatiseringsactiviteiten beslaan het dagelijkse doen en laten van de leverancier. Voor afnemers zijn automatiseringsactiviteiten veelal incidenteel. Hetzelfde kan gezegd worden over de opstelling van automatiseringsovereenkomsten.

7.1.2 Produkt van samenwerking

Automatiseringsprojecten worden als produkt van samenwerking gekenmerkt doordat het eindresultaat niet voor 100% bepaalbaar is, het veelal een iteratief proces betreft, dat niet in een keer foutloos kan worden doorlopen.

Een computerprogramma kan uit tienduizenden programmaregels bestaan, opgesplitst in honderden programmabestanden, die op de meest uiteenlopende wijzen met elkaar in verbinding worden gebracht. Er zullen altijd combinaties van gebruikershandelingen kunnen optreden waarin door de programmeurs niet is voorzien. Hierdoor komen dan de zogenoemde ‘bugs’ aan het licht, die ervoor zorgen dat het computerprogramma ‘vastloopt’.

Natuurlijk is er een samenhang tussen de kwaliteit van de programmeurs en het aantal voorkomende bugs, maar het is een illusie te veronderstellen dat volledig bugsvrije software kan worden ontwikkeld.

Voorts is het doorgaans niet mogelijk om het eindresultaat van automatiseringsprojecten van tevoren voor 100% te definiëren. De uitwerking is dermate complex, waarbij zo veel onvoorziene gevolgen kunnen optreden, dat volstaan moet worden met een zo goed mogelijk op hoofdlijnen vastgelegde projectbeschrijving. Ook hier geldt dat het een illusie is te menen dat een projectbeschrijving - evenmin als een contract - volledig c.q. uitputtend kan zijn.

Dit heeft tot gevolg dat software-ontwikkeling plaats heeft in de vorm van een iteratief proces van ontwikkelen, testen en bijstellen, dat bovendien een nauwe interactie tussen leverancier en afnemer veronderstelt.

7.1.3 Vitaal belang

Automatiseringsactiviteiten zijn van vitaal belang voor organisaties, voor wat betreft hun invloed op de interne organisatie en de continuïteit.

Automatiseringsactiviteiten kunnen nooit worden ondernomen zonder dat zij van invloed zijn op de bestaande interne organisatie. (Soms zijn zij zelfs van invloed op de externe organisatie, bijvoorbeeld de communicatie door middel van electronic data interchange - zie hoofdstuk 9.) Werkzaamheden worden anders georganiseerd, de uitvoering wordt anders en de werkplek verandert. Een belangrijke factor is ook dat het personeel voldoende affiniteit met de nieuwe situatie moet krijgen en goed moet worden opgeleid.

Organisaties die van het ene (geautomatiseerd) systeem overschakelen op een ander, komen in een kwetsbare situatie te verkeren. Een nieuw automatiseringsproject dat faalt, terwijl men het oude systeem reeds heeft verlaten, kan een organisatie in zijn voortbestaan raken. Een tweede argument met betrekking tot de continuïteit van de organisatie is gelegen in de mate van afhankelijkheid van het geautomatiseerd systeem.

En, tenslotte, ook het strategisch belang van informatietechnologie wordt steeds groter.

7.1.4 Langdurig

Leveranciers en afnemers van automatiseringsprodukten dienen zich te realiseren dat zij een langdurig samenwerkingsverband aangaan, dat zich uitstrekt van ontwikkeling en implementatie tot en met garantie en onderhoud.

Met de ontwikkeling van software is een behoorlijke spanne tijds gemoeid. In die periode kunnen eisen van buiten dan wel binnen de organisatie bovendien nogal eens tot de nodige aanpassingen van het ontwerp dwingen.

Het implementatietraject, dat bestaat uit het toesnijden van de software op de organisatie van de afnemer en uit het opleiden van de gebruikers, is eveneens een langdurige aangelegenheid.

Is het systeem eenmaal ontwikkeld, geïnstalleerd en geïmplementeerd, dan breekt de fase aan waarin het systeem geschikt gehouden moet worden voor de toepassing van de afnemer. Hiervoor zijn verschillende oorzaken aan te geven. In de loop der tijd zullen er wijzigingen optreden in de organisatie van de afnemer, wettelijke voorschriften kunnen veranderen, de onderliggende besturingssoftware kan wijzigen, er kunnen nieuwe wensen opkomen e.d. Het is dan van belang om zeker te stellen dat de hiermee gemoeid zijnde werkzaamheden gedurende een aantal jaren zullen worden verricht.

7.2 Traject

Een automatiseringstraject kunnen we, afgezet in de tijd, onderverdelen in verschillende stadia: de precontractuele fase (7.2.1), de fase van tot stand koming van de overeenkomst (7.2.2), de uitvoering van het contract (7.2.3) en de garantie en onderhoud van het geleverde (7.2.4). In iedere fase zijn juridische verplichtingen te onderkennen.

7.2.1 Precontractuele fase

Onder de precontractuele fase verstaan we de (onderhandelings)fase waarin er nog geen contract is gesloten. In deze fase worden niettemin over en weer reeds verschillende verplichtingen onderkend:

Zowel op leveranciers als op afnemers rust in deze fase de verplichting voldoende informatie te verstrekken over de mogelijkheden van het systeem, respectievelijk de organisatie en wensen van de afnemer. Hoe groter het verschil in deskundigheid tussen afnemer en leverancier, des te zwaarder komt deze verplichting te drukken op de laatste. Leveranciers dienen zich in deze fase enigszins op te stellen als adviseur. Op het verweer dat de leverancier niet aansprakelijk gehouden kon worden voor de ondeskundigheid van de afnemer, waar deze zich toch had kunnen laten bijstaan door een automatiseringsadviseur, oordeelde de rechter dat in het algemeen van een dergelijke verplichting voor de afnemer geen sprake is.

De informatieplicht van leveranciers is niet beperkt tot het slechts passief verstrekken van informatie over het systeem. Zij dienen zich daarbij actief op te stellen en te onderzoeken of de voorgestane oplossing ook geschikt is voor

de door de afnemer gewenste toepassing en voor zijn organisatie. Deze onderzoeksplicht omvat mede een waarschuwingsplicht aangaande eventuele beperkingen van het systeem, of van een door de afnemer gewenste aanwending daarvan. De waarschuwingsplicht gaat hier echter niet zo ver als bij een automatiseringsadviseur, in die zin dat leveranciers niet gehouden zijn te wijzen op het bestaan van andere, meer geschikte toepassingen van derden.

De wederzijdse informatieplichten kunnen met zich mee brengen dat vertrouwelijke informatie moet worden uitgewisseld. Is het zo, dat op grond van de goede trouw reeds een geheimhoudingsplicht wordt aangenomen voor de in dit kader vertrouwelijk ter beschikking gestelde informatie, afhankelijk van het belang van deze informatie is het niettemin raadzaam daartoe een separate voorovereenkomst aan te gaan.

Tenslotte wordt er hier op gewezen dat wanneer onderhandelingen zich in een vergevorderd stadium bevinden, er in sommige situaties een verplichting is ontstaan tot dooronderhandelen. Men mag de onderhandeling niet meer eenzijdig afbreken.

7.2.2 Tot stand koming

Bij de tot stand koming van automatiseringsovereenkomsten dienen we te bedenken dat er veelal geen sprake is van een enkele overeenkomst, maar van diverse overeenkomsten, en moeten we rekening houden met vormvereisten en wilsgebreken.

Bij complexe automatiseringsprojecten is vrijwel nooit sprake van het sluiten van slechts een enkele overeenkomst. Vaak zien we dat tussen leveranciers en afnemers zogenoemde raamovereenkomsten worden gesloten, binnen welk kader diverse specifieke overeenkomsten worden aangegaan. Dit kunnen zowel benoemde (huur of koop), als onbenoemde (licenties) overeenkomsten zijn. Van belang hierbij zijn de in het BW opgenomen bepalingen van regelend recht, regels dus die gelden voorzover er niet bij overeenkomst van is afgeweken. Voorbeelden van specifieke automatiseringsovereenkomsten zijn: de koop, huur of lease van hardware, de ontwikkeling van of de licentieverlening op software en het verrichten van diensten zoals implementatie, opleiding, conversie, interfacing e.d.

In beginsel is ons contractenrecht vormvrij. Er is een beperkt aantal verbintenissen waarvoor de wet een bepaalde vorm voorschrijft. Te denken valt aan de verkoop en levering van onroerende goederen en colportageverkoop. Met betrekking tot automatisering is van belang te weten dat voor de overdracht van auteursrechten een authentieke (notariële) of onderhandse (een gedateerd schriftelijk stuk ondertekend door partijen) akte vereist is. Hoewel in het algemeen dus geen vereiste geldt dat overeenkomsten schriftelijk moeten zijn aangegaan, is het wel de praktijk, en zeer verstandig met het oog

op het bewijs van de bestaanbaarheid van de overeenkomst en op hetgeen wat men daarbinnen is overeengekomen.

Voorts is op de tot stand koming van overeenkomsten natuurlijk het algemene leerstuk van de wilsgebreken van toepassing (bedreiging, bedrog en misbruik van omstandigheden (art. 3:44 BW) en dwaling (art. 6:228 BW)).

7.2.3 Uitvoering

In de fase van uitvoering van het project spelen aspecten als wanprestatie een rol en de vraag of een tekortkoming toerekenbaar is. Levert dit voorts een grond voor aansprakelijkheidsstelling op, of is aansprakelijkheid uitgesloten of beperkt, eventueel met een vrijwaringsbeding.

In de bespreking van de aansprakelijkheid uit wanprestatie in paragraaf 7.3 en bij de opstelling van de contractsindeling in paragraaf 7.4 worden deze aandachtspunten nader geconcretiseerd.

7.2.4 Garantie/onderhoud

Is een automatiseringsproject eenmaal uitgevoerd en geïmplementeerd, dan breekt de fase van garantie aan, gevolgd door de periode waarin het systeem moet worden onderhouden. Hierin is van belang de aanvang en duur van de betreffende periodes, de inhoud van garantiebepalingen en onderhoudsovereenkomsten, en de ‘verzekering’ dat onderhoud bij een eventueel wegvallen van de leverancier kan blijven worden uitgevoerd, door middel van een source code regeling.

In de meeste automatiseringsovereenkomsten komen we garantiebepalingen tegen. Onderhoud wordt meestal geregeld in separate onderhoudsovereenkomsten. Als het goed is, sluiten garantiebepalingen terzake van de werking van het systeem naadloos aan bij de afspraken in de onderhoudsovereenkomst. Garantie maakt onderdeel uit van de prijs van het project. De ingangsdatum en de duur van de garantie zijn van belang, vanwege de samenhang met de ingang van de onderhoudsovereenkomst, dus met de aanvang van de betaling van de onderhoudsvergoeding. Vragen daarbij zijn of de garantie ingaat op het moment van levering (installatie), het moment van testen, het moment van oplevering (implementatie) het moment van geaccepteerde oplevering, of enig moment daarna, en voorts of de garantietermijn wordt verlengd met de duur die nodig is gebleken om fouten te herstellen.

De inhoud van de garantie zien we doorgaans terug in de onderhoudsovereenkomst. Daarmee wordt het belang van garantie relatief en gereduceerd tot een prijskwestie. Wordt een garantie verleend van bijvoorbeeld twaalf maanden, dan zal in de projectprijs het bedrag van de jaarlijkse onderhoudsvergoeding zijn opgenomen. Een aspect dat wel de aandacht verdient is in hoeverre een garantie niet vooral de werking zal krijgen van het uitsluiten van aansprakelijkheid voor de goede werking van het systeem. Een garantiebepaling wil tenslotte niet meer zeggen dan dat de leverancier met de afnemer is overeengekomen dat de eerste alleen maar zou behoeven in te staan voor hetgeen hij daarin uitdrukkelijk garandeert, gedurende de daarin opgenomen termijn. Vanuit deze optiek wordt wel beweerd dat een overeenkomst zonder expliciete garantie voor de afnemer aantrekkelijker kan zijn.

Om software te kunnen onderhouden, is het nodig om over de sourcecode te beschikken. Veel afnemers treffen daartoe een voorziening met de leverancier in de vorm van een sourcecode escrow. Dit is een overeenkomst tussen drie partijen: de leverancier, de afnemer en een derde aan wie een exemplaar van de sourcecode in bewaring wordt gegeven. In de overeenkomst wordt vastgelegd dat in het geval zich bepaalde omstandigheden aandienen, zoals het faillissement van de leverancier dan wel andere omstandigheden waardoor onderhoud niet langer wordt uitgevoerd, de bewaarnemer de sourcecode ter beschikking stelt van de afnemer. Deze mag het softwareonderhoud vervolgens zelf uitvoeren, of laten uitvoeren door een door hem in te schakelen derde. Een software-escrow moet derhalve bepalingen bevatten die de escrow-agent de bevoegdheid (in zijn relatie tot de leverancier) en de verplichting (in zijn relatie met de afnemer) verschaffen de software ter hand te stellen van de afnemer bij het intreden van met name genoemde omstandigheden, alsmede bepalingen die de afnemer bevoegd maken dit onderhoud te (laten) verrichten.

Werden broncodes in het verleden nog wel eens gedeponeerd bij een notaris, tegenwoordig is het gebruikelijk dat partijen zich wenden tot een daarin gespecialiseerde dienstverlener. Deze heeft de kennis om vast te kunnen stellen of het gedeponeerde daadwerkelijk de bedoelde software is, hij kan behulpzaam zijn met conversies en hij houdt toezicht op het up-to-date houden van het softwaredepot met nieuwe versies en documentatie.

7.3 Aansprakelijkheid uit wanprestatie

Op grond van art. 6:74 BW is de schuldenaar verplicht de schade te vergoeden die de schuldeiser lijdt tengevolge van een aan de schuldenaar toerekenbare tekortkoming in de nakoming van de verbintenis. Er is sprake van een *tekortkoming* indien de schuldenaar niet, niet tijdig, niet geheel of gebrekkig presteert. Is de tekortkoming toerekenbaar aan de schuldenaar, dan staan de

schuldeiser in beginsel de volgende *vorderingen* ter beschikking: nakoming, vervangende schadevergoeding of ontbinding van de overeenkomst, alledrie met de mogelijkheid tot vordering van aanvullende schadevergoeding.

De mogelijkheid om met succes een dergelijke vordering te kunnen instellen, moet worden bezien tegen de achtergrond van het in het contractenrecht geldende beginsel van *contractsvrijheid*. Partijen zijn vrij om met elkaar verbintenissen aan te gaan, voorzover deze niet ingaan tegen de wet, de openbare orde of de goede zeden.

In de praktijk betekent dit dat overeenkomsten veelal worden ingekleurd door standaardvoorwaarden, meestal van de zijde van leveranciers. Voorts dient men zich te realiseren dat de contractsvrijheid met zich mee brengt dat exoneraties - uitsluiting of beperking van aansprakelijkheid - zijn toegestaan. Daar tegenover staat weer dat niet altijd met succes een beroep gedaan kan worden op een exoneratie, tengevolge van de beperkende werking door de 'goede trouw'

In de volgende paragrafen zullen we nagaan of dit juridisch instrumentarium voldoende waarborg is voor het doen slagen van een automatiseringsproject. Daartoe zullen enkele praktijkvoorbeelden uit algemene voorwaarden van leveranciers de revue passeren.

7.3.1 Toerekenbare tekortkoming?

In veel algemene voorwaarden lezen we onder art. X, 'Aansprakelijkheid', dat de leverancier aansprakelijk is voor de schade tengevolge van *niet-tijdige* levering. Op het eerste gezicht lijkt dit een alleszins acceptabel uitgangspunt. Bij nadere bestudering echter van de algemene voorwaarden blijken verschillende artikelen deze aansprakelijkheid veelal te beperken:

- leveringstijden zijn 'naar beste weten' opgegeven; bij overschrijding daarvan heeft leverancier de verplichting met afnemer te *overleggen*;
- de afnemer heeft zelf verschillende verplichtingen tot meewerken;
- wijzigingen door afnemer hebben vertraging in de leveringstijd tot gevolg;
- afnemer dient 'alle gewenste inlichtingen' te verschaffen.

Evenzo lezen we vaak dat ingeval van *gebrekkige levering* de leverancier fouten zonder kosten zal herstellen. Hier doet zich echter de complicatie voor hoe vast te stellen wanneer er nu eigenlijk sprake is van 'fouten'. De volgende aandachtspunten spelen hierbij een rol:

- 'fouten' ten opzichte van definities;
- 'fouten' ten opzichte van handleiding;
- 'fouten' ten opzichte van produktspecificaties;

- ‘fouten’ ten opzichte van niet benoemde, maar vanzelfsprekende eigenschappen;
- vierhoekenbeding (alleen hetgeen uiteindelijk expliciet ‘binnen de vier hoeken’ van het contract is opgenomen geldt);
- ‘leverancier is niet aansprakelijk voor adviezen gedaan voordat de overeenkomst tot stand kwam’;
- ‘de software is niet geschikt voor een speciaal doel’;
- ‘klant is verantwoordelijk voor keuze van de programmatuur’;
- garanties.

Het gevolg is dat vaak niet duidelijk is of en aan wie nu de vertraging of de gebrekkige levering is toe te rekenen. Maar veronderstel dat zou kunnen worden vastgesteld dat de leverancier inderdaad in gebreke is gebleven, dat de niet-tijdige en/of gebrekkige levering inderdaad zijn aandeel is, dan rest nog de vraag of de tekortkoming hem wel valt toe te rekenen. In dit verband speelt bijvoorbeeld het begrip overmacht een rol.

Niet zelden treffen we in algemene voorwaarden aan - ‘verdekt opgesteld’ tussen oorlogen, atoom- en natuurrampen - dat stakingen in het bedrijf van leverancier of diens toeleveranciers onder overmacht worden begrepen. Dit, terwijl in de jurisprudentie is uitgemaakt, dat zonder deze exoneratie stakingen niet onder het overmachtsbegrip vallen. Tenzij een toeleverancier door de afnemer is voorgeschreven, ligt de keuze voor werknemers, arbeidsvoorwaarden en toeleveranciers in de risicosfeer van de leverancier ligt.

Indien echter de tekortkoming toerekenbaar is aan de leverancier, dan nog is het niet zeker dat met succes een beroep op de aansprakelijkheidsbepaling gedaan kan worden. Vaak treffen we in de algemene voorwaarden dan nog op verschillende plaatsen bepalingen aan, waarin verplichtingen van afnemer zijn opgenomen. Indien hij daaraan niet heeft voldaan, kan de afnemer niet altijd aanspraak maken op de toezegging van de leverancier. Zo dient afnemer:
- de laatste versies van het programma en van de besturingssoftware te hebben geïnstalleerd (soms echter, is dit voor hem niet wenselijk);
- geen aanpassingen aan de programmatuur te hebben gemaakt;
- geen verbindingen te hebben met niet door leverancier goedgekeurde modems, interfaces, en programmatuur;
- binnen een bepaalde tijd te reageren;
- zelf tijdig back-ups te maken;
- het transportrisico te dragen.

Tot slot wordt hier nog gewezen op de veelal expliciet opgenomen *algemene beperkingen* van de aansprakelijkheid van de leverancier. Dus, is de afnemer in staat om aan te tonen dat de leverancier daadwerkelijk in gebreke is gebleven,

bovendien toerekenbaar en dat hijzelf aan al zijn verplichtingen heeft voldaan, dan wordt hij nog geconfronteerd met beperkingen zoals:

- De hoogte van schadevergoeding is meestal gemaximeerd. In het geval van duurovereenkomsten (bodyshopping bijvoorbeeld) is de schadevergoeding meestal beperkt tot het bedrag van de facturen over de laatste maanden.
- Indirecte of gevolgschade is vrijwel altijd uitgesloten. Voorts wordt 'schade' zo veel mogelijk onder het begrip indirecte schade gebracht.
- Een gedeelte eigen schuld van afnemer vermindert de hoogte van de schadevergoeding.
- Er was een deugdelijke ingebrekestelling vereist.

7.3.2 Opties

Gesteld dat de leverancier wel zou hebben nagekomen, indien hij daartoe in staat was, lijken van de hiervoor genoemde opties voor de afnemer de meest 'reële' die van ontbinding en/of schadevergoeding.

Zoals we hebben gezien, zijn de mogelijkheden tot schadevergoeding meestal beperkt. Bij ontbinding speelt de vraag of men dat al dan niet met terugwerkende kracht had moeten overeenkomen, of de reeds verrichte prestaties al dan niet in tact dienen te blijven (of mogen blijven).

Al met al is een beroep op een aansprakelijkheidsparagraaf een langdurige aangelegenheid, met veelal een onbevredigende oplossing. Ongeacht de afloop van een procedure, is de uitkomst dat de afnemer na al die tijd nog steeds geen werkend systeem heeft, de reputatie van de leverancier is beschadigd en beide partijen een gevoelig verlies hebben geleden. Juristen dienen zich bewust te zijn van de beperkingen van het juridisch instrumentarium, indien daarop eenmaal een beroep moet worden gedaan.

Het zal duidelijk zijn, dat het domweg willen schrappen van exoneraties geen echte oplossing biedt, en bovendien onwenselijk kan zijn. In plaats van 'schijnzekerheden' die met het fixeren van verplichtingen worden bereikt, is het beter oog te hebben voor aspecten van projectorganisatie en -begeleiding. De belangrijkste functie van een automatiseringsovereenkomst is die van *risicobeheersing*. Dat betekent dat partijen, ondersteund door juristen, in eerste instantie de risico's van het project in kaart dienen te brengen. Contractuele bepalingen dienen vervolgens ter sturing en beheersing van het project te worden aangewend, en vooral ter voorkoming dat een beroep op de aansprakelijkheidsparagraaf nodig wordt.

Een actieve, creatieve en ter zake deskundige opstelling van juristen is nodig en zij dienen bij voorkeur in een vroegtijdig stadium bij de contractsonderhandelingen te worden betrokken. Inhoudelijk zijn er reëlere opties te beden-

ken voor de hier gesignaleerde problematiek. Ter voorkoming van niet-tijdige levering, kan men beter denken aan bepalingen die, gedurende het verloop van het traject, voor enige sturing kunnen zorgen. Te denken valt aan bepalingen omtrent:

- gefaseerde oplevering, opdat tijdige bijsturing mogelijk is;
- meer mensen inzetten, zo nodig van een ander softwarehouse;
- kwaliteit mensen bepalen;
- 'redelijke', in beginsel haalbare termijnen afspreken, met hersteltermijnen;
- boeteclausules, indien 'redelijke' hersteltermijnen niet worden gehaald;
- gefaseerd betalingsschema;
- procedures ten aanzien van wijzigingen.

De hiervoor genoemde aandachtspunten zullen ook van invloed kunnen zijn ten aanzien van het voorkomen van gebrekkige levering. Daar kunnen nog bepalingen aan worden toegevoegd met betrekking tot:

- *functionele* specificaties, als basis voor 'fouten';
- het specificeren van het beoogd gebruik, opdat dit mede kan dienen voor de beoordeling van 'fouten';
- test- en acceptatieprocedures, zo mogelijk per fase;
- test- en acceptatiecriteria.

7.3.3 Conclusies

De belangrijkste conclusies ten aanzien van het aansprakelijkheidsvraagstuk zijn dat men niet te licht moet vertrouwen op het fixeren van verplichtingen, maar dat het contract vooral moet worden opgesteld met het oog op het *vermijden* dat er een beroep op een aansprakelijkheidsparagraaf nodig wordt. Als uitgangspunten daarvoor gelden:

- het doel van het automatiseringsproject formuleren;
- het analyseren van risico's die daarbij kunnen optreden;
- wat men materieel/inhoudelijk kàn beschrijven, opnemen in (de bijlagen van) het contract;
- vervolgens, waar het materieel niet meer zo goed te beschrijven is, procedures afspreken, ook ten aanzien van het omgaan met risico's en onvoorziene omstandigheden. Niet de 'toevlucht' nemen tot het vooruitschuiven of afwentelen van onbestemde risico's op de wederpartij.
- en voor het geval deze regelingen geen uitkomst zouden bieden, een flexibele geschillenregeling opnemen, waarop, laagdrempelig, gedurende de loop van het traject steeds een beroep kan worden gedaan.

In de volgende paragraaf worden drie ‘risicovelden’ onderscheiden, waarna we zullen komen tot de opstelling van een algemene contractsindeling, die als checklist zou kunnen worden toegepast.

7.4 Systematische contractsindeling

Bij de analyse van risico’s kunnen we uitgaan van drie belangrijke ‘risicovelden’: i) wanprestatie (toerekenbare tekortkoming in de nakoming), ii) garanties en daarmee samenhangende beperkingen en iii) exoneraties (uitsluiting, beperking of aanvaarding van aansprakelijkheden).

Deze indeling kent overlappingen, maar biedt niettemin drie specifieke invalshoeken die vaak als zodanig herkenbaar zijn in contracten. De indeling is echter te algemeen om een effectieve controle mogelijk te maken. Daarom worden de risicovelden toegepast op een systematische contractsindeling. Dit levert een soort matrix van ‘risicopunten’ op. Het resultaat is een lijst van vragen die risicopunten signaleren in de te onderscheiden categorieën van contractsbepalingen.

De combinatie van risicovelden en contractsindeling maakt het mogelijk automatiseringscontracten op een efficiënte en systematische manier te beoordelen. Het toepassen van de checklist is zo een vorm van risico-analyse die ook nieuwe situaties het hoofd kan bieden. Opgedane ervaringen kunnen leiden tot het toevoegen van nieuwe risicopunten aan de lijst of het afvoeren van irrelevante punten.

De methode van contractsindeling gaat uit van een categorisering van contractsbepalingen met als doel het signaleren van risico opleverende elementen. Hiertoe wordt een contract ingedeeld in de volgende categorieën:

1. De considerans (7.4.1)
   De considerans bevat de overwegingen die partijen tot het sluiten van het contract hebben bewogen. Zij is mede bepalend voor de uitleg van de overeenkomst.
2. Definities (7.4.2)
   Definities moeten er voor zorgen dat partijen aan belangrijke termen dezelfde (normatieve) betekenis en reikwijdte toekennen.
3. Primaire prestatie-verplichtingen (7.4.3)
   Deze bepalingen bevatten materiële omschrijvingen van wat men zou kunnen noemen de primaire verplichtingen, de belangrijkste prestatie-verplichtingen die voortkomen uit de overeenkomst.
4. Secundaire prestatie-verplichtingen (7.4.4)
   Deze bepalingen bevatten aanvullingen op functionele specificaties met betrekking tot performance, eisen waaronder prestaties worden geleverd, garanties e.d.

5. Procedures (7.4.5)
   Procedurele bepalingen bevatten voorschriften over hoe te handelen in onvoorziene, ongewenste situaties of ter voorkoming van deze situaties.
6. Afsluitende juridische bepalingen (7.4.6)
   Deze categorie bevat bepalingen van meer algemeen juridische aard;
7. Algemene voorwaarden (7.4.7)
   Indien van toepassing, bepalen de algemene voorwaarden bepalen het kader waarbinnen de contractsverhouding zich doorgaans afspeelt.

Deze indeling is arbitrair, andere indelingen zijn mogelijk. Indeling van een contract volgens deze methode is echter functioneel en overzichtelijk en de indeling naar betekenis van bepalingen in een bepaalde categorie maakt het zoeken naar risico's makkelijker. Het lezen en vervolgens indelen van de inhoud van een bestaand contract naar bovenstaand model kan een goede methode zijn om het contract te analyseren.

Hieronder volgt een nadere toelichting op de contractsindeling. Per categorie wordt een opsomming gegeven van onderwerpen die in dat onderdeel van het contract geregeld zouden kunnen worden. Per onderwerp wordt dan puntsgewijs aandacht besteed aan de inhoud van de bepaling die dat onderwerp regelt.

7.4.1 Considerans

De considerans geeft de overwegingen weer van beide partijen die geleid hebben tot het sluiten van de overeenkomst. De considerans bevat:
- het doel van het automatiseringsproject;
- wat iedere partij met zijn organisatie nastreeft;
- de wederzijdse verwachtingen omtrent onderwerp van de overeenkomst;

7.4.2 Definities

Definities bepalen het kader en dus mede de omvang van de te verrichten prestaties. Daarom dienen definities:
- een accurate omschrijving te bevatten van termen en begrippen;
- geen uitbreidende of beperkende voorwaarden te bevatten;
- geen specificaties te bevatten, of bij voorkeur in bijlagen.

7.4.3 Primaire prestatie-verplichtingen

Onder primaire prestaties vindt men de beschrijving van de verschillende onderwerpen, tijden, prijzen en betaling.

ONDERWERP VAN DE OVEREENKOMST

- benoeming onderwerp:
  - koop
  - huur
  - lease
  - softwareontwikkeling
  - gebruiksrecht (licentie)
  - verrichten van diensten (installatie, implementatie, conversie)
- welke rechten worden overgedragen?
- op welke goederen hebben deze betrekking?

LEVERING

- levertijden
- plaats van levering
- transport bij prijs inbegrepen?

PRIJZEN

- specificatie
- zijn prijzen en tarieven vast / veranderlijk?
- valuta, koerswijzigingen
- belastingen, wijzigingen in belastingtarieven
- bankgarantie tot zekerheid

BETALING

- facturerings- en betalingsschema
- is eigendomsoverdracht (of gebruiksrecht) gekoppeld aan betalingen?
- wel/geen opschortende werking betaling c.q. prestaties

7.4.4 Secundaire prestatie-verplichtingen

De secundaire prestaties bestaan uit nadere hoedanigheden en specificaties met betrekking tot de primaire prestaties, alsmede uit prestaties die nodig zijn voor een correcte uitvoering daarvan.

GEBRUIKSOMGEVING

- specifieke eisen met betrekking tot plaats / ruimte van levering c.q. gebruik
- performance van het geleverde in de te realiseren omgeving ; garantie

DOCUMENTATIE
- eisen die aan de documentatie worden gesteld (taal, aantal, reproduktie)

ONDERSTEUNING
- inhoud en omvang van installatie, implementatie, opleiding, conversie
- regeling voor materialen benodigd bij uitvoering van installatie e.d.

GARANTIE
- specificatie van goederen waarop de garantie betrekking heeft
- aanvangsdatum en termijn; verlenging garantie na uitval
- verplichtingen die garantie meebrengt voor leverancier
- voorwaarden waaraan gebruiker zich moet houden
- bewijslastverdeling om oorzaak van uitval aan te tonen
- termijn waarbinnen herstel aangevangen c.q. gerealiseerd zal worden
- vervanging van apparatuur / programmatuur tijdens herstel
- compatibiliteitsgarantie
- responsetijdgarantie
- ‘virusvrij’garantie
- garantie met betrekking tot internationale standaarden

ONDERHOUD
- onderhoudsverplichtingen
- sourcecode escrow; condities

GEHEIMHOUDING EN BEVEILIGING
- verplichting tot geheimhouding van vertrouwelijke gegevens wederpartij
- ‘huisregels’ die nageleefd dienen te worden
- publiciteitsmogelijkheden met betrekking tot de overeenkomst

7.4.5 Procedures

PROJECTSTRUCTUUR
- samenstelling en werkwijze van stuur- / project- / werkgroep
- taken, bevoegdheden, verantwoordelijkheden stuur- / project- / werkgroep
- hoe worden voor beide partijen bindende besluiten genomen?
- relatie besluitvorming stuurgroep ten opzichte van contract
- rol stuurgroep bij geschillenbeslechting

RAPPORTAGE
- aanwijzen projectleiding / contactpersonen
- voortgangsrapportage
- mogelijkheid tot uitvoeren audit

TIJDSCHEMA
- tijdschema van uitvoering project
- meldingsplicht met betrekking tot (te verwachten) vertragingen
- regeling met betrekking tot vertraging in de levering, uitloopmogelijkheid

ACCEPTATIE
- procedures, tests, criteria
- deelacceptaties versus eindacceptatie
- materialen benodigd bij acceptatie
- gevolgen van goed- / afkeuren

WIJZIGINGEN / MEERWERK / MINDERWERK
- is wijziging van overeengekomen specificaties toegestaan?
- verplichting tot het melden van alternatieven / betere mogelijkheden
- effecten van wijzigingen op tijdschema's en prijzen
- betalingsregeling voor meerwerk

OVERSCHRIJDEN LEVERINGSDATUM
- gevolgen van overschrijden leveringstermijn
- boeteregeling
- schadevergoeding
- gevolgen crediteursverzuim
- overmacht

BETALINGEN
- incasso
- rente bij overschrijding betalingstermijn

RISICO VOOR BESCHADIGING / VERLIES
- tijdstip van risico-overgang van te leveren goederen
- verzekeringsplicht

INTELLECTUELE RECHTEN
- intellectuele rechten van programmatuur, documentatie
- intellectuele eigendomgarantie c.q. vrijwaring
- bewijslastverdeling bij geschillen

AANSPRAKELIJKHEID
- formele eisen (ingebrekestelling)
- definiëring schade / directe schade / gevolgschade
- gevolgen: nakoming, ontbinding, schadevergoeding
- aansprakelijkheidsbeperkingen
- verzekering van risico's mogelijk?

ONDERAANNEMING
- voorwaarden voor onderaanneming

ONTBINDING
- voorwaarden voor ontbinding van overeenkomst
- formele eisen
- regeling met betrekking tot reeds geleverde prestaties
- gevolgen voor gebruiksrecht

BOETECLAUSULES
- boeteregelingen voor specifieke tekortkomingen

7.4.6 Afsluitende juridische bepalingen

VRIJWARING
- vrijwaringsregeling voor aanspraken van derden

VERZEKERINGEN
- verplichtingen tot het afsluiten van bepaalde verzekeringen

OVERDRACHT RECHTEN / VERPLICHTINGEN
- is overdracht van rechten / verplichtingen toegestaan?

OVERMACHT
- definiëring overmacht

GESCHILLEN
- bevoegde rechter
- specifieke geschillenregelingen (minitrial, arbitrage)
- toepasselijk recht
- domicilie

ALGEMENE VOORWAARDEN WEDERPARTIJ
- toepasselijkheid / uitsluiting van algemene voorwaarden wederpartij

INDIENSTNEMING WERKNEMERS WEDERPARTIJ
- regeling met betrekking tot indienstneming van werknemers van de wederpartij

BEPERKING AANSPRAKELIJKHEID
- algemeen geldend maximum schadevergoedingsbedrag
- regeling voor cumulatie van boetes

DUUR OVEREENKOMST
- duur van de overeenkomst
- verplichtingen die ook na beëindiging voortduren

7.4.7 Algemene voorwaarden

Algemene voorwaarden vormen een integraal onderdeel van een contract als er op correcte wijze naar verwezen wordt. De algemene voorwaarden fungeren als 'sluitstuk' en zullen vooral bepalingen bevatten uit de categorieën Procedures (7.4.5) en Afsluitende juridische bepalingen (7.4.6)

7.5 Jurisprudentie

RB ROTTERDAM, 7 MEI 1982, HANEMAAYER EN VAN ES - BURROUGHS, CR 1984/2
Voor een beroep op wanprestatie wegens telkens uitgestelde levering dan wel ondeugdelijke levering is niettemin een ingebrekestelling vereist.

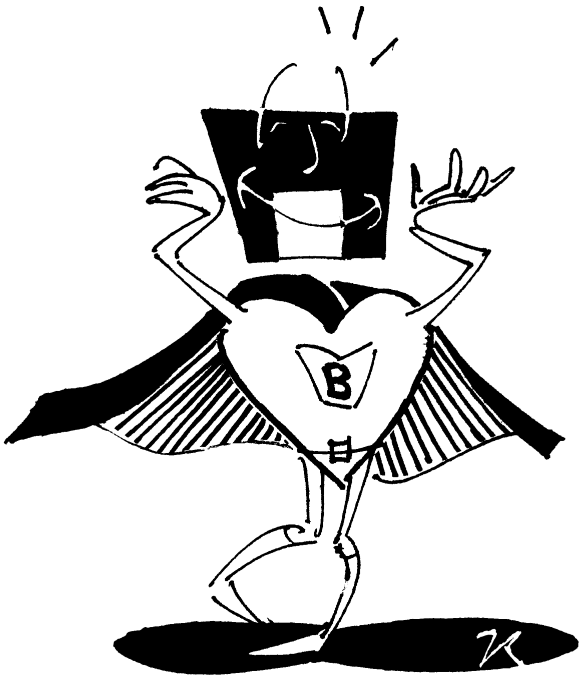
RB ROTTERDAM, 28 JANUARI 1983, X - Y, CR 1987/4
Software-ontwikkelingsovereenkomst levert resultaatverbintenis op.

Hr 11 APRIL 1986, RBC - BRINKERS, CR 1986/3
Wanneer Bronner (van RBC) de risico's, verbonden aan de gekozen snelle methode, niet voor zijn rekening wenste te nemen, had hij zulks uitdrukkelijk dienen te stipuleren. Dit spreekt temeer waar Bronner begrijpen moest en ook begrepen heeft dat in een aangelegenheid als de onderhavige de cliënt vaart op het kompas van de door hem ingeschakelde deskundige adviseur. Het door Bronner gegeven advies voldeed niet aan de mate van zorgvuldigheid die van een redelijk handelend en bekwaam automatiseringsdeskundige geëist mag worden. (Hof)

7.6 Literatuur

- Berkvens, J.M.A., J.J.F.M. Borking, C.F. van Geest, N.J. Rinkel, en H.A. van de Schraaf, 'Achter de schermen van automatiseringscontracten', Samsom H.D. Tjeenk Willink, Alphen aan den Rijn, 1989.
- Duthler, A.W., 'Beheersing van automatiseringsrisico's', Samsom, Alphen aan den Rijn / Zaventem, 1995.
- Kemna, A.M.Ch., 'Source code depot; softwaregeheimen en faillissement', W.E.J. Tjeenk Willink, Zwolle, 1988.
- Klaauw, F. van der en C. Prins, 'IT-contracten', Kluwer, Deventer, 1995.

- ‘Modelcontracten automatisering’, (losbl.), Samsom, Alphen aan den Rijn.
- Vandenberghe, G.P.V., ‘Partijaansprakelijkheid bij softwarecontracten’, Kluwer, Antwerpen - Deventer, 1984.
- Stuurman, C., ‘Aansprakelijkheid en automatisering’, Vermande, Lelystad, 1986.



8 Zelfregulering in de automatiseringsbranche

De automatiseringsbranche is relatief jong, kent een grote diversiteit en heeft een dynamisch en technologisch innovatief karakter. Deze omstandigheden zijn er de oorzaak van dat er binnen de branche nog nauwelijks sprake is van algemeen geldende normen en gebruiken waartegen het handelen van automatiseringsdeskundigen kan worden beoordeeld. De in de jurisprudentie ontwikkelde criteria terzake van leveranciersverplichtingen in de precontractuele fase en die van de aansprakelijkheid van adviseurs hebben inmiddels ook hun toepassing binnen de automatiseringsbranche gehad (RBC - Brinkers). Niettemin heeft de branche belang bij een proces dat tot verhoging van het kwaliteitsniveau en van het imago leidt. Eén van de geëigende instrumenten daartoe is 'zelfregulering'. Er is binnen de branche dan ook een aantal initiatieven ontplooid op het gebied van softwarecertificatie (8.1), beroepscode voor informatici (8.2) en geschillenbeslechting (8.3).

Andere terreinen waar sprake is van vormen van zelfregulering treffen we onder meer aan in 'interchange agreements' - overeenkomsten die onder meer procedures, aansprakelijkheid en bewijs regelen in een elektronische handelsomgeving (zie verder paragraaf 9.3) - en gedragscodes ingevolge de Wet persoonsregistraties: bepalingen met betrekking tot het omgaan met persoonsgegevensbestanden (zie verder paragraaf 11.2.2). In dit hoofdstuk worden enkele opmerkingen gemaakt over de eerste drie onderwerpen.

8.1 Softwarecertificatie

In deze paragraaf zullen we nagaan welke betekenis we kunnen toekennen aan een certificaat. Daartoe zullen we eerst kort stilstaan bij de hoedanigheden van een certificaat (8.1.1), het object van certificatie (8.1.2) en de verwachtingen we daarop mogen baseren (8.1.3).

8.1.1 Certificatie

Een certificaat is een keurmerk, vergelijkbaar met het KEMA-keurmerk voor de elektrische veiligheid van apparaten en het keurmerk van de Nederlandse Vereniging van Huisvrouwen voor de praktische geschiktheid van huishoudelijke gebruiksvoorwerpen. Onder een certificaat verstaan we:

> *een document, uitgegeven volgens de regels van een certificatiesysteem, om kenbaar te maken dat een gerechtvaardigd vertrouwen bestaat dat een bepaald produkt in overeenstemming is met een bepaalde norm.*

In de softwarebranche kan aansluiting gezocht worden bij de ISO normeringen (International Organization for Standardization), voor wat betreft ontwikkeltrajecten en interne organisatie. De ISO-9000 serie bevat een vijftal normenstelsels voor keuring van kwaliteitssystemen, een begrippenlijst en eisen aan instellingen die de keuring verzorgen. De ISO-9000 kwaliteitsstandaarden bevatten richtlijnen voor het garanderen van de kwaliteit van produkten en diensten, door middel van het keuren van organisaties of ontwikkelafdelingen. De volgende stappen zijn hierin te onderscheiden:

- marketing en marktonderzoek;
- ontwerp / opstellen van functionele en technische specificaties en produktontwikkeling;
- inkoop;
- planning en ontwikkeling van processen;
- vervaardiging;
- keuring, beproeving en onderzoek;
- verpakking en opslag;
- verkoop en distributie;
- installatie en inwerkingstelling;
- technische ondersteuning en onderhoud;
- opruiming na gebruik.

