

ERASMUS HOGESCHOOL
TRIERSTRAAT 84
1040 BRUSSEL

**INLEIDING TOT HET INFORMATICA-
EN TELECOMMUNICATIERECHT**

Docent: F. ROBBEN

Syllabus:
J. DUMORTIER, F. ROBBEN,
M. TAEYMANS en J. VERCRUYSSSE

Voorwoord

Deze syllabus is bestemd voor de studenten die aan de Erasmushogeschool het vak "Inleiding tot het informatica- en telecommunicatierecht" volgen. Hij is samengesteld op basis van teksten uitgewerkt door diverse medewerkers van het Interdisciplinair Centrum voor Recht en Informatica van de K.U. Leuven, waarvan de docent medeoprichter is. Aan dat centrum wordt onderzoek wordt verricht m.b.t. juridische informatica en informatica- en telecommunicatierecht. Het grootste deel van deze cursus werd overgenomen uit de syllabus opgesteld door Prof. Dr. J. Dumortier in het kader van het vak "Informaticarecht" dat in de derde licentie rechten aan de K.U. Leuven gedoceerd wordt. Delen uit deze syllabus werden geschreven of bijgewerkt door F. Robben (Wet Verwerking Persoonsgegevens, softwarebescherming), M. Taeymans (chipsbescherming, continuïteit van informaticaprojecten en de oplossing van informaticageschillen) en J. Vercruysse (informaticacontracten).

Lange tijd heeft er aarzeling bestaan om het informatica- en telecommunicatierecht als afzonderlijk vak te beschouwen. Tegenstanders waren van oordeel dat juridische aspecten van informatica en telecommunicatie best konden worden behandeld in de klassieke juridische deelgebieden zoals strafrecht, verbintenissenrecht, rechten en vrijheden, ... Dat standpunt is geleidelijk opgegeven omdat dergelijke behandeling van de materie in de andere rechtscolleges in grote mate dode letter bleef en het informatica- en telecommunicatierecht zich de facto meer en meer als discipline heeft opgedrongen. In heel wat landen, en sedert enige jaren ook in België, bestaan inmiddels specifieke universitaire onderzoekscentra op dit vlak.

Als nieuw rechtsdomein, dat nauw aanleunt bij de snel voortschrijdende technologische ontwikkeling, is het informatica- en telecommunicatierecht in permanente evolutie en expansie. Op heel wat vlakken is of was het bestaande recht niet afdoende om de juridische aspecten van de technologische evolutie gepast te regelen, en worden of zijn nieuwe regelingen uitgewerkt. De Europese Unie geeft hierbij vaak de beslissende impulsen. De confrontatie, op het einde van een onderwijscurriculum, met een rechtssdomein dat in volle uitbouw is en op Europese leest wordt geschoeid, is o.i. een zeer nuttige concrete ervaring in creatief rechtsdenken voor studenten bestuurswetenschappen.

De cursus "Inleiding tot het informatica- en telecommunicatierecht" en de bijhorende syllabus is dan ook opgevat om dergelijk oefening te ondersteunen. In de hoorcolleges wordt zoveel mogelijk gewerkt aan de hand van uitgedeelde wetteksten. Deze syllabus heeft tot doel de materies waarover deze wetteksten handelen, op een meer systematische manier toegankelijk te maken.

Het beperkte aantal lesuren dat voor het vak "Inleiding tot het informatica- en telecommunicatierecht" werd uitgetrokken laat niet toe de problematiek tijdens de hoorcolleges exhaustief of grondig te behandelen. In de geschreven syllabus wordt de materie op een meer analytische wijze beschreven, zodat de student over een uitvoerige terugvalbasis beschikt. Wel wordt verondersteld dat de basisprincipes van de klassieke rechtsdomeinen zoals burgerlijk

recht, strafrecht, ... gekend zijn; hoogstens worden ze kort in herinnering gebracht. Toch mag de syllabus zeker niet worden beschouwd als een alomvattend handboek m.b.t. het informatica- en telecommunicatierecht. De rechtstak is immers dermate in evolutie dat het uitwerken van een stabiele syllabus vooralsnog quasi onmogelijk lijkt.

Frank ROBBEN
April 1995

Inleiding

1. WAAROM "INFORMATICARECHT"?

Er is al veel inkt gevloeid over de vraag of "informaticarecht" als een aparte discipline of een autonome rechtstak mag beschouwd worden. Volgens ons moet die vraag negatief beantwoord worden. Voor de definitie van een rechtstak kan namelijk de specificiteit van het object alleen niet volstaan. Van een aparte rechtstak is slechts sprake als er een specifieke, vrij goed af te grenzen, verzameling van rechtsregels aanwezig is. In die zin is "telecommunicatierecht" eerder een aparte rechtstak dan "informaticarecht". De telecommunicatie heeft namelijk, veel meer dan de informatica, aanleiding gegeven tot een specifieke reglementering. Er zijn echter vrij weinig rechtsregels te vinden die uitsluitend met informatica te maken hebben, althans niet genoeg om er een aparte cursus aan te wijden.

"Informaticarecht" is eerder een verzamelnaam voor een heel gamma van juridische aspecten die samenhangen met de introductie van computers en - meer en meer ook - met de groeiende verwevenheid tussen computers en telecommunicatiemediën (de "telematica"). Heel vaak zijn die problemen zelfs niet nieuw. Tussen de verkoop van een computer en de verkoop van een auto bestaan geen wezenlijke juridische verschillen. Een sanctie van de Europese Commissie tegen een concurrentievervalsend gedrag op de informaticamarkt is niet essentieel verschillend van concurrentiemaatregelen in andere sectoren. In het laatste voorbeeld zitten we op het terrein van het Europees mededingingsrecht. Het eerste voorbeeld situeert zich in het verbintenissenrecht. Waarom is het dan nodig van een aparte cursus aan "informaticarecht" te wijden?

De rechtvaardiging daarvoor ligt in de volgende redenen:

- informatica en telematica zijn vrij nieuwe domeinen en daarom worden de juridische aspecten daarvan meestal in de bestaande cursussen en handboeken niet behandeld;
- informatica en telematica zijn technisch zeer complexe gebieden en de behandeling van de juridische aspecten vergt vaak enig technisch inzicht; dit inzicht ontbreekt nog bij de meeste juristen;
- informatica en telecommunicatie worden in onze samenleving als zeer belangrijke domeinen aanzien; vrijwel iedereen heeft er rechtstreeks of onrechtstreeks mee te maken; voor dergelijke "belangrijke" domeinen is een aparte juridische behandeling niet ongewoon (vergelijk met "gezondheidsrecht", "onderwijsrecht", "verkeersrecht", "milieurecht", "welzijnsrecht", "mediarecht", enz.);
- "informaticarecht" en "telecommunicatierecht" hebben zich de laatste jaren de facto geprofileerd tot min of meer specifieke disciplines; dit komt tot uiting in specifieke handboeken, tijdschriften, universitaire leerstoelen en onderzoekscentra en zelfs gespecialiseerde advocatenkantoren.

2. TERMINOLOGIE

Het is niet de bedoeling om in deze inleiding een uitgebreide lijst van gespecialiseerde termen uit de informatica en de telecommunicatie weer te geven. Hierna worden alleen enkele van de belangrijkste begrippen gedefinieerd die in deze cursus gebruikt worden: informatica, hardware, software, besturingssysteem, programmeertaal en toepassingsprogramma.

2.1. INFORMATICA

In de meest ruime zin duidt het begrip "informatica" het vakgebied aan dat zich bezighoudt met "informatiesystemen". Een informatiesysteem is een geheel van middelen waarmee de informatievoorziening op een bepaald gebied en in een bepaalde organisatorische context wordt verwezenlijkt¹. Dit geheel wordt onderscheiden in vijf componenten: apparatuur, programmatuur, personen, procedures en gegevens. Informatievoorziening is een proces waaronder zowel de invoerverwerking, de opslag, de overdracht, de bewerking, het onderhoud, de presentatie en het gebruik van informatie worden verstaan. Bij alle onderdelen van dit proces wordt gebruik gemaakt van computerapparatuur ("hardware") en van computerprogramma's ("software"). Daarom wordt het begrip "informatica" meestal vereenzelvigd met "computers". Dat is echter niet geheel correct. Zoals uit de bovenstaande definitie blijkt, dekt "informatica" een veel ruimer domein.

2.2. COMPUTERAPPARATUUR ("HARDWARE")

Onder "computerapparatuur" of "hardware" wordt meestal, naast de computer zelf, ook (een deel van) de in- en uitvoerapparatuur verstaan. De computer zelf is een elektronisch apparaat, waarvan een verwerkingseenheid (één of meer "processoren") en het intern geheugen de centrale elementen uitmaken.

De verwerkingseenheid is de centrale "motor" van de computer. Hier worden alle bewerkingen uitgevoerd. Bij de meest eenvoudige computers bestaat de verwerkingseenheid uit één enkele processor. In dat geval worden alle bewerkingen één na één verricht. Uitvoering van gelijktijdige bewerkingen is onmogelijk. Daarom wordt vaak met meer dan één processor gewerkt. De snelheid waarmee de processor bewerkingen kan uitvoeren en het aantal processoren is bepalend voor de snelheid van de computer.

Naast de computer zelf, is er steeds invoer- en uitvoerapparatuur nodig. Typische invoerapparaten zijn het toetsenbord (klavier), de "muis", de "sensor" (bijv. in een alarminstallatie of een robot), de microfoon (voor geluidsverwerking), de camera (voor beeldverwerking), de tekstscanner, enz. Voorbeelden van uitvoerapparaten zijn: het beeldscherm, de schijf ("disk" of

¹ Franken, H., e.a., Informatietechnologie en recht. Rapport van de tijdelijke adviescommissie Informatietechnologie en Recht met betrekking tot de opzet van onderzoek op het gebied van informatietechnologie en recht, Lelystad, Koninklijke Vermande, 1991, p. 9.

"diskette"), de band ("tape"), de CD-ROM, de "printer". Vaak kan een apparaat zowel voor de invoer als voor de uitvoer gebruikt worden. Dat is meestal het geval voor de schijf of de band. Gegevens worden van de schijf of de band "gelezen" om door de computer te worden bewerkt (invoer), en vervolgens, na de bewerking, op dezelfde schijf of band "geschreven" om te worden bewaard (uitvoer).

2.3. COMPUTERPROGRAMMATUUR ("SOFTWARE")

Een computerprogramma is een geheel van instructies aan de computer, waarmee aangegeven wordt welke bewerkingen de computer moet uitvoeren. We onderscheiden daarbij verschillende niveaus.

De computer zelf is een apparaat dat enkel gehoorzaamt aan elektronische impulsen. Op het niveau van de computer zelf (het machine-niveau) is een programma dus een aaneenschakeling van elektronische impulsen. Typisch voor de hedendaagse computers is dat de programma's met slechts twee soorten impulsen werken ("positief" en "negatief", of "1" en "0"). Ze werken m.a.w. met een "binaire" ("bi-" duidt op "twee") codetaal. Een eenvoudig computerprogramma bestaat al snel uit een paar miljoen binaire machine-instructies ("bits"). Op dit "machineniveau" wordt het programma ook wel "objectcode" genoemd.

Omdat het menselijk gesproken ondoenbaar zou zijn om een computer te programmeren op machineniveau, werkt de mens met de computer op een hoger niveau. Programma's worden geschreven in een vorm die min of meer hanteerbaar is voor de mens en daarna vertaald in objectcode. De taal waarin de mens computerprogramma's schrijft noemt men "hogere programmeertaal". Op dit "menselijk" niveau spreekt men ook wel van "broncode" of "source code". Dit is dus het programma in "mensentaal". De vertaling van het programma in "machinetaal" gebeurt door een soort vertaalprogramma. Men spreekt over "vertalen" of "compileren".

2.4. BESTURINGSSYSTEEM

Het besturingssysteem is een programma dat een aantal zeer elementaire instructies voor de computer bevat. Het is een programma waar men altijd beroep op doet, wat men ook met de computer wil uitvoeren. Het is dus een soort "basisprogramma". Zonder dit basisprogramma zou de computer niet weten hoe hij aan een ander programma zou moeten beginnen. Het besturingssysteem zorgt ervoor dat de computer de meest elementaire instructies begrijpt en maakt de computer op die manier voor de mens "toegankelijk". Als men de computer start, staat het besturingssysteem automatisch klaar. Via het besturingssysteem kan de mens dan bijvoorbeeld de computer een bepaald toepassingsprogramma laten uitvoeren of een zelf geschreven programma "compileren". Het besturingssysteem wordt in het jargon "operating system" genoemd. Voorbeelden van besturingssystemen zijn "DOS" (Disk Operating System), "UNIX" of "OS/2".

2.5 PROGRAMMEERTAAL

Een programma wordt steeds geschreven in een (hogere) programmeertaal. Een programma bestaat uit een geheel van instructies die aan de computer gegeven worden om een bepaald probleem op te lossen. In de loop van de (korte) informaticageschiedenis zijn al heel wat programmeertalen ontwikkeld.

Een voorbeeld van een eenvoudig programma ziet er als volgt uit:

```
PROGRAM Som_van_positieve_getallen (input, output);  
{inlezen van een aantal niet negatieve gehele getallen}  
{gevolgd door een negatief getal;}  
{bepalen en neerschrijven van de som van die getallen}
```

```
VAR getal, som : integer;
```

```
BEGIN  
    som := 0;  
    read(getal);  
    WHILE getal >= 0 DO  
        BEGIN  
            som:= som + getal;  
            read(getal)  
        END;  
    write(som)  
END
```

Het bovenstaande programma is geschreven in de programmeertaal "PASCAL" . Het maakt de som van een reeks positieve getallen. Het aantal getallen is niet vooraf gekend. Daarom wordt aan het einde van de reeks een willekeurig negatief getal geplaatst als signaal. De computer weet dan dat hij met optellen moet stoppen.

Op de eerste lijn worden twee "variabelen" gedefinieerd. Men zegt dus aan de computer dat hij twee adressen moet reserveren met de namen "getal" en "som". In de loop van het programma zal de waarde van de variabelen wijzigen. In het begin staat "som" op nul (som := 0). Dan wordt een eerste getal ingetikt op het toetsenbord. De computer moet dat getal lezen en het in de variabele "getal" stoppen. Als de gebruiker bijv. het getal "345" heeft ingetikt, dan heeft de variabele "getal" op dat moment de waarde "354". Dan test men of het getal groter is dan nul (getal >= 0). Als dat het geval is, telt men de waarde van "som" (op dat moment nog nul) bij die van "getal" (345). De uitkomst zet men in de variabele "som". Vervolgens wacht het programma op het volgende getal. Zo gaat men door tot de gebruiker een negatief getal intikt.

2.6. TOEPASSINGSPROGRAMMA

Aan de hand van een programmeertaal zoals "PASCAL" wordt een toepassingsprogramma geschreven. Toepassingsprogramma's, ook wel "applicatieprogramma's" of eenvoudigweg "applicaties" genoemd, zijn programma's die een specifieke functie voor de mens vervullen, bijvoorbeeld tekstverwerking, gegevensbeheer of boekhouding. Men kan toepassingsprogramma's schrijven "op maat" of standaardprogrammapakketten maken. Een programma "op maat" wordt voor één of meer gebruikers op bestelling gemaakt, zoals een maatpak. De meeste computergebruikers gebruiken echter "prêt-à-porter" standaardprogrammatuur. Voorbeelden van standaardpakketten op dit niveau zijn WordPerfect (tekstverwerking), Lotus 1-2-3 (rekenblad), dBaseIV (gegevensbeheer) en Harvard Graphics (tekenprogramma).

3. BRONNEN VAN HET INFORMATICARECHT

Hierna geven we een lijst van enkele belangrijke handboeken en tijdschriften op het gebied van het informaticarecht. Literatuur over specifieke problemen of deelgebieden uit het informaticarecht komt niet hier aan bod, maar wordt telkens bij het betrokken hoofdstuk aangeduid.

3.1. HANDBOEKEN

Er bestaat (nog) geen goed Belgisch handboek over informaticarecht. Wel verscheen enkele jaren geleden een zeer fragmentair en wat oppervlakkig Franstalig boekje van P. Glineur, "Droit et Ethique de l'Informatique", Brussel, Story, 1991.

Voor Nederland is momenteel het verzamelwerk "Recht en Computer" uit de "Serie recht en praktijk" van Kluwer, Deventer aan te bevelen. Het bevat bijdragen van een vijftiental Nederlandse professoren en assistenten die op het gebied van het informaticarecht bedrijvig zijn.

In Frankrijk is vooral "Lamy Droit de l'Informatique" van belang. Het is zeer volledig en actueel. Elk jaar verschijnt een nieuwe editie. Daarnaast zijn er ook de handboeken van H. Maisl & J. Huet (Droit de l'Informatique et des Télécommunications, Parijs, Litec, 1989) en A. Lucas (Droit de l'Informatique, Parijs, PUF, 1987).

3.2. REEKSEN

De meest uitgebreide Nederlandstalige boekenreeks over informaticarecht is de reeks "Recht en Informatica" die door Kluwer wordt uitgegeven. De reeks bevat momenteel een veertiental monografieën over o.m. softwarebescherming, computercriminaliteit, computerverzekeringen en elektronisch betalingsverkeer. Naast deze reeks moet ook de onlangs gestarte reeks van het ICRI (Brugge, Die Keure) vermeld worden. In deze reeks worden de verslagen van de studiedagen van ICRI, onderzoeksrapporten en cursussen gepubliceerd. Behandelde thema's zijn bijvoorbeeld informaticageschillen, privacybescherming en EDI.

In het Franstalig landsgedeelte is vooral de reeks "Cahiers du CRID" belangrijk (Story Scientia). In deze reeks verschijnen o.m. reeds boeken over bewijsrecht, elektronische betaalkaarten, juridische bescherming van databanken, software-onderhoudscontracten, telecom-municatiereglementering en overheidsopdrachten inzake software.

Tenslotte moeten we ook de internationale Engelstalige "Computer/Law Series" vermelden (Kluwer Law and Taxation).

3.3. TIJDSCHRIFTEN

Het belangrijkste Nederlandstalig tijdschrift op het hier besproken domein is "Computerrecht". Het tijdschrift bevat vooral bijdragen over Nederland, maar sinds enkele jaren wordt een inspanning gedaan om meer bijdragen uit België op te nemen.

De Franstalige tegenhanger van "Computerrecht" is het Belgo-Franse tijdschrift "Droit de l'Informatique et des Télécommunications".

Verder zijn er ook gespecialiseerde Duitse (o.m. "Computer und Recht"), Britse (o.m. "Computers and Law") en Amerikaanse (o.m. "Software Law Journal", "Rutgers Journal of Law and Technology", "International Journal of Law and Information Technology", "Harvard Law and Technology Review", "The Computer Lawyer", "Santa Clara Computer and High Technology Law Journal", e.a.) tijdschriften.

4. STRUCTUUR VAN DE CURSUS

De cursus "Inleiding tot het informatica- en telecommunicatierecht" bestaat uit vijf hoofdstukken:

- de regulering van de informaticamarkt;
- de bescherming van de persoonlijke levenssfeer bij de verwerking van persoonsgegevens;
- de bestaande wetgeving van informaticacriminaliteit
- informatica en contractenrecht;
- telecommunicatierecht.

Hoofdstuk 1 De regulering van de informaticamarkt

Het eerste deel van deze cursus handelt over de regulering van de informaticamarkt. Daarin onderscheiden we drie onderdelen:

- inleiding tot de informaticamarkt;
- regulering via het Europees mededingingsrecht;
- regulering via het intellectueel eigendomsrecht.

1. INLEIDING IN DE INFORMATICAMARKT

Om een inzicht te krijgen in de informaticamarkt maken we best een onderscheid tussen:

- de markt voor computerapparatuur (hardwaremarkt);
- de markt voor computerprogramma's (softwaremarkt);
- de markt voor informaticadiensten.

1.1. HARDWAREMARKT

In de hardwaremarkt wordt meestal een onderscheid gemaakt tussen:

- computers;
- computeronderdelen (componenten, vooral chips);
- randapparaten (bv. printers).

Computers worden vaak ingedeeld in vier categorieën:

- grote systemen ("mainframes");
- departementale systemen (minicomputers);
- werkstations (krachtige individuele computers);
- persoonlijke computers (microcomputers)

Mainframes zijn grote computersystemen waarmee honderden gebruikers tegelijk kunnen werken via een netwerk van "terminalen" (een beeldscherm plus een klavier). Mainframes treffen we aan in grote organisaties: grote banken, verzekeringsmaatschappijen, universiteiten, openbare instellingen, enz... . De beeldschermen in de faculteitsbibliotheek van de K.U. Leuven bijvoorbeeld zijn gekoppeld aan de mainframe van de K.U. Leuven, die in het Universitair Rekencentrum in Heverlee staat. Elke student die de geautomatiseerde bibliotheekcatalogus (LIBIS) gebruikt, werkt in feite rechtstreeks met een mainframecomputer. Soms zijn de gebruikers op grote afstand van de mainframecomputer. Dat is bijvoorbeeld het geval voor studenten die LIBIS gebruiken in de bibliotheek van de universitaire campus van de K.U. Leuven in Kortrijk. Een ander voorbeeld: de elektronische bankterminalen (Bancontact, Mister Cash, Postomat) zijn eveneens terminalen die op een mainframecomputer zijn aangesloten.

Er zijn niet zoveel mainframeconstructeurs. De absolute marktleider is IBM. De belangrijkste Europese constructeurs van mainframes zijn het Duitse Siemens en het Franse Bull.

Minicomputers worden gebruikt in kleinere organisaties of op het departementaal niveau van grote organisaties. Het zijn machines waarmee gewoonlijk enkele tientallen gebruikers tegelijk kunnen werken. Ook in deze sector is IBM de belangrijkste constructeur. Andere belangrijke firma's op deze markt zijn Digital Equipment Corp. (DEC), Unisys, Wang en Hewlett-Packard.

Werkstations zijn krachtige computers voor individueel professioneel gebruik. Hun succes was aanvankelijk vooral te danken aan de grafische mogelijkheden. Dat is vooral belangrijk voor beroepen als architecten of ingenieurs. Een bekende constructeur van werkstations is de Amerikaanse firma Sun.

Tenslotte zijn er de "personal computers". Het gaat om een relatief jong fenomeen. De eerste PC's, o.m. van Apple, zijn op het einde van de zeventiger jaren op de markt verschenen. De IBM PC werd in 1981 op de markt gebracht, en werd meteen als een feitelijke standaard beschouwd en door de meeste andere constructeurs geïmiteerd. Men maakt dus meestal "IBM-compatibele" PC's. Deze computers gebruiken de INTEL-processor en het besturingssysteem DOS. Slechts enkele constructeurs bleven hun eigen weg gaan. De bekendste voorbeelden zijn Apple en Atari. De hevige concurrentiestrijd op de markt van de personal computers geeft echter steeds weer aanleiding tot nieuwe evoluties en allianties.

De produktie van computers in de Europese Unie dekt slechts twee derden van de interne vraag. Ruim 60 % van de Europese computemarkt is in handen van Amerikaanse bedrijven. Dat is niet verwonderlijk. Als men de lijst bekijkt van de tien grootste computerconstructeurs, vindt men daarbij vier Amerikaanse (IBM, Unisys, DEC en HP), drie Japanse (Fujitsu, NEC en Hitachi) en drie Europese bedrijven (Siemens, Olivetti en Bull). De omzet van IBM op de Europese computemarkt is echter groter dan de gezamenlijke omzet van de vier grootste Europese constructeurs (Siemens, Olivetti, Bull en Philips). Bovendien zijn ruim 60 % van de Europese computerconstructeurs onder Amerikaanse controle. De informaticabranche van Philips bijvoorbeeld werd enige tijd geleden overgenomen door DEC.

Op de markt van de computeronderdelen is het Japanse overwicht zeer groot. Voor de actieve componenten (vooral chips) had Japan in 1990 een wereldmarktaandeel van 49,5 %, tegen 36,5 % voor de Verenigde Staten en 10 % voor de Europese Unie. Bijna 90 % van de geheugenchips zijn van Japanse makelij (NEC, Toshiba, Hitachi, Fujitsu, Mitsubishi). De Amerikaanse producenten overheersen de markt van de processorchips (Intel, Motorola). De belangrijkste Europese chipsproducenten zijn Philips (inmiddels overgenomen door DEC), SGS-Thomson en Siemens. Hun gezamenlijke omzet is echter kleiner dan die van de tweede grootste Japanse chipsproducent (Toshiba).

Ook randapparatuur (printers, beeldschermen, schijven, ...) wordt voor een groot deel door Japanse firma's op de markt gebracht (ongeveer 40 %). Het aandeel van de Verenigde Staten is ongeveer 25 % en dat van de Europese Unie nauwelijks 15 %.

Naast conjuncturele factoren (de lage koersen van de dollar en de yen) liggen vooral structurele

factoren aan de basis van de zwakke positie van de Europese Unie op de computerhardwaremarkt. De Europese bedrijven zijn nog sterk gehinderd door de fragmentatie van de Europese markt in kleine nationale deelmarkten. Globale strategieën op wereldschaal werden veel later ontwikkeld dan bij de Amerikaanse en Japanse concurrenten. De schaalvergroting via o.m. concentraties en samenwerkingsverbanden kwam in Europa eveneens zeer laat op gang (o.m. de overname van Nixdorf door Siemens, de controle over Honeywell en Zenith door Bull).

1.2. SOFTWAREMARKT

De markt voor computerprogrammatuur kan onderverdeeld worden in drie segmenten:

- besturingssystemen;
- standaardprogrammatuur;
- maatprogrammatuur.

Aanvankelijk bouwde elke computerproducent machines met een eigen besturingssysteem. Er was geen enkele standaard. Dat gold niet alleen voor de mainframemarkt, maar ook voor de minicomputers en de PC-markt.

In de tachtiger jaren is op de PC-markt het besturingssysteem DOS van de Amerikaanse firma Microsoft de feitelijke standaard geworden. De reden was dat dit besturingssysteem werd uitgekozen door IBM, toen in 1981 de IBM-PC werd gelanceerd. Sinds enkele jaren probeert IBM met eigen besturingssysteem (OS/2) het overwicht van Microsoft-DOS te doorbreken maar het heeft daarbij weinig succes. DOS is als besturingssysteem weliswaar niet zeer gebruikersvriendelijk. Microsoft probeerde daaraan echter te verhelpen door de lancering van een "interfaceprogramma" (Microsoft-Windows). Een interfaceprogramma als Microsoft-Windows vormt een soort "dashboard" tussen de gebruiker en het besturingssysteem. De computer-eindgebruiker wordt niet meer rechtstreeks met het onvriendelijke besturingssysteem geconfronteerd (het is transparant, onzichtbaar geworden), maar communiceert met de computer via een gebruikersvriendelijk grafisch "gebruikerspaneel". Programma's als Microsoft-Windows worden in het jargon "grafische user-interfaces" genoemd. Over deze "grafische user-interfaces" (GUI's) is in de Verenigde Staten veel rumoer ontstaan n.a.v. de juridische betwistingen over het auteurschap daarvan (bijv. Apple vs. Microsoft). De hevige concurrentiestrijd op de markt van de personal computers wordt ook uitgevochten op het domein van de besturingssystemen. Samen met de processorchip en de zgn. busarchitectuur (de wijze waarop intern in de computer gegevens worden doorgegeven naar randapparatuur), is het besturingssysteem immers een zeer centraal element in de computer. Verschillende firma's, waaronder IBM en Microsoft, kondigen nieuwe besturingssystemen aan, die wellicht in de volgende jaren DOS zullen vervangen.

Op de markt van de minicomputers wordt met wisselend succes naar een gemeenschappelijk besturingssysteem gestreefd. De keuze is uiteindelijk op UNIX (van het Amerikaanse AT&T) gevallen. Voorlopig hanteren de grote constructeurs echter nog hun eigen versie van UNIX (bijv. IBM met AIX, SUN met Solaris, Siemens met SINIX) en is UNIX nog niet echt een standaard. Op de markt van de mainframes staat men met de standardisering nog nergens. Elke

mainframeconstructeur behoudt voorlopig nog zijn eigen besturingssysteem.

Standaardsoftware zijn programmapakketten die in grote aantallen worden vermenigvuldigd en als produkt op grote schaal worden verkocht. Men spreekt daarom ook soms van "toonbankprogramma's". Ze bestaan voor de meest uiteenlopende toepassingen. De bekendste zijn:

- tekstverwerking (WordPerfect, Microsoft Word, Lotus AmiPro, ...);
- gegevensverwerking (Oracle, Informix, Ingres, dBaseIV, Filemaker, SAS, ...);
- rekenblad (Lotus 1-2-3, Microsoft Excel, Quattro Pro, Supercalc, ...);
- grafisch werk (Powerpoint, Harvard Graphics, Freelance Plus, GEM, CorelDraw, ...);
- desktop publishing (Pagemaker, Ventura, Aldus Persuasion, ...);
- communicatie (Crosstalk, Procomm Plus, PC Anywhere, Carbon Copy, ...).

De grootste producenten zijn bijna allemaal Amerikaanse bedrijven. De vier belangrijkste daaronder zijn Microsoft, Novell (dat o.m. WordPerfect en Borland opslokte), Computer Associates en Lotus Development.

De situatie van de Europese softwarebedrijven is iets beter op de markt van het "maatwerk". Bekende Europese bedrijven zijn Cap Volmac, Sema Group, Logica e.a.

1.3. INFORMATICA DIENSTEN

Naast apparatuur en programmatuur wordt op de informaticamarkt een zeer brede waaier van diensten aangeboden:

- expertise (bv. advies bij automatiseringsprojecten);
- organisatie (bv. coördinatie bij grote projecten);
- analyse (ter voorbereiding van softwareontwikkeling);
- communicatie (transport van gegevens via netwerken);
- personeel (bv. hulp bij aanwerving van informatici);
- beveiliging (uitwijkcentra, escrowbedrijven, e.a.);
- verzekering (specifieke polissen voor informaticarisico's);
- onderhoud (zowel hardware- als softwareonderhoud);
- opleiding (opleidingsinstituten, cursussen, conferenties);
- financiering (financiering van informatica-investeringen);
- informatiediensten (ter beschikking stellen van databanken);
- enz.

Het is vooral op deze markt dat een groot aantal kleine bedrijven actief zijn.

1.4. TRENDS

De belangrijkste trends op de informaticamarkt van de negentiger jaren zijn de volgende:

- globalisatie (internationalisering): zowel hardware- als softwareproducenten opereren op wereldschaal; de indeling in nationale markten vervaagt; dat heeft grote gevolgen voor de juridische problemen op informaticagebied;
- open systemen: informaticasystemen bestaan uit componenten van verschillende oorsprong; alles moet aan alles gekoppeld moeten worden; constructeurs moeten met elkaars specificaties rekening houden; deze noodzaak heeft directe gevolgen voor o.m. de toepassing van het concurrentie- en het intellectueel eigendomsrecht;
- samenwerking: de kosten voor onderzoek en ontwikkeling zijn voor moderne informatieproducten (vooral voor chips en voor besturingssystemen) zó hoog geworden dat individuele firma's die kosten niet meer alleen kunnen dragen; er ontstaan samenwerkingsverbanden, zelfs tussen de grootste concurrenten (bv. Apple en IBM);
- miniaturisering: computers worden kleiner en krachtiger; men spreekt van het einde van de mainframe; de computer wordt een werktuig dat men overal met zich mee kan dragen; in die kleine zakcomputer worden nieuwe technieken geïntegreerd zoals schriftherkenning (de "pencomputer") en communicatiefaciliteiten (integratie van zakcomputer en mobiele telefoon tot "personal communicator");
- netwerken: de computer wordt meer en meer een instrument om te communiceren; er worden lokale netwerken opgezet in bedrijven om gegevens, programma's en randapparaten gemakkelijk te kunnen delen; via publieke netwerken kunnen computers op grote afstand met elkaar in verbinding treden en grenzen en oceanen overbruggen;
- popularisering: de computer wordt een instrument dat stilaan in alle huishoudens doordringt en ingezet wordt voor allerlei dagelijkse behoeften: financiële verrichtingen, interactieve televisie, reserveringen, informatiediensten, e.a.; de bediening wordt zeer eenvoudig en transparant;
- multimedia: de computer wordt een instrument waarmee niet alleen meer tekst en cijfers worden gemanipuleerd maar in toenemende mate ook beeld en geluid; men spreekt van "multimediale" toepassingen.

2. REGULERING VIA HET EUROPEES MEDEDINGINGSRECHT

De belangrijkste bepalingen op het vlak van het Europees mededingingsrecht zijn de artikelen 85 en 86 van het Verdrag van Rome.

2.1. ARTIKEL 85 VAN HET EEG-VERDRAG

Artikel 85 verbiedt alle overeenkomsten tussen ondernemingen, alle besluiten van ondernemingsverenigingen en alle onderling afgestemde feitelijke gedragingen die de handel tussen de Lid-Staten ongunstig kunnen beïnvloeden en ertoe strekken of tot gevolg hebben dat de mededinging binnen de gemeenschappelijke markt wordt verhinderd, beperkt of vervalst. Dergelijke overeenkomsten zijn van rechtswege nietig. De Europese Commissie kan echter

onder bepaalde voorwaarden vrijstellingen verlenen. Via de toepassing van artikel 85 heeft de Commissie reeds herhaaldelijk ingegrepen op de informaticamarkt. De ingrepen betroffen zowel verticale overeenkomsten, als samenwerkingsakkoorden (horizontale overeenkomsten) en licentiecontracten.

2.1.1. Verticale overeenkomsten

Verticale overeenkomsten zijn overeenkomsten tussen bedrijven die zich in een verschillend stadium van het economisch proces van productie en distributie bevinden. Een typevoorbeeld is de overeenkomst tussen een producent en een verdeler. Ook de zogenaamde agentuurovereenkomst is een verticale overeenkomst. Een voorbeeld daarvan zou de overeenkomst zijn waarbij een automatiseringsbedrijf de computerapparatuur niet zelf levert, maar voor dat onderdeel van het informaticaprojekt een agent, gespecialiseerd in de verdeling, installatie en onderhoud van hardware inschakelt. In een bekendmaking van 1962 heeft de Europese Commissie zuivere agentuurovereenkomsten van de toepassing van artikel 85 uitgesloten.

Horizontale overeenkomsten worden daarentegen gesloten tussen bedrijven die elkaars concurrenten zijn.

De meest bekende toepassingen van artikel 85 inzake verticale overeenkomsten, gaan over de distributie-overeenkomst. De vraag of een distributie-overeenkomst onder het verbod van artikel 85 valt, hangt vooral af van de vraag of de betrokken contracterende bedrijven hun commerciële vrijheid beperken.

Voor alleenverkoopovereenkomsten, waarbij een leverancier overeenkomst om op een bepaald grondgebied maar aan één enkele verdeler te verkopen, geldt een algemene vrijstelling. Er zijn echter enkele voorwaarden: zo mag in de overeenkomst bijvoorbeeld geen verbod van parallelinvoer opgenomen zijn (waarbij een andere handelaar via een ander kanaal dan de exclusieve verdeler het produkt invoert). Evenmin zijn uitvoerverboden toegestaan, waarbij de exclusieve verdeler belooft nooit buiten het grondgebied te zullen verkopen. Ook prijsafspraken blijven verboden.

In de zaak ICL/Fujitsu heeft de Europese Commissie zich uitgesproken over de vraag of een "OEM"-overeenkomst als een alleenverkoopovereenkomst kon beschouwd worden. Bij "Original Equipment Manufacturing"-overeenkomsten, wordt overeengekomen dat het OEM-bedrijf produkten van de andere contractpartij mag verkopen onder eigen merknaam. In casu kocht het Britse ICL computers van Fujitsu en verkocht ze alsof het ICL-produkten betrof. ICL mocht deze computers echter uitsluitend binnen een bepaald grondgebied verkopen en Fujitsu verbond zich om binnen het Verenigd Koninkrijk enkel computers aan ICL te leveren. Volgens de Commissie was dit geen alleenverkoopovereenkomst omdat ze niet uitsluitend "verkoop" betrof.

Een andere zaak m.b.t. de informaticamarkt betrof het selectieve distributiesysteem voor de IBM-PC. Enkel "erkende dealers", die voldeden aan door IBM vastgestelde kwalitatieve criteria,

kregen het recht om de IBM-PC te verdelen. De criteria hadden te maken met de materiële infrastructuur, de opleiding van het personeel en de financiële situatie. IBM voerde aan dat een dergelijke selectie noodzakelijk was om deskundig advies en goede service voor de klanten te waarborgen. De Europese Commissie stemde daarmee in. Ze oordeelde dat de criteria van IBM objectief werden toegepast en geen discriminatie als gevolg hadden. Bovendien vond de Commissie dat de technische complexiteit van de betrokken produkten, nl. personal computers, een selectief distributiesysteem rechtvaardigden.

De tegenhanger van de alleenverkoopovereenkomst is de exclusieve afname-overeenkomst, waarbij een verdeler belooft om zich uitsluitend bij een bepaalde producent te bevoorraden. Dergelijke overeenkomsten zijn eveneens onder bepaalde voorwaarden toegestaan, als de maximum looptijd niet langer is dan vijf jaar en de betrokken produkten met elkaar verband houden.

Tenslotte heeft de Commissie zich ook al dienen uit te spreken over de toelaatbaarheid van franchise-overeenkomsten. Zo werd een vrijstelling verleend in de beschikking m.b.t. Computerland. De franchisenemers van Computerland verkopen personal computers en toebehoren van uiteenlopende merken, en gebruiken de naam, de opleidingsfaciliteiten, de technische en commerciële know-how en de naverkoopdiensten van Computerland. Een franchisenemer kan echter binnen een bepaalde geografische zone maar één verkooppunt openen en hij mag ook enkel aan eindgebruikers verkopen. Ondanks deze concurrentiebeperkingen oordeelde de Commissie dat het systeem de kwaliteit van de distributie en de belangen van de consument diende. Een jaar later, in 1988, werd voor de meeste franchise-overeenkomsten een generieke vrijstelling verleend.

2.1.2. Horizontale overeenkomsten

Voor bepaalde horizontale overeenkomsten, met name deze m.b.t. specialisatie en onderzoek & ontwikkeling, heeft de Commissie generieke vrijstellingen verleend. In een specialisatie-overeenkomst spreken de contracterende bedrijven af dat ze de gespecialiseerde produkten van de andere partij niet zullen produceren. Er worden dus specialisatiegebieden afgesproken. Bij R&D-overeenkomsten spreken de ondernemingen af dat ze samen aan onderzoek en ontwikkeling zullen doen en/of hoe ze de resultaten van gemeenschappelijk onderzoek en ontwikkeling zullen exploiteren. Een voorbeeld daarvan is de recente overeenkomst tussen IBM en Bull. IBM heeft een leidinggevende positie inzake de nieuwe RISC-technologie (RISC of "Reduced Instruction Set Computing" is een techniek waarbij alle instructies van de processor dezelfde lengte hebben; RISC-processoren hebben dus een "gereduceerd" opdrachtenrepertoire en kunnen daarom gemakkelijker geoptimaliseerd worden). Bull heeft een sterke reputatie inzake multiprocessoren (computers met meer dan één processor). Beide bedrijven hebben nu afgesproken om hun R&D-activiteiten op deze punten te bundelen, maar zullen de resultaten afzonderlijk en vrij in hun eigen produkten mogen integreren.

Naast de generieke vrijstellingen heeft de Commissie in een aantal gevallen ook individuele

ontheffingen op het verbod van artikel 85 EEG-Verdrag verleend aan informaticabedrijven.

De belangrijkste beschikking is deze over X/Open Group. Een groot aantal bedrijven, waaronder Bull, DEC, ICL, Olivetti, Siemens en Unisys (toen nog Sperry Corp.), sloten een overeenkomst met het oog op de ontwikkeling en invoering van een standaard-interface voor toepassingsprogrammatuur onder het UNIX-besturingssysteem. Normaliter worden toepassingsprogramma's geschreven voor een bepaald besturingssysteem. Een toepassingsprogramma dat geschreven is voor een bepaald besturingssysteem kan dus niet gebruikt worden met een ander besturingssysteem. Besturingssystemen, zeker bij mainframes en in mindere mate bij minicomputers, verschillen van constructeur tot constructeur. Wie dus een programma schrijft voor een IBM-computer kan dat programma niet kwijt aan de eigenaars van een Siemens-computer. Hoger zagen we reeds dat met UNIX gestreefd wordt naar een gestandaardiseerd besturingssysteem dat "constructeur-onafhankelijk" is en derhalve op machines van verschillende merken zou kunnen worden gebruikt. Dit is de beweging naar "open systemen". Voor softwareproducenten betekent dit dat ook de toepassingsprogramma's op machines van uiteenlopende oorsprong en architectuur zullen kunnen gebruikt worden. In de X/Open Groep proberen een aantal bedrijven tot afspraken te komen over de "interface" (het "dashboard") van deze toepassingsprogramma's. Hoe eenvormiger de interface, hoe gemakkelijker de eindgebruiker - net als bij een automobiel - van het ene naar het andere programma zal overschakelen. Dat laatste overtuigde de Europese Commissie om voor de betrokken overeenkomst een ontheffing te verlenen.

In de beschikking inzake Olivetti/Canon ging het over een gemeenschappelijke dochteronderneming ("joint venture"). De bedoeling daarvan was de gezamenlijke productie van kopieerapparaten, facsimile's en laserprinters. De Commissie oordeelde dat deze gezamenlijke dochteronderneming de mededinging beperkte en de handel tussen de Lid-Staten ongunstig beïnvloedde. Olivetti en Canon waren immers concurrenten op de markt van kopiëerapparatuur. Toch verleende de Commissie een tijdelijke ontheffing voor 12 jaar op grond van het motief dat de samenwerking de investeringskosten verminderde, daarom kostenverlagend werkte en dus uiteindelijk ten goede kwam aan de gebruiker.

Bij de beoordeling van horizontale overeenkomsten moet men ook rekening houden met de nieuwe Europese Verordening over de controle van concentraties, die op 21 september 1990 in werking is getreden. Als voorbeelden van goedgekeurde concentraties op de informaticasector worden meestal de overeenkomst tussen General Electric en Siemens met het oog op de overname van Plessey, en de participatie van 80 % van Fujitsu in het Britse ICL in 1990 geciteerd.

2.1.3. Licentie-overeenkomsten

Bij een licentie-overeenkomst geeft de rechthebbende van een intellectueel recht het gebruiksrecht over aan een derde. Dergelijke overeenkomsten vallen in principe onder de toepassing van artikel 85 EEG-Verdrag. De Commissie heeft echter via verordeningen generieke vrijstellingen verleend voor het in licentie geven van know how en voor octrooilicenties.

Hierna zullen we zien dat computerprogramma's echter beschermd worden door het auteursrecht. Daarvoor is er geen algemene vrijstelling. Dat wil niet zeggen dat de normale uitoefening van een softwarelicentie door artikel 85 EEG-Verdrag verboden zou zijn. Daarvoor is het nodig dat de concurrentie beperkt en de handel tussen de Lid-Staten ongunstig beïnvloed wordt. Zo zou bijvoorbeeld een licentie met een exportverbod of een "tying arrangement" (het koppelen van een licentie aan de verplichting om ook een licentie op een ander produkt te nemen) niet toegelaten zijn. Over softwarelicenties waarbij het gebruik van de software beperkt wordt tot een bepaalde computer, is door de Nederlandse rechter aan het Europees Hof van Justitie in 1991 een prejudiciële vraag gesteld n.a.v. de zaak Bull vs. Vomar Voordeelmarkt. Vomar wilde de software die door Bull was geleverd, van haar oude Bull-machine overplaatsen naar een nieuw aangekochte IBM-mainframe. Bull verzocht de rechter om Vomar te bevelen met deze conversie te stoppen. Het Europees Hof zal zich nu over de toepassing van artikel 85 EEG-Verdrag in dergelijke kwesties moeten uitspreken.

2.2. ARTIKEL 86 VAN HET EEG-VERDRAG

Artikel 86 EEG-Verdrag verbiedt het misbruik van een economische machtspositie op de gemeenschappelijke markt of op een wezenlijk deel daarvan, als daardoor de handel tussen de Lid-Staten ongunstig kan worden beïnvloed.

Op grond van deze bepaling werd IBM in 1984 door de Europese Commissie verplicht tot het vrijgeven van technische informatie over de interfaces van het IBM Systeem/370. In deze context wordt onder een interface de hardware en software verstaan via dewelke andere apparaten en programma's op het IBM Systeem kunnen worden aangesloten. IBM werd ervan beschuldigd de informatie over deze interfaces niet tijdig beschikbaar te stellen, zodat andere constructeurs niet tijdig IBM-compatible hardware en software op de markt konden brengen. De Europese Commissie beschouwde het achterhouden van deze informatie als een misbruik van een economische machtspositie. Het kwam echter nooit tot een formele beschikking omdat IBM zich t.o.v. de Commissie verbond de informatie vrijwillig ter beschikking te stellen.

3. REGULERING VIA HET INTELLECTUEEL EIGENDOMSRECHT

3.1. OVERZICHT

Bij de beschrijving van de informaticamarkt hebben we reeds de klemtoon gelegd op de zwakke positie van de Europese informaticabedrijven. Hierboven zagen we hoe de Commissie van de Europese Unie via het mededingingsrecht de concurrentiepositie van de Europese informatica-industrie probeert te verstevigen. Naast het voeren van een Europese concurrentiepolitiek op de informaticamarkt, heeft de Commissie ook een reeks initiatieven ontwikkeld op het gebied van het intellectueel eigendomsrecht. Die initiatieven overstijgen weliswaar de informaticamarkt, omdat ze ook bedoeld zijn voor andere sectoren van de Europese economie, maar in de informaticasector zijn die initiatieven toch van zeer groot belang. Over welke initiatieven

gaat het hier ?

In 1985 heeft de Europese Commissie in haar "Witboek" over de voltooiing van de interne markt een reeks harmonisatievoorstellen aangekondigd op het gebied van het intellectueel eigendomsrecht:

- op het gebied van het merkenrecht heeft het Commissievoorstel geleid tot de eerste Richtlijn van 21 december 1988 over de harmonisering van de wetgevingen van de Lid-Staten m.b.t. handelsmerken (PB 1989, L40);
- op het gebied van de bescherming van computerprogramma's hebben de inspanningen geleid tot de Richtlijn van 14 mei 1991 betreffende de rechtsbescherming van computerprogramma's (de zgn. "softwarerichtlijn", PB 1991, L122);
- op het gebied van het octrooirecht drong de Commissie aan op een snelle ratificatie van het Gemeenschapsoctrooi-verdrag van 1975 (zie hierna);
- op het gebied van de juridische bescherming van de topografieën van halfgeleiderprodukten werd in 1987 een specifieke richtlijn uitgevaardigd (zie bespreking infra);
- op het gebied van het auteursrecht heeft de Commissie onlangs een ontwerp-Richtlijn gepubliceerd ter harmonisering van de duur van de auteursrechtelijke bescherming in de verschillende Lid-Staten (PB 1992, C92);
- op het gebied van databanken heeft de Commissie een voorontwerp van richtlijn opgesteld waarin een specifieke bescherming voor databanken wordt voorgesteld.

Voor de ontwikkeling van de Europese informaticamarkt is de harmonisering van het intellectueel eigendomsrecht belangrijk om drie redenen:

- de verschillen in de wetgevingen van de Lid-Staten vormen een belemmering van de handel tussen de landen van de Unie;
- de verschillen belemmeren een snelle verspreiding van innovaties binnen de Unie;
- de verschillen bemoeilijken de handel met derde landen.

In de volgende bladzijden wordt meer in detail ingegaan op drie specifieke problemen i.v.m. het intellectueel eigendomsrecht en de informaticamarkt:

- de rechtsbescherming van computerprogramma's ("softwarebescherming");
- de bescherming van topografieën van halfgeleiderprodukten ("chipsbescherming");
- de bescherming van databanken;
- de bescherming van "computerwerken".

3.2. RECHTSBESCHERMING VAN COMPUTERPROGRAMMA'S

3.2.1. Inleiding

Er is, vooral in de zeventiger en het begin van de tachtiger jaren veel gediscussieerd over de vraag of computerprogramma's beschermd moesten worden via het octrooirecht of via het auteursrecht. Aanvankelijk dacht men vooral aan het octrooirecht, o.m. wegens het technisch karakter van software. De octrooiering van software stuit echter op veel moeilijkheden, waarop

we hierna nog terugkomen. Zowel de materiële als de formele voorwaarden om een uitvinding te octrooieren zijn zeer streng.

Ook de toepassing van het auteursrecht op software stuit echter op veel bezwaren. Daarom hebben velen gepleit voor een bescherming "sui generis". Ondanks alle bezwaren heeft het auteursrecht zich op het domein van de softwarebescherming toch doorgezet. In de Verenigde Staten is men zeer snel overgegaan tot de bescherming van software via het auteursrecht. Al in 1964 gaf het Copyright Office in Washington te kennen dat software kon worden geregistreerd. Toch werd pas in 1980 software expliciet in de Amerikaanse Copyright Act opgenomen. In Europa gebeurde dat eerst in Duitsland (in 1985) en kort daarop in Frankrijk en Engeland. De discussie is definitief beslecht nu ook in de softwarerichtlijn van de Europese Unie voor een bescherming via het auteursrecht is geopteerd. De vraag naar de octrooieerbaarheid van software stelt zich vooral nog wanneer een computerprogramma deel uitmaakt van een ander produkt.

3.2.2. Octrooieerbaarheid van software

3.2.2.1. Bronnen van het octrooirecht

De oude Belgische octrooiwet van 1854 is thans vervangen door de wet van 28 maart 1984 op de uitvindingsoctrooien. Deze wet stemt het Belgische octrooirecht af op de Europese harmoniseringsbeweging inzake octrooirecht die sinds het begin van de jaren zeventig is ingezet. Deze harmoniseringsbeweging heeft geleid tot:

- het Europees Octrooioverdrag van München dat op 5 oktober 1973 tussen de Lid-Staten van de Europese Unie werd gesloten en dat op 7 oktober 1977 in werking is getreden;
- het Gemeenschapsoctrooioverdrag van Luxemburg van 15 december 1975 dat momenteel nog niet in werking is getreden.

Het Europees Octrooioverdrag heeft de mogelijkheid geschapen voor een uitvinder om één octrooivraag in te dienen op één plaats, nl. in München bij het Europees Octrooibureau. Het is dus niet meer nodig om in elke Lid-Staat afzonderlijk een aanvraag in te dienen. Indien een uitvinder in München een octrooiaanvraag indient, kiest hij zelf voor welke landen hij een octrooi wenst. Als de aanvraag wordt goedgekeurd, zal de uitvinder meteen een aantal nationale octrooien verkrijgen, die vanaf dat ogenblik elk hun eigen nationale weg gaan. Indien het octrooi in één van de betrokken landen betwist wordt, zal de nationale rechter van dat land het octrooi beoordelen volgens zijn eigen nationaal octrooirecht. Het Europees Octrooioverdrag stelt dus geen Europees octrooi in. Het is eerder een samenwerking op het vlak van de behandeling van octrooiaanvragen. Een Europees octrooi of "Gemeenschapsoctrooi" komt er pas als het Gemeenschapsoctrooioverdrag van Luxemburg in werking zal treden.

3.2.2.2. Octrooieerbaarheidsvereisten

Om octrooieerbaar te zijn moet een uitvinding aan een aantal materiële en formele vereisten voldoen.

Materiële vereisten:

- het moet gaan om een uitvinding, d.w.z. een voortbrengsel (een produkt, een werktuig of machine, een bepaalde stof) of een werkwijze (een methode om een bepaald resultaat te bereiken); louter abstracte creaties van de menselijke geest (wiskundige formules, wetenschappelijke theorieën) die niet onmiddellijk toepasbaar zijn op het gebied van de nijverheid zijn niet octrooieerbaar;
- het moet gaan om iets nieuws, d.w.z. dat de uitvinding geen deel mag uitmaken van de huidige stand van de techniek; de stand van de techniek wordt gevormd door al hetgeen voor de datum van de aanvraag, waar ook ter wereld, openbaar toegankelijk is gemaakt;
- de uitvinding moet ook het resultaat zijn van een uitvinderswerkzaamheid, d.w.z. dat zij voor een deskundige niet op een voor de hand liggende wijze mag voortvloeien uit de stand van de techniek; de uitvinding mag dus niet "evident" zijn, ze moet het resultaat zijn van een intellectuele inspanning; de duur van die inspanning speelt geen rol; het kan ook gaan om een geniale flits;
- de uitvinding moet onmiddellijk toepasbaar in de nijverheid zijn; nijverheid moet daarbij in zeer ruime zin worden verstaan;
- de uitvinding mag tenslotte niet in strijd met de openbare orde en de goede zeden zijn.

Formele vereisten: naast de materiële vereisten, moet de octrooiaanvraag aan een aantal formele criteria voldoen m.b.t. de inhoud van de aanvraag, de bijgevoegde stukken. Een in België geldend octrooi kan thans op drie manieren worden aangevraagd: via de nationale procedure, via een Europese octrooiaanvraag (rechtstreeks bij het Europees octrooibureau of onrechtstreeks via de bemiddeling van de Belgische dienst voor industriële eigendom, of via een internationale aanvraag (op grond van het Verdrag tot Samenwerking inzake Octrooien, dat in België sinds 1981 van kracht is)

3.2.2.3. Octrooi voor software ?

Artikel 52 van het Europees Octrooiverdrag, waarin de materiële vereisten voor de octrooiverlening worden vastgesteld, bepaalt dat computerprogramma's niet onder het begrip "uitvinding" vallen. Deze bepaling werd in artikel 3 van de Belgische Octrooiwet overgenomen.

Tot 1985 heeft men de bovengenoemde regel zeer strikt geïnterpreteerd en toegepast. Ook indien een computerprogramma deel uitmaakte van een ander produkt of een andere methode, die als geheel wél in aanmerking zou komen voor een octrooi, werd het geheel niet als een uitvinding beschouwd als de nieuwigheid enkel in het computerprogramma lag.

In 1985 kwam daar verandering in met de Richtlijnen van het Europees Octrooibureau, waarin gesteld werd dat men steeds de uitvinding in zijn geheel moest bekijken. Weliswaar werd software "als dusdanig" nog niet als octrooieerbaar beschouwd.

Het Europees Octrooibureau paste zijn standpunt o.m. toe in zijn beslissingen over "Vicom Systems" (digitale filtering van beelden afkomstig van satellieten d.m.v. een computerprogram-

ma) en in de zaak "Koch & Sterzel vs. Siemens/Philips Patentverwaltung" (1987).

In een latere beslissing van 1989 n.a.v. een aanvraag van IBM i.v.m. een automatische "text grade level analyzer" voor een tekstverwerkingssysteem, die automatisch synoniemen voor moeilijke woorden plaatste, kwam het Europees Octrooibureau echter op zijn stappen terug. Er werd namelijk beslist dat de "kern" van de uitvinding toch in de hardware moest gesitueerd zijn. Volgens het Octrooibureau had het plaatsen van synoniemen voor moeilijke woorden geen enkel "technisch" karakter. Men beschouwde het eerder als een methode voor het verrichten van mentale activiteiten.

Met de IBM-beslissing is het Europees Octrooibureau, in navolging van de Duitse rechtspraak, opnieuw zeer restrictief geworden inzake de octschouwd, maar indien de globale uitvinding een technisch karakter had, kon een octrooi verleend worden, ook indien de nieuwheid enkel in het geïntegreerde computerprogramma lag. Daarmee werd ingegaan tegen de Duitse rechtspraak volgens dewelke van een uitvinding geen sprake kon zijn als het enige nieuwe te vinden was in een computerprogramma en dus in een element zonder technisch karakter. rooieerbaarheid van computerprogramma's. De voorstanders van deze beschermingstechniek voeren langzamerhand een achterhoedegevecht.

3.2.3. Rechtsbescherming via het auteursrecht

3.2.3.1. Inleiding

In juni 1988 publiceerde de Commissie van de Europese Unie een "Groenboek" onder de titel "Auteursrecht en de uitdaging van de technologie"². Hoofdstuk 5 van dit Groenboek handelt over computerprogramma's.

De Commissie beklemtoont in het Groenboek het belang van computerprogramma's voor de Europese economie. Tegelijk uit ze haar bezorgdheid over het bestaan van gesloten systemen, waarvoor geen interfaces op de markt verkrijgbaar zijn. Volgens de Commissie moet er gestreefd worden naar vrije en gestandaardiseerde interfaces tussen computersystemen of tussen programma's. Machines en programma's van verschillende producenten moeten zonder al te veel moeilijkheden aan elkaar gekoppeld kunnen worden. Situaties waarbij bij een besturingssysteem enkel toepassingsprogramma's van dezelfde producent gebruikt kunnen worden, zijn volgens de Commissie een belemmering voor de vrije concurrentie in de Unie. Bovendien bemoeilijkt het ook het concurrentievermogen van de Europese softwareproducenten.

In het Groenboek van 1988 wordt door de Commissie de snelle indiening van een richtlijn over de rechtsbescherming van computerprogramma's aangekondigd op basis van art. 100 van het

² Mededeling van de Commissie, Com(88)172, 7 juni 1988. Voor een bespreking van dit document verwijzen we naar F. Gotzen (ed.), Copyright and the European Community. The green paper on copyright and the challenge of new technology, Brussel, Story Scientia, 1989, Reeks CIR, nr. 1.

EEG-Verdrag. Daarin zou worden geopteerd voor een bescherming van computerprogramma's via het auteursrecht. Hoewel deze oplossing door sommigen werd afgeraden, o.m. op grond van het argument dat software wegens het technisch karakter ervan niet "geschikt" zou zijn voor een toepassing van het auteursrecht³, sloot dit voorstel aan bij een niet meer te stuiten evolutie. Het auteursrecht wordt al lang niet meer uitsluitend toegepast op het klassieke domein van kunst en letterkunde maar ook op wetenschappelijke en technische produkten. Een grote meerderheid van de doctrine verdedigde al enige tijd de toepassing van het auteursrecht op computerprogramma's.⁴ De rechtspraak in de meeste Europese landen had die tendens gevolgd⁵. Dit werd tenslotte ook bevestigd in de wetgeving van o.m. Duitsland, Frankrijk, het Verenigd Koninkrijk en Spanje⁶. Daarom vroegen sommigen zich af of een Europese richtlijn nog wel nodig was, vermits er een spontane eensgezindheid groeide over de bescherming van computerprogramma's via het auteursrecht⁷. Desondanks werd het ontwerp van richtlijn reeds begin 1989 door de Commissie ingediend⁸. Na zeer intensieve discussies en stevig lobbywerk werd een volledig herziene versie van dit ontwerp op 14 mei 1991 door de Raad goedgekeurd⁹.

Volgens artikel 10 van de richtlijn (hierna "softwarerichtlijn" genoemd) moeten de Lid-Staten uiterlijk op 31 december 1992 de nodige wettelijke en administratieve bepalingen in werking doen treden om aan deze richtlijn te voldoen. België heeft alvast deze datum niet gehaald. Slechts bij wet van 30 juni 1994 houdende omzetting in Belgisch recht van de Europese richtlijn van 14 mei 1991 betreffende de rechtsbescherming van computerprogramma's werd aan de

³ Zie o.m. G. Vandenberghe, *Bescherming van Computersoftware*, Antwerpen, Kluwer, Reeks Informatica en Recht, 1984; K. Van Hoecke, "Software piraten", R.W., 1983-1984, 1661-1663; L. Melville, "Computer software and the relevance of copyright", EIPR, 1980, 356-357, e.a.

⁴ Zie de lange lijst van de geciteerde auteurs in voetnoot 16 van : F. Gotzen, "Programmes d'ordinateurs et banques de données", in : F. Gotzen (ed), *Copyright and the European Community*, o.c., P.26.

⁵ Voor een aantal referenties uit Frankrijk, Duitsland en Nederland, zie ibidem, p. 26, voetnoot 17.

⁶ In Duitsland gebeurde dit door de wet van 24 juni 1985, tot wijziging van o.m. §§ 2 en 53 van de auteurswet van 9 september 1965 (BGBl, I, 1985, 1137); in Frankrijk door art. 3 van de wet van 11 maart 1957, gewijzigd door de wet van 3 juli 1985 (J.O., 4 juli 1985, 7495); in het Verenigd Koninkrijk door de "Copyright (Computer Software) Amendment Act" van 16 juli 1985 (Current Law Statutes, 1985, 2,41); in Spanje door de wet van 11 november 1987 (B.O.E., 17/11/87, art. 10).

⁷ Tot deze conclusie was men in de WIPO gekomen. Zie "Rapport du comité d'experts sur la protection juridique du logiciel", D.A., 1983, p 243 e.v. De WIPO (World Intellectual Property Organisation) werd opgericht op de Conferentie van Stockholm in 1967.

⁸ Het eerste ontwerp is gepubliceerd in Publ. E.G., nr C 91 van 12 april 1989, p.4; het tweede ontwerp vindt men in Publ. E.G., nr C 320 van 20 december 1990, p 22. Zie ook Publ. E.G., nr C 231 van 17 september 1990, p 78 voor het advies van het Europees Parlement en Publ. E.G., nr C 329 van 30 december 1989, p 4 voor het advies van het Economisch en Sociaal Comité.

⁹ Richtlijn van de Raad van 14 mei 1991 betreffende de rechtsbescherming van computerprogramma's.

softwarerichtlijn uitvoering gegeven. Op dezelfde dag werd ook een meer algemene wet goedgekeurd betreffende het auteursrecht en de naburige rechten. Om beide wetten te onderscheiden, wordt de eerste wet hierna de softwarebeschermingswet genoemd en de tweede de auteurswet.

3.2.3.2. Bronnen van het Belgisch positief recht inzake de auteursrechtelijke bescherming van computerprogramma's

De auteursrechtelijke bescherming van computerprogramma's wordt in België dus in de eerste plaats geregeld door de softwarebeschermingswet, die de Europese softwarerichtlijn omzet in intern recht. Hoewel deze richtlijn geen rechtstreekse werking heeft, vormen de bepalingen en de aanhef ervan een belangrijke basis voor de interpretatie van de Belgische softwarebeschermingswet. Bovendien kunnen inbreuken door deze Belgische wet op de richtlijn worden aangevochten voor het Hof van Justitie.

De softwarerichtlijn bepaalt echter dat computerprogramma's beschermd worden als werk van letterkunde. Dit impliceert dat ook de algemene bepalingen en de bepalingen m.b.t. werken van letterkunde van de algemene auteurswet van toepassing zijn op computerprogramma's, tenzij de softwarebeschermingswet ervan afwijkt of de softwarerichtlijn een specifieke regeling eist.

Tenslotte is het auteursrecht op computerprogramma's krachtens artikel 1 van softwarebeschermingswet en artikel 1, 1° van de Europese softwarerichtlijn internationaal gewaarborgd door de Conventie van Bern van 9 september 1886 voor de bescherming van letterkundige en kunstwerken, gewijzigd op 26 juni 1948¹⁰. De Conventie van Bern bevat een lange lijst van "werken van letterkunde", maar computerprogramma's worden daarbij niet genoemd. De softwarerichtlijn heeft dus als gevolg dat voor de Lid-Staten van de Unie, computerprogramma's bij deze lijst moeten worden bijgedacht. Alle bepalingen van de Berner Conventie die toepasselijk zijn op werken van letterkunde vinden dan ook toepassing op computerprogramma's. Met de Europese softwarerichtlijn worden bovendien aan de algemene bepalingen van de Berner Conventie die voor alle werken van letterkunde gelden, een aantal specifieke bepalingen voor computerprogramma's toegevoegd. Deze specifieke bepalingen hebben m.b.t. computerprogramma's voorrang op de algemene bepalingen die voor alle werken van letterkunde gelden¹¹.

De toepasselijkheid van de Berner Conventie op computerprogramma's heeft als gevolg dat op dit terrein het principe van de nationale behandeling op programma's van buitenlandse auteurs moet toegepast worden¹². Amerikaanse programma's krijgen in België dus dezelfde bescherming

¹⁰ Het Unieverdrag van Bern van 9 september 1886 werd door België geratificeerd bij wet van 30 september 1887.

¹¹ B. Czarnota & R. Hart, *Legal Protection of Computer Programs in Europe. A guide to the EC Directive*, London, e.a.: Butterworths, 1991, pp. 30-32

¹² Art. 5.1 van de Berner Conventie

als Belgische programma's. Bovendien kan voor het genieten van auteursrechtelijke bescherming geen enkele formaliteit worden opgelegd.

Volgens het Hof van Cassatie heeft de Conventie van Bern tenslotte voorrang op de bepalingen van de interne Belgische wetgeving.

3.2.3.3. Wat is een computerprogramma ?

Noch de Belgische softwarebeschermingswet, noch de Europese softwarerichtlijn van 14 mei 1991 bevatten een definitie van het begrip "computerprogramma". In de WIPO "Model Provisions on the Protection of Computer Software" definieert men het begrip als volgt: "a set of instructions expressed in words, codes, schemes or in any other form, which is capable, when incorporated in a machine-readable medium, of causing a computer to perform or achieve a particular task or result".

Een computerprogramma is dus een geheel van instructies die in een bepaalde taal (in ruime zin) zijn uitgedrukt en die door een computer kunnen worden uitgevoerd. Artikel 1 van de softwarebeschermingswet voegt daaraan toe dat een computerprogramma ook het voorbereidend materiaal omvat. Hieronder moet het materiaal worden verstaan dat onmiddellijk in programma-code kan worden omgezet. De sequentie, de structuur en de organisatie van het programma moeten al in het materiaal besloten liggen. Een analyserapport, waarin deze elementen van het programma nog niet zijn vastgelegd, behoort dus niet tot het computerprogramma. Voor dergelijke rapporten geldt dezelfde regel als voor documentatie of ander begeleidend materiaal bij het programma, nl. dat dit afzonderlijke werken van letterkunde zijn en als dusdanig auteursrechtelijke bescherming genieten. Hoe de helpfunctie in een programma moet behandeld worden, is onduidelijk. Geautomatiseerde documentatie die in een programma is geïncorporeerd, beantwoordt eerder aan de definitie van een "databank" (zie later).

Het spreekt voor zich dat alle computerprogramma's onder de toepassing van de softwarebeschermingswet vallen: besturingssystemen en toepassingsprogramma's, standaardprogramma's of maatwerk, e.a. Bovendien speelt de vorm waarin het programma is uitgedrukt geen enkele rol. Het kan dus gaan om een programma in een hogere programmeertaal (Cobol of Pascal bv.), in assembleertaal of in machinecode. De vormen die een programma kan aannemen en de manier waarop het tot stand komt zijn zeer uiteenlopend. Meestal denkt men aan code in een hogere programmeertaal. Men kan echter ook een programma schrijven door iets "voor te doen". Dat is bv. het geval bij een robot. De eerste keer moet men de arm van de robot manueel sturen, maar na enkele keren kan de robot het alleen. De robot heeft dan het programma geregistreerd. Iets gelijkaardigs heeft men bij zgn. "macro's" in tekstverwerking of rekenbladen. Men verricht een aantal handelingen en die handelingen worden geregistreerd zodat men ze achteraf opnieuw kan "afspelen".

Om programma's te maken zijn er tal van hulpmiddelen. Er bestaan uitgebreide programmabibliotheken, met nuttige programma-onderdelen of berekeningen. Vaak is een programma niet

meer dan een compilatie van bestaande routines. Meer en meer wordt software ook met de computer gemaakt. In plaats van code neer te schrijven of in te tikken, klikt men op een scherm aan wat het programma moet doen, men geeft aan hoe de opeenvolgende schermen eruit moeten zien, enz. Het eigenlijke programma wordt daarna automatisch gegenereerd. Dergelijke softwaregeneratoren, "screen builders", e.a. zijn een onderdeel van wat men "CASE-tools" noemt. CASE staat voor "Computer Assisted Software Engineering".

Ondanks de diversiteit blijft een programma echter fundamenteel een tekst die door de mens, rechtstreeks of onrechtstreeks, wordt geschreven en die door een machine kan worden uitgevoerd.

3.2.3.4. Geen bescherming voor ideeën en beginselen

Artikel 2, tweede lid van de softwarebeschermingswet bepaalt dat de auteursrechtelijke bescherming wordt verleend aan de uitdrukkingswijze, in welke vorm dan ook, van een computerprogramma. "De ideeën en beginselen die aan enig element van een computerprogramma ten grondslag liggen, met inbegrip van de ideeën en beginselen die aan de interfaces daarvan ten grondslag liggen, worden niet auteursrechtelijk beschermd".

Dat de auteursrechtelijke bescherming beperkt is tot de uitdrukkingswijze, is in het auteursrecht klassiek. Een auteurswerk is de uitdrukking door de mens van een bepaalde idee in een concrete en originele vorm¹³. De functionaliteit van een programma wordt dus niet beschermd.

Belangrijk is dat de uitdrukkingswijze onder elke vorm wordt beschermd. Het gaat dus niet alleen over de programmacode; de bescherming slaat ook op de structuur, de sequentie en de organisatie van het programma. Zodra deze elementen vastliggen, is het programma ontstaan. De opeenvolgende omzettingen van het programma, van stroomschema naar hogere programmeertaal en vervolgens naar machinecode betreffen allemaal één en hetzelfde programma.

De term "interfaces" wordt in zeer verschillende betekenissen gebruikt. Het kan gaan over interfaces tussen machines onderling. Iedereen die al eens een hifi-installatie heeft geïnstalleerd weet wat dat is. Om een CD-speler aan te sluiten op een dergelijke installatie moeten een aantal voorwaarden vervuld zijn. Als men een verschillende stekker heeft, dan werkt het niet. Bij computers is dat nog veel complexer. Denken we maar aan het nog simpele geval van de aansluiting van een printer bij een computer. Men heeft daarnaast ook "interfaces" tussen programma's. Als men in een programma opeens een module uit een of andere programmabibliotheek wil inschakelen, dan moeten ook hier de nodige raakvlakken aanwezig zijn. Anders "past" de module niet in het programma. Tenslotte spreekt men ook van "interfaces" tussen de programma's en de gebruikers, de zgn. "user interfaces". Hiermee bedoelt men het geheel van elementen waarmee de gebruiker het programma kan bedienen: menu's, iconen, e.d.

13

F. van Isacker, Kritische synthese van het Belgische auteursrecht, Antwerpen, Kluwer, 1985, p.3

In de softwarebeschermingswet heeft men het vooral over de eerste twee vormen van "interfaces", namelijk die tussen machines onderling of tussen programma's onderling. Zowel voor interfaces als voor programmeertalen heeft de Europese Commissie haar oorspronkelijke idee, om deze elementen buiten de auteursrechtelijke bescherming te houden, moeten opgeven. In de uiteindelijke richtlijn worden interfaces op dezelfde leest geschoeid als de andere onderdelen van een computerprogramma. Interfaces maken deel uit van het programma en derhalve wordt enkel de uitdrukkingswijze ervan beschermd, niet de ideeën en beginselen die eraan ten grondslag liggen. Van de specificaties van de interfaces van een programma mag een auteur, die deze specificaties nodig heeft om een compatibel programma te maken, dus enkel de informatie gebruiken, die in deze specificaties besloten ligt. Hij mag niet de programmacode van deze interfaces reproduceren en in zijn eigen programma opnemen. Soms zal een interface maar op één manier uitgedrukt kunnen worden. Dan heeft de tweede auteur geen keuze en zal hij ook niet de rechten van de eerste auteur schenden, als hij dezelfde uitdrukkingswijze gebruikt (zgn. "merger doctrine"). Het moet echter gaan om een technische beperking. Tijdwinst of andere economische overwegingen vormen geen excuus.

Voor programmeertalen ligt de zaak enigszins anders. Er is een onderscheid tussen de taal waarin een programma geschreven wordt en het programma zelf. Zoals de natuurlijke taal (Nederlands, Engels,...) het instrument is om een literaire tekst te schrijven, zo is de programmeertaal het instrument om een programma te schrijven. Net zoals de natuurlijke taal heeft de programmeertaal een woordenschat en een grammatica. Bij een programmeertaal hoort een programma om voor de vertaling te zorgen van hogere programmeertaal naar uitvoerbare machinecode. Die vertaler of "compiler" is een programma dat uiteraard wél onder de auteursrechtelijke bescherming valt. Vaak wordt onder "programmeertaal" echter zowel de taal als de compiler verstaan. Om discussie te vermijden, heeft de Commissie in het tweede ontwerp van de softwarerichtlijn de verwijzing naar programmeertalen eenvoudig weggelaten. Slechts in zoverre een programmeertaal beschouwd kan worden als een geheel van ideeën en principes, valt ze buiten de auteursrechtelijke bescherming¹⁴.

Het onderscheid tussen idee en uitdrukkingswijze bij een computerprogramma is niet altijd duidelijk. Een bewijs daarvan is de aanslepende discussie in de Amerikaanse rechtspraak over de "look and feel" theorie, o.m. naar aanleiding van het conflict tussen Apple en Microsoft.

Apple Computer Inc. bracht voor de Macintosh computerlijn een zeer gebruiksvriendelijke grafische interface uit, met vensters, iconen en afrolmenu's. Een aantal jaren nadien bracht Microsoft een gelijkaardige interface op de markt voor DOS-computers, onder de naam "Windows". In 1985 tekenden Microsoft en Apple een akkoord waarbij Microsoft een vrije licentie verkreeg om Windows te gebruiken en in licentie te geven, in ruil voor een verklaring waarbij Microsoft erkende dat de Windows 1.0 schermen afgeleid waren van de Macintosh. Microsoft verleende daarop een licentie aan Hewlett-Packard om de interface eveneens op de markt te brengen. Drie jaar later startte Apple een geding tegen Microsoft en Hewlett-Packard omdat haar auteursrecht zou zijn geschonden door de interface van Windows 2.03 en van HP's interface "NewWave". Het district court oordeelde aanvankelijk dat het

¹⁴

Dit staat uitdrukkelijk in de overwegingen die de tekst van de richtlijn voorafgaan.

akkoord van 1985 ook sloeg op Windows 2.03, met uitzondering van 10 elementen in Windows en een aantal meer in NewWave die buiten het akkoord vielen maar toch van de Apple gebruikersinterface waren overgenomen. In een latere beslissing werd vervolgens gesteld dat de 10 elementen uit Windows 2.03 die niet onder het akkoord van 1985 vielen, buiten de bescherming van het auteursrecht vielen. Apple ging tegen deze beslissing in beroep en stelde dat, ook al waren deze 10 elementen elk afzonderlijk niet beschermd door het auteursrecht, minstens de wijze waarop deze elementen met elkaar gecombineerd waren een "look and feel" uitmaakten die wél voor bescherming in aanmerking kwam. Het Hof van Beroep verwierp deze stelling¹⁵. Volgens het Hof is de gebruikersinterface van Apple, die een metafoor is van een bureautafel met kantoorobjecten, geen element waarvan Apple als de auteur kon worden beschouwd. De metafoor is volgens het Hof een geheel van visuele elementen en gebruikersbevelen die essentieel dienen om de bediening van de computer te vergemakkelijken. De betrokken interface dient dus een puur utilitair oogmerk, vergelijkbaar met een instrumentenpaneel in een auto. Het feit dat Apple voor de bediening van de computer een metafoor gebruikte, betekent niet dat dit niet om puur functionele redenen gebeurde. De gebruikte visuele symbolen zijn bovendien zo nauw met deze functionaliteit verbonden dat ze een standaard uitmaken. De standaardisatie van de bediening van de computer is, net zoals bij de automobielen, essentieel voor de gebruikers.

3.2.3.5. Enkel oorspronkelijke programma's

Artikel 2, eerste lid van de softwarebeschermingswet bepaalt: "Een computerprogramma geniet bescherming indien het oorspronkelijk is in die zin, dat het een eigen intellectuele schepping van de auteur is. Om te bepalen of het programma voor auteursrechtelijke bescherming in aanmerking komt, mogen geen andere criteria worden aangelegd".

In de toelichting bij het eerste ontwerp van de softwarerichtlijn stelde de Commissie dat, om te bepalen of een computerprogramma in aanmerking komt voor de bescherming van het auteursrecht, enkel het criterium van de "originaliteit" mag gehanteerd worden. Onder originaliteit werd verstaan "dat het werk niet was gekopieerd". Geen andere kwalitatieve of esthetische testen mogen worden toegepast. Daarmee ging de Commissie regelrecht in tegen de opvatting van de Duitse rechtspraak. In het bekende "Inkasso-arrest" besliste het Duitse Bundesgerichtshof dat een programma slechts aan de originaliteitsvereiste voldoet als de maker ervan een duidelijk hogere creativiteit aan de dag heeft gelegd, dan gemiddeld het geval is¹⁶. De andere Europese landen hanteerden een veel lagere norm voor de toepasselijkheid van het auteursrecht.

In dezelfde toelichting stelde de Commissie tevens dat een programma een compilatie kan zijn

¹⁵ Apple Computer Inc. v. Microsoft Corp., 799 F. Supp. 1006 (N.D. Cal. 1992)(August 10, 1992) 1992, samengevat in *The Computer Law Monitor*, Vol 10, Nr 2, November 1992, 523.

¹⁶ BGH 9 mei 1985, zie EIPR 1986, pp.179 en 185. Deze beslissing werd gevestigd in BGH 4 oktober 1990, Nixdorf v. Nixdorf, zie EIPR 1991, p.301: "Creatieve originaliteit wordt vastgesteld door een globale vergelijking met bestaande uitdrukkingwijzen. Als deze globale vergelijking aantoont dat het programma creatieve karakteristieken vertoont, dan moeten deze gesteld worden tegenover het werk van een gemiddelde programmeur. Het niveau van creativiteit dat nodig voor het auteursrecht is, is slechts aanwezig als het geleverde werk merkbaar boven het niveau van een gemiddelde programmeur staat..." Zie ook Kindermann, "Copyright Protection of Computer Programs in Germany: Nixdorf v. Nixdorf", EIPR 1991, p 296

van routines en subroutines. Elk onderdeel van een programma komt voor bescherming in aanmerking, evenals de compilatie van de onderdelen tot een geheel. Een compilatie van routines en subroutines die elk afzonderlijk tot het publiek domein behoren, kan dus toch een "origineel" programma zijn, op voorwaarde dat de compilatie zelf als een schepping van de maker beschouwd kan worden. In de uiteindelijke overwegingen bij de softwarerichtlijn staat dat "bij de vaststelling of een computerprogramma een oorspronkelijk werk is, geen criteria mogen worden toegepast met betrekking tot de kwalitatieve of esthetische waarde van het programma".

3.2.3.6. Subject van de bescherming

Volgens artikel 2, 1° van de softwarerichtlijn is de maker van een computerprogramma "de natuurlijke persoon of de groep van natuurlijke personen die het programma gemaakt heeft of, indien de wetgeving van de Lid-Staat zulks toestaat, de rechtspersoon die door de nationale wetgeving als rechthebbende wordt aangemerkt. Wanneer de wetgeving van een Lid-Staat collectieve werken erkent, wordt degene die volgens die wetgeving geacht wordt het programma gemaakt te hebben, als de maker ervan beschouwd".

In België kunnen krachtens artikel 6 van de auteurswet enkel natuurlijke personen als auteur van een werk van letterkunde, en derhalve van een computerprogramma beschouwd worden. Een auteurswerk vereist een menselijke tussenkomst. Zonder menselijke tussenkomst is er geen sprake van creatie. De patrimoniale auteursrechten kunnen natuurlijk wel aan een rechtspersoon worden overgedragen. De morele rechten daarentegen zijn onvervreemdbaar (zie hierna).

In de eerste versie van de ontwerp-richtlijn stond ook nog een bepaling over computerprogramma's die in opdracht wordt gemaakt. Daarin stond dat, wanneer een programma wordt gemaakt in uitvoering van een contract, de natuurlijke of de rechtspersoon die de opdracht had gegeven voor het maken van het programma, alle rechten daarop verkrijgt, tenzij anders overeengekomen wordt in het contract¹⁷. Deze bepaling werd in latere versies opgegeven. Wie een programma maakt in opdracht van iemand anders, behoudt nu het auteursrecht op dat programma en de opdrachtgever verkrijgt enkel een licentie, tenzij de partijen overeenkomen dat ook het auteursrecht wordt overgedragen. In dat geval behoudt de maker van het programma enkel de morele rechten.

Volgens artikel 3 van Belgische auteurswet zijn de vermogensrechten voortvloeiend uit het auteursrecht vatbaar voor gehele of gedeeltelijke overdracht, maar moeten alle contracten met betrekking tot de uitoefening van dat recht schriftelijk zijn. De contractuele bedingen met betrekking tot het auteursrecht en de exploitatiewijze ervan moeten restrictief worden geïnterpreteerd. Voor elke exploitatiewijze moeten de vergoeding voor de auteur, de reikwijdte en de duur van de overdracht afzonderlijk worden bepaald.

¹⁷ Over deze bepaling in de eerste versie van de ontwerp-richtlijn, zie A. Lucas, "Copyright in the European Community : the Green Paper and the Proposal for a Directive concerning Legal Protection of Computer Programs", Columbia Journal of Transnational Law, 1991, Vol. 29, p 158.

Indien een computerprogramma door een groep van natuurlijke personen gezamenlijk is gemaakt, zijn deze personen gezamenlijk houder van de exclusieve rechten. In de praktijk komt dit zeer vaak voor. De meeste programma's zijn "collaboratiewerken". Bij automatiseringsprojecten of bij de ontwikkeling van standaardsoftware worden meestal ganse ploegen ingeschakeld, met analisten, programmeurs, e.a., net zoals bij het maken van een film. Iedereen die een creatieve bijdrage heeft geleverd aan de totstandkoming van het programma, wordt als co-auteur beschouwd. In sommige gevallen zal men de bijdrage of het onderdeel van elke auteur nog kunnen onderscheiden. Dan is uiteraard elke bijdrage afzonderlijk een auteurswerk. Maar zeer dikwijls zijn de verschillende bijdragen niet meer te identificeren. Dan heeft men te maken met een echt collaboratiewerk.

Co-auteurschap ontstaat echter niet alleen uit collaboratie. Men kan ook te maken hebben met "adaptatie". Een voorbeeld daarvan is een "macrobibliotheek" voor bv. een tekstverwerkingsprogramma.

De co-auteurs moeten hun rechten gezamenlijk uitoefenen. Dat kan soms praktische problemen opleveren, o.m. omdat voor bv. het verlenen van een licentie het unaniem akkoord van de co-auteurs nodig is. De beste waarborg om deze problemen te vermijden is het opstellen van duidelijke overeenkomsten tussen de co-auteurs.

Indien een computerprogramma gemaakt is door een werknemer of een beambte bij de uitoefening van zijn taken of in opdracht van zijn werkgever, is de werkgever bij uitsluiting bevoegd de economische rechten met betrekking tot het programma uit te oefenen, tenzij bij overeenkomst of statuut anders werd bepaald (artikel 3 softwarebeschermingswet). Om te vermijden dat betwistingen zouden rijzen over de vraag of de werkgever al dan niet precieze opdracht heeft gegeven tot het maken van het programma, is de zinsnede "bij de uitoefening van zijn taken" toegevoegd. Een werknemer of beambte die zelf, in het kader van zijn werk, het initiatief heeft genomen om het programma te maken, ontsnapt dus niet aan de toepassing van deze bepaling. De werknemer of beambte blijft uiteraard de auteur en behoudt de morele rechten op het programma. De werkgever, eventueel een rechtspersoon, verwerft enkel de economische rechten. Noteer dat bij overeenkomst of statuut van deze regeling kan worden afgeweken.

Uit artikel 3 van de softwarerichtlijn volgt dat de bescherming geldt voor alle auteurs die volgens de nationale wetgeving als auteurs van werken van letterkunde beschermd worden. In de Conventie van Bern is overeengekomen dat voor werken van letterkunde de plaats van de eerste publicatie en de verblijfplaats van de auteur als aanknopingspunten gelden.

3.2.3.7. De vermogensrechten van de auteur

De vermogensrechten van de auteur van een computerprogramma zijn viererlei: het reproductierecht, het adaptatie- en vertalingsrecht, het distributie- en volgrecht en het recht op mededeling aan het publiek (zie artikel 5 softwarebeschermingswet en de artikelen 1, § 1 en 3 auteurswet).

In de eerste plaats heeft de auteur van een computerprogramma het exclusief reproductierecht. Dit recht slaat op alle wijzen of vormen van reproductie en op alle onderdelen van het programma. Zowel tijdelijke als permanente reproductie worden bedoeld.

Inzoverre het laden, het in beeld brengen, het uitvoeren, het opslaan of het overbrengen van een computerprogramma een reproductie van dat programma vereist, is eveneens de toelating van de auteursrechthebbende vereist. In de huidige stand van de techniek kan een computerprogramma nooit worden gebruikt zonder een of andere vorm van reproductie. Uit artikel 6, § 1 van de softwarebeschermingswet volgt echter dat geen toestemming vereist is als dergelijke vormen van reproductie noodzakelijk zijn voor het gebruik van het computerprogramma door een rechtmatige verkrijger in overeenstemming met het door het programma beoogde doel (zie hierna).

Artikel 5 b) van de softwarebeschermingswet handelt over het adaptatierecht van de auteur en is overgenomen uit de Berner Conventie (artikelen 8 en 12). Toestemming van de auteur is o.m. vereist voor de vertaling van een programma van de ene programmeertaal naar de andere, van broncode naar machinecode of vice versa. Hetzelfde geldt voor alle toevoegingen, verbeteringen en andere wijzigingen aan het programma. Hier moet echter ook rekening gehouden worden met de uitzondering van artikel 6, § 1 van de softwarebeschermingswet (zie hierna).

Artikel 5 c) van de softwarebeschermingswet regelt het distributierecht. Deze bepaling zal in de praktijk voor het Belgisch recht de meest ingrijpende verandering vormen omdat ze het "bestemmingsrecht" van de auteur voor computerprogramma's zeer sterk beperkt. Het recht op de controle van de distributie van een copie van een programma is voortaan uitgeput, zodra die copie voor de eerste keer in de Europese Unie is verkocht. De auteursrechthebbende kan vanaf dat moment enkel nog controle uitoefenen op de verdere uitlening of verhuring van het programma of van die copie. Onder "verhuring" wordt de terbeschikkingstelling van de betrokken copie voor een beperkte tijdsduur en tegen vergoeding verstaan. Een licentie met een beperkte tijdsduur is dus een verhuring in de zin van deze bepaling.

De "uitputting" van de rechten van de auteur op de verdere distributie van zijn programma treedt enkel op voor exemplaren die in de Unie zijn verkocht. Als een gebruiker in België via de post een exemplaar van een programma koopt bij een verdeler in de Verenigde Staten, is dat exemplaar "in" de Unie verkocht. De Belgische koper kan zijn exemplaar dus zonder toestemming van de auteur verder verkopen in alle landen van de Unie. De softwarebeschermingswet vereist wel dat de verkoop door de auteursrechthebbende of minstens met zijn akkoord is gebeurd. Niet-toegelaten, zgn. "grijze" parallelverkoop vanuit de V.S. is dus geen "verkoop in de Europese Unie". Ook als de Belgische koper zelf het programma in de Verenigde Staten gaat halen, is het exemplaar niet in de Unie verkocht. Het is dan in de V.S. verkocht en achteraf in de Unie ingevoerd. Voor het verder verkopen van dat exemplaar is dan de toestemming van de auteur vereist.

Artikel 1, § 1, vierde lid van de auteurswet kent tenslotte aan de auteur het exclusieve recht toe om het computerprogramma volgens om het even welk procédé aan het publiek mee te delen.

3.2.3.8. De morele rechten van de auteur

Naast de vermogensrechten, is de auteur ook titularis van een aantal morele rechten (artikel 1, § 2 auteurswet en artikel 4 softwarebeschermingswet). Deze rechten zijn onvervreemdbaar; de globale afstand van de toekomstige uitoefening ervan is nietig. De morele rechten betreffen het recht om het werk bekend te maken, het recht om het vaderschap van het werk op te eisen of te weigeren en het recht om zich te verzetten tegen iedere vervorming, vermindering, wijziging of aantasting die de eer of de faam van de auteur kunnen schaden. Uit de voorbereidende werken bij de softwarebeschermingswet blijkt duidelijk dat men m.b.t. computerprogramma's het recht op eerbied in het algemeen, d.w.z. het recht om zich te verzetten tegen elke wijziging zonder meer, zoals dit wordt erkend door artikel 1, § 2 van de auteurswet, buiten werking heeft willen stellen.

3.2.3.9. Rechten van de gebruikers

In artikel 6, § 1 van de softwarebeschermingswet staat dat de rechtmatige gebruiker van een computerprogramma zonder toestemming van de auteursrechthebbende mag overgaan tot reproductie, adaptatie en vertaling van dat programma, in zoverre dat noodzakelijk is voor het gebruik ervan voor het beoogde doel, o.m. om fouten te verbeteren. Van deze regeling mag echter contractueel worden afgeweken. De geldigheid van dergelijke contractuele afwijkingen moet weliswaar worden getoetst aan de principes van het verbintenissenrecht. Hierbij rijst de vraag naar de geldigheid van bepalingen in zgn. "shrink wrap" licenties (zie later).

Het recht om, behoudens tegenstrijdig contractueel beding, de software te reproduceren en aan te passen als dat noodzakelijk is voor het gebruik voor het beoogde doel, wordt enkel toegekend aan de "rechtmatige gebruiker". Dit is niet beperkt tot de persoon die het betrokken exemplaar heeft gekocht, maar sluit ook alle personen in die rechtmatig dit exemplaar mogen gebruiken (familieleden, collega's, e.a.), voorzover dat in de licentie-overeenkomst niet is uitgesloten¹⁸.

Tenslotte is het recht van de rechtmatige verkrijger ook beperkt tot handelingen die noodzakelijk zijn voor het beoogde gebruik van het programma. Dit beoogde gebruik kan afgeleid worden uit de licentie-overeenkomst of uit andere elementen waaruit de wil van de partijen kan worden afgeleid.

Het maken van een veiligheidskopie door een persoon die gerechtigd was om het programma te gebruiken, mag niet worden belet in een overeenkomst (artikel 6, § 2 softwarebeschermingswet). De veiligheidskopie moet echter noodzakelijk zijn voor het gebruik. Het is bijvoorbeeld mogelijk dat de leverancier zelf de veiligheidskopie levert of dat andere omstandigheden het maken van een veiligheidskopie door de gebruiker overbodig maken. De wet spreekt ook van "een copie" en

¹⁸

B. Czarnota & R. Hart, o.c., p.64

niet van verschillende veiligheidskopies. Tenslotte moet de copie ook bedoeld zijn voor de veiligheid en mag ze niet voor andere doeleinden worden gebruikt.

3.2.3.10. Reverse engineering en decompilatie

Op de informaticamarkt worden "interfaces" vaak geheim gehouden. De bedoeling is "bundling": men wil de klant ertoe brengen alles bij dezelfde constructeur aan te schaffen. Apparaten en programma's van andere makelij zijn namelijk niet "compatibel" met de hardware en de software van eigen constructie. Dit kan tot monopolievorming leiden.

Eén van de bedoelingen van de softwarerichtlijn bestond er precies in dit tegen te gaan. In één van de overwegingen bij de richtlijn staat "dat een computerprogramma de communicatie en wisselwerking met andere componenten van een computersysteem (...) moet verzorgen en dat hiervoor een logische en, waar nodig, fysieke koppeling en interactie is vereist, waardoor tussen alle elementen van de programmatuur en apparatuur in alle door deze te vervullen functies, en andere programmatuur en apparatuur, een passende wisselwerking mogelijk is".

Om de markt open te houden en monopolievorming tegen te gaan, streeft men naar "interoperabiliteit". Men wil de "aankoppelbaarheid" van de machines en de programma's met machines en programma's van andere makelij vergemakkelijken. Omdat de programma's van andere oorsprong op de informaticamarkt enkel in gecompileerde en dus geëncrypteerde vorm te krijgen zijn, neemt men zijn toevlucht tot "decompilatie". Men tracht m.a.w. het programma terug om te zetten naar (leesbare) programmacode. Daarvoor moet men uit de machinecode de "menselijke" code proberen af te leiden. Deze praktijk heeft bij de voorbereiding van de softwarerichtlijn tot hevige discussies tussen voor- en tegenstanders geleid.

Eén van de moeilijkste bepalingen van de softwarerichtlijn is deze vervat in artikel 5, 3°, die werd overgenomen in artikel 6, § 3 van de Belgische softwarebeschermingswet. Daarin staat dat de rechtmatige gebruiker van een kopie van het programma, zonder toestemming van de rechthebbende, de werking van het programma mag observeren, bestuderen en uittesten, ten einde vast te stellen welke ideeën en beginselen aan een element van het programma ten grondslag liggen. Op het eerste gezicht is de rechtmatige gebruiker dus vrij om het programma te analyseren om er de ideeën en principes van te achterhalen. Dit lijkt ook evident omdat de ideeën en principes die aan de grondslag liggen van het computerprogramma, niet door het auteursrecht worden beschermd.

Eigenaardiger is dat de analyse van een computerprogramma, met de bedoeling er de ideeën en principes van te achterhalen, niet op om het even welke manier mag gebeuren. Dit is in het auteursrecht zeer ongewoon. Een schilder kan bijvoorbeeld zijn toevlucht nemen tot X-stralen om de verfstraken en de verschillende lagen van andermans schilderij te analyseren met de bedoeling om de gebruikte technieken beter te begrijpen. Dit zou volgens de Conventie van Bern over het auteursrecht ongetwijfeld toegelaten zijn. Nochtans is de röntgenfoto in zekere zin ook

een copie van het schilderij¹⁹. Artikel 6, § 3 van de softwarebeschermingswet zegt echter m.b.t. computerprogramma's dat de analyse enkel toegelaten is in zoverre dit gebeurt bij het rechtmatig laden of in beeld brengen, de uitvoering, transmissie of opslag van het programma. De reproductie van de code en de vertaling van de codevorm, in welke termen de softwarebeschermingswet decompilatie omschrijft, zijn dus uitgesloten. Men mag analyseren, maar zonder te decompileren. Decompilatie is enkel toegelaten onder de voorwaarden die in artikel 7 van de softwarebeschermingswet in navolging van artikel 6 van de richtlijn zijn beschreven.

Het eerste Commissievoorstel voor een softwarerichtlijn bevatte geen expliciete regeling m.b.t. decompilatie van computerprogramma's. Artikel 4 bepaalde enkel dat de reproductie van een computerprogramma op eender welke wijze en met eender welke middelen, zowel geheel als gedeeltelijk, de toestemming vergde van de auteursrechthebbende.

De publicatie van de eerste versie van het ontwerp van softwarerichtlijn deed een golf van kritiek ontstaan en van diverse zijden begon het lobbywerk om de Commissie ertoe te brengen de tekst te wijzigen. Een van de organisaties die aan het debat participeerden was de "Software Action Group for Europe", afgekort "SAGE". Deze organisatie verenigde ongeveer 170 software- en hardwareproducenten, waaronder IBM, Digital, Apple, Siemens, Microsoft, Lotus, e.a. De actie van SAGE was o.m. gericht tegen het feit dat de tekst van de Commissie geen expliciet verbod bevatte om programma's zonder de toestemming van de auteur te decompileren. SAGE kritiseerde de voorstanders van de "clean room" techniek. Daarbij wordt met twee teams gewerkt. Eén team decompileert het programma en probeert de niet-beschermden ideeën en principes te scheiden van de auteursrechtelijke elementen van het programma. Daarvoor moet uiteraard het hele programma worden gedecompileerd. Het eerste team wordt dan verondersteld om aan het tweede team enkel de niet-beschermden ideeën en principes door te geven. Daarmee ontwikkelt het tweede team dan een nieuw programma. SAGE argumenteerde dat deze "clean room" techniek alleen maar schijnbaar het auteursrecht van de auteur van het programma respecteert. Volgens SAGE leidde de techniek onvermijdelijk tot misbruiken. Bovendien hield SAGE staande dat enkel de grotere producenten hun toevlucht konden nemen tot "clean room" technieken. SAGE ging ermee akkoord dat het auteursrecht enkel de uitdrukkingwijze van een programma en niet de ideeën en principes kan beschermen. Om de ideeën en principes van een programma te achterhalen, was echter volgens SAGE geen decompilatie nodig. Ook het achterhalen van informatie over interfaces rechtvaardigde, volgens SAGE, geen decompilatie van een computerprogramma. Als een onderneming de toegang tot informatie over de interfaces van haar programma's opzettelijk zou beletten, kon de Commissie haar toevlucht nemen tot art. 86 EEG-Verdrag omdat dit een misbruik van economische machtspositie zou uitmaken. Naast de kritiek op het Commissievoorstel inzake decompilatie uitte SAGE ook nog bezwaren tegen het expliciet uit de auteursrechtelijke bescherming uitsluiten van de logica, de programmeertaal en de algoritmen van een programma (zie hoger).

Als reactie op SAGE werd het "European Committee for Interoperable Systems" ("ECIS") opgericht, waarin o.m. Amdahl, NCR, Oracle, Olivetti, Unisys, Sun Microsystems, e.a. deelnamen. ECIS ijverde voor de uitsluiting van interface specificaties uit de bescherming van het auteursrecht en voor het toelaten van decompilatie omdat dat de interoperabiliteit en de mededinging op de informaticamarkt zou stimuleren. ECIS vreesde dat een algemeen verbod om een programma te reproduceren zonder de toestemming van de

¹⁹ aldus J. Huet & J. Ginsburg, "Computer Programs in Europe: A Comparative Analysis of the 1991 EC Software Directive", *Columbia Journal of Transnational Law*, 1992, Vol. 30, nr 2 p. 358-359.

auteursrechthebbende elke vorm van decompilatie buiten de wet zou stellen.

De uiteindelijke tekst van artikel 6 van de softwarerichtlijn (artikel 7 van de softwarebeschermingswet) is een compromis. Voor de reproductie van de code en de vertaling van de codevorm in de zin van artikel 5 a) en b) van de softwarebeschermingswet is geen toestemming van de rechthebbende vereist als ze onmisbaar zijn om de informatie te verkrijgen die nodig is om de compatibiliteit van een onafhankelijk gecreëerd computerprogramma met andere programma's tot stand te brengen, op voorwaarde dat:

- deze handelingen worden verricht door de licentiehouder of door een ander die het recht heeft om een kopie van het programma te gebruiken, of voor hun rekening door een daartoe gemachtigd persoon;
- de gegevens die nodig zijn om de compatibiliteit tot stand te brengen nog niet eerder snel en gemakkelijk beschikbaar zijn gesteld voor deze personen;
- deze handelingen beperkt blijven tot die onderdelen van het oorspronkelijk programma die voor het tot stand brengen van compatibiliteit noodzakelijk zijn.

Ofschoon de bewoordingen van artikel 7 van de softwarebeschermingswet zeer streng lijken, laten ze toch vrij veel ruimte:

- decompilatie wordt in de enge betekenis van "reproductie van de code en vertalen van de codevorm verstaan"; het gaat dus enkel over het proberen terug te vinden van de broncode van het programma in een voor de mens leesbare vorm, op basis van de machinecode; dit is één vorm van "reverse engineering";
- decompilatie is zonder toestemming van de rechthebbende toegestaan als het onmisbaar is om de compatibiliteit van een eigen programma met andere programma's mogelijk te maken; men mag dus een programma decompileren om de compatibiliteit tussen twee andere programma's te realiseren; de decompilatie moet dus niet noodzakelijk gericht zijn om een programma aan het gedecompileerde programma te koppelen; het kan dus zijn dat men een netwerkbeheersprogramma moet decompileren om de koppeling tussen twee of meer toepassingen of tussen een toepassing en een besturingssysteem mogelijk te maken;
- artikel 7 zegt weliswaar dat de decompilatie beperkt moet blijven tot de onderdelen die voor het realiseren van de compatibiliteit noodzakelijk zijn; hoe kan men dat echter op voorhand weten ?; meestal zal men toch het hele programma moeten decompileren om de juiste werking ervan te achterhalen en vervolgens de informatie over de interfaces correct te kunnen interpreteren; bovendien kan men moeilijk op voorhand weten in welk onderdeel van het programma informatie over de interfaces verscholen zit, zonder eerst heel het programma te decompileren.

In het tweede lid van artikel 7 van de softwarebeschermingswet worden een reeks beperkingen opgelegd m.b.t. het gebruik van de informatie die men via de decompilatie verkregen heeft. De aldus verkregen informatie mag niet worden gebruikt:

- voor een ander doel dan het tot stand brengen van de compatibiliteit van het onafhankelijk gecreëerde programma;

- voor mededeling aan derden, tenzij dat noodzakelijk is met het oog op de compatibiliteit van het onafhankelijk gecreëerde programma;
- voor de ontwikkeling, productie of het in de handel brengen van een "qua uitdrukkingwijze in grote lijnen gelijk" programma of voor andere inbreuken op het auteursrecht.

Volgens sommige auteurs wordt door deze beperkingen niet de "clean room" techniek uitgesloten. Een eerste team decompileert het programma met de bedoeling om compatibiliteit tot stand te brengen. Het team geeft de informatie over de (niet auteursrechtelijk beschermde) ideeën en principes die aan de grondslag liggen van het programma door aan een tweede team. Dit tweede team maakt dan een qua functionaliteit (bv. tekstverwerking) gelijkaardig en dus concurrerend programma²⁰.

Tenslotte wordt in artikel 7, § 3 van de softwarebeschermingswet een formulering overgenomen uit de Conventie van Bern. In overeenstemming met de bepalingen van die Conventie mag artikel 7 niet zodanig worden uitgelegd dat de toepassing ervan ongerechtvaardigd nadeel voor de rechtmatige belangen van de rechthebbende oplevert of het normale gebruik van het computerprogramma belemmert. Het is voorlopig nog niet duidelijk welke uitleg aan de termen "ongerechtvaardigd nadeel" en "normaal gebruik" zal gegeven worden.

De bepalingen van de artikelen 6, § 3 en 7 van de softwarebeschermingswet zijn dwingend. Er kan niet van worden afgeweken bij overeenkomst. Dit volgt uit artikel 8 van de softwarebeschermingswet.

Ook de Amerikaanse rechtspraak oordeelde, o.m. in de zaak *Sega vs. Accolade*²¹ dat het decompileren van een computerprogramma onder bepaalde voorwaarden rechtmatig kan zijn.

Sega ontwikkelt en verkoopt de "Genesis" videospelcomputer. Accolade is in dezelfde sector actief en produceert spelprogramma's, o.m. cassettes die op de Genesis-console van Sega gebruikt kunnen worden. Sega stelt weliswaar haar software en haar naam onder licentie ter beschikking aan andere ontwikkelaars van spelprogramma's maar met Accolade bereikte Sega nooit een dergelijk akkoord. De belangrijkste reden was dat Accolade niet wenste in te gaan op de eis van Sega om voortaan enkel nog computerspelletjes onder licentie van Sega op de markt te brengen. Om desondanks de interfaces van de Genesis-console te kennen, nam Accolade haar toevlucht tot "reverse engineering". Zo slaagde Accolade erin om toch een nieuw spel voor deze console, onder de naam "Ishido" op de markt te brengen. Rond dezelfde tijd ontwikkelde Sega een systeem om haar console tegen dergelijke praktijken te beveiligen. Met dit systeem onderzoekt de console bij het opstarten of op de cassette met het spelprogramma een aantal bytes aanwezig zijn die de letters S-E-G-A voorstellen, en als dat het geval is wordt een boodschap op het scherm gebracht die zegt dat het programma op de cassette ontwikkeld is door, of onder licentie van, Sega. Accolade ontdekte de code door een reeks spelprogramma's van Sega te decompileren, en plaatste het systeem voortaan ook op de eigen cassettes. Daarbij werd echter nagelaten om de boodschap op het scherm ("dit programma

²⁰ aldus J. Huet & J. Ginsburg, o.c., p. 365, voetnoot 134

²¹ *Sega Enterprises Ltd. v. Accolade, Inc.*, _F.2d_ (9th Cir. 1992)(October 20, 1992 U.S. App. LEXIS 26645. Samenvatting in the Computer Law Monitor, Vol. 10, Nr 2, November 1992, 521.

is ontwikkeld door Sega...") te neutraliseren of te veranderen. Daarop bracht Sega de zaak voor de rechter. In april 1992 besliste het District Court dat decompilatie van een computerprogramma een inbreuk op het auteursrecht kon uitmaken en beval het Accolade om voorlopig deze activiteit stop te zetten. Deze beslissing werd echter in oktober 1992 door het Hof van Beroep verbroken. Volgens het Amerikaanse Hof decompileerde Accolade de betwiste software enkel om niet beschermde ideeën en functionele concepten van de Genesis-console te ontdekken. Om deze niet-beschermde elementen te ontdekken, was er voor Accolade geen andere weg. Accolade decompileerde de software van Sega niet met de bedoeling om aan namaak te doen, maar om, naast de door Sega of onder licentie van Sega ontwikkelde videospelen, aan de consument ook andere videospelen aan te kunnen bieden. Dit kon volgens de Amerikaanse rechters niet onrechtmatig genoemd worden²².

De inzake software geboden mogelijkheid tot decompilatie is veel beperkter dan de mogelijkheid tot reproductie van beschermde topografieën (zie infra).

3.2.3.11. Sancties

De softwarebeschermingswet voorziet in het bijzonder in strafsancties bij

- het in het verkeer brengen van onrechtmatige kopieën van softwareprogramma's; daarbij is het voldoende dat de betrokkene wist of redenen had om te geloven dat het om een onrechtmatige copie ging;
- het bezitten van onrechtmatige kopieën van softwareprogramma's voor commerciële doeleinden;
- het in het verkeer brengen of bezitten voor commerciële doeleinden van o.m. programma's die uitsluitend bestemd zijn om de ongeoorloofde verwijdering of ontwijking van de kopiëerbeveiliging van andere programma's mogelijk te maken.

Daarnaast gelden uiteraard ook de strafsancties m.b.t. inbreuken op de bepalingen van algemene aard of m.b.t. de werken van letterkunde uit de auteurswet.

3.2.3.12. Duur van de bescherming

De duur van de bescherming loopt tijdens het leven van de auteur, tot zeventig jaar na zijn overlijden of na het overlijden van de langstlevende auteur. Voor programma's die anoniem zijn of die door een rechtspersoon gemaakt zijn, duurt de bescherming zeventig jaar nadat het programma voor het eerst op geoorloofde wijze voor het publiek toegankelijk is gemaakt.

²² Voor een korte bespreking van deze beslissing, zie R. Stern, "Reverse Engineering of Software as Copyright Infringement - An update: Sega Enterprises Ltd. v. Accolade Inc.," EIPR, 1993,34.

3.3. DE RECHTSBESCHERMING VAN DATABANKEN

3.3.1. Inleiding

Artikel 1 van de Berner Conventie beschermt "de rechten van de auteurs op hun werken van kunst en letterkunde". Artikel 2, 1° bepaalt vervolgens dat de uitdrukking "werken van kunst en letterkunde" elke produktie omvat in de domeinen van letterkunde, wetenschap en kunst, ongeacht de uitdrukkingswijze en -vorm. Er volgt dan een lange lijst van voorbeelden van werken die door alle leden van de Berner Conventie aanvaard worden als uitdrukkingsvormen en -wijzen van werken op het domein van letterkunde, kunst of wetenschap. Dit is echter slechts een basislijst. Art. 2, 5° van de Berner Conventie (na de Akte van Parijs van 1971) luidt als volgt: "Collections of literary and artistic works such as encyclopaedias and anthologies which by reason of the selection and arrangement of their contents, constitute intellectual creations shall be protected as such, without prejudice to the copyright in each of the works forming part of such collections".

Uit deze laatste bepaling volgt dat de Berner Conventie slechts in een bescherming voor "collecties" voorziet als twee voorwaarden zijn vervuld. De eerste is dat het om een collectie van werken van kunst en letterkunde moet gaan. De tweede is dat de collectie zelf een intellectuele creatie moet zijn; de creativiteit kan liggen in de selectie of de ordening van de werken in de collectie. Compilaties van feitenmateriaal krijgen onder de Berner Conventie dus geen auteursrechtelijke bescherming. Hetzelfde geldt voor de auteurswet in België, die op dat punt de tekst van de Berner Conventie volgt²³.

3.3.2. Situering van de elektronische informatiemarkt

Iedereen weet dat "informatie" als een economisch produkt kan worden verhandeld. In ruil voor het verstrekken van een of andere informatie kan men m.a.w. een tegenprestatie of betaling eisen. De meest klassieke vorm waaronder informatie in het economisch verkeer wordt verhandeld is de gedrukte vorm. Dagbladen, tijdschriften, boeken, en andere papieren informatiedragers vormen dus een eerste segment in de informatiemarkt. Dat segment is wellicht nog altijd het belangrijkste maar het wordt toch langzamerhand verdrongen door de informatie-verstrekking via de ether, m.a.w. door de radio en - veel meer nog - de televisie. In dit segment van de informatiemarkt gaat het dus over (via de ether) uitgezonden informatie.

Een derde segment in de informatiemarkt is de rechtstreekse informatie. Hierbij denken we vooral aan de momenteel zeer drukke markt van studiedagen, conferenties, colloquia en symposia. Ook de opleidingen, bijvoorbeeld in de informaticasector, zijn een onderdeel van deze markt. Bovendien hoeft "rechtstreekse" informatie zich niet tot "gesproken" informatie te beperken. Net zoals bij gedrukte en uitgezonden informatie is de vorm - woord of beeld - niet

²³ Voor de andere Lid-Staten van de Unie, zie V. Porter, "The Copyright Protection of Compilations and Pseudo-literary works in EC Member States", *Journal of Business Law*, 1993, p. 1.

relevant.

De elektronische informatieprodukten en -diensten vormen het vierde segment van de informatiemarkt. Deze vorm van informatie wordt momenteel meer en meer in "digitale" vorm verstrekt. Er zijn echter ook nog een hele reeks "analoge" elektronische informatieprodukten en -diensten, o.m. videocassettes of telefonische inlichtingendiensten. Een ander onderscheid binnen dit segment is dat tussen "on-line" en "off-line" produkten en diensten. "On-line" wordt de informatie verstrekt d.m.v. een telecommunicatieverbinding (kabelnetwerken of draadloze verbindingen). Voorbeelden van "off-line" produkten zijn magnetische of optische schijven (o.m. de CD-Rom).

Het onderscheid tussen deze vier segmenten van de informatiemarkt moet natuurlijk met een korrel zout begrepen worden. In de werkelijkheid zijn de grenzen tussen deze segmenten niet zo scherp. Heel vaak wordt dezelfde informatie ook onder verschillende vormen aangeboden. Een goed voorbeeld zijn de financiële beurskoersen. Deze worden niet alleen in de dagbladen gedrukt, maar ook door de radio uitgezonden of in de vorm van een elektronische databank aangeboden. Sommige produkten horen in meer dan één segment thuis. Zo worden "databanken" met gegevens als beurskoersen, sportuitslagen, weersvoorspellingen, nieuwsberichten, e.d. vaak "uitgezonden" via de ether. In Europa vindt men deze vorm van informatieverstrekking vooral terug onder de vorm van "teletekst", d.w.z. via permanente uitstraling van videotekstpagina's. De echte doorbraak van de "data broadcasting" markt blijft in Europa uit o.m. omwille van het tekort aan beschikbare zendfrequenties en de talrijke onzekerheden over wettelijke regelingen en marktrespons.

Op de elektronische informatiemarkt wordt een zeer uitgebreide waaier van produkten en diensten aangeboden. Om enigszins een overzicht te bewaren, wordt vaak teruggegrepen naar het onderscheid tussen elektronische informatie in de vorm van "gegevens" en elektronische informatie in de vorm van "documenten". "Gegevens" in deze zin zijn bv. adressen, beurskoersen, e.a. Men noemt dat vaak ook "primaire" informatie. Een CD-Rom met de gegevens van alle telefoonboeken van België zou een voorbeeld zijn van een "primaire" informatieprodukt. Een ander voorbeeld is een on-line databank met gegevens over conferenties en beurzen. Gegevens worden niet alleen via tekstkarakters op een beeldscherm ter beschikking gesteld. Het kan ook gaan om gesproken gegevensverstrekking. Men denke bv. aan de ook in België aangeboden "audiotext" of "infokiosk" diensten die via de gewone telefoon op te vragen zijn. Ook al dan niet bewegende beelden worden aangeboden, bv. via de optische beeldplaten. Er zijn ook al "multimediale" produkten, met daarenboven interactieve mogelijkheden, op de markt. Een goed voorbeeld is de interactieve beeldplaat (CD-I) waarin gegevens in de vorm van beelden, geluid en tekst over België zijn opgeslagen.

Bij "secundaire" informatie worden eigenlijk geen rechtstreekse gegevens aangeboden maar documenten in elektronische vorm ter beschikking gesteld. Een voorbeeld is databank waarin de belangrijkste artikelen van een dagblad worden opgenomen. Vaak wordt in dergelijke produkten niet het document in zijn geheel ter beschikking gesteld maar vindt men enkel een documentbe-

schrijving. Een voorbeeld daarvan is een elektronische bibliotheekcatalogus of een klassieke bibliografische databank. "Documenten" kunnen uiteraard tekst bevatten, maar ook al dan niet bewegende beelden en geluid, net zoals dat voor primaire gegevens het geval is.

Het onderscheid tussen primaire en secundaire informatieprodukten is, opnieuw, niet altijd even duidelijk. Heel vaak hebben we met "gemengde" produkten te doen. Een databank met bedrijfsinformatie bevat meestal een reeks primaire gegevens (adres, telefoon, telefax, samenstelling beheerraad, omzetcijfer, balansgegevens, e.a.) maar vaak ook persberichten over het betrokken bedrijf. Een ander voorbeeld van een gemengd systeem is een expertsysteem, waarin vaak ook een documentair onderdeel is ingebouwd. Hoe dan ook, belangrijk is vooral dat we ons bewust blijven van de zeer grote verscheidenheid wanneer we over de elektronische informatiemarkt spreken.

3.3.3. De toestand van de Europese elektronische informatiemarkt

Naar schatting zijn momenteel ongeveer 25% van alle toegankelijke on-line databanken van Europese origine. De Verenigde Staten produceren echter ruim 56% van alle on-line databanken. Het overwicht van de Verenigde Staten wordt nog versterkt omdat zij, meer dan de Europese databankproducenten, geïnvesteerd hebben in de meest rendabele onderdelen van de elektronische informatiemarkt, nl. de financiële en de economische databanken. De Europese producenten zijn traditioneel actiever in de minder winstgevende sectoren, o.m. die van de bibliografische databanken. Bovendien is het aandeel van de overheid in Europa veel groter dan in de Verenigde Staten. De positie van de Europese elektronische informatieproducenten is daardoor eigenlijk nog zwakker dan op het eerste gezicht uit de cijfers over het marktaandeel blijkt.

Een van de belangrijkste redenen voor de zwakke concurrentiepositie van de Europese Unie op de elektronische informatiemarkt is de fragmentatie van de Europese markt in een reeks kleine deelmarkten omwille van technische, linguïstieke en juridische barrières. Een goed voorbeeld van technische barrières is de onenigheid binnen de Europese Unie over de te volgen normen op het gebied van videotex. De taalbarrière is nog veel moeilijker. De overgrote meerderheid van de elektronische informatieprodukten en -diensten die in de Europese Gemeenschap worden geproduceerd, worden enkel in de taal van de producent aangeboden. Men richt zich dus meestal tot een beperkt nationaal publiek.

De juridische barrières vloeien vooral voort uit de onzekerheid nopens de rechtsbescherming van elektronische informatieprodukten en -diensten in de meeste Lid-Staten van de Europese Unie. In geen enkele nationale auteurswetgeving wordt op dit moment expliciet melding gemaakt van "databanken". Daarvoor is het verschijnsel wellicht nog te nieuw. Bovendien verloopt de ontwikkeling van de elektronische informatiemarkt in de onderscheiden Lid-Staten zeer onevenwichtig. Ruim de helft van de omzet van de Europese Unie op de on-line informatiemarkt wordt gerealiseerd in het Verenigd Koninkrijk. Ook Frankrijk en Duitsland zijn nog van enig belang, maar in de andere Lid-Staten is de omzet bijna verwaarloosbaar. Een ander onevenwicht

vinden we op de videotextmarkt, die vooral in Frankrijk (met de Minitel) is uitgebouwd. In 1988 telde men in Frankrijk al meer dan 5 miljoen videotextterminals, terwijl in de overige 11 Lid-Staten nauwelijks 330.000 videotextterminals werden geregistreerd.

Hierboven werd er reeds op gewezen dat compilaties van materiaal dat niet onder de bescherming van het auteursrecht valt, volgens de Berner Conventie, zelf ook geen auteursrechtelijke bescherming genieten. De Berner Conventie bevat echter slechts minimumregels en de meeste landen van de Europese Unie hebben een gunstiger regime. Het is dus goed mogelijk dat een specifieke databank wél door het auteursrecht beschermd wordt in de ene Lid-Staat maar daarom nog niet in een andere Lid-Staat van de Unie. Dit vormt een hinderpaal voor de ontwikkeling van een Europese informatiemarkt. Daarvoor is een gelijkwaardige rechtsbescherming voor databanken in alle Lid-Staten vereist. Bovendien moet die bescherming ook vergelijkbaar zijn met deze die aan databanken wordt verleend bij de belangrijkste handelspartners van de Europese Unie, vooral dus met de rechtsbescherming van databanken in de Verenigde Staten van Amerika.

3.3.4. Rechtsbescherming voor databanken in de USA

Voor de rechtsbescherming van databanken in de Verenigde Staten wordt meestal verwezen naar de beslissing van het Amerikaanse Hoogste Gerechtshof in de zaak *Feist Publications Inc. vs. Rural Telephone Service Co*²⁴.

Rural Telephone is een telefoonmaatschappij met het monopolie over de telefoondienst in een aantal zones in Kansas. De maatschappij verdeelt o.m. onder haar abonnees eenvoudige alfabetisch geordende telefoongidsen met enkel de naam, de stad het telefoonnummer van de abonnees. Feist Publications wilde een omvangrijkere telefoongids uitgeven die o.m. ook de zones van Rural Telephone bevatte, naast die van een reeks andere telefoonmaatschappijen. Met de meeste van die maatschappijen bereikte Feist een akkoord waarbij de rechten op de regionale telefoongidsen in licentie werden gegeven. Rural Telephone weigerde echter om met Feist samen te werken. Daarop kopieerde Feist de telefoongidsen van Rural Telephone. Veertig procent van de abonnees werden geëlimineerd omdat ze buiten het gebied woonden dat Feist wenste te bestrijken. Bovendien stuurde Feist bedienden op pad om voor elke resterende abonnee van Rural Telephone ook de straat en het huisnummer te achterhalen. Deze gegevens werden in de gidsen van Rural Telephone niet opgenomen. Blijkbaar slaagde Feist er niet in om alle gegevens uit de gidsen van Rural Telephone te verifiëren en aan te vullen. Uiteindelijk werden de gegevens van ongeveer 1300 abonnees (op het totaal van 7700 Rural abonnees) door Feist zonder meer gecopieerd. Daaronder zaten ook vier fictieve abonnees die Rural Telephone in zijn gidsen had ingelast om onwettige copies te kunnen opsporen. Rural Telephone daagde Feist dus voor de rechter wegens inbreuk op het "copyright". Zowel in eerste aanleg als in hoger beroep werd Feist veroordeeld op grond van de stelling dat telefoongidsen door het copyright worden beschermd. Het Hoogste Gerechtshof oordeelde er echter unaniem anders over. Het Hof oordeelde dat loutere feiten niet voor bescherming onder de copyrightwetgeving in aanmerking komen. Compilaties van feitelijke gegevens komen eventueel wél in aanmerking voor een dergelijke

²⁴ 111 S. Ct. 1282 (1991) ; zie o.m. R. Gorman, "The Feist Case : Reflections on a path breaking copyright decision", *Rutgers Computer and Technology Journal*, 1992, 731 ; Ph. Miller, "Life after Feist: facts, the First Amendment, and the copyright status of automated databases", *Fordham Law Review*, 1991, 507; Ph Bartz & J. Band, "Feist v. Rural Telephone: the beginning of the end of software overprotection", *Computer Law*, July 1991, 10.

bescherming, echter alleen op voorwaarde dat met de selectie en de ordening van die gegevens een zekere mate van "authorship" gepaard is gegaan. Dat veronderstelt niet alleen dat de compilatie op een onafhankelijke wijze tot stand is gekomen (en dus niet gekopieerd werd van iemand anders), maar tevens dat dit gebeurd is met een minimale "creativiteit". Volgens het Hof voldeden de telefoongidsen van Rural Telephone niet aan die voorwaarde omdat ze beperkt bleven tot een louter alfabetisch geordende lijst van abonnees. Het Hoogste Gerechtshof verwierp uitdrukkelijk de doctrine volgens dewelke "authorship" ook zou kunnen voortvloeien uit de moeite en de tijd die nodig was om de compilatie samen te stellen (de zgn. "sweat of the brow" doctrine). Moeite en tijd kan geen substituut zijn voor creativiteit, aldus de Amerikaanse rechters. Het gevolg was dat Feist toch gerechtigd was om de telefoongidsen van Rural Telephone te kopiëren, omdat die gidsen niet door het auteursrecht waren beschermd.

3.3.5. Rechtsbescherming van databanken: een overzicht

In het hierboven uiteengezette geding tussen Feist Publications en Rural Telephone gaat het over de vraag of een compilatie van feitelijke gegevens aan de voorwaarden voldoet om van de auteursrechtelijke bescherming te kunnen genieten. De feitelijke gegevens zelf worden nergens door het auteursrecht beschermd. Daarover is iedereen het eens. Compilaties van gegevens kunnen wél beschermd zijn, op voorwaarde dat ze aan de door het auteursrecht opgelegde originaliteitsvereiste voldoen.

Er zijn dus duidelijk verschillende niveaus. In de eerste plaats is er de vraag naar de auteursrechtelijke bescherming van het materiaal waaruit de databank is samengesteld. Anders gesteld: welke gegevens of documenten mag men vrij in een databank opnemen, zonder toestemming van de eventuele auteur van die gegevens of documenten. Om op die vraag te antwoorden moeten we terugrijpen naar de basisprincipes van onze auteurswet. Alle "werken" die door het auteursrecht worden beschermd, kunnen enkel mits toestemming van de auteur in een databank worden opgenomen. Niet beschermde gegevens en documenten, die vrij in een databank kunnen opgenomen worden, zijn o.m. werken die niet aan de originaliteitsvereiste van het auteursrecht voldoen, werken waarvan de termijn van auteursrechtelijke bescherming (70 jaar) is afgelopen, officiële akten, e.d.

Op een tweede niveau gaat het over de auteursrechtelijke bescherming van de databank zelf. Daarbinnen is er echter ook een onderscheid nodig. Men kan zich namelijk afvragen wát precies, m.a.w. welk aspect, van de databank eigenlijk beschermd kan worden.

Vooreerst kan het gaan over de selectie van het materiaal dat in de databank wordt opgenomen. Het selecteren van het materiaal kan gepaard gaan met een hoge mate van creativiteit. Men kan bijvoorbeeld een interessante databank aanleggen met een bloemlezing uit de middeleeuwse Russische poëzie. De selectie van de gedichten op zichzelf komt voor auteursrechtelijke bescherming in aanmerking, ook al is geen enkel ander aspect van de databank origineel genoeg om van het auteursrecht te kunnen genieten.