In 1981 is de Stichting Raad voor de Certificatie in het leven geroepen. Deze stichting houdt zich bezig met het toetsen van keuringsinstellingen en hun keuringssystemen, teneinde deze instellingen een erkenning als keurings-

instituut te kunnen verschaffen. Voor wat betreft de keuringsinstituten in de informatietechnologie (waaronder begrepen chips, interfaces, hardware-componenten e.d.) is deze taak overgedragen aan het in 1986 opgerichte ICIT (Instituut voor Certificatie van Informatietechnologie). Inmiddels heeft het ICIT verschillende keuringsinstellingen erkend.

8.1.2 Object van certificatie

Object van certificatie kunnen zijn kwaliteitssystemen dan wel produkten. Onder kwaliteitssystemen worden verstaan diensten, ontwikkelafdelingen en de organisatie; onder produkten kan worden verstaan hardware en software.

De keuring van kwaliteits*systemen* en staan niet garant voor de kwaliteit van het eindprodukt, noch voor de geschiktheid daarvan voor het door de afnemer beoogde gebruik.

Voor wat betreft de certificatie van *produkten* neemt computerhardware niet zo'n bijzondere plaats in. Keuringscriteria kunnen zijn of de hardware overeenstemt met de opgegeven technische specificaties, protocols en (internationale) standaarden.

Bij computersoftware kunnen we onderscheiden tussen maatsoftware en standaardsoftware. In het geval van maatsoftware ligt het niet voor de hand om het eindprodukt als zodanig als object van certificatie te kiezen. Dit zou immers betekenen dat speciaal voor deze software eenmalig eisen moeten worden geformuleerd, op basis waarvan gekeurd kan worden. In deze situatie kan beter voor een ISO-certificaat met betrekking tot de ontwikkelafdeling of de software-organisatie worden gekozen.

Voor het keuren van standaardsoftware zullen er keuringseisen moeten worden ontwikkeld. Er zijn verschillende mogelijkheden denkbaar:

- keuren tegen produktbeschrijvingen;
  Deze keuringsmethode beperkt zich tot het nagaan of de software werkt overeenkomstig de door de leverancier opgestelde specificaties.
- keuren tegen *goedgekeurde* produktbeschrijvingen;
  Hier worden minimum eisen gesteld aan de produktbeschrijving, zodat niet uitsluitend de opgave van de leverancier bepalend is.
- keuren op basis van algemene eisen voor pakketten van dezelfde soort.
  Deze laatste methode gaat uit van de opstelling van algemeen geldende eisen waaraan software-applicaties dienen te voldoen, bijvoorbeeld eisen voor tekstverwerkingspakketten, eisen voor databasepakketten, eisen voor administratieve pakketten enz.

Zagen we hierboven dat het keuren van maatsoftware problematisch is en het keuren van kwaliteitssystemen geen directe relatie heeft met de kwaliteit of de

geschiktheid van het eindprodukt, aan de certificatie van het eindprodukt zelf kleven eveneens enige bezwaren. Zo zal keuren nooit eenmalig kunnen zijn, maar steeds opnieuw dienen te geschieden voor iedere nieuwe release en voor iedere nieuwe versie. En ook hier zegt de goedkeuring van standaardsoftware nog niets over de geschiktheid van de software in relatie met de door de gebruiker beoogde toepassing. En over de keuringseisen, tenslotte, zal uiterst moeizaam overeenstemming zijn te bereiken (zo dit al zal gebeuren). Een keuze voor hoge keuringseisen, om het kaf van het koren te scheiden, zou het risico inhouden van mededingingsrechtelijke processen, terwijl lage keuringseisen de waarde van het certificaat teniet doen.

Zoals binnen de gehele industrie is men ook in de automatiseringsbranche gebrand op een ISO-certificaat. De certificaten die tot heden in de branche zijn verstrekt, hebben echter alle betrekking op de keuring van kwaliteitssystemen, zoals organisatie en ontwikkelingsafdelingen.

8.1.3 Gevolgen van certificatie voor aansprakelijkheid

Softwarecertificatie is vanuit marketingoverwegingen en imago aantrekkelijk voor ondernemingen omdat ze daarmee hun potentiële afnemers een onafhankelijk kwaliteitskeurmerk kunnen voorhouden. Interessant vanuit juridisch oogpunt is derhalve de vraag of de gerechtvaardigde verwachtingen van afnemers in dat geval mogen worden opgeschroefd. (Vanuit praktisch oogpunt is deze vraag aanzienlijk minder van belang, gelet op het gebruik van exoneraties in automatiseringsovereenkomsten.)

De gevolgen van certificatie voor aansprakelijkheid zijn afhankelijk van de relaties tussen de partijen die bij de overeenkomst betrokken zijn. We onderscheiden de volgende relaties:

1. afnemer - leverancier;
2. leverancier - keuringsinstantie;
3. afnemer - keuringsinstantie.

In de relatie afnemer-leverancier zien we enerzijds dat de door de leverancier opgewekte verwachting neigt naar een verhoging van diens aansprakelijkheid, terwijl anderzijds de leverancier kan wijzen op een onafhankelijke instantie die het produkt nu juist als kwalitatief voldoende heeft geoordeeld.

Voorts is denkbaar dat de leverancier de keuringsinstantie aanspreekt op de eisen zelf (kwaliteit, verouderd) en op de gevolgen van goed- of afkeuren.

De afnemer zou de keuringsinstantie in de claim kunnen betrekken in het geval van fouten in de keuringsprocedure of bij vermeend te lage keuringseisen.

Alledrie de situaties zullen in de keuringsovereenkomst die de keuringsinstantie met de leverancier is aangegaan en in de overeenkomst die de leverancier met de afnemer is aangegaan, wel worden afgedekt, door middel van exoneraties respectievelijk vrijwaringsbedingen.

Een voorzichtige conclusie is dat het instrument van certificatie voor leveranciers aantrekkelijk lijkt als marketinginstrument en als methode om de interne kwaliteitsborging door te lichten (met inachtneming van het feit dat certificatie toch altijd een momentopname blijft). Afnemers blijven er goed aan doen om zich toch vooral toe te leggen op de vraag of het betreffende produkt daadwerkelijk is toegesneden op de door hen beoogde toepassingen.

8.2 Beroepscode voor informatici

Een tweede onderwerp van zelfregulering waar we in dit hoofdstuk aandacht aan besteden, is het verschijnsel beroepscodes. Een beroepscode wordt wel gezien als een instrument om het kwaliteitsniveau binnen een bedrijfstak te verhogen en te bewaken. Op het eerste gezicht liggen hier dus kwaliteitsaspecten en ook wel ethische motieven aan ten grondslag. Zo vangt de code van de Nederlandse Vereniging van Registerinformatici aan met: ‘Bij mijn handelen als informaticus zal ik steeds het belang van de samenleving in al haar facetten positief dienen. ...’. In deze paragraaf zullen we nader stilstaan bij de functie van beroepscodes. Allereerst worden enkele verenigingen en hun doelstellingen in kaart gebracht (8.2.1). In paragraaf 8.2.2 worden enkele redenen die aan de opstelling van beroepscodes ten grondslag liggen opgenoemd, waarna in paragraaf 8.2.3 wordt stilgestaan bij de gevolgen van gedragscodes voor wat betreft arbeidsverhouding en verwachtingen.

8.2.1 Verenigingen van informatici

Binnen de automatiseringsbranche kennen we naast de brancheverenigingFENIT (Federatie Nederlandse IT-bedrijven) een aantal verenigingen waarvan informatici op persoonlijke titel lid zijn.

De oudste is het Nederlands Genootschap voor Informatici (NGI). Deze vereniging kent geen toelatingscriteria en staat derhalve open voor eenieder die werkzaam is of belangstelling heeft in informatica en de toepassingen daarvan.

In 1984 is opgericht de Nederlandse Vereniging van Registerinformatici (VRI), met als belangrijkste doelstellingen het bevorderen van de herkenbaarheid van professionele informatici en het leveren van een bijdrage aan een verantwoorde beroepsuitoefening. Aan de toelating tot deze vereniging zijn

echter wel eisen verbonden met betrekking tot genoten opleiding en relevante praktijkervaring in een bepaalde functie. Bovendien dient men referenties te overleggen. De leden worden ingeschreven in een register en noemen zich registerinformaticus (RI). De term RI is niet beschermd op grond van de Wet op het wetenschappelijk onderwijs juncto art. 435 Sr. Wel kan het voeren van de aanduiding 'RI' door anderen dan VRI-leden onrechtmatig zijn jegens deze leden. De achtergrond voor de oprichting van de VRI is dat men, meer dan binnen het NGI het geval was, een beroepsvereniging van professionals en een (wettelijke) erkenning van het beroep van informaticus nastreefde. Consequentie van een *wettelijke* erkenning zou zijn dat niet iedereen zich meer zonder meer 'informaticus' zou mogen noemen, evenmin als administrateurs zich registeraccountant mogen noemen. Het 'nobele' motief lijkt enigszins te verschralen bij de nagestreefde monopolisering van de beroepsuitoefening. Tot een wettelijke erkenning hebben de activiteiten van de VRI nog niet geleid.

In 1991 is opgericht de Nederlandse Vereniging van Beëdigde Informaticadeskundigen (NVBI). De leden van deze vereniging zijn beëdigd als taxateur op grond van art. 16 van de Wet op de Kamers van Koophandel en Fabrieken 1963, of als makelaar (in computerhard- en software) op grond van art. 62 van het Wetboek van Koophandel. Zij profileren zich als 'onafhankelijke' automatiseringsdeskundigen. Blijkens het jaarverslag 1994 beslaat 'bemiddeling' zo'n tweederde van de activiteiten van de leden; de overige activiteiten bestaan uit audit, escrow en geschillen.

In 1992 heeft het oprichtingssymposium van de Nederlandse Orde van Register EDP-Auditors (NOREA) plaats gevonden. EDP staat voor Electronic Data Processing (elektronische gegevensverwerking); met de term 'audit' wordt doorlichting bedoeld. De NOREA is derhalve een vereniging van informatici die actief zijn op het terrein van de doorlichting van informatiesystemen teneinde een uitspraak te kunnen doen omtrent de betrouwbaarheid van deze systemen en de door die systemen opgeleverde informatie. Ook bij deze beroepsgroep dringt de vergelijking met registeraccountants zich op, zij het dat waar de RA (register-accountant) als werkterrein heeft de bedrijfsadministratie en de jaarrekening, de RE (register-EDP-auditor) zich bezig houdt met geautomatiseerde gegevensverwerking.

8.2.2 Redenen voor een beroepscode

Uit de ontstaansgeschiedenis en werkterrein van de in de vorige paragraaf genoemde verenigingen blijkt reeds een aantal redenen om een beroepscode op te stellen. Naast de al genoemde kwaliteitsdoelstelling kunnen worden genoemd:

- het concretiseren van opvattingen binnen de branche;

- het creëren van eenduidigheid in benamingen;
- het creëren van eenduidigheid in functie-omschrijvingen;
- intern instrument om het handelen van informatici aan af te meten;
- instrument om 'het kaf van het koren te scheiden' door intern tuchtrecht;
- de behoefte tot 'bescherming' (afscherming?); iedereen kan zich 'informatie-analist' of 'systeemanalist' noemen.

Een kanttekening die bij deze doelstellingen kan worden gemaakt is dat een gedragscode in de praktijk veelal de werking krijgt van het legitimeren van het eigen gedrag, waar men door middel van de code de 'scherpe kantjes' vanaf tracht te halen.

Kijkt men voorts naar de samenstelling van de leden, dan kan men zich afvragen of de betreffende vereniging wel een homogene groep vormt. Uiteindelijk lijkt de doelstelling van beroepsvereniging en beroepscode voornamelijk die van 'marketingtool' te zijn, voortkomend uit de behoefte zich te profileren ten opzichte van andere branchegenoten door (meer) vertrouwen in te boezemen bij afnemers. In dit opzicht kan men het optreden van het NIVRA (Nederlands Instituut van Register-Accountants) als het meest effectief betitelen, aangezien zij van de hier genoemde beroepsverenigingen de enige is die in staat is geweest het werkterrein wettelijk verankerd te monopoliseren.

8.2.3 Gevolgen van gedragscodes

Het bestaan van gedragscodes kan van invloed zijn op de arbeidsverhouding en op de mate waarin er bij afnemers gerechtvaardigde verwachtingen worden opgeroepen.

Zo lezen we in art. 3 van de reeds gememoreerde VRI-gedragscode, dat de registerinformaticus bij zijn werkzaamheden dient te handelen in overeenstemming met het belang van de opdrachtgever. Een vraag die zich in dit verband kan aandienen is hoe een RI, in de hoedanigheid van werknemer, om moet gaan met de belangen van de werkgever ten opzichte van die van de klant, indien zij botsen. Mag een werknemer/RI, die als projectleider is gestationeerd bij een opdrachtgever, personeel uit de eigen organisatie inzetten, of is hij gehouden tot de keuze voor een derde indien dat bedrijf voor de bedoelde werkzaamheden meer gespecialiseerd zou zijn? Mag een werknemer/RI werk van de werkgever neer leggen, zich daarbij beroepend op de gedragscode?

Een andere vraag is wat voor consequenties de gedragscode kan hebben terzake van aansprakelijkheid. Kan een opdrachtgever zich - naast de overeenkomst - in een geding beroepen op de bepalingen uit de gedragscode? Bij de VRI kan men het handelen van de RI voorleggen aan een tuchtcommissie.

Of een afnemer er goed aan doet om daar in concreto gebruik van te maken is zeer de vraag, aangezien het tuchtreglement bepaalt dat een voorwaarde voor de ontvankelijkheid om van de klacht kennis te nemen is dat de klager niet tevens een civiele actie onderneemt. Gelet op de beperkte sanctiemogelijkheden die het tuchtcollege ten dienste staan - de zwaarste is het schrappen van de RI uit het register - zal een opdrachtgever vaak meer baat hebben bij een civiele vordering tot schadevergoeding. Kan voorts desgewenst de gedragscode zelf getoetst worden?

Het lijkt voor afnemers verstandig om aan het bestaan van gedragscodes in eerste instantie een intern belang toe te kennen. Voor de keuze of men al dan niet met een RA, RE of RI in zee zal gaan, komt gezond verstand op de eerste plaats, gevolgd door aantoonbare deskundigheid, voor de doelstelling van de afnemer relevante ervaring, ingebed in een overeenkomst waarin verwachtingen, verantwoordelijkheden en aansprakelijkheid expliciet zijn overeengekomen.

8.3 Geschillenbeslechting in de automatisering

Het derde terrein van zelfregulering is geschillenbeslechting. Naast geschillenbeslechting door de gewone rechter kennen we twee vormen van buitengerechtelijke geschillenbeslechting, namelijk arbitrage en bindend advies.

Arbitrage en bindend advies worden tussen partijen overeengekomen, hetzij vooraf bij de overeenkomst, hetzij op het moment dat het geschil zich aandient. Zowel de overeenkomst tot arbitrage als die tot bindend advies maakt de civiele rechter in beginsel onbevoegd. Arbitrage is geregeld in het Wetboek van Burgerlijke Rechtsvordering, art. 1020 e.v. Voor bindend advies bestaat er geen expliciete wettelijke regeling. In het geval van bindend advies komen partijen overeen om een derde te laten beslissen over de inhoud of uitvoering van de overeenkomst. Omdat partijen bij voorbaat verklaard hebben zich jegens elkaar aan het advies van de derde gebonden te achten, betekent dit dat diens beslissing, die gezien moet worden als een onderdeel van de eerdere overeenkomst, bindend is. De beslissing in een arbitragezaak wordt neergelegd in een vonnis, dat krachtens de wet tenuitvoergelegd kan worden. Voor de executie van een arbitraal eindvonnis is verlof van de president van de rechtbank nodig. In beide gevallen staat slechts beperkt beroep open op de gewone rechter, namelijk indien de gevolgde procesgang met onvoldoende waarborgen is omkleed, de inhoud of de wijze van tot stand koming in strijd is met de openbare orde of de goede zeden, dan wel een geldige overeenkomst ontbreekt. Als bindend advies is opgenomen in algemene voorwaarden, dan is het beding vernietigbaar, want onderhevig aan de bepaling van art. 6:236 BW, de zogenoemde ‘zwarte lijst’ van onredelijk bezwarende bedingen. Dit artikel is van toepassing in de rechtsverhouding

tussen de gebruiker van algemene voorwaarden en een wederpartij, natuurlijk persoon, die niet handelt in de uitoefening van een beroep of bedrijf.

De laatste jaren tekent zich een toenemende belangstelling af voor alternatieve vormen van geschillenbeslechting. Met name in de VS is een keur aan ADR-technieken (Alternative Dispute Resolution) ontwikkeld. Bleyer ('ADR in het Amerikaanse bedrijfsleven') noemt:

- bemiddeling / conciliatie / mediation;
- med-arb (mediation-arbitration);
- minitrial;
- adviserende arbitrage;
- fact-finding;
- rent-a-judge en
- summary jury trial.

Zonder hier verder op de - soms minieme - verschillen van deze vormen van geschillenbeslechting in te gaan, kan met Minkjan ('Het kan ook anders: ADR') gesteld worden dat iedere ADR-methode gebruik maakt van drie basisvormen van geschillenbeslechting: onderhandelen, bemiddelen en beslissen.

Na een korte kenschets van het verschijnsel 'minitrial' (8.3.1) zullen we in paragraaf 8.3.2, aan de hand van in de literatuur wel onderkende voor- en nadelen, inventariseren of zich voor de beslechting van geschillen in de automatiseringsbranche een duidelijke voorkeur aandient voor een bepaalde methode van geschillenbeslechting. Omdat in de praktijk van geschillenbeslechting in de automatisering arbitrage verre de overhand heeft boven bindend advies, en minitrial boven de andere ADR-technieken, beperken we ons tot een vergelijking tussen de gewone rechter, arbitrage en minitrial.

8.3.1 Minitrial

Minitrial kan in feite beschouwd worden als een voortgezette onderhandeling tussen de bij het conflict betrokken contractspartijen, onder begeleiding van een derde. De doelstelling van een minitrial is te voorkomen dat een gang naar de rechter of arbiter nodig is. De derde neemt een onafhankelijke positie in en heeft de functie de partijen nader tot elkaar te brengen. Hij kan optreden als procesbegeleider - als partijen met voorstellen komen - of kiezen voor een actievere rol en zelf met voorstellen komen. Het voorstel van de derde is nimmer bindend. Als partijen niet nader tot overeenstemming komen, eindigt de minitrial.

Om de kansen op een succesvolle minitrial zo groot mogelijk te doen zijn, is het verstandig de procedure in een zo vroeg mogelijke fase te beginnen, bij voorkeur als het verschil van mening nog niet is geëscaleerd tot een conflict.

Omdat de wil tot conflictbeslechting mede afhankelijk kan zijn van de persoonlijke verhoudingen, is het zinvol als de personen die de contractspartijen vertegenwoordigen zelf niet direct bij het geschil betrokken zijn geweest. Om te voorkomen dat binnen het minitrial-panel bereikte overeenstemming nog ter goedkeuring aan het management moet worden voorgelegd, is het voorts praktisch als de vertegenwoordigers zelf beslissingsbevoegd zijn, zoals directieleden.

Gelet op de karakteristieken van automatiseringsprojecten (zie paragraaf 7.1: verschil in verplichtingen; produkt van samenwerking; vitaal belang en langdurig traject) kunnen als belangrijke voordelen van minitrial worden genoemd:

- snelheid van de procedure;
- kosteneffectiviteit;
- het project kan voortgang behouden;
- voorkoming escalatie;
- bewaren van de goede verstandhouding;
- onderhandelen is een methode die aansluiting heeft bij de wijze van opereren van ondernemers.

Dat minitrial niet tot een de partijen bindende uitkomst hoeft te leiden, wordt wel eens gezien als nadeel van de procedure. Dit lijkt ten onrechte: het niet-bindende karakter van minitrial is juist een voorwaarde voor succes. Geen enkele manager zou bereid zijn mee te werken aan een geschiloplossing op informele manier, zonder proceswaarborgen en zonder bijstand (juridisch of deskundigen), indien hij daarna gehouden zou zijn aan wat de meerderheid besluit. Het argument, dat er in het geval er geen overeenstemming wordt bereikt kostbare tijd verloren zou zijn gegaan, is betrekkelijk. Een minitrial heeft altijd als uitkomst dat partijen beter geïnformeerd zijn over elkaars standpunt. Dus, indien later toch een procedure voor de gewone rechter of arbitrage nodig mocht zijn, is de minitrial een uiterst nuttige fase ter voorbereiding geweest.

8.3.2 Criteria bij forumkeuze

Indien men wil overgaan tot arbitrage voor de beslechting van geschillen, al dan niet voorafgegaan door een minitrial, zal dit met de wederpartij moeten zijn overeengekomen. Omdat ten tijde van het optreden van het geschil er andere zaken kunnen meespelen (een partij heeft geen belang bij een snelle oplossing; verhoudingen zijn getroebleerd e.d.) is het raadzaam arbitrage en/of minitrial reeds bij aanvang van het automatiseringsproject overeen te komen. Dat betekent dat we ons vooraf een oordeel dienen te verschaffen

naar welke vorm(en) van geschillenbeslechting de voorkeur uit gaat. We zullen hier enkele criteria de revue laten passeren:

DESKUNDIGHEID

Als voordeel van arbitrage in automatiseringsgeschillen wordt genoemd dat er beslist wordt door arbiters met materie-deskundigheid. Onderwerpen echter zoals hierboven in paragraaf 7.4 geschetst, zullen veelal *specifieke* deskundigheid behoeven, zoals kennis van de betrokken organisaties, van de 'ins and outs' van de betreffende branche, van de mogelijkheden en toepassingen van specifieke systeemsoftware en computerhardware, van communicatie-protocollen, van interfaces, van de toegepaste software-ontwikkelmethode en van de betreffende applicatie. Los van de vraag of een deskundige arbiter geacht kan worden zo veelzijdig te zijn, mag worden aangenomen dat de hier bedoelde deskundigheid niet tot de *taakopvatting* van de arbiter kan worden gerekend. Het voordeel van deskundigheid is derhalve relatief; hij is bekend met de gang van zaken rondom automatiseringsprojecten.

We dienen ons bovendien te realiseren dat geschillen weliswaar een feitelijke achtergrond kunnen hebben, doch dat deze feiten - voorzover ze kunnen worden vastgesteld - een redelijke uitleg behoeven. En daarmee komen we op het type deskundigheid dat niet a priori tot de bagage van automatiseringsdeskundigen gerekend kan worden, maar wel tot die van juristen. Van juristen mag worden verwacht dat zij beter toegerust zijn voor wat betreft conflictoplossing dan automatiseringsdeskundigen. Zij kunnen dogmatiek en jurisprudentie vanuit andere, al dan niet aanpalende, rechtsgebieden bij de zaak betrekken en zijn bekend met vigerende rechtsnormen en opgeleid om deze te hanteren.

Het ontberen van specifieke (automatiserings)kennis lijkt derhalve niet zo relevant. Is in de praktijk dergelijke kennis haast altijd ontoereikend, het kan bovendien leiden tot een onwenselijke verwevenheid in het te geven oordeel. Het is aan partijen om de blote feiten aan te dragen, zo nodig ondersteund met informatie ingewonnen bij deskundigen op het betreffende (deel)vakgebied.

SNELHEID

Als belangrijk voordeel van arbitrage ten opzichte van de gewone rechter wordt de snelheid van de procedure genoemd. Gezien de toegenomen populariteit van de Kort Geding procedure is het twijfelachtig of dit voordeel onverkort houdbaar is. De reactie hierop in de vorm van art. 1051 Rv, dat de mogelijkheid opent tot het wijzen van een vonnis in arbitraal kort geding, trekt de concurrentieverhoudingen althans in dit opzicht weer recht.

WAARBORGEN

Een volgend argument, dat gehanteerd lijkt te worden zoals het uitkomt, is dat van de waarborgen van de procedure (procesregels, procesvertegenwoordiging, bewijsregels). Ten gunste van de gewone rechter wordt vaak het belang aangevoerd van de algemene beginselen van behoorlijke rechtspraak. Alsof dat onverbrekelijk verbonden zou zijn met de overheidsrechter. Daar tegenover wordt bij alternatieve vormen van conflictoplossing nu juist gewezen op het voordeel van de flexibiliteit van de procedure. Welnu, de gewone rechter blijkt niet ongevoelig voor dit gat in de markt en ontfermt zich over dit argument met name door middel van bepaalde mogelijkheden die het Kort Geding biedt.

Arbitrage kan evenmin een tweeslachtig karakter worden ontzegd in het streven zoveel mogelijk marktpotentie aan te spreken. Ten opzichte van de gewone rechter wordt gewezen op het voordeel van grotere flexibiliteit, terwijl er ten opzichte van andere vormen van ADR gelijktijdig gewezen wordt op het voordeel van de grotere waarborgen in de arbitrage-procedure. Zo zien we dat hetgeen aan een kant als een nadeel wordt gezien, aan de andere kant ineens een voordeel blijkt te zijn.

KOSTEN

Tenslotte de kosten van de procedure. Gelukkig zien we allengs minder generaliserende uitspraken dat bijvoorbeeld arbitrage goedkoper zou zijn dan de gewone rechter (of andersom). Een snelle arbitrageprocedure kan uiteindelijk goedkoper zijn dan een langdurig voortslepend conflict voor de gewone rechter, ondanks de soms forse vergoedingen voor de arbiters. Blijkt daarentegen het geschil ook voor de gewone rechter snel tot een oplossing gekomen, dan zou een vergelijking van de kosten in het nadeel van arbitrage kunnen uitvallen. Helaas kan men echter niet op voorhand de duur van procedures voorspellen.

FORMEEL/INFORMEEL KARAKTER

In de automatiseringsbranche kan men zich sinds 1989 wenden tot een eigen arbitrage-instituut, de Stichting Geschillenoplossing Automatisering. In de brochure wordt melding gemaakt van procedures voor minitrial, spoedarbitrage en kort-geding-arbitrage. Er zijn voordelen te onderkennen aan de in ADR-technieken ten grondslag liggende onderhandelingsgedachte. De karakteristieken van automatiseringsprojecten wijzen op het belang om tot een conflictoplossing te geraken die primair gericht is op de continuïteit van de samenwerking. Zoals partijen zich bij de *opstelling* van de overeenkomst kunnen laten bijstaan door derden (adviseurs, organisatie-, automatiserings- en/of juridische deskundigen), zo kan dit evengoed zinvol zijn bij de nadere *invulling c.q. uitleg* van de overeenkomst. Onderhandelen tussen partijen is dan de nuttigste gedragswijze. Onderhandelen kan echter tot ongewenste gevol-

gen leiden wanneer de onderhandelingsmacht van beide partijen sterk verschilt. Juist dan kunnen de voordelen van informele arbitrage manifest worden. Het is nog even afwachten of één aanspreekpunt voor de branche, en dan nog wel een stichting met een formaliserende procedure, ook ten aanzien van dit aspect de pretenties zal kunnen waarmaken.

Hierbij wordt aangetekend dat arbiters in de gebruikelijke omschrijving in belangrijke mate dezelfde rol vervullen als een overheidsrechter. Een belangrijk bezwaar tegen deze rol is het verschijnsel van de 'instabiliteit van de oplossing': een rechter kan de vordering niet matigen om de reden dat hij er onzeker van is de juiste beslissing te hebben genomen. Wanneer het informele karakter van de arbitrage inhoudt, dat de arbiter zich aan dit verschijnsel kan onttrekken, is er veel gewonnen.

Conclusie

De diverse hierboven beschreven rechtsmogelijkheden staan in nogal ondoorzichtige concurrentieverhoudingen tot elkaar. Het lijkt geen eenvoudige opgave voor de justitiabele om tot een keuze te komen die voor zijn situatie het meest passend is. De algemene argumenten pro en contra die we in de literatuur tegen komen, zijn daartoe onvoldoende doorslaggevend. Een arbitrage-instituut dat zich specialiseert in de beslechting van automatiseringsgeschillen verdient wellicht een lichte voorkeur. De Stichting Geschillenoplossing Automatisering biedt zowel arbitrage als minitrial en het arbitragecollege kan worden samengesteld uit zowel juristen als automatiseringsdeskundigen. Op termijn kan het mogelijk nadeel van een te eenzijdige gerichtheid wellicht minder zwaar blijken te wegen. Dit zal mede afhangen van de kwaliteit van de arbiters, de binnen de stichting na te streven consistentie en het vermogen van de juristen voeling te houden met hetgeen zich bij andere arbitrage-instituten en bij de gewone rechter als geldend recht lijkt te ontwikkelen.

8.4 Jurisprudentie

Geschillenkamer van de Raad van Toezicht van de Nederlandse Vereniging voor Registerinformatici, 6 maart 1989, CR 1989/5.

Naar de mening van de Geschillenkamer dient van een registerinformaticus een hoge graad van loyaliteit te worden verwacht. Het strookt hiermee in het geheel niet dat een registerinformaticus zijn of haar positie bij een werkgever gebruikt voor het behalen van persoonlijk voordeel (i.c. bemiddelingskosten bij ingekochte diensten van derden). Volgt verwijdering uit het register.

8.5 Literatuur

- Bleyer, K., ‘ADR in het Amerikaanse bedrijfsleven’, TvA 1988/1
- Minkjan, E.E., ‘Het kan ook anders: ADR’, Advocatenblad 1993/15
- Stuurman, C., ‘Het recht rond software-certificatie’, in: Computerrecht 1989/5
- Stuurman, C., ‘Technische normen en het recht’, (diss), Kluwer, Deventer, 1995

9 EDI elektronisch handelsverkeer

Onder invloed van telematica ontstaat een groot aantal nieuwe diensten. De verwachting is dat de groei van draadloze telefonie daaraan nog zal bijdragen. Voorbeelden van nieuwe diensten zijn: elektronische post (email), teleconferencing, telewerken, GBA (gemeentelijke basisadministratie), EFT, (electronic fund transfer - elektronisch geldverkeer) en EDI, (electronic data interchange - elektronisch handelsverkeer).

Zolang samenwerkende bedrijven het goed met elkaar kunnen vinden, is EDI een aantrekkelijk middel om overeenkomsten tot stand te brengen. Bij onenigheid echter, wordt het ontbreken van specifieke wetgeving aangaande EDI wel als een probleem ervaren. Regelgeving met betrekking tot EDI wordt momenteel als een belangrijk aandachtsgebied gezien door EDI-gebruikers. Ook de handelsrecht-commissie van de Verenigde Naties lijkt deze mening toegedaan. De commissie heeft onlangs vastgesteld dat er behoefte is aan een 'EDI model law' met behulp waarvan wetgevers in verschillende lidstaten bestaande codificaties kunnen aanpassen aan de ontwikkelingen op het gebied van elektronische berichtenuitwisseling. Volgens anderen daarentegen, zouden rechtsregels het elektronische handelsverkeer kunnen belemmeren. Deelnemers kunnen (voorlopig) beter met iedere EDI-organisatie afzonderlijk overeenkomsten af sluiten. Deze methode moet wel gebruikersvriendelijker worden georganiseerd om in de toekomst knelpunten te voorkomen.

Electronic Data Interchange roept, evenals andere computergerelateerde ontwikkelingen, vragen op met betrekking tot regelgeving. In ons land zijn dergelijke vragen inmiddels beantwoord, o.m. in de vorm van een softwarebeschermingswet, een chipswet, de Wet Persoonsregistraties en de Wet Computercriminaliteit. Voorts zijn er wetswijzigingen te verwachten naar aanleiding van de recentelijk aangenomen EU-richtlijnen betreffende de juridische bescherming van databanken en de bescherming van persoonsgegevens.

Waar elders in dit boekje de opportuniteit van de verschillende wetgevende initiatieven ter discussie is gesteld, zo kan men zich ook hier afvragen of het nodig is dat aan deze lijst regelgeving met betrekking tot EDI wordt toegevoegd. Met andere woorden: brengt EDI problemen met zich mee die nopen tot de ontwikkeling van nieuwe wetgeving? Hier zal de stelling worden verdedigd dat specifieke EDI-wetgeving vooralsnog niet wenselijk is en tegelijkertijd worden betoogd dat het ontbreken daarvan geen belemmering op de invoering van EDI behoeft te betekenen.

Na een korte inleiding in de volgende paragraaf over het waarom van EDI, zal in paragraaf 9.2 aandacht worden besteed aan de vraag naar de rechtsgeldigheid van door middel van EDI tot stand gekomen handelsovereenkomsten. In paragraaf 9.3 wordt vervolgens ingegaan op de zogenoemde 'interchange agreement'. Dit is een overeenkomst waarin EDI-partners afspraken vastleggen met betrekking tot het gebruik van EDI. In paragraaf 9.4 tenslotte zal aandacht worden besteed aan conflictbeslechting en zal een toekomstperspectief worden geschetst.

9.1 Waarom EDI?

EDI staat voor electronic data interchange en betreft de uitwisseling van gegevens door middel van computers, via telecommunicatieverbindingen. Volgens het EDI-handboek kan EDI worden gedefinieerd als

> *'de geautomatiseerde, elektronische uitwisseling van gestructureerde en genormeerde gegevens tussen computers van bij (handels)transacties betrokken partijen'.*

In deze definitie liggen voor een belangrijk deel de voordelen, de beperkingen en enkele daaruit voortvloeiende juridische aspecten besloten.

GEAUTOMATISEERDE UITWISSELING

Dit betekent dat de uitwisseling van gegevens (aanmaak, verzending, ontvangst en verwerking) geschiedt door de computersystemen, zonder menselijke tussenkomst. Voordelen daarvan zijn dat de uitwisseling 'tijdonafhan-

kelijk' kan geschieden en dat de kans op invoer- en overnamefouten wordt beperkt. Nadeel kan zijn dat er geen direct menselijk toezicht meer is.

ELEKTRONISCHE UITWISSELING
Het voordeel van elektronische uitwisseling is dat gegevens zonder tijdverlies bij de ontvanger aankomen, ongeacht afstand en grenzen.

GESTRUCTUREERDE GEGEVENS
Met gestructureerde gegevens wordt bedoeld dat de berichten worden uitgewisseld volgens een vooraf afgesproken indeling en lay-out, in verband met een voor geautomatiseerde verwerking benodigde eenduidige interpretatie van de gegevens.

GENORMEERDE GEGEVENS
De normering van gegevens, door gebruikmaking van standaardcoderingen, maakt een eenduidige interpretatie van de inhoud van de berichten mogelijk.

TUSSEN COMPUTERS VAN BIJ (HANDELS)TRANSACTIES BETROKKEN PARTIJEN
Hieruit volgt dat de door die verschillende organisaties gebruikte computersystemen op elkaar dienen te worden afgestemd en dat omtrent de door de organisaties te hanteren werkwijze afspraken gemaakt dienen te worden.

In het algemeen worden de volgende voordelen onderscheiden aan het gebruik van EDI:

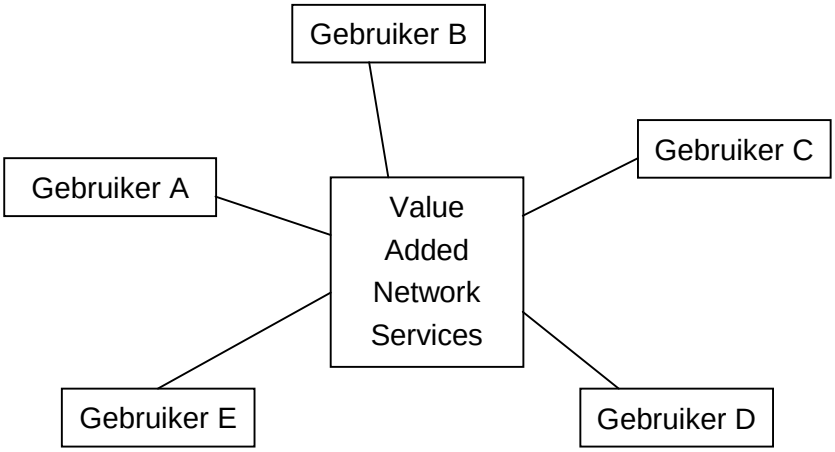
- beschikbaarheid
  EDI-bestellingen kunnen 24 uur per dag, 7 dagen per week worden ingegeven. Organisaties zijn daarvoor niet meer afhankelijk van de 'kantoortijden' van hun wederpartij. Zo mogelijk worden bestellingen automatisch gegenereerd.
- verminderde kans op fouten
  Omdat gegevens veelal maar éénmaal worden ingevoerd, is er minder kans op fouten in de bestelling, of van foutieve overname door de wederpartij.
- afname logistieke kosten
  Er ligt minder tijd tussen bestelling en levering, waardoor kleinere voorraden aangehouden kunnen worden en minder opslagruimte nodig is.
- afname administratieve kosten
  De grote mate van geautomatiseerde verwerking (en soms ook invoer) van bestellingen zorgt voor lagere behandelingskosten. Ook het gebruik van postzegels, enveloppen, papier, e.d. vermindert.

De eis dat gegevens met het oog op de geautomatiseerde verwerking daarvan gestructureerd en genormeerd dienen te zijn, is in de praktijk nogal eens een belemmering gebleken voor invoering van EDI. In die situaties waarin niet aan

deze eis kan worden voldaan en in situaties waar het incidentele karakter van de handelstransacties een vergaande integratie van de wederzijdse administratieve systemen niet lonend maakt, zien we dat het gebruik van bulletin board systemen en/of internet steeds vaker als alternatief voor EDI gaat functioneren. In het algemeen is in het elektronisch handelsverkeer een tendens waarneembaar van besloten EDI-netwerken naar open 'netwerken', onder gebruikmaking van internet. Een aantal voordelen van EDI wordt ingeleverd, tegenover een verhoging van flexibiliteit. De organisatie in Nederland die zich bezig houdt met bevordering van EDI-toepassingen is Ediforum

We kunnen een aantal partijen onderscheiden die zijn betrokken bij EDI-transacties:

- de afzender van een bericht;
- de ontvanger van het bericht;
- de telecommunicatieleverancier, die zorgt voor de lijnen/transport;
- een Value Added Network Services leverancier (VANS), organisaties die op basis van veelal bestaande telefoon- en datalijnen faciliteiten voor netwerken aanbieden.



Figuur 3: Organisatie van een VANS.

Een VANS-leverancier wordt ingeschakeld om technische en organisatorische problemen te omzeilen of af te schuiven. Gebruik van een VANS-leverancier heeft bijvoorbeeld tot gevolg dat een rechtstreekse verbinding tussen de verschillende gebruikers niet nodig is; de VANS-leverancier zorgt dan voor (tijdelijke) opslag en distributie. Ook behoeven merk en type computer van de verschillende gebruikers niet overeen te stemmen, omdat de VANS-leverancier converteert. Het netwerk bestaat vaak al, waardoor minder startproblemen ontstaan, en wordt door VANS-leverancier onderhouden. Andere toegevoegde waarden kunnen bestaan uit (de)codering van het berichtenverkeer en assistentie bij correctie van fouten. Voorbeelden van VANS-leveranciers in

Nederland zijn GEIS (General Electric Information Services), RAET informatieverwerking en SWIFT (banken).

9.2 Rechtsgeldigheid van EDI-transacties

Partijen die gebruik willen gaan maken van EDI kunnen daartoe een overeenkomst afsluiten. Een dergelijke overeenkomst wordt een 'interchange agreement' genoemd. In deze overeenkomst kan een aantal onderwerpen worden opgenomen teneinde problemen tijdens de uitwisseling van gegevens te voorkomen, dan wel problemen die daaruit ontstaan uit de weg te ruimen. De *interchange agreement* die wordt gesloten met het oog op het *gebruik* van EDI - onder meer het formaliseren van de wijze van uitwisseling van gegevens tussen partijen - dient te worden onderscheiden van de *(handels)overeenkomsten* die worden gesloten *door middel van* EDI. In deze laatste overeenkomsten worden de afspraken met betrekking tot de handelstransacties zelf vastgelegd. Een vraag die daarbij aan de orde komt, is die naar de rechtsgeldigheid van met behulp van EDI gesloten (handels)overeenkomsten. In paragraaf 9.2.1, 9.2.2 en 9.2.3 worden achtereenvolgens stil gestaan bij vormvereisten, wilsovereenstemming en eventuele overige vereisten. In paragraaf 9.3 wordt de interchange agreement besproken.

9.2.1 Vormvereisten

In beginsel is het Nederlandse contractenrecht vormvrij. 'Tenzij anders is bepaald, kunnen verklaringen in iedere vorm geschieden...', aldus art. 3:37 lid 1 BW. Verklaringen kunnen dus mondeling, schriftelijk, maar ook op elektronische wijze geschieden. Handelsovereenkomsten kunnen in het algemeen dus met behulp van EDI tot stand komen. Wetgeving staat aan het sluiten van dergelijke overeenkomsten niet in de weg.

Anders ligt dit mogelijk met, bijvoorbeeld, een overeenkomst tot overdracht van auteursrecht. Een dergelijke overdracht dient namelijk bij akte te geschieden (art. 2 Aw). Ingevolge art. 183 lid 1 Rv zijn akten ondertekende geschriften, bestemd om tot bewijs te dienen. Geschriften zijn alle dragers van verstaanbare leestekens. Verstaat men onder een akte een op *papier* geschreven of getypt stuk, dan zou dit tot de conclusie leiden dat dit soort overeenkomsten niet met behulp van EDI gesloten kunnen worden. Algemeen wordt echter aangenomen dat gegevens vastgelegd op magnetische informatiedragers - mits aan deze vastlegging een zekere duurzaamheid kan worden verbonden - eveneens een geschrift vormen, zodat ten aanzien van dit aspect een overeenkomst tot overdracht van auteursrecht gesloten door middel van

EDI rechtsgeldig kan zijn. De Uncitral Model Law on International Commercial Arbitration blijkt deze opvatting in art. 7 lid 2 te onderschrijven:

> *'An agreement is in writing if it is contained in a document signed by the parties or in an exchange of letters, telex, telegrams or other means of telecommunication which provide a record of the agreement...'.*

Het geschrift, de akte, dient evenwel ondertekend te worden en daarvan kan niet zonder meer worden gezegd dat dit elektronisch kan geschieden. Aan een *password* of inlogcode bijvoorbeeld mag niet dezelfde betekenis worden toegekend als aan een traditionele handtekening (zie ook paragraaf 10.1.2 hierna). Belangrijke verschillen zijn met name gelegen in de functies die zij vervullen.