Na de selectie van het materiaal, komt, bij het ontwerpen van een databank, meestal de vraag naar de representatie. Hóe gaat men elk gegeven of document in de databank opnemen? In een klassieke gegevensbank rijst op dit niveau de vraag naar de "recordstructuur". Welke velden zal

men definiëren? Ook bij de oplossing van dergelijke vragen komt vaak een hoge mate van creativiteit kijken. Daardoor komt het dat een databank beschermd kan zijn door het auteursrecht, enkel vanuit het oogpunt van de representatiewijze van het opgenomen materiaal. Vervolgens is er de vraag naar de ordening van het materiaal in de databank. In de zaak tussen Feist en Rural Telephone hebben we een voorbeeld gezien van een louter alfabetische ordening. Het Amerikaanse Hoogste Gerechtshof oordeelde daarover dat een dergelijke ordening niet voldoende "authorship" bezat om onder de bescherming van het copyright te vallen. Een ordening kan echter veel gesofistikeerder zijn. Het materiaal kan bijvoorbeeld geordend zijn volgens het onderwerp. In een documentaire databank veronderstelt een dergelijke onderwerps-gerichte ordening van het materiaal een vaak zeer subjectieve beoordeling. Zo'n ordening is daarom ook meestal door het auteursrecht beschermd. Voor de ordening van het materiaal worden ook vaak auteursrechtelijk beschermde hulpmiddelen gebruikt, zoals thesauri of classificatieschema's.

De volgende stap is het programma dat voor de besturing van de databank wordt gebruikt. Dit is een gans ander onderwerp omdat we hier op het terrein komen van de rechtsbescherming van softwareprodukten (zie hoger).

Ook bepaalde vormen van gebruik van databanken kunnen voor bescherming in aanmerking komen. Ik denk hier o.m. aan het voorbeeld van een ervaren databankgebruiker die een uitgebreide bibliotheek van zoekformules over allerlei onderwerpen heeft aangelegd. Iedereen die met dit terrein wat vertrouwd is, weet dat het samenstellen van zo'n bibliotheek vaak veel creativiteit en intellectuele inspanning vereist.

Hetzelfde geldt wellicht ook voor het resultaat van een databankondervraging. Daarmee is de cirkel rond, want het resultaat dat men uit een ingewikkelde databankondervraging verkrijgt, is eigenlijk een "selectie", die op haar beurt door het auteursrecht beschermd kan zijn.

3.3.6. Rechtsbescherming van databanken in de Europese ontwerprijtlijn

3.3.6.1. Algemene bepalingen

In haar voorstel van richtlijn betreffende de rechtsbescherming van databanken²⁵ heeft de Commissie de verplichting opgenomen voor de Lid-Staten om te voorzien in de bescherming van databanken via het auteursrecht en databanken te beschouwen als "verzamelingen" in de zin van artikel 2, vijfde lid van de Berner Conventie voor de bescherming van werken van letterkunde en

²⁵ Voorstel voor een richtlijn van de Raad betreffende de rechtsbescherming van databanken, *PB.*, C 156 van 23 juni 1992, p.4. Zie verder : T. Dreier, "Die Harmonisierung des Rechtsschutzes von Datenbanken in der EG", *GRUR Int.*, 1992, pp.739-749; C. Gummig, "Der Schutz von Datenbanken vor dem Hintergrund der Harmonisierungsbemühungen der EG", *ZUM*, 1992, pp. 354-356; W.B.J. van Overbeek, "De ontwerp EEG Richtlijn betreffende de rechtsbescherming van databanken" , *Informatierecht*, 1992, pp 123-129; M. Röttinger, "Der Rechtsschutz von Datenbanken nach EG-Recht", *ZUM*, 1992, pp. 594-607.

kunst. Databanken zijn dus door het auteursrecht beschermd als "verzamelingen". Niet om het even welke verzameling komt echter in aanmerking. Artikel 2, derde van de ontwerprichtlijn zegt dat het moet gaan over een verzameling van werken of materiaal "die op grond van de keuze of de rangschikking ervan de eigen intellectuele schepping van de auteur vormt" en voegt daaraan toe: "Er worden geen andere criteria toegepast om te bepalen of een databank voor die bescherming in aanmerking komt". Met die bepaling wil de Commissie een min of meer geharmoniseerde toepassing van de originaliteitstest in de verschillende Lid-Staten van de Unie bereiken. De notie "eigen intellectuele schepping" is echter nog vaag genoeg om uiteenlopende beoordelingen mogelijk te maken. Daarentegen is de Commissie vrij restrictief gebleven door in artikel 2, derde lid te stellen dat de eigen intellectuele schepping van de auteur van de databank te maken moet hebben met "de keuze of de rangschikking" van het materiaal. Hoger hebben gezien dat de samenstelling van een databank, als een verzameling van werken of materiaal, ook andere aspecten behelst, zoals bv. de representatie van het materiaal. De term "rangschikking" is een ongelukkige, want veel te beperkte, Nederlandse vertaling van het Engelse "arrangement". Beter had men hier in de Nederlandse tekst over "ordening" gesproken.

Een "databank" is volgens artikel 1, 1 van de ontwerprichtlijn "een verzameling van werken of materiaal die met elektronische middelen zijn geordend en opgeslagen en op elektronische wijze kunnen worden opgevraagd, alsmede het elektronisch materiaal dat nodig is voor de werking van de databank, zoals het lexicon, de index of het systeem voor verkrijging of presentatie van informatie; de computerprogramma's die worden gebruikt voor de totstandbrenging of de werking van de databank vallen niet onder deze term". Deze definitie beperkt de term "databank" tot verzamelingen waarbij elektronische middelen worden gebruikt. Men mag daaruit niet a contrario afleiden dat verzamelingen waarbij geen elektronische middelen worden gebruikt, geen auteursrechtelijke bescherming kunnen genieten. Dat staat uitdrukkelijk in artikel 2, tweede lid van de ontwerprichtlijn. Het betekent enkel dat de bepalingen van de ontwerprichtlijn enkel voor verzamelingen op basis van elektronische media gelden. Voor "manuele" verzamelingen gelden de "gewone" auteursrechtelijke bepalingen.

De bepalingen van de ontwerprichtlijn gelden daarentegen voor verzamelingen van om het even welke "werken of materiaal". Het is dus niet relevant of het daarbij over tekstuele informatie gaat, of over al dan niet bewegende beelden of geluid. In de toekomst zullen deze vormen van informatie trouwens in toenemende mate samen worden aangeboden in zogenaamde "multimediale" databanken. Men moet er ook rekening mee houden dat voortdurend nieuwe technologische innovaties op dit terrein het licht zien. Op sommige terreinen, bijvoorbeeld de lucht- en ruimtevaart, worden "virtuele omgevingen" (zgn. "virtual reality") gecreëerd. In principe zijn dat eveneens "databanken" in de zin van de ontwerprichtlijn hoewel het op het eerste gezicht over driedimensionale objecten gaat. De derde dimensie is echter bij virtuele omgevingen slechts "virtueel" aanwezig. Ze wordt hoogstens gesimuleerd.

Uit de definitie blijkt verder dat men een onderscheid moet maken tussen de databank enerzijds, en de computerprogramma's die voor de samenstelling en/of het gebruik van de databank gebruikt worden, anderzijds. Dit onderscheid zal in de praktijk soms moeilijk te maken zijn.

Vele computerprogramma's die in deze sector gebruikt worden, bieden vaak een reeks initiële instrumenten waarmee de databank-ontwikkelaar zijn eigen produkt creëert. Deels wordt dus een eigen "programma" en deels een eigen "databank" opgezet. Daarbij kan een zekere verwarring ontstaan omdat in de definitie van de ontwerprichtlijn uitdrukkelijk staat dat "het systeem voor de verkrijging of presentatie van informatie" wèl tot de databank (en niet tot het programma) behoort. Maar anderzijds hebben we eerder al gezien dat de originaliteit enkel in de "keuze of de rangschikking" van het materiaal kan bestaan. Hoe valt dat te combineren ?

Volgens artikel 3 van de ontwerprichtlijn is de auteur van een databank "de natuurlijke persoon of groep van natuurlijke personen die de databank tot stand heeft gebracht of, voor zover het recht van de Lid-Staten het toestaat, de rechtspersoon die overeenkomstig dat recht als de houder van het recht wordt aangewezen. In België kan enkel een natuurlijke persoon als een auteur worden beschouwd. Dat wil echter niet zeggen dat de economische rechten van een auteur niet door een rechtspersoon zouden kunnen worden uitgeoefend. Een toepassing van dat principe vinden we in het vierde lid van artikel 3 m.b.t. databanken die tot stand worden gebracht door een werknemer in het kader van zijn dienstbetrekking of in opdracht van een werkgever. In dat geval is de werkgever - vaak een rechtspersoon - bij uitsluiting bevoegd om alle economische rechten met betrekking tot die databank uit te oefenen, tenzij bij overeenkomst anders werd bepaald.

De belangrijkste moeilijkheid bij de definitie van de "auteur" van een databank lijkt te liggen in de vraag wie de databank in de praktijk "tot stand heeft gebracht". Vaak is de ontwikkeling van een databank een langdurig, vaak nooit voltooid proces. Een databank kan worden gestart in een bepaald bedrijf en worden overgenomen en verder ontwikkeld in een ander bedrijf. Is er dan meerdere "co-auteurs" sprake. Dit zal vaak moeilijk uit te maken zijn.

De auteur van de databank heeft in elk geval, overeenkomstig artikel 5 van de ontwerprichtlijn het exclusief recht op de uitvoering en het verlenen van toestemming voor elke vorm van gehele of gedeeltelijke verveelvoudiging van de databank "op welke wijze en in welke vorm dan ook", voor de vertaling, de aanpassing, de bewerking of elke andere wijziging van de databank, voor de verveelvoudiging van de resultaten van vertalingen, bewerkingen, enz..., voor de distributie aan het publiek en voor de mededeling, demonstratie of uitvoering van de databank voor het publiek. Interessant om te weten is misschien dat, volgens de ontwerprichtlijn het "verhuren" van de databank of van kopieën ervan, tot de exclusieve rechten van auteur behoort. Men kan dus, zonder diens toestemming, bijvoorbeeld geen databanken op CD-Rom verhuren, bijvoorbeeld in het kader van een publieke bibliotheek of van een documentatiecentrum. Ook het ondervragen van databanken voor derden, dat vaak door documentatiediensten wordt toegepast, is aan de toestemming van de auteur onderworpen.

Daarentegen kan een rechtmatige gebruiker van de databank alle hogergenoemde handelingen uitvoeren, in zoverre die handelingen "noodzakelijk zijn voor het gebruik van die databank, op de wijze die is vastgesteld in contractuele overeenkomsten met de houder van het recht" (art. 6). Als er geen overeenkomst bestaat, kan de rechtmatige gebruiker, zonder toestemming van de houder

van het recht, alle hogergenoemde handelingen uitvoeren "die nodig zijn om de inhoud van de databank te raadplegen en te gebruiken". Deze laatste formulering is uiteraard bijzonder rekbaar en ze laat uiteenlopende interpretaties toe. Welke handelingen (bv. kopiëren van een deel van de databank op de eigen harde schijf) nodig zijn om de inhoud van een databank te gebruiken, is een zeer subjectieve kwestie.

In het voorgaande hebben we er al enkele keren op gewezen dat de Europese ontwerprichtlijn over de rechtsbescherming van databanken niet de inhoud van de databanken beoogt te beschermen. Deze bescherming is een aparte kwestie. Databanken kunnen - dat kwam ook reeds aan bod - zeer uiteenlopende soorten van "werken en materiaal" bevatten (tekst, geluid, al dan niet bewegende beelden). De auteursrechtelijke bescherming daarvan is in de onderscheiden Lid-Staten van de Europese Unie op zeer uiteenlopende wijze geregeld. De ontwerp-databankrichtlijn probeert daar geen harmonisatie in te brengen. Dat is veel te ingewikkeld en te delicaat. De ontwerprichtlijn laat de verscheidenheid binnen de Unie op dat domein dus verder bestaan. Uitzonderingen op het gebruik van auteursrechtelijk beschermde werken, bijvoorbeeld voor korte citaten of voor educatieve doeleinden, zoals die in het recht van sommige Lid-Staten worden toegekend, worden door de ontwerprichtlijn gehandhaafd, ook als die werken in een databank zijn opgenomen (art. 7).

De in het ontwerp voorgestelde duur van de auteursrechtelijke bescherming van databanken is dezelfde als die van literaire werken. In België is dat dus momenteel tot 70 jaar na de dood van de auteur. Databanken komen echter zelden op een bepaald moment tot stand. Er wordt voortdurend aan gewerkt en gesleuteld. Daarom is het niet zo eenvoudig om vast te stellen vanaf wanneer de auteursrechtelijke bescherming begint. Volgens de ontwerprichtlijn kunnen alvast enkel "wezenlijke wijzigingen" in de keuze of de rangschikking van de databank een nieuwe beschermingstermijn doen ontstaan. Niet-wezenlijke wijzigingen worden gedefinieerd als toevoegingen bij, weglatingen in of wijzigingen van de keuze of de rangschikking van de inhoud van de databank, die noodzakelijk zijn opdat de databank zou kunnen blijven werken op de door de maker ervan beoogde wijze". Dit is bijzonder restrictief! Weinig wijzigingen zijn echt noodzakelijk. Meestal gaat het over verbeteringen, die bijvoorbeeld het gebruik vergemakkelijken of de efficiëntie verhogen. Dat zouden dan volgens de definitie "wezenlijke wijzigingen" zijn.

3.3.6.2. Bibliografische beschrijvingen, uittreksels, citaten en samenvattingen

Tot hiertoe hebben we het gehad over de auteursrechtelijke bescherming van de databank zelf. Het gaat dan over de bescherming van de databank als een originele verzameling, origineel omwille van de doorgevoerde selectie of de rangschikking van het opgenomen materiaal. Op een ander niveau staat de auteursrechtelijke bescherming van de werken en het materiaal dat in de databank wordt opgenomen. Dit niveau wordt in de ontwerprichtlijn niet geregeld. Om te weten welke werken en welk materiaal in een databank mogen opgenomen worden, moet men dus rekening houden met het "gewone" auteursrecht van elke Lid-Staat.

Op één punt wil de Commissie echter toch ingrijpen m.b.t. dit niveau. Artikel 4 van het voorstel voor een databankrichtlijn bepaalt dat de toestemming van de auteursrechthebbende niet is vereist voor de opname in een databank van bibliografisch materiaal of korte uittreksels, citaten of samenvattingen die de originele werken niet kunnen vervangen. Dit laatste criterium - de al dan niet substitueerbaarheid - is overgenomen van de Franse cassatierechtspraak in de zaak "Microfor vs. Le Monde"²⁶. In deze zaak had het Hof van Beroep van Parijs geoordeeld dat Microfor niet gerechtigd was om zonder toelating de titels en de verwijzingen van artikels van het maandblad "Le Monde Diplomatique" en het dagblad "Le Monde" in een index op te nemen. Deze beslissing werd echter door het Hof van Cassatie tot tweemaal toe verbroken.

3.3.6.3. Bescherming tegen onrechtmatige opvraging

Zoals hierboven reeds enkele keren werd vermeld, kan de producent van een databank voor zijn produkt als zodanig slechts de bescherming van het auteursrecht inroepen op voorwaarde dat de databank door een zekere oorspronkelijkheid is gekenmerkt. Let echter op! Het gaat hier over de oorspronkelijkheid van de databank zelf, niet over de oorspronkelijkheid van het materiaal dat in de databank is opgenomen.

Vaak komt echter noch de databank zelf (m.a.w. de selectie, representatie, en ordening), noch het materiaal in aanmerking voor de bescherming van het auteursrecht. Dat laatste is vaak het geval wanneer het over een databank met louter feitelijke gegevens gaat. Feiten worden niet gegenereerd door een auteur. Ze bestaan zonder meer en worden door iemand waargenomen. Feiten, zoals beurskoersen, bedrijfsgegevens, namen en adressen van telefoonabonnees, e.d. komen dus niet voor de bescherming van het auteursrecht in aanmerking.

Toch kan de verzameling van feitelijke gegevens met het oog op het samenstellen van een databank een grote professionele en financiële investering vergen. Het ligt dus voor de hand dat men de persoon of het bedrijf die het risico neemt om een moeizaam samengestelde databank met feitelijke gegevens - of ander, niet door het auteursrecht beschermd materiaal - op de markt te brengen, een zekere bescherming biedt. Een dergelijke bescherming lijkt des te noodzakelijker nu het aftappen van een databank met de huidige technologie zo eenvoudig geworden is. Eender wie kan substantiële delen van een dergelijke databank op zijn eigen computer "downloaden", de gegevens herschikken en dan als een eigen produkt op de markt brengen. Het spreekt vanzelf dat niemand nog geneigd is om grote investeringen te doen in elektronische databanken met niet beschermde gegevens, indien daartegen geen enkele juridische bescherming voorhanden is.

Het is precies daarom dat de Europese Commissie in haar ontwerp-richtlijn een specifieke bescherming voorstelt. Aan de Lid-Staten wordt gevraagd om in hun wetgeving te voorzien in een recht voor de maker van een databank om te verhinderen dat de inhoud van die databank, geheel of voor een wezenlijk gedeelte, zonder zijn toestemming wordt opgevraagd en hergebruikt voor commerciële doeleinden (art. 2, 5). Dit recht, om de onrechtmatige opvraging

²⁶

Zie o.m. A. Kéréver, "Les Arrêts Microfor", R.I.D.A., 1988, nr 137, p 17.

van materiaal uit een databank te verhinderen, geldt ongeacht of die databank zelf auteursrechtelijke bescherming geniet of niet. In een voorbeeld als dat van Feist en Rural Telephone, zou laatstgenoemde telefoonmaatschappij via dit recht dus een middel hebben om Feist te verhinderen de telefoongidsen te kopiëren en te integreren in een eigen produkt. Het recht om onrechtmatige opvraging te verhinderen geldt dus altijd. Noch de databank zelf, noch het materiaal dat in die databank is opgenomen, moeten door het auteursrecht beschermd zijn.

Het recht om onrechtmatige opvraging te verhinderen zou, in het voorstel van de Commissie, enkel gelden voor de opvraging van wezenlijke onderdelen, en ook enkel voor commerciële doeleinden. De ontwerprichtlijn bepaalt dat de rechtmatige gebruiker van een databank zonder toestemming van de maker (d.i. de auteur) "niet-wezenlijke onderdelen" van werken of materiaal van een databank mag opvragen en hergebruiken voor persoonlijk gebruik in de privésfeer. Hetzelfde mag ook voor commerciële doeleinden maar dan moet de bron worden vermeld. Een "niet-wezenlijk onderdeel" wordt gedefinieerd als "onderdelen van een databank waarvan de verveelvoudiging, in het licht van een kwantitatieve en kwalitatieve evaluatie ten opzicht van de databank waaruit zij zijn gekopieerd, kan worden geacht geen schade toe te brengen aan de exclusieve rechten van de maker van die databank op de exploitatie ervan". Men kan zich afvragen of een dergelijke "definitie" in de praktijk enig nut zal opleveren.

De duur van het recht op verhindering van onrechtmatige opvraging bedraagt vangt aan op de datum waarop werken of materiaal in de databank worden opgenomen. Hij verstrijkt tien jaar na de dag waarop de inhoud van de databank voor het eerst rechtmatig ter beschikking werd gesteld van het publiek. De oorspronkelijke termijn van tien jaar wordt niet verlengd "door niet-wezenlijke wijzigingen in de inhoud". Hoger zagen we reeds dat met dat laatste noodzakelijke wijzigingen in de keuze of de rangschikking van de inhoud worden bedoeld. De normale bijwerkingen en zelfs verbeteringen in de structuur e.d. doen dus geen nieuwe tienjarige termijn ontstaan.

Wat gebeurt er dan met databanken die al meer dan tien jaar op de markt zijn? Behalve in het geval van wezenlijke inhoudelijke wijzigingen, moet men m.i. ervan uitgaan dat deze databanken niet door het recht op verhindering van onrechtmatige opvraging worden beschermd. Men zal dus in die gevallen, zoals thans, zijn toevlucht moeten nemen tot de regels die oneerlijke mededinging verbieden in het handelsverkeer. In elk geval is de termijn van tien jaar, die geïnspireerd is door de zgn. "catalogusregel" uit de auteurswetgeving van o.m. Denemarken, een belangrijke beperking van de door de Commissie geviseerde bescherming. Men kan zich afvragen of dat veel bijkomende investeerders zal kunnen verleiden tot het op het markt brengen van databanken met feitelijke gegevens.

De bescherming tegen onrechtmatige opvraging of onrechtmatig hergebruik geldt enkel voor databanken waarvan de maker onderdaan is van een Lid-Staat of zijn gewone verblijfplaats op het grondgebied van de Unie heeft. Indien de databank door een bedrijf is geproduceerd, moet dat bedrijf haar zetel, hoofdkantoor of voornaamste vestiging in de Unie hebben. Indien de onderneming die is opgericht overeenkomstig het recht van een Lid-Staat alleen haar

hoofdkantoor heeft op het grondgebied van de Unie, moeten haar verrichtingen een daadwerkelijke en duurzame band hebben met de economie van één van de Lid-Staten. Uitbreiding is mogelijk tot databanken uit derde landen via een beslissing van de Raad op voorstel van de Commissie. De Commissie stelt dus voor om de tienjarige bescherming tegen onrechtmatige opvraging in eerste instantie te beperken tot databanken van Europese makelij. Anderen kunnen er eventueel ook van genieten, maar wellicht enkel op voorwaarde van wederkerigheid.

3.3.6.4. De verplichte licentie van werken en materiaal

Artikel 8, 1 van de ontwerprichtlijn bepaalt dat voor werken of materiaal uit databanken die ter beschikking van het publiek zijn gesteld en die niet onafhankelijk kunnen worden gecreëerd of verzameld of uit andere bron verkregen, het recht om die werken of dat materiaal geheel of voor een wezenlijk deel voor commerciële doeleinden op te vragen en te hergebruiken, onder licentie ter beschikking moet worden gesteld onder eerlijke en niet-discriminerende voorwaarden. Het in licentie geven van het materiaal voor commercieel gebruik is dus enkel verplicht als het materiaal niet onafhankelijk kan worden gecreëerd of verzameld of uit een andere bron kan worden verkregen.

Het is niet zeer duidelijk aan welke voorbeelden de Commissie hier heeft gedacht. In haar commentaar bij de ontwerprichtlijn geeft de Commissie het voorbeeld van de beurs. "Als een Beurs in een Lid-Staat aan één of meer vragende partijen haar eindkoersen ter beschikking stelt, welke vervolgens door één van die partijen in een databank worden opgenomen, dan kunnen anderen, die ook de beurskoersen willen publiceren voor commerciële doeleinden deze beurskoersen krijgen aan dezelfde voorwaarden als de eerste databankproducent of, als ze verkiezen de databank van die eerste producent als bron te gebruiken, met die producent onderhandelen in dat perspectief".

Wat is echter de bedoeling? Moet, in het voorbeeld van de Commissie, de Beurs haar eindkoersen aan alle producenten onder dezelfde voorwaarden ter beschikking stellen? Dit lijkt een normale toepassing van het concurrentierecht. Of richt de verplichting zich tot de eerste databankproducent? In het voorbeeld van de Commissie kunnen de andere producenten de koersen toch op onafhankelijke wijze zelf van de Beurs krijgen. De eerste databankproducent is toch niet de enige bron voor die gegevens. In artikel 8, 1 wordt de verplichte licentie echter beperkt tot het geval dat het materiaal niet op onafhankelijke wijze kan worden gecreëerd of verzameld of uit een andere bron kan worden verkregen. Daarbij moet het blijkbaar gaan om een echte onmogelijkheid. Een verzoek om dergelijke licenties mag niet worden gebaseerd op commerciële overwegingen, zoals besparingen van tijd, werk of financiële investeringen (aldus de Commissie in Overweging nr. 33).

Er is ook al geopperd dat de Commissie wellicht gedacht heeft aan het voorbeeld van de

televisieprogrammaroosters²⁷, waarover een rechtsgeding werd gevoerd voor de Europese gerechtsinstanties (Independent Television Publications v. Commissie). In dit geval was de auteursrechthebbende de enige bron voor de uurroosters van de betrokken zender. Iedereen die deze roosters ook wou publiceren, moest ze dus verkrijgen van dezelfde eigenaar. De weigering om de roosters aan andere uitgevers ter beschikking te stellen werd door de Europese Rechtbank van Eerste Aanleg als een misbruik van economische machtspositie (art. 86 EEG-Verdrag) beschouwd. In dit voorbeeld ging het echter over auteursrechtelijk beschermd materiaal.

De verplichte licentie, die in artikel 8, 1 wordt voorgesteld, is echter beperkt tot het geval dat het materiaal in de databank niet door het auteursrecht is beschermd. Bovendien geldt de verplichting ook alleen maar als de databank, die de enige bron is voor de betrokken gegevens, ter beschikking van het publiek is gesteld.

In artikel 8, 2 van de ontwerprichtlijn wordt de verplichting om de inhoud van een databank onder bepaalde voorwaarden ter beschikking te stellen aan andere uitbaters uitgebreid tot het geval dat "de databank ter beschikking is gesteld van het publiek door een overheidsinstantie die bij wet is opgericht om informatie te verzamelen of ter beschikking te stellen, of die de algemene verplichting heeft om zulks te doen". Gedacht wordt o.m. aan juridische databanken of databanken met overheidsstatistieken. De bedoeling van de Commissie bestaat er vooral in om private investeerders toe te laten databanken op de markt te brengen met gegevens (bv. wetteksten) die tot nu toe enkel door een overheidsinstantie ter beschikking werden gesteld. Wat zijn echter "overheidsinstanties die bij wet zijn opgericht om informatie te verzamelen of ter beschikking te stellen of die de algemene verplichting hebben om zulks te doen"? In België zou daar zeker het Nationaal Instituut voor de Statistiek onder vallen. Maar het N.I.S. stelt in België voorlopig nog geen databank ter beschikking van het publiek, waarop een dergelijke verplichte licentie van toepassing zou kunnen zijn. Ook het Belgisch Staatsblad is een goed voorbeeld, maar ook deze administratie stelt voorlopig nog niet haar informatie via een databank ter beschikking van het publiek. Een administratie die daarentegen wel onder de verplichting zou vallen is "Justel", de juridische databank van het Ministerie van Justitie.

Tenslotte moet in dit kader ook nog art. 8, 3 worden vermeld, waarin aan de Lid-Staten wordt opgelegd om passende maatregelen te treffen met het oog op een regeling van geschillen tussen partijen in verband met de betrokken licenties.

3.4. DE BESCHERMING VAN TOPOGRAFIEËN VAN HALFGELEIDERPRODUKTEN

3.4.1. Inleiding

Op 26 januari 1990 verscheen in het Belgisch Staatsblad de wet van 10 januari 1990 betreffende rechtsbescherming van topografieën van halfgeleiderprodukten, naar Nederlands

²⁷ M. Pattison, "The European Commission's proposal on protection of computer databases", *European Intellectual Property Review*, 1992, 113.

voorbeeld, de "chipswet" genoemd. Ter naleving van de verplichtingen voortvloeiende uit de Richtlijn 87/54/EEG van 16 december 1986 van de Raad van de Europese Unie, strekt deze wet tot het invoeren van een specifieke wettelijke bescherming ten voordele van de maker - of van wie met de maker wordt gelijkgesteld - van een topografie van een halfgeleiderprodukt.

De wet strekt aldus tot het wettelijk erkennen van een nieuw intellectueel eigendomsrecht. Al de bestaande intellectuele eigendomsrechten, als daar zijn het auteursrecht, het octrooirecht, het merkenrecht, het tekeningen- en modellenrecht en het kwekersrecht, worden ongemoeid gelaten. Het uitgangspunt van deze wet is duidelijk om een sui generis beschermingsregime in het leven te roepen.

3.4.2. Wat zijn chips ?

"Chips zijn kleine, splinterdunne plakjes halfgeleidend materiaal - meestal silicium - waarop een enorm aantal microscopisch kleine, geschakelde elektronische componenten, zoals transistoren, condensatoren en weerstanden, zijn samengebracht."

Het samenbrengen van die elektronische componenten gebeurt op basis van tekeningen of designs die in het juridisch taalgebruik "topografieën" worden genoemd. Die designs worden geëst in een systeem van ingewikkelde lagen, en vormen aldus een circuit waarin de elektronische impulsen zo gestuurd worden dat de computer specifieke taken uitvoert. Vandaar de benaming geïntegreerde schakeling of "integrated circuit", in de praktijk meestal afgekort tot 'IC'.

Halfgeleiderprodukten spelen een steeds belangrijker rol, niet alleen in de elektronica-industrie zelf, maar in een hele waaier industriële sectoren. Grote investeringen zijn nodig om nieuwe en meer geavanceerde halfgeleiderprodukten te ontwikkelen, met name die welke steeds complexer moeten zijn om doeltreffend te kunnen worden gebruikt in de informatica-industrie. Het ontwerp- en fabricageproces van chips kan in het kort als volgt beschreven worden.

Het ontwerpen van een topografie wordt meestal voorafgegaan door een grondig onderzoek om vast te stellen aan welke technische en functionele specificaties de chip zal moeten voldoen (grootte, geheugencapaciteit, snelheid, enz.). Aan de hand van deze specificaties wordt de logische structuur van de toekomstige chip bepaald (logic design). Vervolgens worden elektronici aan het werk gezet, die tot taak krijgen een elektronische schakeling in schematische vorm te ontwerpen die aan deze structuur beantwoordt (circuit design).

Op basis hiervan gaat dan de eigenlijke chips-ontwerper aan de slag. Aan hem de zeer complexe taak het schakelschema in een driedimensionaal ontwerp van minimale afmetingen om te zetten (lay-out determination). Het spreekt vanzelf dat hierbij de hulp van de computer wordt ingeroepen. In toenemende mate maken ontwerpers bijvoorbeeld gebruik van in databanken opgeslagen standaard 'bouwstenen' (standard cells). Een andere manier om het de ontwerper gemakkelijker te maken is uit te gaan van bestaande gate arrays. Dat zijn standaard leverbare

chips, die nog een laatste bewerking moeten ondergaan : alleen de verbindingen tussen de verschillende (blokken van) componenten moeten nog worden ontworpen.

Het resultaat van de ontwerpfase is een serie op elkaar passende werktekeningen, die ieder één laagje chip voorstellen, veelal vastgelegd op een computerband (de databasetape). Van deze tekeningen, wordt vervolgens voor ieder laagje afzonderlijk een sjabloon, een zogeheten masker, gemaakt. Met behulp van deze, op glazen platen vastgelegde maskers vindt de fabricage plaats, waarbij gebruik gemaakt wordt van 'foto-lithografische' etstechnieken om de chip laagje voor laagje op te bouwen. Het eindprodukt van dit procédé is een wafer (wafel), een dunne schijf silicium met een doorsnee van ongeveer tien centimeter, bestaande uit honderden chips. De chips worden vervolgens uit de wafer losgezaagd en gemonteerd in een plastic of keramisch omhulsel, voorzien van pootjes voor de verbindingen met de buitenwereld. In het eindprodukt is de eigenlijke chip dan niet meer te zien.

De voornaamste voordelen van semiconductor chips zijn betrouwbaarheid, compactheid, massaproductie en laag stroomverbruik. In haast alle hedendaagse elektronische produkten is de chip het hart van de apparatuur. Geheugenchips worden voornamelijk toegepast in computers, terwijl men micro-processoren terugvindt in allerlei andere produkten zoals foto- en filmcamera's, auto's, radio's, telefoons, televisies, wasmachines en tal van andere consumentgerichte electronica-apparatuur.

3.4.3. Ontstaansgeschiedenis van de chipswet

3.4.3.1. De Verenigde Staten

De economische dreiging van de invoer van nagemaakte chips door voornamelijk Japanse producenten was de voornaamste drijfveer voor het Amerikaans Congres om legifererend op te treden. In het begin van de jaren tachtig werd de vraag om bescherming van de eigen chip-industrie door de Reagan administratie positief beantwoord. De Semiconductor Chip Protection Act, die werd afgekondigd op 8 november 1984, houdt belangrijke handelsbelemmeringen voor niet-Amerikaanse producenten in.

De Amerikaanse wet beschermt maskers of 'mask works' die zijn gefixeerd in een semiconductor chip. De bescherming wordt verworven vanaf de datum van de registratie of van de eerste commerciële exploitatie van het masker. De Amerikaanse wet vertoont een dubbele bijzonderheid : enerzijds betreft het de eerste wetgeving ter wereld inzake topografieën van halfgeleiderprodukten en, anderzijds voert zij een systeem van wederkerigheid in. De wet bepaalt onder welke voorwaarden maskers van onderdanen van vreemde staten kunnen genieten van de Amerikaanse rechtsbescherming. Hierdoor wijkt deze wet af van het in auteursrecht erkende assimilatiebeginsel. Door de aanvaarding van de Universele Conventie voor het Auteursrecht (van 6 september 1952) en de Conventie van Bern (van 26 juni 1948) verleent een verdragsluitende staat aan een onderdaan van een der aangesloten landen dezelfde auteursrechtelijke bescherming als aan de eigen onderdanen. Een Amerikaanse softwareproducent

bijvoorbeeld zal, voor de produkten die in België gecommmercialiseerd worden, op het Belgische auteursrecht beroep kunnen doen.

Buiten het geval waarin de eigenaar van een masker een statenloos persoon is of een onderdaan van een vreemde staat is met verblijfplaats in de V.S., en buiten het geval waarin de eigenaar van het masker zijn eigendomsrechten op dit masker aan een Amerikaanse onderneming overdraagt, kunnen mask works van niet-V.S. onderdanen in de V.S. slechts van de door de wet geboden bescherming genieten in een viertal situaties.

Een eerste situatie is die waarin de eerste commerciële exploitatie van het masker plaatsvindt in de V.S., en een tweede situatie is die waarin de auteur van het masker staatsburger of ingezetene is van een vreemde staat die partij is bij een verdrag betreffende de bescherming van maskers waarbij ook de V.S. partij is.

Een derde situatie, waaruit zeer duidelijk de toepassing van het reciprociteitsbeginsel blijkt, betreft de situatie waarin het masker van de niet-V.S. onderdaan onder de werking van een Presidential Proclamation valt. Telkens de President van de Verenigde Staten vaststelt dat een vreemd land aan de eigenaars van maskers die burgers of ingezetenen zijn van de V.S., het voordeel toekent van een bescherming gelijkaardig aan die toegekend door de Amerikaanse wet, kan hij, bij wijze van proclamatie, de bescherming uitbreiden tot de onderdanen en ingezetenen van het gegeven land.

Staten moeten dus om niet naast een Presidential Proclamation te grijpen, best een chipswetgeving in het leven roepen die een kopie is van de Amerikaanse chipswet.

Duidelijk blijkt in ieder geval dat indien staten hun onderdanen op definitieve wijze, d.w.z. onbeperkt in tijd, van de door de Amerikaanse wet geboden bescherming willen laten genieten zij ofwel moeten toetreden tot een verdrag betreffende de bescherming van chips waartoe ook de V.S. is toegetreden, ofwel moeten trachten in het bezit te komen van een Presidential Proclamation.

Gezien evenwel de totstandkoming en ratificatie van een verdrag veel tijd vraagt, is het in het bezit komen van een bovengenoemde presidentiële proclamatie op middellange termijn de enige oplossing.

Het legifereren binnen het kader van de nationale rechtsorde kan echter ook veel tijd in beslag nemen. Vandaar dat de Amerikaanse wet een vierde situatie van wederkerigheid voorziet. De Secretary of Commerce kan interim-bescherming toestaan aan de burgers van een vreemd land, voor een duur van drie jaar, te rekenen vanaf de afkondiging van de wet, indien hij van mening is dat dit land ernstige inspanningen en redelijke vooruitgang bereikt om een verdrag met de Verenigde Staten in dit domein af te sluiten of om een zulkdanige wetgeving aan te nemen dat de President later de wederkerigheid kan proclameren. Deze tussentijdse bescherming wordt bekomen bij wege van ordonnantie.

3.4.3.2. Europa

Een aantal geïndustrialiseerde landen, waaronder Japan, Zweden, Australië, Canada, Groot-Brittannië en Nederland wilden hun onderdanen zo snel mogelijk laten genieten van de door de Amerikaanse chipswet geboden bescherming. Daarom richtten zij vrij vlug na de inwerkingtreding van deze wet een verzoek tot het verkrijgen van een interim-order. Ook de Commissie van de Europese Unie diende vrij snel een verzoek in.

Vertegenwoordigers van de Europese elektronische industrie hadden aan de Commissie hun bezorgdheid medegedeeld om de toestand gecreëerd door de afkondiging van de Amerikaanse wet en de aandacht gevestigd op de nadelen en risico's die een inadequate of te trage aanpassing van de wetgeving in de Lid-Staten zou kunnen vertegenwoordigen. Inderdaad, bij gebreke aan een duidelijke bescherming in het land van oorsprong, zouden de halfgeleiderprodukten gecreëerd in de Unie niet passend worden beschermd op de belangrijke Amerikaanse markt want, onafhankelijk van de mogelijkheid een tussentijdse bescherming te vragen, zou de President van de Verenigde Staten zeker niet de wederkerigheid verklaren op grond van het bestaande octrooi- of auteursrecht.

Daarom oordeelde de Europese Commissie het wenselijk een ontwerp van richtlijn op te stellen om een coherente ontwikkeling te verzekeren van de wetgevingen van de verschillende lidstaten van de Europese Unie in dit domein.

Op 19 juni 1985 nam de Raad van Europese Unie een resolutie aan, waarin beslist werd het voorstel van richtlijn van de Commissie te onderzoeken teneinde zo snel mogelijk over de aanvaarding daarvan te beslissen. Het voornemen van de Commissie tot het uitvaardigen van een richtlijn en de resolutie van de Raad van 19 juni 1985, hebben het mogelijk gemaakt dat een verzoek tot interim-bescherming met succes kon voorgesteld worden. Aldus hebben de producenten van halfgeleiderprodukten in de Unie eerst een tussentijdse bescherming gekregen tot 8 november 1987. Na deze verlening van interim-bescherming gingen de werkzaamheden binnen de E.G. in snel tempo verder om uiteindelijk op 16 december 1986 uit te monden in een Richtlijn betreffende de rechtsbescherming van topografieën van halfgeleiderprodukten.

De Richtlijn voorziet dat de Lidstaten uiterlijk op 7 november 1987 de nodige wettelijke bepalingen in werking moesten stellen om aan de richtlijn te voldoen en dit omdat 8 november 1987 de uiterste datum was waarvoor krachtens de Amerikaanse wet interim-bescherming kan worden verleend. Ten gevolge van de wijziging van de Amerikaanse wet die het de Minister van Handel mogelijk maakt een tussentijdse bescherming toe te staan tot 1 juli 1991, werd de interim-order verscheidene malen verlengd. Op 31 december 1990 diende elk land van de Unie te beschikken over een aangepaste wetgeving opdat zijn onderdanen zouden kunnen genieten van de wederkerigheid krachtens een presidentiële proclamatie. De Belgische wet werd uitgevaardigd op 10 januari 1990.

3.4.4. Beschermingsregime

Zoals uit de ontstaansgeschiedenis van de chipswetten blijkt, werd geopteerd voor de creatie van een nieuw intellectueel eigendomsrecht om topografieën te beschermen. Men spreekt van een sui generis beschermingsregime. De bescherming van de Amerikaanse industriële belangen (via het wederkerigheidsbeginsel) is hier niet vreemd aan.

Maar was de fabrikant van een halfgeleiderprodukt dan niet beschermd door de bestaande beschermingsregimes zoals octrooi- en/of auteursrecht ?

Zoals gekend beschermt het auteursrecht "werken van letterkunde" wat evenwel alle soorten geschriften kunnen zijn die voldoende origineel zijn. De schakelschema's of patronen van een chip kunnen dezelfde originaliteit vertonen als de lay-out van een examenantwoordblad dat door een computer wordt nagekeken. In de Verenigde Staten wordt aan dergelijk geschrift auteursrechtelijke bescherming gegeven. De Copyright Office in de V.S. aanvaardde deze diagrammen en foto-beelden als "technische tekeningen" (cfr. plannen en ontwerpen onder de Bern Conventie).

Maar deze bescherming is beperkt omdat een topografie uiteindelijk uit "samenhangende beelden" bestaat, zodat de chip kan nagemaakt worden zonder inbreuk te maken op het auteursrecht op één tekening. Anders gezegd: het is het driedimensionaal patroon dat dient beschermd te worden, en dit is door copyright niet mogelijk.

Bovendien verleent de Copyright Act in de V.S. geen bescherming aan het ontwerp van gebruiksvoorwerpen (useful articles) tenzij het ontwerp beeldende of grafische eigenschappen vertoont die afzonderlijk en onafhankelijk van de nuttige eigenschappen van het produkt kunnen aangeduid worden en bestaan. Op grond van deze regel werd geoordeeld dat chips geen "ornamental articles" doch "useful articles" waren en dat de ontwerpen (lay-outs) gebruikt in de chip louter functioneel waren en onafscheidelijk verbonden aan de nutsfunctie van de chip.

De conclusie van dit alles is dat, ondanks de verdedigers van de toepassing van het auteursrecht, geen enkele Amerikaanse rechtbank uitspraak heeft gedaan over de bescherming van chips door het auteursrecht zodat de rechtsonzekerheid uiteindelijk leidde tot een wetgevend initiatief.

Dat de nieuwe wet geen amendement op de Copyright Act werd, heeft te maken enerzijds met de bekommernis om de systematiek van de Copyright Act te bewaren, doch anderzijds met de behoefte tot afscherming van de Amerikaanse industrie tegen vreemde concurrentie (cfr. supra). Hoewel de V.S. op dat ogenblik nog niet toegetreden waren tot de Conventie van Bern, was deze toetreding, en de aanvaarding van de universele auteursrechtelijke bescherming, in het vooruitzicht gesteld.

3.4.5. Beschermingsvoorwaarden

Wat zijn nu de voorwaarden waaraan een topografie moet voldoen wil zij voor bescherming in aanmerking komen ? Krachtens de wet moet de topografie het voortbrengsel zijn van de eigen intellectuele inspanning van de maker en mag zij in de halfgeleiderindustrie niet algemeen bekend zijn (artikel 2 Chipswet). Hiermede wordt letterlijk de tekst van de Richtlijn overgenomen.

In het voorstel van Commissie voorafgaand aan de Richtlijn, was de in aanmerking genomen beschermingsvoorwaarde de originaliteit. Dit is het criterium dat ook in de Amerikaanse wet gehanteerd wordt. Section 902 (b) van deze wet luidt : "Protection under this chapter shall not be available for a mask work that (1) is not original; or (2) consists of designs that are staple, commonplace or familiar in the semiconductor industry, or variations of such designs, combined in a way that, considered as a whole, is not original".

Gelukkig heeft men in de Richtlijn afstand genomen van het begrip oorspronkelijkheid als beschermingsvoorwaarde omdat dit enkel tot verwarring met de beschermingsvoorwaarden uit ons auteurs- of octrooirecht aanleiding zou hebben gegeven. Bovendien was vrij vlug gebleken dat oorspronkelijkheid gedefinieerd moest worden want dat dit begrip tot verschillende interpretaties in de verschillende Lid-Staten aanleiding zou geven. Gemakshalve is het begrip zelf verdwenen ten voordele van de twee bovenvermelde voorwaarden.

In wat verschillen deze twee beschermingsvoorwaarden inhoudelijk van de beschermingsvoorwaarden zoals die in onze auteurs- of octrooiwet gekend zijn ?

De voorwaarde dat de topografie van voortbrengsel moet zijn van de eigen intellectuele inspanning van de maker is verschillend en te onderscheiden van de in het auteursrecht gekende beschermingsvoorwaarde dat het door het auteursrecht beschermde werk de vrucht moet zijn van een originele schepping, d.w.z. dat het doordrongen en gekenmerkt moet zijn door de persoonlijkheid van de maker. In de chipswet ligt de nadruk op de geleverde inspanning van de maker, en niet zoals in de auteurswet, op het tot stand brengen door de maker van een "originele creatie".

De voorwaarde dat de topografie in de halfgeleiderindustrie niet algemeen bekend mag zijn, verschilt op haar beurt van de in onze octrooiwet aanwezige "nieuwheidsvereiste" van een uitvinding. De voorwaarde van nieuwheid in onze octrooiwet is absoluut en dus strenger dan de beschermingsvoorwaarde in de chipswet waar alleen vereist wordt dat rekening gehouden wordt met algemeen bekende anterioriteiten. Bovendien wordt in de meeste octrooiwetten een nieuwheidsonderzoek geëist, terwijl de bescherming van de topografieën automatisch gebeurt, zoals in het auteursrecht.

De beschermingsvoorwaarden in de chipswet bezitten een heel eigen inhoud, zij het dat zij nauwer aansluiten bij het auteursrecht dan bij het octrooirecht. De rechter zal wel in iedere voor

hem aanhangige zaak, en dit aan de hand van de feitelijke gegevens eigen aan die zaak, een beslissing moet nemen over het al dan niet vervuld zijn van de gestelde beschermingsvoorwaarden. Dit zal kunnen gebeuren in gedingen die voor hem hangende zijn naar aanleiding van een inbreuk op de op een topografie rustende rechten, waarbij de inbreukmaker in de loop van het geding opwerpt dat de topografie van de eiser niet aan de gestelde beschermingsvoorwaarden voldoet. Men kan dus geredelijk stellen dat het de partij is die beweert dat niet aan de wettelijke voorwaarden is voldaan, de bewijslast van haar bewering draagt.

3.4.6. Ontwikkeling van chips en software in dienstverband

Zoals dit ook voor octrooieerbare uitvindingen het geval is, komen de meeste topografieën tot stand in de schoot van een onderneming of worden zij op bestelling voor een opdrachtgever gemaakt. Wie moet in zo'n geval als maker van de topografie worden beschouwd ?

Volgens de gangbare interpretatie is de maker degene die de topografie heeft geschapen d.w.z. degene die het ontwerp van de topografie heeft ontwikkeld en de daaraan gegeven vorm heeft bepaald.

In tegenstelling met wat het geval is voor octrooieerbare uitvindingen door werknemers, voorziet de chipswet in deze gevallen in een uitdrukkelijke uitzondering op het beginsel van artikel 1 van de wet dat het exclusief recht toekomt aan de maker. De wet neemt de regeling uit de Richtlijn over, zoals ze overigens in het Belgisch recht reeds gekend is in de éénvormige Beneluxwet van 25 oktober 1966 inzake tekeningen of modellen. Indien een topografie door een werknemer in de uitoefening van zijn functie is gemaakt, wordt, behoudens andersluidend beding, de werkgever als de maker beschouwd (artikel 4, § 1).

Dit is een billijke regeling aangezien de werkgever de verantwoordelijkheid en het risico draagt van de grote investeringen die gemoeid gaan met het ontwikkelen van topografieën. Indien een topografie van een halfgeleiderprodukt op bestelling is gemaakt, wordt degene die de bestelling heeft gedaan als maker beschouwd, tenzij de overeenkomst anders bepaald (artikel 4, § 2).

Gelet op de uitdrukkelijke wettelijke regeling terzake lijkt het op het eerste zicht niet nodig in arbeidsovereenkomsten of overeenkomsten tot ontwikkeling van topografieën, een clause over de intellectuele eigendomsrechten op te nemen. In ontwikkelings- of aannemingsovereenkomsten is het echter raadzaam voor de opdrachtgever om te voorzien dat de wederpartij over de rechten beschikt die eventueel in hoofde van de personen die aan het project medewerken (personeelsleden, onderaannemers, etc.) zouden toekomen. Bij wijze van voorbeeld : "Opdrachtnemer zal erover waken alle eigendomsrechten te verwerven van alle personen die in haar dienst of opdracht werken, en dit zonder verdere vergoeding vanwege opdrachtgever."

Anderzijds is het ook zo dat het sluiten van een overeenkomst over de rechten de voorkeur verdient in alle internationale kontrakten, ook al omdat niet alle landen een regeling in hun wet hebben opgenomen. Zo kent de Nederlandse wet bijvoorbeeld geen suppletieve regeling omtrent

in opdracht ontworpen chips.

3.4.7. Decompilatie (reverse engineering)

De exclusieve rechten die krachtens de chipswet in hoofde van de maker van een topografie van een halfgeleiderprodukt ontstaan zijn het exclusief recht de topografie te reproduceren en ze commercieel te exploiteren (artikel 1 Chipswet). Volgens de memorie van toelichting bij de wet moeten deze rechten zeer ruim worden opgevat. Het monopolie beoogt alle vormen van reproductie, commerciële exploitatie en alle middelen om ertoe te geraken.

Anderzijds bevat de wet een Hoofdstuk 2 dat volledig gewijd is aan de beperkingen van de exclusieve rechten. Een exclusief recht beperken kan paradoxaal lijken, daar een exclusief recht per definitie geen enkele uitzondering kan hebben, want het verleent een monopolie. Het lijkt evenwel noodzakelijk enkele grenzen inzake de bescherming van topografieën van halfgeleiderprodukten in aanmerking te nemen, gelet op de specificiteit van de betrokken techniek en van de praktijk die eruit voortvloeit. Dit is ook het standpunt van de Amerikaanse wet en van de Europese Richtlijn, die drie gevallen voorziet waarin de lidstaten verplicht zijn, beperkingen in te voeren. Een van die beperkingen wordt gemeenzaam "reverse engineering" genoemd.

De regeling is vervat in artikel 10 van de wet, dat overeenstemt met het bepaalde in artikel 5, leden 3 en 4, van de Richtlijn. Letterlijk vertaald betekent reverse engineering de techniek van het "achterwaarts ontwerpen" ook decompilatie genoemd.

De beperking is gebaseerd op de praktijken van de fabrikanten van geïntegreerde schakelingen die, wanneer zij een geïntegreerd circuit van hun concurrent reproduceren, hierop een verbetering aanbrengen of het ontwerp ervan wijzigen. Het feit dat de tweede fabrikant zich belangrijke investeringen in werk en kapitalen getroost om het "tweede" geïntegreerd circuit op punt te stellen eerder dan klakkeloos te kopiëren, wordt gezien als een voldoende rechtvaardiging om reverse engineering toe te laten onder bepaalde voorwaarden. Bijgevolg schakelt artikel 10, littera a de toepassing van het exclusief recht uit wanneer de reproductie uitsluitend gebeurt voor de analyse, de evaluatie of het onderwijzen van de topografie of van de concepten, processen, systemen of technieken die in de topografie belichaamd zijn.

Hierbij eindigt het doorgaans niet. In het algemeen zal de concurrerende fabrikant de resultaten van deze analyses combineren met de inspanningen van zijn eigen ingenieurs om te komen tot een nieuwe en misschien verbeterde versie van het geïntegreerd circuit. Deze "nieuwe" versie zal de fabrikant willen vervaardigen en commercialiseren wat krachtens littera b van artikel 10 mogelijk is in de mate de twee voorwaarden vereist om te kunnen genieten van de bescherming toegekend door het exclusief recht verenigd zijn in hoofde van de concurrerende fabrikant : intellectuele inspanning en afwezigheid van banaliteit in de sector van de halfgeleiders.

Het leidt geen twijfel dat deze regeling aanleiding kan geven tot geschillen want de wettelijke uitzondering op het exclusief reproductierecht maakt het moeilijker om inbreuken aan te tonen:

daar waar klakkeloos kopiëren uit den boze is, is kopiëren en verbeteren geen plagiaat. De maker van een nieuwe topografie zal bijvoorbeeld willen aantonen, door het voorleggen van een uitgebreide documentatie van zijn werkzaamheden ('paper trail' genoemd), dat de nieuw ontwikkelde topografie het resultaat is van eigen inspanning.

3.5. RECHTSBESCHERMING VAN "COMPUTERWERKEN"

Een computer kan van dienst zijn bij het maken van bijvoorbeeld muziek, gedichten, tekeningen en ontwerpen. "Computer aided design" (CAD) is een belangrijk hulpmiddel geworden in de architectuur en in de industrie. Ook over het computerondersteund componeren van muziek wordt tegenwoordig veel gesproken. Vanzelfsprekend genieten ook deze zogenaamde computerwerken auteursrechtelijke bescherming, indien de door de auteurswet opgelegde voorwaarden zijn vervuld. Het volstaat dat het werk het resultaat is van een creatieve prestatie van een auteur. Dat de auteur bij de creatie van zijn werk gebruik maakt van een computer of van andere instrumenten doet niet ter zake.

Bij computergestuurde composities gaat men meestal uit van een basiswerk of van een matrix-werk. Op muzikaal vlak kan bijvoorbeeld een "computercomponist" een soort muzikaal sjabloon samenstellen. Met behulp van dit matrix-werk kan de componist of een derde een groot aantal afgewerkte muzikale werken produceren, op een volledig computergestuurde wijze. Men kan zich afvragen of deze eindwerken nog auteursrechtelijk beschermd moeten worden.

O.i. geldt echter ook hier de regel dat, indien de gebruiker van een matrix-werk zijn eigen persoonlijke stempel heeft gedrukt op zijn eindwerk, dit laatste bescherming geniet.

In elk geval kan nooit de computer zelf als "auteur" beschouwd worden. Een machine kan geen rechtssubject zijn. De Nederlandse auteur Van Offeren schrijft terecht dat, indien men deze "antropocentische" grondslag van het auteursrecht zou verlaten, bijvoorbeeld ook een kat die over een stempelkussen loopt en vervolgens over een stuk papier, daarbij een spoor achterlatend, als "auteur" van dit voortbrengsel beschouwd kunnen worden. Enkel een natuurlijke persoon kan dus als de maker van een auteurswerk beschouwd worden. De kernvraag daarbij is steeds of men kan spreken van een persoonlijke inbreng van de maker.

Met deze regel voor ogen moet men ook nieuwe fenomenen als automatische vertalingen of automatische creatie met behulp van een toevalsgenerator bekijken. Voor laatstgenoemde toepassingen geldt dat het gebruik maken van het toeval niet noodzakelijk een eigen persoonlijke inbreng van de maker uitsluit. Van Offeren maakt op dit punt een vergelijking met de schilderijen van Karel Appel die tot stand kwamen doordat hij de verf van op een afstand op het doek slingerde. Deze schilderijen zijn ook voor een deel met behulp van het toeval gemaakt, en toch twijfelt niemand aan de auteursrechtelijke bescherming ervan.

Hoofdstuk 2 De bescherming van de persoonlijk levenssfeer bij de verwerking van persoonsgegevens

1. UITGANGSPUNT VAN DE REGLEMENTERING

1.1. INLEIDING

Door de snelle verspreiding van computers in alle sectoren van onze samenleving en door de toename van de verbindingen tussen deze computers via private en publieke netwerken, zijn indrukwekkende mogelijkheden ontstaan op het gebied van de informatieverwerking. De verleiding om deze technieken maximaal te benutten bij de behandeling van persoonsgegevens is bijzonder groot. Vanaf de geboorte (of zelfs daarvoor) tot na het overlijden van een persoon kan, aan de hand van duizenden gegevens, een zeer gedetailleerde levensbeschrijving opgesteld worden voor elke burger: gegevens over zijn afkomst, zijn geboorte, zijn kinderjaren, zijn schooljaren, zijn militaire dienst, zijn huwelijk, zijn beroeps carrière, zijn gezin, zijn inkomen, zijn reizen, zijn interesses, zijn bezittingen, zijn ziektes, zijn verplaatsingen, enz. Een dergelijke, zeer volledige persoonsbeschrijving is bijzonder efficiënt voor de overheid, bijvoorbeeld bij het berekenen van persoonsbelastingen of sociale uitkeringen, bij de misdadbesteding of bij het tewerkstellingsbeleid.

Ook voor andere doeleinden is een zo groot mogelijke concentratie van persoonsgegevens bijzonder nuttig, bijvoorbeeld voor het personeelsbeleid of het commercieel beleid van een onderneming, of voor het onderzoeken van de betrouwbaarheid en de kredietwaardigheid van eventuele partners (in de meest ruime zin). Kortom, overal waar beslissingen moeten genomen worden over een persoon, is het nuttig om over die persoon zoveel mogelijk informatie te verzamelen. Dit streven naar efficiëntie bij de behandeling van persoonsgegevens houdt zeker gevaren in voor de individuele persoon. Enerzijds komt de persoonlijke levenssfeer ("privacy") in het gedrang, anderzijds kan een burger ook concrete morele of materiële schade lijden door het foutief gebruik van persoonsgegevens.

Het begrip "persoonlijke levenssfeer" is zeer moeilijk te omschrijven. Het is een bij uitstek relatief begrip waarvan de reikwijdte afhangt van de gevoeligheid van de betrokkene zelf of van de groep waartoe hij behoort, van omstandigheden, van tijd en plaats, enz. Meestal hanteert men het begrip op intuïtieve wijze: men voelt aan hoever de persoonlijke levenssfeer bij zichzelf reikt en past deze norm dan op anderen toe. Voor een jurist kan dit echter niet volstaan : hij moet aan het begrip een rechtsinhoud geven zodat het hanteerbaar wordt in het rechtsverkeer. Betreffende de bescherming van persoonsgegevens zou men kunnen stellen dat elke persoon in principe het recht heeft om zelf te beslissen welke informatie er over hem vrijgegeven wordt. Iedereen is dus meester over zijn eigen persoonsgegevens. Natuurlijk zijn daar grenzen aan. Men kan bijvoorbeeld niet weigeren aan de burgerlijke stand mee te delen dat men een kind heeft, of aan de fiscus hoeveel men verdiend heeft in het afgelopen jaar.

Ook zonder de toestemming van de betrokkene kunnen dus persoonsgegevens opgeslagen worden, zowel door de overheid als door private personen (werkgevers, scholen, banken, verzekeringsmaatschappijen, enz.).

Waar ligt in dat geval de grens ? Wellicht moet men die grens zoeken in het doel van het gegevensbestand (bv. fiscaal beleid, tewerkstellingsbeleid, onderzoek kredietwaardigheid, evaluatie van verzekeringsrisico, enz...). De realisatie van dit doel moet afgewogen worden tegen het principe dat iedereen meester is over zijn eigen persoonsgegevens. Voor deze afweging bestaan er geen toverformules. Hoogstens kan men enkele algemene richtlijnen formuleren maar de concrete afweging zal men moeten overlaten aan een - vooral t.o.v. de overheid - zo onafhankelijk mogelijk orgaan. Een algemene richtlijn is dan bijvoorbeeld dat een aantal persoonsgegevens (naam, adres, enz.) zo nodig zijn voor de normale communicatie tussen personen dat zij niet tot de persoonlijke levenssfeer gerekend kunnen worden. Een andere richtlijn zou kunnen zijn dat nooit meer persoonsgegevens mogen opgeslagen worden dan strict noodzakelijk is voor de realisatie van het doel waarvoor het gegevensbestand is aangelegd.

Naast het gevaar voor mogelijke inbreuken op de persoonlijke levenssfeer kan het gebruik - of misbruik - van persoonsgegevens ook aanleiding geven tot concrete morele of materiële schade. Zo kunnen er bijvoorbeeld verkeerde beslissingen over een persoon worden genomen omdat men zich op onjuiste, achterhaalde of onvolledige persoonsgegevens heeft gebaseerd: beslissingen over promotie, over toekenning van een krediet of een uitkering, over belastingen of sociale bijdragen.

De bescherming van persoonsgegevens is geen thema dat de Belgische publieke opinie sterk beroert. De discussie hierover blijft in zeer beperkte kring en bereikt zelden de massamedia. Enkele uitzonderingen hierop waren de oprichting van het Rijksregister, de persberichten over de fichiers van de Rijkswacht en het gebruik van sommige persoonsgegevens bij de toekenning van werkloosheidsuitkeringen door de Rijksdienst voor Arbeidsvoorziening. Doorgaans maakt de Belg zich echter weinig zorgen over het gebruik van zijn persoonsgegevens, en meestal ziet hij ook niet onmiddellijk in welke gevaren daaraan voor hem verbonden zouden kunnen zijn. Wellicht is dat de belangrijkste reden waarom in België zo weinig haast gemaakt is met het uitvaardigen van een wet over de bescherming van persoonsgegevens, ondanks de druk van onze buurlanden om daar snel werk van te maken. Laatstgenoemden vreesden, niet geheel ten onrechte, dat België een soort "dataparadijs" zou worden, waardoor de efficiëntie van hun eigen wetgeving in het gedrang kon komen.

Sedert einde 1992 beschikt België evenwel over dergelijke reglementering en begin 1994 werd zelfs in de Grondwet een artikel ingevoegd dat het recht op bescherming van de persoonlijke levenssfeer als grondrecht erkent.

1.2. PRIVACY EN BEROEPSGEHEIM

Nauw verwant met de bescherming van de persoonlijke levenssfeer is de regeling van het

beroepsgeheim. Het belangrijkste wetsartikel in dat verband is art. 458 van het Strafwetboek. "Geneesheren, heilkundigen, officieren van gezondheid, apothekers, vroedvrouwen en alle andere personen die uit hoofde van hun staat of beroep kennis dragen van geheimen die hun zijn toevertrouwd en deze bekendmaken buiten het geval dat zij geroepen worden om in rechte getuigenis af te leggen en buiten het geval dat de wet hen verplicht die geheimen bekend te maken, worden gestraft met gevangenisstraf van acht dagen tot zes maanden en met geldboete van honderd frank tot vijfhonderd frank".

Buiten dit algemeen artikel zijn er nog tal van specifieke bepalingen die de schending van het beroepsgeheim van specifieke groepen of beroepen sanctioneren. We denken o.m. aan art. 459 Sw. m.b.t. de agenten of bedienden van de Berg voor Barmhartigheid, art. 77 van de wet van 8 april 1965 voor het personeel van de jeugdbescherming of art. 244 van het Wetboek voor Inkomstenbelasting i.v.m. het beroepsgeheim van de fiscale ambtenaren.

De termen van art. 458 Sw. mogen niet te restrictief geïnterpreteerd worden. Zo is niet nodig dat de geheimen werden "meegedeeld". Een geneesheer die een vaststelling doet, krijgt evenzeer kennis van een geheim dat hem werd "toevertrouwd". Er is dus geen "actieve" mededeling van een boodschap vanwege de patiënt nodig. Verder moet art. 458 Sw. toegepast worden op alle personen bekleed met een ambt of een zending van vertrouwen, die aldus, ingevolge de wet of de gebruiken, de noodzakelijke vertrouwelingen van de hun toevertrouwde geheimen zijn²⁸. Het criterium van "noodzakelijke vertrouweling" is drievoudig: de bijstand van de beoefenaar van het beroep moet vereist zijn, het vertrouwen moet noodzakelijk zijn voor de uitoefening van het beroep en het beroep moet verband houden met het algemeen belang²⁹. Deze criteria moeten door de rechters getoetst worden n.a.v. concrete betwistingen.

Aldus heeft de rechtspraak al geoordeeld dat tot het beroepsgeheim gehouden zijn: advocaten, notarissen, priesters, magistraten en griffiers, officieren van de gerechtelijke politie, gerechtsdeurwaarders en curatoren. Daarentegen werd beslist dat art. 458 Sw. niet toepasselijk is op journalisten, wisselagenten, bankiers en verzekeringsmakelaars. Tot het beroepsgeheim zijn ook gehouden, de personen die naast de geneesheer, toegang hebben tot het medisch dossier, zoals het verplegend personeel, de kinesiterapeuten, e.a. Een geneesheer is ook gehouden tot het beroepsgeheim t.a.v. de verzekeringsinstelling waarvoor hij werkt, bv. voor het medisch onderzoek voor een levensverzekering.

Art. 458 Sw. vereist ook een kwaadwillig opzet. Het loutere inzicht of algemeen opzet is voldoende. Daarentegen zal art. 458 Sw. niet kunnen toegepast worden als de bekendmaking van een beroepsgeheim enkel te wijten is aan nalatigheid of onvoorzichtigheid. In dat geval zal het slachtoffer enkel een eis tot schadevergoeding op grond van art. 1382 BW kunnen indienen. Het gevolg van art. 458 Sw. is een zwijgplicht voor de geheimhouder. Daaraan beantwoordt echter

²⁸ Cass. 20 februari 1905, Pas., 1905, I, 141.

²⁹ Concl. Adv. Gen. Collard voor Cass., 26 september 1966, R.D.P., 1966-1967, 301.

ook een zwijgrecht. Men mag zich dus verschuilen achter het beroepsgeheim, ook als getuige t.o.v. een rechter. "L'obligation est celui de se taire, excepté en justice; le droit est de se taire, même en justice"³⁰.

Hoewel de regels inzake het beroepsgeheim nauw verwant zijn met de bescherming van de persoonlijke levenssfeer zijn er toch een aantal opmerkelijke verschillen. In de eerste plaats is de verplichting tot het bewaren van het beroepsgeheim vooral ingegeven door de bezorgdheid voor het voortbestaan van de betrokken ambten. De geneesheer, de advocaat, de notaris, de gerechtsdeurwaarder, de magistraat, e.a. ambten zijn grotendeels gebaseerd op het vertrouwen dat de verstrekte informatie niet bekendgemaakt zal worden. Die bezorgdheid blijkt o.m. uit het feit dat art. 458 Sw. van openbare orde is. Het is geen recht waarvan men afstand kan doen. Ze blijkt ook de leer van de "noodzakelijke vertrouweling", die o.m. vereist dat het om een ambt van openbaar belang moet gaan en dat de bijstand van de beoefenaar van het beroep vereist moet zijn. In de tweede plaats heeft het bewaren van het beroepsgeheim enkel te maken met de mededeling van geheimen. Een geheim heeft betrekking op zaken die men uit eigen voordeel best verborgen houdt. Bij het nagaan of men te maken heeft met een geheim zal de rechter dus niet alleen onderzoeken of het beweerd geheim al dan niet gekend was, maar ook of de bekendmaking de belangen van de betrokkene heeft benadeeld. Deze toetsing is niet vereist bij het invoeren van een schending van de persoonlijke levenssfeer. Daar hoeft het niet noodzakelijk over geheimen te gaan. In de derde plaats is het bewaren van beroepsgeheimen beperkt tot communicatie van gegevens. Bij de bescherming van de persoonlijke levenssfeer heeft men daarnaast ook oog voor de wijze waarop gegevens worden verkregen, opgeslagen, verwerkt en gebruikt. Ook als gegevens niet aan derden worden meegedeeld kan men dus met een schending van de persoonlijke levenssfeer te maken hebben. De plicht tot het bewaren van het beroepsgeheim is één van de middelen om de persoonlijke levenssfeer van de betrokken personen te beschermen. Getuigen daarvan zijn de verschillende bepalingen over het beroepsgeheim in de wet over de bescherming van de persoonlijke levenssfeer bij de verwerking van persoonsgegevens (o.m. van de verwerkers van persoonsgegevens, van de leden van de Commissie voor de bescherming van de persoonlijke levenssfeer, e.a.).

2. INTERNATIONALE BEPALINGEN

2.1. HET UNO-PAKT OVER DE BURGERLIJKE EN POLITIEKE RECHTEN

Artikel 17 van het UNO-Pakt van 19 december 1966 over de burgerlijke en politieke rechten (wet van 6 juli 1983) bepaalt: "Niemand mag worden onderworpen aan willekeurige of onwettige inmenging in zijn privé-leven, zijn gezinsleven, zijn huis en zijn briefwisseling, noch aan onwettige aantasting van zijn eer en goede naam. Een ieder heeft recht op bescherming door de wet tegen zodanige inmenging of aantasting".

³⁰ G. Schuind, *Traité pratique de droit criminel* (mise à jour par A. Vandeplas), I, Brussel, Swinnen, 1980, 416.

Het Hof van Cassatie heeft in verschillende arresten reeds in positieve zin uitspraak gedaan over de rechtstreekse toepasbaarheid van bepalingen van het genoemde UNO-Pakt in België. We mogen dus aannemen dat ook artikel 17 van dit Pakt door elke burger voor de rechters van dit land ingeroepen kan worden.

2.2. HET EUROPEES VERDRAG VAN DE RECHTEN VAN DE MENS

Artikel 8 van het Europees Verdrag tot Bescherming van de Rechten van de Mens (EVRM) luidt als volgt:

- "1. Eenieder heeft recht op eerbiediging van zijn privé-leven, zijn gezinsleven, zijn huis en zijn briefwisseling.
2. Geen inmenging van enig openbaar gezag is toegestaan m.b.t. de uitoefening van dit recht dan voor zover bij de wet is voorzien en in een democratische samenleving nodig is in het belang van 's lands veiligheid, de openbare veiligheid en het economisch welzijn van het land, de bescherming van de openbare orde en het voorkomen van strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen".

Bij de lectuur van artikel 8 EVRM merkt men dat in deze bepaling de bescherming van het privéleven aan talrijke uitzonderingen onderworpen is. Toch mag de juridische waarde van deze tekst niet worden onderschat.

Artikel 8 EVRM kan immers niet alleen voor de Belgische rechter worden ingeroepen. Na uitputting van de interne rechtsmiddelen, kan een eventuele schending ervan bovendien aanhangig gemaakt worden bij de Commissie en het Europees Hof voor de Rechten van de Mens in Straatsburg. Zowel de Commissie als het Hof hebben al interessante preciseringen geleverd van artikel 8 EVRM.

De beperkingen ingebouwd in artikel 8 werden door het Europees Hof vrij scherp omlijnd. Wat betreft de vereiste dat elke beperking moet worden voorzien in een wet bijvoorbeeld, heeft het Hof gepreciseerd dat het niet voldoende is dat de beperking een rechtsgrond heeft in het interne recht, maar dat de betrokken wet ook kenbaar en voorzienbaar moet zijn voor de betrokken personen. Een eventuele wet die overheidsinmenging in het privéleven toelaat moet dus in duidelijke bewoordingen gesteld zijn zodanig dat iedereen weet in welke gevallen en onder welke voorwaarden deze inmenging geoorloofd is. Het Europees Hof behoudt zich overigens het recht voor om zelf na te gaan in hoeverre een overheidsinmenging in het privéleven "noodzakelijk is in een democratische samenleving". De nationale overheden hebben hierover dus geen onbegrensde appreciatiebevoegdheid.

Art. 8 EVRM kan niet alleen door natuurlijke personen maar ook door rechtspersonen, bijvoorbeeld door een v.z.w. worden ingeroepen, en in bepaalde gevallen zelfs door een groep. De Commissie voor de Bescherming van de Rechten van de Mens heeft bijvoorbeeld ooit onderzocht of de inplanting van een groot gebouwencomplex in een regio waar enkel herders,

jagers en vissers leefden, geen schending was van art. 8 EVRM³¹. De bepaling kan verder niet alleen worden ingeroepen bij inmengingen vanwege de overheid, zoals uit de tweede alinea van art. 8 ten onrechte zou kunnen afgeleid worden. Het kan daarentegen ook toegepast worden op betrekkingen tussen particulieren³².

De reikwijdte van art. 8 is ook zeer breed. Art. 8 is bijvoorbeeld het artikel dat als basis diende voor de veroordeling van België wegens de discriminatie van natuurlijke kinderen in het bekende Marckx-arrest. Het is ook op grond van dit artikel dat Ierland is veroordeeld voor het de facto onmogelijk maken van de scheiding en tafel en bed³³.

Uit de toepassing van art. 8 EVRM kan men interessante preciseringen halen over het begrip "persoonlijke levenssfeer". Zo weet men nu bijvoorbeeld dat men bij de interpretatie daarvan rekening moet houden met de betrokken persoon en met plaats en tijd. De persoonlijke levenssfeer van een magistraat of een overheidsambtenaar vraagt bijzondere zorg en bescherming omdat dit zo belangrijk is voor het vertrouwen van het publiek. Het is belangrijk dat het privé-leven van een magistraat goed gescheiden blijft van de uitoefening van zijn ambt. Die scheiding is, naast de ambtsgewaden en de architectuur van de rechtszaal, zeer belangrijk voor het functioneren van de justitie. Omgekeerd is de persoonlijke levenssfeer van publieke personen, bijvoorbeeld uit de amusementssector of de koninklijke families, enger dan voor een doodgewone Jan met de pet.

Naast deze elasticiteit heeft het begrip "persoonlijke levenssfeer" ook een verschillende betekenis naargelang het slaat op de integriteit van de eigen lichamelijkeheid of op de relaties met anderen. In het eerste geval gaat het over de vraag in hoeverre een persoon over zijn eigen lichaam mag beschikken (zie bijvoorbeeld de discussies over de bloedproef bij verkeerscontroles, de verplichting tot het dragen van veiligheidshelm of autogordel, maar ook: het verbod om de as van een overledene in diens eigen tuin te verstrooien, en de discussies over de toepassing van art. 8 op verbodsbepalingen inzake o.m. homoseksualiteit, geslachtsverandering of abortus). In het tweede geval gaat het over de wijze waarop de persoon de relaties met zijn onmiddellijke omgeving organiseert (zie o.m. de beslissingen over de isolatiecellen bij vrijheidsberoving, de uitwijzing van vreemdelingen of het af luisteren van telefoongesprekken). Naast de integriteit van de eigen lichamelijkeheid en de relaties met de onmiddellijke omgeving, heeft het begrip "persoonlijke levenssfeer" ook te maken met het zelfbeschikkingsrecht op de informatie over zichzelf, of datgene wat in het Duits "informationelle Selbstbestimmung" wordt genoemd. Op dit aspect zullen we hierna nog in detail terugkomen, omdat het bij het gebruik van informatica van directer belang is.

³¹ Comm. 3/10/83, n° 9278-9415/81, D.R., Vol. 35, p. 30.

³² R. Ergec, *Protection européenne et internationale des droits de l'homme*, Vol. III, Brussel, Presses Universitaires, 1989-1990, p. 490.

³³ Arrest Airey van 9 oktober 1979, serie A, nr. 32.

De toepassing van art. 8 EVRM is meestal een kwestie van afweging en van zoeken naar een evenwicht tussen de bescherming van het individu en de noden van de overheid. Dat ziet men o.m. in de beslissingen over het recht van de fiscus om de privé-uitgaven van de belastingplichtige op te vragen. Het Hof van Cassatie oordeelde dat dit geen schending was van art. 8 EVRM³⁴. Daarentegen wordt het gebruik van een leugendetector bij een ondervraging door de politie wel als een inbreuk beschouwd, en hetzelfde geldt voor technieken als narco-analyse (het ondervragen onder verdoving). Ook een vraag van een bedrogen echtgenote om de in het bed van haar man gevonden pubisharen te vergelijken met die van de beweerdde maîtresse, werd als een inbreuk op de persoonlijke levenssfeer aanzien³⁵. Daarentegen werd het fotograferen van personen tijdens een manifestatie of de camerabewaking in een grootwarenhuis niet als een inbreuk beschouwd. Bij al deze beslissingen wordt telkens nagegaan of argumenten als openbare orde en veiligheid, misdaadpreventie, enz. opwegen tegen het fundamenteel recht dat door art. 8 wordt gegarandeerd.

Naast de "persoonlijke levenssfeer" beschermt art. 8 EVRM ook het familieleven (o.m. toegepast inzake bezoekrecht bij echtscheiding of gezinshereniging van migranten), de woning en het briefgeheim. De laatste twee aspecten kunnen in verband gebracht worden met twee artikelen van de Belgische grondwet. Art. 15 bepaalt dat de woning onschendbaar is en dat een huiszoeking slechts mag plaatsvinden in de gevallen en volgens de procedures die in de wet zijn bepaald. Art. 29 van de Grondwet handelt over de onschendbaarheid van het briefgeheim en zegt dat de wet dient te bepalen welke ambtenaren verantwoordelijk zijn bij een schending van het geheim van brieven die aan de post werden toevertrouwd. Het recht op het briefgeheim komt o.m. ter sprake bij de discussie over het recht van de werkgever om de brieven te openen die aan de werknemer op zijn werkadres zijn gericht. Dit kan worden uitgebreid tot het registreren van de telefoongesprekken in de onderneming of het controleren van de elektronische post. Door de Belgische rechtspraak is dit recht van de werkgever in principe aanvaard³⁶.

Art. 8 EVRM heeft weliswaar directe werking in de Belgische rechtsorde maar de directe werking is beperkt tot het verbod om zich in het privé- en het familieleven van een individu te mengen. Men kan op grond van dit artikel dus niet van de Belgische Staat een of andere positieve actie eisen op het recht op bescherming van de persoonlijke levenssfeer te waarborgen. Daarvoor is de formulering van art. 8 te vaag³⁷.

³⁴ Cass. 19 november 1981, J.T., 1982, p. 619, met noot J. Dassel.

³⁵ Corr. Luik, 19 oktober 1978, Ann. Conv., vol. XXIII, p. 513, geciteerd door R. Ergec, o.c., p. 496, nr. 763.

³⁶ R. Delarue, "Bescherming van de privacy in de onderneming en de begrenzing van de patronale prerogatieven", noot bij Arbrb. Brussel (2de kamer), 26 maart 1990, Sociaalrechtelijke Kronieken, 1992, 133-141.

³⁷ J. Velu, Les effets directs des instruments internationaux en matière des droits de l'homme, Brussel, 1981, p. 152 e.v.; P. Lambert, La Convention européenne des droits de l'homme dans la jurisprudence belge, Brussel, 1987, p. 74 e.v.

2.3. VERDRAG NR. 108 VAN DE RAAD VAN EUROPA

België heeft bij wet van 17 juni 1991³⁸ het Verdrag nr. 108 van 28 januari 1981 geratificeerd, die m.b.t. de bescherming van personen bij de automatische verwerking van persoonsgegevens werd gesloten in de schoot van de Raad van Europa. Dit verdrag is in werking getreden op 1 oktober 1985 en werd tot dusver door een zestiental lidstaten van de Raad van Europa bekrachtigd. België had dit verdrag reeds op 7 mei 1982 ondertekend, maar één van de voorwaarden om tot ratificatie te kunnen overgaan, was het uitvaardigen van een nationale wetgeving over de privacybescherming bij de verwerking van persoonsgegevens. Zolang België niet over een dergelijke wetgeving beschikte, kon het verdrag niet geratificeerd worden. Hoewel de ratificatiewet reeds medio 1991 door het Parlement goedgekeurd, werd ze slechts in het einde 1993 in het Belgisch Staatsblad gepubliceerd, nadat de Wet Verwerking Persoonsgegevens van 8 december 1992 (zie lager) (gedeeltelijk) in werking was getreden.

Het doel van het verdrag bestaat erin bij de geautomatiseerde verwerking van persoonsgegevens het respect te verzekeren voor de rechten en de fundamentele vrijheden, inzonderheid het recht op privé-leven, van elk natuurlijk persoon, ongeacht zijn nationaliteit of woonplaats, en op het grondgebied van elke lidstaat. Belangrijk hierbij is de vaststelling uit het verklarend verslag dat bij gebrek aan internationale regeling op dit vlak het principe van het vrij verkeer van informatie over de grenzen heen in het gedrang dreigt te komen tengevolge van beperkende nationale regelen inzake export van gegevens.

Het verdrag wil zijn doel bereiken door aan de lidstaten een drievoudige verplichting op te leggen. In de eerste plaats moet in het nationale recht een aantal basisprincipes worden opgenomen zodat bij gegevensverwerking een minimaal respect voor het recht op privé-leven wordt gewaarborgd van elk individu dat zich op het grondgebied bevindt. Op termijn moet dit leiden tot een zekere harmonisatie van de reglementering op dit domein en tot een vermindering van de wetsconflicten. In de mate dat deze basisbescherming wordt gegarandeerd, wordt aan de lidstaten daarnaast het principiële verbod opgelegd om het onderling verkeer van persoonsgegevens te verhinderen of aan enige vorm van voorafgaande machtiging te onderwerpen. Tenslotte wordt een samenwerkingskader uitgewerkt tussen de lidstaten voor de toepassing van het verdrag en de wederzijdse informatieverstrekking. Een Raadgevend Comité wordt belast met de toepassing en de nadere uitwerking van het verdrag.

Na de uitwerking van het verdrag nr. 108 inzake de bescherming van personen ten aanzien van de geautomatiseerde verwerking van persoonsgegevens werd door de Raad van Europa onderzocht hoe de algemene principes van het verdrag concreet kunnen worden toegepast op de onderscheiden maatschappelijke activiteiten en sectoren, rekening houdend met hun specifieke

³⁸ Wet van 17 juni 1991 houdende goedkeuring van het Verdrag tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens, opgemaakt te Straatsburg op 28 januari 1981, B.S., 30 december 1993.

kenmerken en behoeften. Dit gaf inmiddels aanleiding tot een aantal aanbevelingen uitgaande van de Raad van Ministers van de Raad van Europa in uitvoering van het verdrag, onder meer met betrekking tot de bescherming van persoonsgegevens in het kader van de medische sector, de statistiek en het wetenschappelijk onderzoek, de sociale zekerheid, de direct marketing, de politiesector en de arbeidsvoorziening.

In de artikelen 5 tot 9 van het verdrag over de bescherming van personen bij de geautomatiseerde verwerking van persoonsgegevens worden een aantal zeer algemene principes geformuleerd die bij een dergelijke verwerking in acht genomen moeten worden.

Art. 5 handelt over de kwaliteit van de gegevens: er wordt bepaald dat persoonsgegevens rechtmatig verzameld moeten worden, dat ze enkel mogen opgeslagen worden voor specifieke en gerechtvaardigde doeleinden en niet gebruikt mogen worden voor andere doeleinden, dat de gegevens relevant en adequaat moeten zijn, dat er niet meer gegevens mogen worden opgeslagen dan nodig voor het beoogde doel, dat de gegevens accuraat moeten zijn en blijven, en dat ze, in geïndividualiseerde vorm, niet langer mogen bewaard worden dan nodig voor het doel waarvoor ze werden opgeslagen.

Art. 6 bepaalt dat persoonsgegevens m.b.t. het ras, de politieke opinie, religieuze of andere overtuiging, gezondheid, seksueel gedrag en strafrechtelijke veroordelingen, niet het voorwerp mogen zijn van geautomatiseerde verwerking zonder dat de nationale wet in aangepaste waarborgen heeft voorzien.

Art. 7 zegt dat aangepaste veiligheidsmaatregelen moeten worden genomen voor de bescherming van persoonsgegevens in geautomatiseerde bestanden tegen accidentele of niet-geautoriseerde vernietiging, accidenteel verlies of niet-geautoriseerde toegang, wijziging of verspreiding.

Art. 8 bepaalt dat eenieder moet kunnen beschikken over de volgende vier rechten: de mogelijkheid hebben om het bestaan te achterhalen van een geautomatiseerd bestand met persoonsgegevens, de bedoeling ervan en de identiteit en het adres van de verantwoordelijke; met redelijke tussenpozen en zonder overdreven vertraging of kost bevestiging krijgen of persoonsgegevens over hem of haar in het bestand zijn opgeslagen, met mededeling van die gegevens in een begrijpelijke vorm; eventueel verbetering bekomen van onjuiste gegevens of vernietiging van gegevens die in strijd met de nationale wet over de bescherming van persoonsgegevens zijn opgeslagen; de mogelijkheid hebben om een beroep in te stellen indien op een verzoek tot kennisgeving, mededeling van gegevens, verbetering of vernietiging niet wordt ingegaan.

Art. 9 bepaalt dat uitzonderingen op de hogervermelde principes van art. 5, 6 en 8 enkel toegelaten zijn als daarin bij wet is voorzien en noodzakelijk in een democratische samenleving voor de bescherming van de veiligheid van de Staat, de openbare veiligheid, de monetaire belangen van de Staat of de bestrijding van de criminaliteit; de bescherming van de betrokkene zelf of de rechten en vrijheden van derden.

Tenslotte is in dit kader ook nog art. 12 van belang, omdat het over grensoverschrijdend gegevensverkeer handelt. Het bepaalt dat een Staat, enkel met het oog op de bescherming van de persoonlijke levenssfeer, het grensoverschrijdend verkeer van persoonsgegevens naar het grondgebied van een andere Staat, partij bij het verdrag, niet mag verbieden of onderwerpen aan een speciale toelating. Van dat principe kan enkel worden afgeweken voor bepaalde categorieën van persoonsgegevens waarvoor de nationale wet een speciale behandeling voorschrijft en bij gegevensuitvoer naar landen die geen partij zijn bij het verdrag, via een Staat die wel partij is bij de verdrag.

Sedert de ratificatie werken de bepalingen van het verdrag in principe ook door in ons intern recht. Dat geldt uiteraard maar in zoverre die bepalingen "self-executing" zijn. De meeste artikelen van het verdrag kunnen niet rechtstreeks door individuen worden ingeroepen omdat ze geen concrete, afdwingbare rechten in het leven roepen maar veeleer de Staten verplichten tot het uitvaardigen van maatregelen. Enkel artikel 12 legt een verbod op aan de Lidstaten. Omwille van de voorrang van het internationaal verdragsrecht, zoals erkend in het "smeltkaasarrest" van het Hof van Cassatie, kunnen particulieren zich o.i. op dit verbod beroepen wanneer zij zouden belet worden persoonsgegevens te exporteren naar een andere Lid-Staat die het verdrag heeft geratificeerd.

2.4. O.E.S.O.

In september 1980 werden in het kader van de O.E.S.O. richtlijnen aangenomen betreffende de bescherming van het privé-leven en het grensoverschrijdend verkeer van persoonsgegevens.

De richtlijnen zijn niet verbindend voor de lidstaten. A fortiori kunnen de burgers er geen subjectieve rechten aan ontleen. De aanvaarding ervan kan enkel worden beschouwd als een intentieverklaring om de nationale initiatieven tot reglementering van de bescherming van het privé-leven en de grensoverschrijdende gegevensstromen te baseren en/of af te stemmen op de principes vervat in de richtlijnen.

Het doel van de richtlijnen bestaat erin het vrij verkeer van informatie te verzekeren om de ontwikkeling van internationale betrekkingen op sociaal-economisch vlak te bevorderen. In dit kader worden de lidstaten verzocht in hun interne wetgeving een aantal minimale basisprincipes op te nemen inzake de bescherming van het privé-leven en de individuele vrijheden bij de gegevensverwerking en deze op gelijke wijze toe te passen op alle natuurlijke personen. Daardoor zullen de verschillen tussen de nationale regelingen en administratieve praktijken tot een minimum worden herleid en de redenen voor de instelling van beperkingen ten aanzien van transnationale gegevensexport verdwijnen. Parallel met de aanvaarding van fundamentele beginselen inzake gegevensbescherming wordt de lidstaten gevraagd af te zien van ongerechtvaardigde belemmeringen ten aanzien van het grensoverschrijdend verkeer van persoonsgegevens. Het wordt de lidstaten ten slotte aanbevolen samen te werken bij de uitvoering en de verdere ontwikkeling van de richtlijnen en daartoe de nodige specifieke procedures overeen te

komen.

3. BUITENLANDSE WETGEVING

3.1. DUITSLAND

In Duitsland is de bescherming van persoonsgegevens - "Datenschutz" - zowel geregeld op het niveau van de Bond als op dat van de Länder. Het "Bundesdatenschutzgesetz" dateert al van 27 januari 1977 maar in 1990 werd deze wet grondig herzien. Dat was o.m. nodig omwille van een arrest van het Bundesverfassungsgericht waarin het principe van de "informationelle Selbstbestimmung" werd erkend, m.a.w. het recht van het individu om, binnen bepaalde grenzen zelf te beslissen over het gebruik van gegevens over zichzelf. Dit principe is in de nieuwe wet tot uitdrukking gebracht in de regel dat de verwerking en het gebruik van persoonsgegevens verboden zijn tenzij de wet het toelaat of de betrokkene zijn toestemming heeft gegeven (Datenschutzverbot mit Erlaubnisvorbehalt). De bedoeling van "Datenschutz" reikt dus voor de Duitsers veel verder dan uitsluitend het bestrijden of vermijden van misbruiken bij de verwerking van persoonsgegevens. Het betreft daarentegen de bescherming van een fundamenteel persoonlijkheidsrecht.

Typisch voor Duitsland zijn de "Datenschutzbeauftragte": elke onderneming die persoonsgegevens verwerkt en minstens vijf werknemers tewerkstelt, moet een verantwoordelijke voor de privacybescherming in de onderneming aanduiden. De betrokkene heeft het statuut van een "beschermde werknemer". Daarnaast functioneren voor de publieke sector de Datenschutzbeauftragte van de Länder en de "Bundesdatenschutzbeauftragte". Deze instanties moeten toezien op de naleving van de regels en hebben daarvoor onbeperkte toegang tot alle bestanden met persoonsgegevens.

De nieuwe Duitse wetgeving breidt de toepassing van haar regels in de publieke sector nu ook uit tot persoonsgegevens in "akten", en dus niet alleen meer in "bestanden". Nieuw is ook het principe van "schadevergoeding zonder fout" voor de publieke sector en de omkering van de bewijslast ten gunste van het individu bij verwerkingen in de private sector.

Elke overheidsinstantie die, door niet-toegelaten of onjuist gebruik van persoonsgegevens, aan de betrokkene schade berokkent, moet deze schade vergoeden, ook al is er geen fout gebeurd.

Aanmeldingen van verwerkingen voor ondernemingen in de private sector gebeuren aan de Datenschutzbeauftragte, naargelang het geval op federaal niveau of op het niveau van de Länder. Deze aangifteplicht is echter beperkt tot ondernemingen "die Datenverarbeitung im Auftrag als Dienstleistung oder zur geschäftsmässigen Übermittlung betreiben". Enkel ondernemingen die persoonsgegevens verwerken in opdracht als dienstverlening of voor professionele verspreiding (bijv. "listbrokers") moeten hun verwerkingen derhalve aanmelden.

3.2 FRANKRIJK

Hierboven hebben we gezien dat de Duitsers bij hun regeling m.b.t. de bescherming van persoonsgegevens vooral uitgaan van het grondwettelijk recht van elk individu om zelf over zijn eigen persoonsgegevens te beschikken ("informationelle Selbstbestimmung"). Daarentegen hebben de Fransen, in hun wet "Informatique, fichiers et libertes" van 6 januari 1978, veeleer aandacht voor de risico's van onjuiste beslissingen over individuen, wanneer die beslissingen gesteund worden op foutieve, onvolledige of verouderde gegevens. Centraal staat hier dus veel meer het principe van "due process". Zo wordt o.m. bepaald dat geen enkele administratieve beslissing die een beoordeling over een menselijke gedraging impliceert, uitsluitend gesteund mag zijn op een geautomatiseerde informatieverwerking waarin het profiel en de persoonlijkheid van de betrokkene worden gedefinieerd. Elke persoon heeft ook het recht om de informatie en de redeneringen die gehanteerd worden in geautomatiseerde verwerkingen, en waarvan de resultaten tegen hem worden gebruikt, te kennen en te betwisten.

In de tweede plaats wordt de Franse wetgeving gekenmerkt door de zeer ruime bevoegdheden die aan een centrale controle-autoriteit, de "Commission Nationale de l'Informatique et des Libertés" (de "CNIL"), worden gegeven. Deze commissie heeft in bepaalde gevallen zelfs een reglementerende bevoegdheid. Ook zijn er opvallend veel garanties ingebouwd om de onafhankelijkheid van de commissie te bewaren, o.m. ten aanzien van de regering. Tenslotte heeft de commissie ook een zeer krachtige onderzoeksbevoegdheid gekregen.

In de derde plaats wordt in Frankrijk, net zoals in Duitsland, een onderscheid gemaakt tussen de regeling voor de publieke sector en die voor de particuliere sector. In de publieke sector zijn persoonsregistraties enkel mogelijk mits een wet of een reglement en na gemotiveerd advies van de CNIL. In de particuliere sector moeten alle geautomatiseerde persoonsregistraties het voorwerp uitmaken van een voorafgaande aangifte bij de CNIL.

Uiteraard is de aangifte van al die verwerkingen bij een centrale controle-autoriteit uitgesloten. In Frankrijk heeft men dit probleem pogen op te lossen door de praktijk van de "normes simplifiées". De wet geeft namelijk aan de CNIL de bevoegdheid om voor de meest courante categorieën van verwerkingen, die kennelijk geen gevaar opleveren voor de persoonlijke levenssfeer, vereenvoudigde normen uit te vaardigen. In deze "normen" worden voor alle courante categorieën van verwerkingen een aantal zeer algemene regels vastgesteld m.b.t. de finaliteit, het gebruik, de toegang, de beveiliging, de bewaartermijn, enz... Om te mogen starten met een geautomatiseerde verwerking volstaat dan een verklaring waarin de houder bevestigt dat hij de vereenvoudigde normen zal respecteren. Voor meer dan 30 categorieën van verwerkingen heeft de CNIL dergelijke normen opgesteld, o.m. voor klantenadministratie, personeelsbeheer, leveranciersadministratie, verzekeringen, postorderverkoop, abonnementenbeheer, beheer van onroerende goederen, ledenadministratie, leerlingen- en studentenadministratie, enz... In al deze gevallen moet het gewone aanmeldingsformulier niet meer ingevuld worden en is in de publieke sector geen wet, decreet of besluit meer nodig. Vooral voor de publieke sector, maar ook in de private sector, is deze weg van uitzondering tot regel geworden. In meer dan 80 % van de

aanmeldingen bij de CNIL wordt de vereenvoudigde weg gevolgd. Jaarlijks ontvangt de CNIL ongeveer 4000 gewone meldingen. In het publiek register staan er momenteel iets meer dan 30.000. Het aantal vereenvoudigde meldingen wisselt sterk van jaar tot jaar (bv. 24.184 in 1989; slechts 10.180 in 1990). De reden daarvoor is onduidelijk maar heeft wellicht veel te maken met de informatiecampagnes die de CNIL onderneemt.

3.3. VERENIGD KONINKRIJK

De Britse "Data Protection Act" werd door de Koningin op 12 juli 1984 ondertekend. Ze regelt "the use of automatically-processed information relating to individuals and the provision of services in respect of such information" De wet roept een "Data Protection Registrar" en een "Data Protection Tribunal" in het leven.

Bij de Registrar moeten alle houders van persoonsgegevens zich laten "registreren". Niet-geregistreerden mogen in principe geen geautomatiseerde verwerkingen van persoonsgegevens verrichten. Er zijn uiteraard tal van uitzonderingen o.m. voor "home users". Bij de registratie kan de Registrar aan de houders van persoonsgegevens ("data users") richtlijnen ("notices") opleggen. Tegen beslissingen van de Registrar is beroep mogelijk bij het "Data Protection Tribunal".

In Groot-Brittannië bedraagt het aantal registraties ongeveer 16.000 per jaar. In 1992 waren in het publiek register ongeveer 175.000 registraties opgenomen. Met de registraties werd gestart in november 1985. Belangrijk is dat in Groot-Brittannië een registratie slechts drie jaar geldig is. Daarna moet men de registratie hernieuwen. Op dit moment zijn meer dan dertig procent van de verlopen registraties niet hernieuwd. Uit een enquête is gebleken dat ongeveer de helft daarvan nochtans daartoe verplicht was. Dergelijke enquêtes worden ook ondernomen om na te gaan hoe goed de registratieplicht wordt nageleefd. Uit de enquête van 1987 bijvoorbeeld blijkt dat de registratieplicht het best is toegepast door de lokale besturen en de direct marketing sector. Accountants en garagehouders (65 % overtredingen), advocaten en makelaars in onroerende goederen (75 % overtredingen), en selectiebureaus en huwelijksbemiddelaars (87 % overtredingen) kwamen het slechtst uit de bus. Uit dezelfde enquête van 1987 bleek ook dat 66 % van de bevroegden nog nooit van de privacywet (van '84) had gehoord. Maar dank zij de intensieve informatiecampagnes had de Registrar in 1991 al bereikt dat bij de grote bedrijven en instellingen (> 50 werknemers), die geautomatiseerde verwerkingen van persoonsgegevens verrichtten, 95% op de hoogte was van het bestaan van de "Data Protection Act" (87 % bij de bedrijven met < 50 werknemers). Daarentegen waren bij de grote bedrijven nog altijd maar 82 % op de hoogte van de verplichting tot registratie. Bij de kleine en middelgrote bedrijven (< 50 werknemers) was dat zelfs maar 62 % (cijfers van 1991).

Bij registratie moet men ook in Groot-Brittannië opgeven welke finaliteit men met de verwerking nastreeft. De meest aangeduide finaliteit is "personeelsadministratie", gevolgd door "klantenadministratie", "leveranciersadministratie", "marketing en verkoop", "pensioenen", "accounting", "planning en management", "ledenadministratie", "public relations",

"kredietadministratie", "verzekeringen", "financiële diensten", "patiëntenadministratie", "leerlingenadministratie", "fund raising", enz.... Om de registratie te vergemakkelijken heeft de Britse Registrar een "purpose code" opgesteld met 70 mogelijke finaliteiten. Bij de aangifte hoeft men dan maar enkel een of meer van de voorgestelde finaliteiten aan te kruisen.

3.4. LUXEMBURG

De Luxemburgse wet over "nominatieve gegevens in informaticaverwerkingen" van 31 maart 1979 is vooral bekend omdat ze ook van toepassing is op rechtspersonen, en niet alleen op natuurlijke personen, zoals in de meeste andere landen. De Luxemburgers vinden dat zeer vaak gegevens over - vooral kleine - vennootschappen gemakkelijk terug te voeren zijn tot identificeerbare natuurlijke personen.

Voor persoonsregistraties in de private sector is in Luxemburg de voorafgaandelijke toestemming van de Minister nodig. Deze laatste vraagt daarvoor een advies aan de controlecommissie. Voor de creatie en de exploitatie van een persoonsregistratie in de publieke sector is een wet of een groothertogelijk besluit nodig. Elk ontwerp van wet of besluit in dat verband moet voorgelegd worden aan de controlecommissie.

Zowel in de publieke als in de private sector geldt een toelating voor een persoonsregistratie ten hoogste gedurende tien jaar.

Er is een nationaal repertorium waarin de gegevens over alle persoonsregistraties zijn opgenomen. De regering kan voor registraties m.b.t. de veiligheid van de Staat en de openbare veiligheid een uitzondering op de verplichte inschrijving in het repertorium toestaan. Iedereen heeft gratis toegang tot het repertorium en, mits betaling van een vergoeding, kan men ook een copie krijgen van de gegevens over een bepaalde registratie.

Als bij iemand persoonsgegevens worden verzameld met het oog op een geautomatiseerde verwerking, moet de betrokkene geïnformeerd worden over de bedoeling en de bestemming van de registratie, over het al dan niet verplicht karakter van de antwoorden, over de bestemming van de gegevens en over het recht van toegang en verbetering. Die informatie moet echter niet gegeven worden bij de vervolging van misdrijven.

Verder kan de betrokkene zich richten tot de verantwoordelijke van de registratie om toegang te krijgen tot zijn eigen gegevens. Interessant is dat het recht tot verbetering van die gegevens ook een recht tot verduidelijking en tot aanvulling inhoudt. Het meest opvallende in de Luxemburgse wet is echter dat de controle op de toepassing gebeurt door de Minister die het nationaal repertorium onder zijn bevoegdheid heeft. Klachten van individuele personen worden aan de Minister gericht en het is ook de Minister die eventueel een onderzoek beveelt. De "commission consultative" heeft dus enkel een advizerende bevoegdheid.

3.5 NEDERLAND

In Nederland werd eind 1988 de wet "houdende regels ter bescherming van de persoonlijke levenssfeer in verband met persoonsregistraties" (afgekort: de wet persoonsregistraties) uitgevaardigd. Het centrale begrip van de Nederlandse wet is dat van de "persoonsregistratie", gedefinieerd als "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" (aldus art. 1). De wet is niet van toepassing op persoonsregistraties die naar hun aard voor persoonlijk of huiselijk gebruik bestemd zijn en evenmin op persoonsregistraties die uitsluitend ten dienste staan van de openbare informatievoorziening door pers, radio of televisie. Verder is de wet ook niet van toepassing op boeken en andere schriftelijke publikaties, alsmede catalogisering en daarvan. Daarbij horen o.m. telefoonboeken en almanakken. Een "Who is who?" in boekvorm valt buiten het domein van de wet, een dergelijke publicatie op optische schijf daarentegen wel. In de publieke sector is de wet niet van toepassing op openbare registers die door de wet zijn ingesteld (bijv. de registers van de burgerlijke stand), op de persoonsregistraties van de inlichtingen- en veiligheidsdiensten en op deze van de politie. Over de beide laatste registraties bestaan echter afzonderlijke wetgevingen, nl. de wet op de inlichtingen- en veiligheidsdiensten en de wet op de politieregisters (wet van 21 juni 1990, Stb. 1990, 414)

De kernbepaling van de Nederlandse wet persoonsregistraties is artikel 4. Daarin staat dat een persoonsregistratie slechts mag worden aangelegd voor een bepaald doel "waartoe het belang van de houder redelijkerwijze aanleiding geeft". Een persoonsregistratie mag slechts persoonsgegevens bevatten die rechtmatig zijn verkregen en in overeenstemming zijn met het doel waarvoor de registratie is aangelegd (art. 5). De opgenomen persoonsgegevens mogen slechts gebruikt worden voor doeleinden die met het doel van de persoonsregistraties verenigbaar zijn (art. 6). De verwerking van gevoelige gegevens (godsdienst, levensovertuiging, ras, politieke gezindheid, seksualiteit, intiem levensgedrag, alsmede gegevens van medische, psychologische, strafrechtelijke of tuchtrechtelijke aard) worden niet geregeld in de wet zelf maar in een specifieke algemene maatregel van bestuur. Daarin wordt de verwerking van gevoelige gegevens o.m. toegelaten met schriftelijke toestemming van de betrokkene of indien de verwerking "noodzakelijk is met het oog op de gewichtige belangen van de houder en de persoonlijke levenssfeer van de betrokkene daardoor niet onevenredig wordt geschaad". Deze afweging tussen de belangen van de houder en de persoonlijke levenssfeer van de betrokkene is kenmerkend voor de Nederlandse wet.

De houders moeten elke betrokkene over wie voor de eerste keer persoonsgegevens in een registratie worden opgenomen, daarvan binnen de maand schriftelijk op de hoogte stellen. Dat is niet nodig o.m. indien de betrokkene redelijkerwijs kan weten dat een dergelijke opname heeft plaatsgevonden, of indien een gewichtig belang van de betrokkene zich tegen het doen van een schriftelijke mededeling verzet (art. 28).

De Nederlandse wetgever legt sterk de nadruk op "zelfregulering" bij het aanleggen van

persoonsregistraties. Elke organisatie, die een gedragscode heeft vastgesteld, kan aan de Registratiekamer vragen om deze code in overeenstemming met de wet te verklaren. De organisatie moet representatief zijn voor de betrokken sector. Er moet gelegenheid geweest zijn tot bezwaren en opmerkingen. De verklaring van de Registratiekamer geldt maar voor vijf jaar en is niet bindend voor hoven en rechtbanken. Oorspronkelijk was het de bedoeling om via het systeem van de gedragscodes meer soepelheid in te bouwen in de wet. In de praktijk is het uitwerken en onderhandelen van een gedragscode in de meeste sectoren een langdurige en bureaucratische procedure geworden. Momenteel bestaan er o.m. gedragscodes voor de banksector en voor de direct marketing sector.

In de publieke sector moet voor elke verwerking van persoonsgegevens een "reglement" opgesteld worden, dat meegedeeld moet worden aan de nationale controle-instantie, in Nederland "Registratiekamer" genoemd. Voor gegevensverwerkingen in de private sector is in een "aanmelding" voorzien. In het "Besluit genormeerde vrijstelling" worden een hele reeks registraties van de verplichting tot aanmelding vrijgesteld, o.m. voor administraties van leden of begunstigers, abonnementsadministraties, personeelsadministraties, salarisadministraties, administraties betreffende aanspraken op uitkeringen, boekhoudingen, administraties van afnemers en leveranciers, administraties van leerlingen en studenten. Ook registraties met uitsluitend voor communicatie benodigde gegevens (naam, voornamen, titulatuur, functie, geslacht, adres, telefoonnummer, e.a.) hoeven niet te worden aangemeld.

3.6 PORTUGAL

De Portugese wet van 29 april 1991 is zeer sterk geïnspireerd door de Franse wet "Informatique et Libertés" van 1978. Ze is niet van toepassing op de verwerking van persoonsgegevens voor persoonlijk of huiselijk gebruik, de verwerking van loonadministratie en andere administratieve verwerkingen in het kader van een arbeidsverhouding, de facturatie van goederen en diensten en de inzameling van lidgelden door organisaties. Ook de verwerking van persoonsgegevens door de Portugese Inlichtingendienst valt buiten de wet (art. 3, 3°).

De Portugese controle-autoriteit op het vlak van de databescherming is de "Nationale Commissie voor de Bescherming van Geautomatiseerde Persoonsgegevens" (CNPDPI). Ze bestaat uit zeven leden, waarvan drie gekozen worden door het Parlement, twee door de Magistratuur en twee door de Regering. De CNPDPI heeft, naar het voorbeeld van de Franse CNIL, zeer ruime bevoegdheden, ook op reglementerend vlak. Voor de verwerking van "gevoelige" gegevens, ook door overheidsinstellingen zoals de politie, is de voorafgaande toestemming van de CNPDPI nodig (art. 11, 3°).

Zoals de Franse, bepaalt ook de Portugese wet dat geen gerechtelijke, administratieve of disciplinaire beslissing m.b.t. iemands' gedrag mag genomen worden, als die beslissing uitsluitend gebaseerd is op het resultaat van een geautomatiseerde gegevensverwerking waarin het profiel of de persoonlijkheid van de betrokkene wordt weergegeven (art. 16).

Het belangrijkste kenmerk van de Portugese wet is het gebrek aan duidelijkheid en de vaak tegenstrijdige bepalingen. Met de uitvoering van de wet is nog steeds niet begonnen en de CNPDPI is nog niet officieel geïnstalleerd.

3.7. SPANJE

In Spanje is op 26 oktober 1992 de wet (Ley organica) "del tratamiento automatizado de los datos de caracter personal" afgekondigd (afgekort "LORTAD"). In de Spaanse Grondwet van 1978 werd al het principe van de databescherming overeenkomstig de beginselen van het Verdrag van de Raad van Europa opgenomen. Spanje heeft dat Verdrag trouwens reeds geratificeerd, hoewel het (nog) niet aan de ratificatievoorwaarden voldoet.

De wet maakt een onderscheid tussen de private en de publieke sector. De publieke sector moet reglementen publiceren in het officieel mededelingenblad, de private sector moet de geautomatiseerde verwerkingen van persoonsgegevens melden bij een centrale controle-autoriteit.

De Spaanse wet is sterk op de Franse wet geïnspireerd maar geeft een ruimere plaats aan de toestemming van de betrokkene. Dat is het centrale criterium voor het geoorloofd karakter van een persoonsregistratie. Verder vallen in de Spaanse wet ook de afzonderlijke bepalingen op voor o.m. direct marketing, telecommunicatie, kredietregistratie en opiniepeilingen. Er is ook in sectoriële gedragscodes voorzien.

3.8. DENEMARKEN

In Denemarken wordt de verwerking van persoonsgegevens in de publieke sector en in de private sector in afzonderlijke wetten geregeld. De wet voor de private sector is op 1 januari 1979 in werking getreden en op 1 april 1988 gewijzigd.

Kenmerkend voor de Deense wet is dat ze zowel op natuurlijke personen als op rechtspersonen slaat. Financiële of andere gegevens over bedrijven die door een ander bedrijf worden bijgehouden vallen dus onder het toepassingsgebied van de wet. Uitzonderingen gelden o.m. voor registraties van de pers of van het wetenschappelijk onderzoek maar die registraties moeten worden aangemeld en er mogen geen gevoelige gegevens in worden opgenomen. De Deense wet kent verder afzonderlijke bepalingen voor kredietregistratie, direct mailing en computerservicebureau's.

Registratie van persoonsgegevens door bedrijven zijn in principe toegelaten als zij een natuurlijk onderdeel vormen van de in de branche van het desbetreffende bedrijf gebruikelijke activiteiten. Gegevens ouder dan vijf jaar mogen in principe niet zonder toestemming van de betrokkene aan derden worden verstrekt, tenzij er een duidelijk dwingend belang aanwezig is of de verstrekking door de wet is opgelegd.

Koppelingen van registraties van verschillende bedrijven zijn in principe verboden tenzij voor het up-to-date houden van elkaars bestanden of wanneer er een toestemming verkregen wordt

van de privacycommissie.

Typisch voor de Denen is ook dat ze de registratie van een uniek persoonsnummer (zoals ons Rijksregisternummer) aan dezelfde regels onderwerpen als de registratie van gevoelige gegevens.

Verder kent Denemarken geen algemene aanmeldingsplicht voor registraties in de particuliere sector. Enkel bepaalde registraties moeten aangemeld worden, zoals kredietregistraties, registraties met gevoelige gegevens of registraties van computerservicebureaus.

Wat men onder "gevoelige gegevens" verstaat, wordt niet limitatief in de wet opgesomd. Bij de voorbeelden vermeldt de Deense wet ook gegevens over huidskleur, over sociale problemen of over het gebruik van verdovende middelen. Bedrijven die adressen verkopen of die mailings verzorgen voor derden, mogen enkel naam-, adres- en functiegegevens en vrij verkrijgbare gegevens uit het centrale handelsregister opnemen.

In bedrijven is het registreren van de vanuit het bedrijf opgebelde telefoonnummers in principe verboden.

De Deense controle-autoriteit, de "Registertilsyn", heeft ruime bevoegdheden. Ze kan bijvoorbeeld bedrijven verplichten om verwerkingen stop te zetten of te wijzigen.

4. DE ONTWERPRICHTLIJN VAN DE EUROPESE UNIE

4.1. INLEIDING

De bezorgdheid van de Europese instanties voor de bescherming van de persoonlijke levenssfeer bij de verwerking van persoonsgegevens is geen nieuw gegeven. De grote verschillen tussen de nationale wetgevingen van de Lid-Staten zijn al enige tijd een doorn in het oog van de Europese Commissie, niet in het minst omdat deze verschillen een belemmering kunnen vormen voor het vrij verkeer van persoonsgegevens binnen de Unie. Lange tijd heeft men zich op het vlak van de Europese Gemeenschap beperkt tot Resoluties van het Parlement en Aanbevelingen van de Commissie waarin aan de Lid-Staten werd gevraagd om het verdrag nr. 108 van de Raad van Europa uit te voeren en te ratificeren. De beoogde gevolgen bleven echter uit: niet alle Lid-Staten ratificeerden het dataprotectieverdrag en een aantal onder hen beschikken zelfs thans nog steeds niet over een algemene wetgeving over de bescherming van de persoonlijke levenssfeer bij de verwerking van persoonsgegevens.

Daarom heeft de Europese Commissie besloten om een Europees programma op dit terrein uit te werken in het kader van de verwezenlijking van de Europese eenheidsmarkt in 1993. Op 18 juli 1990 deed de Europese Commissie een Mededeling aan de Raad waarbij zes initiatieven werden aangekondigd. Het belangrijkste van die zes was ongetwijfeld het voorstel voor een richtlijn van de Raad betreffende de bescherming van personen in verband met de behandeling van persoons-

gegevens.

Met haar initiatief poogt de Europese Commissie binnen de Unie te komen tot een gelijkwaardige bescherming, die van een zeer hoog niveau moet zijn en waarbij rekening wordt gehouden met de reeds bestaande wetgeving in de verschillende landen. Omdat deze bestaande nationale wetgeving in de verschillende Lid-Staten zo verschillend is - niet in het minst omdat er tussen de redactie van de oudste wet en die van de recentste wet meer dan vijftien jaar ligt, is dat een zeer hachelijke onderneming. De tekst van de ontwerp-richtlijn is dan ook op zeer veel kritiek onthaald. In het Europees Parlement werden meer dan 150 amendementen ingediend. Een honderdtal werden daarvan uiteindelijk ook aanvaard. De Commissie heeft een groot aantal van deze amendementen verwerkt in een nieuw voorstel dat op 16 oktober 1992 werd ingediend.

4.2. TOEPASSINGSGEBIED

De ontwerp-richtlijn is van toepassing op de geheel of gedeeltelijk geautomatiseerde behandeling van persoonsgegevens en op de niet-geautomatiseerde behandeling van persoonsgegevens die in bestanden zijn opgenomen of bestemd zijn om daarin te worden opgenomen. "Persoonsgegevens" worden gedefinieerd als elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon; als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer of van één of meer specifieke elementen, die voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit kenmerkend zijn. Gegevens die op zodanige wijze in de vorm van statistieken worden samengevoegd, dat de betrokkenen redelijkerwijze niet meer identificeerbaar zijn, worden niet als persoonsgegevens beschouwd.

"Behandeling" wordt gedefinieerd als elke verrichting of elk geheel van verrichtingen met betrekking tot persoonsgegevens, al dan niet uitgevoerd met behulp van geautomatiseerde procédés, zoals het verzamelen, vastleggen, ordenen, bewaren, uitwerken, wijzigen, opvraagbaar maken, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, verwijderen of vernietigen van gegevens.

Een "bestand" is elk gestructureerd geheel van op één plaats samengebrachte of over verschillende plaatsen verspreide persoonsgegevens die volgens bepaalde criteria toegankelijk zijn, met als doel of als gevolg dat het gebruik en het met elkaar in verband brengen van gegevens betreffende de betrokkene(n) worden vergemakkelijkt. Deze definities roepen tal van vragen op. Vooral het begrip "bestand" is onduidelijk. Is een dossierkast met alfabetisch geordende personeelsdossiers, een bestand ?

De ontwerp-richtlijn is niet van toepassing op:

- behandelingen van persoonsgegevens voor activiteiten die buiten de werkingssfeer van het Gemeenschapsrecht vallen, zoals bijvoorbeeld de Staatsveiligheid;
- behandelingen van persoonsgegevens voor activiteiten van uitsluitend privé- en

persoonlijke aard door natuurlijke personen, zoals bijv. de elektronische agenda.

Voor de behandelingen van persoonsgegevens voor journalistieke doeleinden door de organen van de pers en van de audiovisuele media, alsmede door journalisten, moeten de Lid-Staten in afwijkingen op de bepalingen van de richtlijn voorzien, om het recht op bescherming van de persoonlijke levenssfeer te verzoenen met de regels betreffende de vrijheid van meningsuiting.

4.3. VERBOD TOT BEHANDELING VAN PERSOONSGEGEVENS

De kern van de ontwerp-richtlijn bestaat in het principieel verbod om persoonsgegevens te behandelen, tenzij in zes gevallen:

- toestemming van de betrokkene, d.w.z. een uitdrukkelijke wilsuiting waarmee de betrokkene aanvaardt dat hem/haar betreffende persoonsgegevens worden behandeld, mits de betrokkene over inlichtingen beschikt over het doel van de behandeling, omtrent de gegevens of categorieën van gegevens waar het bij de behandeling om gaat, omtrent de personen voor wie de persoonsgegevens zijn bestemd en omtrent de naam en het adres van de voor de behandeling verantwoordelijke en, in voorkomend geval, van zijn vertegenwoordiger; de toestemming moet vrij en specifiek zijn en mag door de betrokkene te allen tijde, zonder terugwerkende kracht worden teruggetrokken;
- indien de behandeling noodzakelijk is voor de uitvoering van een met de betrokkene gesloten overeenkomst of van precontractuele maatregelen waarmee op een verzoek van de betrokkene wordt ingegaan;
- indien de behandeling noodzakelijk is voor de uitvoering van een wettelijke verplichting;
- indien de behandeling noodzakelijk is voor de bescherming van een vitaal belang van de betrokkene; men denkt daarbij aan het geval waarin de betrokkene niet in staat is om zijn toestemming te geven (bv. ziekte);
- indien de behandeling noodzakelijk is voor de vervulling van een opdracht van algemeen belang of van een taak die deel uitmaakt van de uitoefening van het openbaar gezag waarvan de voor de behandeling verantwoordelijke of de derde aan wie de gegevens worden verstrekt, de drager is;
- indien de behandeling noodzakelijk is voor de behartiging van het algemeen belang of van het rechtmatig belang van de voor de behandeling verantwoordelijke of van de derde aan wie de gegevens worden verstrekt, mits het belang van de betrokkene niet doorslaggevend is.

Voor de behandeling van gevoelige (waaronder medische) gegevens gelden strengere voorwaarden. Het betreft gegevens die betrekking hebben op de raciale of de etnische afkomst, de politieke gezindheid, de godsdienstige, levensbeschouwelijke of morele overtuigingen, het aangesloten zijn bij een vakvereniging, alsook de gegevens die de gezondheid of het seksuele gedrag betreffen. Deze gegevens mogen enkel behandeld worden als de betrokkene daarin schriftelijk heeft toegestemd, tenzij in de wetgeving van de Lid-Staat is bepaald dat het principieel verbod om dergelijke gegevens te behandelen, niet door de toestemming van de betrokkene ongedaan gemaakt kan worden. De vermelde "gevoelige" gegevens kunnen wel

worden behandeld door een stichting of een vereniging zonder winstoogmerk, met name een vereniging die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is, binnen het raam van haar wettig doel en op voorwaarde dat de behandeling uitsluitend betrekking heeft op de leden en correspondenten van de stichting of vereniging en dat de gegevens niet zonder de toestemming van de betrokkenen aan derden worden doorgegeven. In elk geval moet de behandeling geschieden in omstandigheden die duidelijk geen inbreuk maken op de persoonlijke levenssfeer en de vrijheden.

De Lid-Staten zullen bovendien nog afwijkingen kunnen toestaan op het principieel verbod tot behandeling van "gevoelige" gegevens om redenen van zwaarwegend algemeen belang op grond van een nationale wettelijke bepaling of op grond van een besluit van de toezichthoudende autoriteit, waarbij de soorten van gegevens die het voorwerp van behandeling mogen zijn, de personen voor wie de gegevens zijn bestemd, de hoedanigheid van de voor de behandeling verantwoordelijke en de passende waarborgen nader worden bepaald. Gegevens betreffende strafrechtelijke veroordelingen mogen slechts door de gerechtelijke autoriteiten en door de rechtstreeks bij de desbetreffende uitspraak betrokken personen of hun vertegenwoordigers worden bewaard. De Lid-Staten kunnen evenwel op grond van een nationale wettelijke bepaling waarin passende waarborgen worden geboden, in afwijkingen voorzien.

4.4. VERPLICHTINGEN BIJ DE BEHANDELING VAN PERSOONSgegevens

Als in één van de hierboven vermelde gevallen kan overgegaan worden tot de rechtmatige behandeling van persoonsgegevens, zal de verantwoordelijke van de behandeling een aantal spelregels moeten naleven.

4.4.1. Fundamentele principes

In de eerste plaats moeten een reeks fundamentele principes in acht genomen worden:

- de behandeling moet "eerlijk" geschieden;
- de gegevens moeten voor welbepaalde, uitdrukkelijk omschreven en wettige doeleinden worden verzameld en gebruikt op een wijze die met die doeleinden verenigbaar is;
- de gegevens moeten toereikend, ter zake dienend en niet overmatig zijn, uitgaande van de doeleinden waarvoor zij worden behandeld;
- de gegevens moeten nauwkeurig zijn en, zo nodig, dienen zij te worden bijgewerkt; alle maatregelen moeten worden getroffen om de gegevens te verwijderen of te corrigeren die voor de doeleinden waarvoor zij zijn verzameld, onnauwkeurig of onvolledig zijn;
- de gegevens mogen, in een vorm die het mogelijk maakt de betrokkenen te identificeren, niet langer worden bewaard dan voor de verwezenlijking van de beoogde doeleinden noodzakelijk is; de Lid-Staten kunnen in passende waarborgen voorzien voor persoonsgegevens die voor historische, statistische en wetenschappelijke doeleinden worden bewaard.
- de verantwoordelijke voor de behandeling moet erover waken dat zonder zijn toestemming nooit persoonsgegevens aan derden worden verstrekt door personen die tot die

gegevens toegang hebben, tenzij ter nakoming van in de nationale of communautaire wetgeving besloten liggende verplichtingen (art. 17, 5°).

4.4.2. Beveiliging

In de tweede plaats moeten de verantwoordelijken hun behandelingen van persoonsgegevens voldoende beveiligen. Art. 17 van de ontwerp-richtlijn zegt dat de voor de behandeling verantwoordelijke de technische en organisatorische maatregelen dient te treffen die voor de beveiliging tegen de volgende risico's "passend en noodzakelijk" zijn:

- vernietiging (per ongeluk of onrechtmatig);
- toevallig verlies;
- vervalsing;
- gegevensverstrekking;
- onbevoegde behandeling.

De vermelde beveiligingsverplichtingen richten zich zowel tot de verantwoordelijke voor de behandeling als tot de verantwoordelijke voor de uitvoering (bijv. het extern rekencentrum). Art. 24 van de ontwerp-richtlijn bepaalt dat de verantwoordelijke voor de behandeling een "m.b.t. de beveiliging voldoende waarborgen biedende behandelende persoon" moet kiezen. Deze laatste mag uitsluitend de behandeling van persoonsgegevens verrichten die in de overeenkomst met de verantwoordelijke is vastgelegd. Hij mag in dit verband ook alleen maar de instructies van de verantwoordelijke opvolgen. Belangrijk is dat de overeenkomst tussen de verantwoordelijke en de behandelende persoon schriftelijk moet zijn. In de overeenkomst moet expliciet bepaald worden dat de persoonsgegevens uitsluitend na toestemming van de verantwoordelijke aan derden zullen worden verstrekt. De te nemen maatregelen moeten een "passend beveiligings-niveau" waarborgen. Of dat niveau is bereikt, zal beoordeeld worden rekening houdende met:

- de stand van de techniek;
- de aard van de te beveiligen gegevens;
- de potentiële risico's.

4.4.3. Aanmelding

In de derde plaats moet de behandeling van persoonsgegevens worden aangemeld bij de toezichthoudende autoriteit (art. 18). Die aanmelding is nodig "elke keer dat wordt overgegaan tot een volledige of gedeeltelijke geautomatiseerde behandeling van gegevens of tot een geheel van behandelingen van dezelfde aard die voor de verwezenlijking van een doeleinde of van verscheidene samenhangende doeleinden zijn bestemd". Dit lijkt ons zeer ongelukkig geformuleerd. Immers, hierboven zagen we dat een "behandeling" in de ontwerp-richtlijn (art. 2 b) is gedefinieerd als "elke verrichting of elk geheel van verrichtingen met betrekking tot persoonsgegevens, zoals het verzamelen, vastleggen, ordenen, bewaren, uitwerken, wijzigen, opvraagbaar maken, raadplegen, gebruiken, verstrekken, samenbrengen, met elkaar in verband brengen, afschermen, verwijderen of vernietigen van gegevens". Het kan toch niet de bedoeling zijn dat dergelijke handelingen telkens moeten worden aangemeld! In de toelichting bij het

ontwerp schrijft de Commissie dat "teneinde een overmatige hoeveelheid aanmeldingen te vermijden, is voorgesteld dat één en dezelfde aanmelding betrekking heeft op het geheel van bewerkingen, meerdere malen uitgevoerd of niet, die bestemd zijn voor de realisatie van een of meerdere onderling verbonden doeleinden (...). Bijvoorbeeld: er is slechts één aanmelding vereist voor het geheel van bewerkingen betreffende het beheer van leningen die door een kredietinstelling verstrekt zijn en die bestemd zijn voor de registratie en het onderzoek van leningen, het toekennen van leningen, het incasseren van de openstaande schuldvorderingen en het bijhouden van geschillendossiers" (zie toelichting blz. 30).

In de aanmelding moeten minimaal de volgende inlichtingen worden opgenomen:

- naam en adres van de verantwoordelijke;
- doel van de behandeling;
- categorieën van opgenomen personen;
- beschrijving van de gegevens of categorieën van gegevens;
- derden aan wie de gegevens kunnen verstrekt worden;
- t.a.v. derde landen voorgenomen overdrachten;
- beschrijving van de beveiligingsmaatregelen.