Bij de traditionele handtekening kunnen een drietal functies worden onderscheiden: identificatie van de ondertekenaar, bevestiging van de inhoud en het bewijs van instemming van de ondertekenaar met de juistheid c.q. volledigheid van de informatie die in het document is vervat. Een 'elektronische handtekening' is niet persoonsgebonden en minder 'uniek' dan een traditionele handtekening, zodat met een aanzienlijk minder grote stelligheid beweerd kan worden dat de (bevoegde) ondertekenaar deze heeft gebruikt. Belangrijker echter is dat codes veelal de functie van *toegangscode* vervullen. De inhoud van het te versturen bericht staat op het moment van de toegang nog niet vast, laat staan dat er bewijs van instemming met betrekking tot de juistheid van het bericht is. Het lijkt dan ook niet juist hieraan gelijke juridische waarde toe te kennen als aan de traditionele handtekening.

Indien ook nà opmaak en verzending van het bericht een code gestuurd wordt ter bekrachtiging daarvan, een handeling die qua functie een gelijkenis vertoont met de traditionele handtekening, zal het juridisch nog niet geheel verantwoord zijn een akte elektronisch op te maken en te versturen. Immers, daarna zal nog elektronische verzending en vastlegging volgen, een traject waarbinnen fouten of manipulaties kunnen optreden.

Met betrekking tot de toepassing van EDI levert het al dan niet gelijkstellen van een 'elektronische' aan een schriftelijke handtekening evenwel geen problemen op, aangezien voor het merendeel van de overeenkomsten die thans met gebruik van EDI-technieken worden afgesloten geen vormvereisten gelden.

9.2.2 Wilsovereenstemming

Dat de meeste overeenkomsten vormvrij zijn, betekent overigens niet zonder meer dat deze kunnen worden aangegaan door middel van EDI. Overeenkomsten komen tot stand door de aanvaarding van een aanbod (art. 6:217 BW).

Partijen dienen het eens te zijn over de te verrichten prestaties; er dient wilsovereenstemming te zijn. Zowel aanbod als aanvaarding kunnen in beginsel in iedere vorm geschieden. Bovendien kunnen zij opgesloten liggen in gedragingen.

Is er nu bij gebruik van EDI-systemen voor het sluiten van overeenkomsten sprake van een aanbod? Als bijvoorbeeld bij een handelsonderneming de voorraad beneden een bepaald peil zakt waardoor automatisch, middels EDI, een bestelling bij een groothandel wordt geplaatst, is dan een aanbod gedaan? De groothandel heeft niets gedaan. De bestelling is misschien wel 's nachts gegenereerd, op een moment dat de groothandel gesloten was. Van een aanbod lijkt dan geen sprake. Zoals gezegd echter, kan een aanbod echter ook in de vorm van een gedraging geschieden. In aansluiting op het Ediforum-rapport 'Juridische aspecten van moderne transactie communicatie' kunnen we dan ook stellen dat het aanbod bij EDI reeds eerder geschiedt in de vorm van de installatie van EDI-hardware en/of -software; een gedraging dus. Met de installatie geeft een bedrijf aan, dat het met geautoriseerde gebruikers een overeenkomst tot het leveren van goederen wil aangaan. In deze installatie zit tevens de aanvaarding opgesloten. De gebruiker maakt het immers mogelijk dat, wanneer de voorraad tot beneden een door deze gebruiker vastgesteld niveau daalt, automatisch een bestelling wordt geplaatst.

Kan, voorts, bij een bestelling zonder directe menselijke tussenkomst echter wel worden gesproken van wilsovereenstemming? Ook hier moet worden geoordeeld aan de hand van gedragingen; opnieuw de installatie, maar daarnaast ook het toezicht tijdens het gebruik van het EDI-systeem, maken duidelijk dat er overeenstemming is.

9.2.3 Overige vereisten

Naast vormvereisten en wilsovereenstemming dienen verbintenissen die partijen op zich nemen bepaalbaar te zijn (art. 6:227 BW). Een bestelling van fietsen is niet bepaalbaar, een bestelling van 30 fietsen wel. Voorts mag een overeenkomst niet in strijd zijn met de goede zeden of de openbare orde (art. 3:40 BW) en dienen de sluiters van een overeenkomst handelingsbekwaam te zijn (art. 3:32 BW). Dit laatste betekent dat minderjarigen en onder curatele gestelden (voor zover de wet niet anders bepaalt) geen overeenkomsten mogen afsluiten.

Ook voor de tot stand koming van rechtsgeldige overeenkomsten met behulp van EDI dient aan deze eisen te zijn voldaan. Dit lijkt evenwel geen problemen op te leveren. Is één van de partijen bij een EDI-overeenkomst bijvoorbeeld handelingsonbekwaam, dan had die partij geen overeenkomst mogen afsluiten en is deze daarom vernietigbaar. Indien dezelfde overeenkomst zonder gebruik van EDI was gesloten, dan zou dit niet tot een andere

conclusie leiden. Al met al stelt de toepassing van deze nieuwe techniek de gebruikers nauwelijks voor juridische verrassingen met betrekking tot de eisen waaraan een overeenkomst dient te voldoen. Slechts in sommige gevallen zullen vormvereisten het gebruik van EDI niet mogelijk maken.

9.3 Interchange agreement

Als uitgangspunt voor de bespreking van de diverse onderdelen die opgenomen kunnen worden in een interchange agreement nemen we een EDI-organisatie waarin een VANS-leverancier een centrale rol speelt. Uit cijfers blijkt namelijk dat VANS-leveranciers inmiddels 82% van de EDI-berichten voor hun rekening nemen. Naar verwachting zal dit percentage de komende jaren groeien, waardoor het niet reëel is de VANS-leverancier te negeren. Door de toename van EDI-gebruik zal in de toekomst voor leveranciers van toegevoegde waarde aan het netwerk een steeds belangrijker rol zijn weggelegd.

Met betrekking tot de uitwisseling van gegevens door middel van computers dienen partijen duidelijke afspraken te maken. Deels zullen deze afspraken van technische aard zijn, veelal vastgelegd in een communicatieprotocol, en worden opgenomen in gebruikershandleidingen. Daarnaast zullen partijen in een overeenkomst hun rechten en plichten betreffende het gebruik van EDI dienen vast te leggen in de interchange agreement. Deze overeenkomst kan worden gesloten tussen een toekomstige gebruiker en een VANS-leverancier, maar ook tussen gebruikers onderling. In het eerste geval zal er veelal sprake zijn van een standaard-overeenkomst die ook met reeds aangesloten partijen is afgesloten. De VANS-leverancier zal immers nieuwe gebruikers niet meer rechten en/of plichten willen geven dan reeds aangesloten gebruikers. Overigens zal deze overeenkomst worden onderscheiden in een onderdeel betrekking hebbend op de uitwisseling van gegevens tussen de computers van de gebruikers, de interchange agreement, en een onderdeel met betrekking tot het gebruik van het netwerk, de zogenaamde aansluitingsovereenkomst. In het tweede geval zal een nieuwe gebruiker met elke reeds aangesloten partij rond de tafel gaan zitten om afspraken te maken. Nadeel hiervan is dat dit een langdurige en dus kostbare procedure is, en zal kunnen leiden tot overeenkomsten met verschillende inhoud. Ook dan lijkt het gebruik van modelcontracten een effectieve uitkomst te bieden. Diverse instellingen hebben daarom reeds initiatieven in die richting ontplooid. Voor alle duidelijkheid: indien partijen onderling afspraken maken met betrekking tot de uitwisseling van berichten, behoeven zij met de VANS-leverancier geen interchange agreement af te sluiten. Met de VANS-leverancier is het dan slechts nodig een aansluitingsovereenkomst af te sluiten.

De inspanningen om tot een modelovereenkomst voor het gebruik van EDI te komen, hebben inmiddels tot inzichten geleid welke onderwerpen in een interchange agreement zouden moeten worden behandeld om de uitwisseling van gegevens zo betrouwbaar mogelijk te laten plaatsvinden. Een aantal van deze onderwerpen zal hieronder aan de orde komen.

9.3.1 Identificatie

EDI-transacties geschieden per computer en zijn dus papierloos. Dit heeft tot gevolg dat bepaalde traditionele mogelijkheden tot identificatie van de afzender van een bericht - briefhoofd en/of handtekening - zijn verdwenen. Uiteraard behoeft het ontbreken daarvan aan het gebruik van EDI niet in de weg te staan, evenmin als dat het geval is bij telex en telegraaf. In geval van een eventueel rechtsgeschil echter, kunnen betrokken partijen er belang bij hebben aannemelijk te kunnen maken dat een elektronisch bericht ontvangen dan wel verstuurd is. In een interchange agreement dient daarom een paragraaf te worden opgenomen waarin staat dat partijen zich moeten identificeren, hoe zij dit moeten doen en welke maatregelen genomen moeten worden als identificatie gebrekkig is of geheel ontbreekt.

Partijen kunnen een keuze maken uit verschillende middelen om een tegenpartij te identificeren, zoals pincode, password of encryptie (versleuteling van het bericht). Daarnaast kunnen zij bijvoorbeeld afspreken dat bij het ontbreken van een (volledig) identificatie-middel de ontvangende partij, indien mogelijk, contact dient op te nemen met de afzender.

9.3.2 Vertegenwoordigingsbevoegdheid

Doordat een traditionele handtekening onder een EDI-bericht ontbreekt, kan een ontvanger niet controleren of een bericht is verstuurd door een persoon die ook daadwerkelijk bevoegd was het bedrijf of de instelling te vertegenwoordigen. Een code kan immers gereproduceerd zijn. Bevoegdheid is echter wel van belang, want een rechtspersoon is niet gebonden aan een overeenkomst namens deze aangegaan door een onbevoegde. EDI-berichtenverkeer lijkt als gevolg hiervan een riskante onderneming, ware het niet dat op dit beginsel een uitzondering bestaat. Als namelijk het ene bedrijf bij het andere de schijn heeft gewekt dat de persoon met wie gehandeld is bevoegd was het bedrijf te vertegenwoordigen, dan kan dat (eerste) bedrijf aan de door deze persoon gemaakte afspraak worden gehouden (het zogenoemde ‘toedoen-beginsel’, art. 3:61 lid 2 BW).

In het geval van EDI zou dit kunnen betekenen dat de ontvanger van een bericht er in beginsel van uit mag gaan dat het bericht, indien voorzien van de

juiste identificatie van een bedrijf, verstuurd is door een bevoegd persoon. Het is dus de taak van het versturende bedrijf om misbruik van identificatiemiddelen te voorkomen. De ontvangende partij mag niet de dupe worden van fouten gemaakt bij de versturende partij. Om misbruik minder eenvoudig te maken, zou aan de bedrijfscode een persoonlijke code kunnen worden toegevoegd; een code slechts bekend bij bevoegde personen. Bij het ontbreken van een dergelijke persoonlijke code mag de ontvanger niet zonder meer veronderstellen dat het versturende bedrijf gebonden is en lijkt het verstandig contact op te nemen. Dit laatste kan, evenals het gebruik van een persoonlijke code naast een bedrijfscode, in de interchange agreement worden afgesproken.

9.3.3 Beveiliging

Uitwisseling van gegevens met behulp van computers dient (volledig) betrouwbaar te zijn. Het is immers heel vervelend als bedrijven goederen geleverd krijgen die niet besteld zijn. Ter vergroting van de betrouwbaarheid kunnen partijen overeenkomen hun berichten te beveiligen. In veel gevallen zullen hiervoor technische en organisatorische maatregelen en procedures getroffen dienen te worden. Deze specificaties horen niet thuis in een interchange agreement en worden daarom veelal opgenomen in een aparte gebruikershandleiding. In de beveiligingsparagraaf in de interchange agreement wordt dan, wanneer noodzakelijk, verwezen naar deze handleiding. In de interchange agreement zelf wordt slechts opgenomen dat berichten beveiligd verstuurd moeten worden volgens een bepaalde methode.

Aangezien beveiliging kostbaar is, kunnen partijen eveneens overeenkomen alleen een bepaald type bericht beveiligd te versturen. Tevens zullen bepaalde verplichtingen ten aanzien van de beveiliging worden afgesproken. EDI-deelnemers kunnen in de beveiligingsparagraaf melding maken van een zorgplicht ten aanzien van de beveiliging: partijen dienen zorgvuldig met de beveiligingsmethode om te gaan. Ontstaan er toch problemen omtrent de beveiliging, of komt bijvoorbeeld de beveiligingsmethode in handen van onbevoegden, dan kan worden afgesproken dat daarvan onmiddellijk melding wordt gemaakt aan de deelnemers: een meldingsplicht.

9.3.4 Gebreken en procedures

Het is denkbaar dat, ondanks zorgplicht en beveiliging, bij gebruikmaking van EDI-systemen gebreken in de berichtgeving ontstaan. Een bericht komt in het geheel niet aan, het komt onvolledig aan of mogelijk dubbel. Ter constatering

van eventuele gebreken kunnen in de interchange agreement afspraken worden gemaakt over controle van berichten.

Partijen kunnen bijvoorbeeld overeenkomen dat berichten een volgnummer krijgen. Als een bericht dan niet of dubbel aankomt, mist de ontvangende partij in het eerste geval een bericht en heeft deze in het laatste geval twee berichten met hetzelfde nummer. Indien partijen geen intensief contact hebben zou het echter wel enige tijd kunnen duren alvorens ontdekt wordt dat een bericht niet is aangekomen. In dat geval zou het verstandig zijn dat partijen afspreken in plaats van volgnummers te gebruiken, een bericht van ontvangst terug te sturen.

Onvolledigheid van een bericht wordt uiteraard niet geconstateerd met gebruik van volgnummers. Om te kunnen controleren of een bericht al dan niet volledig is aangekomen, dienen daarom andere procedures te worden afgesproken. Controle hiervan kan bijvoorbeeld plaatsvinden door een berekening los te laten op het totaal aantal karakters van een bericht. Het resultaat van de berekening wordt vervolgens aan het bericht toegevoegd. De ontvangende partij voert dezelfde berekening uit op het ontvangen bericht en kan aan de hand van het meegeleverde getal controleren of het bericht volledig is.

Ten aanzien van gebreken dienen partijen tevens af te spreken dat onmiddellijk melding wordt gemaakt van een gebrek. Ook hier dus een meldingsplicht.

9.3.5 Aansprakelijkheid

Indien geen aansprakelijkheidsparagraaf zou zijn opgenomen, dan zouden fouten in de berichten of tijdens het gebruik van het EDI-systeem in beginsel aan de afzender worden toegerekend. Dit wordt anders, indien de fout is tot stand gekomen door toedoen van de ontvanger, een werknemer van de ontvanger, een door de ontvanger ingeschakelde derde, of indien de ontvanger het gebruik van het EDI-systeem aan de afzender heeft voorgeschreven. Het lijkt evenwel verstandiger een regeling op te nemen in de interchange agreement waarin staat dat wanneer één van de partijen de verplichtingen niet nakomt, zoals bijvoorbeeld de hierboven genoemde meldingsplicht bij beveiliging, deze partij aansprakelijk is voor de ontstane schade. Voor eventuele calamiteiten zouden partijen kunnen overeenkomen de schade evenredig over de deelnemers aan het EDI-netwerk te verdelen.

9.3.6 Bewijs

Ook in de papierloze EDI-omgeving kunnen problemen ontstaan die mogelijk leiden tot een rechtsgeschil. Mogen partijen de elektronische berichten als bewijs opvoeren in een geschil? Hoe zal de rechter deze berichten waarderen en wie dient wat te bewijzen? Ingevolge art. 179 lid 1 Burgerlijke Rechtsvordering mag bewijs door alle middelen geleverd worden. Dit zou betekenen dat EDI-berichten vastgelegd op moderne informatiedragers (tape, diskette) geschikt zijn als bewijsmiddel. Lid 2 van hetzelfde wetsartikel geeft echter aan dat de waardering van het bewijs, de bewijskracht, aan het oordeel van de rechter wordt overgelaten. Hoewel geschikt als bewijsmiddel, zal een rechter kunnen twijfelen aan de bewijskracht van berichten op tape of diskette. Deze zijn immers 'eenvoudig' te wijzigen zonder sporen na te laten. Een bewijsleverende partij zou de berichten kunnen wijzigen om op die wijze een voor die partij voordelige beslissing te bewerkstelligen. Een rechter zal aan de berichten op tape of diskette niet kunnen zien dat deze zijn gewijzigd.

Partijen kunnen ter voorkoming van terzijde legging van EDI-berichten als bewijsmiddel, afspreken bepaalde technische en organisatorische maatregelen te nemen die de bewijskracht van deze middelen kunnen versterken. In de interchange agreement kunnen regelingen worden opgenomen aangaande opslag, registratie en beveiliging van ontvangen EDI-berichten. Bedrijven kunnen bovendien afspreken daartoe een functie te creëren in de vorm van een bestandsbeheerder, of iemand inhuren die een dergelijke taak op zich neemt, bijvoorbeeld een VANS-leverancier.

Wanneer partijen echter zekerheid wensen omtrent de toelaatbaarheid van elektronische berichten als bewijsmiddel en over de bewijskracht daarvan, kunnen bewijskwesties beter in een aparte bewijsovereenkomst worden geregeld. In dit soort overeenkomsten kunnen partijen regelen dat moderne informatiedragers als bewijsmiddelen bij een rechtsgeschil toegelaten dienen te worden. Tevens kan worden vastgelegd dat de middelen volledige bewijskracht hebben, mits aan bepaalde procedures ten aanzien van opslag, registratie en beveiliging is voldaan. Tegenbewijs en de bewijslastverdeling worden veelal ook in een bewijsovereenkomst geregeld.

9.3.7 Bewaring

Een laatste onderwerp uit de interchange agreement dat hier wordt besproken betreft de bewaring van EDI-berichten. Drie verplichtingen ten aanzien van bewaring worden onderkend: de boekhoudplicht, de bewaarplicht en de verplichting tot het verlenen van inzage in de gegevens.

De artt. 2:10 en 3:15a BW, zoals laatstelijk gewijzigd bij de wet van 8 november 1993, met het oog op de in de praktijk gegroeide situatie van

geautomatiseerde administraties (in werking getreden per 1 januari 1994) bevatten de boekhoud- en bewaarplicht voor een ieder die een beroep of een bedrijf uitoefent. In deze artikelen, die in de plaats komen van art. 6 van het Wetboek van Koophandel, is naast 'boeken en bescheiden' opgenomen 'andere gegevensdragers'.

Deze wetswijziging maakte een einde aan de onzekerheid of onder 'boeken en bescheiden' ook geautomatiseerde administraties konden worden begrepen. De bewaringstermijn bedraagt ingevolge art. 2:10 lid 3 BW tien jaar. Met uitzondering van de op papier te stellen balans en staat van baten en lasten, mogen gegevens op andere gegevensdragers worden overgebracht en bewaard, indien dit juist en volledig gebeurt en zij binnen redelijke tijd leesbaar kunnen worden gemaakt (art. 2:10 lid 4 BW). Aan een dergelijk overbrengen blijft overigens een risico verbonden. Uit de in dit artikel geschapen mogelijkheid volgt namelijk niet dat de *bewijskracht* van aldus in digitale vorm omgezette documenten dezelfde blijft als die van de oorspronkelijke, ondertekende documenten, zoals akten.

In geval van een rechtsgeschil kan de rechter openlegging van de boeken, bescheiden en andere gegevensdragers vragen (art. 8 Wetboek van Koophandel). Aanschaf van nieuwe hard- en/of software zou aan inzage in de weg kunnen staan. Oude gegevens zijn met de nieuwe programmatuur en/of apparatuur mogelijk niet meer te benaderen. Bedrijven dienen daarom maatregelen te nemen om de bewaarde gegevens toegankelijk te houden. Daartoe zou in de interchange agreement de verplichting opgenomen kunnen worden oude gegevens te allen tijde toegankelijk te houden door middel van conversie, of door bewaring van oude hard- en/of software.

9.4 Conflictbeslechting

In paragraaf 9.2 is betoogd dat het huidige recht niet in de weg behoeft te staan aan het sluiten van (het merendeel) van transacties door middel van EDI-technieken. Ten aanzien van de voorwaarden waaronder handelspartners kunnen deelnemen aan EDI-verkeer, hebben we in paragraaf 9.3 een aantal onderwerpen aangestipt waarvan het wenselijk is deze vooraf te regelen, bij voorkeur in een interchange agreement. Voor zover het EDI-verkeer zich afspeelt binnen min of meer besloten systemen, bijvoorbeeld in een bedrijfskolom, zal het aangaan van een interchange agreement tussen de VANS-leverancier (of EDI-beheerder) met de verschillende participanten geen noemenswaardige obstakels met zich mee brengen. Dit kan anders zijn in het geval de ontwikkeling naar meer 'open' EDI-netwerken zich in de toekomst zal voortzetten. In zijn 'handboek voor revolutionair management' stelt Tom Peters:

'De techniek is een andere autonome variabele, die van invloed is op alle aspecten van het zakenleven. Zoals reeds genoemd heeft die geleid tot een revolutie in het geldwezen, maar ook onderstaande gebieden zijn daardoor voor altijd veranderd: (...).'

Het voor dit betoog van toepassing zijnde gebied is dat van de distributie.

'Computer- en telecommunicatietechniek maken het mogelijk over de hele wereld een welhaast eindeloze reeks samenwerkingsverbanden aan te gaan.'

Voorts zijn er talloze voorbeelden aan te dragen van de toename van internationalisering van het handelsverkeer. Het zou de flexibiliteit die nodig is voor een slagvaardig optreden van ondernemingen aanzienlijk inperken, indien in deze situaties telkens vooraf een interchange agreement zou moeten worden gesloten. In de volgende paragraaf wordt stil gestaan bij de vraag of de met het EDI-berichtenverkeer samenhangende problematiek eigenlijk wel een oplossing behoeft vanuit een juridische optiek, of dit wel een 'juridisch' vraagstuk is. In de paragrafen 9.4.2 en 9.4.3 tenslotte wordt een perspectief geschetst waarin ten aanzien van sommige geschillen in het veld van EDI-transacties de rol van de traditionele geschillenbeslechter - de rechter - aan belang kan inboeten, ten gunste van - bijvoorbeeld - EDI-netwerkbeheerders.

9.4.1 Recht versus techniek

Zowel bij besloten als bij open netwerken wordt door EDI-gebruikers en technici verwachtingsvol uitgekeken naar oplossingen van juristen om de hierboven gesignaleerde problemen met betrekking tot het EDI-verkeer weg te nemen. Men kan zich echter afvragen wat het recht hieraan heeft toe te voegen. Natuurlijk zullen er conflicten optreden wanneer men zich bedient van EDI. Nemen we als voorbeeld problemen terzake van de authentificatie van de afzender, of beweerde discrepanties tussen het verzonden bericht en het ontvangen bericht. 'Juridisch' gezien, zijn dit geen onoplosbare problemen. Op basis van huidige rechtsregels, dogmatiek en jurisprudentie zijn juristen (en rechters) heel wel in staat te beoordelen in wiens risicosfeer dergelijke problemen vallen. Al naar gelang de omstandigheden van het geval (Is EDI door een van de partijen voorgeschreven?; Heeft een van de partijen zich niet gehouden aan procedure-afspraken?; Mocht de ontvanger van het bericht in het licht van het voorafgaande EDI-gebruik erop vertrouwen dat het ontvangen bericht inderdaad van de daarop vermelde afzender afkomstig was?; enzovoorts) zal een partij met de bewijslast worden opgezadeld, waarbij het vervolgens dan niet denkbeeldig is dat hij tengevolge van bewijsnood aan het kortste eind zal trekken. *Wetsaanpassingen*, bijvoorbeeld een wettelijke gelijkstelling van een elektronische toegangscode aan een traditionele hand-

tekening, of een wettelijke regeling met betrekking tot de bewijskracht van een elektronisch bericht, zullen tot een andere *verdeling* van het risico kunnen leiden. Maar dat is nog steeds geen oplossing voor het eigenlijke probleem, namelijk dat er kennelijk twijfel bestaat omtrent de authenticiteit dan wel de integriteit van het bericht. En aangezien het bedrijfsleven niet gediend is met oplossingen waardoor voortaan niet meer partij A, maar partij B de schade zal moeten dragen - en een dergelijke oplossing evenmin tot stimulering van EDI-verkeer zal leiden - kijken juristen voor dit soort problemen verwachtingsvol uit naar oplossingen aangedragen door EDI-gebruikers en technici. Indien de gebruiker, dan wel de gebruikte techniek de twijfel kan wegnemen, dan hebben juristen vervolgens geen moeite met de juridische merites van het geschil.

Voorts dient de vraag zich aan of (aanpassing van) het nationale recht nog wel adequaat is om de voorwaarden te constitueren waaronder deze ontwikkeling plaats kan hebben, mede gelet op het grensoverschrijdend karakter van EDI. Een ontkennend antwoord roept de vraag op, of internationale verdragen wèl de juridische aspecten van EDI zouden kunnen bepalen, of dat zij slechts een verschuiving van de problematiek zouden betekenen. Naar het schijnt zijn juridische aspecten van het grensoverschrijdend elektronisch handelsverkeer niet meer effectief te regelen door nationale of internationale overheden en zullen betrokkenen - de deelnemers aan EDI en de netwerkbeheerders - steeds meer hun toevlucht nemen tot de opstelling van eigen, grensoverschrijdende regelingen. Een voorzichtige verwachting is dan ook dat de (nabije) toekomst een verschuiving te zien zal geven van interveniërende (nationale) overheidsrechtspraak naar een meer autonoom opererend (internationaal) bedrijfsleven waarbinnen vooraf de 'spelregels' worden vastgelegd op basis waarvan conflictoplossende beslissingen worden genomen.

9.4.2 EDI-beheerder als conflictbeslechter

De keuze voor een bepaalde vorm van conflictoplossing kan door rationele criteria bepaald worden, waarvoor beslissend is de verwachte mate van effectiviteit. Niet-juridiserende vormen van conflictoplossing blijken soms effectiever te kunnen werken dan bijvoorbeeld overheidsrechtspraak of formele vormen van arbitrage. Gezien de specifieke eisen die het EDI-verkeer stelt ten aanzien van de juridische implicaties, is het nog slechts een kleine stap om ook de oplossing van mogelijke conflicten die kunnen voortvloeien uit een door middel van EDI gesloten overeenkomst op te nemen in de interchange agreement, dan wel in de 'Algemene Voorwaarden' van de netwerkbeheerder. Deze laatste lijkt vervolgens de aangewezen instantie om de rol van bemiddelaar op zich te nemen, en uiteindelijk ook de beslissing te

nemen. Het is de vraag of daarna nog een beroep op de gewone rechter nuttig is. Aan deze vraag ligt onder meer de overweging ten grondslag, dat de marktwerking regelend zal optreden. Wanneer de netwerkarbiter te dikwijls beslissingen neemt die voor een zekere partij onaantrekkelijk zijn, wordt het voor die partij aantrekkelijk zijn EDI-transacties over een ander netwerk te laten lopen.

9.4.3 Een rechtstoekomstig perspectief

Recht is een neerslag van de noden van de tijd. Het is niet per definitie zo dat de huidige organisatie daarvan ook voor de toekomst het meest effectief zou zijn. Het is zeer wel denkbaar dat de oplossing van sommige geschillen meer gebaat is bij het passeren van de gewone rechter. Een toenemend EDI-gebruik zal de 'monopoliepositie' van de gewone rechter (voor zover daarvan op dit moment nog sprake is) met zijn nationale beperkingen meer en meer ter discussie stellen. Ook supranationale ontwikkelingen als een verenigd Europa zullen onvoldoende geschikt blijken om de economische ontwikkelingen in internationaal verband op de oude voet te blijven volgen. Er is nu eenmaal ook een toenemend handels- en dataverkeer met landen buiten de EU.

We hebben hier overheidsvertegenwoordigers als marktpartij laten fungeren, met hun 'aanbod' van (inter)nationale rechtsregels en gewone rechters als conflictbeslechters. De gedachte dat ook overheidsdienaren rationeel zijn en dus hun eigen belangen trachten te bevorderen is de kern van de 'public choice' theorie. Ook in een 'rechtsfuturologisch' perspectief is deze zienswijze waarschijnlijk uiterst nuttig. Te verwachten is een versterkte, voortgezette strijd tussen internationale bedrijven - die meer en meer ook 'juridisch' werk voor hun rekening nemen - en nationale en supranationale overheden, waarvan de vertegenwoordigers zullen trachten het verlies van het marktaandeel in conflictbeslechtende produkten zoveel mogelijk te voorkomen. In democratieën zou de strijd aldus moeten verlopen, dat die vormen van conflictoplossing die voor de burgers het nuttigst zijn, beschikbaar zijn en blijven.

9.5 Jurisprudentie

HR 27 NOVEMBER 1992, FAX VERZOEKSCHRIFT IS GELDIG, CR 1993/1

Een redelijke, met de voortgang van de communicatietechniek rekening houdende en met de eisen van een goede procesorde verenigbare wetstoepassing brengt mee dat, ingeval een naar behoren ondertekend verzoekschrift volledig, met de daarop zichtbare ondertekening, per fax wordt verzonden naar en ontvangen door de griffie van het gerecht waarbij het moet worden

ingediend, de ter griffie ingekomen faxkopie dient te worden aangemerkt als een naar behoren ondertekend verzoekschrift.

HR 19 NOVEMBER 1993, STG. cova - nmb, CR 1994/4
De aard van de rechtsverhouding tussen een bank en haar cliënt/kredietnemer brengt niet mee dat de nadelige gevolgen van onbevoegd gebruik van een tussen de bank en haar cliënt overeengekomen beveiligingscode voor het verzenden van betalingsopdrachten per telex, in beginsel - behoudens afwijkend beding in de overeenkomst van partijen - voor rekening van de bank behoren te komen. De vraag wie van partijen, bij gebreke van een contractuele regeling op dit punt, het risico van misbruik van een overeengekomen code behoort te dragen, dient te worden beantwoord aan de hand van de concrete omstandigheden van het geval, waarbij in het bijzonder van belang is aan wie valt toe te rekenen dat de code ter kennis van de onbevoegde is gekomen. Is de onbevoegde in dienst van de cliënt of staat hij anderszins in een relatie tot de cliënt waardoor hij gemakkelijker dan willekeurige derden toegang tot de code heeft kunnen verkrijgen, dan zal er in het algemeen grond voor een dergelijke toerekening aan de cliënt zijn, nu alsdan in beginsel mag worden aangenomen dat het misbruik aan gebrek aan diens zorg te wijten is. Dit zal slechts anders zijn in door de cliënt te stellen en te bewijzen omstandigheden die een zodanig gebrek aan zorg uitsluiten.

9.6 Literatuur

- Esch, R.E. van en C. Prins (red.), 'Recht en EDI', Kluwer, Deventer, 1993
- Graaf, F. De e.a., 'Juridische aspecten van netwerken', NVVIR, 1990.
- Hofman, W.J., 'Edi-handboek; Elektronische gegevensuitwisseling tussen organisaties', Tutein Nolthenius, Amsterdam, 1989.
- Mitrakas, A., 'Changes in the interchange agreements', in: Electronic Commerce, N. Adam en Y. Yesha, Springer Verlag, Berlijn, 1996.

10 Elektronisch betalingsverkeer

Betalingen kunnen tegenwoordig op verschillende manieren plaats vinden. Naast contante betaling in 'wettig betaalmiddel' (chartaal geld: muntgeld en bankbiljetten, art. 6:112 BW) en girale betaling (bijschrijving van het verschuldigde bedrag op de rekening van de schuldeiser, art. 6:114) kennen we betaalcheques, credit cards, magneetstripkaarten en chipkaarten. De laatste drie betaalvormen vallen onder de noemer 'elektronisch betalingsverkeer'. Het verschil tussen de magneetstripkaart en de chipkaart is dat met behulp van de eerste in een on-line verbinding met de bank een bedrag wordt *overgeboekt* van de ene bank- of girorekening naar de andere, waar de chipkaart meer de functie vervult van portemonnee omdat deze zelf een geldswaarde vertegenwoordigt. Bij betaling door middel van een chipkaart neemt de geldswaarde op de chipkaart af en komt het betreffende bedrag - gelijk chartaal geld - direct ter beschikking van de schuldeiser. De aldus door de schuldeiser in diens betaalautomaat verzamelde bedragen worden vervolgens - gelijk chartaal geld - 'bijgestort' op diens rekening. Op grond van de Algemene voorwaarden acceptatie chipknip heeft de schuldeiser zich verbonden een betaling door middel van een chipknip te aanvaarden als voldoening van een geldschuld zonder enig voorbehoud.

De term 'elektronisch *geld*verkeer' is ruimer; daaronder kunnen ook de elektronisch verzonden betaalopdrachten naar bank of giro worden begrepen,

het elektronisch bankieren, en bijvoorbeeld de opname van contant geld uit geldautomaten. Betalingen via internet kunnen tegenwoordig geschieden door bedragen over te schrijven van de eigen 'internetrekening' naar die van de schuldeiser (het I-Pay-systeem), maar ook door middel van de chipkaart. In dat geval moet de chipkaart in een aparte kaartlezer worden gestoken, waarna de geldswaarde op de chipkaart wordt verminderd met het bedrag van de aankopen die via internet zijn gedaan, welk bedrag dan weer direct ter beschikking komt van de schuldeiser. De eerste vorm van betaling via I-pay heeft een 'giraal karakter'; internetbetalingen met de chipkaart hebben weer meer het karakter van een 'contante betaling'.

Ten aanzien van het elektronisch betalingsverkeer zijn er, naast de juridische kwalificatie van de betaling, twee aspecten van belang vanuit juridisch oogpunt: misbruik of onbevoegd gebruik van pas, kaart of code (paragraaf 10.1), en privacy van de houder daarvan (paragraaf 10.2). Evenals in de situatie van het elektronisch *handels*verkeer (hoofdstuk 9), kunnen we ons ook hier afvragen of de gesignaleerde problematiek wel adequaat met behulp van juridische regels valt weg te nemen. In paragraaf 10.3 wordt de suggestie neergelegd dat technische maatregelen, te nemen door de uitgevers van betaalmiddelen, niet alleen meer effect zullen ressorteren, doch ook van betekenis kunnen voor de verdeling van aansprakelijkheid en bewijs. In paragraaf 10.4 tenslotte wordt aandacht besteed aan de wijze van conflictbeslechting en het instrument van zelfregulering dat daarbij wordt gehanteerd.

10.1 Misbruik

Het gebruik van betaalautomaten, geldautomaten en (bank)pasjes brengt met zich mee dat niet altijd met zekerheid is vast te stellen dat zij door een daartoe bevoegd persoon zijn gebruikt. Misbruik van het betaalmiddel spitst zich natuurlijk toe op het vraagstuk van de authenticiteit (paragraaf 10.1.1) en, in het verlengde daarvan, dat van aansprakelijkheid en bewijs (paragraaf 10.1.2).

10.1.1 Authenticiteit

In het huidig elektronisch betalingsverkeer staat nog het gebruik van de magneetstripkaart met pincode centraal. Het belangrijkste probleem hierbij is dat, hoewel de pincode persoonsgebonden is, niet met zekerheid is vast te stellen of de pas ook daadwerkelijk door de daartoe bevoegde persoon is gebruikt. De code kan aan een ander zijn medegedeeld, hij kan zijn opgeschreven (zeker indien men over een aantal pasjes met verschillende pincodes beschikt wordt het lastig om ze allemaal te onthouden en uit elkaar te hou-

den), of hij kan door derden zijn uitgelezen. In het geval van een betwiste afschrijving komt de vraag aan de orde welke waarde men kan toekennen aan het gebruik van de pincode. De gehanteerde woordkeuze 'elektronische handtekening' doet te gemakkelijk suggereren dat aan een pas met pincode dezelfde juridische gevolgen zijn verbonden als aan een handtekening.

Vandenberghe ('De betekenis van de handtekening bij het elektronisch betalingsverkeer en teleshopping', in: Elektronisch betalingsverkeer en teleshopping) kent aan de traditionele handtekening in het algemeen drie functies toe:

1. Identificatie van de afkomst van het document,
2. Bevestiging van de inhoud en
3. Het bewijs van instemming van de ondertekenaar met de juistheid c.q. volledigheid.

Omdat zij met de hand geschreven is, vervult de handtekening de functie van *identificatie* van de ondertekenaar. Omdat zij niet zomaar gezet wordt, doch doorgaans na lezing van het document, wordt de handtekening opgevat als een bevestiging dat *van de inhoud van het document is kennis genomen*. Tenslotte geeft de handtekening weer de *instemming* van de ondertekenaar met de inhoud van het document. De handtekening authentificeert derhalve de fysieke aanwezigheid van de ondertekenaar, alsmede de wil van de ondertekenaar om van de inhoud kennis te nemen en erdoor gebonden te worden.

Vergelijken we dit met de functie van de pincode, dan zien we dat de pincode niet meer is dan een *toegangscode* om van de geldautomaat of van de betaalautomaat gebruik te kunnen maken. De pincode vervult noch de functie van identificatie van de gebruiker - gegeven de mogelijkheid dat de code bij een derde bekend kan zijn geworden - noch de functie van bewijs voor wilsovereenstemming. De pincode wordt immers ingetoetst *voorafgaand* aan de transactie en kan derhalve niet dienen als *bekrachtiging* daarvan. In dit licht gezien ware het dan ook juister te spreken van een 'elektronische toegangscode' dan van een 'elektronische handtekening'.

10.1.2 Aansprakelijkheid en bewijs

De relatie tussen bank en consument wordt in Nederland hoofdzakelijk bepaald door de Voorwaarden gebruik Geld- en Betaalautomaten. Deze voorwaarden verklaren tevens van toepassing de Algemene Voorwaarden. Op grond van deze Algemene Voorwaarden worden geschillen omtrent betwiste afschrijvingen van de bankrekening geregeerd door de bekende 'boekenclausule' van de banken: de administratie van de bank geldt als volledig bewijs, behoudens tegenbewijs door de rekeninghouder.

In het geval van verlies of diefstal van de pas, dient de rekeninghouder dit zo spoedig mogelijk te melden bij de bank. Tot het moment van melding draagt de rekeninghouder een eigen risico van fl. 350,-. Echter, zowel op de bank als op de rekeninghouder rust een zorgplicht. Als we kijken naar die van de rekeninghouder - deze dient zorgvuldig om te gaan met pas en bijbehorende pincode - dan zien we dat in de geschillen die voor de Geschillencommissie Bankbedrijf zijn gebracht, bijna zonder uitzondering is aangenomen dat de rekeninghouder niet voldoende zorgvuldig is geweest, zodat de beperking van het eigen risico tot fl. 350,- veelal niet meer dan papieren bescherming biedt. Men kan zich afvragen of de rekeninghouder die de Algemene Voorwaarden voor het gebruik van pas en pincode heeft gelezen, en zich daarmee akkoord heeft verklaard vanuit de gedachte dat een onbevoegde opname kennelijk nooit meer dan fl. 350,- zou kosten, zich hier wel voldoende rekenschap van heeft gegeven.

Eén opmerkelijk feit kan hier nog vermeld worden. Geschillen met betrekking tot betwiste opnames zijn te onderscheiden in die gevallen waarbij de rekeninghouder niet meer beschikte over de pas, en geschillen waarbij de rekeninghouder nog wel in het bezit was van de pas.

Deze laatste type gevallen zijn door de Geschillencommissie Bankbedrijf zonder uitzondering beslecht in het nadeel van de rekeninghouder. De redenering hierachter is dat de rekeninghouder wel op enigerlei wijze onzorgvuldig moet zijn geweest met de pas en de geheimhouding van de pincode, anders zou de opname niet hebben kunnen plaats vinden. Hoewel ook de eerste type gevallen doorgaans in het nadeel van de rekeninghouder worden beslecht, lijkt de diepere wijsheid toch vooral hierin gelegen dat, mocht een pashouder ooit geconfronteerd worden met een naar zijn mening onterechte afschrijving en verschrikt in zijn portemonnee kijken of de pas er nog wel is, hij dan vooral niet opgelucht moet ademhalen als blijkt dat de pas niet is verloren of gestolen, maar de pas onmiddellijk weg moet gooien.

10.2 Privacy

Een volgend aspect is dat van de privacy; de vraag in hoeverre het gebruik van elektronische betaalmiddelen - en de daarmee gepaard gaande registratie van betalingen - een inbreuk kan zijn op de persoonlijke levenssfeer van de gebruiker.

Een kenmerkend verschil met de situatie dat geld wordt opgenomen aan de balie van de bank waarmee vervolgens aankopen contant worden betaald is dat bij elektronisch betalingsverkeer de anonimiteit van het koopgedrag verdwijnt. Elektronisch geldverkeer kan voor de organisatie die dit betalingsverkeer beheert - bank of grootwinkelbedrijf bijvoorbeeld - inzicht opleveren in de bestedingspatronen en voorkeuren van gebruikers, met name indien de

afrekeningen centraal worden geregistreerd. De informatie die uit de vastlegging van gegevens wordt opgedaan, kan worden gebruikt voor bijvoorbeeld het al dan niet toekennen van een krediet, of voor marketingdoeleinden.