Veranderingen in deze informatie moeten eveneens bij de toezichthoudende autoriteit worden aangegeven.

Voor behandelingen die t.a.v. de rechten en vrijheden van personen bijzondere risico's meebrengen, moet de toezichthoudende autoriteit een onderzoek instellen vooraleer met de behandeling kan begonnen worden. Voor dat onderzoek beschikt de autoriteit over een termijn van 15 dagen. Na afloop van die termijn maakt zij haar bevindingen bekend. Als voorbeeld van "risicovolle" behandelingen vermeldt de Commissie in de toelichting "zwarte lijsten" of behandelingen die bestemd zijn om derden te informeren over de solvabiliteit van natuurlijke personen (toelichting blz. 32).

Er is een vereenvoudigde aanmelding of vrijstelling mogelijk voor bepaalde categorieën van behandelingen die aan de rechten en vrijheden van de betrokkenen geen afbreuk doen. Volgens art. 19 omvatten deze categorieën van behandelingen o.m. de overlegging van brieven of documenten, de vervulling van wettelijke, boekhoudkundige, fiscale of sociale verplichtingen of de raadpleging van voor het publiek toegankelijke documentaire diensten. In de toelichting zegt de Commissie: "Het is bij voorbeeld denkbaar dat deze maatregelen eveneens betrekking hebben op behandelingen waarmee de betalingen aan het personeel van een overheidsinstantie of een onderneming verricht worden, bepaalde behandelingen die bedoeld zijn voor wetenschappelijk onderzoek of bepaalde behandelingen waarmee medische dossiers worden bijgehouden van de patiënten van personen die werkzaam zijn in de gezondheidssector" (toelichting blz. 33).

Voor verenigingen en stichtingen geldt m.b.t. de gegevens over eigen leden en correspondenten een automatische vrijstelling van aanmeldingsplicht (art. 8, c, 2° lid). De toezichthoudende autoriteit moet van de aangemelde behandelingen een publiek register bijhouden, dat voor iedere

burger toegankelijk moet zijn.

4.5. RECHTEN VAN DE BETROKKENEN

In de ontwerp-richtlijn worden aan de datasubjecten, d.w.z. de personen wier gegevens het voorwerp van de behandeling zijn (de ontwerp-richtlijn noemt ze "de betrokkenen") niet minder dan elf individuele rechten toegekend.

4.5.1. Informatie over het bestaan van een behandeling

Op zijn of haar verzoek moet de betrokkene in kennis worden gesteld van een behandeling, van de doeleinden daarvan, van de categorieën van de gegevens waarop de behandeling betrekking heeft, van de derden of categorieën van derden aan wie de gegevens worden verstrekt en van de naam en het adres van de voor de behandeling verantwoordelijke (of van zijn vertegenwoordiger) (art. 10). Van deze verplichting kan worden afgeweken door het recht van de Lid-Staten als dat noodzakelijk is voor:

- de veiligheid van de Staat;
- landsverdediging;
- strafvervolgingen;
- de openbare veiligheid;
- een dwingend en naar behoren gestaafd economisch of financieel belang van de Lid-Staat of van de Europese Unie (bijv. deviezencontrole, fiscale controle, e.a.);
- een controle- of inspectietaak die deel uitmaakt van de uitoefening van het openbaar gezag of de medewerking daaraan;
- een gelijkwaardig recht van een andere persoon of de rechten en vrijheden van anderen (zakengeheimen van derden, medische en juridische beroepen, mensenrechtenorganisaties die hun bronnen niet kunnen bekend maken zonder gevaar voor deze laatsten).

4.5.2. Informatie bij de verzameling

De voor de behandeling verantwoordelijke dient er zich van te vergewissen dat de betrokkene bij wie gegevens worden verzameld, worden ingelicht over:

- de doeleinden van de behandeling;
- het feit of men al dan niet verplicht is om op de gestelde vragen te antwoorden;
- de gevolgen waaraan men zich bij niet-beantwoording blootstelt; de persoon of categorieën van personen voor wie de gegevens zijn bestemd;
- het bestaan van het recht op toegang tot de gegevens en op de verbetering ervan;
- de naam en het adres van de voor de behandeling verantwoordelijke (of van zijn vertegenwoordiger). Deze inlichtingen moeten aan de betrokkene niet worden verstrekt indien dat een tot de uitoefening van het openbaar gezag behorende controle- of inspectietaak of de medewerking aan een dergelijke taak, of de handhaving van de openbare orde zou beletten.

4.5.3. Informatie bij verstrekking van gegevens aan derden

Behalve in de gevallen waarin de betrokkene voor de behandeling van zijn persoonsgegevens zijn toestemming heeft gegeven of waarin de behandeling noodzakelijk is voor de bescherming van een vitaal belang van de betrokkene, moet deze laatste op het geschikte ogenblik en uiterlijk bij de eerste verstrekking van gegevens aan een derde, verwittigd worden en volgende inlichtingen krijgen:

- naam en adres van de voor de behandeling verantwoordelijke;
- doeleinden van de behandeling;
- categorieën van gegevens waarop de behandeling betrekking heeft; persoon of categorieën van personen voor wie de gegevens bestemd zijn;
- bestaan van een recht van toegang tot de gegevens, van rechtzetting en van verzet (zie hierna). Op deze verplichting tot informatie zijn de volgende uitzonderingen aangebracht:
- de betrokkene is van de verstrekking of de mogelijkheid daartoe vooraf reeds op de hoogte gebracht;
- de verstrekking aan een derde is bij wet voorgeschreven en daarin is in een afwijking van de verplichting tot inlichting van de betrokkene voorzien;
- de verstrekking is noodzakelijk voor de veiligheid van de Staat, de landsverdediging, strafvervolgingen, de openbare veiligheid, een dwingend en naar behoren gestaafd economisch of financieel belang van een Lid-Staat of van de Unie, een controle- of inspectietaak die deel uitmaakt van de uitoefening van het openbaar gezag of om een gelijkwaardig recht van een andere persoon of de rechten en vrijheden van derden te vrijwaren. Indien inlichting van de betrokkene onmogelijk blijkt, onevenredige inspanningen vergt of indien zwaarder wegende rechtmatige belangen van de voor de behandeling verantwoordelijke of een soortgelijk belang van een derde zich daartegen verzetten, kan het nationaal recht van een Lid-Staat bepalen dat de toezichthoudende autoriteit een afwijking mag toestaan. In dat geval moet in passende waarborgen worden voorzien (art. 10, 3°).

4.5.4. Recht op toegang

De betrokkenen moeten het recht hebben om, op verzoek, met redelijke tussenpozen en zonder grote vertraging of overdreven kosten, bevestiging te krijgen van het al dan niet bestaan van hen betreffende persoonsgegevens. Zij moeten die gegevens in begrijpelijke vorm meegedeeld krijgen en over de oorsprong en het gebruik van die gegevens worden ingelicht. De uitzonderingen op het recht op toegang zijn dezelfde als deze die hierboven m.b.t. het recht op informatie op het bestaan van een behandeling werden vermeld (nationale veiligheid, e.a.). In het recht van de Lid-Staten kan worden bepaald dat het recht op toegang tot medische gegevens slechts door bemiddeling van een arts mag worden uitgeoefend. Interessant is dat de ontwerp-richtlijn ook bepaalt dat een betrokkene niet kan worden verplicht om zijn recht op toegang uit te oefenen. Er is daarbij gedacht aan het geval waarbij een derde een betrokkene zou dwingen zijn recht op toegang uit te oefenen en vervolgens de aldus verkregen gegevens mee te delen aan die derde of aan iemand anders.

4.5.5. Recht op rechtzetting

Naargelang het geval moeten de betrokkenen kunnen verkrijgen dat onnauwkeurige of onvolledige gegevens worden rechtgezet, verwijderd of afgeschermd, indien de behandeling niet in overeenstemming met de bepalingen van de richtlijn is. Indien de gegevens aan derden zijn verstrekt, moeten de betrokkenen verkrijgen dat deze derden van de rechtzetting, de verwijdering of de afscherming van de gegevens in kennis worden gesteld.

4.5.6. Recht op informatie over behandelingen die aan de betrokkene worden tegengeworpen

Volgens art. 13, 5° van de ontwerp-richtlijn heeft de betrokkene het recht om, op verzoek, in kennis te worden gesteld van de redeneringen die zijn gevolgd bij de geautomatiseerde behandelingen van gegevens, waarvan de resultaten hem/haar worden tegengeworpen.

4.5.7. Recht om zich om gewettigde redenen te verzetten tegen behandeling

Op grond van art. 15 heeft de betrokkene het recht zich om gewettigde redenen ertegen te verzetten dat gegevens die hem betreffen het voorwerp van een behandeling vormen. De bedoelde gewettigde redenen kunnen bijvoorbeeld liggen in het ontbreken van een wettige rechtvaardiging voor de behandeling, met name indien niet aan de voorwaarden van de richtlijn is voldaan. Daarentegen kan een betrokkene zich niet verzetten tegen een rechtmatige behandeling die noodzakelijk is de uitvoering van een overeenkomst tussen hem en de voor de behandeling verantwoordelijke. In geval van gerechtvaardigd verzet moet de verantwoordelijke de behandeling beëindigen.

4.5.8. Informatie over het recht op kosteloze verwijdering

Art 15, 3° bepaalt dat de voor de behandeling verantwoordelijke zich ervan moet vergewissen dat de mogelijkheid om de gegevens kosteloos te laten verwijderen, uitdrukkelijk aan de betrokkenen ter kennis is gebracht. Opgelet: deze mededeling is enkel nodig vooraleer de gegevens aan derden worden verstrekt of voor rekening van derden voor over de post lopend marktonderzoek worden gebruikt. Het kan hierbij gaan om een commercieel marktonderzoek of om een marktonderzoek uitgevoerd voor of door een caritatieve instelling of een politieke partij. De verantwoordelijke kan zijn verplichting om de betrokkene in te lichten nakomen via zijn gebruikelijke contacten met de betrokkenen. Hij moet dus daarover geen aparte correspondentie voeren. Dat in deze bepaling enkel over het schriftelijk marktonderzoek wordt gesproken, is te wijten aan het feit dat marktonderzoek via elektronische kanalen behandeld wordt in de ontwerp-richtlijn over de bescherming van personen in het kader van telecommunicatienetwerken.

4.5.9. Geautomatiseerde individuele besluiten

Volgens art. 16, 1° van de ontwerp-richtlijn heeft eenieder het recht om niet te worden vermeld in een voor hem/haar bezwarend administratief of particulier besluit dat louter op grond van een persoonlijkheidsprofiel opleverende geautomatiseerde behandeling van gegevens is genomen. Er moet dus aan drie voorwaarden gelijktijdig voldaan zijn:

- de persoon moet het voorwerp zijn van een besluit dat hem benadeelt;
- het besluit moet uitsluitend genomen zijn op grond van een geautomatiseerde behandeling; als de informatica enkel een hulpmiddel was bij de besluitvorming, die aangevuld werd met menselijke interpretatie, is deze voorwaarde niet vervuld;
- de behandeling moet van toepassing zijn op gegevens betreffende de betrokkene over variabelen waaruit een typeprofiel (goed of slecht) van de persoonlijkheid wordt afgeleid; gevallen waarin het systeem geen definitie geeft van het persoonlijkheidsprofiel, zijn dus uitgesloten (bijv. als een bankautomaat een betaling weigert omdat het vereiste saldo op de rekening ontbreekt: dit is geen persoonlijkheidsprofiel). Deze regel kent twee uitzonderingen:
- het besluit werd genomen in het kader van een overeenkomst; deze uitzondering geldt echter alleen als aan het verzoek van de betrokkene is voldaan of er passende maatregelen zijn genomen ter bescherming van zijn rechtmatig belang; met deze beperking wil men het geval van ongelijke machtsverhouding, bijv. tussen een werkgever en een sollicitant, of tussen een bank en een kredietaanvrager, regelen; in dat laatste geval mag een negatieve "score" niet automatisch leiden tot een kredietweigering; er moet nog een "menselijke" evaluatie volgen;
- het besluit vindt zijn grondslag in een wet waarin de tot bescherming van het gerechtvaardigde belang van de betrokkene strekkende maatregelen zijn omschreven (?).

4.5.10. Recht om naar de rechter te stappen

Art. 22 zegt dat een ieder zich bij schending van de in de (ontwerp-)richtlijn gewaarborgde rechten moet kunnen wenden tot de rechter.

4.5.11. Recht op schadevergoeding

Wie schade lijdt ten gevolge van een onrechtmatige behandeling van zijn persoonsgegevens heeft recht op schadevergoeding vanwege de verantwoordelijke voor de behandeling. Het recht van de Lid-Staten kan bepalen dat de verantwoordelijke van zijn verantwoordelijkheid kan worden ontheven, indien hij het bewijs levert dat hij passende beveiligingsmaatregelen heeft genomen.

4.6. DIVERSE BEPALINGEN

De tien laatste artikelen van de ontwerp-richtlijn bevatten diverse bepalingen over de volgende onderwerpen:

4.6.1. Export van persoonsgegevens naar derde landen

Uitvoer van persoonsgegevens naar derde landen buiten de Europese Unie zal slechts toegelaten zijn als het betrokken land een "passend beschermingsniveau" waarborgt; op deze regel zijn volgende uitzonderingen:

- de betrokkene heeft zijn toestemming gegeven voor export in het kader van een contract of van precontractuele betrekkingen;
- de doorgifte is noodzakelijk voor de uitvoering van een overeenkomst met de betrokkene en deze laatste is op de hoogte gebracht dat het land van bestemming geen passend beschermingsniveau waarborgt;
- de doorgifte is noodzakelijk voor de vrijwaring van een zwaarwegend openbaar belang;
- de doorgifte is noodzakelijk voor de bescherming van vitale belangen van de betrokkene.

4.6.2. Gedragcodes

De ontwerp-richtlijn laat de mogelijkheid open voor gedragcodes met aanvullende regels, die door de betrokken kringen van het beroeps- en bedrijfsleven worden opgesteld met het oog op de specifieke kenmerken van bepaalde sectoren. Er wordt daarbij zowel aan nationale als aan Europese gedragcodes gedacht.

4.6.3. Toezichthoudende autoriteit

Artikel 30 van de ontwerp-richtlijn bevat enkele zeer algemene bepalingen over de toezichthoudende autoriteit die in elke Lid-Staat aanwezig moet zijn. In ons land is dat de Commissie voor de bescherming voor de persoonlijke levenssfeer.

4.6.4. Groep voor de bescherming van personen i.v.m. de behandeling van persoonsgegevens

Op Europees niveau komt er een groep van raadgevende aard bestaande uit vertegenwoordigers van de nationale toezichthoudende autoriteiten. Deze groep moet zorgen voor de homogene toepassing van de ter uitvoering van de richtlijn vastgestelde nationale voorschriften. Ze moet ook advies uitbrengen over het beschermingsniveau van derde landen met het oog op export van persoonsgegevens. Ze moet de Europese Commissie adviseren over ontwerpen tot wijziging van de richtlijn of over andere maatregelen op dit terrein. Ook over eventuele Europese sectoriële gedragcodes heeft zij een adviserende bevoegdheid.

4.6.5. Regelgevende bevoegdheid van de Commissie

In samenwerking met een Raadgevend Comité met vertegenwoordigers van de Lid-Staten zal de Europese Commissie uitvoeringsbepalingen kunnen uitvaardigen. Daarin zullen bijv. op Europees vlak concretere bepalingen staan voor specifieke sectoren. Het kan ook gaan om maatregelen die noodzakelijk zijn om een homogene toepassing van de bepalingen van de richtlijn te waarborgen. Dit lijkt noodzakelijk omdat de tekst van de ontwerp-richtlijn op vele punten tot zeer uiteenlopende interpretaties aanleiding kan geven.

4.6.6. Uitvoeringsdatum

De Lid-Staten moeten uiterlijk op 1 juli 1994 de bepalingen van de ontwerp-richtlijn (indien ze tijdig door de Raad wordt goedgekeurd) omzetten in hun nationale rechtsorde. Voor bestaande "handelingen" is tot 30 juni 1997 tijd om zich in regel te stellen.

5. ANTECEDENTEN VAN DE BELGISCHE WET VERWERKING PERSOONS- GEGEVENS

5.1. ALGEMEEN

De voorbereiding van de Belgische Wet Verwerking Persoonsgegevens begon al in het begin van de zeventiger jaren³⁹. Vanaf 1967 was men begonnen met de eerste experimenten voor een Rijksregister van de natuurlijke personen. De regering beloofde toen dat samen met een wetsontwerp over het Rijksregister ook een ontwerp voor een globale privacywet zou ingediend worden. Dat ontwerp werd uiteindelijk in 1976 door de toenmalige Justitieminister Herman Vanderpoorten ingediend⁴⁰. Het handelde zowel over het af luisteren en bespieden als over de gegevensbanken. Toen in 1983 uiteindelijk de wet op het Rijksregister⁴¹ werd uitgevaardigd, was het ontwerp Vanderpoorten al in de onderste lade verzeild geraakt. Nochtans had België in 1981 mee het hoger beschreven Verdrag van de Raad van Europa over de bescherming van personen bij de geautomatiseerde verwerking van persoonsgegevens ondertekend.

In de Rijksregisterwet werden een aantal specifieke bepalingen opgenomen over de bescherming

³⁹ De eerste wetsvoorstellen over het onderwerp dateren van het einde van de zestiger jaren. Zie bv. het wetsvoorstel van Baert, Jorissen, e.a. dat op 7 oktober 1969 in de Senaat werd ingediend, Parl. Doc. Senaat, 1968-1969, 562. Daarin wordt voorgesteld om op apparatuur voor het af luisteren, bespieden en registreren een wapenvergunning te eisen.

⁴⁰ Ontwerp van wet tot bescherming van bepaalde aspecten van de persoonlijke levenssfeer, Parl. Doc. Senaat, 1975-1976, 846.

⁴¹ Wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, B.S. 21 april 1984. Zie over deze wet vooral: J. Barthélémy, De wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, De Gemeente, 1987, p. 63-66, 123-128, 185-190, 321-326 en 446-452.

van de persoonlijke levenssfeer, o.m. het toegangs- en het correctierecht. Er werd ook een "Raadgevende commissie voor de bescherming van de persoonlijke levenssfeer" in het leven geroepen voor het toezicht op die bepalingen. Dezelfde techniek werd ook al gebruikt in het volmachtsbesluit over de databank van het overheidspersoneel⁴². Een toegangs- en correctierecht voor de geregistreerden werd ook opgenomen in het koninklijk besluit betreffende de registratie van afbetalingscontracten⁴³.

De tekst van het wetsontwerp Vanderpoorten werd eind 1983 in gewijzigde vorm terug ingediend door Justitieminister Gol⁴⁴. In de eerste versie sloeg het nog steeds op het af luisteren en bespieden én op de "geautomatiseerde persoonsregistraties". Beide thema's werden achteraf van elkaar losgekoppeld⁴⁵.

De problematiek kwam opnieuw te berde bij de oprichting van de Kruispuntbank voor de Sociale Zekerheid, begin 1990⁴⁶. Naast een aantal klassieke bepalingen over de bescherming van de persoonlijke levenssfeer, werd in de betrokken wet ook een bepaling opgenomen waarin de "Commissie voor de bescherming van de persoonlijke levenssfeer" werd opgericht⁴⁷. Deze Commissie wordt door de nieuwe wet tot bescherming van de persoonlijke levenssfeer behouden. Haar bevoegdheid werd inmiddels ook al uitgebreid door de wet van 18 juli 1990 tot wijziging van de wet betreffende de politie van het wegverkeer⁴⁸, door de wet van 12 juni 1991 op het consumentenkrediet⁴⁹ en door de wet van 19 juli 1991 betreffende de bevolkingsregisters

⁴² Koninklijk Besluit nr. 141 van 30 december 1982 tot oprichting van een databank betreffende de personeelsleden van de overheidssector, B.S., 13 januari 1983.

⁴³ Koninklijk Besluit van 15 april 1985 betreffende de registratie van afbetalingscontracten, B.S., 20 april 1985.

⁴⁴ Wetsontwerp tot bepaalde aspecten van de persoonlijke levenssfeer, Parl. Doc. Kamer, 1983-1984, 778.

⁴⁵ Wetsontwerp tot bescherming van de persoonlijke levenssfeer ten opzichte van geautomatiseerde persoonsregistraties, Parl. Doc. Kamer, 1984-1985, 1330.

⁴⁶ Wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid, B.S., 22 februari 1990.

⁴⁷ Zie art. 92 van de wet. In de artikelen 83 en 84 wordt de vroegere "Raadgevende commissie voor de bescherming van de persoonlijke levenssfeer" afgeschaft, die was opgericht bij art. 6 van het K.B. nr. 141 van 30 december 1982 en door art. 12 van de wet van 8 augustus 1983 tot regeling van het Rijksregister.

⁴⁸ Dit heeft te maken met de invoering van het "rijbewijs met strafpunten" en de inrichting van de databank voor het beheer daarvan.

⁴⁹ Wet van 12 juni 1991 op het consumentenkrediet, B.S., 9 juli 1991; zie ook het K.B. van 20 november 1992 betreffende de verwerking van persoonsgegevens inzake consumentenkrediet en het K.B. van dezelfde datum betreffende de registratie door de Nationale Bank van België van wanbetalingen inzake consumentenkrediet, B.S., 11 december 1992.

en de identiteitskaarten⁵⁰.

Ondertussen werden met de regelmaat van de klok in het Parlement wetsvoorstellen over de bescherming van de persoonlijke levenssfeer neergelegd⁵¹. Er moest echter worden gewacht op een regeringsinitiatief. Op 6 mei 1991 werd het wetsontwerp van oud-Justitieminister Gol door zijn opvolger Wathelet opnieuw ingediend⁵². Mede onder de druk van de internationale verplichtingen waartoe ons land zich had verbonden⁵³, raakte de trein ditmaal op de sporen. Door de val van de regering Martens VIII werden de werkzaamheden weliswaar onderbroken maar vanaf april 1992 konden ze worden voortgezet⁵⁴. Uiteindelijk werd de tekst op 26 november goedgekeurd 1992.

5.2. HET RIJKSREGISTER

5.2.1. Inhoud van het Rijksregister

Volgens artikel 1 van de wet is het Rijksregister "een systeem dat instaat voor de opnemings, de memorisatie en de mededeling van informatie betreffende de identificatie van natuurlijke personen". Artikel 2 bepaalt dat in het Rijksregister worden ingeschreven: de personen die ingeschreven zijn in de bevolkingsregisters of in de vreemdelingenregisters gehouden in de gemeenten, en de personen die ingeschreven zijn in de registers gehouden in de diplomatieke zendingen en de consulaire posten in het buitenland. Iedere persoon krijgt een identificatienum-

⁵⁰ Wet van 19 juli 1991 betreffende de bevolkingsregisters en de identiteitskaarten en tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, B.S., 3 september 1991. Zie ook de vier Koninklijke Besluiten tot uitvoering van deze wet, B.S., 15 augustus 1992.

⁵¹ Naast het al eerder aangehaalde wetsvoorstel van Baert, Jorissen, e.a. (Parl. Doc. Senaat, 1968-1969, 562), dat opnieuw werd ingediend op 4 januari 1972 (Parl. Doc. Senaat 1971-1972, 72) en nog eens op 10 juli 1974 (Parl. Doc. Senaat, B.Z. 1974, 338) vermelden we o.m. nog het wetsvoorstel van De Baeck, Herbiet en Pierson van 19 juli 1971, Parl. Doc. Senaat, 1970-1971 (opnieuw ingediend op 26 januari 1972, Parl. Doc. Senaat, 1971-1972, 142 en nog eens op 18 augustus 1977, Parl. Doc. Senaat, B.Z. 1977, 136), het wetsvoorstel van Scokaert, Brouhon, Van Elewijck en Van Lent van 24 april 1973, Parl. Doc. Kamer, 1972-1973, 537, het wetsvoorstel van Van Steenkiste, Baert en Belmans van 7 december 1977, Parl. Doc. Kamer, 1977-1978, 200, het wetsvoorstel van L. Van den Bossche van 3 februari 1986, Parl. Doc. Kamer, 1985-1986, 274, het wetsvoorstel van Verhaegen van 16 juni 1989, Parl. Doc. Kamer, 1984-1985, 1227 en het wetsvoorstel van Michel van 13 december 1989, Parl. Doc. Kamer, 1989-1990, 1029.

⁵² Wetsontwerp tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, Parl. Doc. Kamer, 1990-1991, 1610.

⁵³ Hierbij denken we in de eerste plaats aan de Schengen-Uitvoeringsovereenkomst van 19 juni 1990. Daarin komen de partners overeen dat in elk deelnemend land een wetgeving over de bescherming van de persoonlijke levenssfeer bij de verwerking van persoonsgegevens moet bestaan, voor de Overeenkomst kan worden geratificeerd.

⁵⁴ Parl. Doc. Kamer 1991-1992, 413; zie ook Parl. Hand. Kamer, 8 juli 1992 ; Parl. Doc. Senaat, 1991-1992, 445; Parl. Hand. Senaat, 10 november 1992.

mer. Het koninklijk besluit van 3 april 1984 stelt de samenstelling van dat nummer vast (elf cijfers waarvan zes cijfers de geboortedatum weergeven, drie cijfers dienen om de personen te identificeren die dezelfde dag geboren zijn en bovendien ook het geslacht aangegeven en twee cijfers die een controlegetal vormen).

Luidens artikel 3 worden voor iedere persoon de volgende gegevens opgenomen en bewaard : 1) naam en voornamen, 2) de geboorteplaats en -datum, 3) het geslacht, 4) de nationaliteit, 5) de hoofdverblijfplaats, 6) de plaats en datum van overlijden, 7) het beroep, 8) de burgerlijke staat en 9) de samenstelling van het gezin. Op verzoek van een gemeentebestuur kan andere informatie in het Rijksregister worden opgenomen, doch deze bijkomende informatie mag enkel worden meegedeeld aan de gemeente die ze heeft verstrekt. Deze bepaling is het gevolg van het feit dat, vanaf 1968, andere gegevens in het Rijksregister hadden doen opnemen dan enkel deze die uiteindelijk in de wet werden voorzien.

5.2.2. Toegang tot het Rijksregister

Artikel 5 van de wet zegt dat de Koning toegang kan verlenen tot het Rijksregister aan de openbare overheden, de instellingen van openbaar nut en de notarissen en de gerechtsdeurwaarders. Bij een in Ministerraad overlegd besluit, en na advies van een Raadgevende Commissie (zie hierna), kan de Koning de toegang uitbreiden tot "instellingen van Belgisch recht die opdrachten van algemeen belang vervullen". Op grond van artikel 5 hebben een groot aantal instellingen toegang gekregen tot het Rijksregister, o.m. de dienst Vreemdelingen bij het Ministerie van Justitie, het Ministerie van Financiën, het Nationaal Instituut voor de Statistiek, de Dienst Kijk- en Luistergeld, het Hoog Comité van Toezicht, de Provinciegoeverneurs en de Bestendige Deputaties, het Ministerie van Sociale Voorzorg, de instellingen van sociale zekerheid, de onderzoeksrechters, de gerechtsdeurwaarders, de notarissen, de Rijkswacht, enz. Volgens artikel 8 kan de Koning, bij een in Ministerraad overlegd besluit en na advies van de Raadgevende Commissie, toelating verlenen, om het identificatienummer van het Rijksregister te gebruiken. Ook deze lijst van instellingen is ondertussen al zeer lang geworden en regelmatig worden nog nieuwe toelatingen verleend.

5.2.3. Bescherming van de persoonlijke levenssfeer

Ter bescherming van de persoonlijke levenssfeer zijn in de wet op het Rijksregister voornamelijk drie soorten maatregelen voorzien: inzage- en correctierecht voor de geregistreerde personen, plichten voor de personen die tussenkomen bij de werking van het Rijksregister, en oprichting van een Raadgevende Commissie.

5.2.3.1. Inzage- en correctierecht

Volgens artikel 10 van de wet heeft ieder in het Rijksregister ingeschreven persoon of zijn wettelijke vertegenwoordiger het recht op mededeling van de hem betreffende gegevens, en op verbetering van de gegevens (enkel de negen verplichte gegevens!) die onjuist of onvolledig zijn.

Bij Koninklijk besluit van 3 april 1984 worden de details van dit inzage- en correctierecht geregeld. De betrokkene dient persoonlijk of per aangetekende brief een aanvraag te richten bij de gemeente waar hij ingeschreven is. Indien technisch mogelijk wordt er onmiddellijk gevolg gegeven aan de aanvraag. Anders krijgt de aanvrager een ontvangstmelding en moet binnen de maand aan de aanvraag worden voldaan. De informatie uit het Rijksregister wordt "schriftelijk en in een eenvoudig te begrijpen vorm" meegedeeld.

5.2.3.2. Plichten voor de personen die meewerken aan het Rijksregister

De personen die bij het uitoefenen van hun functies tussenkomen in de werking van het Rijksregister (ook in de gemeenten !) (artikel 11 van de wet):

- zijn gehouden tot het beroepsgeheim;
- moeten alles in het werk stellen om de gegevens bij te houden, de onjuiste gegevens te verbeteren en vervallen gegevens te schrappen;
- moeten de veiligheid van de gegevens verzekeren.

5.2.3.3. Raadgevende Commissie

Artikel 12 van de wet voorziet de oprichting van een Raadgevende Commissie. De samenstelling en de werkwijze van deze commissie is geregeld in het Koninklijk besluit van 20 april 1984.

De commissie bestaat uit acht leden (4 NL + 4 F) waarvan er vier worden voorgedragen door de Minister van Justitie (een magistraat, een ambtenaar, een advocaat en een academicus), drie door de Minister van Binnenlandse Zaken (een ambtenaar, een academicus en een expert) en één door de Minister van Economische Zaken (een lid van de Hoge Raad voor de Statistiek). De Raadgevende Commissie is ondertussen vervangen door de Commissie voor de Bescherming van de Persoonlijke Levenssfeer, die werd opgericht door de wet van 15 januari 1990 op de kruispuntbank voor de sociale zekerheid (zie hierna).

5.3. DE DATABANK VAN HET OVERHEIDSPERSONEEL

Bij volmachtsbesluit nr. 141 van 30 december 1982 werd een databank opgericht betreffende de personeelsleden van de overheidssector. De bedoeling van de regering was te kunnen beschikken over de nodige statistische gegevens inzake het personeel van de overheidssector om maatregelen te kunnen nemen in het kader van de sanering der openbare financiën. Artikel 2 van het besluit geeft een lijst van de overheden en instellingen waarvan de personeelsleden worden opgenomen in de databank:

- de besturen en andere diensten van de Staat;
- de krijgsmacht;
- de door de Staat georganiseerde of gesubsidieerde onderwijsinrichtingen, diensten voor school- en beroepsoriëntering en P.M.S.-centra;
- de magistratuur en de diensten van de rechterlijke macht;
- de Raad van State;
- de instellingen van openbaar nut onderworpen aan het gezag, de controle of het toezicht

- van de Staat;
- de diensten van de buitenlandse betrekkingen;
- het bestuur Erediensten, Giften, Legaten en Stichtingen.

Al deze diensten en instellingen dienden volgende gegevens te verstrekken aan het Ministerie van Openbaar Ambt:

- de administratieve en geldelijke toestand van de personen waarvan de bezoldiging wordt aangerekend op hun begroting;
- het aantal betrekkingen of ambten overeenstemmend met elke graad of functie de globale uitgaven verbonden aan de bezoldigingen.

Het besluit bevat, naar analogie met de wet op het Rijksregister, een drietal maatregelen ter bescherming van de persoonlijke levenssfeer:

- een inzage- en correctierecht;
- een aantal plichten voor de personen die betrokken zijn bij de werking van de databank, nl. beroepsgeheim, zorgvuldigheidsplicht en beveiligingsplicht;
- de oprichting van een Raadgevende Commissie (deze commissie is dezelfde als deze die werd opgericht in het kader van de wet op het Rijksregister).

5.4. DE KRUISPUNTBANK VOOR DE SOCIALE ZEKERHEID

Bij de wet van 15 januari 1990 werd de "Kruispuntbank voor de sociale zekerheid" opgericht. Deze instelling is belast met het leiden, het organiseren en het machtigen van de uitwisseling van sociale gegevens tussen de sociale gegevensbanken. Zoals bekend is ons systeem van sociale zekerheid zeer complex, o.m. door het groot aantal betrokken instellingen: ministeries, parastatalen, ziekenfondsen, werkloosheidskassen, verzekeringsinstellingen, enz. Volgens de memorie van toelichting was het teregt om telkens, voor elk soort van uitkering, aan de betrokken burgers opnieuw dezelfde gegevens te moeten opvragen. Dat kostte niet alleen veel tijd en geld, maar de verspreiding van de sociale gegevens over zoveel geïsoleerde databanken maakte ook een efficiënte controle onmogelijk, o.m. van de toepassing van cumulatieregels. Een fusie van de verschillende sociale gegevensbanken tot één centrale databank was uiteraard niet haalbaar en misschien zelfs niet wenselijk. Daarom heeft men een "kruispuntbank" opgericht. Deze kruispuntbank bevat zelf zeer weinig inhoudelijke informatie. De kruispuntbank beheert een repertorium waarin, per persoon, wordt aangegeven bij welke instelling welke sociale gegevens aanwezig zijn. De gegevens zelf blijven dus bij de afzonderlijke instellingen. De bedoeling bestaat er dan in dat, telkens een instelling een gegeven nodig heeft, zij eerst moet nakijken of deze informatie niet reeds bij een andere instelling aanwezig is. Dit gebeurt door consultatie van de kruispuntbank. Indien de gegevens reeds bij een andere instelling aanwezig zijn, en de vraag om deze gegevens rechtmatig is, vraagt de kruispuntbank de gegevens op de juiste plaats op en stelt ze elektronisch ter beschikking van de instelling die ze nodig heeft.

De Kruispuntbankwet slaat, in tegenstelling tot wat haar titel laat vermoeden, niet enkel op de kruispuntbank, haar werking en haar betrekking met de andere sociale zekerheidsinstellingen.

De bepalingen tot bescherming van de sociale persoonsgegevens gelden voor alle sociale zekerheidsinstellingen en dit voor hun volle activiteit inzake sociale zekerheid, d.w.z. niet enkel in hun betrekkingen met de kruispuntbank. Bovendien gelden deze beschermingsregels voor alle "sociale gegevens van persoonlijke aard", ongeacht de informatiedrager. "Sociale gegevens van persoonlijke aard" worden gedefinieerd als alle gegevens die nodig zijn voor de toepassing van de sociale zekerheid met betrekking tot een persoon die is of kan worden geïdentificeerd en die door een sociale zekerheidsinstelling worden bewaard.

In de Kruispuntbankwet legt men de meeste verplichtingen op aan de "instellingen van sociale zekerheid". In art. 24 wordt het aanstellen van een veiligheidsconsulent, die is belast met adviesverstrekking en interne controle inzake informatieveiligheid, verplicht gesteld. Volgens art. 23, tweede lid van de Kruispuntbankwet, mogen sociale gegevens "uitsluitend worden aangewend voor de doeleinden vastgelegd door of krachtens deze wet of voor het vervullen van hun wettelijke verplichtingen" en mag over die persoonsgegevens slechts worden beschikt "gedurende de tijd nodig voor de toepassing van de sociale zekerheid". Betreffende de beveiliging vinden we in de Kruispuntbankwet in art. 20 een zeer algemene verplichting: de instellingen van sociale zekerheid moeten nl. "alle maatregelen treffen om een perfecte bewaring van de sociale gegevens van persoonlijke aard te verzekeren".

Speciale bescherming genieten medische gegevens. Medische gegevens zijn persoonsgegevens "waaruit informatie kan worden afgeleid omtrent diens vroegere, huidige of toekomstige fysieke of psychische gezondheidstoestand, met uitzondering van de louter administratieve of boekhoudkundige gegevens betreffende de geneeskundige behandelingen of verzorging" (art. 2, eerste lid, 7° Kruispuntbankwet). Deze medische gegevens mogen volgens de algemene privacywet van 8 december 1992, die hierna zal worden besproken, uitsluitend onder het toezicht en de verantwoordelijkheid van een beoefenaar van de geneeskunst worden verwerkt. Deze vereiste valt echter weg wanneer de betrokkene een bijzondere schriftelijke toestemming heeft verleend (art. 7, tweede lid van de wet van 8 december 1992). Onder de term "beoefenaar van de geneeskunst" vallen geneesheren, tandartsen, apothekers e.d. De Kruispuntbankwet is op twee vlakken strenger. De uitzondering bij een bijzondere schriftelijke toestemming van de betrokkene is nl. niet voorzien in de Kruispuntbankwet. Bovendien wordt daarin bepaald dat het toezicht en de verantwoordelijkheid door een geneesheer uitgeoefend moeten worden (art. 26, § 1). In beide wetten (Kruispuntbankwet en Wet Verwerking Persoonsgegevens) is, betreffende medische gegevens, bepaald dat de personen die betrokken zijn bij de verwerking van die gegevens of die er toegang toe hebben bij name moeten worden aangewezen en dat de inhoud en de draagwijdte van de toegangsmachtiging moeten worden vastgelegd waarvan melding wordt gemaakt in een regelmatig bijgehouden register. In de Wet Verwerking Persoonsgegevens wordt expliciet gezegd dat ook de namen in dat register moeten vermeld worden en dat de personen die betrokken zijn bij de verwerking of toegang hebben tot medische gegevens, nominatim moeten worden aangewezen door de verantwoordelijke. De Kruispuntbankwet voorziet echter nog een bijkomende beveiliging i.v.m. de toegang tot de medische gegevens: "De toegang tot de medische gegevens opgeslagen in de geautomatiseerde sociale-gegevensbanken geschiedt door middel van individuele toegangs- en bevoegdheidscodes.

De titularissen van deze codes mogen ze aan niemand bekend maken. De bewaring van de medische gegevens van persoonlijke aard in een geautomatiseerd archief moet gebeuren op niet rechtstreeks toegankelijke informatiedragers". Deze regel uit art. 26, § 3 van de Kruispuntbankwet houdt een grote bescherming van de persoonsgegevens in en is een zinvolle aanvulling bij de verplichting van het opstellen van een register. Welke bescherming biedt immers een register waar geschreven staat tot welke gegevens de persoon gemachtigd is toegang te hebben, als hij de facto toegang heeft tot alle medische gegevens ?

De Kruispuntbankwet voorziet in de artikelen 10 tot en met 16 een regeling van mededeling van gegevens binnen en buiten het netwerk van de kruispuntbank. Zo zijn de instellingen van de sociale zekerheid verplicht aan de kruispuntbank alle sociale gegevens mee te delen die deze nodig heeft voor de uitvoering van haar taak. Voorzover de sociale gegevens in het netwerk beschikbaar zijn, zijn de instellingen verplicht ze uitsluitend bij de kruispuntbank op te vragen, ook wanneer men de juistheid van gegevens wil nagaan, tenzij de opslag van deze gegevens juist aan de betrokken instelling is toevertrouwd. Buiten enkele uitzonderingen, bijvoorbeeld wanneer men zich richt tot de betrokkene zelf, gebeurt de mededeling van sociale gegevens steeds door bemiddeling van de kruispuntbank. De Koning kan ook gevallen bepalen waarin dit niet zal vereist zijn i.v.m. mededeling van gegevens aan instellingen van sociale zekerheid. Nochtans vereist elke mededeling binnen of buiten het netwerk een principiële machtiging van het Toezichtscomité. Voor mededelingen binnen het netwerk kan de Koning hierop uitzonderingen voorzien.

De Koning kan bij een in Ministerraad overlegd besluit de personen aanwijzen die in oorlogstijd, in omstandigheden daarmee gelijkgesteld of tijdens de bezetting van het grondgebied door de vijand de verwerkt gegevens moet vernietigen (art. 29 Kruispuntbankwet). De Koning bepaalt de modaliteiten en de voorwaarden van de vernietiging. In de Wet Verwerking Persoonsgegevens is er voorzien dat de Koning ook een bedrag kan vaststellen ter vergoeding voor de vernietigingen. Opmerkelijk is wel dat de Kruispuntbankwet bij niet naleving van deze artikelen straffen voorziet van tweehonderd frank tot en met een jaar gevangenisstraf plus tienduizend frank (art. 63, 2 Kruispuntbankwet). Volgens de Wet Verwerking Persoonsgegevens kan men enkel met een geldboete bestraft worden, nl. van honderd frank tot honderdduizend frank.

Volgens de Kruispuntbankwet heeft eenieder "het recht op mededeling van de hem betreffende sociale gegevens van persoonlijke aard die zijn opgenomen in de sociale gegevensbanken" (art. 19, eerste lid, 1°). Als verplichting ter uitvoering van dit artikel wordt aan de instellingen opgelegd mede te delen "de sociale gegevens van persoonlijke aard waarop zij zich gesteund hebben bij de bepaling of de beoordeling van hun rechten. De mededeling geschiedt uiterlijk op het ogenblik van de kennisgeving van de beslissing over het recht dat is beoordeeld op basis van de betrokken gegevens. Elke wijziging in de beoordeling van het recht moet eveneens aanleiding geven tot een mededeling. De Koning kan afwijkingen voorzien bij een in Ministerraad overlegd besluit" (art. 20, § 1, 1°). Artikel 21 voorziet een bijkomende verplichting i.v.m. mededeling van gegevens, deze moet nl. "op een voor het publiek verstaanbare wijze gebeuren". Het recht om kennis te krijgen van de eigen gegevens en het recht om onjuiste gegevens te doen

verbeteren is in de Kruispuntbankwet op dezelfde wijze geregeld als in de algemene Wet Verwerking Persoonsgegevens (art. 19 en 20).

Indien de betrokkene geen voldoening krijgt, kan hij zich wenden tot een onafhankelijk Toezichtscomité. De naam van de persoon die zich tot het Toezichtscomité wendt, mag niet worden bekendgemaakt, tenzij de betrokkene daartoe uitdrukkelijk de toestemming voor geeft (art. 48 en 49). Binnen een redelijke termijn stelt de voorzitter van het Toezichtscomité de indieners van klachten, aanvragen of voorstellen in kennis van het gevolg dat aan hun tussenkomst werd gegeven, de redenen die ten grondslag liggen aan hun standpunt of, in voorkomend geval, van het standpunt van de Commissie voor Bescherming van de Persoonlijke Levenssfeer (art. 50). Het Toezichtscomité (of de Commissie) moet op de hoogte worden gebracht van het gevolg dat aan zijn "bemoeiing" is gegeven (art. 51) of men kan de aanbeveling of beslissing openbaar maken. De voorzitter kan ieder geschil aangaande de toepassing van de Kruispuntbankwet en haar uitvoeringsbesluiten aan de arbeidsgerechten voorleggen (art. 52).

Volgens de Kruispuntbankwet moet de werkgever op een zichtbare en toegankelijke plaats een bericht aanplakken waarin de plaats wordt meegedeeld waar in de onderneming de tekst van de wet en van haar uitvoeringsbesluiten kan worden geraadpleegd. Iedere werknemer moet dan ook op elk ogenblik en zonder tussenpersoon kennis kunnen nemen van deze wet en van haar uitvoeringsbesluiten (art. 27 Kruispuntbankwet).

5.5. DE WET OP HET CONSUMENTENKREDIET

Hoofdstuk VI van de wet van 12 juni 1991 handelt specifiek over de bescherming van persoonsgegevens betreffende het consumentenkrediet. Het gaat daarbij over de verwerking van persoonsgegevens door de kredietverlener. De belangrijkste principes zijn⁵⁵:

- het finaliteits- en proportionaliteitsprincipe;
- een beperking van het aantal toegelaten gegevens: identiteit, bedrag en duur van het krediet, periodiciteit van de betalingen, betalingsfaciliteiten, achterstanden, kredietgever;
- een beperking van de personen en instellingen aan wie de gegevens mogen worden meegedeeld;
- een beperking van de bewaartijd en de verplichting om de gegevens afdoend te beveiligen.

Verder worden een aantal controlemechanismen opgenomen die grotendeels overeenkomen met deze die in de wet van 8 december 1992 voorkomen:

- de kennisgeving bij de eerste registratie;
- het kosteloze toegangsrecht;
- het recht tot verbetering en aanvulling (bv. met de reden van wanbetaling);
- het recht van beroep.

⁵⁵ Zie verder ook E. Meysmans, "De verwerking van persoonsgegevens inzake consumentenkrediet", Computerrecht, 1993/1, p. 2.

De wet op het consumentenkrediet regelt ook de centrale databank over het consumentenkrediet die in de schoot van de Nationale Bank wordt beheerd. Deze materie wordt verder gedetailleerd in een Koninklijk besluit van 20 november 1992⁵⁶.

Het begrippenkader is in artikel 1, 14° tot en met 16° neergelegd. Daarbij is vooral de, in vergelijking met de algemene Wet Verwerking Persoonsgegevens van 8 december 1992, afwijkende definitie van "houder van het bestand". Volgens art. 1, 16° is dat "de natuurlijke persoon of rechtspersoon of de instelling zonder rechtspersoonlijkheid die het bestand bijhoudt". De definitie van "bestand" is dezelfde als deze in de algemene Wet Verwerking Persoonsgegevens, doch de voorbereidende werken leren ons dat onder een systematische raadpleging dient te worden verstaan een ondervraging van een bestand door een derde, afkomstig van buiten de instelling waar het bestand wordt aangelegd. Het toepassingsveld van Hoofdstuk VI van de wet op het consumentenkrediet wordt hiermee tot "externe" bestanden beperkt en interne bestanden worden geacht door de algemene wet te worden beheerst. Het sectorieel karakter van het wetgevend initiatief komt in artikel 68 tot uiting. Naar luid van dit artikel worden enkel al dan niet geautomatiseerde verwerkingen van persoonsgegevens die betrekking op het consumentenkrediet hebben, gevisieerd. Uit de parlementaire bespreking van artikel 69, ° 4, tweede lid, eerste zin, blijkt dat raadplegingen van externe bestanden eveneens met het oog op kredietverlening voor zowel gemengde als uitsluitende beroepsdoeleinden mogen geschieden, voor zover de kredieten op het privé-vermogen van de kredietnemer zullen wegen.

Het finaliteitsprincipe is in het gewijzigde artikel 69, § 1 neergelegd. Het is de wet - en niet de houder van het bestand - die de doelstelling van de verwerking bepaalt, nl. "de beoordeling van de financiële toestand en de solvabiliteit van de consument". Niet alle gegevens die relevant, aangepast en niet overdreven - in termen van de algemene wet: toereikend, ter zake dienend en niet overmatig - zijn om de financiële toestand en de solvabiliteit van de consument te beoordelen, mogen worden verwerkt. Op advies van de Raad van State heeft de wetgever in artikel 69, § 3 een limitatieve lijst van registreerbare gegevens ingevoerd. De inhoud van deze gegevens is gepreciseerd in het koninklijk besluit van 20 november 1992⁵⁷.

Artikel 69, § 4, eerste lid bevat een beperkende opsomming van de categorieën van personen die de externe bestanden mogen consulteren. Door de wet van 6 juli 1992 is deze opsomming uitgebreid met drie categorieën van personen die weliswaar strict genomen geen kredietovereenkomsten in de zin van de wet van 12 juni 1991 sluiten, maar toch er alle belang bij hebben dat zij van het bestaan van een aan een consument verleend krediet dan wel van een gebeurlijke wanbetaling in kennis worden gesteld (o.m. tot ondernemingen die betaalkaarten ter beschikking

⁵⁶ Koninklijk besluit van 20 november 1992 betreffende de registratie door de Nationale Bank van België van wanbetalingen inzake consumentenkrediet, B.S., 11 december 1992, p. 25622.

⁵⁷ Koninklijk Besluit van 20 november 1992 betreffende de verwerking van persoonsgegevens inzake consumentenkrediet, B.S., 11 december 1992, p. 25620.

stellen⁵⁸.

In het reeds aangehaalde artikel 69, § 4, tweede lid is het gebruik van de verkregen gegevens beperkt. Ook de tijdsperiode gedurende dewelke dergelijk gebruik geoorloofd is, is in artikel 69, § 6, tweede lid begrensd.

Het gewijzigde artikel 69, § 4, derde lid legt een beginsel van selectieve toegang vast. Een gegroepeerde raadpleging wordt slechts aanvaard, voor zover de groepering uit aparte, individuele en nominatieve aanvragen bestaat. Hieraan ten grondslag ligt de vrees voor een gebruik van dergelijke bestanden voor marketingdoeleinden.

Artikel 70 voorziet in een aantal rechten voor de geregistreerden : een recht van informatie, van toegang, van verbetering, van aanvulling, van verwijdering en van niet-aanwending. Het recht op kennisgeving bij de eerste registratie is in artikel 70, § 1 neergelegd. Bijzonder aan deze bepaling is de mogelijkheid tot een onrechtstreekse kennisgeving aan de geregistreerde. De wet noch de voorbereidende werken bevatten hieromtrent preciseringen. Overeenkomstig artikel 70, § 2 heeft de geregistreerde een kosteloos recht van toegang, tenminste voor zover de uitoefening ervan niet als onrechtmatig of overdreven moet worden beschouwd. Deze voorwaarde is in artikel 10 van het koninklijk besluit van 20 november 1993 nader gepreciseerd (maximaal eenmaal per trimester kosteloos). Artikel 70, § 2, laatste lid van de wet op het consumentenkrediet geeft aan de geregistreerden een "recht op aanvulling" en limiteert het meteen ook tot de mogelijkheid om de reden van wanbetaling toe te voegen. De voorbereidende werken leren ons bovendien dat de houder van het bestand niet verplicht is om de accurateid van de aanvullende en door de consument verstrekte gegevens na te gaan.

Artikel 71 van de wet op het consumentenkrediet bevat de regeling inzake de Centrale Gegevensbank. Deze regeling vervangt het koninklijk besluit van 15 april 1985 dat de juridische grondslag voor de Verbruikerskredietcentrale vormde. De Verbruikerskredietcentrale was een beperkte negatieve centrale: enkel wanneer er met betrekking tot verkopen en leningen op afbetaling, onderworpen aan de wet van 9 juli 1957, een kink in de kabel was, volgde een registratie. Bij de Centrale Gegevensbank heeft men deze beperking laten varen en de registratie opengetrokken tot wanbetalingen voortvloeiend uit alle mogelijke kredietovereenkomsten die onder de toepassing van de wet vallen en die aan door de Koning vastgestelde criteria beantwoorden.

Artikel 71, § 2 voorziet op termijn in de mogelijkheid van een positieve centrale. Dit zou betekenen dat men niet alleen die overeenkomsten waarbij zich een wanbetaling voordoet, registreert, maar wel alle of een deel van de onder het toepassingsgebied van de wet vallende

⁵⁸ Over de voorwaarden waaraan deze ondernemingen dan moeten voldoen, zie het koninklijk besluit van 11 januari 1993 tot vaststelling van de raadplegingsmodaliteiten en de voorwaarden waaraan de rechtspersonen die betaalkaarten ter beschikking stellen van de consument moeten voldoen om mededeling van persoonsgegevens te ontvangen, B.S., 9 februari 1993, p. 2881.

overeenkomsten, ongeacht het feit of er sprake is van een wanbetaling. Voor het toezicht op de bepalingen over de verwerking van persoonsgegevens inzake consumentenkrediet wordt in de oprichting van een Toezichtscomité voorzien (art. 72, § 2). Dit comité is nog niet operationeel.

5.6. DE WET BETREFFENDE DE POLITIE VAN HET WEGVERKEER

De meest opvallende nieuwigheid ingevoerd door de wet van 18 juli 1990 tot wijziging van de wet op de politie van het wegverkeer is ongetwijfeld het stelsel van het zogenaamde "rijbewijs met punten". Bij het begaan van een zware verkeersovertreding worden aan de overtreder strafpunten toegekend. Als men een aantal strafpunten heeft verzameld, krijgt men een sanctie. Zo moet men bij zes strafpunten bijvoorbeeld een veiligheidscursus volgen. De ultieme sanctie is de intrekking van het rijbewijs. Het bijhouden van de overtredingen en de strafpunten gebeurt via een centrale databank. Hierbij rijzen een aantal vragen over de bescherming van de persoonsgegevens. In de wet zijn een aantal regels ingebouwd die grotendeels gelijklopen met deze van de wet op de bescherming van de persoonlijke levenssfeer t.o.v. de verwerking van persoonsgegevens. De controle over de databank is toegewezen aan de Commissie voor de Bescherming van de Persoonlijke Levenssfeer (art. 6 van de wet van 18 juli 1990, dat in de wet op de politie van het wegverkeer van 16 maart 1968 opnieuw een art. 25 invoert). Momenteel is het systeem nog niet operationeel.

5.7. DE WET BETREFFENDE DE BEVOLKINGSREGISTERS

Op 3 september 1991 verscheen in het Belgisch Staatsblad de wet van 19 juli 1991 betreffende de bevolkingsregisters en de identiteitskaarten⁵⁹. Hierdoor werd de oude wet van 2 juni 1856 over de registers der bevolking opgeheven en werd, op een enkel punt, de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, gewijzigd. Met de inwerkingtreding van de vier koninklijke uitvoeringsbesluiten op 1 november 1992⁶⁰ werd een einde gesteld aan de praktijk die erin bestond gemeentelijke adreslijsten te verstrekken aan eenieder die het vroeg, en bereid was ervoor te betalen⁶¹.

Een eerste uitvoeringsbesluit van 16 juli 1992 "betreffende de bevolkingsregisters en het vreemdelingenregister"⁶² bepaalt de modaliteiten voor het houden van de registers (artikels 4 t/m 15) en stelt de aanvullende regels vast voor het bepalen van de hoofdverblijfplaats (artikels 16

⁵⁹ Wet van 19 juli 1991 betreffende de bevolkingsregisters en de identiteitskaarten en tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, B.S., 3 september 1991, 19075.

⁶⁰ De uitvoeringsbesluiten verschenen in het B.S. van 15 augustus 1992 en traden in werking op de eerste dag van de derde maand volgend op hun publicatie.

⁶¹ Verslag aan de Koning, B.S., 15 augustus 1992, 18042 en Alg. Onderr., nr. 112.

⁶² B.S., 15 augustus 1992, 18028.

t/m 20). Artikel 2, eerste lid van de wet bepaalt dat alleen de volgende informatiegegevens in de registers mogen worden opgenomen:

- gegevens waarvan de wet uitdrukkelijk bepaalt dat ze geregistreerd moeten worden;
- gegevens betreffende de identificatie en localisatie van de inwoners;
- gegevens die noodzakelijk zijn voor de verbinding met andere bestanden van het gemeentebestuur of van de centrale administratie.

Binnen die grenzen, en op limitatieve wijze, bepaalt een tweede K.B. van 16 juli 1992 "tot vaststelling van de informatie die opgenomen wordt in de bevolkingsregisters en in het vreemdelingenregister"⁶³ de aard van deze informatiegegevens.

Het derde K.B. van 16 juli 1992 "betreffende het recht op toegang tot de bevolkingsregisters en het vreemdelingenregister en betreffende het recht op verbetering van deze registers"⁶⁴ regelt de modaliteiten volgens welke de personen die in de registers ingeschreven zijn kennis kunnen nemen van alle informatie die er over hen bewaard wordt, en die eventueel kunnen laten verbeteren.

Het vierde K.B. van 16 juli 1991, tenslotte, "betreffende het verkrijgen van informatie uit de bevolkingsregisters en uit het vreemdelingenregister"⁶⁵ stelt de regels vast volgens welke gegevens uit de register kunnen worden meegedeeld aan derden. Principieel geldt een verbod van raadpleging door of mededeling aan derden. De overtreding van dit verbod wordt gestraft met een geldboete van 26 tot 500 frank. Derde is iedere andere persoon dan degene waarop de meegedeelde of geraadpleegde gegevens betrekking hebben. De vier modaliteiten volgens welke de informatie door de gemeentelijke overheid wel kan worden verstrekt zijn:

- in de vorm van uittreksels uit de registers of getuigschriften die aan de hand van die registers opgemaakt zijn (artikelen 2 t/m 4); eenieder die een hem betreffend uittreksel uit de registers vraagt of een getuigschrift dat aan de hand van die registers is opgemaakt, verkrijgt er afgifte van zonder te moeten doen blijken van enig bijzonder belang; deze aanvraag kan zelfs mondeling gebeuren; ook derden kunnen een uittreksel of een getuigschrift betreffende om het even welke inwoner uit een gemeente verkrijgen; de voorwaarden waaraan voldaan moet zijn, luiden als volgt:
 - * de aanvraag moet schriftelijk gebeuren en moet ondertekend zijn; hoewel niet uitdrukkelijk in het besluit bepaalt zal de aanvrager ook moeten vermelden met welk doel hij afgifte verlangt : het uittreksel moet dit immers vermelden;
 - * de derden moeten niet aantonen welk het belang is dat zij hebben bij de afgifte; die moet enkel "door of krachtens de wet voorgeschreven of toegestaan zijn"; deze voorwaarde moet door de gemeentelijke overheid worden gecontroleerd; als

⁶³ B.S., 15 augustus 1992, 18038.

⁶⁴ B.S., 15 augustus 1992, 18040.

⁶⁵ B.S., 15 augustus 1992, 18041.

voorbeeld vermelden de Alg. Onderr. artikel 1344bis Ger. W.: afgifte van een getuigschrift van de woonplaats van de gedaagde is noodzakelijk als bijlage bij het verzoekschrift tot inleiding van een huurgeschil voor de vrederechter; sinds de inwerkingtreding op 1 januari 1993 van de wet van 3 augustus 1992 tot wijziging van het Gerechtelijk Wetboek bestaat deze verplichting thans voor alle geschillen die door middel van een verzoekschrift kunnen worden ingeleid; overeenkomstig art. 1034quater moet op straffe van nietigheid bij elk verzoekschrift een door het gemeentebestuur afgegeven en niet vroeger dan vijftien dagen voor het verzoekschrift gedagtekend getuigschrift van woonplaats van de op te roepen persoon gevoegd worden; deze wetsbepaling is duidelijke een door de wet voorgeschreven grond tot afgifte;

- door raadpleging van de registers (artikel 5); luidens artikel 5 van het koninklijk besluit van 16 juli 1992 is de raadpleging van de registers verboden aan private personen; hierop is geen uitzondering; de enige personen die de registers mogen raadplegen zijn:
 - * publieke overheden of openbare instellingen wanneer dit door of krachtens de wet wordt toegestaan;
 - * de gemeentelijke diensten en de diensten die afhangen van het O.C.M.W. wanneer dit gebeurt voor interne doeleinden;
- door verstrekking van personenlijsten uit de registers (artikelen 6 t/m 10); de informatie die door middel van uittreksels en getuigschriften kan worden bekomen, heeft steeds betrekking op één persoon; wanneer men over meerdere inwoners persoonsgegevens wil vermelden, gebeurt dit op personenlijsten; luidens artikel 6 van het K.B. is het verstrekken van lijsten met personen ingeschreven in de registers verboden; op dit verbod van verstrekking van lijsten bestaan vijf, strict te interpreteren, uitzonderingen:
 - * overheden of openbare instellingen;
 - * instellingen die taken van algemeen belang vervullen; zij moeten daartoe een schriftelijke aanvraag doen met opgaaf van het gebruik dat van die lijsten zal worden gemaakt; het college van burgemeester en schepenen oordeelt over deze aanvraag;
 - * buitenlandse overheden met het voorafgaand akkoord van de Minister van Buitenlandse Zaken;
 - * politieke partijen, enkel voor verkiezingsdoeleinden, en in een beperkte periode voorafgaand aan de verkiezingen;
 - * opiniepeilingsinstellingen die erkend zijn door de Minister van Economische Zaken;
- in de vorm van statistische informatie (artikel 12); over het schriftelijk verzoek wordt door het college van burgemeester en schepenen beslist.

Het vierde koninklijk besluit van 16 juli 1992 regelt ook de manier waarop aan de ingeschreven persoon zelf de gegevens worden meegedeeld die op hem betrekking hebben. De voorwaarden voor de mededeling van de persoonsgegevens zijn de volgende:

- de aanvraag moet ingediend worden door een persoon die ingeschreven is in de registers voor de hem betreffende gegevens; ook de wettelijke vertegenwoordiger of een bijzonder

- mandataris mag de aanvraag doen; het is niet nodig dat de geregistreerde van een bijzonder belang doet blijken;
- de aanvraag moet schriftelijk gebeuren, gedagtekend en ondertekend zijn; zij wordt gericht in persoon tot de bevoegde dienst van de gemeente van inschrijving of tot het college van burgemeester en schepenen per aangetekende brief.

Wordt de aanvraag in persoon overhandigd, dan wordt er, na een identiteitscontrole van de aanvrager, onmiddellijk gevolg aan gegeven. Wordt de aanvraag per post verzonden, dan wordt er binnen de vijftien dagen geantwoord.

De informatie moet schriftelijk worden meegedeeld en het document moet op nauwkeurige en bevattelijke wijze alle gegevens over de betrokken persoon vermelden. Het moet een aantal verplichte vermeldingen bevatten en draagt de titel "uittreksel uit het bevolkingsregister/vreemdelingenregister afgegeven met toepassing van het koninklijk besluit van 16 juli 1992 betreffende het recht van toegang tot de registers".

Naast het recht op toegang bestaat er ook nog een recht op verbetering. Onnauwkeurige, onvolledige, onjuiste of overbodige gegevens geven aanleiding tot verbetering van de registers. De gemotiveerde aanvraag tot verbetering moet schriftelijk en met toevoeging van de bewijselementen door de geregistreerde worden ingediend. Dit kan alleen met een ter post aangetekende brief.

Niettegenstaande het feit dat in het Rijksregister niet meer of andere persoonsgegevens dan in de bevolkingsregisters worden bewaard, geldt voor beide bestanden afzonderlijke rechten op toegang en tot verbetering. De modaliteiten voor de uitoefening van deze rechten ten aanzien van het Rijksregister zijn vervat in het koninklijk besluit van 3 april 1984. Zij zijn in ruime mate gelijklopend aan de hiervoren besproken modaliteiten van het K.B. van 16 juli 1992 inzake dezelfde rechten m.b.t. de bevolkingsregisters. Waarom er twee verschillende besluiten moeten zijn, is niet duidelijk, temeer daar de uitoefening van de in de Rijksregisterwet toegekende rechten gebeurt bij de gemeente waar de geregistreerde in de bevolkingsregisters is ingeschreven. Weliswaar wordt het document dat wordt verstrekt in antwoord op de uitoefening van het recht op mededeling of verbetering afgeleverd door het Rijksregister en niet door de gemeente, maar het wordt wel ondertekend namens het college van burgemeester en schepenen. Het naast elkaar bestaan van deze twee besluiten werkt verwarring in de hand, en is overbodig. Ook de relatie tussen de zopas besproken wetgeving betreffende de bevolkingsregisters enerzijds, en de algemene Wet Verwerking Persoonsgegevens van 8 december 1992 anderzijds, is zeer onduidelijk⁶⁶.

⁶⁶ Zie verder de uitstekende analyse van Marc Taeymans, "Privacybescherming en de bevolkingsregisters", die binnenkort wordt gepubliceerd in DUMORTIER, J. en ROBBEN, F. (ed.), Persoonsgegevens en privacybescherming. Commentaar op de wet tot bescherming van de persoonlijke levenssfeer, Brugge, Die Keure, in druk. Het voorgaande onderdeel is in ruime mate op deze bijdrage gesteund.

6. DE WET VERWERKING PERSOONSGEGEVENS VAN 8 DECEMBER 1992

6.1. INLEIDING

Sedert 8 december 1992 beschikt België over een algemene wet ter bescherming van de persoonlijke levenssfeer ten aanzien van de verwerking van persoonsgegevens⁶⁷. Zoals hoger beschreven werden voordien weliswaar reeds gegevensbeschermende bepalingen ingeschreven in specifieke wetten m.b.t. bepaalde (soorten van) verwerkingen, maar een regeling met algemene draagwijdte heeft geruime tijd op zich laten wachten.

Ook de wet van 8 december 1992 heeft evenwel een beperkte werkingssfeer. Zij bevat enkel regelen ter waarborging van de privacybescherming bij de verwerking van persoonsgegevens. Andere aspecten van de bescherming van de persoonlijke levenssfeer, zoals het af luisteren en bespieden, de privacybescherming op de arbeidsplaats, ... komen in se in deze wet niet aan bod. Daarom wordt ook voorgesteld de wet af te korten als "Wet Verwerking Persoonsgegevens (WVP)" eerder dan als "Wet Bescherming Persoonlijke Levenssfeer" of "Privacywet".

Zoals omzeggens alle wetten die gedurende de laatste twee decennia inzake de bescherming van de persoonlijke levenssfeer t.a.v. de verwerking van persoonsgegevens zijn uitgevaardigd, volgt ook de Belgische wet het vierledig stamien dat voor het eerst in het Datenschutzgesetz van de Duitse deelstaat Hessen dd. 7 oktober 1970 werd gepropageerd. Vooreerst worden aan de houders van de persoonsgegevens een reeks verplichtingen opgelegd m.b.t. de kwaliteitseisen waaraan deze moeten voldoen en beperkingen m.b.t. het gebruik dat ervan mag worden gemaakt. Ten tweede wordt aan de geregistreerde personen het recht toegekend op eerbiediging van hun persoonlijke levenssfeer en op medezeggenschap over hun gegevens. Ten derde wordt een onafhankelijk toezienend orgaan, de Commissie voor de Bescherming van de Persoonlijke Levenssfeer (CBPL), in het leven geroepen. En tenslotte worden strafmaatregelen voorzien bij de schending van de wettelijke normen.

Na een beschrijving van het toepassingsgebied van de wet, wordt wat volgt overeenkomstig het vermelde stamien gestructureerd. Gelet op het beperkte bestek, blijft één en ander beperkt tot een gebalde beschrijving van de wet en de reeds uitgevaardigde uitvoeringsbesluiten. Voor een meer uitvoerige commentaar zij verwezen naar andere (op til staande) publicaties⁶⁸.

⁶⁷ B.S., 18 maart 1993, 5801, gewijzigd bij wet van 22 juli 1993, B.S., 24 juli 1993 en bij wet van 30 juni 1994, B.S., 18 augustus 1994, 20839.

⁶⁸ Zie bijvoorbeeld BOULANGER, M., DE TERWANGHE, C. en LEONARD, T., "La protection de la vie privée à l'égard des traitements de données à caractère personnel. La loi du 8 décembre 1992", Journal des Tribunaux, 1993, 369-388; CENTRUM VOOR INTERNATIONAAL STRAFRECHT VAN DE VRIJE UNIVERSITEIT BRUSSEL, "De Belgische privacy-wetgeving, een eerste analyse", Rechtskundig Weekblad, 1992-1993, 1146-1154; DUMORTIER, J., "De privacywet onder de loep" in Handboek Informatiebeveiliging, deel wettelijke aspecten - België, Diegem, Kluwer Editorial, losbladig, 1-54; DUMORTIER, J. en ROBBEN, F. (ed.), Persoonsgegevens en privacybescherming. Commentaar op de wet tot bescherming van de persoonlijke levenssfeer, Brugge, Die Keure, in druk.

6.2. TOEPASSINGSGEBIED

6.2.1. Toepassingsgebied *ratione materiae*

De rechten en verplichtingen vervat in de wet hebben tot doel de persoonlijke levenssfeer te beschermen ten opzichte van de verwerking van persoonsgegevens.

6.2.1.1. Persoonsgegevens

Persoonsgegevens zijn "gegevens die betrekking hebben op een natuurlijke persoon die is of kan worden geïdentificeerd" (artikel 1 § 5 WVP).

Het begrip "gegeven" wordt in de wet niet gedefinieerd. Uit de besprekingen in de Senaatscommissie⁶⁹ blijkt evenwel dat de term "gegeven" een zeer ruime betekenis heeft, en niet enkel slaat op teksten; ook foto's, video- en filmbeelden, klankopnames en vingerafdrukken bevatten gegevens in de zin van de wet. Observatiesystemen die dergelijke gegevens registreren en opslaan, vallen dan ook onder de toepassing van de wet, indien aan de andere toepassingsvoorwaarden voldaan is.

Enkel gegevens die betrekking hebben op een natuurlijk persoon zijn persoonsgegevens in de zin van de wet. Gegevens betreffende rechtspersonen zijn dus geen persoonsgegevens⁷⁰.

De wet vergt niet dat de natuurlijke persoon waarop het gegeven betrekking heeft (nog of al) in leven is. Ook gegevens m.b.t. al overleden personen dienen m.i. als persoonsgegevens te worden beschouwd, op voorwaarde dat het overlijden min of meer recent is⁷¹. De natuurlijke persoon waarop het gegeven betrekking heeft moet geïdentificeerd of minstens identificeerbaar zijn.

Naar analogie met de commentaar bij het verdrag nr. 108 van de Raad van Europa en de Nederlandse wet mag worden aangenomen dat een natuurlijk persoon niet als identificeerbaar

⁶⁹ Gedr. St., Senaat, B.Z. 1991-1992, 445-2, 57.

⁷⁰ De definitie van "persoonsgegevens" in de wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens is dus niet identiek aan deze vervat in de wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid (B.S., 22 februari 1990, 3288). De gegevensbeschermende bepalingen vervat in deze laatste wet zijn ook van toepassing op gegevens betreffende geïdentificeerde of identificeerbare rechtspersonen of feitelijke verenigingen (zie artikel 2, eerste lid).

⁷¹ In dezelfde zin, DUMORTIER, J., "Privacybescherming en gegevensverwerking. Aantekeningen bij de wet tot bescherming van de persoonlijke levenssfeer t.o.v. de verwerking van persoonsgegevens", Vlaams Jurist Vandaag, 1993, 7.

wordt beschouwd wanneer het identificatieproces onredelijke inspanningen of kosten vergt in verhouding tot het nut ervan⁷².

Het feit dat een gegeven, om als persoonsgegevens te worden gekwalificeerd, op een geïdentificeerd of identificeerbaar persoon betrekking dient te hebben, impliceert evenwel niet dat het persoonsgegevens op zich moet toelaten de betrokken persoon te identificeren. Het volstaat dat het gegeven met een bepaalde of een bepaalbare persoon in verband kan worden gebracht.

6.2.1.2. Verwerking

Uit artikel 1 § 1 WVP blijkt dat 2 soorten van verwerkingen worden onderscheiden: enerzijds "de geautomatiseerde verwerking" en anderzijds "het houden van een manueel bestand". De beschermingsregeling is in beginsel van toepassing op beide soorten verwerkingen, zij het dat bepaalde regelen (bijvoorbeeld de verplichting tot voorafgaande aangifte van de verwerking bij de CBPL) slechts gelden voor de eerste soort verwerkingen. In dat licht is dus een duidelijk onderscheid tussen beide categorieën noodzakelijk.

6.2.1.2.1. Geautomatiseerde verwerking

Een "geautomatiseerde verwerking" wordt in artikel 1 § 3 WVP omschreven als "elk geheel van bewerkingen die geheel of gedeeltelijk langs geautomatiseerde weg zijn uitgevoerd en betrekking hebben op de registratie en de bewaring van persoonsgegevens, alsook op de wijziging, de uitwissing, de raadpleging of de verspreiding van deze gegevens".

Een verwerking wordt aldus beschouwd als een geheel van specifieke bewerkingen, die verschillend van aard kunnen zijn. Belangrijk is te weten wanneer er sprake is van één dan wel van meerdere verwerkingen. Eén en ander is belangrijk in het licht van de aangifteplicht vervat in artikel 17 WVP (per verwerking dient een aangifte gedaan en een vergoeding betaald), van de mogelijkheid tot vrijstelling van aangifte overeenkomstig artikel 17 § 8 WVP (slechts wanneer een verwerking geen andere doeleinden dient of gegevens bevat dan deze opgesomd in het vrijstellende besluit, zal geen aangifte moeten worden gedaan), de plicht tot mededeling van wijzigingen aan vroegere aangiften (artikel 17 § 7 WVP) en de beoordeling van de naleving van het doelmatigheidsbeginsel (naarmate de beoogde doelstellingen specifiek zijn, zullen de verwerkte gegevens allicht minder snel als overmatig en sneller als ter zake dienend kunnen worden beschouwd).

Uit twee adviezen⁷³ die de CBPL uitbracht m.b.t. de wet, toen deze nog in ontwerpvorm was,

⁷² CONSEIL D'EUROPE, Rapport explicatif concernant la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, 1981, 14, nr. 28; Regels ter bescherming van de persoonlijke levenssfeer in verband met persoonsregistraties (Wet persoonsregistraties), Memorie van Toelichting, Tweede Kamer, vergaderjaar 1984-1985, 19095, nr. 3, 35.

⁷³ Zie Gedr. St., Kamer, B.Z. 1991-1992, 413/12, 80-81 en Gedr. St., Senaat, B.Z. 1991-1992, 445-2,

kan worden afgeleid dat een reeks bewerkingen als één verwerking worden beschouwd indien ze als een samenhangend geheel met één generiek doel worden uitgevoerd. De technische of ruimtelijke organisatie van de verwerking (zoals de opdeling in computerprogramma's, de al dan niet volledige automatisering ervan, de opsplitsing tussen verschillende fysieke locaties, ...) zijn dus niet relevant⁷⁴, maar wel de gemeenschappelijke generieke doelstelling.

In navolging van de rechtsleer⁷⁵ en een advies van de Raad van State⁷⁶, werd in het verslag aan de Koning bij het in uitvoering van artikel 17 WVP genomen koninklijk besluit nr. 12 bovendien duidelijk gepreciseerd dat elke verwerking slechts één generieke doelstelling kan hebben⁷⁷. Indien dezelfde persoonsgegevens worden verwerkt voor meerdere generieke doelstellingen, maken ze dus deel uit van verschillende verwerkingen.

Blijft dan de vraag wat als één generieke doelstelling kan worden beschouwd. Nuttig in dat verband is het lexicon van generieke doelstellingen dat door de CBPL werd uitgewerkt, en dat werd gepubliceerd in bijlage bij het hoger vermelde koninklijk besluit nr. 12⁷⁸. In dat lexicon worden een aantal veel voorkomende doeleinden omschreven. Deze definities kunnen een leidraad vormen bij het bepalen van het niveau van precisie waarmee de beschrijving van de doelstellingen in het algemeen dient te gebeuren, en dus van de criteria om een onderscheid te maken tussen verwerkingen.

Om van een geautomatiseerde verwerking te kunnen gewagen, is krachtens de bovenvermelde wettelijke definitie niet vereist dat alle bewerkingen die daarvan deel uitmaken, op geautomatiseerde wijze geschieden. Het volstaat dat een deel ervan geautomatiseerd gebeurt.

121.

⁷⁴ In heel wat gevallen zal één geautomatiseerde verwerking in de zin van de wet aldus in realiteit overeenkomen met een reeks van toepassingen en bestanden. In dezelfde zin BOULANGER, M., DE TERWANGHE, C. en LEONARD, T., Lc., 1993, 372.

⁷⁵ Zie bijvoorbeeld GUTWIRTH, S., "De toepassing van het finaliteitsbeginsel van de privacywet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer t.a.v. de verwerking van persoonsgegevens", T.P.R., 1994, 1409-1477; DUMORTIER, J. en ROBBEN, F., "Relatiebankieren en de finaliteitsregel van artikel 5 WVP", Computerrecht, 1994, 247-250.

⁷⁶ Advies van de Raad van State m.b.t. het ontwerp van koninklijk besluit nr. 12 tot vaststelling van de bedragen die aan de Commissie voor de bescherming van de persoonlijke levenssfeer moeten worden gestort bij de aangifte van verwerkingen van persoonsgegevens, B.S., 14 maart 1995, 5663.

⁷⁷ Verslag aan de Koning m.b.t. het koninklijk besluit nr. 12 tot vaststelling van de bedragen die aan de Commissie voor de bescherming van de persoonlijke levenssfeer moeten worden gestort bij de aangifte van verwerkingen van persoonsgegevens, B.S., 14 maart 1995, 5661.

⁷⁸ Zie B.S., 14 maart 1995, 5689.

Gezien de bewaring op zich als bewerking wordt beschouwd, is het niet van belang of de gegevens daadwerkelijk worden gebruikt. Voldoende is dat de gegevens voor geautomatiseerde bewerkingen beschikbaar worden gehouden of de mogelijkheid daartoe bestaat.

Om persoonsgegevens op geautomatiseerde wijze te bewaren, te wijzigen, uit te wissen, te raadplegen of te verspreiden, moeten deze, althans gedeeltelijk, op een automatisch toegankelijke drager beschikbaar zijn⁷⁹. Dat een elektronische drager automatisch toegankelijk is, lijdt geen twijfel. Of bijvoorbeeld micro-fiches of papieren steekkaarten automatisch toegankelijk zijn, hangt af van de automatische bewerkingsmiddelen die de gebruiker ter beschikking heeft. Op geautomatiseerde wijze betekent echter zeker niet zonder meer computerondersteund, maar doelt op alle technieken waarbij één of meerdere bewerkingen niet rechtstreeks door de menselijke hand worden gestuurd⁸⁰.

In de lijst van bewerkingen komt naast de bewaring, wijziging, uitwissing, raadpleging of verspreiding van persoonsgegevens, evenwel ook de registratie voor. Naar de letter van de wet zou de loutere geautomatiseerde registratie van persoonsgegevens, die nadien niet op automatisch toegankelijke dragers worden bewaard, dan ook als geautomatiseerde verwerking kunnen worden beschouwd. Men denke bijvoorbeeld aan het gebruik van een tekstverwerker voor het aanmaken van teksten, die nadien enkel op papier worden bewaard⁸¹. Allicht heeft de wetgever dit niet bedoeld.

Bemerk tenslotte dat de inzameling van gegevens op zich niet als verwerking wordt beschouwd.

6.2.1.2.2. *Houden van een manueel bestand*

Het "houden van een manueel bestand" wordt in artikel 1 § 4 WVP omschreven als "de registratie, de bewaring, de wijziging, de uitwissing, de raadpleging of de verspreiding van persoonsgegevens in de vorm van een bestand op een niet-geautomatiseerde drager".

Het begrip "houden van een manueel bestand" vormt dus een soort restcategorie. Zodra persoonsgegevens worden bewaard in de vorm van een bestand, zonder dat het bijhouden op een automatisch toegankelijke drager geschiedt en zonder dat een (deel van) de bewerkingen die op de gegevens worden toegepast, op geautomatiseerde wijze geschieden, is er sprake van het houden van een manueel bestand.

⁷⁹ Indien een bestand op een niet-automatisch toegankelijke drager wordt bewaard, is er sprake van het houden van een manueel bestand (artikel 1, § 4).

⁸⁰ GEERTS, G., HEESTERMANS, H., Van Dale Groot Woordenboek van de Nederlandse Taal, Van Dale Lexicografie, 1984, 221.

⁸¹ DUMORTIER, J., Lc., 1993, 8.

Om van een "bestand" te kunnen gewagen, moet het gaan om "een geheel van persoonsgegevens (...), samengesteld en bewaard op een logisch gestructureerde wijze (structuur die is ingevoerd, FR) met het oog op een systematische raadpleging ervan" (artikel 1 § 2 WVP).

Niet-automatisch toegankelijke gegevensverzamelingen zonder logische structuur vallen dus niet onder de wet. Als voorbeeld van een ongeordende gegevensverzameling, die aldus niet als bestand wordt beschouwd in de zin van de wet, wordt in de commentaar van de artikelen in eerste instantie een niet-automatisch toegankelijke dossierverzameling vermeld die louter alfabetisch of rekenkundig is gerangschikt⁸². A fortiori zal een enkelvoudig papieren dossier, met losse aantekeningen en min of meer chronologisch gerangschikte documenten van velerlei aard niet aan de vereiste van systematische toegankelijkheid voldoen. Anders wordt het wanneer de houder van een dossierverzameling per dossier exact weet welke persoonsgegevens hij waar kan terugvinden, omdat de dossiers volgens een vaste structuur zijn georganiseerd, of als er sprake is van een al dan niet geautomatiseerde index. In geval dergelijk verwijzingsbestand bestaat, dient de controle van de CBPL overigens ook te worden uitgebreid tot de corresponderende dossiers om de juistheid en de pertinentie van gegevens in het verwijzingsbestand te kunnen nagaan⁸³.

Verdere, nog relevante voorbeelden uit de commentaar van de artikelen van gegevensverzamelingen die niet als bestand worden beschouwd, zijn boeken en andere schriftelijke publicaties zoals telefoonboeken.

In de praktijk zijn in elk geval heel wat interpretatiemoeilijkheden te verwachten bij de vaststelling of een bepaalde, niet-geautomatiseerde gegevensverzameling al dan niet voldoende gestructureerd is om als bestand in de zin van de wet te worden beschouwd⁸⁴.

6.2.1.3. Uitsluitingen

Niet elke verwerking van persoonsgegevens die aan hogervermelde voorwaarden voldoet, valt echter binnen het bereik van de wet. Artikel 3 § 2 WVP sluit een aantal soorten verwerkingen uit.

6.2.1.3.1. Privé-verwerkingen

Dit is in de eerste plaats het geval voor verwerkingen van persoonsgegevens beheerd door

⁸² Gedr. St., Kamer, 1990-91, 1610/1, 5. De vereiste van de niet-automatische toegankelijkheid van de dossierverzameling is in de commentaar van de artikelen niet terug te vinden, gezien in het Regeringsontwerp ook voor geautomatiseerde verwerkingen de bestandsvormvereiste gold. Deze vereiste werd echter tijdens de parlementaire behandeling geschrapt voor geautomatiseerde verwerkingen.

⁸³ Gedr. St., Kamer, B.Z. 1991-1992, 413/12, 16.

⁸⁴ Over de moeilijkheden waartoe een gelijkaardige bepaling uit de Franse wet geleid heeft, zie de literatuur vermeld in BOULANGER, M., DE TERWANGHE, C. en LEONARD, T., Le, 1993, 372, voetnoot 21.

natuurlijke personen die wegens hun aard bestemd zijn voor privé-, gezins- of huishoudelijk gebruik, en die bestemming behouden (artikel 3 § 2, 1° WVP).

Luidens de commentaar van de artikelen⁸⁵ wordt het als buitensporig ervaren, uit naam van de bescherming van de persoonlijke levenssfeer een reglementering uit te vaardigen die ook van toepassing zou zijn op al dan niet geautomatiseerde verwerkingen van persoonsgegevens voor louter privé-doeleinden door een natuurlijk persoon. Hierbij worden voorbeelden gegeven zoals adressenboekjes, agenda's, enz., ongeacht of deze op papier worden bijgehouden of bijvoorbeeld op een huiscomputer.

Wel wordt een zeer stricte driedubbele vereiste gesteld. Vooreerst dienen de verwerkte persoonsgegevens te worden beheerd door een natuurlijk persoon. Verwerkingen van persoonsgegevens beheerd door feitelijke verenigingen of rechtspersonen vallen dus in geen geval onder de uitsluiting.

Bovendien moeten de verwerkte persoonsgegevens omwille van hun aard bestemd zijn voor louter privé-, gezins- of huishoudelijke doeleinden. Persoonsgegevens die door een werknemer thuis worden verwerkt voor zijn bedrijf (zoals adressen van zakenrelaties, klanten of medewerkers), examenresultaten bewaard door een leraar of parochieregisters bijgehouden door een pastoor zijn niet bestemd voor privé-doeleinden; het verwerken van een ledenlijst van een kleine voetbalclub zou volgens de Minister van Justitie wel onder de uitzondering kunnen vallen⁸⁶.

Tenslotte moet de verwerking haar privé-, gezins- of huishoudelijke bestemming bewaren. Gezien in de wet wordt verwezen naar de bestemming van de verwerking, en niet naar het effectieve gebruik ervan, zal een louter toevallig of sporadisch aanwenden van de persoonsgegevens voor andere dan loutere privé-doeleinden (bijvoorbeeld het eenmalig versturen aan vrienden van uitnodigingen voor een bedrijfsactiviteit) m.i. geen toepasselijkheid van de reglementering met zich brengen. Anders wordt het uiteraard wanneer dergelijk gebruik systematisch geschiedt, zodat mag worden vermoed dat de verwerking voortaan ook met deze bestemming wordt verricht.

6.2.1.3.2. Verwerkingen van openbare gegevens

De beschermingsregeling is evenmin toepasselijk indien alle verwerkte persoonsgegevens als openbaar worden beschouwd, hetzij omdat ze onder een wettelijk of reglementair voorschrift tot openbaarmaking vallen (artikel 3 § 2, 2° WVP) hetzij omdat de betrokkene zelf de openbaarmaking verricht of doet verrichten (artikel 3 § 2, 3° WVP). In dat laatste geval valt de verwerking evenwel slechts buiten de toepassing van de wet voorzover de verwerking de finaliteit van de openbaarmaking eerbiedigt.

⁸⁵ Gedr. St., Kamer, 1990-91, 1610/1, 7.

⁸⁶ Gedr. St., Kamer, B.Z. 1991-1992, 413/12, 22-23.

Onder een wettelijke verplichting van openbaarmaking vallen bijvoorbeeld de gegevens opgenomen in openbare registers (handelsregister, hypotheekregister, ...) of gegevens die dienen te worden gepubliceerd in het Belgisch Staatsblad of zijn bijlagen (benoemingen en ontslagen in de overheidssector en in vennootschappen, onbekwaamverklaringen, ...).

Openbaarmaking door of op vraag van de betrokkene impliceert diens uitdrukkelijke wil tot het openbaren van de gegevens. In de commentaar van de artikelen wordt het voorbeeld gegeven van handelsreclame; tijdens de parlementaire bespreking werd ook verwezen naar geboortekaartjes of huwelijksberichten⁸⁷. Het loutere feit dat bepaalde persoonsgegevens kunnen worden afgeleid door bepaalde openbare gedragingen van een persoon te observeren, impliceert dus geenszins dat de verwerking van deze gegevens niet zou zijn onderworpen aan de beschermingsregeling. Openbaren betekent bovendien publiek maken. Een mededeling tijdens een privé-gesprek of een sollicitatie-interview is dus geen openbaarmaking in de zin van deze bepaling⁸⁸.

Er weze tenslotte vermeld dat de uitsluiting uit het toepassingsgebied van de wet slechts geldt in de mate dat alle verwerkte persoonsgegevens als openbaar kunnen worden beschouwd. Indien aldus ook andere gegevens worden verwerkt, herwint de wet haar toepassing.

6.2.1.3.3. Verwerkingen in uitvoering van de wet op de openbare statistiek

Tenslotte is de beschermingsregeling niet van toepassing op verwerkingen verricht in uitvoering van de wet op de openbare statistiek, met uitzondering van de mededeling van statistieken waaruit persoonsgegevens kunnen worden afgeleid⁸⁹ (artikel 3 § 2, 4° WVP).

Inmiddels werd echter in de Statistiekwet in december 1994 een nieuw artikel 2bis ingevoegd, dat stelt dat "de gegevens die het Nationaal Instituut voor de Statistiek in zijn bezit heeft voor zuiver statistische doeleinden, hetzij rechtstreeks ingezameld bij de aangevers krachtens de artikelen 1, 5, 9, 10 en 12 van deze wet, hetzij onrechtstreeks uit administratieve bestanden krachtens artikel 24bis, worden geregeld en beschermd door de Statistiekwet, ongeacht alle andersluidende wettelijke bepalingen". Krachtens de commentaar van de artikelen is het de uitdrukkelijke bedoeling van deze bepaling om alle informatie die door het Nationaal Instituut voor de Statistiek wordt verwerkt voor statistische doeleinden te onttrekken aan het toepassingsgebied van de Wet Verwerking Persoonsgegevens. Dit wordt gemotiveerd door het feit dat de beschermingsregeling van de Statistiekwet geacht wordt evenwaardig te zijn aan deze vervat in

⁸⁷ Gedr. St., Kamer, B.Z. 1991-1992, 413/12, 26.

⁸⁸ DUMORTIER, J., Lc., 1993, 9.

⁸⁹ Zie artikel 2, c, tweede lid van de wet van 4 juli 1962 betreffende de openbare statistiek, en de artikelen die daarnaar verwijzen.

de Wet Verwerking Persoonsgegevens⁹⁰. Deze motivatie is echter onjuist, gezien essentiële principes zoals de verplichting tot naleving van het finaliteitsbeginsel, het toekennen van een inzage-recht aan de betrokkene of het respecteren van een aantal veiligheidsverplichtingen door de houder van de verwerking, in de Statistiekwet niet vermeld staan. Het is dan ook niet verwonderlijk dat de CBPL recentelijk heeft gereageerd tegen het nieuwe artikel 2bis van de Statistiekwet, althans in de mate dat het betrekking heeft op verwerkingen van persoonsgegevens. De CBPL acht het betrokken artikel strijdig met het door België geratificeerde verdrag nr. 108 van de Raad van Europa.

6.2.1.3.4. Verwerkingen noodzakelijk voor de toepassing van de wet tot voorkoming van het witwassen van geld

Bepaalde artikelen⁹¹ van de wet zijn niet van toepassing op verwerkingen van persoonsgegevens die noodzakelijk zijn voor de toepassing van de wet van 11 januari 1993 tot voorkoming van het financiële stelsel voor het witwassen van geld. Deze wet, die uitvoering geeft aan een Europese richtlijn van de Raad van 1991, verplicht een aantal opgesomde financiële ondernemingen om tot minstens 5 jaar na het beëindigen van de relatie met de betrokkene, bepaalde identificatiegegevens (naam, voornaam, adres of maatschappelijke zetel) en -stukken bij te houden van elkeen die een verrichting wenst uit te voeren, die een bepaald bedrag overschijdt, of waarvan wordt vermoed dat het gaat om witwassen van geld. Ook wordt een Cel voor financiële informatieverwerking opgericht als administratieve autoriteit met rechtspersoonlijkheid onder het toezicht van de Ministers van Justitie en Financiën, die o.a. is belast met de verwerking en ontleding van de informatie die haar in bepaalde omstandigheden door de financiële ondernemingen wordt overgemaakt. Zowel de verwerkingen van de financiële ondernemingen als deze van de Cel voor financiële informatieverwerking worden onttrokken aan een aantal bepalingen van de Wet Verwerking Persoonsgegevens, uiteraard voorzover zij enkel het doeleinde "voorkomen of opsporen van witwassen van geld" dienen.

6.2.2. Toepassingsgebied *ratione personae*

De vraag op wie gegevens betrekking moeten hebben opdat de beschermingsregeling toepasbaar zou zijn, werd reeds hoger behandeld en komt hier niet opnieuw aan de orde. Wel wordt getracht aan te geven wie de verplichtingen vervat in de beschermingsregeling dient na te leven wanneer hij persoonsgegevens verwerkt in de zin van de wet.

De beschermingsregeling is van toepassing ongeacht of de instantie die de gegevens verwerkt een natuurlijke persoon, een rechtspersoon of een feitelijke vereniging is. Evenmin wordt

⁹⁰ Gedr. St., Senaat, 1994-1995, 1218-1, 53.

⁹¹ Het betreft de verplichting tot informatie van de betrokkene bij de inzameling van gegevens en bij de eerste registratie in een bestand en de mogelijkheid tot rechtstreekse uitoefening van de rechten van toegang tot, en verbetering en niet-aanwending van gegevens bij de houder van een bestand.

onderscheid gemaakt naargelang de instantie die de gegevens verwerkt een privaat- of een publiekrechtelijk karakter heeft. Bepaalde regelen⁹² zijn evenwel niet van toepassing op verwerkingen verricht in het kader van de uitvoering van hun opdrachten door het Bestuur Veiligheid van de Staat van het Ministerie van Justitie of de Algemene Dienst Inlichting en Veiligheid van het Ministerie van Landsverdediging (zie artikel 3 § 3 WVP), ofschoon deze diensten als dusdanig niet worden uitgesloten uit de werkingssfeer van de wet. Ook openbare overheden belast met taken van gerechtelijke politie en bepaalde openbare overheden belast met taken van bestuurlijke politie worden van een aantal verplichtingen ontheven⁹³.

Om, ongeacht de concrete wijze van verwerking van persoonsgegevens, duidelijk aan te geven op wie de eindverantwoordelijkheid rust voor de naleving van de verplichtingen, wordt in artikel 1 §§ 6 en 7 WVP een belangrijk begrippenpaar gedefinieerd. Het betreft de noties "houder van het bestand" en "bewerker". Onder "houder van het bestand" wordt verstaan, "de natuurlijke persoon of de rechtspersoon of de feitelijke vereniging (...) die bevoegd is om te beslissen over het doel van de verwerking of over de soorten gegevens die erin moeten voorkomen. Indien het doel van de verwerking of de soorten gegevens die erin moeten voorkomen bij de wet zijn bepaald, is de houder van het bestand de natuurlijke persoon of de rechtspersoon die bij de wet is aangewezen om het bestand te houden. De houder van het bestand, natuurlijke persoon, die geen woonplaats in België heeft, moet, om toe te laten dat de rechten bedoeld in de artikelen 10 en 12 - recht op toegang, verbetering, verwijdering en niet-aanwending, FR - uitgeoefend worden, woonplaats in België kiezen. De houder van een bestand, rechtspersoon of feitelijke vereniging, waarvan de zetel zich in het buitenland bevindt, moet een vertegenwoordiger in België aanduiden bij wie de rechten bedoeld in de artikelen 10 en 12 kunnen uitgeoefend worden". De "bewerker" is "de natuurlijke persoon of de rechtspersoon of de feitelijke vereniging (...) aan wie de organisatie en de uitvoering van de verwerking worden toevertrouwd".

De eindverantwoordelijkheid omtrent de naleving van de verplichtingen vervat in de wet ligt bij de houder van het bestand.

Het begrip "houder van een bestand" is aldus functioneel van aard: het verwijst naar de instantie die de bevoegdheid heeft om te beslissen over het doel van een verwerking of de soorten te verwerken gegevens. Indien niet dezelfde instantie bevoegd is om te beslissen over het doel van de verwerking en over de soorten te verwerken gegevens, lijkt de voorkeur te moeten worden gegeven aan de instantie die het doel bepaalt⁹⁴.

⁹² Het betreft de bepalingen i.v.m. het recht op informatie bij gegevensinzameling en bij de eerste registratie in een bestand, de bijzondere beschermingsregelen voor gevoelige gegevens, de rechtstreekse uitoefening van de rechten van toegang, verbetering en niet-aanwending bij de houder van een bestand, het recht op verhaal bij de rechter en bij de CBPL en de verplichting tot voorafgaande aangifte van geautomatiseerde gegevensverwerking.

⁹³ Het betreft de verplichting tot informatie van de betrokkene bij de inzameling van gegevens en bij de eerste registratie in een bestand en de mogelijkheid tot rechtstreekse uitoefening van de rechten van toegang tot, en verbetering en niet-aanwending van gegevens bij de houder van een bestand.

⁹⁴ In dezelfde zin, CENTRUM VOOR INTERNATIONAAL STRAFRECHT VAN DE VRIJE UNIVERSITEIT BRUSSEL, *Le*, 1992-1993, 1147.

Zoals reeds tijdens de parlementaire bespreking van de wet werd opgemerkt⁹⁵, is de uitdrukking "houder van een bestand" eigenlijk slecht gekozen. Vooreerst is niet de term "bestand" het centrale begrip van de wet, maar wel "verwerking". Gezien in de definitie van een geautomatiseerde verwerking geen bestandsvorm wordt vereist, zullen er "houders van bestanden" zijn zonder bestand⁹⁶. Bovendien wordt met "houder" degene bedoeld die de beslissingsbevoegdheid heeft over een verwerking. Dit is evenwel niet noodzakelijk dezelfde instantie die de verwerking houdt, in de zin dat hij op de gegevens bewerkingen uitvoert. Het begrippenapparaat van de wet verdient aldus op dit vlak een aanpassing, bijvoorbeeld door het gebruik van een term als "verantwoordelijke voor de verwerking"⁹⁷.

De wet schrijft bewust niet dwingend voor waar men binnen een organisatie het houderschap dient te situeren, maar legt enkel de functionele criteria vast. Enkel wanneer het doel van een verwerking en de aard van de verwerkte gegevens bepaald worden bij wet, wordt uitdrukkelijk aangegeven dat de door de wet met de verwerking belaste instantie als houder dient te worden beschouwd.

In organisaties of ondernemingen, zal het houderschap zich meestal bij de organisatie of de onderneming als rechtspersoon of feitelijke vereniging situeren. Zij hebben de uiteindelijke beslissingsmacht over de verwerking. In elk geval heeft het uitbesteden of delegeren van het beheer van of de feitelijke omgang met de gegevens geen invloed op het houderschap. Ook de eventuele afsplitsing van de verantwoordelijkheid voor de inhoud van de gegevens is niet van aard om het houderschap te verleggen. Dit blijft berusten bij de instantie die de zeggenschap en de eindverantwoordelijkheid heeft over het geheel.

Is het doel van een verwerking en de aard van de verwerkte gegevens in de overheidssfeer niet wettelijk vastgelegd, zal doorgaans het betrokken overheidsorgaan (de gemeente, de provincie, de Minister, de parastatale, ...) of, onder diens verantwoordelijkheid, het hoofd van de betrokken dienst, als houder worden beschouwd, eerder dan het bestuur (gemeentebestuur, provinciebestuur, beheerscomité) van de betrokken instelling.

Een andere situatie is deze waarin verschillende verwerkingen geheel of gedeeltelijk zijn geïntegreerd, zonder dat daarbij één houder valt aan te wijzen. Mede afhankelijk van het doel en de aard van die verwerkingen en de wijze waarop de zeggenschap is geregeld, zal dan moeten

⁹⁵ Gedr. St., Kamer, 1990-1991, 1610/4, 2-3. Een amendement om de uitdrukking "houder van het bestand" te vervangen door "houder van de verwerking" werd door de Minister evenwel afgewezen met het m.i. weinig overtuigende argument dat de term "houder van het bestand" ook wordt gehanteerd in het verdrag nr. 108 van de Raad van Europa.

⁹⁶ DUMORTIER, J., Lc., 1993, 9.

⁹⁷ Ibid., 9.

worden besloten tot een afzonderlijk houderschap per deelverwerking of tot één globale verwerking met een gezamenlijk houderschap.

6.2.3. Toepassingsgebied *ratione loci*

De wet is van toepassing op "het houden van een manueel bestand in België" en "op elke geautomatiseerde verwerking, ook als de bewerkingen geheel of gedeeltelijk in het buitenland worden gedaan, maar die verwerking in België rechtstreeks toegankelijk is met behulp van middelen die aan de verwerking eigen zijn" (artikel 3 § 1 WVP).

Het ruimtelijke toepassingsgebied van de Belgische wet is dus, wat betreft geautomatiseerde verwerkingen, erg breed. De tekst van artikel 3 § 1, 2° is niet erg duidelijk omtrent de vraag of geautomatiseerde verwerkingen die fysisch (gedeeltelijk) op het Belgische grondgebied worden verricht, maar er niet rechtstreeks toegankelijk zijn, al dan niet onder de regeling vallen. Allicht was dit de bedoeling van de wetgever⁹⁸, maar hij had dit duidelijker kunnen aangeven.

Tijdens de parlementaire besprekingen werd gepreciseerd dat een verwerking rechtstreeks toegankelijk is met behulp van middelen die haar eigen zijn, zodra het systeem waarop de verwerking draait toegankelijk is zonder verder menselijk ingrijpen⁹⁹. In de commentaar van de artikelen wordt als voorbeeld de raadpleging van gegevens via een terminal gegeven¹⁰⁰.

Interactieve raadplegingen, via het telefoon- of een privaat netwerk, van elektronische verwerkingen van persoonsgegevens die in het buitenland worden beheerd, vallen dus zonder meer onder het toepassingsgebied van de wet. De vraag kan worden gesteld of de wet ook toepasselijk is wanneer via de terminal enkel een stapelverwerking in het buitenland kan worden opgestart, waarvan het resultaat achteraf op papier of via file transfer wordt meegedeeld, zonder dat de gebruiker van de terminal een interactieve toegang tot de gegevens bezit. M.i. valt dergelijke bewerking als dusdanig niet onder het toepassingsgebied van de wet, op voorwaarde dat het verkregen resultaat echter in België geen verdere bewerkingen ondergaat die onder het materiële toepassingsgebied ressorteren.

De informatieplicht van de betrokkene bij de inzameling van gegevens is toepasselijk zodra op het Belgische grondgebied persoonsgegevens worden ingezameld met het oog op een verwerking ervan, ongeacht de plaats waar de verwerking geschiedt (artikel 4 § 1 WVP).

⁹⁸ In dezelfde zin, BOULANGER, M., DE TERWANGHE, C. en LEONARD, T., *Lc.*, 1993, 375; CENTRUM VOOR INTERNATIONAAL STRAFRECHT VAN DE VRIJE UNIVERSITEIT BRUSSEL, *Lc.*, 1992-1993, 1148.

⁹⁹ *Gedr. St.*, Kamer, B.Z. 1991-1992, 413/12, 22.

¹⁰⁰ *Gedr. St.*, Kamer, 1990-1991, 1610/1, 6.

Tenslotte wordt het verbod tot inzameling van bepaalde gevoelige gegevens op het Belgische grondgebied verruimd tot de gevallen waarin dergelijke inzameling geschiedt met het oog op een verwerking in het buitenland die in België zou zijn verboden (artikel 4 § 2 WVP).

6.2.4. Toepassingsgebied *ratione temporis*

Artikel 52 van de wet kent aan de Koning de bevoegdheid toe om enerzijds de datum van inwerkingtreding van de onderscheiden bepalingen van de wet vast te stellen, met als uiterste datum de eerste dag van de vierentwintigste maand¹⁰¹ na degene waarin de wet in het Belgisch Staatsblad is bekendgemaakt (in casu dus 1 maart 1995), en anderzijds te bepalen binnen welke termijn de verwerkingen die bestaan op het ogenblik van inwerkingtreding in overeenstemming moeten zijn gebracht met de wetsbepalingen.

Eén en ander geschiedde door middel van twee koninklijke besluiten, uitgevaardigd op 28 februari 1993¹⁰². Het eerste besluit werd sindsdien reeds twee maal gewijzigd¹⁰³ omdat de oorspronkelijk voorziene datum van inwerkingtreding van een aantal bepalingen niet kon worden aangehouden bij gebrek aan uitvaardiging van de nodige uitvoeringsbesluiten.

Gezien enerzijds werd geopteerd voor een gefaseerde inwerkingtreding van de verschillende bepalingen, en anderzijds 3 soorten termijnen worden ingesteld voor de inregelstelling van bestaande verwerkingen, zijn niet minder dan 10 tijdstippen relevant voor degenen die de wet dienen toe te passen of er rechten aan ontlenen. Al bij al niet erg eenvoudig dus voor de houders van bestanden om te weten wanneer zij welke verplichtingen moeten naleven, en voor de personen waarover gegevens worden verwerkt om uit te maken vanaf wanneer zij welke rechten kunnen laten gelden.

¹⁰¹ Oorspronkelijk moesten alle bepalingen uiterlijk de eerste dag van de achttiende maand na deze van de publicatie van de wet in het Belgisch Staatsblad in werking zijn getreden, maar omdat een aantal belangrijke uitvoeringsbesluiten op zich lieten wachten, werd dit tijdstip 6 maanden verlaat bij het enig artikel van de wet van 30 juni 1994 houdende wijziging van artikel 52 van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, B.S., 18 augustus 1994, 20839.

¹⁰² Het koninklijk besluit nr. 1 van 28 februari 1993 tot vaststelling van de datum van inwerkingtreding van de bepalingen van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, B.S., 18 maart 1993, 5816, gewijzigd bij koninklijk besluit nr. 6 van 13 september 1993, B.S., 25 september 1993, 21260 en bij koninklijk besluit nr. 11 van 14 maart 1994, B.S., 12 april 1994, 9649, en het koninklijk besluit nr. 2 van 28 februari 1993 tot vaststelling van de termijn binnen welke een houder van een bestand zich moet schikken naar de bepalingen van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens met betrekking tot de verwerkingen die op het tijdstip van de inwerkingtreding bestaan, B.S., 18 maart 1993, 5817.

¹⁰³ Zie de koninklijke besluiten nrs. 6 en 11 van respectievelijk 13 september 1993 en 14 maart 1994 tot wijziging van het koninklijk besluit nr. 1 van 28 februari 1993 tot vaststelling van de datum van inwerkingtreding van de bepalingen van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, B.S., 25 september 1993, 21260 en B.S., 12 april 1994, 9649.

Hoewel de meeste tijdstippen reeds zijn verstreken, en omzeggens alle bepalingen van de Wet Verwerking Persoonsgegevens dus reeds in werking zijn getreden, volgt hieronder toch een overzicht in tabelvorm. Enerzijds omdat een tweetal data nog in de (nabije) toekomst gesitueerd zijn, en anderzijds omdat een volledig overzicht van het toepassingsgebied *ratione temporis* sowieso relevant is bij eventuele betwistingen m.b.t. de Wet Verwerking Persoonsgegevens omtrent feiten uit het verleden.

Om eenduidig te kunnen vaststellen vanaf wanneer welke verplichtingen gelden of rechten kunnen worden afgedwongen, dient echter kort te worden stilgestaan bij de vraag wanneer een verwerking "nieuw" is, in de zin dat de overgangsregeling geldend voor "bestaande" verwerkingen niet van toepassing is.

Wanneer een persoon of vereniging überhaupt slechts persoonsgegevens begint te verwerken na de datum van inwerkingtreding van een welbepaald artikel van de wet, stelt zich uiteraard geen probleem. De verwerking zal niet als een bestaande verwerking kunnen worden beschouwd, en de overgangsregeling is dus niet van toepassing. De voorschriften van de wet die vóór het opstarten van de verwerking reeds in werking zijn getreden, moeten onmiddellijk worden nageleefd.

Problemen kunnen zich evenwel stellen met verwerkingen die reeds bestaan op het ogenblik van de inwerkingtreding van een bepaald artikel waarvoor een overgangstermijn is voorzien, en die korte tijd nadien aan wijzigingen onderhevig zijn, zoals een uitbreiding van de verwerkte gegevens, van het soort uitgevoerde bewerkingen of van het doel van de verwerking. Ontstaat door deze aanpassingen dan een nieuwe verwerking, waarop de reeds in werking getreden bepalingen onmiddellijk van toepassing zijn, en waarvoor geen beroep meer kan worden gedaan op de overgangsregeling ?

Vooraf weze duidelijk gesteld dat de inhoudelijke relevantie van de vraag relatief beperkt is: hoogstens worden een aantal verplichtingen 9 maanden later van kracht. Niettemin kan de niet-tijdige naleving van bepaalde verplichtingen aanleiding geven tot vrij strenge strafsancities, zodat de praktische gevolgen van een verkeerde beoordeling van de nieuwigheidsgraad van een verwerking aanzienlijk kunnen zijn.

De vraag naar het onderscheid tussen een nieuwe en een bestaande verwerking hangt samen met de meer fundamentele, hoger besproken kwestie, die erin bestaat te weten wanneer er in de zin van de wet dient te worden gesproken over één, dan wel over meerdere verwerkingen. Hoe ruimer het begrip verwerking wordt geïnterpreteerd, hoe minder snel er immers bij de aanpassing van een verwerking sprake zal zijn van een nieuwe verwerking.

Op basis van de standpunten m.b.t. deze problematiek ingenomen door de Commissie voor de Bescherming van de Persoonlijke Levenssfeer in twee adviezen die ze uitbracht m.b.t. de wet,

toen deze nog in ontwerpvorm was¹⁰⁴, mag worden aangenomen dat wanneer de aangebrachte aanpassingen relatief onaanzienlijk zijn en volledig in de lijn liggen van het generieke doel van de bestaande verwerking, geen sprake is van een nieuwe verwerking. Leiden de wijzigingen van een verwerking tot een verandering in het doeleinde of zijn ze fundamenteel, is het voorzichtig de verwerking als een nieuwe verwerking te beschouwen.

Hieronder wordt in een samenvattende tijdstabel een schematisch overzicht geboden van de data vanaf wanneer de onderscheiden bepalingen concreet dienen te worden nageleefd. Voor de duidelijkheid worden in de tabel beide hogervermelde koninklijke besluiten samen behandeld, zonder onderscheid of het gaat om de eigenlijke inwerkingtreding van een bepaling, dan wel om het aflopen van een regularisatietermijn.

Datum	Bepalingen die dienen te worden nageleefd
1 april 1993	artikelen 1 tot en met 3 (begripsomschrijvingen en toepassingsgebied) artikel 5 (doelmatigheidsbeginsel) voor nieuwe verwerkingen artikel 16, § 1,1° (opmaken van een beschrijvende staat van elke geautomatiseerde verwerking) voor nieuwe verwerkingen artikelen 21 en 22 (mogelijkheid tot regeling van onderlinge verbindingen van verwerkingen en grensoverschrijdend gegevensverkeer) artikelen 23 tot en met 37¹⁰⁵ (werking van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer) artikelen 40 tot en met 43 (bepaalde strafbepalingen) artikel 44 (mogelijkheid tot het stellen van regels voor de toepassing van de wetsbepalingen op specifieke sectoren) artikel 45 (vernietingsplicht van verwerkingen in oorlogstijd of bij bezettingen van het grondgebied) artikelen 48, 49 en 51 (opheffing van bepaalde artikelen in andere wetten) artikel 52 (inwerkingtreding)

¹⁰⁴ Zie Gedr. St., Kamer, B.Z. 1991-1992, 413/12, 80-81 en Gedr. St., Senaat, B.Z. 1991-1992, 445-2, 121.

¹⁰⁵ Met uitzondering van artikel 34, tweede lid, dat bepaalt dat de bijdrage betaald door de houder van een bestand bij de aangifte van een geautomatiseerde verwerking door de rekenplichtige van de CBPL wordt gestort op een speciaal daartoe geopend artikel van de Rijksmiddelenbegroting. Deze bepaling treedt in werking op 1 maart 1994, hoewel de aangifteplicht (artikel 17) voor nieuwe verwerkingen slechts in werking treedt op 1 maart 1995.

Datum	Bepalingen die dienen te worden nageleefd
1 september 1993	artikel 4 (verplichting tot informatieverstrekking bij inzameling van gegevens bij de betrokkene) artikel 7, eerste tot derde lid (beperkingen m.b.t. tot de verwerking van medische gegevens) voor nieuwe verwerkingen artikelen 10 tot en met 15 (recht op toegang, verbetering en uitwissing van gegevens) artikel 16, § 1, 3^o (kwaliteitsbeginsel) artikelen 46 en 47 (aanpassing van bepalingen uit het gerechtelijk wetboek) artikel 50 (opheffing van bepaalde artikelen in andere wetten)
1 oktober 1993	artikel 5 (doelmatigheidsbeginsel) voor verwerkingen bestaande op 1 april 1993
1 januari 1994	artikel 16, § 1, 1 ^o (opmaken van een beschrijvende staat van elke geautomatiseerde verwerking) voor verwerkingen bestaande op 1 april 1993
1 maart 1994	artikel 16, § 1, 2^o (controle op de conformiteit van geautomatiseerde verwerkingen met de gegevens vermeld in de aangifte) artikelen 19, 20 en 34, tweede lid (register van de verwerkingen bijgehouden door de Commissie voor de Bescherming van de Persoonlijke Levenssfeer)
1 juni 1994	artikel 7, eerste tot derde lid (beperkingen m.b.t. de verwerking van medische gegevens) voor verwerkingen bestaande op 1 september 1993
1 maart 1995	artikelen 6 en 8 (beperkingen m.b.t. tot de verwerking van gevoelige en gerechtelijke gegevens) voor nieuwe verwerkingen artikel 9 (verplichting tot kennisgeving aan de betrokkene van de eerste registratie van persoonsgegevens in een verwerking) voor nieuwe verwerkingen artikel 17 (verplichting tot voorafgaande aangifte van verwerkingen) voor nieuwe verwerkingen artikel 18, eerste tot derde lid¹⁰⁶ (register van de verwerkingen bijgehouden door de Commissie voor de Bescherming van de Persoonlijke Levenssfeer) artikel 18, vierde lid¹⁰⁶ (verplichting tot vermelding van het identificatienummer van een verwerking op elk geproduceerd document) voor nieuwe verwerkingen

¹⁰⁶

Artikel 18 WVP treedt overeenkomstig artikel 4ter van het hoger vermelde koninklijk besluit nr. 1, zoals gewijzigd door het reeds geciteerde koninklijk besluit nr. 11, slechts in werking op de dag van de inwerkingtreding van het eerste uitvoeringsbesluit van artikel 18. Tot nog toe werd in uitvoering van dit artikel weliswaar nog geen besluit uitgevaardigd, maar artikel 52 WVP stelt 1 maart 1995 vast als uiterste datum van inwerkingtreding van om het even welke bepaling van de Wet Verwerking Persoonsgegevens.

Datum	Bepalingen die dienen te worden nageleefd
1 september 1994	artikel 7, vierde en vijfde lid (beperking van de mogelijkheid tot mededeling van medische gegevens) voor nieuwe verwerkingen artikel 16, § 1, 4° en 5°, § 2 en 3 (verplichting van de houder tot toegangscontrole en beveiliging van de verwerkingen)
1 juni 1995	artikel 7, vierde en vijfde lid (beperking van de mogelijkheid tot mededeling van medische gegevens) voor verwerkingen bestaande op 1 september 1994
1 december 1995	artikelen 6 en 8 (beperkingen m.b.t. de verwerking van gevoelige en gerechtelijke gegevens) voor verwerkingen bestaande op 1 maart 1995 artikel 9 (verplichting tot kennisgeving aan de betrokkene van de eerste registratie van persoonsgegevens in een verwerking) voor verwerkingen bestaande op 1 maart 1995 artikel 17 (verplichting tot voorafgaande aangifte van verwerkingen) voor verwerkingen bestaande op 1 maart 1995

De strafbepalingen vermeld in artikelen 38 en 39 worden van kracht op de dag van inwerking-treding van de artikelen waarvan ze de schending sanctioneren.

Artikel 18, vierde lid (verplichting tot vermelding van het identificatienummer van een verwerking op elk geproduceerd document) treedt voor verwerkingen bestaande op 1 maart 1995 in werking 3 maanden na de toekenning, door de Commissie van de Bescherming van de Persoonlijke Levenssfeer, van een identificatienummer aan de verwerking in het door haar bijgehouden register.

6.3. PLICHTEN VAN DE HOUDER VAN HET BESTAND

Elke houder van een bestand moet een aantal minimumverplichtingen naleven bij de verwerking van persoonsgegevens.

6.3.1. Naleving van het doelmatigheidsbeginsel (artikel 5 WVP)

Persoonsgegevens mogen vooreerst slechts worden verwerkt voor duidelijk omschreven en wettige doeleinden en mogen niet gebruikt worden op een wijze die onverenigbaar is met deze doeleinden. Bovendien dienen de gegevens, uitgaande van de vooropgestelde doeleinden, toereikend, terzake dienend en niet overmatig te zijn.

Het is dus vooreerst niet toegestaan gegevens te verwerken zonder dat een wettig doeleinde is vooropgesteld en duidelijk omschreven. De wetgever wil aldus aan de geregistreerde een minimum aan transparantie waarborgen omtrent het soort gebruik dat van persoonsgegevens kan worden gemaakt. De duidelijke omschrijving van het doeleinde is een moeilijke maar belangrijke

opgave. Het omschreven doeleinden is immers de cruciale toetssteen voor de vaststelling van rechtmatigheid van de omgang met de verwerkte persoonsgegevens. Zoals hoger al werd aangegeven, kan elke verwerking slechts één generieke doelstelling kan hebben. Indien dezelfde persoonsgegevens worden verwerkt voor meerdere generieke doelstellingen, maken ze dus deel uit van verschillende verwerkingen.

In de praktijk zal bij de beschrijving van de doeleinden een redelijk evenwicht dienen te worden gezocht tussen 2 te mijden uitersten. Enerzijds een zeer ruime definitie van de doelstellingen, waardoor de vrijheid van gegevensverwerking quasi totaal blijft en de wettelijke bescherming de facto wordt uitgehold; anderzijds een al te concrete beschrijving van de doeleinden, waardoor elke efficiënte gegevensverwerking lamgelegd dreigt te worden en de controle instanties overstelpt worden met aangiften en wijzigingen ervan.

De kunst bestaat er m.a.w. in de doelstellingen op dusdanige wijze te formuleren dat enerzijds de wettelijk voorziene bescherming afdoende wordt gewaarborgd, maar anderzijds niet elke gegevensverwerking nodeloos wordt bemoeilijkt. Het lexicon van de doeleinden dat werd gepubliceerd in bijlage bij het modelformulier voor de aangifte van geautomatiseerde verwerkingen aan de CBPL¹⁰⁷ (zie lager) wil de houders van bestanden op dit vlak aardig op pad zetten.

De nagestreefde doeleinden moeten bovendien wettig zijn. Noch in de wet, noch in de voorbereidende werken wordt dit begrip nader gepreciseerd. Het begrip 'wettig' is in elk geval ruimer dan de notie 'wettelijk'. Wat anderzijds in strijd is met wets- of reglementsbepalingen, of met de openbare orde of de goede zeden, is duidelijk onwettig. Daarbuiten zullen de CBPL en de rechtbanken het begrip nader moeten invullen op basis van de afweging van de rechtmatige belangen van enerzijds de geregistreerde en anderzijds de houder van het bestand. Een doelstelling die de individuele, rechtmatige belangen van een geregistreerde schendt zonder dat een hoger belang wordt nagestreefd, moet dus als onwettig worden beschouwd¹⁰⁸.

Eenmaal de (wettige) doeleinden van de verwerkingen omschreven, moet erover worden gewaakt dat de verwerkte persoonsgegevens, uitgaande van die doeleinden, toereikend, terzake dienend en niet overmatig zijn.

De toereikendheidsvereiste houdt in dat de verwerking voldoende gegevens moet bevatten om de vooropgestelde doelstellingen te realiseren. Deze afweging dient uiteraard te geschieden vanuit het licht van de bescherming van de persoonlijke levenssfeer, en niet vanuit de invalshoek van de maximale efficiëntie voor de houder. Impliciet kan hieruit aldus een recht van de geregistreerde worden afgeleid tot aanvulling van persoonsgegevens indien hij van oordeel is dat het beeld dat over hem wordt verstrekt door een verwerking steunt op te beperkte gegevens.

¹⁰⁷ B.S., 14 maart 1995, 5689.

¹⁰⁸ In dezelfde zin, BOULANGER, M., DE TERWANGHE, C. en LEONARD, T., Lc., 1993, 377.

Tegenhanger van de toereikendheidsvereiste is het verbod om overmatige persoonsgegevens te verwerken. Door de combinatie van beide vereisten heeft de wetgever willen aangeven dat zowel de verwerking van te weinig als van te veel persoonsgegevens kunnen aanleiding geven tot onrechtmatige inbreuken op de persoonlijke levenssfeer. Overmatige gegevensverwerking doet zich niet alleen voor wanneer de verwerkte gegevens te omvangrijk zijn, maar ook wanneer ze, gelet op de vooropgestelde doeleinden, te lang worden bewaard.

Ten derde moeten de verwerkte gegevens dienend, relevant zijn voor het bereiken van de vooropgestelde doeleinden. Wat relevant is, zal casuïstisch moeten worden ingevuld in functie van de concrete omstandigheden van de verwerking, met in het achterhoofd de reeds hoger vermelde belangenafweging.

Tenslotte mogen gegevens niet worden gebruikt op een wijze die onverenigbaar is met het omschreven wettig doeleinde. Dit betekent niet dat elk gebruik van de gegevens dat niet stricto sensu binnen het doeleinde valt, verboden. Wel dient te worden nagegaan of dergelijk gebruik in de lijn ligt van het omschreven doeleinde. Dat is in de eerste plaats een kwestie van casuïstiek. Mogelijke criteria bij de beoordeling hierbij kunnen zijn: de aard van de gegevens, de redelijke verwachtingen van de geregistreerde personen, het belang van de houder van het bestand, de potentiële risico's voor de persoonlijke levenssfeer, ...

6.3.2. Naleving van de beperkingen inzake de verwerking van gevoelige gegevens (artikel 6 WVP en koninklijk besluit nr. 7 van 7 februari 1995¹⁰⁹)

Artikel 6 WVP voorziet in beperkingen m.b.t. de verwerking van "gevoelige" persoonsgegevens, zijnde persoonsgegevens m.b.t. het ras, de etnische afstamming, het seksueel gedrag, de overtuiging of activiteit op politiek, levensbeschouwelijk of godsdienstig gebied en het lidmaatschap van een vakbond of ziekenfonds. Het begrip "etnisch" verwijst daarbij niet alleen naar de volkenkunde, maar ook naar een cultureel criterium: zo vormen de zigeuners bijvoorbeeld een "etnie"¹¹⁰.

Dergelijke gegevens mogen slechts worden verwerkt voor door of krachtens de wet vastgestelde doeleinden. Bovendien kunnen bij in Ministerraad overlegd koninklijk besluit en na advies van de CBPL bijzondere beschermingsregelen worden uitgevaardigd. In de wet zelf wordt alvast uitdrukkelijk vermeld dat het verbod tot verwerking van gevoelige gegevens verenigingen niet verbiedt eigen ledenbestanden bij te houden.

¹⁰⁹ Koninklijk besluit nr. 7 van 7 februari 1995 tot vaststelling van de doeleinden, de criteria en de voorwaarden van toegestane verwerkingen van de gegevens bedoeld in artikel 6 van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *B.S.*, 28 februari 1995, 4409.

¹¹⁰ *Gedr. St.*, Senaat, B.Z. 1991-1992, 445-2, 88.

Bij koninklijk besluit nr. 7 van 7 februari 1995 werden in uitvoering van artikel 6 WVP enerzijds een aantal machtigingen verstrekt voor de verwerking van gevoelige gegevens, en anderzijds de verwerking ervan aan een aantal bijzondere waarborgen onderworpen.

De verwerking van alle soorten van gevoelige gegevens wordt toegestaan

- indien dit noodzakelijk is voor het nakomen van een verplichting bepaald bij of krachtens een wet, een decreet of een ordonantie;
- indien dit noodzakelijk is voor het nakomen van een verplichting die voortvloeit uit een wet van een staat die partij is bij het verdrag nr. 108 van de Raad van Europa en die aan gevoelige gegevens een gelijkwaardige bescherming biedt als de Belgische WVP;
- ter uitvoering van een verplichting opgelegd door een rechtstreeks toepasbare bepaling van het internationaal publiekrecht, indien dit uitdrukkelijk wordt toegestaan bij in Ministerraad overlegd koninklijk besluit, genomen na advies van de CBPL;
- indien dit noodzakelijk is voor het nemen van een beslissing op verzoek van de betrokkene of voor het verrichten, op zijn verzoek, van een voor de betrokkene voordelige prestatie;
- indien dit noodzakelijk is om te voldoen aan een gewettigd belang van de betrokkene; de verwerking moet dan tot doel hebben aan de betrokkene een werkelijk voordeel op te leveren; de informatieëlementen bedoeld in art. 4 WVP moeten aan betrokkene zijn meegedeeld en hij mag zich niet tegen de verwerking hebben verzet;
- mits schriftelijk toestemming van de betrokkene, nadat hem de informatieëlementen bedoeld in art. 4 WVP zijn meegedeeld
- indien dit noodzakelijk is voor opinieonderzoek, mits de betrokkene heeft toegestemd nadat hem de informatieëlementen bedoeld in art. 4 WVP zijn meegedeeld; binnen de 5 dagen na het inzamelen van de gevoelige gegevens moeten zij gescheiden worden van de identificatiegegevens en binnen ten hoogste 60 dagen moeten zij volledig anoniem worden gemaakt;
- indien dit noodzakelijk is voor de verdediging en de bevordering van de rechten van de mens, voorzover de verwerking geschiedt door bij koninklijk besluit, genomen na advies van de CBPL, gemachtigde verenigingen met rechtspersoonlijkheid of instellingen van openbaar nut met deze verdediging als hoofdzakelijke statutaire doelstelling.