Registraties als hier bedoeld vallen onder de werking van de Wet Persoonsregistraties (zie hoofdstuk 11, hierna). Dat betekent bijvoorbeeld dat gegevens uit deze registraties niet zonder meer aan derden mogen worden verstrekt. Voorts is het de vraag of deze gegevens wel op die manier door de organisatie zelf mogen worden gebruikt, aangezien zij voor een ander doel zijn verkregen, namelijk ten behoeve van de rekening-courant registratie. Op voorhand lijkt het een te ver gaande 'oplossing' om dan maar in de doelomschrijving van een registratie, die wordt gevoerd met het oog op de verwerking van 'elektronische betalingen', op te nemen dat de registratie tevens is bedoeld voor het verkrijgen van marketinginformatie. Niettemin is het denkbaar dat geregistreerden uit zichzelf bereid zijn een gedeelte van hun privacy prijs te geven. Zo zouden zij *toestemming* kunnen geven tot het vastleggen en het gebruiken van gegevens met betrekking tot hun aankopen. Vooral consumenten uit lagere inkomensgroepen zouden daartoe wel eens eerder bereid kunnen zijn, indien zij daarvoor 'beloond' worden met aanbiedingen van de kruidenier. De ontwikkelingen op het gebied van 'spaarprogramma's' zijn illustratief.

Dat elektronische vastlegging van persoonsgegevens een ontwikkeling te zien geeft naar een steeds grotere controle over individuen hebben we bijvoorbeeld meegemaakt met het Fi-nummer, het fiscaal nummer. Bij de invoering daarvan werd gesteld dat het fiscaal nummer uitsluitend bedoeld was voor *intern* gebruik door de fiscus. Echter, onder aanvoering van het argument van doelmatigheid (lees: effectievere fraudebestrijding), werd niet lang na de invoering het fiscaal nummer omgedoopt in sociaal/fiscaal nummer, het SoFi-nummer, opdat ook uitkerende instanties van hetzelfde nummer gebruik konden maken. En nu de reorganisatie van de gemeentelijke bevolkingsboekhouding is afgerond met de invoering van de Gemeentelijke Basis-Administratie, zien we dat voor het daarin gehanteerde A-nummer, het administratienummer, wederom voor het sofinummer is gekozen, zodat we thans kunnen spreken van het SoFiA-nummer, dus hetzelfde nummer ook in de gemeentelijke registers. Voegen we dit bij het gegeven van de (thans nog beperkte) legitimatieplicht, dan zijn we niet ver meer verwijderd van het SoFiA-legitimatiebewijs.

Ziet het gebruik van magneetstripkaart en credit card met name op vormen van girale betaling, met de komst van 'chipknip', 'chipper' en andere betaalsystemen wordt ook het terrein van het chartaal geld betreden (elektronische contante betaling). Initiatieven als deze worden vaak gemeenschappelijk ondernomen door banken, grootwinkelbedrijven en telecommunicatieleveranciers. Hier ligt een belangrijke taak voor de Registratiekamer en voor consumentenorganisaties om tot normering te komen. Het binnen het

Nationaal Chipcard Platform - een overlegorgaan waarin overheid, bedrijfsleven en consumentenbond zijn vertegenwoordigd - tot stand gekomen akkoord over de privacyregels terzake van het gebruik van chipkaarten, is daartoe een uitgangspunt.

10.3 Juridische of technische oplossingen?

Hierboven zijn een drietal gebieden geschetst rondom welke de problematiek met betrekking tot vormen van elektronisch betalingsverkeer zich afspelen: authenticiteit, aansprakelijkheid en bewijs en privacy. Participanten in dat verkeer - banken, retailers en gebruikers - verwachten veelal een juridische oplossing voor deze problemen. Het valt echter te betwijfelen of daar veel heil van is te verwachten.

De *authenticiteit* van pincodes is juridisch niet te regelen. Het voor de wet gelijk stellen van een 'elektronische toegangscode', de pincode dus, aan een handtekening - iets dat om wege hetgeen hierboven is vermeld reeds verre van aan te bevelen is - zal op zichzelf geen oplossingen bieden voor de onderliggende problemen, namelijk dat van misbruik en dat van verminderde betrouwbaarheid. Het zou wel tot een verdergaande inbreuk op de rechtsbescherming van consumenten leiden.

Er zijn reeds wettelijke regels met betrekking tot *aansprakelijkheid en bewijs*. Een andere verdeling daarvan - wellicht in sommige concrete gevallen billijker; in andere niet - leidt evenmin tot een oplossing. Het recht maakt een eind aan het geschil, niet aan het daaraan ten grondslag liggende probleem

Er is momenteel een Wet Persoonsregistraties alsmede een EU-richtlijn voor de bescherming van persoonsgegevens. Niettemin zullen deze wettelijke maatregelen slechts van geringe invloed zijn, indien individuen zelfstandig hun *privacy* opgeven, teneinde daarvoor een - gezien hun omstandigheden - onmisbaar voordeel mee te behalen. Het valt sowieso te betwijfelen of we van de overheid adequate maatregelen ter bescherming van de privacy van burgers mogen verwachten, gezien de geschetste ontwikkeling in het gebruik van persoonsgegevens door de overheid zelf (zie ook paragraaf 11.3 hierna).

Het heeft er alle schijn van dat deze door de techniek gecreëerde problematiek ook door de techniek zal moeten worden opgelost. Het vraagstuk van de identificatie (niet dat van de wilsuiting) zou kunnen worden opgelost door het gebruik van meer persoonsgebonden kenmerken zoals vingerafdrukken, netvliesstructuur of hersenimpulsen. Maar los van de ontwikkelingen op het gebied van de biometrie zou alleen al de vervanging van de magneetstrip op de huidige pinpas door een chip de omvang van deze problematiek aanzienlijk kunnen doen afnemen.

Door de mogelijkheid gevarieerder algoritmen, door de gebruiker zelf te bepalen, in de chip vast te leggen, zal het steeds aannemelijker te maken zijn dat de pas ook daadwerkelijk door de rekeninghouder is gebruikt. Bovendien lijkt het in dat geval 'billijker' dat het bewijsrisico bij de rekeninghouder ligt, in zoverre de chip-technologie onbevoegd gebruik zo goed als onmogelijk zou maken. Omdat gegevens op de chip zelf kunnen worden vastgelegd, vervalt bovendien de noodzaak tot het bijhouden van gedetailleerde centrale registraties.

Bij chipkaarten die zijn bedoeld voor het doen van 'contante betalingen' behoeft voor de betalingen zelf geen pincode te worden ingetoetst; alleen voor het 'opladen' van de kaart bij de geldautomaat (teneinde geldswaarde van de eigen rekening over te hevelen naar de chipkaart) is de pincode vereist. Het zal duidelijk zijn dat deze chipkaarten in beginsel zo kunnen worden toegepast dat geen inbreuk op privacy van kaarthouders behoeft te worden gemaakt. Of dit in de praktijk ook het geval zal zijn, valt te betwijfelen. Gelet op de combinatie van kaartnummer, rekening-courantnummer en betaalgegevens is in ieder geval een deel van het betalingsgedrag van de kaarthouder voor banken inzichtelijk. Omdat de chipkaart daarnaast 'onderdak' kan bieden aan andere dienstenaanbieders, die mogelijk ook gebaat zijn met het registreren van gegevens omtrent bestedingsgedrag van de kaarthouder, is het zeker niet denkbeeldig dat het anonimiserende element dat in het gebruik van chipkaarten ligt besloten niet zal worden benut.

De suggestie om de oplossingen van de hier gesignaleerde problemen te zoeken in techniek, betekent niet dat we met een blind vertrouwen in techniek alleen kunnen volstaan. Vanzelfsprekend blijven er eisen te stellen aan de organisatie rond het elektronisch betalingsverkeer, aan de beveiliging daarvan (waarin *encryptie-techniek* een onmisbare factor vormt) en (zorgvuldigheids)-eisen aan de gebruiker.

De banken hebben de afgelopen jaren op grote schaal geïnvesteerd in automaten gebaseerd op de magneetstripkaart. Indien echter chiptechnologie inderdaad betrouwbaarder zou zijn en voor minder juridische problemen zou zorgen, verdient het aanbeveling ook de magneetstrip op de kaart voor 'girale overschrijvingen' - de huidige 'pinpas' - te vervangen door een chip. Zolang banken nalaten om zodoende bij te dragen tot een meer betrouwbaar elektronisch geldverkeer, is het interessant om te volgen of dit nalaten van de banken de Geschillencommissies ertoe zal brengen de bewijspositie van consumenten te versterken.

10.4 Zelfregulering en conflictbeslechting

Bij gebreke van de mogelijkheid tot adequate wettelijke regelingen, zien we een tendens tot zelfregulering om te trachten de hier besproken problemen rond het elektronisch betalingsverkeer beheersbaar te maken:

Zo biedt de Wet Persoonsregistraties de mogelijkheid tot het opstellen van gedragscodes. Een voor een bepaalde branche representatieve organisatie kan, na genoegzaam overleg met organisaties van belanghebbenden, nadere regels opstellen in het belang van de bescherming van de persoonlijke levenssfeer van geregistreerden. In dit verband zijn er gedragscodes opgesteld door het bankbedrijf en door het direct marketingbedrijf (waaronder ook het gebruik van direct marketing technieken voor het eigen bedrijf wordt gerekend), en is, zoals hierboven reeds genoemd, binnen het Nationaal Chipcard Platform overeenstemming bereikt over een privacycode met betrekking tot het gebruik van chipkaarten.

Deelname aan het elektronisch betalingsverkeer en het gebruik van cards worden beheerst door privaatrechtelijke overeenkomsten tussen banken en consumenten en de door de banken opgestelde voorwaarden: Algemene Voorwaarden (1996), Voorwaarden gebruik Geld- en Betaalautomaten (1989), Voorwaarden Chipknip en Algemene Voorwaarden Acceptatie Chipknip (beiden uit 1995))

Geschillen die voortvloeien uit de deelname aan het elektronisch betalingsverkeer worden beslecht door de Geschillencommissie Bankbedrijf voor wat betreft transacties met de banken, en door de Geschillencommissie Bankzaken waar het de Postbank betreft. Ook hier met als uitgangspunt de algemene bankvoorwaarden en de ‘boekenclausule’.

Dit hoofdstuk wordt besloten met het signaleren van een ontwikkeling waardoor die tendens tot zelfregulering zich in de toekomst waarschijnlijk nog verder zal voortzetten.

Door het onderscheiden van de verschillende functies in het betalingsverkeer zullen in het marktsegment van de bancaire dienstverlening nieuwe aanbieders zich aandienen. Zo zou met de beëindiging van de monopoliepositie van BEA-net (een dochteronderneming van Interpay, die op zijn beurt weer een dochteronderneming is van een aantal Nederlandse banken), de verwerking van betalingstransacties ook verzorgd kunnen worden door nieuwe facilitaire aanbieders, of bijvoorbeeld door de grootwinkelbedrijven zelf. Een ontwikkeling waardoor een onderlinge concurrentieverhouding zal ontstaan, waarbinnen ook de gehanteerde voorwaarden voor deelname aan het betalingsverkeer betrokken kunnen worden. Voorts zien we dat bijvoorbeeld credit card organisaties inmiddels een belangrijk aandeel hebben in het betalingsverkeer, tot aan de verstrekking van kredietfaciliteiten toe.

Tenslotte kan nog worden gewezen op het toenemende belang van EDI en internet als middel voor het tot stand brengen van handelstransacties. Het is zeker niet ondenkbaar dat EDI-netwerkbeheerders ook een rol zullen gaan spelen in de afhandeling van betalingen. Indien er een conflict ontstaat met betrekking tot een (vermeende) onjuiste afschrijving, zal de consument het meest gebaat zijn bij die organisatie die de voor hem of haar aantrekkelijkste voorwaarden hanteert. Voor zover het geen geschil met de facilitaire dienstverlener zelf betreft, is er in de toekomst voor deze laatste nog een rol weggelegd in het oplossen van geschillen tussen leveranciers en afnemers, indien de transactie via diens netwerk tot stand is gekomen.

10.5 Jurisprudentie

GESCHILLENCOMMISSIE BANKBEDRIJF, 21 OKTOBER 1987, CR 1988/3

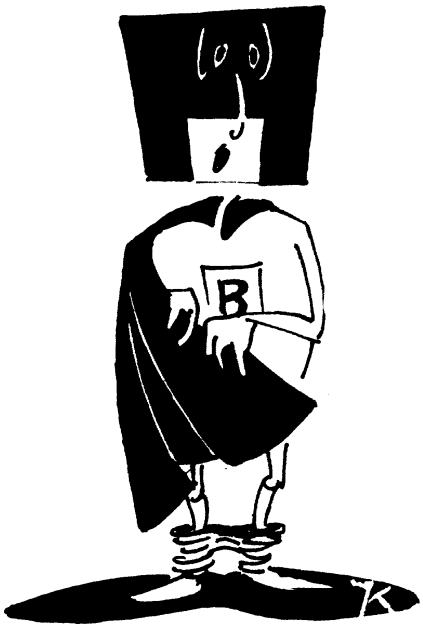
Het systeem waarbij van een geldautomaat gebruik wordt gemaakt, laat immers niet toe dat fouten, waarvan niet kan worden bewezen dat zij door de bank zijn gemaakt, zonder meer voor haar risico komen indien het geld met behulp van een bankpas blijkt te zijn opgenomen. Dit geldt in het bijzonder ook in het geval als het onderhavige waarin cliënt geen onvrijwillig bezitsverlies van bankpas en code kan aantonen. Cliënt heeft niet aangetoond dat bij het ten laste van zijn rekening brengen van de op 25 februari 1987 opgenomen gelden, door de bank een fout is gemaakt. Cliënt heeft daarmee het tegenbewijs, als bedoeld in art. 8 van het reglement, niet geleverd. (Alle uitspraken terzake van de zogenoemde 'spookopnames' - waarbij de pas dus niet wordt vermist - zijn uitgelegd in het nadeel van de rekeninghouder.)

GESCHILLENCOMMISSIE BANKBEDRIJF, 24 APRIL 1990, CR 1990/4

Uit de resultaten van het door de bank verrichte onderzoek is komen vast te staan, dat cliëntes bankpas bij de onbevoegde opnames is gebruikt en dat in ieder geval binnen drie pogingen de juiste pincode is gebruikt. De commissie overweegt evenwel, dat de bank daarmee nog niet heeft aangetoond dat cliënte niet aan haar verplichtingen heeft voldaan. Art. 18 lid 2.c.3 van de voorwaarden Bankpas en Geld- en Betaalautomaten bepaalt immers, dat de aansprakelijkheid van cliënt voor de gevolgen van onbevoegd gebruik vóór de melding wordt verhoogd tot het bedrag van de onbevoegde transacties, indien de bank kan aantonen dat de onbevoegde transacties hebben kunnen plaatsvinden doordat de houder van de bankpas zijn verplichtingen uit hoofde van art. 15 lid 2 van bovengenoemde voorwaarden niet heeft nageleefd. (Van alle uitspraken waarbij de pas wèl wordt vermist, is dit de enige uitspraak waarbij de bank in het ongelijk is gesteld, omdat de bank niet voldoende bijkomende omstandigheden had aangevoerd.)

10.6 Literatuur

- Ballon, G.L., F. De Ly en R.E. de Rooy, 'Juridische aspecten van moderne betaalmiddelen', preadvies van de Vereeniging Handelsrecht, W.E.J. Tjeenk Willink, Zwolle, 1987.
- Esch, R.E. van, 'De chipknip: het virtuele chartale geld', in: Computerrecht 1996/4.
- Esch, R.E. van en J.M.A. Berkvens, 'Giraal betalingsverkeer / Elektronisch betalingsverkeer', Kluwer, Deventer, 1988.
- Knobbout Bethlem, Ch.E., 'Konsumentgericht elektronisch betalings-verkeer', (diss.), Utrecht, Deventer, 1992.
- Rooy, R.E., 'De chipknip: een (juridische) verkenning', in: Nederlands Juristenblad 1996/14.
- Schutte, H. en C. Stuurman (red.), 'Elektronisch betalingsverkeer en teleshopping', Kluwer, Deventer, 1988.



11 Bescherming van persoonsgegevens

Iedere Nederlander bevindt zich gemiddeld in enkele tientallen persoonsregistraties. De registraties lopen uiteen van geboortenregister en bevolkingsadministratie, registraties bij de fiscus en de sociale verzekeringsinstanties, onderwijsregistraties, personeelsregistraties en medische registers, registraties bij banken en verzekeringen tot en met allerhande ledenadministraties en persoonsregistraties voor commerciële doeleinden. Ook de aard van de gegevens loopt uiteen: van 'eenvoudige' NAW-gegevens tot gevoelige gegevens, bijvoorbeeld omtrent gezondheid, overtuiging, sex of strafrechtelijk verleden.

Het ter beschikking stellen van persoonsinformatie is niet zo vanzelfsprekend als het aantal registraties doet voorkomen. Vanwege de inmenging in de persoonlijke levenssfeer zullen mensen niet zonder meer bereid zijn hen betreffende gegevens te openbaren, zeker niet als de betreffende gegevens door hen als 'gevoelig' worden ervaren. Ook de onzekerheid over wat er met eenmaal verstrekte gegevens gebeurt draagt bij aan deze terughoudendheid. Daar staat tegenover dat het maatschappelijk nut, en soms ook de legitimiteit, het verzamelen van persoonsgegevens wenselijk maakt. Het vraagstuk van de bescherming van persoonsgegevens kan aldus worden weergegeven dat het noodzakelijk is waarborgen te creëren omtrent de verzameling, de opslag en de verwerking van persoonsgegevens, opdat betrokkenen bereid zullen blijven

tot het verstrekken van persoonlijke gegevens aan de overheid en andere organisaties die daarbij een belang hebben.

Een belangrijke factor die van invloed zal zijn op de ontwikkeling van het privacybegrip is de toename van het gebruik van en het aantal geautomatiseerde persoonsregistraties. Computersystemen worden steeds krachtiger en goedkoper. Professionele programmatuur is ook beschikbaar voor personal computers. Dit maakt het mogelijk dat steeds meer organisaties meer (persoons)gegevens opslaan en vasthouden.

Ook de toepassing van computersystemen is aan verandering onderhevig. Meer en meer worden computers gebruikt voor elektronisch berichtenverkeer. Mededelingen, maar ook hele bestanden, kunnen gemakkelijk van de ene plaats naar de andere worden verstuurd. De grotere en snellere computergeheugens maken het veelal niet nodig bestanden te wissen om schijfruimte te winnen. Eenzelfde bestand kan dan op verschillende plaatsen - binnen en buiten de organisatie - beschikbaar zijn. Het elektronisch berichtenverkeer blijft niet beperkt tot de landsgrenzen.

In dit hoofdstuk zal in paragraaf 11.1 eerst een nadere plaatsbepaling van het vraagstuk van bescherming van persoonsgegevens worden gegeven. In paragraaf 11.2 worden vervolgens enkele hoofdlijnen besproken van de Wet Persoonsregistraties, een wettelijke regeling die met het oog op de hierboven genoemde belangen is tot stand gekomen. Vanwege de bijzondere positie die de overheid inneemt bij dit vraagstuk, namelijk zowel regelgever als gebruiker van persoonsbestanden, wordt dit hoofdstuk in paragraaf 11.3 besloten met de rol van de overheid.

11.1 Plaatsbepaling

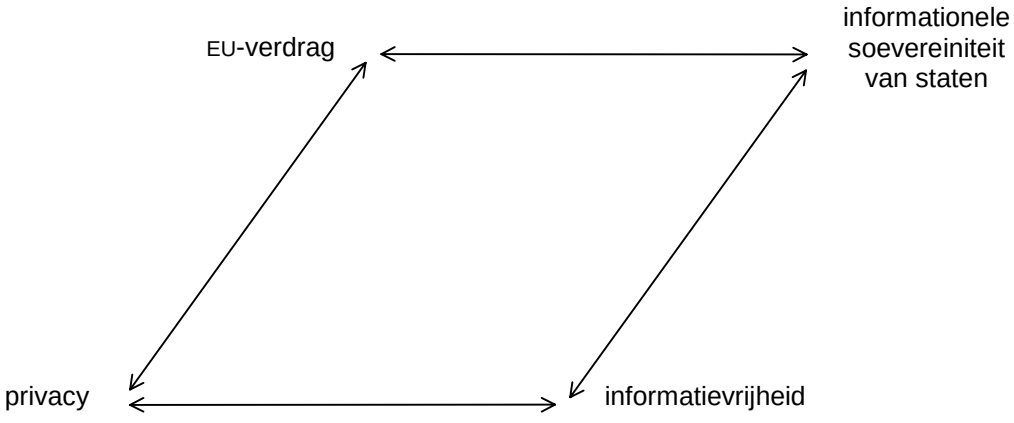
De bescherming van persoonsgegevens is een onderdeel van het informatierecht. In de ‘oudere’ literatuur wordt dit vaak onder *privacybescherming* besproken, maar dan is er sprake van een minder correcte plaatsbepaling. Privacybescherming is namelijk veel ruimer en omvat bijvoorbeeld ook het huisrecht en de bescherming van het privéleven. Voorbeelden hiervan zijn de strafbaarstelling van het afluisteren van gesprekken en het maken van sluipfoto’s. Een rechterlijke uitspraak op dit gebied is bijvoorbeeld die over het plaatsen van camera’s in een fabriekshal, waardoor permanente controle op de werknemers mogelijk was. Dit werd niet toelaatbaar geacht op grond van een te ver gaande inbreuk op de privacy van de werknemers (Rb. Roermond, 12 september 1985, RvdW 1985/6). De bescherming van persoonsgegevens krijgt als jongste loot van het privacyvraagstuk op het moment zoveel aandacht in de privacydiscussie, dat het andere aspecten daarvan lijkt te overschaduwen. De

effecten van automatisering op klassieke privacy-aspecten lijken daardoor soms in het gedrang te komen. Ten onrechte, want deze klassieke aspecten vormen wel de basis voor steeds nieuwe invullingen.

Binnen de moderne ontwikkelingen is een nieuwe vorm van denken ontstaan over persoonsgegevens in de vorm van het *databeschermingsrecht.* Er is daarbij sprake van een emancipatieproces ten opzichte van het klassieke privacybegrip. Bescherming van persoonsgegevens is ook weer slechts een onderdeel van het databeschermingsrecht. Databescherming bestrijkt namelijk ook begrippen die buiten het privéleven vallen. Hierbij spelen onder meer vraagstukken als informatie als economisch goed, de macht die aan informatie ten grondslag ligt en de invloed op sociale verhoudingen.

Een aspect van *privacy*bescherming heeft te maken met de gevoeligheid van gegevens. *Data*bescherming blijkt betrekking te hebben op de strategische waarde van informatie: het moet mede zorgen voor de regulering van informatiestromen, waarbij rekening gehouden moet worden met nationaal strategische belangen. Privacy is in deze problematiek maar een onderdeel.

De consequentie hiervan is dat de visie op het beschermen van persoonsgegevens snel geëvolueerd is. De oorspronkelijke visie, zoals die in de jaren ‘60 naar boven kwam, werd bepaald door het idee dat voorkomen moest worden dat individuele personen schade werd berokkend. Acties werden gebaseerd op de onrechtmatige daad. Er heeft zich echter in hoog tempo een evolutie voltrokken, waardoor die functie nog slechts een onderdeel vormt van de huidige visie. Die houdt in, dat het in het algemeen in een informatiesamenleving nodig is dat er gereguleerd wordt in de informatiestromen. Daarbij spelen er, vanuit maatschappelijk oogpunt, tegenstrijdige belangen. De behoefte aan informatievrijheid staat tegenover andere belangen die vragen om bescherming van de persoonlijke levenssfeer. Deze discrepantie maakt normering en regulering noodzakelijk.



Figuur 4: spanningsveld tussen verschillende belangen.

In figuur 4 zien we enerzijds een spanningsveld tussen de ten behoeve van de bescherming van de persoonlijke levenssfeer gewenste beperking aan de verspreiding van persoonsgegevens ten opzichte van het grondrecht van informatievrijheid en anderzijds een spanningsveld ten opzichte van het in het EU-verdrag neergelegde beginsel van het vrije verkeer van goederen, personen, diensten en kapitaal (en gegevens). Hetzelfde kan men constateren voor wat wel genoemd wordt de 'informationele soevereiniteit van staten', het zelfbeschikkingsrecht van staten met betrekking tot strategische (en andere) informatie. Voorts spelen er in dit verband natuurlijk ook nog belangen als bestrijding van fraude en andere vormen van criminaliteit.

De wettelijke verankering van de eerbiediging van de persoonlijke levenssfeer vinden we in art. 8 EVRM (Europese Verdrag tot bescherming van de Rechten van de Mens en de fundamentele vrijheden), art. 17 BuPo (Internationaal verdrag inzake Burgerrechten en Politieke rechten) en art. 10 lid 1 van de Grondwet. Daarnaast treffen we daarmee samenhangende rechten aan, bijvoorbeeld in art. 11 GW, de integriteit van het menselijk lichaam, art. 12 GW, het huisrecht en art. 13 GW, het brief-, telegraaf- en telefoongeheim.

Voor wat betreft het databeschermingsrecht ziet art. 10 GW in lid 2 op de vastlegging en verstrekking van persoonsgegevens en in lid 3 op het recht op kennisneming daarvan en verbetering.

Het grondrecht van informatievrijheid, ook wel genoemd de 'free flow of information', ligt vast in art. 10 EVRM, art. 19 BuPo en de artt. 7 en 8 GW.

11.1.1 Historische achtergrond

De ontwikkeling van het privacybegrip heeft plaatsgevonden in de laatste 100 jaar. Door de opkomst van de urbanisatie en de toename van de communicatiemedia is er sprake van een gelijktijdige ontwikkeling in Duitsland, Frankrijk en de VS rond 1880-1890.

Waar men in Europa vanuit de persoonsrechten-gedachte meent dat binnen de samenleving bescherming van de persoon moet plaatsvinden, geschiedt de ontwikkeling in de VS veel meer op pragmatische gronden. De advocaten Warren en Brandeis hadden als leden van bekende families last van de Amerikaanse roddelpers (yellow press) en zochten daar als rechtgeaarde juristen bescherming tegen. Deze bescherming vonden zij in een bepaling in de Amerikaanse constitutie. Op deze bepaling baseerden zij een recht op privacy. Een artikel van hun hand in de Harvard Law Review van 15 december 1890, waarin zij privacy beschreven als 'the right to be let alone', maakte school en als gevolg daarvan bleek het mogelijk o.a. te procederen tegen de roddelpers en tegen bepaalde vormen van reclame (Samuel D. Warren en Louis D. Brandeis, 'The right to privacy', Harvard Law Review, 1890 nr. 4).

Eveneens bleek het nadien mogelijk inbreuken op de fysieke privésfeer aan te pakken. Een voorbeeld daarvan is het afluisteren door middel van een microfoon. Daar kon voorheen alleen tegen worden opgetreden indien de microfoon in het huis was geplaatst, op grond van overtreding van het huisrecht. Was deze microfoon echter buiten het huis geplaatst dan viel er niets aan te doen. Dit kon nu ondervangen worden op grond van privacybepalingen. Door deze laatste mogelijkheden was de ontwikkeling binnen de VS tamelijk succesvol.

In Europa ging de ontwikkeling veel minder snel. Daar ontstonden verschillende wetsartikelen en werden rechterlijke uitspraken gedaan, die later onder het privacybegrip konden worden gebracht. In Nederland zien we dit bijvoorbeeld in de opname van persoonlijkheidsrechten in de Auteurswet 1912 en de toepassing van het onrechtmatige daadsartikel uit het BW. Persoonlijkheidsrechten hebben betrekking op de immateriële kant van het auteursrecht: de auteur mocht niet in zijn persoonlijkheid worden geschaad door de wijze van uitgeven. Een voorbeeld van een actie gebaseerd op onrechtmatige daad is het proces dat gevoerd werd ter voorkoming van publikatie van foto's van twee (corpulente) dames op het strand. Het oordeel van de rechter was dat publikatie alleen gericht was op het opwekken van de lachlust. Op grond van de aantasting van de persoonlijkheid werd het daarom verboden. De privacy was, hoewel niet uitdrukkelijk genoemd, wel duidelijk in het geding. In deze tijd zijn onder meer het huisrecht en het telefoongeheim ontstaan.

In 1951 volgt de eerste wetgeving op het gebied van de bescherming van persoonsadministraties: de Wet op de Justitiële Documentatie. In 1971 zien we de eerste wetgeving op het gebied van privacy: de strafbaarstelling van het afluisteren van telefoongesprekken in art. 139 e.v. Sr. Hieraan liggen verschillende ontwikkelingen ten grondslag.

Zo publiceerde Westin in 1967 in de VS het boek 'Privacy & Freedom'. Hierin worden technieken beschreven die inbreuk maken op wat in de VS het klassieke rechtsgoed van de privacy was. Het recht op privacy had vorm gekregen opdat burgers zich ongestoord kunnen ontplooien. Hiervoor was een set van wettelijke instrumenten ontwikkeld. Nieuwe technieken echter, brachten mogelijkheden waar de privacyregeling niet op van toepassing was, waardoor een aanpassing nodig was. Westin omschrijft het recht op privacy als 'de aanspraak van individuen, groepen of organisaties voor zichzelf te bepalen wanneer, hoe en in welke mate informatie omtrent hen kan wordt medegedeeld aan derden'. Hierin wordt ook een recht op privacy voor rechtspersonen ('groepen en organisaties') onderkend, iets dat in sommige ons omringende landen voor een deel ook in privacywetgeving is neergelegd.

De Nederlandse Juristen Vereniging houdt in 1969 een vergadering over de behoefte aan strafrechtelijke bepalingen tegen het afluisteren van telefoon-

gesprekken, het werken met verborgen camera's en verborgen microfoons. Uit de preadviezen komt naar voren dat de strafwetgever terughoudend moet zijn op dit gebied, maar dat de gevaren zo groot zijn dat het noodzakelijk is dat er stappen worden ondernomen. Als gevolg daarvan komen er in 1971 wettelijke bepalingen. Deze zijn echter zeer restrictief.

Een versnelling in de bewustwording vindt plaats door de discussies rond de volkstelling van 1971. Er ontstaat een algemeen gevoel van onvrede zonder dat er veel concrete bezwaren zijn. Die onvrede is gebaseerd op een overheid die massaal gegevens verzamelt, zonder dat er voor de burger zicht op is wat er met die gegevens gedaan zal worden. Onder invloed van deze opinie is er een hoog weigeringspercentage bij het invullen van de formulieren. De verwerking van de gegevens blijkt overigens dermate problematisch dat pas in 1977 informatie beschikbaar komt.

De discussie rond de volkstelling is aanleiding voor een nieuwe reguleringsgolf. Er wordt een staatscommissie ingesteld, de commissie Koopmans, die in 1974 komt met een interimrapport waarin verslag wordt gedaan van de hearings die gehouden zijn. In 1976 volgt een eindrapport. Dit bevat onder meer een voorstel tot een Wet op de Persoonsregistratie. Hoewel in grote mate identiek aan dit ontwerp, volgt eerst in 1981 het wetsontwerp. Op grond van kritiek op de omvang daarvan en mede in verband met de opkomende dereguleringsgolf wordt het ontwerp in de ijskast gezet en later ingetrokken. De commissie Koopmans onderkende een viertal gevarenzones in verband met de vastlegging van persoonsgegevens:

1. De behoefte aan geheimhouding van persoonlijke aangelegenheden: Het gevaar dat persoonlijke informatie wordt losgemaakt uit het verband waarin zij is verkregen;
2. Zelfbeschikkingsrecht: gegevens verkregen voor een bepaald doel mogen niet zonder meer aan anderen ter hand gesteld worden;
3. De behoefte om beslissingen aangaande de eigen persoon te overzien, in plaats dat deze zich, los van de betrokkene, op basis van een persoonsregistratie afspelen.;
4. Commerciële exploitatie.

Soortgelijke bezwaren komen we nadien bijvoorbeeld nog tegen bij Kuitenbrouwer ('Het recht om met rust te worden gelaten', 1991), die wel tien bezwaren weet op te sommen (een van de aardigste daarvan is dat computers niet 'vergeten') en bij Bing, die wijst op het bezwaar dat iemand ineens lid wordt van een groep, in plaats van een uniek en gelijkgerechtigd lid van de samenleving.

Met de grondwetsherziening van 1980 wordt art. 10 opgenomen, met betrekking tot het recht op bescherming van de persoonlijke levenssfeer. In lid 2

van dat artikel wordt de opdracht aan de wetgever neergelegd om regels vast te stellen aangaande de bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens. Voor de invoering van een regeling wordt een termijn van 10 jaar gesteld. In juli 1985 wordt er een nieuw ontwerp ingediend: de Wet Persoonsregistraties. Dit ontwerp wijkt sterk af van het ontwerp van 1981. De ontwikkeling van 1967 tot nu wordt gekenmerkt door een verschuiving van privacy van het huisrecht naar de 'informationele privacy'. Er wordt meer uitgegaan van het data-beschermingsrecht; de bescherming van het privéleven staat meer op de achtergrond.

11.1.2 Europese dimensie

De Wet Persoonsregistraties, die in 1989 in werking is getreden, is de invulling van de in art. 10 GW neergelegde opdracht. Voor de Nederlandse wetgeving zijn ook nog van belang:

- Aanbeveling van de OESO (Organisatie voor Economische Samenwerking en Ontwikkeling) houdende richtlijnen voor bescherming van het privéleven en grensoverschrijdend verkeer van persoonsgegevens, uit 1980;
- Verdrag van de Raad van Europa tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens, Straatsburg, 1981;
- De EU-richtlijn van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (95/46/EG, nr. L Pb 281/31)

Zowel de OESO-aanbeveling als het Verdrag van Straatsburg zijn in eerste instantie bedoeld om een onbelemmerd verkeer van persoonsgegevens tussen de bij de organisaties aangesloten lidstaten mogelijk te maken. Beide bevatten aanwijzingen voor de nationale wetgeving. In de OESO-aanbeveling (die, anders dan EU-richtlijnen, niet verbindend is) wordt een achttal grondbeginselen voor toepassing op nationaal niveau geformuleerd:

1. Het beginsel van beperkte verzameling
   Het verzamelen van persoonsgegevens dient aan beperkingen onderhevig te zijn en ieder van die gegevens dient met oirbare en wettige middelen verkregen te zijn, zo nodig met medeweten of instemming van de betrokkene.
2. Het beginsel van de hoedanigheid van de gegevens
   Persoonsgegevens moeten ter zake dienend zijn, gegeven het doel waarvoor zij bestemd zijn, en voorzover dat doel het eist, juist en volledig te zijn en te worden bijgehouden.

3. Het beginsel van het aangeven der doeleinden
   De doeleinden waarvoor persoonsgegevens verzameld worden dienen te worden aangegeven niet later dan het tijdstip van verzamelen en het gebruik dat er vervolgens van wordt gemaakt dient te worden beperkt tot het nastreven van die doeleinden, of van andere doeleinden die met de voorgaande in overeenstemming zijn en worden aangegeven op het tijdstip van de wijziging.
4. Het beginsel van het beperkt gebruik
   Persoonsgegevens mogen niet worden geopenbaard, verstrekt of gebruikt voor andere doeleinden dan die aangegeven overeenkomstig het vorige beginsel, tenzij
   a) met toestemming van betrokkene; of
   b) uit hoofde van een wettelijke bepaling.
5. Het beginsel van veiligheidsnormen
   Persoonsgegevens dienen door redelijke veiligheidswaarborgen te worden omgeven tegen risico's zoals teloorgaan van gegevens of ongeoorloofde toegang, vernietiging, gebruik, wijziging of onthulling van gegevens.
6. Het beginsel van openheid
   Er dient een algemeen beleid van openheid te worden gevoerd met betrekking tot ontwikkelingen, praktijk en beleid inzake persoonsgegevens. Gerede mogelijkheden moeten voorhanden zijn om het bestaan en de aard van persoonsgegevens te kunnen vaststellen, alsmede de hoofddoeleinden waarvoor zij worden gebruikt en de identiteit en gewoonlijke woonplaats van de opdrachtgever.
7. Het beginsel van individuele inspraak
   Het individu dient het recht te hebben:
   a) van de opdrachtgever of langs andere weg uitsluitsel te verkrijgen over de vraag of de opdrachtgever gegevens over hem bezit;
   b) gegevens die op hem betrekking hebben meegedeeld te krijgen:
      1. binnen een redelijke termijn;
      2. tegen betaling van een bedrag dat, indien dit geheven wordt, niet buitensporig hoog is;
      3. op een bevredigende wijze; en
      4. in een voor hem begrijpelijke vorm;
   c) opgave te krijgen van de redenen voor afwijzing van een verzoek ingediend overeenkomstig de paragrafen a en b en in de gelegenheid te worden gesteld, tegen die weigering verweer te voeren;
   d) gegevens die op hem betrekking hebben te wraken en indien hij in het gelijk wordt gesteld, verwijdering, verbetering, aanvulling of wijziging van die gegevens te verkrijgen.

8. Het beginsel van de verantwoordelijkheid
   Elke opdrachtgever dient de verantwoordelijkheid te dragen voor het naleven van de maatregelen uitvoering gevend aan bovenvermelde beginselen.

Het verdrag van Straatsburg (dat bindend is voor de aangesloten lidstaten die het verdrag hebben geratificeerd) kent in hoofdstuk II soortgelijke 'grondbeginselen van gegevensbescherming'. Omtrent de hoedanigheid van de gegevens stelt art. 5:

Persoonsgegevens die langs geautomatiseerde weg worden verwerkt, dienen:
a) op eerlijke en rechtmatige wijze te worden verkregen en verwerkt;
b) te worden opgeslagen voor bepaalde en legitieme doeleinden en niet te worden gebruikt op een wijze die onverenigbaar is met die doeleinden;
c) toereikend, ter zake dienend en niet overmatig te zijn, uitgaande van de doeleinden waarvoor zij worden opgeslagen;
d) nauwkeurig te zijn en, zo nodig, te worden bijgewerkt;
e) te worden bewaard in een zodanig vorm dat de betrokkene hierdoor niet langer te identificeren is dan strikt noodzakelijk is voor het doel waarvoor de gegevens zijn opgeslagen.

Voorts bevat het verdrag bepalingen ten aanzien van gegevens met betrekking tot ras, politieke overtuiging, godsdienstige of andere levensbeschouwing, gezondheid, seksueel gedrag en strafrechtelijke veroordelingen (art. 6) beveiliging (art. 7) en waarborgen voor de betrokkene met het oog op kennisneming, inzage, verbetering en rechtsmiddelen (art. 8).

Een met art. 5 van het Verdrag overeenkomende bepaling komen we in de EU-richtlijn tegen in art. 6. Bepalingen met betrekking 'gevoelige gegevens' vinden we in art. 8; het inzage- en correctierecht wordt geregeld in de artt. 10 t/m 12.

De beginselen van de OESO-aanbeveling en van het Verdrag van de Raad van Europa dienen we terug te vinden in de huidige Wet Persoonsregistraties. De EU-richtlijn zal deze wet echter aanmerkelijk bijstellen. De combinatie daarvan met richtlijnen terzake van grensoverschrijdende betalingen en digitale communicatienetwerken zal vermoedelijk tot een stringentere regelgeving ter bescherming van de persoonlijke levenssfeer leiden dan thans het geval is. Verantwoordelijk voor deze aanscherping in de gedachtenvorming is de explosie van geautomatiseerde registraties voor allerhande toepassingen, bij overheid zowel als bedrijfsleven, en de toename in vastleggingstechnieken tengevolge van chipkaarten en telecommunicatievoorzieningen. In de volgende paragraaf zullen enkele hoofdlijnen van de Wet Persoonsregistraties worden besproken.

11.2 De Wet Persoonsregistraties

Onder *persoonsregistratie* wordt in de Wet Persoonsregistraties (WPR) verstaan een samenhangende verzameling van op verschillende personen betrekking hebbende persoonsgegevens, die langs geautomatiseerde weg wordt gevoerd of met het oog op een doeltreffende raadpleging van die gegevens systematisch is aangelegd. *Persoonsgegevens* zijn gegevens die herleidbaar zijn tot een individuele natuurlijke persoon (art. 1).

De definitie van persoonsregistraties maakt een onderscheid tussen geautomatiseerde en niet-geautomatiseerde registraties. Dit onderscheid zal onder de werking van de richtlijn komen te vervallen.

Art. 2 bepaalt tezamen met de definitie van persoonsregistratie uit art. 1 de reikwijdte van de wet. De uitzonderingen betreffen persoonsregistraties van gering belang - zoals voor persoonlijk gebruik - (art. 2 lid 1), bij wet ingestelde persoonsregistraties met een openbare functie (lid 2) en persoonsregistraties met een kennelijk bijzonder karakter omdat zij gebaseerd zijn op of wel de Wet op de Inlichtingen- en Veiligheidsdiensten, of wel de Politiewet (lid 3). Voorbeelden van persoonsregistraties voor persoonlijk of huiselijk gebruik zijn behalve de al dan niet geautomatiseerde verjaardagskalender ook zakagenda's en persoonlijke werkaantekeningen. Een criterium voor de beoordeling van deze laatste categorie kan zijn of de aantekeningen aan een eventuele opvolger zouden worden overgedragen.