De verwerking van gegevens betreffende het ras en de etnische afstamming wordt toegestaan, voorzover de betrokkene er zich niet schriftelijk tegen verzet,

- in verwerkingen die loutere identificatiedoeleinden nastreven, voor zover de identificatie niet kan geschieden zonder de betrokken gegevens;
- in verwerkingen die uitsluitend de positieve discriminatie van etnische of raciale minderheden tot doel hebben.

De verwerking van gegevens betreffende het sexueel gedrag wordt toegestaan

- voor de verzorging van personen in door de overheid erkende ziekenhuizen, voorzover de gegevens enkel betrekking hebben op de patiënten of cliënten van deze instellingen of op

- derden die door hen worden vermeld, en de gegevens worden verwerkt onder het toezicht en de verantwoordelijkheid van een beoefenaar van de geneeskunst;
- voor de behandeling van parafielen, voorzover de verwerking geschiedt door door de overheid gesubsidieerde en bij koninklijk besluit, genomen na advies van de CBPL, gemachtigde verenigingen met rechtspersoonlijkheid of instellingen van openbaar nut met deze behandeling als statutaire doelstelling.

De verwerking van gegevens m.b.t. de politieke overtuiging of activiteiten wordt toegestaan

- voor politieke partijen of leden ervan, indien dit nodig is voor de verwezenlijking van een doelstelling van de partij en voorzover de gegevens betrekking hebben op personen die geregeld in contact staan met de partij in het kader van haar doelstellingen; de gegevens mogen slechts worden meegedeeld aan derden mits schriftelijke toestemming van de betrokkene;
- m.b.t. personen met een algemene bekendheid die blijkt uit het ambt, de activiteiten of de schriftelijke en mondelinge verklaringen van de betrokkenen, voorzover enkel gegevens worden verwerkt die de betrokkene openbaar maakt of die nauw verband houden met zijn algemene bekendheid.

De verwerking van gegevens m.b.t. de levensbeschouwelijke of godsdienstige overtuiging of activiteiten wordt toegestaan

- voor instellingen van levensbeschouwelijke of godsdienstige aard, indien dit noodzakelijk is voor de verwezenlijking van hun doelstellingen en voorzover in de verwerking enkel levensbeschouwelijke of godsdienstige gegevens voorkomen waaruit dezelfde overtuiging blijkt als die van de instelling
- m.b.t. personen met een algemene bekendheid die blijkt uit het ambt, de activiteiten of de schriftelijke en mondelinge verklaringen van de betrokkenen, voorzover enkel gegevens worden verwerkt die de betrokkene openbaar maakt of die nauw verband houden met zijn algemene bekendheid.

De verwerking van gegevens over het lidmaatschap van een vakbond of ziekenfonds wordt toegestaan

- voor vakbonden en ziekenfondsen of hun leden, m.b.t. personen waarmee een geregeld contact bestaat in het kader van hun doelstellingen;
- m.b.t. personen met een algemene bekendheid die blijkt uit het ambt, de activiteiten of de schriftelijke en mondelinge verklaringen van de betrokkenen, voorzover enkel gegevens worden verwerkt die de betrokkene openbaar maakt of die nauw verband houden met zijn algemene bekendheid.

In geen geval mogen gevoelige gegevens, afkomstig van andere personen dan de betrokkene, worden gebruikt in een verwerking die een indienstneming of bevordering tot doel heeft, tenzij de gegevens een fundamenteel criterium vormen voor het begeven van de betrekking of het ambt.

Tenslotte moet de houder van een verwerking waarin gevoelige gegevens voorkomen in de voorafgaandelijke aangifte aan de CBPL verwijzen naar de precieze wettelijke of reglementaire grondslag van de verwerking van de gevoelige gegevens, moet hij ten behoeve van de geregistreerde personen en van de CBPL een nominatieve lijst bijhouden van de personen die met de gegevens mogen omgaan, en moeten deze personen gehouden zijn tot een wettelijke, deontologische, statutaire of contractuele geheimhoudingsplicht.

6.3.3. Naleving van de beperkingen inzake de verwerking en mededeling van medische gegevens (artikel 7 WVP)

Ook voor medische persoonsgegevens geldt een bijzondere beschermingsregeling, die echter soepeler is dan deze voor de in het vorige punt beschreven gevoelige gegevens. Krachtens artikel 7, eerste lid WVP worden als "medische persoonsgegevens" beschouwd, persoonsgegevens "waaruit informatie kan worden afgeleid omtrent de vroegere, huidige of toekomstige fysieke of psychische gezondheidstoestand, met uitzondering van de louter administratieve of boekhoudkundige gegevens betreffende de geneeskundige behandeling of verzorging".

Deze definitie werd overgenomen uit de Kruispuntbankwet¹¹¹. Het Toezichtscomité ingesteld bij deze wet, waarvan de Voorzitter en één lid van rechtswege lid zijn van de CBPL, kreeg reeds de gelegenheid te preciseren welke medische gegevens als louter administratief of boekhoudkundig mogen worden beschouwd, en dus niet onderhevig zijn aan het bijzonder beschermingsregime¹¹². Als dusdanig worden bijvoorbeeld bestempeld, de woonplaats van een persoon (ook als daaruit bijvoorbeeld kan worden afgeleid dat hij in een psychiatrische instelling verblijft), de aanduiding dat een persoon een dossier heeft bij een instelling van sociale zekerheid zoals het Fonds voor Beroepsziekten of het Rijksinstituut voor Ziekte- en Invaliditeitsverzekering, of de graad van economische arbeidsongeschiktheid. De medische verslagen die de graad van medische arbeidsongeschiktheid motiveren, de aanvragen tot terugbetaling van medische diensten of prestaties, en, in het algemeen, alle persoonsgegevens die betrekking hebben op medische symptomen, diagnoses, behandelingen of prognoses, worden daarentegen wel als medisch persoonsgegeven beschouwd. M.b.t. nomenclatuurcodes neemt het Toezichtscomité een aarzelende houding aan. Hoewel deze codes op zich louter administratieve of boekhoudkundige doeleinden dienen, kan uit een aantal ervan toch medische informatie worden afgeleid. Voorzichtigheidshalve worden alle codes daarom als medisch persoonsgegeven beschouwd.

Medische persoonsgegevens kunnen slechts worden verwerkt mits een bijzondere schriftelijke toestemming van de titularis, die moet worden verstrekt voor elke medische behandeling

¹¹¹ Zie het artikel 2, eerste lid, 7° van de wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid, B.S., 22 februari 1990, 3289.

¹¹² TOEZICHTSCOMITE BIJ DE KRUISPUNTBANK VAN DE SOCIALE ZEKERHEID, Activiteitenverslag 1992. Het privé-leven aan het kruispunt van de informatica, Brussel, 1992, 34-36.

afzonderlijk¹¹³, of onder het toezicht en de verantwoordelijkheid van een beoefenaar van de geneeskunst. Hiermee worden niet alleen geneesheren bedoeld, maar bijvoorbeeld evenzeer tandartsen of apothekers¹¹⁴.

De personen die betrokken zijn bij de verwerking van medische gegevens of er toegang toe hebben, moeten door de persoon die verantwoordelijk is voor de verwerking, nominatief worden opgenomen in een register dat melding maakt van de inhoud en de reikwijdte van de toegangsmachtigingen.

Tenslotte kunnen medische gegevens slechts worden meegedeeld aan derden indien dit is toegestaan door of krachtens de wet. Wel wordt toegelaten dat de gegevens worden meegedeeld aan een andere beoefenaar van de geneeskunst en aan diens medische ploeg ofwel wanneer de betrokkene daarmee schriftelijk instemt of in spoedgevallen met het oog op een medische behandeling.

6.3.4. Naleving van de beperkingen inzake de verwerking van gerechtelijke gegevens (artikel 8 WVP en koninklijk besluit nr. 8 van 7 februari 1995¹¹⁵)

Artikel 8 WVP voorziet in stricte verwerkingsvoorwaarden voor een aantal gegevens die betrekking hebben op geschillen voorgelegd aan de hoven en rechtbanken, misdrijven, uitgesproken straffen, detenties en allerhande ontzettingen¹¹⁶.

¹¹³ Gedr. St., Kamer, 1991/92 (B.Z.), 413/12, 37.

¹¹⁴ Artikel 1 van het koninklijk besluit nr. 78 van 10 november 1967 betreffende de geneeskunst bepaalt immers dat 'de geneeskunst omvat de geneeskunde, de tandheelkunde inbegrepen, uitgeoefend ten aanzien van menselijke wezens en de artseneerbereidkunde, onder hun curatief of preventief voorkomen'.

¹¹⁵ Koninklijk besluit nr. 8 van 7 februari 1995 tot vaststelling van de doeleinden, de criteria en de voorwaarden van toegestane verwerkingen van de gegevens bedoeld in artikel 8 van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, B.S., 28 februari 1995, 4433.

¹¹⁶ Meer bepaald betreft het persoonsgegevens m.b.t. volgende aangelegenheden:

- de geschillen voorgelegd aan de hoven, rechtbanken of de administratieve rechtscolleges;
- de misdrijven waarvan een persoon wordt verdacht of waarin hij is betrokken;
- de misdrijven waarvoor een persoon is veroordeeld en de straffen die tegen hem zijn uitgesproken;
- de detenties en de terbeschikkingstellingen van de Regering krachtens bepaalde artikelen van de Landloperijwet, het Strafwetboek en de Vreemdelingenwet;
- de interneringsmaatregelen en terbeschikkingstellingen van de Regering krachtens de Wet Bescherming Maatschappij;
- de beslissingen inzake voorlopige hechtenis;
- de verzoeken tot betaling van een geldsom met het oog op het verval van de strafvordering voor sommige misdrijven;
- de maatregelen genomen tegen minderjarigen op grond van de Jeugdbeschermingswet;
- de ontzettingen uit de ouderlijke macht en de maatregelen voor opvoedingsbijstand uitgesproken in uitvoering van de Jeugdbeschermingswet;

Net zoals de gevoelige gegevens, mogen dergelijke "gerechtelijke gegevens" slechts worden verwerkt voor door of krachtens de wet vastgestelde doeleinden en kunnen bij in Ministerraad overlegd koninklijk besluit en na advies van de CBPL bijzondere beschermingsregelen worden uitgevaardigd. Artikel 8 WVP omschrijft alvast welke gegevens mogen worden opgenomen in het centrale en de gemeentelijke strafregisters, en preciseert onder welke voorwaarden een advocaat alle soorten van gerechtelijke gegevens mag verwerken met het oog op de bescherming van de belangen van zijn cliënten.

Bij koninklijk besluit nr. 8 van 7 februari 1995, dat een zekere analogie vertoont met het hoger beschreven koninklijk besluit nr. 7 m.b.t. gevoelige gegevens, werden in uitvoering van artikel 6 WVP enerzijds een aantal machtigingen verstrekt voor de verwerking van gevoelige gegevens, en anderzijds de verwerking ervan aan een aantal bijzondere waarborgen onderworpen.

De verwerking van alle soorten van gerechtelijke gegevens wordt toegestaan

- aan openbare overheden en politiediensten voor de uitvoering van hun taken van gerechtelijke of administratieve politie; de gerechtelijke gegevens mogen slechts aan buitenlandse politiediensten worden megedeeld in het kader van een door België gesloten internationaal verdrag of gouvernementeel akkoord of door tussenkomst van een organisatie voor politieke samenwerking t.o.v. waarvan de Belgische overheden en politiediensten verplichtingen hebben; een lijst van de verzoeken om mededeling en de reden ervan moet 6 maanden worden bijgehouden; indien de mededeling niet geschiedt in het kader van een door België gesloten verdrag en de staat van bestemming aan gerechtelijke gegevens geen gelijkwaardige bescherming biedt als de Belgische WVP, mogen slechts een beperkt aantal categorieën van gerechtelijke gegevens worden megedeeld, enkel in het kader van opdrachten van gemeen recht en enkel in geval van ernstig en dreigend gevaar of met het oog op de bestraffing van een misdaad of wanbedrijf;
- indien dit noodzakelijk is voor de toepassing van de wet ter voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld;
- indien dit noodzakelijk is voor de verdediging en de bevordering van de rechten van de mens, voorzover de verwerking geschiedt door bij koninklijk besluit, genomen na advies van de CBPL, gemachtigde verenigingen met rechtspersoonlijkheid of instellingen van openbaar nut met deze verdediging als hoofdzakelijke statutaire doelstelling.

De verwerking van alle soorten van gerechtelijke gegevens wordt toegestaan 1 maand

-
- de gratiebesluiten en de maatregelen inzake uitwissing van veroordelingen of herstel in eer en rechten;
 - de besluiten die de voorwaardelijke invrijheidstelling gelasten;
 - de wegzendingen uit het leger, uit de politie, uit de rijkswacht of uit de dienst gewetensbezwaarden;
 - de vervallenverklaringen of ontzettingen uitgesproken door hoven of rechtbanken of geldend t.a.v. veroordeelde personen;
 - de opschorting van de uitspraak van veroordeling in uitvoering van de Probatiwet;
 - de maatregelen genomen ten aanzien van geesteszieken op grond van de Geestesziekenwet;
 - andere maatregelen of sancties die m.b.t. een persoon zijn uitgesproken, aan te duiden bij koninklijk besluit.

(betrokkene kan kortere termijn aanvaarden) nadat de informatieelementen bedoeld in art. 4 WVP schriftelijk aan betrokkene zijn meegedeeld

- indien dit noodzakelijk is voor het nakomen van een verplichting bepaald bij of krachtens een wet, een decreet of een ordonantie;
- indien dit noodzakelijk is voor het nakomen van een verplichting die voortvloeit uit een wet van een staat die partij is bij het verdrag nr. 108 van de Raad van Europa en die aan gevoelige gegevens een gelijkwaardige bescherming biedt als de Belgische WVP;
- ter uitvoering van een verplichting opgelegd door een rechtstreeks toepasbare bepaling van het internationaal publiekrecht, indien dit uitdrukkelijk wordt toegestaan bij in Ministerraad overlegd koninklijk besluit, genomen na advies van de CBPL;
- indien dit noodzakelijk is voor het nemen van een beslissing op verzoek van de betrokkene of voor het verrichten, op zijn verzoek, van een voor de betrokkene voordelige prestatie;
- mits schriftelijk toestemming van de betrokkene.

De verwerking van bepaalde soorten van gerechtelijke gegevens wordt toegestaan

- voor het beheer van eigen geschillen;
- voor de behandeling van parafielen, voorzover de verwerking geschiedt door door de overheid gesubsidieerde en bij koninklijk besluit, genomen na advies van de CBPL, gemachtigde verenigingen met rechtspersoonlijkheid of instellingen van openbaar nut met deze behandeling als statutaire doelstelling;
- voor het opmaken van een staat van de rechtspraak in rechtsstelsels waar de vermelding van rechterlijke beslissingen gewoonlijk geschiedt onder verwijzing naar de namen van de partijen, voorzover de verwerkingen als persoonsgegevens betreffende de partijen enkel de naam, het onderwerp en de (korte) inhoud van de beslissing bevatten.

De bijkomende waarborgen die moeten worden nageleefd bij de verwerking van gerechtelijke gegevens zijn dezelfde als bij de verwerking van gevoelige gegevens.

6.3.5. Opmaken van een beschrijvende staat van elke geautomatiseerde verwerking (artikel 16 § 1, 1° WVP)

De houder van een bestand moet een beschrijvende staat opmaken van elke geautomatiseerde verwerking, met aanduiding van de aard van de verwerkte gegevens, het doel van de verwerking, de verbanden en verbindingen met andere verwerkingen, de raadplegingsmogelijkheden en de (categorieën van) personen aan wie de persoonsgegevens worden doorgegeven.

6.3.6. Aangifte van verwerkingen aan de CBPL (artikelen 17-20 WVP)

6.3.6.1. Geautomatiseerde verwerkingen

Vooraleer een geautomatiseerde verwerking van persoonsgegevens wordt gestart, dient de houder daarvan aangifte te doen bij de CBPL. In de aangifte moeten heel wat elementen worden

verstrekt over de verwerking, zoals de identificatie van de houder en eventuele bewerkers, het doel van de verwerking, de soorten verwerkte gegevens, met bijzondere aandacht voor de hoger beschreven gevoelige, gerechtelijke en medische gegevens, de verwerkingsduur, de categorieën personen die toegang hebben tot de gegevens, de wijze waarop het recht op toegang kan worden uitgeoefend door de betrokkenen, en eventueel de soorten gegevens die worden overgemaakt aan het buitenland. Telkens wanneer één van deze kenmerken grondig wijzigt of wanneer een verwerking ophoudt te bestaan, dient de aangifte opnieuw te worden verricht. Bepaalde soorten geautomatiseerde verwerkingen die kennelijk geen gevaar inhouden, kunnen worden vrijgesteld van aangifte of aan een beperkte aangifte worden onderworpen. Dit is tot nog toe niet gebeurd. Bij het verrichten van een aangifte, dient de houder van het bestand een bijdrage te storten die wordt gebruikt om een deel van de werkingskosten van de Commissie te financieren. Het bedrag werd vastgelegd in koninklijk besluit nr. 12 van 7 maart 1995¹¹⁷ en varieert, met een maximum van 10.000 B, naargelang de aard van de aangifte (nieuwe aangifte, wijzigende aangifte of aangifte van beëindiging van de verwerking), het doeleinde van de aangegeven verwerking en wijze waarop de aangifte wordt gedaan (elektronisch, via het papieren modelformulier of op papier in vrije vorm).

Om de indiening van de aangiften ter vergemakkelijken, werd in bijlage bij het vermelde koninklijk besluit nr. 12 een modelformulier gepubliceerd, vergezeld van lexica m.b.t. de meeste rubrieken. Ook kunnen door instanties als beroepsverenigingen of sociale secretariaten standaardaangiften worden uitgewerkt, waarbij individuele houders zich kunnen aansluiten, zodat het administratieve werk bij de aangifte aanzienlijk wordt beperkt. Tenslotte stelt de CBPL een diskette met freeware ter beschikking aan de hand waarvan een elektronische aangifte kan worden gedaan.

Alle elementen uit de aangifte worden door de Commissie opgenomen in een openbaar register, dat elkeen kan raadplegen. Het identificatienummer van de houder en van de verwerking in dat register moet worden vermeld op ieder stuk waarvoor ze gebruikt is.

Verwerkingen die reeds in uitvoering van specifieke wetten aan een systeem van voorafgaande aangiften of machtigingen zijn onderworpen, en waarover de hogervermelde informatie reeds wordt meegedeeld aan een Toezichtscomité en opgenomen in een ander openbaar register, worden tenslotte van de aangifteplicht vrijgesteld indien dat register permanent ter beschikking wordt gehouden van de CBPL.

6.3.6.2. Manuele verwerkingen

Van een manueel bestand dient in principe geen aangifte te worden verricht. De CBPL kan

¹¹⁷ Koninklijk besluit nr. 12 van 7 maart 1995 tot vaststelling van de bedragen die aan de Commissie voor de bescherming van de persoonlijke levenssfeer moeten worden gestort bij de aangifte van verwerkingen van persoonsgegevens, *B.S.*, 14 maart 1995, 5661.

echter wel ambtshalve of op verzoek van een betrokkene aan de houder van dergelijke bestanden bepaalde informatie opvragen, indien ze meent dat het bestand een mogelijke schending van de persoonlijke levenssfeer inhoudt.

6.3.7. Informatieverstrekking aan de betrokkene

6.3.7.1. Bij de inzameling van gegevens bij de betrokkene (artikel 4 WVP)

Wanneer bij een persoon, met het oog op de verwerking ervan, persoonsgegevens worden ingezameld die op hem betrekking hebben, moet de betrokkene voorafgaandelijk aan de overdracht van de gegevens op de hoogte worden gesteld van:

- de identiteitsgegevens van de houder van het bestand en eventueel de bewerker;
- de doeleinden waarvoor de gevraagde gegevens zullen gebruikt worden;
- de eventuele rechtsbasis waarop men zich steunt om de gegevens te verzamelen;
- de mogelijkheid om - in het geval van een geautomatiseerde verwerking - het openbaar register te raadplegen;
- zijn recht op kennisname, verbetering, verwijdering en niet-aanwending.

Deze informatieverstrekking dient te geschieden bij elke inzameling van persoonsgegevens bij de betrokkene, zoals de vraag tot vervollediging van een formulier of een antwoordcoupon, de mondelinge gegevensinzameling aan een loket, ... Het speelt geen rol of de gegevensinzameling kadert in een contractuele of wettelijk geregelde relatie tussen de houder van het bestand en de betrokkene, noch of de inzameling rechtstreeks gebeurt door de houder van het bestand of door een tussenpersoon. De verplichting geldt ook wanneer gegevens worden ingezameld in België met het oog op de verwerking ervan in het buitenland.

Indien de gegevens evenwel niet bij de betrokkene, maar bij een derde worden ingezameld, geldt de informatieplicht niet bij de inzameling, maar bij de eerste registratie (zie hierna). Overheden die persoonsgegevens inzamelen in het kader van de uitvoering van hun taken van administratieve of gerechtelijke politie zijn bovendien vrijgesteld van de informatieverplichting. Ook weze vermeld dat van een inzameling van informatie in de zin van de wet geen sprake is indien de betrokkene volledig op eigen initiatief informatie verstrekt.

De wet stelt dat de betrokkene moet ingelicht worden, maar bepaalt niet de wijze waarop dit dient te gebeuren. Om bewijsproblemen te voorkomen lijkt een, zij het collectieve schriftelijke informatieverstrekking aan te raden.

6.3.7.2. Bij de eerste registratie van persoonsgegevens over de betrokkene (artikel 9 WVP en koninklijk besluit nr. 9 van 7 februari 1995¹¹⁸)

Zoals hoger vermeld, geldt de informatieplicht bij de inzameling van gegevens niet wanneer de gegevens worden ingezameld bij een andere persoon dan degene waarop de gegevens betrekking hebben. In dat geval dient de betrokkene niet te worden ingelicht op het ogenblik van de inzameling, maar op het ogenblik van de eerste registratie van de gegevens. De te verstrekken informatie is dezelfde als deze die moet worden meegedeeld bij de inzameling van persoonsgegevens bij de betrokkene.

De informatieplicht bij de eerste registratie geldt overigens algemeen, behalve in een aantal uitzonderingen vastgelegd in artikel 9 WVP of het uitvoeringsbesluit nr. 9, met name

- wanneer de betrokkene reeds op de hoogte werd gesteld bij de inzameling van de gegevens, en het doeleinde van de verwerking sedertdien niet is gewijzigd;
- wanneer de verwerking kadert in een contractuele relatie tussen de houder van het bestand en de betrokkene; het begrip "contractuele relatie" dient hier niet in de strict juridische zin te worden opgevat, maar wil verwijzen naar een niet-vrijblijvende, gestructureerde verhouding tussen de houder van het bestand en de geregistreerde, die van aard is dat de registratie in een verwerking van deze laatste erdoor wordt verantwoord¹¹⁹;
- de verwerking kadert in een relatie tussen de betrokken persoon en de houder van het bestand, geregeld door of krachtens een wet, een decreet of een ordonnantie;
- de verwerking geschiedt door de Staatsveiligheid, door de Veiligheidsdienst van het Leger of door de administratieve of gerechtelijke politie, in het kader van hun opdrachten
- de verwerking geschiedt in het kader van de wet ter voorkoming van witwassen van geld
- de verwerking uitsluitend tot doel heeft de personen te identificeren met wie de houder van bestand public relations¹²⁰ wenst te leggen of te onderhouden, of met wie hij in het kader van de functie of de activiteiten van die personen maatschappelijke of professionele betrekkingen onderhoudt, evenals het bijhouden van een lijst met namen en adressen van deze personen; bovendien mag de verwerking slechts een beperkt aantal gegevens bevatten (naam, voornamen, toenames, bijnamen, pseudoniemen, beroeps- en contactadres - inclusief aanduiding van telecommunicatienummers, functie, sector en

¹¹⁸ Koninklijk besluit nr. 9 van 7 februari 1995 betreffende het verlenen van vrijstellingen van de toepassing van artikel 9 van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens en tot vaststelling van een procedure van collectieve informatieverstrekking aan de personen op wie bepaalde verwerkingen betrekking hebben, B.S., 28 februari 1995, 4456.

¹¹⁹ Gedr. St., Senaat, B.Z. 1991-1192, 445-2, 93.

¹²⁰ In het advies nr. 09/93 van de CBPL wordt public relations omschreven als "het leggen en onderhouden van betrekkingen met personen met een algemene bekendheid, teneinde een gunstig beeld van hun bedrijf of instelling te bekomen of te behouden". Indien het gaat om personen die niet algemeen bekend zijn, of indien een ander doeleinde, zoals klantenprospectie, ten grondslag ligt van de verwerking, gaat het volgens de CBPL niet om een public relations-verwerking.

aard van de activiteiten, datum van het laatste contact, refertenummer; wanneer het niet louter om public relations gaat, mag dit worden aangevuld met: privé-adres - inclusief aanduiding van telecommunicatienummers, de aard van de relatie met de houder van het bestand, plaats, datum en omstandigheden van de kennismaking, foto) en mag ze, met uitzondering van de foto of informatie voortvloeiend uit de functie, geen gevoelige, medische of gerechtelijke gegevens bevatten;

- de verwerking er uitsluitend op gericht is een staat op te maken van de rechtspraak in rechtsstelsels waar de vermelding van rechterlijke beslissingen gewoonlijk geschiedt onder de verwijzing naar de namen van de partijen en als persoonsgegevens betreffende de partijen enkel de naam, het onderwerp en de (korte) inhoud van de beslissing bevat.

Een vrijstelling van de plicht tot informatieverstrekking bij eerste registratie is bovendien mogelijk bij koninklijk besluit, genomen na advies van de CBPL indien

- de verwerking noodzakelijk is voor de verwezenlijking van een hoofdzakelijke statutaire doelstelling van een vereniging met rechtspersoonlijkheid of een instelling van openbaar nut die bestaat in de verdediging en de bevordering van de rechten van de mens en van de fundamentele vrijheden;
- de verwerking verricht wordt door een vereniging met rechtspersoonlijkheid of een instelling van openbaar nut met als statutaire doelstelling de behandeling van parafielen, die voor de verwezenlijking van die doelstelling subsidies ontvangt van een openbare overheid.

De mee te delen informatie is dezelfde als degene die moet worden meegedeeld bij de inzameling van gegevens bij de betrokkene zelf (zie hoger).

In principe moet elke geregistreerde persoon individueel in kennis worden gesteld. Strict omschreven collectieve procedures van informatieverstrekking zijn (facultatief) toegestaan

- t.a.v. onrechtstreeks geregistreerden; dit zijn personen waarover gegevens worden verwerkt die slechts kunnen worden teruggevonden onder verwijzing naar een ander (natuurlijk of rechts)persoon of entiteit, en niet door een gegeven op te zoeken op grond waarvan de betrokkene kan worden geïdentificeerd; het is dus niet mogelijk systematisch alle gegevens betreffende de betrokkene terug te vinden omdat er geen specifieke toegangssleutels op gegevens m.b.t. hem zijn; men denke aan begunstigden van overschrijvingen van geld in verwerkingen m.b.t. bankrekeningen, tegenpartijen en getuigen in verwerkingen van verzekeringsmaatschappijen, gezinsleden in persoonsinformatiesystemen, ouders in verwerkingen van scholen, ...;
- voor verwerkingen die hoofdzakelijk door de betrokkene openbaar gemaakte of uit een openbare rechterlijke beslissing voortkomende persoonsgegevens bevatten, terwijl de doelstelling van de openbaarmaking wordt gerespecteerd (vb. auteursbestanden van bibliotheken of verwerkingen van gefailleerden);
- t.a.v. personen die op 1 maart 1995 geregistreerd zijn in verwerkingen die enkel het verrichten van marktonderzoek of het uitoefenen van de activiteit van een adresbureau tot doel hebben, waarvan de houder nooit in contact treedt met de geregistreerde personen en

die geen gevoelige, medische of gerechtelijke gegevens bevat.

De wijze van collectieve kennisgeving in de eerste 2 gevallen bestaat in een bekendmaking, minstens één maal om de 5 jaar, in het Belgisch Staatsblad en 4 dagbladen of tijdschriften die gewoonlijk voorhanden zijn in de woonplaats van de betrokkenen van een gemakkelijk begrijpbaar bericht met de mee te delen informatieëlementen. In het derde geval kan gedurende 3 opeenvolgende dagen op een tijdstip van grote kijkdichtheid een gemakkelijk begrijpbaar bericht met welomschreven informatie worden uitgezonden op alle niet-gecodeerde Belgische televisienetten, waarvan de programma's tenminste in één Gemeenschap kunnen worden ontvangen. Deze procedures van collectieve informatieverstrekking zijn dermate bij de haren getrokken en kostelijk dat ze waarschijnlijk nooit zullen worden toegepast.

6.3.8. Waken over het goed en veilig beheer van de verwerkingen (artikel 16 § 1, 2°-5° en §§ 2-3 WVP)

De houder van een bestand moet erover waken dat de programma's gebruikt voor een geautomatiseerde verwerking gebruikt worden in overeenstemming met de voorafgaandelijke aangifte, zijn medewerkers degelijk informeren over de toepasselijke reglementering en erop toezien dat de kwaliteit van de gegevens wordt gewaarborgd en ze regelmatig worden bijgewerkt. Bovendien dient de houder erover te waken dat de toegang tot de gegevens beperkt blijft tot de bevoegde personen, en dat elke bevoegde persoon slechts die handelingen uitvoert waartoe hij gemachtigd is. Tevens moet hij ervoor zorgen dat de gegevens niet aan onbevoegde derden worden meegedeeld.

Om de veiligheid te waarborgen dient de houder van het bestand de gepaste technische en organisatorische maatregelen te treffen die nodig zijn voor de bescherming van de gegevens tegen toevallige of ongeoorloofde vernietiging, toevalig verlies, ongeoorloofde wijziging of toegang, en iedere andere niet toegelaten handeling. De maatregelen moeten een passend beveiligingsniveau verzekeren, rekening houdend met enerzijds de stand der techniek en de kosten voor het toepassen van de maatregelen en anderzijds de aard van de te beveiligen gegevens en de potentiële risico's. Op advies van de CBPL kunnen bij koninklijk besluit voor alle of bepaalde categorieën van verwerkingen nadere veiligheidsnormen worden uitgevaardigd.

In de memorie van toelichting¹²¹ wordt uitdrukkelijk gespecificeerd dat deze verplichtingen slechts middelverbintenissen zijn, zodat bij de beoordeling van de eventuele aansprakelijkheid van de houder van een bestand de gedane inspanningen zullen moeten worden afgewogen t.o.v. het beoogde en bereikte beschermingsresultaat.

6.3.9. Naleving van eventuele bijkomende regelen opgelegd bij uitvoeringsbesluiten (artikelen 21, 22, 44 en 45 WVP)

¹²¹

Gedr. St., Kamer, 1990-91, 1610/1, 21.

De wet voorziet in een vrij ruime mogelijkheid om bij in Ministerraad overlegd koninklijk besluit, na advies van de CBPL, nadere regelen uit te werken op een aantal domeinen. Zo kan het leggen van verbanden tussen persoonsgegevens en het exporteren van gegevens naar het buitenland worden gereguleerd, en kunnen de beginselen van de wet worden geconcretiseerd naar bepaalde maatschappelijke sectoren toe, zoals de sociale zekerheid, de fiscaliteit, de financiële sector, ...

Aan de Koning wordt bovendien de bevoegdheid verleend om de overheden aan te wijzen die in geval van oorlogs- of bezettingstijd het bevel kunnen geven om verwerkte gegevens te (doen) vernietigen. Ook kan hij de bedragen vaststellen van de vergoeding voor dergelijke vernietiging.

6.4. RECHTEN VAN DE GEREgistREERDE

6.4.1. Recht op eerbiediging van de persoonlijke levenssfeer bij de verwerking van persoonsgegevens (artikel 2 WVP)

In algemene termen stelt de wet dat elke natuurlijke persoon recht heeft op eerbiediging van zijn persoonlijke levenssfeer bij de verwerking van persoonsgegevens die op hem betrekking hebben. Hiermee beschikt de burger over een algemene, residuaire rechtsgrond voor de bescherming van zijn privacy bij gegevensverwerking. De andere toegekende rechten zijn als het ware instrumenten om dit fundamenteel recht uit te oefenen. Indien de meer specifieke toegekende rechten niet de mogelijkheid bieden om te ageren tegen onrechtmatige inbreuken op de persoonlijke levenssfeer, kan de geregistreeerde zich steeds op de algemene bepaling van artikel 2 WVP beroepen.

6.4.2. Recht op informatie (artikelen 4, 9 en 18 WVP)

Als eerste concretisatie van het algemeen recht op eerbiediging van de persoonlijke levenssfeer, heeft elke persoon het recht te weten wanneer en voor welke doeleinden gegevens over hem worden verwerkt. Dit recht op weten wordt gewaarborgd door een reeks van maatregelen die tot doel hebben de nodige basisinformatie ter beschikking te stellen aan de betrokkene, hetzij rechtstreeks, bij de inzameling of de eerste registratie van persoonsgegevens, hetzij via de consultatie van het openbare register van de geautomatiseerde verwerkingen bijgehouden door de CBPL. Deze rechten vormen dus het correlarium van aantal verplichtingen van de houder van het bestand, die hiervoor werden beschreven.

6.4.3. Recht op kennisname van gegevens (artikel 10 WVP en koninklijke besluiten nrs. 3 en 4 van 7 september 1993¹²²)

¹²² Koninklijk besluit nr. 3 van 7 september 1993 tot aanwijzing van de personen bij wie het verzoek om mededeling van persoonsgegevens gegrond op artikel 10 van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens moet worden ingediend, *B.S.*, 25 september 1993, 21254 en koninklijk besluit nr. 4 van 7 september 1993 tot vaststelling van het bedrag, de voorwaarden en de wijze van betaling van een voorafgaande heffing aan de houder van het bestand bij de uitoefening

Elke persoon heeft het recht kennis te krijgen van de gegevens die betreffende hem in een verwerking worden bijgehouden. Dit recht kan, naar keuze van de betrokkene, uitgeoefend worden bij de houder van het bestand of een door hem gemachtigde of aangestelde persoon, bij de bewerker of bij de onderneming of vereniging ten behoeve waarvan de houder van het bestand bewerkingen uitvoert. Het volstaat een gedateerde en getekende brief op te sturen of ter plaatse een verzoek in te dienen, tegen een gedagtekend en ondertekend ontvangstbewijs¹²³. Wel dient een vergoeding van 100 BF te worden betaald¹²⁴ per verzoek, ongeacht het aantal verwerkingen t.a.v. welke het recht op kennisname wordt uitgeoefend, en dient de betrokkene zijn identiteit te bewijzen.

De houder van een bestand moet onverwijld en in elk geval binnen de 45 kalenderdagen na de ontvangst van het verzoek om kennisname antwoorden op een voor de betrokkene begrijpelijke wijze. Naast de mededeling van de verwerkte gegevens, dient de betrokkene te worden gewezen op zijn recht op verbetering, verwijdering en niet-aanwending van de gegevens, zijn recht op verhaal bij de voorzitter van de rechtbank van eerste aanleg en zijn recht op raadpleging van het openbaar register van de geautomatiseerde verwerkingen bijgehouden door de CBPL.

Vermeldenswaard is de precisering aangebracht door de Minister van Justitie dat het antwoord op een vraag om kennis te krijgen van gegevens die betreffende de aanvrager worden bijgehouden, slechts die gegevens integraal moet weergeven die niet reeds bij een vorige gelegenheid werden meegedeeld, op voorwaarde dat deze gegevens inmiddels niet werden gewijzigd; voor de andere gegevens mag de houder zich beperken tot de mededeling dat de gegevens niet werden gewijzigd¹²⁵. Om ongebreidelde aanvragen te vermijden, voorziet de wet overigens in het algemeen dat aan een vraag om kennisname van gegevens slechts moet worden voldaan indien sedert de laatste mededeling van de informatie, hetzij op vraag van de betrokkene, hetzij door de houder uit eigen beweging, minstens een jaar is verstreken. De CBPL kan evenwel in buitengewone gevallen of in geval de gegevens zijn gewijzigd, de termijn inkorten.

Een persoon kan krachtens de WVP enkel gegevens opvragen die hemzelf betreffen. Voor het

van het recht om overeenkomstig artikel 10 van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, kennis te krijgen van persoonsgegevens, B.S., 25 september 1993, 21256.

¹²³ Men kan zich afvragen of de mogelijkheid die door het koninklijk besluit nr. 3 van 7 september 1993 wordt voorzien om het recht op kennisname uit te oefenen via een eenvoudig mondeling verzoek ter plaatse tegen een gedagtekend en ondertekend ontvangstbewijs wel in overeenstemming is met artikel 10 WVP, die een gedagtekend en ondertekend, en dus schriftelijk verzoek vereist.

¹²⁴ De wijze van betaling van dit bedrag wordt nader gepreciseerd in het hoger vermelde koninklijk besluit nr. 4.

¹²⁵ Gedr. St., Kamer, 1991-92 (B.Z.), 413/12, 47.

overige is het recht op kennisname erg ruim. Het heeft niet alleen betrekking op feitelijke gegevens, maar evenzeer op appreciaties, beoordelingen of beslissingen op basis van deze gegevens¹²⁶.

Voor bepaalde soorten van gegevens wordt een rechtstreekse kennisname door de betrokkene uitgesloten. Dit is in de eerste plaats het geval voor medische gegevens, die slechts kunnen worden meegedeeld via een door de betrokkene gekozen geneesheer. Daarnaast is evenmin een rechtstreekse kennisname mogelijk van gegevens verwerkt door de administratieve en gerechtelijke politie, de Staatsveiligheid en de Militaire Veiligheidsdienst. Wel kan elkeen zich kosteloos tot de CBPL wenden om te vragen in zijn plaats het recht op toegang uit te oefenen. De CBPL zal dan volgens nader te bepalen modaliteiten alle nuttige controles verrichten en de betrokkene inlichten over het feit dat deze controles zijn verricht. De betrokkene zal evenwel niet in kennis worden gesteld van de geregistreerde gegevens, noch van het feit of gegevens over hem al dan niet worden verwerkt. Via dit systeem wordt gepoogd een evenwicht te vinden tussen de rechten van elkeen op gegevensbescherming en de noodzaak van opsporing en vervolging van overtredingen en het voorkomen van inbreuken op de veiligheid van de Staat.

6.4.4. Recht op verbetering, verwijdering of opleggen van een gebruiksverbod (artikel 12 WVP en koninklijk besluit nr. 5 van 7 september 1993¹²⁷)

In het verlengde en als sluitstuk van het recht op kennisname, worden aan de geregistreerde een aantal rechten toegekend om te kunnen optreden wanneer hij ten gevolge van de kennisname van de gegevens die over hem worden verwerkt abnormaliteiten vaststelt. In de eerste plaats kan hij onjuiste gegevens die op hem betrekking hebben, doen verbeteren. Daarenboven kan hij gegevens doen verwijderen die, gelet op het doel van de verwerking, onvolledig, irrelevant, onrechtmatig verwerkt of te lang bewaard zijn. In plaats van zijn verwijderingsrecht uit te oefenen, kan de betrokkene tenslotte opteren voor het opleggen van een gebruiksverbod. In dat geval mag de houder de gegevens niet fysisch verwijderen, om mogelijke nadelen van een uitwissing te voorkomen (bijvoorbeeld bewijsproblemen), maar wordt hem wel verboden ze nog verder aan te wenden.

De rechten op verbetering, verwijdering en niet-aanwending van gegevens kunnen kosteloos - worden uitgeoefend bij dezelfde instanties als het recht op kennisname, via een gemotiveerd, gedateerd en getekend verzoek. Aan een gerechtvaardigd verzoek moet binnen de maand na de indiening ervan gevolg worden gegeven. Vanaf het ogenblik dat een verzoek tot verbetering, verwijdering of niet-aanwending van persoonsgegevens ontvangen wordt, is de houder van het

¹²⁶ Gedr. St., Kamer, 1991-92, 413/12, 47.

¹²⁷ Koninklijk besluit nr. 5 van 7 september 1993 tot aanwijzing van de personen bij wie de verzoeken tot verbetering, verwijdering of verbod op de aanwending van persoonsgegevens gegrond op artikel 12 van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens moet worden ingediend, B.S., 25 september 1993, 21259.

bestand verplicht bij iedere mededeling van deze gegevens te vermelden dat ze betwist worden.

De houder die gegevens op vraag van de geregistreeerde heeft moeten verbeteren of verwijderen, is er bovendien toe gehouden de personen aan wie hij in het verleden de betrokken gegevens heeft meegedeeld, van de verbeteringen in kennis te stellen en dit binnen een maand na het verzoek tot verbetering. De houder van een bestand is verplicht de identiteit van de bestemmelingen gedurende 12 maanden te bewaren. Bij koninklijk besluit, genomen na advies van de CBPL, kunnen op deze termijn echter afwijkingen worden voorzien voor bepaalde categorieën van verwerkingen.

Voor de heruitoefening van de rechten op verbetering, verwijdering of niet-aanwending is geen wachtermijn voorzien.

Wat betreft de gegevens verwerkt door de administratieve en gerechtelijke politie, de Staatsveiligheid en de Militaire Veiligheidsdienst, kunnen de rechten op verbetering, verwijdering en niet-aanwending, net zoals het recht op kennisname, slechts via de CBPL worden uitgeoefend.

6.4.5. Recht op verhaal

Naast de mogelijkheid om klacht in te dienen bij het parket bij vermoedelijke schending van de strafrechtelijk gesanctioneerde verplichtingen, beschikt de geregistreeerde over een dubbele mogelijkheid tot verhaal indien hij bij de houder van een bestand geen voldoening bekomt wat betreft de uitoefening van zijn rechten.

6.4.5.1. Bij de voorzitter van de rechtbank van eerste aanleg (artikel 14 WVP)

Bij schending van zijn rechten op kennisname, verbetering, verwijdering of niet-aanwending van persoonsgegevens, kan de gelaedeerde zich wenden tot de voorzitter van de rechtbank van eerste aanleg, zetelend als in kortgeding. De vordering wordt ingediend bij verzoekschrift op tegenspraak, en is slechts ontvankelijk na een onvruchtbare poging tot uitoefening van zijn rechten bij de houder van het bestand. De beschikkingen zijn uitvoerbaar bij voorraad, niettegenstaande hoger beroep of verzet.

Interessant zijn de bepalingen die aan de rechter de mogelijkheid verstrekken om bij eenvoudig verzoekschrift alle nodige maatregelen te gelasten ter voorkoming van de verdwijning of verdeling van bewijsmateriaal en die aan de verkrijger van betwiste persoonsgegevens de waarborg bieden van deze betwisting op de hoogte te worden gesteld door de verstrekker ervan (artikel 15 WVP).

6.4.5.2. Bij de CBPL (artikel 31 WVP)

In plaats van of naast de verhaalsmogelijkheid bij de rechtbank, kan de betrokkene aankloppen

bij de CBPL bij een vermeende schending van de bepalingen van de wet. De CBPL heeft immers de bevoegdheid klachten te onderzoeken, "onverminderd enige vordering voor de rechtbanken en tenzij de wet anders bepaalt"¹²⁸. Wie zich benadeeld voelt, is dus niet verplicht zich eerst tot de CBPL te richten alvorens naar de rechtbank te kunnen stappen. Evenmin doet hij door zich tot de CBPL te richten enige afbreuk aan de mogelijkheid om zich nadien tot de rechtbanken te kunnen wenden. De CBPL heeft immers geen jurisprudentiële bevoegdheid. Ze verstrekt enkel adviezen, die noch de betrokkene, noch de rechtbanken binden. De rechtbanken behouden ten volle hun bevoegdheid om de subjectieve rechten van de particulieren te behandelen.

De adviezen van de CBPL zullen niettemin een belangrijke morele waarde bezitten. Overigens is de procedure voor de indiening van een klacht bij de CBPL zeer soepel en gratis, en kan de CBPL een belangrijke bemiddelende rol vervullen, met als doel een minnelijke schikking tussen partijen neergelegd in een proces-verbaal.

6.5. DE COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER (ARTIKELEN 23 - 36 WVP)

6.5.1. Samenstelling van de CBPL

In 1983 werd bij het Ministerie van Justitie een Raadgevende Commissie voor de Bescherming van de Persoonlijke Levenssfeer ingesteld, bestaande uit personen aangesteld door diverse Ministers en met een beperkte bevoegdheid¹²⁹.

Naar aanleiding van de uitwerking van deze wet met algemene draagwijdte inzake eerbiediging van de privacy bij gegevensverwerking, werd ervoor geopteerd de bestaande Commissie op te heffen en te vervangen door een nieuwe met veel ruimere bevoegdheden, en ditmaal samengesteld uit leden die rechtstreeks worden aangewezen door het Parlement, om een maximale onafhankelijkheid te waarborgen.

De nieuwe Commissie voor de Bescherming van de Persoonlijke Levenssfeer bestaat uit zestien leden, aangeduid, voor een hernieuwbare termijn van zes jaar, door het Parlement uit dubbele lijsten voorgedragen door de Ministerraad. Voor elk mandaat wordt een effectief en plaatsvervangend lid aangewezen. De CBPL dient zodanig te worden samengesteld dat de verschillende

¹²⁸ In bepaalde maatschappelijke sectoren, zoals de sociale zekerheid, werd bij wet een specifiek Toezichtscmité ingesteld, dat m.b.t. die sector de behandeling ten gronde van klachten inzake gegevensbescherming behandelt. In deze gevallen wordt aan de CBPL evenwel een evocatierecht verleend m.b.t. de behandelde zaken, om een uniforme toepassing van de algemene principes inzake gegevensbescherming in alle sectoren te waarborgen. Zie, voor een nadere beschrijving van de verhouding tussen de CBPL en het Toezichtscmité bevoegd van de sociale zekerheid, ROBBEN, F., "De werking van de Kruispuntbank van de Sociale Zekerheid", *B.T.S.Z.*, 42.

¹²⁹ De Raadgevende Commissie was enkel bevoegd voor problemen met betrekking tot de bescherming van de persoonlijke levenssfeer bij de werking van twee gegevensbanken uit de openbare sector: het rijksregister en de (eigenlijk nooit van de grond gekomen) gegevensbank betreffende de personeelsleden van de overheidssector.

sociaal-economische groepen evenwichtig vertegenwoordigd zijn, en dat in haar schoot minstens één magistraat, één jurist, één informaticus, één persoon met ervaring inzake gegevensverwerking in de openbare sector en één persoon met ervaring inzake gegevensverwerking in de private sector zetelen. De leden moeten alle waarborgen bieden om hun opdracht op een onafhankelijke wijze te vervullen en bevoegd zijn op het vlak van informatiesystemen.

Daarnaast kunnen bepaalde personen die deel uitmaken van bijzondere Toezichtscomités ingesteld m.b.t. bepaalde sectoren van rechtswege lid zijn van de CBPL¹³⁰.

De CBPL wordt voorgezeten door een lid-magistraat, die zijn functie voltijds uitoefent. De andere mandaten zijn deeltijds.

Bijzondere waarborgen zijn voorzien opdat de leden van de CBPL hun taak in alle onafhankelijkheid zouden uitoefenen.

De werkingskosten van de CBPL worden gedragen door het Ministerie van Justitie.

6.5.2. Taken van de CBPL

De taken die de wet toebedeelt aan de CBPL zijn viervoudig.

In de eerste plaats dient de CBPL een openbaar register bij te houden van de geautomatiseerde verwerkingen, waarin de inlichtingen worden vermeld afkomstig uit de voorafgaande aangifte die de houder van dergelijke verwerkingen dient te verrichten (zie hoger, punt 3.5.1.). Indien zij van oordeel is dat een manueel bestand een mogelijke schending van de persoonlijke levenssfeer inhoudt, kan zij ook bepaalde informatie verzamelen m.b.t. dergelijk bestand.

In de tweede plaats dient de CBPL gemotiveerde adviezen te verstrekken over bepaalde ontwerpbesluiten ter uitvoering van de wet (artikelen 6, 7, 8 §§ 2 en 5, 9, 12, 13, 14, 17 § 8, 21 en 22 WVP) en kan ze uit eigen beweging of op verzoek van bepaalde instanties adviezen of aanbevelingen uitbrengen omtrent iedere aangelegenheid die betrekking heeft op de grondbeginselen van de bescherming van de persoonlijke levenssfeer (artikelen 29 § 1 en 30 § 1 WVP). Een aantal algemene rechtsbeginselen, zoals de plicht tot motivering van aanbevelingen en adviezen en het recht op verdediging van de persoon tegen wie klacht wordt ingediend, worden uitdrukkelijk gevrijwaard.

Ten derde treedt de Commissie op op verzoek van particulieren, hetzij als tussenpersoon voor de uitoefening van het recht op toegang, verbetering, verwijdering of niet-aanwending van gegevens m.b.t. gegevensverwerkingen door de administratieve en gerechtelijke politie, de Staatsveiligheid en de Militaire Veiligheidsdienst (artikel 13 WVP), hetzij tengevolge van een

¹³⁰ Op dit ogenblik zijn enkel de Voorzitter en één lid van het Toezichtsomité ingesteld door de Kruispuntbankwet van rechtswege lid van de CBPL.

klacht waarbij verhaal wordt in gesteld tegen een houder van een bestand (artikel 31 WVP).

Tenslotte wordt aan de CBPL ook de bevoegdheid toegekend om in bepaalde gevallen de termijn te verkorten waarbinnen de houder van een bestand geen gevolg dient te geven aan een verzoek van een persoon tot het bekomen van gegevens die hem betreffen (artikel 10 § 2 WVP).

De CBPL beschikt voor de uitvoering van haar opdrachten over ruime onderzoeksbevoegdheden en kan zich laten bijstaan door deskundigen (artikel 32 § 1 WVP).

Indien de CBPL bij de uitvoering van haar taken overtredingen van strafbepalingen vaststelt, dient ze hiervan in principe aangifte te doen bij het parket (artikel 32 § 2 WVP). Ook beschikt ze over de mogelijkheid om geschillen aanhangig te maken bij de burgerlijke rechtbank (artikel 32 § 3 WVP). Zij stelt tenslotte jaarlijks een activiteitenverslag op ten behoeve van het Parlement (artikel 32 § 2 WVP).

6.6. STRAFESANCTIES

De wet bevat uitvoerige strafsancties in geval van schending van de meeste van zijn bepalingen. Naast de klassieke straffen (gevangenisstraf en geldboete) worden ook specifieke straffen voorzien zoals de publicatie van een veroordeling in één of meer dagbladen, de verbeurdverklaring van de drager van persoonsgegevens, de uitwissing van gegevens of het verbod om gedurende maximum twee jaar het beheer te hebben van enige verwerking van persoonsgegevens.

6.7. BESLUIT

België heeft lang moeten wachten op een algemene reglementering inzake de bescherming van de persoonlijke levenssfeer t.a.v. de verwerking van persoonsgegevens. De internationale druk heeft uiteindelijk het besluitvormingsproces geactiveerd.

De uitgewerkte beschermingsregeling geldt t.a.v. elke verwerking van persoonsgegevens, ongeacht de gebruikte drager en in principe ongeacht de instantie die de verwerking uitvoert. Daarmee is het toepassingsgebied van de Belgische wet, samen met de Franse, het ruimste van Europa, en wordt nauw aangesloten bij de ontwerprichtlijn van de Europese Unie inzake privacybescherming t.a.v. gegevensverwerking¹³¹.

De gekozen beschermingstechnieken zijn klassiek en hebben meestal hun waarde in de ons omringende landen bewezen. Ze zijn in de wet slechts in zeer algemene termen beschreven. Er wordt veel ruimte gelaten aan de Koning om, meestal na advies van de CBPL, de beginselen te

¹³¹ Gewijzigd voorstel voor een richtlijn van de Raad betreffende de bescherming van natuurlijke personen in verband met de behandeling van persoonsgegevens en betreffende het vrije verkeer van die gegevens, Publicatieblad E.G., 27 november 1992, nr. C 311, 30.

concretiseren of uitzonderingen te bepalen.

De uiteindelijke doelstelling van de wet, namelijk het doen respecteren van het grondrecht op bescherming van de persoonlijke levenssfeer, wordt algemeen aanvaard. Sommigen hebben echter kritiek op de wijze waarop getracht wordt dit objectief te bereiken.

Men kan zich inderdaad omtrent een aantal aan de gegevensverwerkende instanties opgelegde verplichtingen de vraag stellen of de administratieve rompslomp die ze veroorzaken niet buiten verhouding staat tot de bijkomende beschermingswaarde die ze kunnen bieden. Het is evenwel mijn opinie dat mits een aangepast gebruik van de uitgebreide bevoegdheden die zijn toevertrouwd aan de Koning en de CBPL om de beginselen te concretiseren, een degelijk beschermingsniveau kan worden bekomen zonder nodeloos efficiëntieverlies of administratieve rompslomp voor de houders van bestanden.

Anderzijds dient de CBPL er ook over te waken dat de uitgebreide bevoegdheidsdelegaties aan de Koning niet worden misbruikt worden om de basisprincipes uit te hollen. Allicht ware het daarom beter geweest minder afwijkingsmogelijkheden te voorzien in de wet, maar voor de concretisering van de beginselen te opteren voor een systeem van gecontroleerde zelfregulering, waarbij de verantwoordelijkheidszin van de gegevensverwerkende instanties wordt gestimuleerd, en waarbij minder gevaren bestaan voor een erosie van de basisprincipes.

Uiteindelijk zal de effectief geboden bescherming in belangrijke mate afhankelijk zijn van de houding van de voornaamsta actoren: enerzijds de houders van de bestanden, die de verplichtingen vanuit een positieve ingesteldheid moeten benaderen, en anderzijds de geregistreerden, die hun rechten moeten uitoefenen, maar op een redelijke wijze. Het is aan de CBPL om op dit vlak gericht te sensibiliseren en het geboden instrumentarium doelgericht te doen inzetten. Daarbij zal selectiviteit in het optreden nodig zijn.

7. DE WET TER BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER TEGEN HET AFLUISTEREN, KENNISNEMEN EN OPNEMEN VAN PRIVÉ-COMMUNICATIE EN -TELECOMMUNICATIE

Voor de bespreking van deze wet wordt verwezen naar de mondelinge uiteenzetting tijdens de hoorcolleges.

Hoofdstuk 3 De bestrafing van informaticacriminaliteit

1. INLEIDING

Het zal niemand verwonderen dat van een krachtig instrument als de computer ook misbruik kan worden gemaakt. Specifieke gevallen van computermisbruik bereikten ook in ons land de aandacht van de persmedia. Iedereen herinnert zich wellicht nog de inbraak in het Bistel-netwerk door een vroegere medewerker van Premier Martens in 1988. Geregeld wordt in de media ook uitvoerig aandacht besteed aan "computervirussen" (Datacrime, Michelangelo, e.a.).

Men kan een onderscheid maken tussen twee soorten van informaticacriminaliteit:

- de informatica kan het middel zijn om een misdrijf te plegen (oplichting, diefstal, ...);
- de informatica kan het voorwerp zijn van het misbruik (computersabotage, softwarepiraterij, vernietiging van gegevens, ...).

Uiteraard kunnen beide vormen ook samen optreden (bv. oplichting via het vervalsen van computergegevens). In elk geval is het noodzakelijk om bij een computermisdrijf uit te gaan van een zeer precieze analyse met behulp van de bestaande categorieën van het strafrecht. Meer dan in andere rechtstakken is in het strafrecht elke vaagheid of analogie uit den boze. Dit volgt uit de stricte toepassing van het legaliteitsprincipe. Het behoort uitsluitend de wetgever toe om te bepalen welke gedragingen strafbaar dienen gesteld te worden. Analogische wetsinterpretaties die aanleiding zouden geven hetzij tot een uitbreiding van strafbaarheid, hetzij tot het verscherpen van de strafactie, zijn dus in het strafrecht niet toegelaten.

2. INFORMATICA, MIDDEL TOT HET PLEGEN VAN EEN MISDRIJF

Traditioneel wordt een onderscheid gemaakt tussen misdrijven tegen goederen en misdrijven tegen personen. Dit onderscheid is ook voor de analyse van informaticamisdrijven bruikbaar.

2.1. INFORMATICAMISDRIJVEN TEGEN GOEDEREN

Natuurlijk zijn er zeer vele misdrijven m.b.t. goederen, waarbij de informatica een "zekere" rol speelt. Iemand zou bijvoorbeeld een geldautomaat kunnen misbruiken om meer geld van zijn rekening te halen dan toegelaten (in zoverre dit ook technisch mogelijk zou zijn !). Door het Franse Hof van Cassatie werd dit niet als een strafbaar feit aanzien. Het Hof besliste dat een dergelijk misbruik te beschouwen is als een niet nakomen van een verbintenis door de cliënt t.o.v. de bank (Cass. crim. 24 november 1983).

Bij de "echte" informaticamisdrijven speelt de informatica echter niet een dergelijke marginale rol. Met informaticamisdrijven bedoelen we enkel de misdrijven waarbij het gebruik van informatica een determinerende en centrale rol speelt. Met behulp van informatica wordt bijvoorbeeld gepoogd zich andermans goed onrechtmatig toe te eigenen. Een bekend voorbeeld is de "salamitechniek" waarbij een informaticus van een financiële instelling ervoor zorgt dat bij

de berekening van de intresten, de afrondingen door de computer enkele tientallen centiemen lager verricht worden en de overschotten naar de rekening van de frauderende informaticus worden overgeschreven.

Een dergelijk feit kan men onder het Belgisch strafrecht niet als diefstal beschouwen. Artikel 461 SW vereist dat er een "bedrieglijke wegneming" zou zijn. Door sommigen wordt dit begrip zeer restrictief uitgelegd, in de zin van een "materiële" handeling van verplaatsing van de gestolen zaak. De opstellers van het Strafwetboek hebben inderdaad wellicht enkel aan tastbare goederen gedacht. Er is echter geen reden om ook andere lichamelijke goederen onder de toepassing van art. 461 SW te brengen, ook al zijn deze goederen niet waarneembaar via de tastorganen maar via andere zintuigen zoals het gehoor of het reukorgaan. Gas, electriciteit, radiogolven, e.d. kunnen daarom eveneens als lichamelijke goederen worden beschouwd, die het voorwerp kunnen zijn van diefstal. M.b.t. de diefstal van electriciteit werd dit expliciet door het Hof van Cassatie bevestigd (Cass. 23 september 1981, Pas., 1982, I, 120). De onrechtmatige creditering van een bankrekening, zoals in hogervermeld voorbeeld, is volgens de meeste strafrechtsgeleerden echter niet onder het begrip "wegneming van een lichamenlijk goed" te brengen. Hier is enkel sprake van een onlichamelijk goed, een recht dat niet het voorwerp kan zijn van een "wegneming" in de fysieke betekenis. Toch is er in de rechtspraak een evolutie merkbaar. In een arrest van 1979 heeft het Hof van Cassatie beslist dat de creditering van een bankrekening gelijk te stellen was met het bezit van een roerend goed in de zin van art. 508 SW (Cass. 16 mei 1979, Pas., 1979, I, 1081). Weliswaar heeft dit arrest enkel betrekking op de toepassing van art. 508 SW maar het wijst toch op een tendens in de richting van een gelijkenschakeling van kontante en girale geldoverdrachten (aldus Simont en Bruyneel, Rev. Banque, 1987, 47, nr. 27).

Minder betwist is echter de toepassing in dergelijke gevallen van het begrip "oplichting" (artikel 496 SW). Artikel 496 van het Strafwetboek bepaalt : "Hij, die met het oogmerk om zich een zaak toe te eigenen die aan een ander toebehoort, zich gelden, roerende goederen, verbintenissen, kwijtingen, schuldbevrijdingen doet afgeven of leveren, hetzij door het gebruik maken van valse namen of valse ondernemingen, van een denkbeeldige macht of van een denkbeeldig krediet, om een goede afloop, een ongeval of enige andere hersenschimmige gebeurtenis te doen verwachten of te doen vrezen of om op andere wijze misbruik te maken van het vertrouwen of van de lichtgelovigheid, wordt gestraft met gevangenisstraf van één maand tot vijf jaar en met een geldboete van zesentwintig frank tot drieduizend frank. (...)".

Voor een groot aantal misdrijven waarbij de computer gebruikt wordt om zich een vermogensvoordeel te verschaffen, biedt de kwalificatie van oplichting in de zin van artikel 496 een oplossing. De manipulatie van de computer heeft hier tot doel zich een zaak toe te eigenen die aan een ander toebehoort, door het zich doen afgeven van geld. Het feit dat de afgifte van de zaak veelal zal geschieden door overschrijving van geld, levert hierbij geen moeilijkheid op. In het reeds aangehaalde arrest van 16 mei 1979 besliste het Hof van Cassatie dat de inschrijving van een som op de creditzijde van een rekening gelijkstaat met het verkrijgen van een roerende zaak. Het misdrijf van oplichting vereist dus geen materiële overhandiging. De wijziging of vervalsing van computergegevens kan beschouwd worden als een listige kunstgreep.

De toepassing van "oplichting" i.v.m. frauduleuze girale overschrijvingen wordt in elke geval aanvaard door de hoogste rechters in Frankrijk (Cass. crim. 17 oktober 1967, Bull. n° 252) en Nederland (Hoge Raad, 11 mei 1982, N.J., 1982, 583).

Voor dit soort "computerdelicten" is dus geen supplementaire wetgeving nodig.