Sommige registraties worden wel gekarakteriseerd als bedrijfsregistraties, als zou dit iets anders zijn dan persoonsregistraties. De term bedrijfsregistratie is onzuiver en werkt misleidend. Een bedrijfsregistratie (beter zou zijn ‘bedrijvenregistratie’) is een registratie van gegevens over bedrijven/rechtspersonen, waarin ook natuurlijke personen voorkomen. In de toelichting bij de WPR wordt in dit verband wel gesproken over gemengde registraties. Het gedeelte van de registratie dat betrekking heeft op rechtspersonen (voorzover de rechtspersoon niet is te herleiden tot een individueel natuurlijk persoon zoals bij een éénmans B.V.) is niet te karakteriseren als een persoonsregistratie. De bepalingen uit de WPR met betrekking tot persoonsregistraties zijn hierop niet van toepassing. Wel bevat de registratie persoonsgegevens, zoals de namen van de directie, commissarissen e.d. De bepalingen uit de WPR met betrekking tot persoonsgegevens zijn hierop wel van toepassing. Het gedeelte van de registratie over niet-rechtspersonen (firma, V.O.F., C.V., natuurlijke personen) is een persoonsregistratie in de zin van de WPR. De bedrijfsregistratie als totaal valt dus onder de werking van (bepalingen van) de WPR. In de wet wordt voorts geen onderscheid aangebracht tussen gegevens met een privékarakter of met een zakelijk karakter.

Op basis van art. 7 van de WPR zijn nadere regels opgesteld voor 'gevoelige' gegevens, zoals gegevens betreffende geloof en ras, maar ook strafrechtelijke

gegevens. De ratio van art. 7 is dat voor deze categorie een strenger regime geldt. De definitie van persoonsgegeven vraagt niet meer dan dat een gegeven herleidbaar is tot een individueel natuurlijk persoon. Dit betreft dus zowel 'gevoelige' gegevens als 'gewone' gegevens.

Soms wordt wel gemeend dat bestanden niet onder de wet vallen als zij zijn opgebouwd uit gegevens uit *openbaar toegankelijke* bronnen, uit gegevens dus die voor eenieder vrij toegankelijk zijn. De wet is tot stand gekomen tegen de achtergrond dat privacy van geregistreerden beter beschermd moet worden. Het opslaan van gegevens - ook openbaar verkrijgbare gegevens - kan bij een bepaald gebruik inbreuk maken op de privacy van die personen. Zelfs op zichzelf onschuldige gegevens kunnen, gecombineerd met andere onschuldige gegevens, door een bepaald gebruik een bedreigend karakter aannemen voor de geregistreerde. De WPR zou haar doel dus voorbijstreven indien zij uitzonderingen toeliet voor openbaar toegankelijke gegevens. Dit houdt in dat vanaf het moment dat gegevens uit een openbaar register in de registratie zijn verwerkt, de betrokkenen zijn opgenomen in een persoonsregistratie waarop de WPR van toepassing is. De WPR is evenwel niet van toepassing op de openbare registers zelf (art. 2 lid 2).

Houder is degene (of de rechtspersoon) die zeggenschap heeft over een persoonsregistratie. Volgens de Memorie van Antwoord is dat degene die bevoegd is het doel, de inhoud en het gebruik van de registratie te bepalen en die beslist over de aanleg en de beëindiging ervan. Het begrip houder is primair functioneel van aard. Onder *bewerker* verstaat de WPR degene die het geheel of een gedeelte van de apparatuur onder zich heeft waarmee een persoonsregistratie, waarvan hij niet de houder is, wordt gevoerd. Deze definitie heeft met name het oog op de zogenaamde 'servicebureaus' en 'rekencentra', wier werkzaamheden bestaan uit het verwerken en beheren van gegevens ten behoeve van cliënten of gelieerde instellingen en het bieden van faciliteiten voor het raadplegen van bestanden door cliënten. Deze werkzaamheden kunnen betrekking hebben op ondermeer loon- en salarisadministraties, financiële administraties, leden- en abonnementsbestanden, marketingbestanden e.d.

De meeste servicebureaus en rekencentra vormen ware bolwerken van verzamelingen van persoonsgegevens. In verband daarmee werd het noodzakelijk geacht de positie van de bewerkers te adresseren, zij het dat hun verantwoordelijkheden in de WPR minder ver strekken dan die van houders van persoonsregistraties. Diverse voorschriften hebben uitdrukkelijk betrekking op bewerkers:

- art. 1: het door een houder verstrekken van persoonsgegevens aan een bewerker valt niet onder het WPR-regime van het verstrekken van gegevens aan een derde;
- art. 8: beveiligingsplicht voor bewerkers;

- art. 9 lid 3: aansprakelijkheid van bewerkers;
- art. 10 lid 1: rechterlijk verbod jegens de bewerker;
- art. 26: de bewerker handelt conform de gegevens welke door de houder aan de Registratiekamer zijn aangegeven;
- art. 50 lid 1 sub b: strafbepaling voor de bewerker.

De Wet Persoonsregistraties is gebaseerd op drie peilers:
1. Materiële normen (paragraaf 11.2.1);
2. Zelfregulering, middels reglementen en gedragscodes (paragraaf 11.2.2);
3. Zichtbaar maken voor geregistreerden dat zij zijn geregistreerd (paragraaf 11.2.3, Belangen van geregistreerden).

11.2.1 Materiële normen

Art. 1 van de WPR bestaat uit definities van kernbegrippen uit de wet. Deze definities zijn summier en laten veel over aan de praktische invulling. Ditzelfde geldt voor andere in de wet voorkomende termen, zoals 'redelijkerwijs', 'onevenredig', 'naar verwachting' enzovoorts. Gezien de veelheid van de in de samenleving voorkomende, uiteenlopende registraties is dit begrijpelijk. Ook vanuit het oogpunt van vorming van de gewenste beschermingsomvang is de ruime definiëring verklaarbaar. Hoewel de jurisprudentie wel heeft bijgedragen tot invulling van het privacybegrip en de discussie over privacybescherming van de afgelopen decennia de diverse belangen heeft verhelderd, is het nog afwachten welke nieuwe impulsen er van wetgeving op dit terrein zullen uitgaan. Van een *afgerond* juridisch leerstuk kan nog niet worden gesproken. De WPR, wel getypeerd als kaderwet, steunt sterk op nadere invulling door belanghebbenden. Eveneens wordt veel aan de afweging van de civiele rechter overgelaten.

Te gedetailleerde wetgeving zou te weinig ruimte kunnen laten aan technologische ontwikkelingen en toepassingen kunnen belemmeren. Zelfs zou deelname aan het internationale handelsverkeer beperkingen kunnen ondervinden. Evenmin is de mate van inbreuk in de persoonlijke levenssfeer van geregistreerden voldoende vastomlijnd. De opzet van de WPR met ruime materiële normen, moet het mogelijk maken dat belanghebbenden - houders van registraties en geregistreerden (en hun belangenvertegenwoordigers) - onderling tot gewenste afbakening geraken. Beziet men de wet echter vanuit haar doelstelling - bescherming van de persoonlijke levenssfeer in verband met persoonsregistraties - dan kan men zich afvragen of dat doel met die vage begripsomschrijvingen is gediend. Waar hier de technologische ontwikkeling als argument wordt genoemd om enige terughoudendheid te betrachten met gedetailleerde regelgeving, schuilt in diezelfde technologie eveneens een bedreiging voor de persoonlijke levenssfeer, waardoor nadere uitwerking juist

wèl als wenselijk kan worden ervaren. Aan de andere kant dient evenwel niet onvermeld te blijven dat technologie ook zo zou kùnnen worden toegepast dat de bescherming van privacy juist wordt bevorderd, de zogenoemde 'Privacy Enhancing Technology'.

Zowel geregistreerden als houders van persoonsregistraties hebben er belang bij dat de in de WPR voorkomende begrippen nauwkeurig worden omschreven, zodat geen onduidelijkheden optreden in de uitvoering van de wet. Geregistreerden verkrijgen meer zekerheid omtrent de in de wet vastgelegde rechten en plichten, terwijl ook houders van persoonsregistraties vooraf beter kunnen vaststellen waar zij aan toe zijn. Ten aanzien van de laatsten kan dit wellicht onnodige kosten uitsparen, terwijl men ook minder risico loopt met een procedure te worden geconfronteerd. Een meer omlijnde begripsomschrijving behoeft overigens niet altijd te betekenen dat de persoonlijke levenssfeer van geregistreerden beter wordt beschermd. Dit kan vanwege een geringere interpretatievrijheid ook leiden tot een beperking in de belangenafweging. Met het dereguleringsfantoom op de achtergrond heeft de wetgever besloten tot deze ruime materiële normen. De wens om tussen geregistreerden en houders van persoonsregistraties onderling tot goede regelingen te komen, komt tot uitdrukking in de instelling van gedragscodes en het (beperkte) toezicht van de Registratiekamer. Als stok achter de deur zijn opgenomen de procesmogelijkheid door belangenorganisaties en de 'dreiging' dat als sectoren niet onderling tot reglementering komen, er van overheidswege nadere regels kunnen worden gesteld. De implementatie van de EU-richtlijn kan mogelijk aan een aantal hier genoemde bezwaren tegemoet komen.

11.2.2 Zelfregulering

Het principe van gecontroleerde zelfregulering vormt een van de belangrijke uitgangspunten in de opzet van de WPR. De in de WPR neergelegde materiële rechtsvoorschriften zijn - algemeen gesproken - globaal van aard, hebben in beginsel betrekking op persoonsregistraties met verschillende functies en van uiteenlopend belang, en differentiëren niet naar de aard van de daarin opgenomen gegevens, hun wijze van verkrijging of het gebruik dat ervan wordt gemaakt. Langs de weg van zelfregulering, dat door de wetgever op diverse plaatsen in de WPR wordt bevorderd, moeten de algemene wettelijke normen op decentraal niveau nader worden geconcretiseerd. De wettelijke voorschriften zullen daarbij met name als 'richtsnoer' kunnen fungeren, aldus de Memorie van Toelichting.

Op het niveau van de afzonderlijke persoonsregistraties biedt de WPR aanknopingspunten voor zelfregulering in de artt. 19 en 24. Eerstgenoemde bepaling heeft betrekking op persoonsregistraties op het gebied van de

overheid, het onderwijs, de gezondheidszorg en de maatschappelijke dienstverlening, welke registraties slechts mogen worden aangelegd indien dat noodzakelijk is voor een goede vervulling van de taak van de houder en waarvoor een reglement dient te worden vastgesteld. Art. 24 regelt de zogenaamde 'formulierplicht' voor persoonsregistraties die niet vallen onder de hiervoor genoemde en die bij de Registratiekamer dienen te worden aangemeld. De wetgever heeft een zekere speelruimte gelaten met betrekking tot het verstrekken van gegevens bij aanmelding aan de Kamer. Zowel reglement als de bij de aanmelding verstrekte gegevens dienen te worden nageleefd en hebben mitsdien normatieve werking (artt. 21 en 26).

Van meer algemene aard is de zelfregulering via een gedragscode: de door een, voor een sector in het maatschappelijk leven representatieve organisatie, in het belang van de bescherming van de persoonlijke levenssfeer gestelde regels of gedane aanbevelingen. Waar de wetgever in de WPR in paragraaf 4 een plaats voor gedragscodes heeft ingeruimd, heeft hij aansluiting gezocht bij bestaande maatschappelijke praktijken. Reeds sedert meerdere jaren normeren vele branche- en werkgeversorganisaties, belangengenootschappen en andere min of meer overkoepelende instellingen de 'informationele privacy' voor hun leden of andere aangeslotenen in 'codes' (onder allerlei naam) met gedragsaanbevelingen of bindende voorschriften. Vrijwel altijd is een groot deel van de inhoud van deze codes branche- of sector-specifiek. Met de WPR is deze vorm van vrijwillige zelfregulering, zowel bij organisaties van houders als van bewerkers, in betekenis toegenomen.

Ten behoeve van maatschappelijke organisaties die representatief zijn voor een bepaalde maatschappelijke sector, schept art. 15, lid 1 van de WPR de bevoegdheid om met betrekking tot de gedragscodes die zij vast stellen, bij de Registratiekamer een zogenoemde 'verklaring van genoegzaamheid' te vragen. In het belang van de rechtszekerheid beoogt zo'n verklaring te voorkomen, dat geregistreerden in het ongewisse komen te verkeren over de vraag of de gedragscode, die immers een regeling van zuiver privaatrechtelijke aard is, niet op gespannen voet staat met de voorschriften van de WPR. Het aanvragen van een verklaring is van facultatief karakter. De verklaring van de Registratiekamer behelst de uitspraak, dat de betreffende gedragscode naar haar oordeel a) in overeenstemming is met het bepaalde bij of krachtens de WPR, en b) voldoet aan redelijkerwijs ter bescherming van de persoonlijke levenssfeer van geregistreerden te stellen eisen.

Indien een voorgelegde gedragscode niet aan beide rechtsvoorschriften beantwoordt, zal de Registratiekamer de verklaring moeten onthouden. Hoewel zulks niet uitdrukkelijk in de WPR is geregeld, is het mogelijk dat de Registratiekamer in dat geval aan de verzoekende organisatie zodanige aanbevelingen tot aanpassing van de gedragscode doet, dat deze een her-

nieuwde toetsing zou kunnen doorstaan. Voor een sturende rol in deze biedt met name art. 37, lid 2 WPR een grondslag.

Alvorens een aan haar voorgelegde gedragscode inhoudelijk te toetsen aan de in art. 15, lid 1 neergelegde eisen, dient de Registratiekamer te onderzoeken of het verzoek voor een verklaring ontvankelijk is. Ook al zou een gedragscode ten volle aan de in dit eerste lid beschreven normen voldoen, dan nog kan het verzoek afstuiten op vragen van ontvankelijkheid. De in het tweede lid gestelde eisen zijn drieërlei: a) de verzoeker van een verklaring dient representatief te zijn voor de sector waarop de gedragscode betrekking heeft, b) de gedragscode dient nauwkeurig te omschrijven voor welke sector zij is opgesteld en c) in genoegzaam overleg met organisaties van belanghebbenden te zijn voorbereid.

11.2.3 Belangen van geregistreerden

Belangen van geregistreerden zijn dat zij zicht erop hebben of er hen betreffende persoonsgegevens in een registratie zijn opgenomen, dat deze gegevens juist zijn en dat het gebruik van die gegevens de persoonlijke levenssfeer van geregistreerden niet onevenredig schaadt.

Een persoonsregistratie mag slechts worden aangelegd voor een bepaald doel (art. 4 lid 1). Ingevolge art. 6 dient ook het gebruik van de opgenomen persoonsgegevens verenigbaar te zijn met het doel van de registratie. Art. 5 bepaalt dat de persoonsgegevens rechtmatig moeten zijn verkregen en in overeenstemming met het doel van de registratie. Voorts rust op de houder de verplichting de juistheid en de volledigheid van de opgenomen persoonsgegevens te bevorderen (art. 5 lid 2). Deze zorgplicht gaat voor registraties die gehouden worden met het oog op de bedrijfsmatige verstrekking van gegevens aan derden nog verder. Art. 13 lid 2 bepaalt dat slechts persoonsgegevens worden opgenomen die op hun juistheid zijn onderzocht. Dit betekent overigens niet, aldus de Memorie van Toelichting, dat de houder voor de juistheid van de gegevens behoeft in te staan.

Art. 8 legt op de houder de verplichting te zorgen voor voorzieningen van technische en organisatorische aard ter beveiliging van de registratie. Indien in strijd met de voorschriften van de WPR ter bescherming van de belangen van geregistreerden wordt gehandeld waardoor iemand schade lijdt, is in art. 9 van de WPR de mogelijkheid gecreëerd de houder (alsmede de bewerker voor zover ontstaan door zijn werkzaamheid) voor zowel materiële als immateriële schade aansprakelijk te stellen. Op grond van art. 10 is het mogelijk bij de rechter te vorderen dat gedrag te verbieden, en maatregelen te treffen om de gevolgen van dat gedrag te herstellen. Het recht om een dergelijke vordering in te stellen wordt ook expliciet toegekend aan belangenorganisaties (zoals consumenten-

organisaties en vakbonden) Daarmee is de zogenoemde ‘class action’ of ‘actio popularis’ in de WPR verankerd.

Paragraaf 7 van de WPR bevat bepalingen die het recht van belanghebbenden op kennisneming en verbetering regelen. Teneinde dit recht te kunnen effectueren is ten behoeve van de geregistreerde in art. 28 een verplichting voor de houder opgenomen om een ieder over wie voor de eerste keer persoonsgegevens in de registratie worden opgenomen, binnen een maand schriftelijk mede te delen dat dit het geval is. De verplichting geldt niet indien de betrokkene weet of redelijkerwijs kan weten dat een dergelijke opname heeft plaatsgevonden.

Op verzoek van een ieder moet de houder binnen een maand meedelen of er hem betreffende persoonsgegevens in de registratie zijn opgenomen, alsmede desgevraagd een volledig overzicht daarvan met inlichtingen over de herkomst verstrekken (art. 29). Eveneens is de houder aan een ieder verplicht mededeling te doen of er in het voorafgaande jaar hem betreffende gegevens aan derden zijn verstrekt, welke gegevens en aan wie (art. 32). Gewichtige belangen van anderen dan de verzoeker, de houder daaronder begrepen, kunnen grond zijn tot weigering (art. 30). Over het recht op verbetering bepaalt art. 31 dat de belanghebbende de houder kan verzoeken hem betreffende persoonsgegevens te verbeteren, aan te vullen of te verwijderen, indien deze feitelijk onjuist zijn of voor het doel van de registratie onvolledig of niet ter zake dienend. Indien de houder niet aan een van deze verzoeken voldoet, kan de geregistreerde zich wenden tot de Registratiekamer of tot de arrondissementsrechtbank.

Paragraaf 3 bestaat uit vier artikelen, die bepalen wanneer verstrekking van gegevens uit een persoonsregistratie aan een derde toelaatbaar is. Onder het verstrekken van gegevens uit een persoonsregistratie verstaat de wet het bekend maken of ter beschikking stellen van persoonsgegevens, voor zover zulks geheel of grotendeels steunt op gegevens die in die persoonsregistratie zijn opgenomen, of door de verwerking daarvan, al dan niet in verband met andere gegevens, zijn verkregen. Onder derden verstaat de wet personen of instanties buiten de organisatie waarover de houder zeggenschap heeft en ten dienste waarvan de registratie wordt gehouden, met uitzondering van de bewerker of de geregistreerde.

Uit een persoonsregistratie mogen slechts gegevens aan een derde worden verstrekt voor zover zulks voortvloeit uit het doel van de registratie, wordt vereist ingevolge een wettelijk voorschrift of geschiedt met toestemming van de geregistreerde (art. 11 lid 1). Indien toestemming van de geregistreerde is vereist, kan deze slechts schriftelijk worden gegeven (art. 12 lid 1).

Art. 13 is van toepassing op persoonsregistraties van waaruit bedrijfsmatig persoonsgegevens, anders dan met toestemming van degenen op wie die

gegevens betrekking hebben, aan derden worden verstrekt. Verstrekking vindt niet plaats, indien a) het doel waarvoor de verstrekking is verzocht, in strijd is met de wet, de openbare orde of de goede zeden; b) de verstrekking redelijkerwijs niet in overeenstemming is met dat doel; of c) door de verstrekking de persoonlijke levenssfeer van de geregistreerde onevenredig zou worden geschaad. Volgens de Memorie van Toelichting ligt in de situatie van interactieve raadpleging in het nemen van een abonnement zowel het verzoek om informatie als het doel waarvoor deze wordt gevraagd besloten.

De Registratiekamer is de instantie die is belast met het toezicht op de werking van de WPR. Houders hebben met de Kamer te maken doordat registraties hier moeten worden aangemeld. Voorts kan aan de Kamer een verklaring omtrent de gedragscode van de branche-organisatie worden gevraagd. Belangrijke bevoegdheden van de Kamer zijn het inwinnen van alle inlichtingen en het toegang hebben tot alle ruimten waar de registratie zich bevindt of toegankelijk is, voor de uitvoering van haar taak. Ook is de Kamer bevoegd apparatuur, programmatuur, boeken en bescheiden te onderzoeken, voor zover dit redelijkerwijs voor de uitoefening van haar taak nodig is. Tenslotte kan de Kamer ambtshalve of op verzoek van een belanghebbende, een belangenorganisatie daaronder begrepen, een onderzoek instellen naar de wijze waarop toepassing wordt gegeven aan de WPR. Indien de bevindingen van de Kamer daartoe aanleiding geven, kan zij aan de houder van de registratie een aanbeveling doen. De Memorie van Toelichting vermeldt dat deze aanbeveling geen rechtsgevolg heeft, doch dat het aan het inzicht van de Kamer wordt overgelaten of aan de aanbeveling openbaarheid wordt gegeven.

11.3 Privacy en de overheid

Onder meer op basis van de voorgeschiedenis bij de tot stand koming van de WPR, wordt wel beweerd dat de overheid weinig privacy-minded is. Het is een feit dat de overheid de grootste inbreukmaker op de persoonlijke levenssfeer is. Is dit voor een deel te verklaren uit de taak van de overheid, niet te ontkennen valt dat de overheid ook overigens weinig belang heeft bij privacybescherming van de burgers. Mensen die de in deze opvatting neergelegde scepsis niet willen delen, wijzen erop dat die overheid - weliswaar na geruime tijd - toch met de WPR is gekomen. Van de andere kant echter, kan evenzogoed beweerd worden dat de overheid diezelfde WPR hard nodig heeft, om inbreuken op de privacy - nu wettelijk gelegitimeerd - te continueren.

Dat niet uitsluitend het nobele grondrecht van ‘bescherming van de persoonlijke levenssfeer’ aan privacywetgeving ten grondslag ligt, werd fijntjes geïllustreerd door een lid van het Britse parlement bij de aanneming van de Data Protection Act 1984. De invoering van deze wet was in een stroom-

versnelling terecht gekomen, toen bleek dat de Zweedse overheid had verboden om de Zweedse ziekenfondskaarten (goedkoper) in Engeland te personaliseren, om wege van het ontbreken van een privacywet aldaar. Het ging met deze wet, aldus het parlementslid kennelijk niet om privacy, maar om geld. Evenzo, blijkt uit de preambules, zijn de OESO-richtlijnen en het Verdrag van Straatsburg opgesteld, juist om persoonsgegevenstransport over de landgrenzen heen niet meer te kunnen beperken met een beroep op het ontbreken van privacybescherming. De achterliggende gedachte is dat indien niet een minimum aan privacybeschermende regels wordt neergelegd, burgers in toenemende mate minder bereid zullen zijn hen betreffende persoonsgegevens te verstrekken.

Teneinde enig zicht te krijgen op het gedrag van de overheid in dit soort zaken, zullen we kort stilstaan bij een aantal hiermee verband houdende wetgevende initiatieven: koppeling van bestanden en het sofinummer (11.3.1), de beperkte legitimatieplicht (11.3.2) en koppeling en fraudebestrijding (11.3.3). In paragraaf 11.3.4 wordt een aanzet gegeven voor een aanwending van overheidsautomatisering die minder uitgaat van repressie en meer van dienstverlening.

11.3.1 Koppeling van bestanden en het sofinummer

Hiervoor (in hoofdstuk 10) is de ontwikkeling van het fiscaal nummer tot sociaal-fiscaal-GBA-nummer reeds gememoreerd. Uitdrukkelijk werd in de Memorie van Toelichting bij de invoering van het fiscaal nummer gesteld dat het nummer uitsluitend intern door de fiscus gebruikt zou worden. Welnu, het duurde niet lang of de kring van betrokkenen werd uitgebreid van belastingbetalers tot verzekerden ingevolge de werknemersverzekeringen en uitkeringsgerechtigden ingevolge de sociale verzekeringswetgeving. Maar niet ‘slechts’ fiscus, uitkeringsinstanties en gemeenten maken gebruik van het sofinummer. Zo’n beetje ieder jaar hebben we kunnen meemaken dat de reikwijdte van het sofinummer groeide, bijvoorbeeld toepassing bij Volkshuisvesting (huursubsidie), de Informatiseringsbank (studiefinanciering), de gemeentelijke sociale diensten en sinds 1995 ook bij de ziekenfondsen. November 1994 lanceerde de Minister van Onderwijs het plan om een onderwijsnummer in te voeren voor eenieder vanaf *vier* jaar. En, jawel, het sofinummer zou daar goed geschikt voor zijn. En thans, met de ontwikkeling van chipkaarten, werkt de Vereniging van Nederlandse Gemeenten aan een ‘burgerservice’-chipkaart, die paspoort en rijbewijs kan vervangen en tevens dienst kan doen bijvoorbeeld als sociale zekerheidspas en ziekenfondskaart.

Dit verschijnsel staat bekend als de ‘salamitactiek’. Ieder jaar een plakje, dat eet de Nederlandse bevolking nog wel. Maar laten we nu eens meters maken, en die worst in één keer naar binnen werken. Leidt een ontwikkeling als deze

over een periode van - zeg eens - 25 tot 50 jaar niet tot een geheel transparante, door de overheid gecontroleerde samenleving? Wat heeft dat voor consequenties voor heden ten dage belangrijke uitgangspunten van rechtstaat en democratie? Is het zo, dat tegen die tijd het hebben van een privéleven als a-sociaal gezien wordt? Zal, bijvoorbeeld, het niet melding maken van het feit dat iemand rookt, aangemerkt worden als fraude, in verband met het te dragen eigen risico in de gezondheidszorg? Niet-rokers hebben daar wellicht een andere opvatting over dan rokers. Maar wat doen we nog meer ? Eten we wel gezond, kunnen we tegen 'spanningen' en - straks kan dat in de biochemie - zijn onze genen wel gezond? Ja, het moet wel raar lopen, wil zo'n worst dan niet een heel onaangename smaak krijgen.

11.3.2 Beperkte legitimatieplicht

Sinds 1 juni 1994 kennen we de zogeheten 'beperkte legitimatieplicht', ingevolge de invoering van de Wet op de Identificatieplicht (WID). De legitimatieplicht is beperkt, omdat die nu nog geldt ter legitimatie

a) in het openbaar vervoer, teneinde zwartrijden te bestrijden;
b) in en rond voetbalstadions, teneinde voetbalvandalisme tegen te gaan;
c) op het werk, teneinde illegaal verblijvende buitenlanders te kunnen opsporen.

De vraag die in dit verband gesteld moet worden is die naar de proportionaliteit. Is de maatregel geschikt, en evenredig in verhouding tot het nagestreefde doel? Een vooropmerking is dat we, gelet op de salamitactiek, aan het bijvoeglijk naamwoord 'beperkte' maar een beperkt gewicht moeten toekennen. Te verwachten is, indien deze wet blijft, dat het beperkte tezijnertijd wel zal vervallen.

Andere kritiek is dat deze wet helemaal niet dienstig is aan de beoogde doeleinden, terwijl we wel allemaal met een verplichting worden opgezadeld. Zo valt allerminst aan te nemen dat de categorie notoire zwartrijders daar nu ineens van gaat afzien, omdat zij zich in het vervolg moet legitimeren. Het bestrijden van het voetbalvandalisme door middel van een pasjessysteem is in eerste instantie een kwestie van de betreffende verenigingen. En uit invallen bij ondernemingen waarvan het vermoeden bestond dat er illegaal in Nederland verblijvende buitenlanders werkten, is niet gebleken dat dit middel effectief is. Een vraag die ook gesteld dient te worden is, of deze wet niet juist ongewenste gevolgen creëert. Het is niet gewaagd om te beweren dat bij de uitgifte van de eerste persoonsbewijzen aan legaal in Nederland verblijvende buitenlanders de nodige 'illegalen' 'gelegaliseerd' zijn. Voorts lijkt de handel in valse persoonsbewijzen bij uitstek lucratief voor de 'georganiseerde misdaad', een contra-effect waarvoor ook het toenmalig hoofd van de Binnenlandse

Veiligheidsdienst heeft gewaarschuwd. Wat de wet overigens wel bevordert is een voedingsbodem voor discriminatie. Want zo moeilijk is het toch niet te voorspellen wie de controleur het eerst om zijn legitimatie zal vragen.

Nu moet men zich natuurlijk wel afvragen waarom de overheid, ondanks de kritiek, niettemin besloten heeft tot invoering van deze wet. De ratio daarvan kan worden gevonden in de suggestie die daarvan uitgaat, dat zwartrijders, voetbalvandalen en illegalen 'keihard' worden aangepakt. Waar de overheid met echte maatregelen achterwege blijft, of de problematiek niet kan beheersen, is er behoefte aan een fopspeen. Maar wel een, die niet in het belang van de doorsnee burger is. Het argument dat een beschaafd land het toch niet zonder legitimatieplicht kan stellen, waarbij gewezen wordt op de ons omringende landen, kan evenmin overtuigen, als we ons bedenken dat het in Canada zelfs niet vereist is om een pasfoto op het rijbewijs te hebben.

11.3.3 Koppeling en fraudebestrijding

In de WPR is geen expliciete aandacht voor het koppelen van bestanden. Dit betekent dat we ons voor de al dan niet toelaatbaarheid van het koppelen van bestanden moeten baseren op hetgeen over verstrekken van gegevens (aan een derde) is opgenomen. Onder verstrekken van gegevens verstaat de wet het bekend maken of ter beschikking stellen van gegevens. Op grond van art. 11 lid 1 mogen gegevens slechts aan derden worden verstrekt voor zover zulks voortvloeit uit het doel van de registratie, wordt vereist ingevolge een wettelijk voorschrift of geschiedt met toestemming van de geregistreerde.

Het koppelen van bestanden kan worden beschreven als de activiteit waarbij gegevens, afkomstig uit verschillende bestanden, naast elkaar worden gelegd en met elkaar worden vergeleken. Teneinde deze activiteit zinvol te kunnen verrichten, is het nodig een unieke ingang te hebben op recordniveau. Dit kan zijn de achternaam, in combinatie met voorletters, geboortedatum en/of adres van de geregistreerde. Tengevolge van invoerfouten en/of onjuiste adresgegevens is een dergelijke ingang in de praktijk niet altijd effectief. Gelet op de situatie dat steeds meer overheidsinstellingen het sofinummer gebruiken, ligt het voor de hand dit nummer bij de koppeling van bestanden als unieke ingang te hanteren.

Het vergelijken van gegevens uit verschillende bestanden kan op verschillende manieren. De ene instantie kan bijvoorbeeld aan de andere instantie het verzoek doen over een met naam (en nummer) genoemde persoon bepaalde inlichtingen te verschaffen, met het oog op de uitoefening van een bij de wet verleende taak en bevoegdheid. Denkbaar is ook, dat de ene instantie de andere een toegangsfaciliteit tot het gegevensbestand verleent, zodanig dat die instantie zelf rechtstreeks het gegevensbestand kan raadplegen. Voorts is denkbaar dat gegevensvergelijking automatisch wordt uitgevoerd door middel

van een computerprogramma, hetwelk de records, al dan niet op grond van bepaalde selectiecriteria, met elkaar vergelijkt, op grond van een of meer ingegeven parameters.

Het moge duidelijk zijn, dat in het eerstgegeven voorbeeld geen twijfel kan bestaan aan de legitimiteit van een dergelijk verzoek, voor zover de andere instantie krachtens de wet gehouden is tot de verstrekking van die gegevens. Gelet op de omschrijving in de wet van de term 'houder', kan in het algemeen niet gesteld worden dat 'de overheid' houder is van de verschillende bestanden, zodat er geen sprake zou zijn van derdenverstrekking. Iedere instantie op zich, of zelfs een bepaald dienstonderdeel, moet worden aangemerkt als houder. Gegevensverstrekking als in dit voorbeeld bedoeld, past evenwel moeiteloos onder de bepaling van art. 11 lid1.

Bij de andere twee voorbeelden is dit niet zonder meer het geval. Zo kan men het verzoek tot toegang tot een registratie (door middel van een terminal) niet gelijk stellen aan een verzoek om inlichtingen. Daarvoor is het gebruik van de terminal onvoldoende bepaald, noch op individueel niveau, noch naar de hoedanigheid van de gegevens. Gelet op de mogelijkheid bepaalde velden uit het gegevensbestand af te schermen, lijkt dit laatste minder problematisch dan het eerste. Voorts bestaat het risico dat gegevens worden geraadpleegd en gebruikt voor een ander doel dan die waarvoor de wettelijke bevoegdheid was verleend.

De geautomatiseerde vergelijking van alle records en alle velden uit twee of meer bestanden vormt verreweg de grootste inbreuk op de bescherming van persoonsgegevens en dientengevolge op de (informationele) persoonlijke levenssfeer van de geregistreerden. Het geeft instanties de mogelijkheid tot het creëren van zogenoemde 'totaalprofielen'; er ontstaat een totaalbeeld van de geregistreerde dat diens levenswandel transparant maakt. Ook in dit geval is het zeer de vraag of een dergelijke vorm van inlichtingenverstrekking gelegitimeerd kan worden door de betrekkelijke wettelijke bevoegdheid in combinatie met art. 11 lid 1. Feit is, dat van een belangenafweging op individueel niveau geen sprake is. Dit aspect blijft meespelen, ook indien men ertoe zou overgaan niet op alle records en alle velden te vergelijken. Daarbij zal in zo'n situatie selectie toch steeds plaats hebben op een vooraf opgesteld profiel van kenmerken, dat niet altijd in het individuele geval van toepassing hoeft te zijn.

Het vraagstuk van het koppelen van bestanden wordt onvoldoende bestreken door de WPR. Bij de vraag naar de wenselijkheid en toelaatbaarheid van het instrument van bestandsvergelijking, moet een afweging plaats vinden tussen doelmatigheid en privacybescherming. Uit uitspraken van de vorige Minister van Justitie blijkt dat we wat die afweging betreft de nodige reserves dienen te hebben voor zover de overheid daarin partij is. Privacy is mooi, maar moet geen alibi worden voor fraude, aldus de minister. Ook meent hij dat privacy wel is aan te duiden, maar nauwelijks valt te definiëren. Hij wijst

op het dynamisch karakter daarvan. Op grond van de public choice theorie is het niet moeilijk te voorspellen in welke richting de afweging tussen privacybescherming en fraudebestrijding dan zal evolueren. De public choice theorie gaat uit van de veronderstelling dat politici en ambtenaren zich bij het nemen van beslissingen niet zozeer laten leiden door overwegingen met betrekking tot het algemeen belang, doch vooral door hetgeen dienstig kan zijn aan de uitvoering van de hen toebedeelde taak. En dan spreekt het voor zich dat een onbelemmerde toegang tot allerlei informatie in het belang is van diegenen die met de uitvoering (en opsporing) van regelgeving zijn belast. Het grondrecht van privacybescherming is echter regel; inbreuken daarop moeten uitzonderingen zijn. Het wijzen op fraude is op zichzelf geen legitimatie voor een dergelijke uitzondering, maar eerder een procedure om in aanmerking te komen voor een vrijbrief om de persoonlijke levenssfeer te schenden.

Over de effectiviteit van koppelingen, de vraag of bestandsvergelijking een doeltreffend en kosteneffectief middel is, bestaat evenmin duidelijkheid. De teneur is wel dat koppeling in de praktijk reuze tegenvalt. Bestanden zijn vaak verouderd, of voor het doel onvolledig, zodat toch weer elders (bij de werkgever bijvoorbeeld) inlichtingen moeten worden ingewonnen. Een ander probleem is dat instanties niet dezelfde software gebruiken, zodat ook om die reden gegevens niet snel verwerkt kunnen worden. Een bezwaar van een andere orde is, dat bestrijding van fraude en criminaliteit weliswaar nuttig is, maar niet door middel van een technisch-administratieve oplossing te zoeken voor maatschappelijke problemen.

11.3.4 Aanwending van overheidsautomatisering: een nieuwe richting

De richting waarin overheidsfunctionarissen nadenken over de inzetbaarheid van geautomatiseerde systemen is dringend aan herziening toe. Uitgangspunt blijkt vooral een repressief gebruik. De tegenreactie hierop is voorspelbaar. Burgers worden alleen maar uitgedaagd nieuwe uitwegen te zoeken, hetgeen leidt tot burgerlijke ongehoorzaamheid en het verschijnsel van de calculerende burger. Het lijkt wel of het gaat om de overheid tégen de burger en andersom. In dit verband lijkt de term ‘calculerende overheid’ evenzeer op zijn plaats. Het is een pad waarvan weinig anders is te verwachten dan geldverspilling, ineffectiviteit en wederzijdse achterdocht, hetgeen bovendien gepaard gaat met steeds verdergaande inbreuken op normen, waarborgen en vrijheden. Zelfs in situaties waar automatiseringssystemen worden ingevoerd onder het mom van betere service, blijkt dat de harde kern toch is verhoging van de ‘pakkans’.

Het wordt hoog tijd dat de overheid inziet dat overheidsautomatisering moet worden aangewend ten dienste van de burgers. Het gaat niet aan de mogelijkheden van computers slechts te benutten tegen ‘verdachte’ burgers;

belangrijker is of ze kunnen worden gebruikt voor de vraag of er wellicht iemand is tekort gedaan. Zo maakt de fiscus gebruik van profielen van belastingbetalers, teneinde belastingfraudeurs te kunnen opsporen. Is het dan niet net zo goed mogelijk profielen samen te stellen om na te gaan of belastingbetalers geen aftrekposten zijn vergeten? Of ze wel voldoende huursubsidie krijgen? Of de kinderbijslag en de studiefinanciering wel klopt?

De verzorgingsstaat biedt voorzieningen aan hen die dat nodig hebben. Bij een beroep op een voorziening is het legitiem dat wordt gecontroleerd of men terecht een beroep daarop doet. De in beginsel verruimde controlemogelijkheden tengevolge van de automatisering worden toegepast zonder dat daar een belangenafweging op individueel niveau aan ten grondslag heeft gelegen en zonder dat daarvoor speciale wettelijke waarborgen zijn neergelegd. De balans tussen de bescherming van de persoonlijke levenssfeer en de fraudebestrijding is doorgeslagen naar de laatste. Wat nodig lijkt, is een heroriëntatie op privacy en verzorgingsstaat. Het eenzijdig gebruik van geautomatiseerde controlesystemen gaat geheel voorbij aan de normstelling van de privacybescherming. Een 'contactambtenaar', die als intermediair fungeert tussen 'zorgverlening' en zorgafnemer en uit dien hoofde - als enige - de beschikking heeft over de relevante gegevens die zich onder de verschillende instanties bevindt, is een alternatief dat betere privacywaarborgen in zich draagt dan wanneer alle instanties over en weer over zo goed als alle gegevens van betrokkenen gaan beschikken.

De basis van de verzorgingsstaat is solidariteit. Solidariteit is onontbeerlijk voor een beschaafde en ontwikkelde samenleving. Zonder solidariteit wordt een samenleving een jungle, waarin ieder voor zich tracht er zo goed mogelijk uit te springen. Misbruik van sociale voorzieningen knaagt aan de wortels van solidariteit. Ontzuiling en de calculerende burger zijn verschijnselen van een afnemende solidariteit. Anders dan met het nemen van niet-efficiënte maatregelen, zoals sofinummers, identificatieplicht en bestandskoppelingen, met repressieve werking, ligt er voor de overheid de belangrijke taak met maatregelen juist solidariteit te bewaren en te herstellen. Dat betekent in ieder geval niet het rigide toepassen van automatiseringssystemen. Evenmin kan men stellen dat onder de toenemende individualisering burgers gelijke behoeften, wensen of interesses hebben. In tegenstelling tot de gedachte dat automatiseringssystemen vragen om uniformering van wet- en regelgeving en het categoriseren van de data-objecten (in dit geval geregistreerde burgers), ligt de kracht van moderne automatiseringssystemen nu juist hierin, dat met een keur aan nuanceringen en verfijningen rekening gehouden kan worden. De conclusie is dat overheidsautomatisering dient te worden aangewend ten dienste van de burgers, en wel zodanig dat daarin onderkend wordt dat wij niet allemaal hetzelfde zijn. De nieuwe solidariteit zal hieruit moeten bestaan, dat niet iedereen hetzelfde krijgt, maar iedereen het zijne. Het gelijkheidsbeginsel wil niet zeggen dat iedereen gelijk moet worden behandeld, maar

moet aldus worden begrepen dat eenieder gelijk in zijn ongelijkheid wordt tegemoet getreden. Een overheid die in woord en gedrag hiernaar handelt, neemt bij de burgers de vrees weg dat anderen meer dan zij bevoordeeld zullen worden (bijvoorbeeld omdat die anderen handiger zijn in het om de tuin leiden van de overheid) en herstelt daarmee de basis om burgers aan te spreken op hun onderlinge solidariteit alsmede de bereidheid van hen deze op te brengen. In een rechtstaat is dat het uitgangspunt in de verhouding tussen overheid en burgers.

11.4 Jurisprudentie

AMBTENARENGERECHT AMSTERDAM, 28 JULI 1989, WICHERS HOETH - GEMEENTERAAD AMSTERDAM, CR 1989/5

Tussen partijen is in confesso dat de gemeente in strijd heeft gehandeld met de Privacyverordening door de hiervoor omschreven persoonsgegevens over te dragen aan de OHRA UA, zulks buiten medeweten van en zonder toestemming van de betrokkenen.

RB AMSTERDAM, K.G. 14 DECEMBER 1989, ONDERNEMINGSRAAD ptt TELECOM - ptt TELECOM, CR 1990/2

Meetgegevens arbeidsprestaties telefonistes inlichtingen buitenlandse telefoonnummers. Voorbij wordt gegaan aan de vraag of Telecom in strijd handelt met enige bepaling van de Wet op de Ondernemingsraden of van de Arbeidsomstandighedenwet dan wel onvoldoende behoedzaam omgaat met het recht van haar personeel op bescherming van hun privacy. Voldoende grondslag is dat Telecom zich tegenover haar personeel niet gedraagt als een goed werkgever als bedoeld in art. 1638z BW.

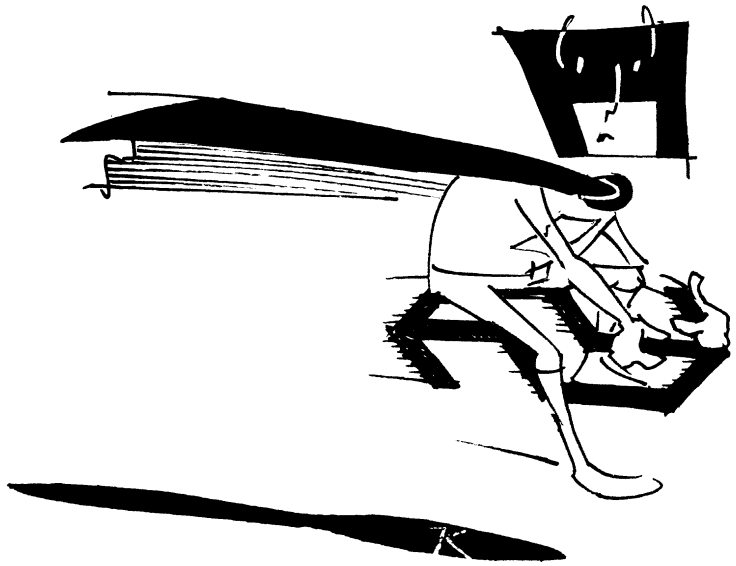
HOF AMSTERDAM, 21 JANUARI 1993, nj 1994, 556

Verzoek om houdster van een persoonsregistratie te bevelen mededeling te doen van in de registratie opgenomen gegevens en deze te verwijderen. Schadevergoeding respectievelijk van houdster en van verzoeker te verlangen? Proceskosten.

11.5 Literatuur

- Graaf, F. de, ‘Rechtsbescherming van persoonlijkheid, privéleven, persoonsgegevens’, (diss.), H.D. Tjeenk Willink, Alphen aan den Rijn, 1977.
- Graaf, F. de, ‘De wet persoonsregistraties’, Vermande, Lelystad, 1986.

- Holvast, J., ‘Persoonsgegevens of niet: dat is de vraag’, ITER 2, Samsom, Alphen aan den Rijn, 1996.
- Kuitenbrouwer, F., ‘Het recht om met rust gelaten te worden’, Uitgeverij Balans, Amsterdam, 1991.
- Overkleeft-Verburg, G., ‘De Wet Persoonsregistraties, Norm, toepassing en evaluatie’, (diss.), W.E.J. Tjeenk Willink, Zwolle, 1995.
- Prins, J.E.J. e.a., ‘In het licht van de Wet Persoonsregistraties: Zon, maan of ster?’, ITER 1, Samsom, Alphen aan den Rijn, 1995.



12 Grensoverschrijdend gegevensverkeer

Onder grensoverschrijdend gegevensverkeer wordt verstaan het transport van gegevens over de landsgrenzen heen. Dat kan zijn de verzending van gegevens naar het buitenland, de toegang tot gegevens vanuit het buitenland en de toegang tot gegevens in het buitenland. Vanzelfsprekend wordt de belangstelling voor grensoverschrijdend gegevensverkeer voor een belangrijk deel ingegeven door de mogelijkheden die de technologie daartoe biedt. Hierbij valt te denken aan geautomatiseerde gegevensverwerking en -distributie (datacommunicatie tussen computers) en bijvoorbeeld aan grensoverschrijdende omroep. De gebruikte infrastructuur kan het openbare telefoonnet zijn, het telexnet of de datanetten, maar ook telecommunicatiesatellieten of omroepsatellieten. Grensoverschrijdend gegevensverkeer is echter niet beperkt tot deze vormen van *elektronische* gegevensuitwisseling. De wijze van transport of de daarbij gebruikte gegevensdrager zijn daarvoor niet beslissend. Evenmin is grensoverschrijdend gegevensverkeer beperkt tot het transport via 'openbare' communicatiekanalen. Het aantal internationale grensoverschrijdende (besloten) netwerken loopt in de honderden. De OESO 'Richtlijnen voor de bescherming van het privéleven en grensoverschrijdend verkeer van persoonsgegevens' (1980) en het 'Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens' (1981) van de Raad van Europa bepalen zich met name op *persoons-*

gegevens. De uitwisseling van persoonsgegevens maakt weliswaar een belangrijk onderdeel uit van het internationale gegevenstransport, doch de term 'grensoverschrijdend gegevensverkeer' is niet gereserveerd voor alleen persoonsgegevens. De aard van de gegevens is velerlei.

Een bespreking van het onderwerp grensoverschrijdend gegevensverkeer aan de hand van de *aard* van de gegevens - persoonsgegevens, financiële gegevens of transport begeleidende goederengegevens bijvoorbeeld - is ondoenlijk. Niet alleen is de indeling ofwel te grof dan wel haast onuitputtelijk, een indeling naar de aard van gegevens biedt ook nauwelijks eenduidige juridisch relevante aanknopingspunten. Een indeling naar de *wijze van transport* is evenmin zinvol. Zoals hierboven gesteld, is de wijze van transport niet van belang. Financiële gegevens bijvoorbeeld kunnen via datacommunicatie getransporteerd worden, maar ook op magneetbanden of als jaarverslag in de aktentas. Een indeling naar het *gebruik* van de gegevens tenslotte, bijvoorbeeld voor commerciële doeleinden, bancair verkeer of belastingen, of naar de *gebruikers* van de gegevens, heeft als nadeel dat de categorie-indeling tamelijk arbitrair zal zijn, terwijl regels van onderscheidenlijke rechtsgebieden door elkaar heen lopen, hetgeen niet bevorderlijk is voor de samenhang. Zoals met veel onderwerpen uit het informaticarecht is ook ten aanzien van grensoverschrijdend gegevensverkeer een samenhangende bespreking een lastige opgave. Als we echter kijken naar wat het denken over grensoverschrijdend gegevensverkeer heeft beïnvloed, is er wel een aantal belangen te onderscheiden. De opzet van dit hoofdstuk is om aan de hand van enkele algemene aspecten van grensoverschrijdend gegevensverkeer de daarmee gepaard gaande *belangen* in kaart te brengen, alsmede de daaruit voortvloeiende behoefte aan regulering. Hieraan vooraf gaat een inleiding over de aard en omvang van grensoverschrijdend gegevensverkeer. Besloten wordt met een oriëntatie op de internationale consequenties en regelgeving van grensoverschrijdend gegevensverkeer.

12.1 Aard en omvang van grensoverschrijdend gegevensverkeer

Internationaal gegevenstransport is schier onuitputtelijk. Dit betreft zowel de soort van gegevens, de doeleinden als de omvang. Gegevenstransport vindt op grote schaal plaats in zowel de private sector als in de publieke sector, een onderscheid dat later nog van belang blijkt met het oog op de reikwijdte van het begrip 'free flow of information'. Enkele voorbeelden uit de private sector zijn: handelsinformatie over bedrijven, goederentransport, verzekeringen, reserveringsgegevens van hotelketens en luchtvaartmaatschappijen, researchresultaten van onderzoekcentra, toerisme, financiële concerngegevens, bancair verkeer, beurskoersen, valutatransacties, en computersoftware. In de publieke sector vindt gegevensuitwisseling plaats met betrekking tot bijvoor-

beeld sociale verzekeringen, belastingen, politieregistraties, vreemdelingencontrole, vluchtelingen en statistiek.

In 1984 is door KMG Klynveld Kraayenhof & Co een onderzoek verricht naar de aard en omvang van grensoverschrijdend gegevensverkeer onder het Nederlandse bedrijfsleven. Waar de cijfers daaruit niet meer representatief zullen zijn voor de huidige omvang van dit verkeer, geldt dit waarschijnlijk minder voor de conclusies. Uit het onderzoek kwamen als belangrijkste motieven voor internationaal gegevensverkeer naar voren: snelle beschikbaarheid van informatie, financiële verslaggeving, afdekking van valutarisico's en kostenbesparing.

De *omvang* van het gegevenstransport bedroeg onder de respondenten destijds al gemiddeld 31 megabytes per bedrijf per dag aan export en gemiddeld 19 megabytes per bedrijf per dag aan import. Een kwart van de getransporteerde gegevens betrof gegevens omtrent personen. Van de respondenten verwachtten 90% een toename in het grensoverschrijdend gegevensverkeer. De belangrijkste oorzaken die daarvoor werden genoemd: technologische ontwikkelingen van de automatisering, organisatorische eisen, bedrijfsomvang en de 'depapierisering' van de maatschappij.

12.1.1 Algemene aspecten

Om uiteenlopende redenen, variërend van privacybescherming tot gegevensprotectionisme, is er vanaf 1970 een tendens ontstaan tot regulering van gegevensstromen. Daarvoor is een aantal oorzaken aan te wijzen:

De ontwikkelingen op het gebied van telecommunicatie en informatica, ook wel telematica genoemd, maken gegevenstransport over grenzen mogelijk in een enorme omvang, zonder dat enige controle op de inhoud plaats vindt.

Grensoverschrijdend *persoons*gegevensverkeer kan een aantasting van de persoonlijke levenssfeer tot gevolg hebben. Als het in het eigen land al vaak ondoenlijk is voor geregistreerden om inzicht te verkrijgen in welke registraties, en met welke doeleinden, men is opgenomen, dan is het aannemelijk dat deze problematiek alleen maar ondoorzichtiger zal worden als ook registraties in het buitenland daarin worden betrokken. Zo heeft de Zweedse overheid (een van de eerste landen met een privacywetgeving) in 1973 haar toestemming onthouden aan Siemens om personeelsgegevens van Siemens-werknemers in Zweden centraal te registreren in de Bondsrepubliek, bij gebreke van een adequate privacywetgeving.

Gegevensverwerking in het buitenland kan een bedreiging vormen voor de nationale soevereiniteit. Informatie is een belangrijke hulpbron. Het afsluiten van voor het betreffende land vitale informatie maakt inbreuk op het zelfbeschikkingsrecht van de staat.

Een volgende oorzaak voor de tendens tot regulering van gegevenstransport is de betekenis daarvan voor de staatsveiligheid. In dit verband moet niet alleen gedacht worden aan het over de grens brengen van (geheime) strategische informatie, maar bijvoorbeeld ook aan spionage en zelfs sabotage op afstand. Telecommunicatiesatellieten maken het mogelijk continu en nauwkeurig het grondgebied van andere mogendheden af te tasten, zodat informatie beschikbaar komt over troepenstationeringen en militaire opslagplaatsen. Ook de bouw van energiecentrales en telecommunicatie-infrastructuurvoorzieningen kan gevolgd worden.

Gegevenstransport en telecommunicatie zorgen voor een toenemende slagvaardigheid bij het internationale bedrijfsleven. De vrees ontstaat dat internationaal opererende bedrijven beslissingen kunnen nemen met economische, politieke en sociale gevolgen voor een land. Financiële hoofdvestigingen bijvoorbeeld zijn niet meer nationaal gebonden.

Het belang van vrije gegevensverwerking kan een vlucht naar zogenaamde 'dataparadijzen' veroorzaken. Onder dataparadijzen moeten we landen verstaan zonder of met geringe regelgeving op het gebied van gegevensverwerking, waardoor het aantrekkelijk kan zijn voor bedrijven om in zo'n land hun gegevens te verwerken.

Ook het economisch belang van informatie kan als belangrijke oorzaak voor regulering van grensoverschrijdende gegevensstromen worden aangewezen. Steeds vaker neigen organisaties er toe hun gegevensverwerking daar te laten plaats vinden waar dat het goedkoopst is, of waar de beste technologie ter beschikking staat. Deze tendens kan voor gegevens-exporterende landen de ontwikkeling van een eigen telematica-industrie afremmen.

Als laatste wordt nog gewezen op de onevenredige verdeling van de kennis van geautomatiseerde gegevensverwerking en de beschikbaarheid van geautomatiseerde systemen. Ontwikkelingslanden hebben een aanzienlijke achterstand op het gebied van telematica. Het aantal in werking zijnde systemen per hoofd van de bevolking is in Afrika, Azië en Zuid-Amerika tientallen malen en in sommige landen zelfs honderden malen kleiner dan in Noord-Amerika en West-Europa. Dit leidt tot het verschijnsel dat ontwikkelingslanden de geringe verwerking en gegevensopslag die zij hebben volledig afschermen voor de invloed van Westerse landen. Dit verschil bestaat overigens niet alleen in de relatie 'Noord-Zuid'. Ook bij de Canadese overheid bijvoorbeeld bestaat er ongenoegen over de mate van afhankelijkheid van de Verenigde Staten ten aanzien van de gegevensverwerking

Het zal duidelijk zijn dat een aantal van deze aspecten met elkaar in verband staan. Het verbod van (wederom) de Zweedse overheid aan het ziekenfonds, vanwege het privacyrisico voor de Zweedse burgers, om de verwerking van gepersonaliseerde plastic kaartjes in Engeland te laten geschieden is hiervoor kenmerkend. Het is aannemelijk dat de aanvankelijke keuze van het zieken-

fonds voor verwerking in het buitenland gebaseerd is op economische motieven. Het verbod daarvan door de Zweedse overheid vindt plaats met een beroep op privacyaspecten. Het onmiskenbare gevolg is echter dat de verwerking vervolgens in Zweden plaats zal hebben, hetgeen van invloed is op de werkgelegenheidssituatie in Zweden en op de ontwikkeling van informatietechnologie. De daaropvolgende invoering door Engeland van de Dataprotection Act tenslotte, kan in relatie gebracht worden met de economische belangen verbonden aan een adequate privacybescherming, en raakt aan de kwestie van de nationale soevereiniteit.

12.1.2 Belangen

Uit bovenstaande opsomming blijkt dat bij grensoverschrijdend gegevensverkeer tenminste de volgende belangen in het geding kunnen zijn:

- Belangen van individuen, met name op het gebied van de persoonlijke levenssfeer;
- (Commerciële) belangen van ondernemingen;
- Het belang van de staat, ook wel uitgedrukt als staatssoevereiniteit of als 'privacy van de staat'.

Bovendien is er de 'Noord-Zuid' component, waarbij wel de term 'informatieproletariaat' wordt gehanteerd, als gevolg van de vergroting van de kloof tussen de informatietechnologie-landen en de ontwikkelingslanden.

Informatie is tegenwoordig een belangrijk economisch goed. Het grensoverschrijdend karakter stelt een tegenstelling aan de orde die voor een ongewenst effect kan zorgen. De hierboven genoemde algemene aspecten veroorzaken een tendens naar gegevensprotectionisme. Het is de vraag of dit wel verenigbaar is met het op art. 10 EVRM en art. 19 BuPo gebaseerd recht op informatievrijheid, ook wel aangeduid als de 'free flow of information'. Een tweede aspect met betrekking tot de free flow of information is het in het EU-verdrag neergelegde uitgangspunt van een interstatelijk vrij verkeer van personen en goederen. Ook in onze relaties met belangrijke handelspartners uit niet-EU landen, zoals de Verenigde Staten en Japan, speelt het vermijden van handelsbarrières een belangrijke rol. Een ongewenst effect is dat gegevensprotectionisme een te trage groei van grensoverschrijdend gegevensverkeer tot gevolg heeft.

12.2 Gegevensbescherming

Een meer neutrale term voor gegevensprotectionisme is gegevensbescherming. Protectionisme wordt veelal geassocieerd met het veilig stellen van handelsbelangen. De Engelse term 'dataprotection' is in dit opzicht eveneens minder determinerend. Gegevensbescherming brengt restricties aan in het vrije (grensoverschrijdende) gegevensverkeer. Deze restricties kunnen ten doel hebben gegevens in het eigen land te verwerken, te verkopen of te transporteren, maar kunnen ook de bescherming van de persoonlijke levenssfeer van geregistreerden of het staatsbelang op het oog hebben. De sinds het begin van de zeventiger jaren in verschillende staten tot stand gekomen wetgeving op dit gebied toont aan dat gegevensbescherming alle hierboven onderscheiden belangen kan dienen.

WETGEVING OP HET GEBIED VAN DE TELECOMMUNICATIE

Vooral de laatste jaren is de telecommunicatie-wetgeving in beweging. Een voorname reden hiervoor is de noodzaak tot internationale standaardisering, om een internationale infrastructuur te garanderen. Het belangrijkste overlegorgaan hiervoor is de ITU, de Internationale Telecommunicatie Unie.

Een tweede aspect is de liberalisering van de telecommunicatiemarkt. Per 1 januari 1989 is de monopoliesituatie voor de Nederlandse PTT met betrekking tot de levering van telecommunicatie-randapparatuur (bedrijfstelefooncentrales en telefoontoestellen) opgeheven. Enerzijds vloeit dit voort uit de EU-wetgeving op het gebied van de mededinging, doch anderzijds speelt hier ook de opvatting dat de verzorging van telecommunicatievoorzieningen door slechts één leverancier een remmende werking op de ontwikkeling en toepassing van nieuwe technologie zou hebben. Nadat in 1996 al concurrentie mogelijk is geworden op het gebied van mobiele telefonie, zal per juli 1997 het monopolie op spraaktelefonie helemaal zijn vervallen.

Daarentegen bestaat in Brazilië bijvoorbeeld de verplichting om lokaal geproduceerde systemen aan te schaffen. Ook bestaat er een verbod op gegevensverwerking in het buitenland en op het raadplegen van economische databanken in het buitenland, als deze voorzieningen ook in Brazilië kunnen worden opgebouwd.

BELASTINGWETGEVING

Informatie als economisch goed heeft een waarde in het economisch verkeer, en kan dus object voor het heffen van belastingen vormen. Onder invloed van het toenemende internet-dataverkeer wordt wel de mogelijkheid van een 'bit-tax' geopperd, te berekenen over de intensiteit van elektronische gegevensoverdracht. In Brazilië is de export van informatie-diensten belast.

DOUANE

Bij een verordening uit 1985 heeft de EU bepaald dat de bepaling van de douanewaarde van ingevoerde informatiedragers die gegevens of instructies bevatten, bestemd voor gebruik in gegevensverwerkende apparatuur (software), wordt gebaseerd op de waarde van de gegevensdrager. De voorheen gehanteerde transactionele waarde van de GATT is losgelaten, omdat, volgens de EU, deze handelwijze zal kunnen bijdragen tot een harmonische ontwikkeling van de wereldhandel.

De inventiviteit van de fiscus is overigens groot. In het geval er geen *invoerrechten* op geïmporteerde software verschuldigd is, kan de fiscus de betreffende software aanmerken als een 'dienst' welke in Nederland is verricht, zodat daarover *BTW* verschuldigd is.

In Brazilië overigens overweegt men om de 'interdata' gateway als volwaardig douanekantoor te laten functioneren. (Een gateway kan beschouwd worden als een toegangspoort tot de nationale telecommunicatie-infrastructuur, en kan worden gebruikt voor controle op de invoer en uitvoer van gegevens.)

EXPORTVERGUNNINGEN

De export van informatietechnologie kan aan vergunningen gebonden worden, om te voorkomen dat bepaalde, geavanceerde technologie ter beschikking komt van niet-bevriende naties. Een voorbeeld daarvan is de US Export Administration Act. Hoe ver de opstelling van de Verenigde Staten, toch algemeen gezien als de voorvechter van de vrije wereldhandel, kan gaan, blijkt uit een voorval eind tachtiger jaren. De Amerikaanse overheid gaf opdracht aan Dresser om de vestiging in Frankrijk de toegang tot computerfaciliteiten te onthouden, teneinde te bewerkstelligen dat de Franse vestiging geen medewerking kon verlenen aan de aanleg van de aardgaspijpleiding in Rusland.

STRAFRECHTELIJKE SANCTIES

Het spreekt voor zich dat overtreding van wettelijke voorschriften, zoals exportvergunningen, douanebepalingen of privacybescherming met strafbedreiging gepaard kan gaan. Ten aanzien van uitingen via internet kan de onduidelijke situatie optreden dat sommige uitingen in het ene land wèl onder strafbepalingen vallen, maar in het andere land weer niet.

BEWARING

Op verschillende plaatsen in de wet kunnen eisen worden opgenomen ten aanzien van de bewaarplicht van elektronisch vastgelegde gegevens. Een voorbeeld in dit verband is de verplichting ingevolge de Wet Persoonsregistraties om gedurende een jaar bij te houden aan welke derden bepaalde persoonsgegevens zijn verstrekt.

De in 1980 geformuleerde OESO-richtlijnen worden algemeen beschouwd als de internationale minimum standaard voor de bescherming van de persoonlijke levenssfeer bij grensoverschrijdend persoonsgegevensverkeer. Zij hebben voor Nederland hun neerslag gekregen in het Verdrag van Straatsburg van de Raad van Europa (1981), door Nederland geratificeerd in 1985, en de hierop gebaseerde Wet Persoonsregistraties (1988). Vanuit de EU is voorts een aantal richtlijnen geïnitieerd met betrekking tot de bescherming van persoonsgegevens (zie paragraaf 11.1.2).

12.2.1 De Wet Persoonsregistraties

Ook de in 1989 in werking getreden Wet Persoonsregistraties (WPR, zie hoofdstuk 11) bevat een internationale paragraaf. Art. 47 verklaart de WPR van toepassing op persoonsregistraties die zich in het buitenland bevinden, maar wel een Nederlandse houder hebben. Persoonsregistraties die zich in Nederland bevinden, maar waarvan de houder in het buitenland is gevestigd, vallen op grond van art. 48 onder de WPR. Beide artikelen bevatten voorzieningen voor de situatie dat op de betreffende registraties ook buitenlandse wetgeving van toepassing is. Art. 49 tenslotte ziet op de toegang vanuit Nederland tot registraties in het buitenland waarop de Nederlandse wet niet van toepassing is. De gebruiker dient de nodige beschermingsmaatregelen te treffen, en ten aanzien van landen waar wetgeving op het gebied van privacybescherming geheel ontbreekt, kan het verboden worden vanuit Nederland gegevens te betrekken uit zich aldaar bevindende registraties.

12.2.2 Te trage groei

Door de mogelijkheden die de hedendaagse technologie daartoe biedt, maakt het grensoverschrijdend gegevensverkeer een onstuimige groei door in volume en in variëteit van toepassingen. Dat deze ontwikkeling door overheden nauwgezet gevolgd wordt, is alleszins begrijpelijk. Maatregelen ter bescherming van de hierboven onderscheiden belangen richten zich meestal op regulering van de *gegevensstromen*, hetgeen een ongewenste beperking van gegevensuitwisseling tot gevolg kan hebben.

Informatie-uitwisseling heeft onmiskenbaar een positief effect op de welvaart en het welzijn van de wereldgemeenschap. Dit geldt zeker voor ontwikkelingslanden. Hierbij kan gedacht worden aan het epidemie-waarschuwingssysteem van de Wereld Gezondheids Organisatie en de overdracht van meteorologische gegevens door de World Meteorological Organisation. Voorts kan de beschikbaarheid over kennis omtrent voedselvoorziening,

bosbouw, veeteelt en de bestrijding van woestijnvorming in belangrijke mate bijdragen tot de ontwikkeling. Een tweede aspect is dat de informatica-technologie ook kansen schept. In diverse ontwikkelingslanden, bijvoorbeeld in India, zien we het ontstaan van software-industrieën. Bovendien kan de gegevensverwerking grote financiële besparingen opleveren.

Op wetgevend gebied staat het grensoverschrijdend gegevensverkeer dan ook internationaal in de belangstelling. Vooral de OESO aanbeveling is ontworpen om het vrije verkeer van informatie tussen de lidstaten te bevorderen. Vanuit het besef dat staten op grond van hun, veelal van elkaar verschillende, privacywetgeving belemmeringen kunnen aanbrengen aan dit verkeer, is er door de OESO een achttal grondbeginselen geformuleerd waaraan nationale wetgeving dient te voldoen, ter bescherming van de persoonlijke levenssfeer. Art. 18 onderstreept nog eens de intentie van de OESO richtlijn, door te stellen dat lidstaten niet *in naam van* de privacy-bescherming het grensoverschrijdend persoonsgegevensverkeer meer dan daarvoor nodig is mogen belemmeren. Het verdrag van de Raad van Europa kiest in de preambule voor het uitgangspunt van evenwicht tussen de bescherming van de persoonlijke levenssfeer en het vrije verkeer van informatie. In art. 12 echter wordt gesteld dat het verkeer van persoonsgegevens naar andere verdragsstaten niet mag worden verboden louter met een beroep op de bescherming van het privéleven, indien de wetgeving van die verdragsstaat gelijkwaardige bescherming biedt (en de gegevens niet bestemd zijn om van daaruit naar een niet-verdragspartij verzonden te worden). Het Verdrag steunt op i) een aantal grondbeginselen terzake van de materiële beschermingsbehoefte, ii) een verbod op beperking van grensoverschrijdend persoonsgegevensverkeer uitsluitend met een beroep op privacybescherming en iii) de verplichting tot bijstand aan buitenlandse betrokkenen voor de uitoefening van hun rechten. Ten aanzien van dit laatste bepaalt art. 16 dat een dergelijk verzoek om bijstand mag worden afgewezen onder meer indien het verzoek onverenigbaar is met de soevereiniteit van de verdragspartij of met rechten van personen van de verdragspartij. Strikte opvatting van dit artikel kan echter tot ongewenste effecten leiden, aangezien het verstrekken van gegevens of informatie over geautomatiseerde systemen in toenemende mate niet in het belang van de staat zal zijn.

12.3 Free flow of information

Art. 10 van de Europese Conventie tot bescherming van de Rechten van de Mens (1950) formuleert het recht op vrijheid van meningsuiting als de vrijheid een mening te koesteren en de vrijheid om inlichtingen of denkbeelden te ontvangen of door te geven. De omvang van dit recht wordt in art. 19 van het Internationaal Verdrag inzake Burgerrechten en Politieke Rechten

(BUPO, 1966) verdiept, in de zin dat ook het vergaren van inlichtingen en denkbeelden hieronder wordt begrepen. In onze grondwet komt dit recht tot uitdrukking in art. 7.

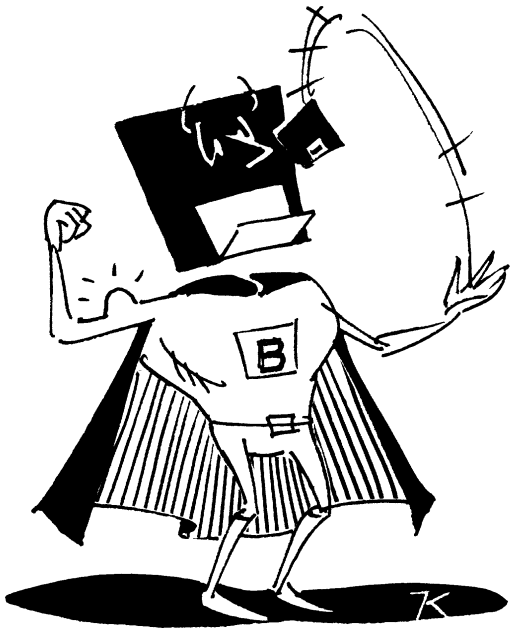
Het aardige van het informaticarecht is dat sommige wetgeving zeer onderhevig is aan een 'verjongingskuur' en zich mag verheugen in een onvermoede, welhaast yuppie-achtige belangstelling. Zo is reeds het belang van de Auteurswet 1912 in de huidige informatiemaatschappij exponentieel toegenomen en zien sommige juristen al verlangend uit naar het moment waarop de bij weinig beroepsgenoten bekende Zaaizaad- en Plantgoedwet van het stof ontdaan mag worden met het oog op de ontwikkelingen in de biotechnologie. Het is dan ook niet toevallig, dat met de toegenomen aandacht voor het fenomeen 'informatie' ook het recht op vrije meningsuiting een hernieuwde belangstelling ondergaat. Met hernieuwd wordt hier dan vooral gedoeld op een verlegging van het traditionele aandachtsterrein om bijvoorbeeld politieke denkbeelden te mogen uitdragen en te mogen ontvangen, naar het niveau van een algemeen beginsel van informatievrijheid. Enige voorzichtigheid met het ten tonele voeren van dit grondrecht en de aanspraken die daar soms op worden gebaseerd is echter op zijn plaats.

In het kader van deze verhandeling is een uitvoerige behandeling van dit onderwerp niet aan de orde. De opvatting echter, om beperkingen aan gegevensverkeer ontoelaatbaar te achten met een beroep op de free flow of information (een beroep dat we overigens ook in de discussie omtrent de strafbaarstelling van 'diefstal van informatie' zijn tegen gekomen), komt te gemakkelijk voor. Grondrechten worden vooreerst geformuleerd met het oog op de relatie tussen burgers en overheid. Horizontale werking, de werking van grondrechten tussen burgers onderling, is niet eenduidig. Eerder betekent dit hier dat een recht kan worden afgeleid om kennis te nemen van bepaalde informatie die onder de overheid rust. Voor de private sector geldt een dergelijke verplichting om mee te werken aan het verschaffen van informatie vooralsnog niet.

12.4 Literatuur

- Esch, R.E. van, 'Richtlijn grensoverschrijdende overmakingen', in: Computerrecht 1996/2.
- Grevenstein, P.V.U. van, 'Restricties op het grensoverschrijdend verkeer van bedrijfsgegevens', in: Computerrecht 1985/3.
- Hondius, F.W., 'De nieuwe privacywet en zijn internationale kader', in: Informatie en Informatiebeleid 1988/2.
- Kuitenbrouwer, F., 'Grensoverschrijdende telematica: uitdaging voor informatie vrijheid', in: Informatie en informatiebeleid 1987/3.

- Kuitenbrouwer, F., 'Nieuwe diensten en privacybescherming', in: Computerrecht 1989/1.
- Nugter, A.C.M., 'Transborder flow of personal data within the EC', (diss.), 1990.
- Schweizer, R.J., 'De conventie van de Raad van Europa betreffende de bescherming van persoonlijke gegevens en de reglementering van grens-overschrijdende gegevensstromen', in: Computerrecht 1987/2.



13 Computercriminaliteit

Op 1 maart 1993 is in werking getreden de wet 'Wijziging van het Wetboek van Strafrecht en van het Wetboek van Strafvordering in verband met de voortschrijdende toepassing van informatietechniek', beter bekend als de Wet Computercriminaliteit. Deze wet bevat naast een groot aantal wijzigingen van het Wetboek van Strafrecht en het Wetboek van Strafvordering, tevens een wijziging van het Burgerlijk Wetboek en van de Wet op de Telecommunicatievoorzieningen. De wet is voor een belangrijk deel gebaseerd op de aanbevelingen in het rapport 'Informatietechniek en strafrecht' van de Commissie Computercriminaliteit ('de commissie Franken'). In dit hoofdstuk zullen we aandacht besteden aan de vraag of de voortschrijdende toepassing van informatietechniek nieuwe vraagstukken opwerpt die een dergelijk omvangrijke aanpassing van het strafrecht legitimeren. Daartoe zal in paragraaf 13.1 eerst een nadere invulling worden gegeven aan de term computercriminaliteit, waarna we in paragraaf 13.2 zullen stilstaan bij de rol die de overheid daarin heeft ingenomen. In paragraaf 13.3 zullen enkele consequenties voor bedrijven worden aangegeven. In paragraaf 13.4 besluiten we met enkele voor het strafrecht belangrijke aandachtspunten van internet.

13.1 Computercriminaliteit - probleem van definitie

Computercriminaliteit is de minder zegenrijke kant van informatietechnologie. In een tijd waarin bedrijven en organisaties voor hun functioneren steeds meer afhankelijk zijn geworden van een juiste werking van geautomatiseerde systemen en van de met die systemen verwerkte data, wordt computercriminaliteit als een grote bedreiging daarvan opgeworpen. Hackers ('hacken' kan beschreven worden als het zich ongeautoriseerd toegang verschaffen tot een computersysteem - 'inloggen' - meestal via het openbare telefoonnet), soms nog zeer jeugdige, loggen in in de computers van het Pentagon, of verspreiden virussen tengevolge waarvan grote delen van de informatievoorziening kunnen worden uitgeschakeld. Het is mogelijk, zonder fysiek aanwezig te zijn, 'in te breken' in computersystemen en daar allerlei onwenselijke handelingen te verrichten. Manipulaties met facturen, geldbedragen of waardevolle informatie worden mogelijk dankzij de computer, terwijl de dader nauwelijks enig risico loopt en veelal geen sporen achterlaat. Althans, volgens de beeldvorming in de media. Uit de berichtgeving vóór en rond de invoering van de wet computercriminaliteit sprak de suggestie dat de overheid (politie en justitie) machteloos tegen deze vormen van criminaliteit zou staan, indien niet snel de strafwetgeving zou worden aangepast. In deze paragraaf zullen we nagaan wat we eigenlijk onder computercriminaliteit moeten verstaan en welke juridische overwegingen daarbij een rol spelen.

13.1.1 Probleem met definitie

Over de invulling van de term computercriminaliteit kan verschillend worden gedacht, onder meer afhankelijk van de vraag of men uitgaat van geldend strafrecht of van wenselijk (toekomstig) strafrecht. Termen die in dit verband wel gebezigd worden zijn 'onduldbaar', 'maatschappelijk ongewenst', 'onbehoorlijk' of 'onethisch'. Het enkele inzien van een computerbestand bijvoorbeeld, is dan wel niet strafbaar - evenmin als het inzien van een dossier -, maar ook niet ethisch. Het lijkt weinig praktisch gedragingen die onder de werking van het strafrecht vallen onder dezelfde noemer (van computercriminaliteit) te plaatsen als gedragingen die daar niet onder vallen. Aan de term 'computermisbruik' lijkt minder een juridische kwalificatie verbonden, en zou in deze algemene context beter passen. Een gebruikelijke definitie van criminaliteit is:

> *'wederrechtelijk gedrag waartegen strafrechtelijk mag worden opgetreden'*

Aan het voorvoegsel 'computer' kan weinig méér worden afgelezen dan dat bedoeld wederrechtelijk gedrag zich afspeelt binnen, of met betrekking tot,

een geautomatiseerde omgeving. De term computercriminaliteit heeft dan ook weinig praktische betekenis. Om het begrip inhoud te geven kunnen we daarom beter kijken naar enkele voorbeelden van gedragingen die algemeen daaronder worden begrepen.

SOFTWAREPIRATERIJ

Verreweg de meest voorkomende en qua geldswaarde belangrijkste vorm van computercriminaliteit is softwarepiraterij: het illegaal kopiëren en (bedrijfsmatig) verhandelen van computerprogramma's. Onder deze categorie valt eveneens plagiaat: het namaken of nabootsen van andermans software. Ook het illegaal kopiëren binnen organisaties wordt wel onder deze noemer geplaatst.

Software is beschermd door het auteursrecht. Reeds sinds 1981 (Rb. Assen, 28 juli 1981, Bartels/Koerhuis, NJ 1982, 74), dus ver vóór in 1994 computerprogramma's in de voorbeeldsgewijze opsomming van art. 10 lid 1 sub 12 Aw werden opgenomen, zijn er in Nederland op het auteursrecht gebaseerde rechterlijke uitspraken terzake van softwarebescherming. Naast civielrechtelijke mogelijkheden, zijn in de auteurswet strafrechtelijke sancties opgenomen in art. 31 e.v.

GEGEVENSBESCHERMING

Een volgend punt dat zich onmiddellijk aandient als we denken aan computercriminaliteit is dat van de bescherming van de in computersystemen opgeslagen gegevens. Voorzover op die gegevens auteursrecht rust (oorspronkelijk en waarneembaar of waarneembaar te maken), wordt dit terrein voldoende bestreken door de Auteurswet 1912, gelijk hierboven geldt ten aanzien van software. In computers opgeslagen gegevens die *niet* zelfstandig auteursrechtelijke bescherming genieten, bijvoorbeeld omdat zij niet oorspronkelijk zijn, kunnen, voorzover het gegevensbestand bedoeld is om te worden openbaar gemaakt, niettemin voor de (niet-oorspronkelijke) geschriftenbescherming in aanmerking komen, dan wel voor het sui generis regime van de databankrichtlijn.

Daarnaast kunnen gegevens, ongeacht of zij wel of niet reeds auteursrechtelijke bescherming genieten, beschermd worden door bepalingen uit het Wetboek van Strafrecht, zoals diefstal (art. 310 Sr) en verduistering (art. 321 Sr). In 1983 heeft het Hof Arnhem een uitspraak gedaan met betrekking tot verduistering van een diskpack met computergegevens (Hof Arnhem, 27 oktober 1983, NJ 1984, 80, Cr 1984/1). Het Hof oordeelde dat computergegevens zijn aan te merken als 'goed' in de zin van art. 321 Sr, omdat zij het karakter hebben van overdraagbaarheid, reproduceerbaarheid en beschikbaarheid, terwijl zij bovendien economisch waardeerbaar zijn. Het Hof baseerde zich bij zijn uitspraak op de criteria van de Hoge Raad in het Elektriciteitsarrest (HR 23 mei 1921, 564), waar het ging om diefstal van

elektriciteit. Het bekend maken van gegevens kan in sommige gevallen ook nog vallen onder de delictsomschrijving van art. 272 of 273 Sr, schending van geheimen.

Gegevens kunnen niet alleen worden overgenomen of weggenomen, zij kunnen ook worden beschadigd of gewist. Hoewel gegevens bijvoorbeeld beschadigd kunnen worden met behulp van een magneet, denken we in dit verband toch vooral aan het verschijnsel 'virussen' en 'logische bommen'. Een computervirus is een (klein) computerprogramma dat naast de instructie zichzelf te kopiëren in andere programma's veelal instructies bevat die schade kunnen aanrichten, zoals het wissen van de harde schijf. Onder logische bom wordt verstaan een computerinstructie die in werking treedt afhankelijk van het al dan niet optreden van bepaalde condities, zoals de instructie de harde schijf te wissen indien gedurende twee maanden geen salaris meer op mijn rekening wordt overgemaakt. De Rechtbank Den Haag heeft in 1989 een uitspraak gedaan, waarin het ontoegankelijk maken van een computersysteem (i.c. door het invoeren van een wachtwoord in de computer zonder dat bekend te maken) als zaaksbeschadiging (art. 350 Sr) werd geoordeeld (Rechtbank Den Haag, 9 juni 1989, Cr 1989/4).

Fraude en valsheden

Weer een andere categorie die tot computercriminaliteit kan worden gerekend, wordt gevormd door vermogenscriminaliteit als fraude en valsheden. Ook hier zijn uitspraken bekend waaruit blijkt dat de rechtspraak weinig moeite heeft met de inpassing van nieuwe technologie. Voor het strafrecht maakt het geen onderscheid of men nu fraudeert in een handmatig bijgehouden boekhouding, dan wel in een geautomatiseerde administratie. Uit 1991 dateert de uitspraak van de Hoge Raad waarin een computerbestand werd aangemerkt als zijnde een geschrift in de zin van art. 225 Sr, valsheid in geschrifte (HR 15 januari 1991, NJ 1991, 668).

In het geval van oplichting (art. 326 Sr) is wel een psychologisch element verondersteld in verband met het 'bewegen van iemand' tot het afgeven van enig goed. Zie voor de (poging tot) afrekening met een gestolen betaalpas evenwel Hoge Raad, 17 mei 1994, NJ 1995, 46: het hof kon 'afgifte' cfm art. 326 Sr opvatten als toelaten dat wordt weggenomen.

Hacken

Hierboven werd reeds het voorbeeld gegeven van schooljongens die 'Star Wars' spelen in de computers van het Pentagon. Hacken wordt vaak geassocieerd met whizz kids die de beveiliging van grote organisaties te slim af zijn. Hacken wordt dan afgedaan als of wel onschuldig, dan wel uiterst nuttig omdat organisaties attent worden gemaakt op zwakke plekken in de beveiliging. Indien uitsluitend toegang wordt gezocht tot een computersysteem en er voorts geen handelingen worden verricht dan hooguit het

inzien van bestanden (niet het bekend maken daarvan!), valt de gedraging niet onder een van de delictsomschrijvingen van de hierboven genoemde strafbepalingen. Dat deze gedragingen *niet* schadelijk zouden zijn, laat staan wenselijk, kan niet worden volgehouden. Ook indien in het geheel niets in het gegevensbestand zou zijn gewijzigd, moet men stellen dat dan tòch de integriteit van de gegevens is aangetast. De bestandsbeheerder kan er immers niet zeker van zijn dat niets aan het bestand is veranderd en zal derhalve maatregelen moeten treffen om de betrouwbaarheid van de gegevens opnieuw vast te stellen.

Nu is het optreden van schade weliswaar een van de criteria voor strafbaarstelling, doch op zichzelf is dit nog niet voldoende. De bestandsbeheerder zou een civiele actie tot schadevergoeding kunnen instellen op grond van een onrechtmatige daad van de hacker. Hier dient zich echter het probleem aan, dat de bestandsbeheerder niet zelf kan achterhalen wie in de computer is ingelogd geweest. Veelal zal daarvoor de assistentie van de telecommunicatieleverancier nodig zijn, die dergelijke informatie echter slechts mag vrijgeven aan justitie op last van de rechter-commissaris. Eerst met hacken belanden we dus bij een gedraging die onwenselijk is, maar niet bestreken werd door enige strafbepaling. De wet computercriminaliteit heeft in art. 138a 'computervredebreuk' strafbaar gesteld met een gevangenisstraf van ten hoogste zes maanden of een geldboete van de derde categorie. Onder computervredebreuk verstaat de wet het opzettelijk wederrechtelijk binnendringen in een geautomatiseerd werk voor de opslag of verwerking van gegevens, indien daarbij een beveiliging wordt doorbroken, of de toegang wordt verkregen door een technische ingreep, met behulp van valse signalen of een valse sleutel dan wel door het aannemen van een valse hoedanigheid.

Minimumlijst van de Raad van Europa

Een laatste manier tenslotte om een afbakening te vinden van wat onder computercriminaliteit kan worden verstaan, treffen we aan in de opstelling van een minimumlijst van een achttal gedragingen die de Raad van Europa de aangesloten lidstaten aanbeveelt in de nationale wetgeving strafbaar te stellen (aanbeveling nr. R (89) 9, Straatsburg, 1990):

1. Computergerelateerde fraude;
2. Computervalsheden;
3. Beschadiging van gegevens en computerprogrammatuur;
4. Computersabotage;
5. Onbevoegde toegang tot computersystemen;
6. Onbevoegde onderschepping van gegevens;
7. Onbevoegde reproduktie van computerprogramma's;
8. Onbevoegde reproduktie van chips.

13.1.2 Juridische overwegingen

Nu we enig idee hebben van wat in het algemeen onder computercriminaliteit wordt verstaan, zien we dat, met de enkele uitzondering van hacken, de algemene - niet speciaal met het oog op de beteugeling van computercriminaliteit opgenomen - strafbepalingen uit het Wetboek van Strafrecht en de Auteurswet 1912 toereikend zijn om tegen de hier beschreven gedragingen strafrechtelijk te mogen optreden. Hoe komt het nu, zo kan men zich afvragen, dat strafbepalingen die zijn opgesteld ruim vóór de intrede van het 'computertijdperk', en waarbij met de opstelling daarvan dus ook geen rekening is kunnen houden, niettemin in staat blijken dit terrein afdoende te bestrijken? Daarvoor kan gewezen worden op een tweetal kenmerken van het strafrecht.

Een belangrijke reden is gelegen in het onderscheid tussen strafbepalingen met een materiële delictsomschrijving - het resultaat van een gedraging is strafbaar gesteld, ongeacht de wijze waarop dit resultaat tot stand is gebracht - en die met een formele delictsomschrijving - de gedraging zelf is strafbaar gesteld, ongeacht of daadwerkelijk een schadelijk gevolg is ingetreden. De hierboven genoemde strafbepalingen zijn zonder uitzondering strafbepalingen met een materiële delictsomschrijving. Zo is het bijvoorbeeld in het geval van faude niet van belang of dat door middel van een handmatig doorschrijfsysteem geschiedt, of met behulp van een geautomatiseerd systeem. In beide gevallen is het het resultaat van de gedraging dat strafbaar is gesteld.

Een tweede reden hangt samen met wat wordt genoemd de autonomie van het strafrecht. Daaronder wordt verstaan dat het strafrechtelijk begrippenapparaat een autonome invulling heeft, zodat termen in het strafrecht niet dezelfde betekenis hoeven te hebben als in het civiel recht. Een voorbeeld daarvan biedt het artikel over heling (art 416 Sr), in welk artikel de term koop wordt genoemd. De advocaat stelde dat de koper van het gestolen goed wist dat het goed gestolen was, zodat er derhalve geen geldige titel was. Dan zou er dus geen koop zijn en ook geen heling. De Hoge Raad heeft toen uitdrukkelijk bepaald dat het begrip koop in het strafrecht een andere inhoud heeft dan in het privaatrecht (NJ 1931, 226). Ook in het spaarbankboekje-arrest (ook wel kappers-arrest genoemd) werd een privaatrechtelijke redenering gesanctioneerd (NJ 1933, 580). In het gouden kronen en stifttanden-arrest (NJ 1946, 503) stelde een lijkknecht dat de gouden kiezen die hij van lijken haalde een res nullius waren, dat wil zeggen aan niemand toebehoorden. De Hoge Raad meende dat er weliswaar geen privaatrechtelijk, subjectief recht op de kiezen viel aan te wijzen, maar dat er toch een soort recht voor de nabestaanden was, zodat er sprake was van toebehoren in de zin van art. 321 Sr.

Nemen we als voorbeeld de vier bestanddelen uit de delictsomschrijving van diefstal (310 Sr) voor de beantwoording van de vraag of tegen kopiëren van computergegevens strafrechtelijk mag worden opgetreden. Hierboven

hebben we gezien dat de strafrechtspraak geen moeite heeft gehad om computergegevens aan te merken als enig goed, waarbij eerder (in het elektriciteitsarrest) ontwikkelde strafrechtelijk relevante criteria zijn gehanteerd. Evenzo is de term 'toebehoren' onafhankelijk van de privaatrechtelijk doctrine ingevuld. Voor wat betreft het 'oogmerk van wederrechtelijke toeëigening' kennen we de uitspraak van de Hoge Raad in het valse sleutelarrest (NJ 1965, 120). Op de stelling van de dader dat hij de sleutel niet heeft weggenomen met het oogmerk van wederrechtelijke toeëigening, doch slechts met het oogmerk er een kopie van te maken en nadien de sleutel terug te hangen, oordeelde de Hoge Raad dat niettemin aan het criterium was voldaan, aangezien hij als 'heer en meester' over de weggenomen sleutel heeft kunnen beschikken. Resteert ons nog het bestanddeel 'wegnemen'. In het geval van kopiëren van gegevens is het zeer wel denkbaar dat voor de vraag of aan het criterium wegnemen is voldaan, niet zozeer bepalend is of de oorspronkelijke bezitter de computergegevens nog wel heeft, maar of de dader ze nu ook heeft. In elk geval heeft hij 'de kopie' weggenomen.

De conclusie lijkt op zijn plaats, dat computercriminaliteit voor de toepasselijkheid van het materiële strafrecht weinig problemen veroorzaakt. Slechts in het geval van hacking kan men menen dat daartegen niet strafrechtelijk mag worden opgetreden zonder voorafgaande aanpassing van de strafwetgeving. Dit betekent overigens niet dat in zo'n geval als een soort automatisme voor de weg van het strafrecht gekozen moet worden. Het strafrecht moet worden ingeschakeld als ultimum remedium, dat wil zeggen als andere rechtsregels niet het gewenste effect kunnen opleveren. Dat betekent dat eerst bezien moet worden of schadeveroorzakend gedrag niet langs de weg van het civiele recht kan worden tegemoet getreden, bijvoorbeeld door middel van een schadevergoedingsactie gebaseerd op de onrechtmatige daad. Voor wat betreft het verschijnsel hacken hebben we hierboven geconcludeerd dat van die civiele optie weinig heil valt te verwachten. Onder meer om wege van de hier genoemde redenen (er zijn immers nog andere vragen van opportuniteit) kan strafbaarstelling van hacken opportuun worden geacht.

13.2 Rol van de overheid

Na de vooropmerkingen in paragraaf 13.1 zullen we in deze paragraaf nagaan hoe de overheid met het fenomeen computercriminaliteit is omgegaan.

13.2.1 Wetgeving

Uit hetgeen we in paragraaf 13.1 hebben geconstateerd, volgt allerminst dat een hele serie wetswijzigingen nodig zou zijn. De wet computercriminaliteit

bevat echter een groot aantal wijzigingen in het materiële strafrecht en het formele strafrecht. Bovendien bevat de wet wijzigingen van het Burgerlijk Wetboek en de Wet op de Telecommunicatievoorzieningen.

Naast de hierboven besproken invoeging van de bepaling van 138a, computervredebreuk, bevat het Wetboek van Strafrecht aanvullingen onder meer in de artt.:

- 80 quinquies en sexies (nieuw), waarin we begripsbepalingen aantreffen van 'gegevens' en van 'geautomatiseerd werk'. Onder gegevens wordt verstaan iedere weergave van feiten, begrippen of instructies, al dan niet op een overeengekomen wijze, geschikt voor overdracht, interpretatie of verwerking door personen of geautomatiseerde werken; onder geautomatiseerd werk wordt verstaan een inrichting die bestemd is om langs elektronische weg gegevens op te slaan en te verwerken.
- 98 e.v., schending van staatsgeheimen;
- 139a e.v., afluisteren van gesprekken;
- 161 sexies en septies (nieuw), vernieling van 'geautomatiseerde werken ten algemenen nutte'; veiligheid van personen of goederen;
- 232 (nieuw), valse betaalpas e.d.;
- 273, schending bedrijfsgeheimen;
- 317, 318, 326, afpersing, afdreiging, oplichting;
- 326c (nieuw), misbruik van telecommunicatiediensten;
- 350a en b (nieuw), computergegevensbeschadiging.

In het Wetboek van Strafvordering zijn onder meer wijzigingen opgenomen ten aanzien van de artt. 125f, 125g en 125h, inlichtingen c.q. telefoontap telecommunicatie-infrastructuur. Nieuw zijn de artt. 125i t/m 125n, terzake van onderzoek van gegevens in geautomatiseerde werken;

Het Burgerlijk Wetboek is in art. 2:393 lid 4 (jaarrekeningenrecht) zodanig gewijzigd dat de accountant bij het uitbrengen van verslag aan de raad van commissarissen en aan het bestuur (de zogenoemde 'managementletter') melding dient te maken van zijn bevindingen met betrekking tot de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking.

In de Wet op de Telecommunicatievoorzieningen heeft in art. 50 een ondergeschikte aanpassing plaats gevonden, tengevolge van wijzigingen in het Wetboek van Strafvordering.

Terminologie

De (vermeende) noodzaak voor deze aanpassingen, die immers geen daadwerkelijke veranderingen in de zin van uitbreiding van het veld van strafbare gedragingen teweeg hebben gebracht, kan op hoofdlijnen worden verklaard

uit het gebruik van terminologie, en wel de termen ‘goed’ en ‘telefoongesprek’. De wetgever, daartoe aangezet door wensen vanuit de wetshandhaving, heeft ervoor gekozen om naast strafbepalingen waar de term ‘goed’ in voorkomt, nieuwe bepalingen in te voegen waarin expliciet de term ‘(computer)gegeven’ wordt gehanteerd, dan wel bestaande strafbepalingen met zodanige terminologie uit te breiden.

De aanleiding daartoe is overigens een uiterst pragmatische en concentreert zich rond de term ‘telefoongesprek’, eerder dan de term ‘goed’. Vóór de wet computercriminaliteit was in de artt. 125f en 125g Sv de bevoegdheid neergelegd voor de officier van justitie om, op vordering van de rechter-commissaris, inlichtingen te verkrijgen met betrekking tot gevoerde telefoongesprekken, respectievelijk tot het plaatsen van een telefoontap voor het afluisteren van telefoongesprekken. Met de toename van het dataverkeer (fax en computers) ontstond er evenwel onzekerheid bij de PTT en bij justitie of de term ‘telefoongesprek’ dit dataverkeer wel (mede) zou omvatten. (Vermeende) beperkingen als deze waren de aanzet tot een algehele oriëntatie op het fenomeen computercriminaliteit. (Andere onzekerheden waarmee opsporingsambtenaren werden geconfronteerd waren bijvoorbeeld hoever de zoekbevoegdheid in computersystemen nu wel reikte en de daaraan verbonden risico’s). Op 13 november 1985 werd derhalve door de minister van justitie ingesteld de Commissie Computercriminaliteit - de ‘Commissie Franken’ - die als taak kreeg de probleemgebieden in het materiële en formele strafrecht aan te geven en te adviseren over de wenselijkheid van wetgeving. De basis voor de wet computercriminaliteit wordt gevormd door het in april 1987 verschenen rapport van de commissie.

Naast de strafbaarstelling van hacken lanceert de commissie nog achtentwintig andere voorstellen voor wetswijziging. Gelet op de geringe betekenis voor de omvang van het veld van strafbare gedragingen, ligt het zwaartepunt van deze voorstellen vooral in de aanpassingen van het formele strafrecht, de uitbreiding van de strafvorderlijke bevoegdheden. De aanpassingen in het materieel strafrecht, die min of meer als ‘bliksemafleider’ gaan fungeren, worden gemotiveerd met de principiële stellingname dat het brengen van computergegevens onder de term goed, zoals in het arrest van het Hof Arnhem, dit laatste begrip te zeer zou oprekken, en daarmee strijdig zou zijn met het in art. 1 Sr neergelegde legaliteitsbeginsel (‘Geen feit is strafbaar dan uit kracht van een daaraan voorafgegane wettelijke strafbepaling.’). Uit dit beginsel volgt wel dat zogenoemde analogie-redeneringen - ‘gegevens moeten behandeld worden als goederen’ - in het strafrecht niet zijn toegestaan (in tegenstelling tot het privaatrecht). Extensieve interpretatie echter - gegevens zijn (ook) goederen - is toelaatbaar. (Voor een nadere beschouwing van deze stellingnames zie hoofdstuk 2, alwaar op grond van diverse benaderingen geconcludeerd wordt dat gegevens niet relevant van (andere) goederen kunnen worden onderscheiden).

Aangiftebereidheid

Een aspect dat meespeelde bij de tot stand koming van wijzigingen in het materiële strafrecht is dat van de geringe aangiftebereidheid van ondernemingen die met vormen van computercriminaliteit te maken hebben gehad. Bij justitie leefde wel de opvatting dat die geringe aangiftebereidheid het gevolg was van een in het bedrijfsleven heersende veronderstelling dat het strafrecht onvoldoende toereikend zou zijn om tegen computercriminaliteit op te treden. Het redigeren van strafbepalingen speciaal met het oog op computercriminaliteit zou die indruk bij het bedrijfsleven moeten wegnemen. Een belangrijke reden echter voor organisaties om géén aangifte te doen van gevallen van (computer)criminaliteit is echter niet het al dan niet aanwezig zijn van toepasselijke wetgeving, doch de schade die aan het imago van die organisatie wordt toegebracht, indien publiekelijk bekend wordt dat zij daarvan slachtoffer zijn geworden. Ondernemingen zijn gewoon dat zelf op te lossen, bijvoorbeeld door het treffen van een schadeloosstelling met de dader of ontslag van de werknemer, en in elk geval door het nemen van maatregelen van technische en/of organisatorische aard ter verhoging van de beveiliging.

De overheid heeft zelf wel belang bij het doen van aangifte door bedrijven. Aangiften zijn voor de overheid van belang voor het verkrijgen van inzicht in de aard en omvang van deze (en andere) vormen van criminaliteit. Maar bovendien zijn zij onontbeerlijk om voldoende know how te kunnen verwerven op het gebied van informatietechnologie en het bestrijden van allerlei andere vormen van criminaliteit waarbij men zich van informatietechnologie bedient. In het streven van de overheid de aangiftebereidheid onder het bedrijfsleven te doen verhogen, werd in 1989 door de Ministeries van Justitie en van Economische zaken, tezamen met het bedrijfsleven, het Platform Computercriminaliteit in het leven geroepen. Binnen het platform werd voor het bedrijfsleven de mogelijkheid gecreëerd melding te maken van gevallen van computercriminaliteit, waarbij dan met de overheid de afspraak gemaakt kon worden dat niet tot vervolging zou worden overgaan.

Empirische gegevens

Het ontbreken van voldoende empirische gegevens omtrent aard en omvang van computercriminaliteit was een belangrijk punt van kritiek ten tijde van het wetsvoorstel. Teneinde alsnog deze lacune op te vullen, is in opdracht van het platform onderzoek verricht naar de omvang en verschijningsvormen van computercriminaliteit. Het onderzoek had betrekking op de periode 1985-1990 en moest dienen ter ondersteuning van de wenselijkheid van nieuwe wetgeving. Van het aantal gemelde gevallen van computercriminaliteit van 375, bestond 51% uit softwarepiraterij, 15% uit schade aan gegevens of programma's, 14% uit onbevoegde toegang, 7% uit computergerelateerde fraude en valsheden en weer eens 7% uit spionage/diefstal van gegevens.

Ten aanzien van de aangiftebereidheid concludeerden de onderzoekers 'dat men in het algemeen de inspanning die benodigd is en de mogelijke problemen die optreden te groot acht om aangifte te doen en daarmee een onderzoek in te stellen. Dit heeft mede te maken met de lage verwachtingen die men heeft ten aanzien van een goede afloop (dat wil zeggen vergoeding van de schade en strafbaarstelling van de dader). Men acht het eenvoudiger om zaken intern af te handelen en pas bij aanzienlijke schade zal men overwegen de politie in te schakelen en een uitgebreid onderzoek te ondergaan. De angst voor negatieve publiciteit speelt ook een rol, zij het minder dan wel eens wordt gedacht'.

13.2.2 Wetshandhaving

Uit paragraaf 13.2.1 kan worden opgemaakt dat de overheid zich vooral veel moeite heeft getroost computercriminaliteit neer te zetten als probleem, waarop zowel het materieel strafrecht als het formeel strafrecht onvoldoende berekend zou zijn. Wat de overheid *zou moeten doen*, is aandacht besteden aan wets*handhaving*. Onder meer uit het hierboven aangehaalde onderzoek is gebleken dat softwarepiraterij verreweg de belangrijkste categorie vormt van computercriminaliteit. De wet computercriminaliteit heeft geen verandering aangebracht in het regime dat op softwarepiraterij van toepassing is. Als er dan al belemmeringen zouden zijn met betrekking tot opsporingsbevoegdheden, dan toch zeker niet ten aanzien van softwarepiraterij. Indien het de overheid ernst zou zijn met de beteugeling van computercriminaliteit, zou verwacht mogen worden dat de mogelijkheden die er zijn, ook volgens de opvatting van de overheid zelf, ten volle benut zouden worden. Het bestrijden van softwarepiraterij heeft tot heden echter nooit hoog op de prioriteitenlijst van opsporingsambtenaren gestaan. Merkwaardig is bovendien, dat de overheid zich wel druk maakt om problemen van bedrijven waarvoor deze de hulp van de overheid niet wensen in te roepen, zoals interne computerfraude, doch activiteiten achterwege laat ten aanzien van problemen waar bedrijven nu juist wèl actief overheidsoptreden verwachten, zoals softwarepiraterij.

Een ander belangrijk aandachtspunt dat hier niet onvermeld mag blijven is de zorg die de overheid dient te besteden aan de eigen informatievoorziening, met het oog op de voorkoming en bestrijding van computercriminaliteit.

13.2.3 Overige en verklaring

Gelet op de afwezigheid van enige feitelijke noodzaak tot aanpassing van het materieel strafrecht, is het accent van de wijzigingen tengevolge van de wet computercriminaliteit in feite komen te liggen op uitbreiding van strafvorder-

lijke bevoegdheden, met name de zoekbevoegdheid in geautomatiseerde werken. Wijziging van het materieel strafrecht lijkt zo slechts nodig te zijn geweest voor de redenering dat, indien materieel-rechtelijk de mogelijkheid wordt gecreëerd om tegen computercriminaliteit te mogen optreden, dan ook de daarvoor benodigde strafvorderlijke bevoegdheden moeten worden toegekend. Het in het geding zijnde belang is voornamelijk dat van de overheid gebleken, teneinde controle te kunnen behouden op informatie.

Zoals we in hoofdstuk 6 hebben gesignaleerd dat bij het verschijnsel 'bodyshopping' belangen van de overheid schijnen mee te spelen in het vergunningenbeleid ingevolge de Arbvowet, en in hoofdstuk 11 privacywetgeving mede ten doel blijkt te hebben persoonsgegevensverkeer zo min mogelijk te belemmeren, zo zien we ook hier dat het handelen van de overheid ten aanzien van het verschijnsel computercriminaliteit past in de public choice theorie, als rationeel gedrag van de overheid om de eigen positie te beschermen en te versterken.

Het arrest van het Hof Arnhem, waarin computergegevens als 'enig goed' werden aangemerkt, werd omstreden vanwege de wens tot nieuwe wetgeving te komen. De vraag kan gesteld worden, of het nu zo 'erg' is dat er nieuwe wetgeving is gekomen, nu er materieel zo'n gering verschil is geconstateerd. Het antwoord hierop is dat dit heel wel het geval kan zijn. Rondom bepalingen waarin de term 'goed' gehanteerd wordt, heeft in de loop der tijd strafrechtelijke doctrine vorm gekregen. Nieuwe strafbepalingen zullen aanleiding zijn tot onzekerheid met betrekking tot inhoud en reikwijdte. Voorts is niet voldoende nagedacht over het vraagstuk van samenloop. Immers, dat nu nieuwe bepalingen terzake van gegevens in de strafwet zijn opgenomen, laat onverlet dat niet tevens bepalingen terzake van goederen van toepassing kunnen zijn op hetzelfde gedrag. Een niet doordachte bijkomstigheid van de introductie van gegevens als aparte entiteit naast goederen, is de inconsistentie waartoe dit kan leiden in de begripsafbakening. Zo zal in de strafrechtpraktijk wel eens kunnen blijken dat nadere afbakening van het begrip gegevens op dezelfde kenmerken als die van goederen zal worden gebaseerd. Een anders merkwaardige inconsistentie zou zijn, dat 'gegevens' weliswaar een 'geschrift' kunnen vormen, dat een geschrift een 'goed' kan zijn, doch dat diezelfde gegevens dat weer niet zouden zijn. Zo bezien is het jammer dat voor deze weg gekozen is. Het is een weg die leidt naar onduidelijkheid, terwijl het arrest van het Hof Arnhem helder was en in lijn met de doctrine. In al die jaren heeft het arrest ook geen andere problemen opgeroepen. Een opmerkelijk feit is bovendien dat het Hof in 1994 nog eens 'op herhaling' is geweest (zie Hof Arnhem, 31 maart 1994, Cr 1994/3, hieronder).

Ook de strafbepaling waarvan de wenselijkheid minder omstreden is, die van computervredebreuk, is onderhevig aan kritiek. Voor de strafwaardigheid onder deze bepaling is het nodig dat een beveiliging wordt doorbroken (138a, lid 1, onder a.). Behalve dat met deze eis een norm wordt geïntroduceerd die

zich richt op het slachtoffer in plaats van op de dader, brengt dit bestanddeel van de delictsomschrijving met zich mee dat ter terechtzitting de kwaliteit van de beveiliging ter discussie zal worden gesteld. En als er nu íets is dat organisaties niet willen, is het met de (al dan niet) genomen veiligheidsmaatregelen in de openbaarheid treden.

13.3 Consequenties voor bedrijven

De discussies over computercriminaliteit zoals deze eind jaren '80/ begin jaren '90 zijn gevoerd, hebben voor bedrijven wel enige consequenties gehad. Zo is er ten eerste een breed besef ontstaan voor de noodzaak tot het aanbrengen van beveiligingen in de geautomatiseerde informatievoorziening. Dit behoeft overigens niet te betekenen dat altijd en maximaal zal moeten worden beveiligd. Een rationeel beveiligingsbeleid zal als uitgangspunt het analyseren van risico's hebben. Risico's kunnen worden gekwantificeerd en worden afgezet tegen de kosten van beveiliging. Een optimale beveiliging betekent dat alleen beveiligd wordt wat nodig is, en bovendien slechts voorzover de kosten daarvan de potentiële schade, tengevolge van de kans op computercriminaliteit vermenigvuldigd met het schadebedrag, niet te boven gaan.

Een tweede aspect dat uit de discussies en onderzoek naar voren is gekomen is dat van de wenselijkheid van 'institutionele immuniteit'. Organisaties neigen indien zij te maken krijgen met computercriminaliteit niet gauw tot juridische oplossingen. Eerder wordt getracht het binnen de organisatie zelf op te lossen.

Ten aanzien van de bescherming van computersoftware is tenslotte van belang de toegenomen kennis binnen organisaties en bij individuen dat kopiëren daarvan op grond van het auteursrecht in beginsel niet is toegestaan. Voor de bestrijding van piraterij echter lijkt het meeste te verwachten van het samenwerkingsverband van softwareproducenten in BSA (Business Software Alliance).

13.4 Strafrecht en internet

Een laatste punt dat in dit hoofdstuk kort besproken wordt, is de strafbaarheid van gedragingen via het internet, alsmede problemen met betrekking tot de handhaving van het strafrecht.

Van internet wordt gezegd dat daar 'anarchie' zou heersen. Daarmee wordt echter gedoeld op het feit dat 'internet' eigenlijk van niemand is, dat niemand regels stelt over het gebruik van internet, waaraan iedere gebruiker zich dient te houden. Het is niet zo, dat gedragingen op het internet zich zouden onttrekken aan de strafwetgeving. Racistische uitingen, het door middel van

internet aanzetten of oproepen tot strafbare feiten, het verspreiden van kinderpornografische afbeeldingen e.d. is allemaal strafbaar. Dit komt wederom vanwege de materiële delictsomschrijvingen van veel strafbepalingen. De daarin beschreven strafbare feiten zijn niet afhankelijk van middel of methode. Justitie is dus zonder meer bevoegd tegen dat soort zaken op te treden. De handhaving van dergelijke strafbepalingen kan in de praktijk echter problematisch komen te liggen. Een tweetal aspecten is daarbij te onderscheiden:

1. Het grensoverschrijdend karakter van internet;
2. De anonimiteit van het dataverkeer.

Ad 1. Het grensoverschrijdend karakter van internet maakt het mogelijk dat de hier bedoelde berichten in Nederland opvraagbaar zijn, zelfs met name op Nederland gericht kunnen zijn. In hoeverre de Nederlandse justitie hiertegen kan optreden, wordt bepaald door de bestaande regels van internationale rechtshulpverlening. Daarbij zijn de volgende complicaties denkbaar. Er kan een verschil zijn tussen de betrokken landen in de strafbaarheid van de gedraging. Consequentie is dat uitingen via internet uiteindelijk onder het zwaarste strafrechtregime zullen vallen. Het verspreiden van pornografische afbeeldingen is in Nederland niet strafbaar, maar zou in de islamitische wereld wel eens onder de strafwet kunnen vallen. Exploitanten van sexdiensten zullen er dan ook verstandig aan doen het daarmee verdiende geld niet te besteden aan een vakantie in een dergelijk land. In de toekomst zal een harmonisatie door middel van internationale verdragen voor deze problematiek een uitkomst moeten bieden. Denkbaar is evenwel dat er landen zullen zijn die aan een dergelijke rechtshulp niet zullen meewerken In die gevallen zullen juridische maatregelen niet toereikend zijn; de weg die in de internationale omgang tussen staten dan wel wordt verkozen is die van economische en/of andere boycot maatregelen (echter meestal alleen voor zover dergelijke maatregelen niet tevens de initiator daarvan schaden).

Ad 2. Een ander probleem is dat berichten soms worden verspreid zonder dat daarbij de afzender nog staat vermeld. Dit geschiedt door middel van de zogenoemde ‘anonymous remailers’. Voor zover onder de huidige wetgeving deze anonymous remailers niet als medeplichtig zijn te bestempelen, lijkt hier de aangewezen oplossing in een verplichting voor die remailers om op vordering van justitie de oorspronkelijke verzender van het bericht alsnog bekend te maken. Op deze wijze blijft de anonimiteit van hen die dat wensen en geen strafbare handelingen verrichten bewaard, terwijl justitie de mogelijkheid wordt geboden tegen wetsovertreders te kunnen optreden.

Een probleem dat vooral door overheidsfunctionarissen wordt gesignaleerd, is dat het dataverkeer in toenemende mate ‘versleuteld’ plaats vindt. Dit kan

door middel van de in de handel zijnde ‘encryptieprogramma’s’, doch evenzo door bijvoorbeeld in een willekeurig gegevensbestand een ‘verboden’ uiting op te nemen. Van effectieve controle lijkt dan geen sprake meer te kunnen zijn. In 1990 heeft deze ontwikkeling de overheid dermate zorgen gebaard, dat een initiatief werd genomen tot encryptiewetgeving. Het gebruik van encryptietechnieken zou aan een vergunning onderworpen moeten worden. Vanwege kritiek alom, moest de overheid dit snode plan intrekken. Niet alleen zou dergelijke wetgeving feitelijk het doel niet bereiken - het is immers eenvoudig om een bericht ‘als gewoon bericht’ te verzenden, zodanig dat alleen de afnemer de verborgen boodschap weet te vinden - maar encryptie is nu juist de hoeksteen van informatiebeveiliging voor ondernemingen. En voor een beveiligingsstrategie is het zonder meer te riskant de overheid daarin een plaats te laten innemen. Het is echter zaak alert te blijven op het ontstaan van nieuwe wetgevende initiatieven op dit gebied. De Raad van Ministers van de Raad van Europa heeft op 8 september 1995 Aanbeveling R (95) 13 aangenomen terzake van opsporing van strafbare feiten in een geautomatiseerde omgeving. Ten aanzien van cryptografie wordt opgemerkt dat het gebruik daarvan de rechtmatige uitoefening van strafrechtelijke bevoegdheden niet mag verhinderen. De lidstaten worden uitgenodigd daartoe toepasselijke maatregelen te treffen.

13.5 Jurisprudentie

Hr 11 MEI 1982, nj 1982, 583 (GIRAAL GELD-ARREST)
Het verweer, dat blijkens de bewezenverklaring door het Hof niet is aanvaard, stelt de rechtsvraag aan de orde, of een in zogenaamd giraal geld bestaand geldsbedrag dat abusievelijk door een ander op iemands bankrekening is overgemaakt al dan niet kan worden aangemerkt als een ‘goed’ dat als ‘toebehorende’ aan die ander vatbaar is voor ‘toeëigening’ - een en ander in de zin van art. 321 Sr, waarop de steller van de tenlastelegging kennelijk het oog had - door de rekeninghouder. Gelet op de functie van zogenaamd giraal geld in het maatschappelijk verkeer brengt redelijke uitleg van voornoemd artikel immers mede, dat evenbedoelde vraag bevestigend beantwoord moet worden.

HOF ARNHEM, 27 OKTOBER 1983, nj 1984, 80, CR 1984/1
Computergegevens dragen het karakter van overdraagbaarheid, reproduceerbaarheid en beschikbaarheid, terwijl zij bovendien economisch waardeerbaar zijn. ‘Goed’ in de zin van art. 321 Sr (verduistering).

RB AMSTERDAM (STRAFKAMER), 5 DECEMBER 1988, CR 1989/5
Diefstal van gesprekseenheden telefoonpulsen. Naar het oordeel van de Rb. zijn deze ‘gesprekseenheden en elektrische impulsen in het telefoonverkeer’

dan ook niet te beschouwen als enig goed dat in de zin van art. 310 Sr kan worden 'weggenomen'. Immers deze 'gesprekseenheden' zijn, anders dan bijvoorbeeld elektrische stroom niet natuurkundig bepaalbaar, en meetbaar en/of zintuiglijk waarneembaar, doch abstracte, naar eigen oordeel vastgestelde, rekeneenheden.

RB DEN HAAG, 9 JUNI 1989, CR 1989/4

Invoeren van wachtwoord in computersysteem zonder dat bekend te maken. De rechtbank heeft hierbij overwogen dat verdachte door zijn handelwijze (manipulatie van het computerprogramma) een toestand in het leven heeft geroepen, die het normale gebruik van het computersysteem - i.c. bestaande uit zowel programmatuur als, onmiskenbaar van stoffelijke aard zijnde, apparatuur - althans tijdelijk heeft belemmerd. Niet ter zake doet dat de apparatuur daarbij onaangetast is gebleven. Zaaksbeschadiging.

RB BREDA (STRAFKAMER), 12 OKTOBER 1989, CR 1990/3, NT R.V. DE MULDER

Fotokopiëren van gegevens - diefstal. De rechtbank is van oordeel dat onder omstandigheden het tijdelijk gebruik van een goed de wederrechtelijke toeëigening daarvan kan opleveren. (Zoals bij het Valse Sleutelarrest). De bijzondere omstandigheid in dit geval is, dat het goed in kwestie een document is waarvan het wezen niet is gelegen in de vellen papier waaruit het bestaat, maar in de gegevens die erop zijn vermeld. Deze bijzonderheid brengt naar het oordeel der rechtbank mede, dat ook het tijdelijk wederrechtelijk wegnemen van dat goed met het oogmerk de daarop voorkomende gegevens ten eigen bate te kopiëren wederrechtelijke toeëigening in de zin van art. 310 Sr oplevert.

Door het fotokopiëren worden de gegevens uit het document op een andere drager - in dit geval een vel papier - overgenomen. Dit aan een document onttrekken van gegevens - wat op velerlei manieren kan geschieden, bijvoorbeeld door die gegevens in het geheugen te prenten en elders op te schrijven of mondeling over te brengen - is naar het oordeel der rechtbank niet het wegnemen van een goed in de zin van art. 310 Sr daar op die manier dit begrip zou worden uitgebreid ver buiten de grenzen die in het in het normale maatschappelijke verkeer heeft.

RB ALKMAAR (STRAFKAMER), 27 APRIL 1990, DAGVAARDING PER FAX, CR 1990/5

Ter zitting is komen vast te staan dat er geen dagvaarding is in de zin van de wet, doch hooguit een telefaxbericht, dat niet als zodanig kan worden beschouwd.

HR 15 JANUARI 1991, NJ 1991, 668, CR 1991/4, NT H.W.K. KASPERSEN

Aan een administratie die bestaat uit computerbestanden pleegt in het hedendaags maatschappelijk verkeer betekenis te worden toegekend voor het

bewijs van de gegevens die daarin zijn opgenomen. Zulk een administratie dient te worden aangemerkt als geschriften in de zin van art. 225 Sr die bestemd zijn om tot het bewijs van enig feit te dienen. Daarbij heeft het hof mede in aanmerking genomen dat het bij de onderwerpelijke computer-bestanden/registers gaat om: a). gegevens die op materie, te weten een magneetschijf, zijn vastgelegd; b) gegevens die op die magneetschijf zijn vastgelegd met de bedoeling om deze aldus te bewaren en c) gegevens die op tamelijk eenvoudige wijze leesbaar kunnen worden gemaakt, te weten op het beeldscherm, hetzij op de op papier neergelegde uitdraai.

Hr 19 NOVEMBER 1991, nj 1992, 124
Oplichting: bewegen van de bank tot afgifte van geld door listige kunst-grepen, te weten het halen van geld uit een geldautomaat door middel van een gestolen Eurochequepas en de daarbij behorende pincode.

Hr 3 DECEMBER 1991, CR 1994/5, NT R.V. DE MULDER
Geprinte formulieren waarmee via het internationale bancaire systeem SWIFT betalingsopdrachten worden gegeven zijn geschriften. Bewijsbestemming van de formulieren.

Hr 28 APRIL 1992, nj 1992, 657, CR 1993/3, NT R.V. DE MULDER
Geldautomaat. Diefstal met bedreiging met geweld of afpersing? 'Wegnemen' en 'toebehoren' cfm. art. 310 Sr.

Hr 26 MEI 1992, nj 1992, 753
'Afluisteren fax.' Het opnemen en leesbaar maken van faxsignalen valt niet op een lijn te stellen met het afluisteren van telefoongesprekken; evenmin zijn faxsignalen gelijk te stellen met een gesloten brief.

Hr 8 DECEMBER 1992, nj 1993, 323, CR 1993/2, NT H.W.K. KASPERSEN
De feitelijke gang van zaken is conform die in HR NJ 1992, 124 (oplichting). Echter: het met behulp van een ontvreemde bankpas met bijbehorende pincode geld halen uit een geldautomaat levert (ook) diefstal door middel van valse sleutels op.

HOF ARNHEM, 31 MAART 1994, CR 1994/3, NT H.W.K. KASPERSEN
Computergegevens bestaande uit een klantenbestand zijn volgens het Hof te kwalificeren als 'enig goed'.

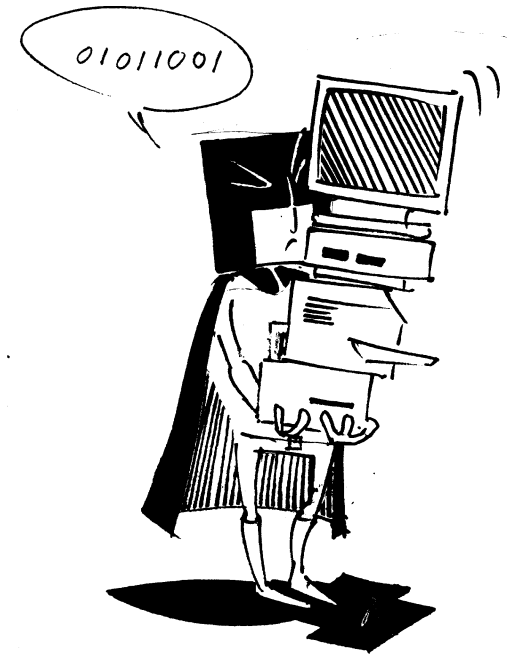
HR 17 MEI 1994, NJ 1995, 46
Poging tot oplichting; het hof kon 'afgifte' cfm. art. 326 Sr opvatten als toelaten dat wordt weggenomen. De bewijsmiddelen (verdachte wil o.a. benzine betalen met gestolen credit card; pomphouder belt cardorganisatie;

verdachte rijdt weg) dwingen niet tot het oordeel dat daadwerkelijk tot ‘afgifte’ is overgegaan.

Hr 13 JUNI 1995, CR 1995/6, NT H.W.K. KASPERSEN
Het middel stelt de vraag aan de orde of, wanneer de houder van een zogenaamde pincode wordt gedwongen die pincode te noemen aan diegenen die hem daartoe met geweld bedreigen of geweld op hem toepassen, sprake is van ‘afgifte van enig goed’ als bedoeld in art. 317 (oud) Sr. Deze vraag moet ontkennend worden beantwoord. Immers, de in de geest van een persoon opgeslagen bekendheid met de bij zijn betaalpas behorende cijfercombinatie kan niet worden aangemerkt als een ‘goed’ in de zin van art. 317 (oud) Sr. Evenmin kan het (onvrijwillig) noemen van een pincode worden aangemerkt als afgifte in de zin van laatstgenoemd artikel: daarvan kan slechts worden gesproken indien door die afgifte de afgever de beschikking over het afgegevene verliest, hetgeen uiteraard bij het noemen van een pincode niet het geval is.

13.6 Literatuur

- Charbon, F.H. en H.W.K. Kaspersen, ‘Computercriminaliteit in Nederland’, rapport in opdracht van het Platform Computercriminaliteit, 1990.
- Commissie Computercriminaliteit, ‘Informatietechniek en strafrecht’, Staatsuitgeverij 1987.
- Dijk, Chr.H. van en J.M.J. Keltjens, ‘Computercriminaliteit’, W.E.J. Tjeenk Willink, Deventer, 1995.
- Kaspersen, H.W.K., ‘Strafbaarstelling van computermisbruik’, (diss.), Kluwer, Deventer, 1990
- Kaspersen, H.W.K., ‘De wet computercriminaliteit is er - nu de boeven nog’, in: Computerrecht 1993/4.
- Kleve, P. en A. Mitrakas, ‘Softwarepiraterij - een rol voor BSA’, in: Computerrecht 1995/2.
- Mulder, R.V. De, ‘Wetgeving maakt technologie tot veelkoppige draak’, in: Nederlands Juristenblad 1993/39.
- Net, C.B. van der, ‘Locus delicti op het internet’, in: Computerrecht 1996/3.
- Schutter, B. De (red.), ‘Informaticacriminaliteit’, Kluwer, Antwerpen/Deventer, 1988.
- Wiemans, F.P.E. (red.), ‘Commentaren op het wetsvoorstel computercriminaliteit’, Cipher Management, Maastricht, 1991.



14 Internetrecht?

Informatietechnologie is van grote invloed op de samenleving en op het recht. In hoofdstuk 1 is zelfs de veronderstelling neergelegd dat informatietechnologie manifester is dan wel wordt aangenomen of ervaren. Vreemd is dit overigens niet. Voor een belangrijk deel wordt ons dagelijks doen en laten beïnvloed door informatietechnologie zonder dat wij daar bij stil staan of zelfs erg in hebben. Technologische ontwikkelingen gaan voorts zo snel dat, waar we geneigd zijn te spreken over *toekomstige* veranderingen, we ons veelal niet realiseren dat die veranderingen voor een deel reeds plaats vinden.

In dit boekje over informaticarecht zijn voornamelijk juridische aspecten van die veranderingen tengevolge van informatietechnologie besproken. Een conclusie die uit de bespreking van de verschillende onderwerpen kan worden getrokken is dat, minder dan wel wordt aangenomen en minder ook dan feitelijk het geval is, wetgevende initiatieven nodig blijken. Een belangrijke reden daarvoor is dat de mogelijkheid tot directe beschikbaarheid van vrijwel alle informatie, onmiddellijk, op ieder gewenst moment en waar ter wereld ook aanwezig, het belang van intermediaire functies in het algemeen aanzienlijk doet verminderen. Hieruit vloeit ook voort een afnemende behoefte aan de rol van de overheid en die van wetgeving, voor wat betreft hun cummunicatieve, intermediaire functie: het met elkaar afspreken van normeringen en

reguleringen; het verschaffen van een gelijk referentiekader e.d. Informatietechnologie heeft een neerwaarts effect op de behoefte aan, c.q. de noodzaak van wettelijke regelingen in het algemeen.

Ten aanzien van informatietechnologie zelf is evenmin gebleken van een noodzaak tot zo'n imposante reguleringsgolf, zoals die heeft plaats gevonden bijvorbeeld op het gebied van softwarebescherming, de bescherming van data en databanken en computercriminaliteit. De belangrijkste wetgevende initiatieven die nodig zijn in de informatiemaatschappij zijn eigenlijk die waar de overheid aan het terugtreden is: liberalisering van de telecommunicatie-markt, het wegnemen van belemmeringen voor (commerciële) grensoverschrijdende communicatiemedia en in het algemeen het wegnemen van belemmeringen om in het contact met de overheid gebruik te maken van informatietechnologie, zoals het mogelijk maken van 'elektronische aangiften' en 'elektronische boekhouding'.

Een aspect dat in dit boekje slechts zijdelings is aangestipt, is de invloed die van informatietechnologie en internet zal uitgaan op het recht zelf. Het is vreemd te bemerken dat de betekenis van dèze ontwikkeling, die nu juist wèl raakt aan de grondvesten van zowel de beoefening als de werking van het recht, nauwelijks onderkend lijkt, terwijl het informaticarecht blijkt te inspireren tot een hausse aan wetgevende initiatieven, zonder dat daar werkelijke, normatieve veranderingen voor zijn aan te wijzen.

Informatietechnologie blijkt voorts van grote invloed op de effectiviteit van naleving, controle en handhaving van sommige regels.

14.1 Internet

Met 'internet', zo zou men kunnen zeggen, heeft de informatiemaatschappij definitief zijn intrede gedaan. Nu kan men al sinds de jaren '70 met enige regelmaat dergelijke tijdperk-typerende uitspraken beluisteren. Het toekomstbeeld van het 'papierloze' kantoor was in die tijd nog slechts een kwestie van geduld. De produktie van papier is echter nog nooit zo hoog geweest als in de afgelopen decennia. Nu is geduld natuurlijk relatief. Achteraf kan men constateren dat de verwachting iets te hoog gespannen is geweest. Maar is het ook niet zo, dat we sinds die boude uitspraken nog maar twintig jaar verder zijn? En is het ook niet zo, dat de industriële maatschappij er een aantal decennia meer voor nodig had om tot volledige ontwikkeling te komen? De 'zin' van dergelijke uitspraken is relatief, en bovendien minder discutabel indien zij - later - door historici wordt gedaan.

Internet heeft op zichzelf (nog) geen andere rechtsvragen opgeworpen dan zoals in dit boekje besproken. Een belangrijke functie van internet is evenwel dat het als katalysator heeft gewerkt met betrekking tot de aandacht die thans aan de hier beschreven problematiek wordt gegeven. Internet als metafoor

voor de informatiemaatschappij. Dat internet nieuwe rechtsvragen zal gaan oproepen, valt overigens nauwelijks te betwijfelen. Die rechtsvragen zullen voortkomen uit de essentie van internet: grensoverschrijdende communicatie. De integratie van computers en telecommunicatie (telematica), waarvan internet thans het meest prominente voorbeeld is, schept het kader en betekent een ongekende stimulans voor een welhaast ongelimiteerde uitwisseling van informatie, van welke aard dan ook, niet gebonden aan enig territorium, toegangsvereiste of censuur. Rees nu al zijn complicaties tengevolge van het internationale bereik van internet zichtbaar, in de beperkingen van op overzichtelijke, 'natuurlijke' grenzen van onafhankelijke staten gebaseerde rechtsmacht.

14.2 Omgaan met technologie

De hier gesignaleerde tendens van toename van wetgeving geïnspireerd door technologische vernieuwingen moet met grote terughoudendheid tegemoet worden getreden. De noodzaak voor nieuwe wetgeving is allerminst evident. Wat wèl belangrijk is, is dat juristen kennis verwerven over technologie en begrip omtrent de werking daarvan, over wat je kunt doen met informatiesystemen, in het algemeen en in de juridische praktijk. Nu is deze eis aan de kwalificaties van juristen ook weer niet zo vreemd, in een tijd waarin moderne managementtheorieën ons leren dat de kracht van organisaties blijkt te liggen in het vermogen zich in te stellen op veranderingen. "Leren houden van veranderingen", dat zal voor juristen toch nog even wennen zijn.

Affiniteit met technologie is belangrijk, naast de juridische vaardigheid tot kwalificeren. Een kenmerk van ons rechtsstelsel, bijvoorbeeld ten opzichte van het Angelsaksische rechtsstelsel, is dat door een adequate kwalificatie van entiteiten niet steeds het middel van nadere wettelijke regulering nodig is gebleken. Veel informatietechnologische ontwikkelingen zijn afkomstig uit de VS. We zien ook, bijvoorbeeld in computercontracten en in het fenomeen ADR (alternatieve vormen van geschillenbeslechting), invloeden vanuit het Amerikaanse rechtsstelsel. Vanwege de 'voorsprong' die de VS heeft in de omgang met vraagstukken met een technologische oorsprong, is het begrijpelijk dat juristen zich oriënteren op de aldaar gekozen juridische oplossingen. Voor een deel zou de beweging richting een attitude van 'ieder vraagstuk zijn eigen wet' veroorzaakt kunnen zijn door die invloed vanuit de VS.

Een voorbeeld waartoe zowel een verschil in benadering van technologie als het gebruik van het instrument van kwalificeren kan leiden, vinden we in de 'hardnekkige discussie' over het goedsbegrip. Wat daarin opvalt is, dat juristen bij wie de uitoefening van hun beroep eigenlijk bestaat uit kwalificeren - de rechterlijke macht - opmerkelijk weinig moeite blijken te hebben met het incorpereren van nieuwe technologie in bestaande inzichten. De

polemiek rond de vraag of software, gegevens of informatie al dan niet te kwalificeren zijn als een ‘zaak’ in goederenrechtelijke zin, of als ‘enig goed’ in strafrechtelijke zin, is dan ook slecht te begrijpen. Maar ja, dat was in 1921 ook het geval rond elektriciteit. En daarover wordt thans minder verdeeld gedacht.

14.3 Prestatiebescherming

Een andere in het oog springende tendens is voorts de uitdijende reikwijdte van rechten ten aanzien van produkten van informatietechnologie. Hiermee wordt niet in de eerste plaats gedoeld op de wijziging van de Auteurswet 1912 betreffende softwarebescherming, of de introductie van een nieuw recht van intellectuele eigendom met betrekking tot de bescherming van chips. Ten aanzien van beide onderwerpen is het nooit zo geweest dat zij voordien bescherming onder het intellectueel eigendomsrecht moesten ontberen. Wat wèl verschilt is de indringendheid van de thans geboden bescherming.

De ‘softwarewet’ bracht een wettelijke verankering van een mededingingsbeperkende regeling van het sterkste soort: een verbod op reverse engineering van software. Ook hier speelt de kwestie van kwalificatie. Tengevolge van een enge opvatting van het begrip ‘verveelvoudigen’, namelijk geënt op een technische uitleg in plaats van op het - maatschappelijk relevanter - criterium van exploitatie, zijn handelingen die inherent zijn aan het kunnen gebruiken van software maar die gepaard gaan met reprodukties in het werkgeheugen van de computer, aan beperkingen onderhevig gesteld. Dit leidt bijvoorbeeld tot het merkwaardige onderscheid dat een docent aan de filmacademie geen inbreuk maakt op auteursrechten bij het vooruit, achteruit of beeldje bij beeldje afspelen van een film, terwijl zijn collega-docent informatica die datzelfde zou willen doen met een computerprogramma dat wel zou doen. Een punt van kritiek op het verbod op reverse engineering van geheel andere aard is overigens dat de regeling nu niet direct ten voordele van de ontwikkeling van een Europese software-industrie kan worden uitgelegd, gelet op de dominante marktpositie die Amerikaanse leveranciers tot nog toe innemen.

Aan het ontstaan van het chipsrecht ligt een eigenzinnig, protectionistisch handelen van de VS ten grondslag. Chipswetgeving lijkt sterk op auteursrecht. De vervanging van het *kopje* ‘auteurswet’ door ‘chipswet’ gaven de VS echter de mogelijkheid om het in de Berner Conventie vastgelegde assimilatiebeginsel te ontwijken en te vervangen door het beginsel van reciprociteit. Een antwoord dat de VS nodig achtten op de geringe of niet-naleving van auteursrechten in sommige landen in zuid-oost Azië. De EG volgde, zich onvoldoende realiserend dat de VS de EG maar al te hard nodig had om de door hen gewenste bescherming ook in de EG te kunnen effectueren.

De claim vanuit de industrie, tot steeds verder strekkende beschermingsregimes, blijkt voorts uit het opschuiven van de bescherming van *oorspronkelijke* voortbrengselen van de menselijke geest naar ook *niet*-oorspronkelijke. De hierboven aangehaalde regeling van reverse engineering is eigenlijk al een voorbeeld waarbij vooral de *inspanning* die ten grondslag heeft gelegen aan het maken van het produkt object van bescherming blijkt te zijn. Niet alleen is het verboden om een gelijkend produkt te maken en op de markt te brengen - dat was al zo op grond van het vigerende auteursrecht - het is nu zelfs verboden om kennis op te doen omtrent het produkt, omdat daardoor gemakkelijker nieuwe produkten ontwikkeld zouden kunnen worden. En dat terwijl de kennis zelf nu juist weer niet beschermd wordt door het auteursrecht. De richtlijn databankbescherming volmaakt in feite het veld van beschermenswaardige objecten, in die zin dat daarmede ook niet-oorspronkelijke werken onder de werking van intellectuele eigendom wordt gebracht. In databanken opgeslagen data, die niet reeds zelfstandig voor bescherming door een recht van intellectuele eigendom in aanmerking komen, worden door de richtlijn beschermd in verband met de inspanning die de databankmaker heeft moeten leveren ten opzichte van het gemak waarmee anderen daarvan kunnen profiteren.

Op zichzelf zal de richtlijn databankbescherming niet zoveel verandering in beschermingsomvang teweeg brengen. Onder de thans nog geldende geschriftenbescherming, die zich mede uitstrekt over niet-oorspronkelijke geschriften, wordt een soortgelijk beschermingsniveau geboden. Wel is het zo dat het leerstuk van prestatiebescherming aan zelfstandige betekenis lijkt in te boeten, nu dit soort prestaties rechtstreeks onder de werking van het intellectueel eigendomsrecht worden gebracht.

Het stelsel van intellectuele eigendom komt wel steeds meer onder druk te staan. Enerzijds geeft de digitalisering van informatieprodukten, en de tengevolge daarvan vereenvoudigde reproduktie- en distributiemogelijkheden, een toename van aanspraken op het intellectueel eigendomsrecht te zien. Bovendien schuift het karakter van dit recht langzaam op in de richting van bescherming van de met de ontwikkeling van die produkten gepaard gaande inspanning, waarbij de band met de bescherming van het creatieve element van produkten van de menselijke geest steeds losser wordt. Anderzijds brengt de digitale vorm van - multimediale - informatieprodukten, tezamen met wereldwijde distributiemogelijkheden juist problemen van beheersbaarheid met zich mee, alsmede het probleem van cumulatie van regimes.

14.4 Internationale dimensie

Otwikkelingen binnen het informaticarecht blijken in belangrijke mate te worden aangestuurd vanuit Europees en internationaal verband. Tal van hier

besproken terreinen zijn inmiddels bestreken door richtlijnen van de Europese Commissie, welke activiteiten nog lang niet ten einde lijken. Ook de Raad van Europa en de Organisatie voor Economische Samenwerking en Ontwikkeling hebben verschillende initiatieven ontplooid met betrekking tot regulering van informatietechnologie. Het grensoverschrijdend karakter van informatievoorziening in aanmerking genomen, is dat op zichzelf begrijpelijk en toe te juichen. Wel is het zo, dat de op deelterreinen toegespitste oriëntatie (software, databanken) soms ten koste blijkt te gaan van de homogeniteit van het rechtsgebied (bijvoorbeeld het auteursrecht) waarbinnen deze onderdelen nadere regulering ondervinden.

Als remedie voor deze ongewenste effecten wordt wel gesteld dat regelgeving bij voorkeur technologie-onafhankelijk geformuleerd zou moeten worden. Dit lijkt een juiste benadering, zij het dat dit niet slechts betreft dat vermeden moet worden dat regelgeving naar aanleiding van technologie een te nauwe verwevenheid krijgt met de toevallige stand der techniek. Belangrijk is te onderkennen dat de betekenis van technologie voor recht, rechtstaat en democratie dan ook inhoudt dat nadere normering vooral geschiedt met het oog op recht, rechtstaat en democratie, en niet dat techniek zelf het object van regelgeving vormt. En daarvoor zal dan eerst moeten blijken dat invloed van technologie een veranderende normering tot gevolg heeft. Een argument derhalve dat de opvatting dat het recht zou achter lopen op technologische ontwikkelingen enigszins aan relevantie doet inboeten.

Een invalshoek die wèl internationale belangstelling vereist is de noodzakelijke overeenstemming met betrekking tot handhavingsaspecten, vooral ook in die situaties waarin sprake is van verschillende normstelling. Met name kan in dit verband gewezen worden op de zogenoemde internetdelicten.

Waar het betreft activiteiten tussen bedrijven onderling lijkt overheidsinterventie veel minder nodig, en soms zelfs ongewenst. Ontwikkelingen als het internationale elektronisch handels- en betalingsverkeer bijvoorbeeld, alsmede de beslechting van geschillen in dit segment, hebben het tot nog toe steeds goed kunnen stellen zonder specifiek daarop gerichte overheidsinterventie.

Hierboven is beargumenteerd dat terughoudendheid wenselijk is ten aanzien van wetgevende initiatieven met technologie als onderwerp. Tevens is het probleem van internationale afstemming terzake van handhavingsaspecten onderkend. Dit laatste betekent echter niet dat handhaving van bestaande wetten thans ontoereikend zou moeten zijn. De overheid zou zich wat dat betreft andere prioriteiten kunnen stellen. Wat echter opvalt is dat de belangstelling van de overheid zich veelal uit in de vorm van maatregelen die een toename van controle door de overheid in zich houden. Zo zien we steeds de discussie rondom encryptietechnieken herleven, waarbij de overheid graag een vorm van regulering zou zien opdat zij, onder het mom van bestrijding

van de georganiseerde misdaad, greep zou verkrijgen op de inhoud van elektronisch verzonden berichten. Al eerder is betoogd dat deze doelstelling door middel van encryptieregulering niet te effectueren valt. Daar staat wel tegenover dat de veiligheid en betrouwbaarheid van het internationale handels- en betalingsverkeer nu juist gediend zijn met een vrije ontwikkeling en aanwending van encryptietechnologie. Ook het overheidsbeleid met betrekking tot privacyvraagstukken wordt door eenzelfde tweeslachtigheid gekenmerkt. Enerzijds zien we de tot stand koming van internationale regelingen, waaronder laatstelijk de EU-richtlijn privacybescherming, met talrijke, soms verstrekkende gevolgen voor het particuliere bedrijfsleven. Anderzijds blijken die regelingen voor wat betreft hun toepassing zich vaak slechts beperkt uit te strijken over het terrein van het overheidsoptreden, gelet op de veelheid aan uitzonderingen die met het oog op de uitvoering van overheidstaken zijn toegelaten.

Blijkt de overheid doorgaans initiatiefrijk met betrekking tot de vergaring van informatie, een terrein waarop de overheid ten onrechte een terughoudende opstelling inneemt, is dat van ontsluiting en beschikbaarstelling van wet- en regelgeving en jurisprudentie.

14.5 Mogelijkheden van integrale toegankelijkheid van rechtsbronnen

Wij leven in de periode van de digitalisering. In de wereld van digitale vastlegging van informatie nemen teksten in ten minste twee opzichten een bijzondere positie in. Ten eerste leveren teksten relatief kleine bestanden op. Op een CD kan men bijvoorbeeld ofwel een uurtje muziek, ofwel de gehele Nederlandse wetgeving (goed voor vele uren leesplezier) kwijt. Het argument dat de beschikbaarheid van alle rechtsbronnen in digitale vorm onmogelijk is door de fysieke omvang is daarom niet houdbaar. De Mulder (‘Toegankelijkheid van rechtspraak in de 21e eeuw; over enkele jaren dus’) schat bijvoorbeeld de tekstproduktie van Nederlandse rechters per jaar op minder dan 10 Gigabytes. Dit is een omvang die bij de huidige prijzen van schijfgeheugens alleszins beheersbaar is.

Een tweede verschil tussen teksten en andere informatie is het betrekkelijke gemak van herkenning. Teksten hebben een groot aantal gemakkelijk te inventariseren en vaak ook te interpreteren eigenschappen. Er komen bepaalde woorden in voor, die een bepaalde frequentie kunnen hebben etc. Alleen al door de frequentie van de gebruikte letters in een bestand te tellen kan men met grote zekerheid vaststellen in welke taal de tekst is geschreven. Uit het onderzoek van Van Noortwijk (‘Het woordgebruik meester’) blijkt dat men op grond van het woordgebruik in een Nederlandse tekst gemakkelijk kan beslissen of het stuk algemeen Nederlands, dan wel een deel van de Nederlandse wetgeving of Nederlandse jurisprudentie betreft.

In ‘Conceptuele geautomatiseerde juridische documentatie-systemen’ is uiteengezet welke bezwaren er tegen de inmiddels klassieke zoeksystemen zijn aan te voeren, in het bijzonder vanuit het gezichtspunt van de juridische beroepsbeoefenaar. Het traditionele ‘Booleaanse’ zoeken (het zoeken op specifieke woorden (‘zoektermen’), eventueel gecombineerd middels logische (aan de zogenoemde Boole-algebra ontleende) operatoren als ‘of’ en ‘en’ en ‘niet’) heeft zijn langste tijd gehad. Nieuwe systemen zullen intelligenter, of ‘conceptueel’ zijn, dat wil zeggen meer recht doen aan de volgende facetten:

- de gebruiker kan zijn vragen stellen in meer natuurlijke vorm;
- de gebruiker kan zijn kennis van juridische concepten inbrengen ten behoeve van het opzoeken;
- de kennis van de gebruiker(s) kan bewaard en geordend worden en later weer toegepast;
- de gevonden resultaten kunnen bewaard en geordend worden en later weer gebruikt;
- het systeem kan een rangorde in relevantie geven in plaats van een lijst van ‘hits’;
- het systeem kan de door de gebruiker ingebrachte kennis en/of de gevonden resultaten in grafische vorm afbeelden (bijvoorbeeld welke documenten vanuit een bepaald gezichtspunt bij elkaar horen);
- het systeem kan de ingebrachte kennis en/of de gevonden resultaten evalueren op innerlijke consistentie en op consistentie met reeds in het systeem aanwezige kennis;
- het systeem laat door de gebruiker *gewenste* inconsistenties toe.

In de praktijk zullen steeds meer commerciële systemen aan steeds meer van deze eisen gaan voldoen. Het ‘Flexlaw Legal Information System’ voldoet er reeds voor een belangrijk deel aan en is sinds kort op de (Noord-Amerikaanse) markt beschikbaar.

Tenslotte, het gaat niet alleen om zoektechnieken. Teksten in het algemeen en juridische kenbronnen in het bijzonder dienen ook doorgebladerd te kunnen worden (‘browsen’). Is het zoeken vooral gericht op probleemoplossing, het beantwoorden van reeds gestelde vragen, het browsen is vooral bedoeld om tot nieuwe vragen te komen, voor het bevredigen van een meer vage nieuwsgierigheid. Ook hier is de techniek op haast overweldigende wijze te hulp geschoten door het ontwikkelen van de hypertext-vorm. Voorbeelden zijn uiteraard de meeste WWW-pagina's op internet, alsmede de help-faciliteiten van veel programma’s onder Windows 95. Voor de toekomst ligt integratie van de ‘browsing’- en ‘retrieval’-mogelijkheden voor de hand. Zo is denkbaar dat men al browsend informatie opbouwt voor conceptueel zoeken, terwijl informatie vergaard met conceptueel zoeken als basis voor het opbouwen van de zogenoemde ‘hyperlinks’ gaat dienen.

De conclusie moet luiden, dat de integrale toegankelijkheid via internet of anderszins van alle juridische kenbronnen de gebruikers geenszins zal behoeven te overweldigen. De voortschrijdende techniek zal de toegang vergemakkelijken, en intelligenter maken, ook in de zin dat de computer onthoudt en tot op zekere hoogte begrijpt welke concepten een gebruiker hanteert. Gebruikers zullen met de beschikbare technieken steeds handiger worden en daarin een zekere ambachtelijkheid kunnen ontwikkelen.

Met de hierboven beschreven mogelijkheden tot zoeken en bladeren in grote tekstbestanden zijn de mogelijkheden niet uitgeput. In 'Juridische begrippen en waarschijnlijkheid' is aangegeven hoe op 'klassiek jurimetrische' wijze rechtspraak kan worden geanalyseerd en meer in het bijzonder, hoe conceptuele technieken gebruikt kunnen worden om ook omvangrijke jurisprudentie-bestanden te onderzoeken. Met zulke gecombineerde technieken kunnen de feiten die in de zaken een rol hebben gespeeld systematisch worden geïnventariseerd en kunnen rechterlijke beslissingen onder bepaalde voorwaarden zeer goed voorspeld worden.

14.6 Noodzakelijke kwantificering en verwetenschappelijking van recht

Met de groei van de westerse en andere economieën en de daarmee samenhangende technologische ontwikkeling en globalisering van het bedrijfsleven neemt de behoefte aan juristen niet af. Integendeel, mede als gevolg van de beperkte concurrentie in de juridische professie is het aantal juristen per hoofd van de bevolking in Nederland laag vergeleken met bijvoorbeeld de Verenigde Staten en de verwachting is gerechtvaardigd dat het aantal juristen nog sterk zal toenemen. Het inschakelen van juridische adviseurs c.q. het juridisch conflictoplossend instrumentarium door het bedrijfsleven wordt alleen maar belangrijker. Weliswaar mag worden aangenomen dat managers steeds beter gaan inzien dat juridische oplossingen als regel hoge kosten en grote onzekerheid met zich meebrengen, maar door de schaalvergroting van bedrijven zijn projecten al gauw de moeite van een juridisch conflict waard. Bovendien wordt het door de omvang van de projecten belangrijker om met betrekking tot juridische problemen preventief op te treden en in een vroegtijdig stadium, dus bijvoorbeeld al in de fase van de ontwikkeling van een nieuw produkt ook de juridische risico's te inventariseren. Bij grote vernieuwingen, bijvoorbeeld die van nieuwe geluids- en beelddragers (zoals nu de vernieuwing van de compact disk naar de digital video disk) maken de juridische complicaties een belangrijk deel uit van de problemen die opgelost moeten worden voordat het produkt grootschalig verspreid kan worden. Bij dit soort problemen, maar ook in alle andere instanties dat het bedrijfsleven

met het recht te maken krijgt, zullen aan de juridische diensten steeds zwaardere eisen gesteld worden.

Het bedrijfsleven heeft een technologisering en verwetenschappelijking doorgemaakt en het is niet waarschijnlijk dat het tot in lengte der dagen van zijn juristen een wollige of oncontroleerbare aanpak zal accepteren. Van juristen zal worden gevraagd een kwantitatieve schatting te maken van de juridische risico's en tenminste het basismateriaal te verschaffen voor het berekenen van de kosten en opbrengsten die bij verschillende scenario's kunnen worden verwacht. Het goede nieuws is, dat wanneer de gegevens van de rechtsbronnen en met name de rechtspraak meer volledig beschikbaar zijn in digitale vorm, deze kwantificering en verwetenschappelijking ook mogelijk worden. Dat wil zeggen, wanneer degenen die met die gegevens moeten omgaan zich ook de bijbehorende vaardigheden eigen maken. Tot heden schort het daar bijvoorbeeld in ons land nog behoorlijk aan en het is ook niet toevallig dat het aantal accountants, EDP-auditors en dergelijken aanzienlijk sneller is gegroeid dan het aantal advocaten - om over de bijbehorende omzetten nog maar te zwijgen. Om het nog duidelijker te zeggen: de voorspelling lijkt gerechtvaardigd dat jurimetrie - de empirische bestudering van het recht - binnen vijfentwintig jaar in of anders naast de juridische opleiding dezelfde geprononceerde plaats zal innemen als de analytisch kwantitatieve vaardigheden nu al doen in bijvoorbeeld de opleidingen bedrijfskunde en economie.

Elders is aandacht besteed aan de gevaren die internet biedt. Inbreuk op auteursrechten, opruiing, kinderporno, smaad, discriminatie, lastig vallen, openbaar maken van staatsgeheimen, illegaal gokken, financiële fraude, omzeilen van bancair toezicht, oplichting, overtreden van in- en uitvoer-verboden, bijna alles is mogelijk. Internet laat zien hoe beperkt de traditionele soevereine staat geworden is bij het bestrijden van ongewenst gedrag. Hoewel de bestaande nationale wetten in de meeste gevallen verboden op de ongewenste gedragingen inhouden wordt effectief optreden ertegen steeds moeilijker. Dit komt enerzijds doordat overheidsdienaren als regel technologisch gewoonlijk wat achterlopen, omdat binnen de overheid de druk die markt uitoefent op het bedrijfsleven om bij te blijven nu eenmaal niet aanwezig is. Met de steeds diversere technologische mogelijkheden zal die achterstand waarschijnlijk alleen maar groeien. Belangrijker is echter dat internet - dus de enorme mogelijkheden van telecommunicatie - de wereld werkelijk heeft veranderd in de zin dat territoriale grenzen steeds minder tellen. Op het territoir van de bestaande staten heeft het recht zijn loop niet meer. Wanneer men er met Kerkmeester (‘Recht en speltheorie’) vanuit gaat dat het recht althans in democratische rechtsstaten een batig saldo biedt aan algemeen nut dan ligt hierin wel degelijk een gevaar van internet.

Dit gevaar bestrijden zal onmogelijk kunnen met traditionele juridische middelen. Nog meer gedrag onrechtmatig of strafbaar verklaren is welhaast onmogelijk. Het voorbeeld van het voorgenomen verbod op cryptografie toont dat op hilarische wijze doordat juist de technologie het omzeilen van het verbod zo gemakkelijk maakt. Daar waar de technologie de controle op het verboden of te verbieden gedrag onmogelijk maakt, zullen de regels zich moeten aanpassen. Voor burgers is dat niet perse nadelig. In de onmogelijkheid om het naleven van een verbod op cryptografie af te dwingen bijvoorbeeld, is de beste garantie voor handhaving van het recht op briefgeheim gelegen. Het is ook niet zo gemakkelijk voorbeelden te bedenken dat het berusten (door de overheid) in de onmogelijkheid van handhaving van bepaalde rechtsregels voor burgers nadeel met zich meebrengt. Wel dat het vermijden van exorbitante kosten bij de handhaving tot hoge kosten bij individuele burgers leidt.

Het geschetste gevaar van internet zal moeten worden bestreden door het recht internationaler te maken. Afstemmen van nationale wetgeving en samenwerking tussen nationale rechtshandhavingsdiensten zal noodzakelijkerwijs toenemen. Ook deze veranderingen zullen de aard van het juridische ambacht en de juridische opleiding wijzigen in een meer internationale, empirisch wetenschappelijke richting. Het zal immers weinig zin hebben als staten het slechts over de *regels en normen* eens worden in die gevallen dat het *effect* daarvan van land tot land verschilt. Realiseert men zich hoezeer internet de wereld zal veranderen, dan lijkt het perspectief van veel grotere soevereine territoren en uiteindelijk de wereld één rechtsstaat onafwendbaar.

14.7 Literatuur

- Kerkmeester, H.O., ‘Recht en Speltheorie’, (diss.), Vermande, Lelystad, 1989.
- Mulder, R.V. De, ‘Een model voor juridische informatica’, (diss.), Vermande, Lelystad, 1984.
- Mulder, R.V. De, C. Wildemast en M.J. van den Hoven, ‘Conceptuele geautomatiseerde juridische documentatie-systemen’, In: Computerrecht 1993/2.
- Mulder, R.V. De, ‘Juridische begrippen en waarschijnlijkheid’, In: Computerrecht 1994/3.
- Mulder, R.V. De, ‘Toegankelijkheid van rechtspraak in de 21e eeuw; over enkele jaren dus’, In: Symposium Toegankelijkheid van Rechtspraak, Serie Rechtsvinding deel 10, J.M. van Dunné en R.J.P. Kottenhagen (red.), Gouda Quint, Arnhem, 1994.
- Mulder, R.V. De, ‘De kracht van het Internet en de zwakte van het Recht’, in: Nederlands Juristenblad 1996/41.

- Mulder, R.V. De en C.J.M. Combrink-Kuiters, 'Is a computer capable of interpreting case law?', in: Journal of Information, Law & Technology, 1996/1.
- Noortwijk, C. Van, 'Het Woordgebruik Meester. Een vergelijking van enkele kwantitatieve aspecten van het woordgebruik in juridische en algemeen Nederlandse teksten', (diss.), Vermande, Lelystad, 1995.

Rechtspraakregister

HR	23 mei 1921, NJ 1921, 564 *(Elektriciteitsarrest)*..... 19, 206
HR	NJ 1931, 226 209
HR	5 december 1930, NJ 1931, 270 *(Suikerrietplantage)* 41
HR	13 februari 1933, nj 1933, 580 (Spaarbankboekje)..... 209
HR	6 mei 1938, NJ 1938, 635 *(Caféradio)*.....37
HR	25 juni 1946, NJ 1946, 503 *(Kronen en stifttanden)* 209
HR	28 juni 1946, NJ 1946, 712 *(Van Gelder/Van Rijn)*.....33
HR	20 januari 1950, NJ 1950, 274 *(Rooilijnen)*.....40
HR	25 januari 1952, NJ 1952, 95 *(Leesportefeuille)*.....37
HR	28 juni 1957, NJ 1958, 457.....41
HR	3 november 1964, NJ 1965, 120 *(Valse sleutel)*..... 210
HR	12 juni 1970, NJ 1970, 434 *(Tomado-kleerhanger)*.....58
Octrooiraad	16 december 1970, BIE 1971, 10 *(Telefooncentrale)* 65
Hof Amsterdam	18 februari 1972, NJ 1972, 210 *(Ponskaart)*.....73
HR	19 januari 1979, NJ 1979, 412 *(Poortvliet)*.....37
Rb Assen	28 juli 1981, NJ 1982, 74 *(Bartels Software - Koerhuis)*.....67, 206
Rb Rotterdam	7 mei 1982, Cr 1984/2 *(Hanemaayer en Van Es - Burroughs)*..... 125
HR	11 mei 1982, NJ 1982, 583 *(Giraal geld)* 218

Rb Amsterdam, k.g	8 oktober 1982, BIE 1983, 100 *(Apple - CAB I)*	67
Rb Rotterdam	28 januari 1983, Cr 1987/4 *(x - y)*	125
Rb Amsterdam, k.g	24 maart 1983, BIE 1983, 101, Cr 1984/3 *(Apple - CAB II)*	67
Hof Amsterdam	31 maart 1983, AMR 1983, p. 56 *(Pac-Man - Happelaar)*	63
Octrooiraad	19 januari 1983, BIE, 1983, 104 *(Tomoscanner)*	65
Hof Arnhem	27 oktober 1983, NJ 1984, 80, Cr 1984/1 *(Computergegevens)*	19, 206, 218
HR	13 april 1984, NJ 1984, 524 *(Suske en Wiske)*	63
BGH	9 mei 1985, GRUR 1985, blz. 109 *(Inkasso)*	54
Octrooiraad	12 september 1985, BIE 1985, p. 435 *(Schakelnetwerk)*	67
Rb. Roermond	12 september 1985, RvdW 1985/6 *(Camera's)*	169
HR	11 april 1986, Cr 1986/3 *(RBC - Brinkers)*	125
HR	27 juni 1986, NJ 1987, 191, BIE 1986, 71, IER 1986, 29, Cr 1986/3*(Decca-Holland Nautic)*	16, 60
Octrooiraad	11 mei 1987, BIE 1987, 42 *(Streepjescode)*	66
Geschillencomm. Bankbedrijf	21 oktober 1987, Cr 1988/3 *(Spookopname)*	166
HR	23 oktober 1987, NJ 1988, 310 *(KNVB-NOS)*	17
HR	20 november 1987, NJ 1988, 311 *(Staat-Den Ouden)*	17
Rb Amsterdam	5 december 1988, Cr 1989/5 *(Gesprekseenheden)*	218
HR	24 februari 1989, NJ 1989, 701 *(Elvis Presley)*	17
Geschillenkamer RvT VRI	6 maart 1989, Cr 1989/5 *(Verwijdering uit register)*	139
Hof Amsterdam	13 april 1989, Cr 1989/4 *(Lensen - Automatiseringsbureau Palm)*	67
Rb Amsterdam	17 mei 1989, Cr 1990/3 *(Grafische industrie Haarlem - Oedip Nederland)*	91
Rb Den Haag	9 juni 1989, Cr 1989/4 *(Zaaksbeschadiging)*	207, 219
Ambtenarengerecht Amsterdam	28 juli 1989, Cr 1989/5 *(Wichers Hoeth - Gemeenteraad Amsterdam)*	191
Rb Breda	12 oktober 1989, Cr 1990/3, nt R.V. De Mulder *(Fotokopiëren van gegevens)*	219
Rb Haarlem, k.g	5 december 1989, Cr 1990/3 *(VNU - Speets, H & H)*	
Rb Amsterdam, k.g	14 december 1989, Cr 1990/2 *(Ondernemingsraad PTT Telecom - PTT Telecom)*	191
Geschillencomm. Bankbedrijf	24 april 1990, Cr 1990/4 *(Vermiste bankpas)*	167
Rb Alkmaar	27 april 1990, Cr 1990/5 *(Dagvaarding per fax)*	219

HR	4 januari 1991, NJ 1991, 608, RvdW 1991, 27, IER 1991, 38 nt FWG, Cr 1991/2 nt P.B. Hugenholtz *(Romme - Van Dale)* 88, 91
HR	15 januari 1991, NJ 1991, 668, Cr 1991/4, nt H.W.K. Kaspersen *(Geschrift)* 207, 219
HR	28 juni 1991, NJ 1992, 787 *(Verkerk - Bouwservice Doetinchem)* 104, 106
Rb Almelo	12 november 1991, Cr 1993/5, nt E.P.M. Thole *(Bulletin board)* 92
HR	19 november 1991, NJ 1992, 124 *(Oplichting)* 220
HR	3 december 1991, Cr 1994/5, nt R.V. De Mulder *(SWIFT)* 220
HR	21 februari 1992, NJ 1993, 164; BIE 1993, 65 *(Barbiepop I)* 17
Rb Amsterdam, k.g	24 februari 1992, BIE 1994, 83 *(Schott e.a. - Stemra e.a.)* 68
HR	28 april 1992, NJ 1992, 657, Cr 1993/3, nt R.V. De Mulder *(Geldautomaat)* 220
HR	26 mei 1992, NJ 1992, 753 *(Afluisteren fax)* 220
Rb Den Haag	27 mei 1992, BIE 1993, 61, Cr 1993/1 *(Gorter/De Vries - PTT Post)* 68
Hof Den Haag	4 juni 1992, Cr 1993/6, nt R.J.J. Westerdijk *(Verzekeringspolis)* 27
Rb Utrecht, k.g	26 november 1992, BIE 1994, 75 *(Komar - Hij Mannenmode)* 68
HR	27 november 1992, Cr 1993/1 *(Fax verzoekschrift)* 156
HR	8 december 1992, NJ 1993, 323, Cr 1993/2, nt H.W.K. Kaspersen *(Oplichting/diefstal)* 220
Hof Amsterdam	21 januari 1993, NJ 1994, 556 *(Persoonsgegevens)* 191
Hof Den Haag	1 april 1993, NJ 1994, 58, IER 1993, 16, Cr 1993/4, nt P.B. Hugenholtz *(Romme - Van Dale)* 32, 92
Hof Den Bosch	19 mei 1993, BIE 1994, 117 *(Textielfabriek Hatefa - Kwantum Nederland)* 68
Hof Den Haag	27 mei 1993, Cr 1993/4 *(Vomar - Bull)* 68
Rb Amsterdam, k.g	18 november 1993, Cr 1994/3, nt A.P. Meijboom *(Gebruikersinterface)* 69
HR	19 november 1993, Cr 1994/4 *(Stg. COVA - NMB)* 157
Hof Den Bosch	7 februari 1994, NJ 1994, 616, BIE 1994, 116, Cr 1994/2, nt E.P.M. Thole *(Broncode)* 55, 69
Hof Amsterdam	3 maart 1994, Informatierecht/AMI 1995/3 *(TV-plot)* ...69
Hof Arnhem	31 maart 1994, Cr 1994/3 nt H.W.K. Kaspersen, *(Computergegevens II)* 19, 215, 220
HR	17 mei 1994, NJ 1995, 46 (Wegnemen)..... 207, 220

Rb Utrecht, k.g	14 juni 1994, KG 1994, 263 *(Datateam - Tas Informatica)* 106
Centrale Raad van Beroep	22 juni 1994, AB 1995, 15 *(G-rekening)* 106
Hof Leeuwarden	27 september 1994, IPAS 1189-1993 *(Detachering)* 106
Hof Den Haag	1 december 1994, Informatierecht / AMI 1995 / 3 *(Privé-videocabines)* 92
HR	7 januari 1995, Informatierecht / AMI (19) 1995 / 4 *(Openbaarmaking)* 92
Rb Arnhem, k.g	24 januari 1995, Cr 1995 / 2 *(Pre-loaden)* 69
Rb Breda, k.g	20 februari 1995, Cr 1995 / 2, nt A.P. Meijboom *(De Wild - Van Genk II)* 69
Hof Den Haag	2 maart 1995, Cr 1995 / 4 *(Conversie)* 69
Rb 's-Gravenhage	7 juni 1995, Cr 1995 / 6 *(Communautaire uitputting)* 69
HR	13 juni 1995, Cr 1995 / 6, nt H.W.K. Kaspersen *(Pincode)* 221
Rb Rotterdam	24 augustus 1995, cr 1996 / 5, nt R.V. De Mulder (Bridgesoft - Lenior) 92
Rb Den Haag, k.g	12 maart 1996, Cr 1996 / 2 *(Scientology-church)* 92
HR	21 juni 1996, RvdW 1996, 145, Cr 1996 / 5, nt A.P. Meijboom *(De Wild - Van Genk)* 56, 69
Rb Haarlem	10 juli 1996, Cr 1996 / 5, nt P.B. Hugenholtz *(CD-foongids op internet)* 92

Trefwoordenregister

auteursrecht, 31
- beperkingen, 39
- beschermingsomvang, 36
- maker, 34
- rechtverkrijgenden, 38
- werk, 31
automatiseringsovereenkomsten, 95
- contractsindeling, 119
- karakteristieken, 109
- traject, 111
- wanprestatie, 114
bulletin board systemen, 78
chipsrecht, 43
- beperkingen, 45
- beschermingsomvang, 45
- rechthebbende, 44
- topografie, 44
computercriminaliteit, 204
- consequenties voor bedrijven, 216
- definitie, 205
- internet, 216
- juridische overwegingen, 209
- rol van de overheid, 210
- wet computercriminaliteit, 210
- wetshandhaving, 214
databanken, 71, 77
- aanleg, 81
- exploitatie, 87
- invoer / opslag, 84
- toestemming, 83
- uitvoer / raadpleging, 86
detachering, 94
- Arbeidsvoorzieningswet, 100
  - toepasselijkheid, 101
  - vergunning, 102
- bodyshopovereenkomst, 97
- inlenersaansprakelijkheid, 104
EDI, 141, 142
- conflictbeslechting, 153, 155, 156

- overige vereisten, 147
- rechtsgeldigheid, 145
- vormvereisten, 145
- wilsovereenstemming, 146
eigendomsbegrippen, 16
elektronisch betalingsverkeer, 158
- aansprakelijkheid, 160
- authenticiteit, 159
- bewijs, 160
- misbruik, 159
- privacy, 161
- technische oplossingen?, 163
grensoverschrijdend gegevensverkeer, 193
- aard en omvang, 194
- algemene aspecten, 195
- belangen, 197
- gegevensbescherming, 198
- Wet Persoonsregistraties, 200
- free flow of information, 200, 201
informaticarecht, 12, 22, 24, 26
informatiemaatschappij, 5
informatierecht, 23
informatietechnologie, 1
- juridische aspecten, 2
- perceptie, 10
- rechtswetenschappelijk onderzoek, 4
informatie, 13
intellectuele rechten, 29, 31, 39, 43
interchange agreement, 148
- aansprakelijkheid, 151
- beveiliging, 150
- bewaring, 152
- bewijs, 152
- gebreken en procedures, 150
- identificatie, 149
- vertegenwoordigingsbevoegdheid, 149
internet, 79
internetrecht?, 222
- internationale dimensie, 226
- internet, 223
- prestatiebescherming, 225
- technologie, 224
- toegankelijkheid rechtsbronnen, 228
- verwetenschappelijking van recht, 230
juridische informatica, 3, 21
multimedia, 71, 72
- cumulatie van regimes, 75
- digitale informatie, 72
- logistieke c.q. distributieproblemen, 75
octrooirecht, 39
- beperkingen, 42
- beschermingsomvang, 41
- rechtverkrijgenden, 42
- uitvinder, 41
- uitvinding, 40
overheidsautomatisering, 189
privacy, 168
- Europese dimensie, 174
- historische achtergrond, 171
- plaatsbepaling, 169
privacy en de overheid, 184
- bestandskoppeling, 185
- legitimatieplicht, 186
- fraudebestrijding, 187
software
- juridische kwalificatie, 17
softwarebescherming, 47
- auteursrechtelijke bescherming, 52
  - decompilatie, 57
  - geschriftenbescherming, 62
  - interoperabiliteit, 61
  - overige aandachtspunten, 63
  - prestatiebescherming, 60
  - richtlijn softwarebescherming, 52
  - softwareontwikkeling, 49
- beschermingsmogelijkheden, 48
- octrooirechtelijke bescherming, 65

- voortbrengsel-octrooi, 66
- werkwijze-octrooi, 65
Wet Persoonsregistraties, 177
- belangen van geregistreerden, 182
- materiële normen, 179
- zelfregulering, 180
zelfregulering, 127
- beroepscode voor informatici, 131
- geschillenbeslechting, 134
- minitrial, 135
- softwarecertificatie, 128

Rechtsvragen over informatietechnologie

‘Rechtsvragen over informatietechnologie’
geeft een actueel overzicht van de juridische
vraagstukken tengevolge van het gebruik van
informatietechnologie.
Per hoofdstuk wordt één vraagstuk behandeld,
zoals de juridische bescherming van software,
databanken en multimedia, detachering,
computercontracten, het elektronisch handels-
en betalingsverkeer en computercriminaliteit.
Ieder hoofdstuk wordt afgesloten met een
overzicht van relevante jurisprudentie en literatuur.

Mr P. Kleve RI (1954) heeft meer dan tien
jaar ervaring in het doceren van de juridische
vraagstukken voor (bestuurlijke) informatici,
economen, bedrijfskundigen en juristen.
Hij is verbonden aan het Centrum voor Informatica
en Recht van de Erasmus Universiteit Rotterdam
en is tevens werkzaam als consultant bij RMA
(Recht, Management en Automatisering) Marketing B.V.