Het gebruik van andermans elektronische bankkaart en code om zich geld toe te eigenen kan eveneens onder de kwalificatie van oplichting worden gebracht (zie hierover G. Demanet, "De l'utilisation frauduleuse des cartes bancaires: une nouvelle incrimination, est-elle nécessaire?", R.D.P.C., 1985, 915). Vaak wordt ook "inbraak met het gebruik van valse sleutels" als kwalificatie gebruikt. Het bedrieglijk wegnemen van de bankkaart op zichzelf is natuurlijk een gewoon geval van diefstal.

2.2. INFORMATICAMISDRIVEN TEGEN PERSONEN

Ook bij de misdrijven tegen personen zijn er tal van misdrijven waarbij de informatica in zekere zin als medium wordt gebruikt. Men denkt bijvoorbeeld aan de openbare schennis van goede zeden door het verspreiden van obscene advertenties in de "messageries roses" van het Franse Minitelsysteem. De computer speelt hier geen specifieke rol doch is enkel een (neutraal) medium. Dergelijke a-specifieke delicten rangschikken we niet bij de informaticadelicten.

Specifieke informaticadelicten tegen personen vinden we daarentegen wel omschreven in bijvoorbeeld de wetgeving over de bescherming van de persoonlijke levenssfeer bij de verwerking van persoonsgegevens.

In de artikelen 37 e.v. van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer (zie hoger) vinden we o.m. volgende misdrijven opgesomd:

- schending van de verplichting tot vertrouwelijkheid door een lid van de Commissie voor de bescherming van de persoonlijke levenssfeer of door een deskundige;
- schending van de plichten i.v.m. het beheer over de verwerking van persoonsgegevens door de houder van het bestand (opmaken van een staat, accuraatheid van de gegevens, vertrouwelijkheid, enz.);
- het verzamelen, van persoonsgegevens zonder de betrokken persoon daarover in te lichten;
- het verwerken van gevoelige, medische gegevens of gerechtelijke gegevens buiten de wettelijk toegelaten gevallen;
- het weigeren van inzage- en correctierecht aan de personen waarvan de gegevens worden verwerkt;
- het nalaten de bij een verwerking van persoonsgegevens vereiste opgave te doen bij de Commissie voor de bescherming van de persoonlijke levenssfeer.

Er dient ook opgemerkt dat de wet van 8 december 1992 naast de klassieke straffen - gevange-

nisstraf en geldboete - ook in andere straffen voorziet:

- publicatie van de veroordeling in één of meer dagbladen;
- verbeurdklaring van de dragers van persoonsgegevens (magneetschijven, magneetbanden, enz.);
- uitwisseling van de gegevens;
- verbod om gedurende maximum twee jaar het beheer te hebben over enige verwerking van persoonsgegevens.

3. INFORMATICA, VOORWERP VAN EEN MISDRIJF

Informatica kan ook het "voorwerp" zijn van een misdrijf: er kan "ingebroken worden in een computer, gegevens kunnen vernield of vervalst worden, virusprogramma's kunnen verspreid worden, enz.

Wellicht maakt men best een onderscheid tussen misdrijven m.b.t. computerapparatuur (hardware), misdrijven m.b.t. programmatuur en misdrijven m.b.t. computergegevens. Elk van deze drie elementen kan het voorwerp zijn van een reeks specifieke handelingen: ontvreemding, binnendringing, sabotage en vervalsing. Begrippen als "ontvreemding", "binnendringing", ... zijn uiteraard geen strafrechtelijke termen. Ze worden echter hier met opzet geïntroduceerd om op de strafrechtelijke kwalificatie van verschillende feitelijke handelingen niet te anticiperen.

3.1. ONTVREEMDING

Zoals vermeld kunnen zowel apparaten als programma's en gegevens ontvreemd worden.

3.1.1. Apparatuur

Ontvreemding van apparatuur kan drie vormen aannemen:

- het kan gaan over ontvreemding van apparatuur als intellectuele creatie, bijvoorbeeld een inbreuk op het recht van de houder van een uitvindingsoctrooi (zie bv. art. 53 van de Octrooiwet van 28 maart 1984) of een inbreuk op art. 14 van de Chipswet van 10 januari 1990;
- het kan ook gaan over ontvreemding van het fysische apparaat zelf, bijvoorbeeld diefstal (want bedrieglijke wegneming van een lichamelijk en zelfs tastbaar goed) van een computer of een printer; eventueel kan het hier ook gaan om "gebruiksdiefstal", wanneer de computer of de printer bedrieglijk wordt weggenomen voor kortstondig gebruik, en nadien wordt teruggeplaatst;
- het kan tenslotte gaan over ontvreemding van computertijd (bv. als men met andermans paswoord een mainframecomputer gebruikt); men kan dan, naar analogie met de diefstal van electriciteit van diefstal spreken, hoewel dit een nogal oneigenlijke aanpak zou zijn: de daders hebben namelijk niet het wegnemen van energie op het oog; in de huidige stand van het strafrecht is het daarom misschien beter om het tweede lid van art. 461 SW ("gebruiksdiefstal") in te roepen: "Met diefstal wordt gelijkgesteld het bedrieglijk

wegnemen van andermans goed voor kortstondig gebruik"; ook deze kwalificatie is echter gebrekkig omdat degene die computertijd ontvreemdt, de computer niet voor kortstondig gebruik "wegneemt"; de computer wordt weliswaar kortstondig onrechtmatig gebruikt, maar hij blijft op zijn plaats staan.

3.1.2. Programma's

Ontvreemding van programma's kan twee vormen aannemen:

- ontvreemding van de drager, bijvoorbeeld het tijdelijk wegnemen van een diskette om ze te kopiëren; hier kan de kwalificatie van gebruiksdiefstal gebruikt worden;
- ontvreemding van het programma als intellectuele creatie, bijvoorbeeld door het programma te "klonen": dergelijke delicten vallen onder de strafbepalingen van de auteurswet (misdrijf van namaking, art. 80 e.v.).

De toepasselijkheid van de strafbepalingen van de auteurswet is echter afhankelijk van de toepasselijkheid van de auteurswet zelf; een misdrijf i.v.m. een programma dat bijvoorbeeld niet aan de originaliteitsvereiste van de auteurswet voldoet, wordt hiermee niet bestraft. Vaak moet dus naar andere kwalificaties worden gezocht.

Voor de correctionele rechtbank te Brussel werd een verdachte vervolgd wegens misbruik van vertrouwen ten nadele van een zelfstandige informaticus die in de lokalen van de verdachte een boekhoudprogramma had ontwikkeld voor de verdachte. Na een geschil tussen beiden, werd de informaticus aan de deur gezet en liet de verdachte het programma verder ontwikkelen door iemand anders. Weliswaar ging de aanklacht over de programmadiskettes, die de informaticus niet had kunnen recupereren. De rechtbank besliste dat niet bewezen was dat die diskettes aan de informaticus toebehoorden. In een obiter dictum zegt de rechtbank echter dat de verdachte "niet alleen het basisprogramma en de programma's in ontwikkeling gehouden heeft en ze ten zijnen voordele heeft aangewend zonder ervoor te betalen, maar ook programma's toebehorende aan de burgerlijke partij heeft vernietigd" (Corr. Brussel, 16 december 1987, onuitg.). Dit vonnis werd door het Hof van Beroep te Brussel bevestigd (Brussel, 21 november 1990, onuitg.).

Het Hof van Beroep te Antwerpen (Antwerpen, 13 december 1984, R.W., 1985-86, 244) paste de kwalificatie van diefstal toe op de ontvreemding van drie softwarepakketten, voor de boekhouding van een eerste bedrijf, voor de facturatie en het voorraadbeheer van een tweede bedrijf en voor het productiebeheer van een derde bedrijf. De verdachte, die ontslagen was als beheerder van de softwareproducent, had die softwarepakketten gecopieerd. Bovendien had hij een copie bezorgd aan een ex-collega die eveneens was ontslagen. Het Hof van Beroep heeft in deze zaak een zeer vooruitstrevende uitlegging gegeven aan art. 461 SW (diefstal), en meer bepaald aan het begrip "wegneming van een zaak". Daarvoor is het Hof ervan uitgegaan dat de betrokken softwarepakketten een onderdeel uitmaakten van het vermogen van de burgerlijke partij. Volgens het Hof is software weliswaar in de eerste plaats een geheel van instructies, intrinsiek van intellectuele aard en van nature ontastbaar en dus niet voor fysische wegneming vatbaar, maar kan ze niettemin worden overgedragen en gereproduceerd en heeft ze een

economische waarde. Deze interpretatie is door sommige penalisten toegejuicht (o.m. door R. Verstraeten, R.W., 1985-86, 215; door Mercx en Vandeplas, R.D.C., 1988, 93; door J.P. Spreutels, R.D.P., 1991, 1041) maar ook door velen verguisd. De Antwerpse rechters hebben in elk geval navolging gekregen. Dat gebeurde o.m. in een arrest van het Hof van Beroep te Brussel (Brussel, 5 december 1986, Dr. Inform., 1987/1, 53). Daarbij ging het over een werknemer die bij zijn werkgever een aantal computerprogramma's had gecopieerd met de bedoeling ze te gebruiken bij het opstarten van een concurrerende firma.

Naast de verruiming van het begrip "zaak", hanteren de hierboven aangehaalde arresten ook een ruimere definitie van "wegneming". Daaronder wordt niet noodzakelijk meer een "fysische verplaatsing" verstaan, doch eerder "het zich toeëigenen wat een ander toebehoort" (aldus de definitie van "wegneming" in het Van Dale Woordenboek). Daarbij is het niet relevant dat, bij het bedrieglijk kopiëren van een softwarepakket, de eigenaar in het bezit blijft van het originele exemplaar (contra: Corr. Verviers, 4 oktober 1989, J.L.M.B., 1990, 709).

3.1.3. Gegevens

Voor de ontvreemding van gegevens gelden mutatis mutandis dezelfde principes als voor de ontvreemding van programmatuur. Ook hier moet men een onderscheid maken tussen de ontvreemding van de drager en de ontvreemding van de intellectuele creatie. De mogelijkheid om ook hier eventueel een beroep te doen op de strafbepalingen van de auteurswet sluit niet uit dat naar andere strafrechtelijke kwalificaties moet worden gezocht. Daarom pleiten sommige auteurs voor de toepassing van "diefstal" als kwalificatie (zie o.m. J.P. Spreutels, "Le vol de données informatiques, R.D.P.C., 1991, 1027). Deze opvatting vindt men ook terug in de rechtspraak, o.m. in een arrest van het Hof van Beroep te Brussel (Brussel, 10 mei 1989, Pas. 1990, I, 1). In dit arrest ging het over een zelfstandige informaticus die in de computer van zijn opdrachtgever, waarvoor hij een softwarepakket moest ontwikkelen, ook een aantal gegevens had ingevoerd. Na een geschil met zijn opdrachtgever wiste de informaticus de ingevoerde gegevens, na ze vooraf op een schijf van de opdrachtgever gecopieerd te hebben en deze schijf vervolgens verborgen te hebben. Het Hof oordeelde dat het hier om "diefstal van gegevens" (en niet alleen van de dragers) ging en beriep zich daarbij expliciet op de evolutieve uitlegging van het begrip "zaak" in de zin van art. 461 SW. Tegen het arrest werd cassatie aangetekend maar de voorziening werd verworpen zonder dat het Hof op dit punt stelling nam (Cass. 8 mei 1990, A.R. nr. 3578).

Het Franse Hof van Cassatie velde over deze problematiek een zeer belangrijk principe-arrest (Cass. crim. 12 januari 1989, Bull. crim. n° 14), waarin het eveneens oordeelde dat computergegevens het voorwerp konden zijn van diefstal.

3.2. BINNENDRINGING

Eén van de meest bekende informaticadelicten is het "kraken" van computersystemen. In België is het momenteel zeer moeilijk om dergelijk misbruik onder een bestaande strafrechtelijke

kwalificatie te brengen. Doorgaans wordt hier dan ook gepleit voor de opname in het strafwetboek van nieuwe incriminaties, zoals is gebeurd in het kader van de Kruispuntbankwet (artikelen 61, 11° en 63, 8°).

In België kwam de strafrechtelijke discussie over deze vorm van misdrijf in de openbaarheid n.a.v. de "Bistel"-zaak. "Bistel" is de naam van een netwerk dat door de Belgische overheid wordt gebruikt voor o.m. het versturen van elektronische berichten, vergaderagenda's, toegang tot databanken e.a. Een oud-medewerker van de Eerste Minister en een medeplichtige hadden diens toegangscode en paswoord gebruikt om onrechtmatig in het netwerk binnen te dringen. De eerste betichte had gezorgd voor de telefoonnummers, de toegangscode en de paswoorden. De tweede betichte had zijn personal computer en zijn modem ter beschikking gesteld. Tot hun eigen verbazing slaagden de betichten erin zonder enige moeilijkheid in het systeem binnen te dringen. Enige tijd daarna maakten zij dit voorval zelf aan de pers bekend.

Voor de correctionele rechtbank werden aan de betrokkenen vier misdrijven ten laste gelegd:

- valsheid in geschriften, door het gebruiken van andermans toegangscode en paswoord, derwijze dat ze zich voordeden als de werkelijke titularissen van de toegangscode en het paswoord;
- diefstal door middel van braak, inklimming of valse sleutels van een onbepaalde hoeveelheid "computerenergie";
- verduistering van een aan de RTT toevertrouwde mededeling;
- schade aan andermans gebouw, kunstwerk of bouwwerk, in casu het elektronisch communicatiesysteem van de Belgische Staat.

De correctionele rechtbank (Corr. Brussel 8 november 1990, J.T., 1990, 11) veroordeelde de twee betichten in de eerste plaats wegens valsheid in geschriften. De rechtbank hanteerde daarbij een extensieve interpretatie van het begrip "geschrift" en oordeelde dat het intikken van een paswoord gelijkgeschakeld kon worden met een geschrift. Deze interpretatie werd door het Hof van Beroep (Brussel, 24 juni 1991) verworpen. Het Hof besliste "dat het introduceren, zelfs op ongeoorloofde wijze, van een paswoord in het Bistelsysteem derelijke vervalsing (van een geschrift) niet uitmaakt en dat het door beklaagden gebezigde paswoord in de vorm van een elektronische code geen geschrift, meer bepaald geen grafisch tekensysteem uitmaakt in de zin van de artikelen 193 e.v.". Bovendien constateerde het Hof dat in casu ook niets werd "vervalst".

De correctionele rechtbank veroordeelde de twee betichten in de tweede plaats wegens "diefstal van computerenergie", doch ook deze beslissing werd door het Hof van Beroep hervormd.

Volgens het Hof hadden de beklaagden niet de bedoeling om computerenergie te ontvreemden en ontbrak het dus aan het voor diefstal vereiste intentionele element. Het is daarbij belangrijk dat het Hof niet besliste dat energie niet voor diefstal in aanmerking kan komen.

Zowel de correctionele rechtbank als het Hof van Beroep behielden de derde tenlastelegging (verduistering van een aan de RTT toevertrouwde mededeling) en verwierpen de vierde

tenlastelegging (schade aan een gebouw of kunstwerk). De twee beklaagden werden dus uiteindelijk veroordeeld wegens overtreding van de RTT-wet van 1930. Deze wet is momenteel vervangen door de wet van 21 maart 1991 op de economische overheidsbedrijven. De artikelen 111 en 112 van die wet handelen over het geheim van telecommunicatieberichten. Artikel 111 bepaalt dat het verboden is om zelf of door toedoen van een derde:

- met bedrieglijk opzet kennis te nemen van het bestaan van telecommunicatieberichten, die herkomstig zijn van én bestemd zijn voor andere personen;
- met bedrieglijk opzet deze telecommunicatieberichten met gelijk welk technisch procédé te wijzigen of weg te laten of de andere personen te identificeren;
- met opzet kennis te nemen van gegevens inzake telecommunicatie, die betrekking hebben op een andere persoon;
- de gegevens die met of zonder opzet werden bekomen, kenbaar te maken, te gebruiken, te wijzigen of te vernietigen.

Artikel 112 laat op het bovenstaande verbod uitzonderingen toe:

- wanneer de wet het toelaat of oplegt;
- wanneer de verboden handelingen worden gesteld ten behoeve van de verzorging van een telecommunicatiedienst.

Bovendien werd medio 1994 een wet ter bescherming van de persoonlijke levenssfeer tegen het af luisteren, kennisnemen en opnemen van privé-communicatie en -telecommunicatie uitgevaardigd (zie hoger).

De hierbovenvermelde bepalingen kunnen echter alleen worden toegepast indien gebruik gemaakt wordt van telecommunicatiemiddelen.

Naargelang de situatie van de binnendringing, zouden nog andere strafbepalingen in aanmerking kunnen komen. Zo bijvoorbeeld misbruik van vertrouwen (artikel 491 Sw.) de schending van het briefgeheim (artikel 460 Sw.).

Het is echter duidelijk dat, wil men de binnendringing in computers op basis van de bestaande strafbepalingen strafbaar stellen, enkel een ruime analogische interpretatie van de bepalingen kan helpen. En dit terwijl de strafwet, zoals reeds vermeld, als van stricte interpretatie moet worden beschouwd. Overigens zijn scenario's van binnendringing in computers denkbaar waar de bestaande strafbepalingen volledig lijken te falen.

Daarom lijkt het nodig om, net zoals in vele andere landen, ook in België de strafbaarheid van ongeoorloofde computerinbraak expliciet in de algemene strafwet in te lassen. Buitenlandse voorbeelden kunnen daarvoor nuttig zijn.

In Frankrijk bepaalt artikel 462-2 van de wet van 5 januari 1988 : "Ieder die zich bedrieglijk toegang verschaft of die toegang behoudt tot het geheel of een deel van een geautomatiseerd systeem voor gegevensverwerking, wordt gestraft met een gevangenisstraf van twee maanden

tot één jaar en een boete van 2.000 tot 50.000 frank of met één van deze beide straffen".

Ook in Nederland werd einde 1992 een Wet Computercriminaliteit uitgevaardigd, die een bepaling bevat die luidt als volgt: "Met gevangenisstraf (...) of geldboete (...) wordt, als schuldig aan computervrederebreuk, gestraft hij die opzettelijk wederrechtelijk binnendringt in een geautomatiseerd werk voor de opslag of verwerking van gegevens, of in een deel daarvan, indien hij a. daarbij enige beveiliging doorbreekt of b. de toegang verwerft door een technische ingreep, met behulp van valse signalen of een valse sleutel dan wel door het aannemen van een valse hoedanigheid."

3.3. SABOTAGE EN VERVALSING

Het opzettelijk vernietigen en/of beschadigen van andermans goed wordt algemeen als een misdrijf aangevoeld en ressorteert dan ook in de meeste landen onder de vigerende strafbepalingen.

Dat wil echter niet zeggen dat er in dit verband geen problemen rijzen. In dit verband moet een onderscheid worden gemaakt tussen sabotage, vernieling, beschadiging of vervalsing van materiële zaken enerzijds en van immateriële zaken (programma's en gegevens) anderzijds. Bij deze laatste categorie horen ook de zogenaamde computervirussen thuis.

3.3.1. Materiële zaken

Sabotage, vernieling en beschadiging van computers en telecommunicatiesystemen zullen in bepaalde gevallen ressorteren onder artikel 528 Sw. Dat artikel bepaalt dat "elke vernieling, elke beschadiging van andermans eigendommen, gepleegd met behulp van geweld of bedreiging, wordt gestraft ...". Een wezenlijke beperking van artikel 528 is evenwel dat het geweld of de bedreiging moet gericht zijn tegen personen en dat er een causaal verband moet zijn tussen het geweld en de vernieling.

Misschien is ook artikel 523 Sw. van toepassing. Dit artikel bestraft de vernieling van een machine die aan een ander toebehoort en "die bestemd is voor voortbrenging, omzetting of verdeling van drijfkracht of voor het verbruik ervan voor andere dan huishoudelijke doeleinden". Deze bepaling lijkt ons echter moeilijk op computers en ander informaticamaterieel toepasbaar.

Natuurlijk is er ook nog artikel 559, 1° Sw., waarin, in het algemeen, opzettelijke beschadiging of vernieling van andermans roerende eigendom wordt bestraft. Deze incriminatie is echter slechts een overtreding en de strafmaat (boete van tien frank tot twintig frank) werkt niet zeer afschrikkend.

3.3.2. Immateriële zaken

Indien we te maken hebben met het opzettelijk vernietigen, wijzigen, beschadigen of

manipuleren van andermans programma's en gegevens, zijn de problemen om een adekwate strafrechtelijke kwalificatie te vinden, veel groter.

Soms wordt gedacht aan de mogelijkheid om dergelijke misdrijven als valsheid in geschriften te aanzien, doch dit lijkt niet altijd gemakkelijk te verdedigen. We staan dus ook op dit punt voor een lacune.

In Frankrijk voorziet de wet van 5 januari 1988 speciale straffen voor het geval dat een computerinbraak resulteert in hetzij een vernietiging of wijziging van gegevens in het systeem, hetzij een wijziging in de werking van het systeem zelf. Ook onvrijwillige beschadiging is dus strafbaar als die het gevolg is van een bedrieglijke computerinbraak. Voor vrijwillige beschadiging gelden afzonderlijke en zwaardere straffen.

4. EEN VOORONTWERP IN DE MAAK

België heeft dringend nood aan specifieke strafrechtelijke bepalingen voor de vervolging van computerfraude. Nieuwe bepalingen zijn minder nodig voor gevallen waarbij informatica enkel het middel is voor het plegen van het misdrijf. Voor gevallen waarin de informatica het voorwerp van de fraude vormt, zijn er duidelijke lacunes.

Momenteel wordt er aan een voorontwerp gewerkt. Het betreft enkel een aantal incriminaties die terug te vinden zijn in de minimumlijst van OESO en Raad van Europa. Drie punten dienen daarbij aangestipt :

- er wordt geopteerd voor integratie in het strafwetboek zelf; dit biedt de mogelijkheid om aansluiting te zoeken bij bestaande beschermende belangen (zoals openbare orde, openbare trouw, vermogen) en de proliferatie van bijzondere wetten tegen te gaan; eenzelfde beweegreden stond voor ogen bij het uitwerken van het ontwerp over de af luistering; bovendien kan aldus worden voorkomen dat door het toenemend belang van informatica, centrale begrippen (vervalsing, oplichting, vernieling) uit het Strafwetboek door de nieuwe technologische mogelijkheden worden uitgehold;
- overcriminalisering wordt vermeden; het lijkt niet aangewezen bepaalde feiten, zoals het louter manipuleren van gegevens op zich, of de ongeoorloofde toegang zonder meer, strafbaar te stellen; uit de minimumlijst werden de zwaarste vormen van informaticamisbruiken strafrechtelijk beteugeld;
- strenge straffen worden voorzien; dit is een logisch gevolg van de gedane selectie; men stelt alleen de zwaarste vormen strafbaar en verbindt daaraan strenge straffen, vooral op het vlak van de geldboete; deze redenering is ingegeven door het feit dat vooral het dissuasieve effect moet spelen: de vattingsmogelijkheid is klein, daarom moet de straf hoog liggen.

Het ontwerp zal in volgende incriminaties voorzien:

- de valsheid in informatica;
- het informaticabedrog of -fraude;

- informaticasabotage;
- de ongeoorloofde toegang.

De eerste drie incriminaties betreffen vormen van computermanipulatie, met telkens een andere bijzondere doelstelling; de laatste betreft een vorm van informaticaspionage.

4.1. VALSHEID IN INFORMATICA

Het betreft een specifieke vorm van computermanipulatie waarbij geïnformatiseerde gegevens op duurzame wijze zodanig worden veranderd dat een vervalsing wordt gerealiseerd. Teruggevallen wordt op de bestaande bepalingen van het strafwetboek. De artikelen 193 e.v. van het SWB blijven dus van toepassing. at zonder de computer een geschrift is, is dat ook op de computer. De wet zal bepalen dat een geschrift uitgedrukt of vastgelegd op een "geïnformatiseerde drager" wordt beschouwd als een geschrift.

4.2. INFORMATICABEDROG

Met de toevoeging van een artikel 426bis in het SWB wordt in feite een geïnformatiseerde versie van het misdrijf oplichting beoogd. Het opzettelijk manipuleren van geïnformatiseerde gegevens met de bedoeling te frauderen, wordt strafbaar gesteld.

4.3. INFORMATICASABOTAGE

Met informaticasabotage wordt bedoeld kwaadwillig vernielen van computersystemen, netwerken, programma's, enz. Het is daarbij zelfs mogelijk om gegevens, databanken, of software te beschadigen of te wissen zonder dat materieel schade wordt toegebracht aan de computerapparatuur zelf. Uiteindelijk gaat hier om sabotagedaden tegen immateriële goederen. Hierdoor wordt evenwel geraakt aan de moeilijke problematiek van het juridisch statuut van deze gegevens en programma's. Zijn ze vatbaar voor eigendom in de klassieke zin ? Wat met het vrij verkeer van informatie ? De intellectueelrechtelijke discussies dienaangaande (auteursrechten, octrooien, sui generis, ...) zijn echter nog in volle ontwikkeling.

Het voorontwerp beoogt daarom enkel de strafrechtelijke beteugeling van elke bedrieglijke sabotagedaad : van het gewoonweg kapotslaan met een hamer van een PC tot het inbrengen van een virus (art. 525bis SWB).

4.4. ONGEOORLOEFDE TOEGANG

Het voorontwerp beschouwt dit als een misdrijf tegen de openbare orde en stelt voor een nieuw hoofdstuk VIII-bis in te voegen over: "Misdrijven betreffende de telecommunicatie en informatica" (art. 314 bis e.v.). Niet elke vorm van ongeoorloofde toegang moet worden strafbaar gesteld. Om tot hacking te komen is het vereist dat bepaalde beveiligingssystemen worden doorbroken. Ook het bedrieglijk opzet is determinerend.

Hierboven was reeds sprake over het afluisteren en onderscheppen van gesprekken en mededelingen. Dit is in feite een bijzondere vorm van ongeoorloofde toegang. De artikelen in kwestie zullen in het SWB in dit hoofdstuk worden ondergebracht.

Vooraf zal een bepaling worden ingelast die het bedrieglijk binnendringen zonder meer zal strafbaar stellen, ongeacht de aanwending van de "ontdekte gegevens" en ongeacht de "schade". Dit alles kan geen afbreuk doen aan de gemeenrechtelijke regels inzake spionage en schending van het geheim die van toepassing blijven ook al is die inbreuk gepleegd met behulp van de informatica.

Hoofdstuk 4 Informatica en contractenrecht

1. INLEIDING

Onder het begrip informaticacontracten (in ruime zin) verstaan we in deze cursus alle contracten die te maken hebben met informatica. Deze contracten kunnen gesloten worden door privé-personen (bv. de aankoop van een personal computer), door bedrijven (bv. een contract voor de uitvoering van een automatiseringsproject) of door de overheid (bv. de aankoop van hardware en software voor de automatisering van de verkiezingen). Aan de andere zijde staat in de regel een informaticabedrijf. Bij het overzicht van de informaticamarkt zagen we reeds dat informaticabedrijven leveranciers zijn van computerapparatuur, computerprogrammatuur en/of informaticadiensten. De waaier van informaticadiensten is zeer breed: expertise, studie, organisatie, ontwikkeling, analyse, communicatie, personeel, beveiliging, verzekering, financiering, onderhoud, opleiding, informatievoorziening, e.a.

Informaticabedrijven sluiten niet alleen overeenkomsten met particulieren, met andere (niet-informaticabedrijven) of met de overheid. Tal van overeenkomsten worden ook tussen informaticabedrijven gesloten: tussen producenten en verdelers (bv. distributiecontracten), tussen producenten onderling (bv. samenwerkingscontracten) of tussen verdelers onderling (bv. franchisecontracten).

Bij grotere automatiseringsprojecten zijn meestal meer dan twee partijen betrokken. Zoals bij een bouwproject is er vaak een bedrijf dat een voorstudie verricht, een ander bedrijf kan belast worden met de analyse, nog een ander bedrijf met de softwareontwikkeling, een ander bedrijf met de levering van de apparatuur, een ander bedrijf met de kwaliteitscontrole, enz. Daarom wordt vaak, net zoals in de bouwsector, een promotor ingeschakeld die het project coördineert.

Hierna bespreken we enkele juridische vraagstukken m.b.t. informaticacontracten. Eerst behandelen we inhoud van het meest voorkomende informaticacontract, nl. het contract voor de levering van computerapparatuur en/of -programmatuur. We noemen dit het "informatica-uitrustingscontract" of het informaticacontract in enge zin. Vervolgens komt het probleem van het bewijs aan bod. Het bewijsrecht stelt niet zozeer een probleem voor informaticacontracten in hogervermelde betekenis. Het vraagstuk duikt vooral op wanneer contracten (van eender welke aard) met behulp van moderne informatie- en telecommunicatietechnieken worden gesloten. Het volgende onderwerp is dan wel weer typisch voor informaticacontracten in enge zin (contracten over informatica). Het betreft het vraagstuk van de continuïteit. Een automatiseringsproject doet meestal een voortdurende relatie tussen de partijen ontstaan. Wie een computerprogramma laat ontwikkelen, zal blijvend de ontwikkelaar nodig hebben om het programma in stand te houden, aan te passen aan gewijzigde omstandigheden of aan nieuwe interfaces, enz. De vraag is dan hoe men zich van deze continuïteit juridisch kan verzekeren.

Tenslotte moet ook nog iets gezegd worden over de oplossing van informaticageschillen.

Met deze keuze van onderwerpen wordt zeker geen volledigheid beoogd. Belangrijke

vraagstukken m.b.t. informaticacontracten komen in deze cursus niet aan bod. Graag hadden we bv. ook de problemen van (producten- en diensten-)aansprakelijkheid bij informaticacontracten, de toepassing van de wetgeving op de handelspraktijken in de informaticasector, overheidsinformaticacontracten, overeenkomsten m.b.t. de informatiemarkt, e.d. behandeld. Wegens het tijdsgebrek werden deze onderwerpen hier voorlopig buiten beschouwing gelaten.

2. HET INFORMATICONTRACT IN ENGE ZIN

Onder informaticacontracten in enge zin verstaan we contracten die de levering van computerapparatuur en/of -programmatuur tot voorwerp hebben. Het gaat dus over een contract tussen een informaticabedrijf en zijn klant (particulier, bedrijf, overheidsinstelling).

Bij de informaticacontracten in enge zin onderscheiden we twee grote categorieën: standaardcontracten en contracten "ad hoc".

2.1. STANDAARDCONTRACTEN

Wie als particulier een computer en een softwarepakket koopt, krijgt uiteraard te maken met een standaardcontract. Hierna wordt enkel in het kort het standaard-softwarecontract behandeld.

Voor de verkoop van standaard-softwarepakketten wordt bijna steeds de techniek van de "shrink-wrap" licentie gebruikt. De diskettes waarop de programma's en de erbijhorende bestanden staan, zitten samen met de documentatie in een verpakking. Meestal zijn de diskettes nog eens afzonderlijk verpakt in een enveloppe. De enveloppe met de diskettes is verzegeld of er zit folie rond. In grote letters staat er in het Engels op gedrukt: "IMPORTANT: READ THIS LICENCE AGREEMENT BEFORE OPENING THE SEALED DISK PACKAGE. BY OPENING THE PACKAGE, YOU AGREE TO BE BOUND BY THE TERMS OF THE AGREEMENT". Daaronder kan men dan in kleine lettertjes de licentievoorwaarden voor het programma lezen.

De softwarefabrikant gaat er bij dit systeem van uit dat hij met de eindgebruiker een overeenkomst sluit vanaf het moment dat deze de krimpfolie rond de enveloppe met de diskettes openscheurt. Daarom wordt de "shrink-wrap" licentie soms in het Nederlands vertaald als "krimpfoliescheurovereenkomst".

Er bestaan enkele varianten op dit systeem. Sommige softwareproducenten (Borland bv.) plaatsen op de verzegelde enveloppe met de programmadiskettes een bericht waarin de koper aangemaand wordt om een ingevulde en ondertekende "licentiekaart" terug te sturen: "If you or your employee have not signed the attached Licence Agreement by which you expressly agree to respect the following Borland's software using conditions, you can't use this software without infringing the copyrights of Borland".

Welke bepalingen vindt men dan in deze zogenaamde "licentiecontracten" ? De belangrijkste bepalingen betreffen:

- het recht om de software te gebruiken op één computer;
- de wijze waarop de software mag gebruikt worden in een netwerk (meestal wordt het gebruik beperkt tot één gelijktijdige gebruiker);
- het verbod om de software te verhuren;
- het recht om één of meer veiligheidscopies te maken;
- het verbod om iets aan de software te veranderen;
- een garantieperiode (meestal 2 à 3 maanden) tijdens dewelke men voor defecte programmadiskettes of foutieve programma's vervanging mag vragen;
- een exoneration ten voordele van de softwareproducent t.a.v. alle mogelijke schade die uit het gebruik van de software zou voortvloeien;
- de bevoegde rechtbank bij eventuele geschillen.

Is de "shrink-wrap" licentie echter een geldige overeenkomst ? Is hier m.a.w. sprake van een wilsovereenstemming tussen de softwareproducent en de eindgebruiker ? Van een wilsovereenstemming kan slechts sprake zijn als ze tot stand is gekomen door een aanbod (van de softwareproducent) en de aanvaarding daarvan (door de eindgebruiker). Aan aanbod en aanvaarding worden geen vormvereisten gesteld. Wél moeten ze beide op een waarneembare en begrijpelijke wijze geschieden. Het aanbod komt ook pas tot stand als het degene, voor wie het is bestemd, heeft bereikt. Een aanbod is dus slechts een geldig aanbod als het door de andere partij is gekend. De wilsovereenstemming komt tot stand op het ogenblik dat de aanbieder verneemt dat de andere partij het aanbod aanvaardt. Daarbij is niet vereist dat de partijen met elkaar in rechtstreeks contact staan. Men kan overeenkomsten sluiten via briefwisseling en via tussenpersonen.

Bij de aankoop van een standaard-softwarepakket heeft de eindgebruiker meestal enkel contact met een verkoper. Softwarepakketten worden verdeeld in het gewone distributiecircuit en verkocht zoals andere produkten. Men stapt dus naar een computerwinkel of zelfs naar een grootwarenhuis om een softwarepakket te kopen. Daarnaast worden vele softwarepakketten ook via postorderbedrijven aangeschaft.

Tussen de koper en de verkoper is er dus zeker een geldig contract. Meestal zal dit als een gewone koopovereenkomst moeten worden beschouwd. De situatie is m.a.w. vergelijkbaar met de aankoop van een boek in de boekhandel.

Is er echter ook een overeenkomst tot stand gekomen tussen de koper en de softwareproducent ? Deze vraag wordt meestal negatief beantwoord.

Wie een softwarepakket koopt, zal meestal pas na de verkoop kennis nemen van de licentievoorwaarden van de softwareproducent. Op dat ogenblik mag de koper er redelijkerwijze van uitgaan dat hij eigenaar geworden is van het pakket en dat hij enkel ertoe gehouden is het auteursrecht van de producent te respecteren. Van een overeenkomst tussen de software-

producent en de eindgebruiker is slechts sprake als men kennis heeft kunnen nemen van de licentievoorwaarden vóór de verkoop, of indien men, na de verkoop, de ingevulde en ondertekende licentiekaart naar de producent opstuurt. In dat laatste geval is er namelijk van een expliciete aanvaarding sprake.

De vraag of er tussen de softwareproducent en de eindgebruiker een contractuele verhouding bestaat, is om twee redenen van belang:

- de softwarebeschermingswet verwijst naar deze overeenkomst, o.m. m.b.t. de toelaatbaarheid van programmawijzigingen om fouten te verbeteren (dit is voor de rechtmatige gebruiker toegelaten, tenzij anders overeengekomen);
- bij gebrek aan een geldige overeenkomst tussen de softwareproducent en de eindgebruiker, gelden niet de bepalingen van de "shrink-wrap" licentie (o.m. de exoneration bij schade door het gebruik van de software, de beperkte garantieperiode, enz.); bij betwistingen zal de rechter de bepalingen van de softwarebeschermingswet en de auteurswet toepassen en voor het overige nagaan welke de "normale" gebruiksvoorwaarden voor standaard-softwarepakketten zijn.

Indien de "shrink-wrap" licentie niet als een geldige overeenkomst kan beschouwd worden, heeft ze toch een zekere juridische waarde ten voordele van de eindgebruiker. De bepalingen van de "shrink-wrap" licentie waarin aan de eindgebruiker supplementaire rechten worden verleend, boven degene waarop hij normaliter recht heeft, zullen door de eindgebruiker kunnen worden ingeroepen. Die bepalingen worden dan beschouwd als een "gebruiksnotitie" vanwege de softwarefabrikant.

Tenslotte dient men, ongeacht het juridisch karakter van de "shrink-wrap" licentie, ook rekening te houden met de wet op de handelspraktijken en meer specifiek met de artikelen 31 (kennelijk onevenwicht tussen de partijen) en 32 (nietige clause) van die wet.

2.2. CONTRACTEN "AD HOC"

Voor "ad hoc" informaticacontracten (in enge zin) kan men moeilijk algemene regels voorstellen. De beste hulp voor het opstellen of beoordelen van deze contracten zijn:

- het gebruik van modellen: dergelijke modellen zijn o.m. opgesteld door de Europese informaticagebruikersorganisatie (CECUA);
- het gebruik van "checklists" met een opsomming van de belangrijkste punten waarmee men bij het opstellen of beoordelen van een informaticacontract rekening moet houden. Hierna volgt een voorbeeld van een dergelijke controlelijst. Daarbij wordt uitgegaan van de meest eenvoudige hypothese, nl. dat één leverancier instaat voor het gehele project.

2.2.1. Voorwerp van de overeenkomst

In de eerste plaats is het uiteraard van belang zo precies mogelijk te omschrijven wat de "ontwikkelaar" moet leveren:

- de globale omschrijving van apparatuur en programmatuur;
- de functionaliteiten waaraan het systeem moet beantwoorden;
- welke volumes moet het aankunnen?
- omschrijving van de economische doelstellingen van het systeem (dit is nuttig indien later schadevergoeding gevorderd wordt bij gebrekkige uitvoering);
- prestatie-aspecten (antwoordtijden, invoer- en uitvoermogelijkheden).

2.2.2. Planning

Het is belangrijk de door de leverancier na te leven planning in het contract op te nemen en te bepalen wanneer precies het definitief in gebreke blijven van de leverancier wordt vastgesteld en acties kunnen ondernomen worden.

2.2.3. Handleidingen en technische documentatie

Het is niet alleen nuttig te bepalen welke handleidingen en documentatie bij het systeem geleverd zullen worden, maar tevens het aantal exemplaren, de taal, e.a. details aan te duiden. Het kan ook nuttig zijn te bedingen dat een onbeperkt aantal copies van de handleiding mogen genomen worden voor het personeel.

2.2.4. Opleiding

Het is aangewezen de opleiding te omschrijven, met de duur, de vorm, het lesmateriaal, het aantal personen per groep, de taal, de verwachte voorkennis van de op te leiden personen, de prijs van eventueel bijkomende opleidingssessies.

2.2.5. Compatibiliteit

Er moet uiteraard worden bepaald dat alle geleverde software onderling compatibel moet zijn.

2.2.6. Levering en installatie

De datum van levering en installatie hoort in de planning (zie hoger) thuis. Er zijn echter nog een aantal andere modaliteiten te regelen (plaats, wie doet wat, omgevingsvoorwaarden als temperatuur, electriciteit, enz..).

2.2.7. Configureren

Het installeren van apparatuur en programmatuur en het aanpassen ervan aan de bestaande

omgeving (bijv. een lokaal netwerk) kan veel tijd en frustraties meebrengen. Het is aangewezen in de overeenkomst te bepalen wie dat op zich zal nemen.

2.2.8. Resultaatsverbintenis

Vaak wordt, vooral in informaticacontracten met de overheid, bepaald dat de overeenkomst voor de leverancier een resultaatsverbintenis inhoudt. Het is niet altijd duidelijk wat de draagwijdte van een dergelijke clause is. Meestal is het nuttiger om het karakter van een resultaatsverbintenis toe te kennen aan specifieke, geconcretiseerde deelverbintenissen (bijv. antwoordtijden) en bovendien een algemene clause op te nemen die bepaalt dat het globale project, met de beschreven functionaliteiten, een "sleutel op de deur" karakter heeft.

2.2.9. Regels der kunst

Het is onmogelijk om alle eventualiteiten in een overeenkomst te voorzien. Daarom is het nuttig te verwijzen naar de "regels van de kunst" die door elke professionele informaticaleverancier moeten toegepast worden, ongeacht hetgeen in de overeenkomst staat.

2.2.10. Beschikbaarheid

In vele contracten wordt een percentage gespecificeerd van de tijd tijdens dewelke het systeem minimaal beschikbaar moet zijn (bijv. 98 %). Dit kan ook worden uitgedrukt in het aantal uren dat maximaal mag verstrijken tussen het opstarten en het eerste defect of de daaropvolgende defecten.

2.2.11. Intellectuele eigendom

In de regel behoudt de softwareproducent de intellectuele eigendom over de geleverde software. Dit kan uiteraard in de overeenkomst worden overgedragen, zoals bijv. vaak in contracten met de overheid het geval is (de overheid wenst zelf over de intellectuele eigendom te beschikken van de software die zij laat ontwikkelen).

2.2.12. Overmacht

Talrijke overeenkomsten bevatten een clause waarin bepaald wordt wat er gebeurt bij een onvoorziene gebeurtenis. De klant moet erover waken dat het begrip "overmacht" geen te ruime betekenis krijgt (bijv. in gebreke blijven van onderaannemers).

2.2.13. Garantieverplichting

Indien men van een softwarebedrijf wil bekomen dat ook na de oplevering van het systeem nog eventuele fouten in de programma's moeten verbeterd worden, dan zal men dit uitdrukkelijk moeten bepalen. Anders valt het verbeteren van fouten na de oplevering onder het

onderhoudscontract (zie hierna).

2.2.14. Risico-overdracht

De risicoclausule moet regelen vanaf welk ogenblik het risico voor de apparatuur bij de klant komt te liggen. Dit is o.m. belangrijk om te weten vanaf welk ogenblik de verzekering van de klant tussenkomt (bijv. bij schade tijdens de installatie).

2.2.15. Kwaliteitseisen personeel

In vele informaticacontracten over de ontwikkeling van informaticasystemen worden in hoofde van de leverancier eisen opgelegd betreffende de algemene professionele kwaliteiten (opleiding, vast dienstverband, e.a.) van het personeel dat het project zal uitvoeren. Vaak worden van de belangrijkste personen (bijv. de projectleider) de curricula bijgevoegd.

2.2.16. Bijlagen

Het kan nuttig zijn om in de overeenkomst een opsomming op te nemen van de bijlagen aan de overeenkomst, die als bindend moeten worden beschouwd. Dit vervangt vaak een gedetailleerde technische beschrijving in de overeenkomst zelf.

2.2.17. Prijs

Meestal wordt aan de gebruikers aangeraden om een vaste globale prijs te bedingen voor het gehele project. Vaak is dit echter onmogelijk. De prijzen van de apparatuur evolueren zeer snel. Vele specificaties zijn nog niet bekend bij het sluiten van het contract. Een oplossing bestaat erin dat men verwijst naar de catalogusprijs en daarop een korting bedingt.

Voor sommige onderdelen (bijv. onderhoud) is een vaste prijs zeer moeilijk. Voor deze onderdelen stelt men dan een prijs per uur ("in regie") vast.

2.2.18. Overdracht aan derden

Een clause die bepaalt dat de apparatuur en de programmatuur mogen overgedragen worden is bijv. nuttig bij overdracht van onderneming (fusie, splitsing, e.a.)

2.2.19. Toevoegingen

Men moet als gebruiker zoveel mogelijk streven naar een "open" systeem, waarop ook apparatuur en programmatuur van andere leveranciers kunnen worden aangesloten.

2.2.20. Onderdelen

De leverancier moet zich ertoe verbinden om gedurende een bepaalde tijd na de oplevering

reserve-onderdelen te blijven leveren.

2.2.21. Verbruiksmaterieel

In sommige contracten wordt de gebruiker verplicht om gedurende een aantal jaren al het verbruiksmaterieel (schijven, tapes, toner, papier, e.a.) bij de leverancier te bestellen. Dit moet uiteraard, vanuit het standpunt van de gebruiker, best vermeden worden.

2.2.22. Exoneratieclausules

Het kan redelijk zijn om de verantwoordelijkheid van de leverancier voor sommige vormen van schade te beperken of uit te sluiten (bijv. voor verlies van gegevens of economische gevolgen van de onbeschikbaarheid van het systeem).

2.2.23. Vertrouwelijkheid en geheimhouding

Wie voor een onderneming een informaticasysteem ontwikkelt, komt natuurlijk met zeer veel vertrouwelijke gegevens over die onderneming in aanraking. Het is vanzelfsprekend dat de leverancier tot vertrouwelijke behandeling en geheimhouding van die informatie verplicht moet worden.

2.2.24. Betalingsvoorwaarden

Zoals in een bouwproject moet ook bij een informaticaprojekt bepaald worden op welke momenten, wat precies betaald moet worden (bijv. na de oplevering van elke faze). Het is ook belangrijk om een bepaling op te nemen over intresten en indexering.

2.2.25. Verdere diensten tegen normale prijzen

Dit is een clause waarbij de leverancier zich verbindt om ook na het einde van de overeenkomst verder niet-gespecificeerde diensten te leveren tegen zijn normale tarieven.

2.2.26. Aanwerving van personeel van de andere partij

Zeer vaak wordt een beding opgenomen waarin bepaald wordt dat de partijen elkaars personeel niet mogen aanwerven. Men moet ook proberen te vermijden dat in dit verband "achterdeurtjes" worden open gelaten (bijv. aanwerving door een andere onderneming van dezelfde groep en vervolgens detachering, inhuren van gewezen personeel van de andere partij op zelfstandig basis, enz.).

2.2.27. Uitbreidingen

Het is aangewezen om bij de aanschaf van een systeem rekening te houden met toekomstige

uitbreidingen, en om de mogelijkheden op dit vlak (met de prijs) op te nemen in de overeenkomst.

2.2.28. Vierhoekenclausule

De vierhoekenclausule is een beding waarbij bepaald wordt dat de overeenkomst uitsluitend bestaat uit wat in het contract zelf is opgenomen, met uitsluiting van wat bijv. in voorafgaande documenten (offertes, briefwisseling, folders, e.a.) werd afgesproken. Deze clausule is meestal nadelig voor de klant.

2.2.29. Inpassing in het bestaande

Het systeem dat geleverd moet worden, moet perfect in te passen zijn in het bestaande. Er wordt vaak bepaald dat de leverancier deze inpassing moet waarborgen.

2.2.30. Infrastructuur van de leverancier

Het kan nuttig zijn te bepalen welke infrastructuur ("hotline", onderhoudsploeg, onderdelen) de leverancier ter beschikking houdt van de klant.

2.2.31. Toegang tot lokalen van de klant

Speciale wensen kunnen zijn: toegang buiten de werkuren, uitvoering van testen op bepaalde tijdstippen, beschikbaarheid van leidinggevend personeel voor interviews tijdens de analysefase, e.a.

2.2.32. Duur van alle verbintenissen die na de oplevering overblijven

Er zijn een aantal verbintenissen (zoals de geheimhoudingsplicht, het verbod om personeel van de andere partij aan te werven, e.a.) die ook na de definitieve oplevering van het systeem blijven bestaan. Het is nuttig om te denken aan de duurtijd van deze verbintenissen.

2.2.33. Tijdbommen en virussen

Softwarepakketten kunnen mechanismen bevatten die in werking treden na een zekere tijd (bijv. weigering om sommige functies uit te voeren) en die enkel door de leverancier gekend zijn en opgeheven kunnen worden. Deze techniek wordt soms aangewend als ultiem drukkmiddel vanwege de leverancier bijv. om betaling te bekomen. Deze technieken moeten vermeden worden.

2.2.34. Onderhoud

Op de onderhoudsovereenkomst komen we later, in het cursusonderdeel betreffende de

continuïteit van informaticaproducten, nog uitvoeriger terug.

2.2.35. Geschillen

Tenslotte wordt meestal ook bepaald welke wegen gevolgd zullen worden bij betwistingen (poging tot minnelijke schikking, arbitrage, e.a.). Ook een regeling over de bewijslast en de bewijsmiddelen (zie hierna) is nuttig.

Buiten deze lijst van eventuele onderwerpen, kan men nog wijzen op volgende tips:

- testen: voor de gebruiker is het nuttig om te specificeren wanneer, hoe, hoelang, enz... de geleverde hardware en software getest zullen worden;
- onderaanneming: voor de gebruiker is het nuttig om inspraak te verkrijgen in eventuele wijziging van een onderaannemer;
- kwaliteitszorg: meer en meer wordt in een informaticaprojekt aandacht besteed aan de kwaliteitsbeheersing; vaak wordt deze opdracht aan een gespecialiseerd bedrijf toevertrouwd;
- fasering: in elk geval moet een informaticaprojekt in verschillende fasen opgedeeld worden met een evaluatie na elke faze en liefst een uitvoeringsovereenkomst bij het begin van elke nieuwe faze.

De bepalingen van het informaticacontract worden aangevuld met de verplichting van uitvoering te goeder trouw. Daarenboven is er in België een uitvoerige rechtspraak over de "informatieplicht" van de informaticaleverancier en de bescherming van de "informaticaleek" (zie o.m. Buyle, Lanoye en Willems, *Chronique de Jurisprudence, l'Informatique*, 1976-1988, JT, 1988, 93 e.v.).

3. INFORMATICA EN BEWIJSRECHT

3.1. ALGEMENE PRINCIPES VAN HET BELGISCH BEWLISRECHT

Meestal wordt een onderscheid gemaakt tussen vrije en gereglementeerde bewijsrechtelijke systemen. Als uitersten gelden daarbij het strafprocesrecht (vrij) en het familierecht (zeer sterk gereglementeerd). De reglementering m.b.t. het bewijs kan slaan op de vraag welke bewijsmiddelen toegelaten zijn, op de vrijheid van de rechter m.b.t. de aangewende middelen om de waarheid te achterhalen, of op de vraag wie het bewijs moet leveren. Er moet ook een onderscheid gemaakt worden tussen het bewijs van rechtshandelingen, het bewijs van feiten en het bewijs van de geldende regels. Hierna is enkel sprake van het bewijs van rechtshandelingen. Het bewijs van feiten is in principe altijd vrij. Inzake het bewijs van "het recht" geldt het adagium "ius novit curia". In de context van deze cursus beperken wij ons tot het bewijs van rechtshandelingen in het verbintenissenrecht.

3.1.1. Overzicht

Artikel 1315 BW bepaalt dat degene die de uitvoering van een verbintenis vordert, daarvan het bestaan moet bewijzen. Omgekeerd moet hij die beweert bevrijd te zijn, het bewijs leveren van de betaling of van het tenietgaan van de verbintenis. Deze bepaling regelt dus de verdeling van het bewijsrisico. Artikel 1316 BW somt limitatief de toegelaten bewijsmiddelen op: het geschrift, het bewijs door getuigen, de vermoedens, de bekentenis en de eed. Daarnaast dienen een reeks onderzoeksmaatregelen vermeld: het deskundig onderzoek, het verhoor van partijen en de plaatsopneming.

De hiërarchie van de bewijsmiddelen is de volgende:

- hoogst in rang staan de gerechtelijke bekentenis en de gedingbeslissende eed: tegen deze bewijsmiddelen is geen tegenbewijs mogelijk;
- vervolgens komen de bewijsmiddelen met een "wettelijke bewijswaarde", d.w.z. dat de rechter verplicht is om ze als voldoende bewijs te aanvaarden; het betreft het schriftelijk bewijs door authentieke of onderhandse akten, de wettelijke vermoedens en de buitengerechtelijke bekentenis;
- tenslotte komen de bewijsmiddelen met "vrije bewijswaarde": de andere geschriften (andere dan authentieke of onderhandse akten), de getuigenverklaringen en de vermoedens.

3.1.2. Akten

Het schriftelijk bewijs, en in het bijzonder de authentieke en onderhandse akte, is in het Burgelijk Wetboek het bewijsmiddel bij uitstek. Een akte is een geschrift dat is opgemaakt op tot bewijs te dienen, ondertekend door de partijen en/of door een openbaar ambtenaar en ter beschikking gesteld van hem ten behoeve van wie de akte is opgemaakt. De akte is een bewijsmiddel dat men bij voorbaat, vóór elke betwisting, tegen zichzelf schept.

Men onderscheidt de authentieke en de onderhandse akte. De pleegvormen m.b.t. de authentieke akte worden beschreven in art. 1317-1321 BW. Voor de onderhandse akte is de handtekening de enige, doch essentiële voorwaarde. Datum en plaats moeten niet noodzakelijk vermeld worden, behalve in specifieke gevallen waarin dat door de wet wordt vereist (bv. bij de wisselbrief).

De onderhandse akte heeft tussen de partijen dezelfde bewijswaarde als de authentieke akte (art. 1322 BW). Daarvoor is uiteraard vereist dat de akte door degene tegen wie ze wordt ingeroepen niet betwist wordt. De betrokkene kan bv. ontkennen dat de handtekening de zijne is. Betreffende de inhoud van de onderhandse akte kan het tegenbewijs tussen partijen enkel geleverd worden door een ander geschrift, of door een eed of een bekentenis.

Tegenover derden bewijst een onderhandse akte zoals tussen de partijen. Derden mogen echter de inhoud van de akte betwisten met alle bewijsmiddelen. Inzake het bewijs van de datum van de akte geldt ten aanzien van derden slechts een vaste datum. Dergelijke vaste datum kan een onderhandse akte slechts verkrijgen als één van de ondertekenaars overleden is (en ingevolge de overlijdensakte vaststaat dat de akte dateert van vóór het overlijden), als de hoofdinhoud van de onderhandse akte in een authentieke akte wordt herhaald (de onderhandse akte bestond dan zeker vóór de authentieke akte) en door de registratie van de onderhandse akte. De vereiste van een vaste datum is vooral bedoeld om derden te beschermen tegen het eventueel door de partijen "antidateren" van de onderhandse akte.

Voor het onderhands bewijs van wederkerige contracten geldt de regel dat er zoveel originelen moeten zijn als partijen met onderscheiden belangen én dat op ieder origineel het aantal exemplaren moet worden vermeld (art. 1325 BW). Deze regel wordt echter door de rechtspraak soepel toegepast. Zo volstaat bv. één enkel exemplaar als dat bij een derde gedeponneerd is, of dat het origineel dat in het bezit is van een partij, ondertekend is door de andere partijen. Voor het bewijs van onderhandse eenzijdige schuldbekentenissen moet de akte voluit door de schuldenaar eigenhandig geschreven zijn, of moet minstens de som geld of de hoeveelheid verschuldigde zaken in volle letters geschreven zijn, voorafgegaan door een formule als "goed voor..." of "aanvaard voor..." (art. 1326 BW). Op die manier heeft men vervalsingen van cijfers willen vermijden. Er gelden echter talrijke uitzonderingen.

3.1.3. Andere geschriften

Buiten de authentieke en de onderhandse akten zijn er nog andere vormen van schriftelijk bewijs, evenwel met een lagere bewijswaarde:

- afschriften;
- koopmansboeken;
- huiselijke papieren en registers;
- aantekeningen op titel;
- briefwisseling.

Een afschrift of copie is een letterlijke en volledig eensluidende weergave van het origineel. Uit art. 1334 BW wordt afgeleid dat een copie zich als bewijs aan de rechter opdringt zolang de conformiteit met het origineel niet wordt betwist en het origineel niet door een partij wordt opgevraagd. Bij betwisting over het bestaan van een origineel of over de conformiteit van de copie, kan deze laatste nog als een begin van schriftelijk bewijs, of minstens als een feitelijk vermoeden worden gehanteerd.

Koopmansboeken hebben tussen handelaars een volledige bewijswaarde. Tegen de handelaar kunnen zij door een niet-handelaar worden ingeroepen. Tegen een niet-handelaar kan een handelaar zijn boeken echter enkel laten gelden als een begin van schriftelijk bewijs dat door een eed kan worden aangevuld.

Huiselijke papieren en registers hebben geen wettelijke bewijswaarde ten voordele van wie ze bijhoudt.

Niet ondertekende of gedagtekende aantekeningen van de bevrijding van de schuldenaar op de titel die de schuldeiser in zijn bezit heeft, geldt als een bewijs. Dergelijke vermeldingen vormen ook een bewijs als ze geschreven zijn door de schuldeiser op het dubbel van de titel dat in het bezit is van de schuldenaar of op het kwijtschrift van een vroegere betaling.

Tenslotte kunnen ook brieven als bewijsmiddel worden gebruikt; zij hebben voldoende en dus wettelijke bewijswaarde tussen de partijen zodra de brief werd opgesteld om als bewijs te dienen en de auteur ervan zijn handtekening erkent.

3.1.4. Getuigen

Voor het bewijs van rechtshandelingen heeft het bewijs door getuigen een ondergeschikte rol. Art. 1341 BW bepaalt dat:

- met getuigen mag nooit bewezen worden voor een rechtshandeling waarvan de waarde 15.000 frank overschrijdt;
- met getuigen mag nooit bewezen worden tegen of naast de inhoud van een akte, ook als het om een rechtshandeling gaat waarvan de waarde het bedrag van 15.000 frank niet overschrijdt; het bewijs door getuigen is hier enkel toegelaten om de dubbelzinnige betekenis van een overeenkomst te verduidelijken.

De vier uitzonderingen op de dubbele regel van art. 1341 BW zijn de volgende:

- de beperking geldt niet op commerciële gebied; daar mag dus met getuigen tegen en boven de inhoud van een akte bewezen worden;
- getuigen en vermoedens kunnen steeds een aanvulling vormen van een begin van schriftelijk bewijs; dat is een geschrift dat uitgaat van - of toegeschreven wordt aan - de persoon aan wie het geschrift en het beweerd rechtsfeit wordt tegengeworpen, en waardoor het beweerd feit waarschijnlijk wordt gemaakt; om van een begin van schriftelijk bewijs te kunnen spreken zijn er dus drie voorwaarden:

- * een geschrift (ruim geïnterpreteerd);
- * uitgaande van of toegeschreven aan de persoon tegen wie het wordt ingeroepen;
- * waardoor het beweerde feit waarschijnlijk wordt gemaakt.
- de beperking van art. 1341 BW geldt niet in geval van een onmogelijkheid om een geschrift op te maken;
- als er een geschrift bestaan heeft en door toeval verloren is gegaan, mag eveneens met getuigen en vermoedens worden bewezen.

Let echter op! De dubbele regel van art. 1341 BW betreft enkel de partijen en geldt niet voor derden. Die mogen het bestaan van een rechtshandeling dus wél met getuigen en vermoedens bewijzen. Artikel 1341 BW is bovendien niet van openbare orde. Er mag van worden afgeweken in een overeenkomst tussen de partijen.

3.1.5. Vermoedens

Wanneer men uit iets dat vaststaat via een redenering datgene afleidt dat moet bewezen worden, spreekt men van een vermoeden. Het is een zwakke vorm van bewijs. Het tegenbewijs is vrijwel steeds mogelijk. Men onderscheidt feitelijke en wettelijke vermoedens, alnaargelang het de rechter of de wetgever is, die uit één of meer bekende gegevens een onbekend gegeven afleidt. Voorbeelden van feitelijke vermoedens zijn o.m.: een magnetische bandopname, een niet-tegensprekelijk deskundig verslag, geschreven verklaringen van derden, verklaringen van een partij in onverdachte omstandigheden.

3.2. INFORMATICA EN BEWIJS

3.2.1. Inleiding

Art. 1315 BW bepaalt dat hij die de uitvoering van een verbintenis vordert, deze moet bewijzen. Hoe kan echter het bestaan van een verbintenis bewezen worden die via elektronische weg tot stand is gekomen? Typische voorbeelden zijn verrichtingen met bankautomaten, bestellingen via "teleshopping" of "EDI".

Om de veiligheid en de betrouwbaarheid van dergelijke rechtshandelingen te waarborgen, zijn een aantal technieken ontwikkeld. Deze technieken zijn vooral gericht op de identificatie van de partijen (toegangscontrole) en op de beveiliging van de verrichting (authenticatie). Identificatietechnieken steunen hetzij op het opvragen van een gegeven dat enkel door de betrokken partij gekend is (PIN-code of paswoord), hetzij op de controle van een uniek element dat uitsluitend in het bezit is van de betrokken partij (een gecodeerde magnetische kaart), hetzij op de herkenning van een unieke eigenschap van de betrokken partij (vingerafdruk, structuur van de ooglenzen, stem), hetzij op de herkenning van een bepaalde handeling die de betrokken partij moet verrichten om zich te identificeren (bijv. een digitale handtekening), hetzij op een combinatie van deze vier technieken. Voor de beveiliging van het bericht worden meestal cryptografische technieken en verificatieprocedures (bijv. juistheidscontrole) gebruikt. Ondanks

deze technische voortuitgang, blijft voor het bewijs van rechtshandelingen de akte het belangrijkste bewijsmiddel.

3.2.2. De noodzaak van een akte

Art. 1341 BW legt belangrijke beperkingen op inzake het bewijs door getuigen of vermoedens tegen of naast de onderhandse of authentieke akte. Een akte is per definitie een ondertekend geschrift. Beschikt men bij een verbintenis die via elektronische weg tot stand is gekomen, over een onderhandse akte? De wet zelf geeft geen definitie van de onderhandse akte maar niemand zal betwisten dat de twee essentiële elementen zijn: een geschrift en een handtekening.

De notie van "geschrift" wordt door de rechtspraak reeds zeer ruim opgevat (zie hierna m.b.t. het begin van schriftelijk bewijs). Betreffende de noodzaak aan een handtekening kan men de vraag stellen of een "elektronische handtekening" de gewone geschreven handtekening kan vervangen. De handtekening heeft een dubbele functie:

- het is een middel om de auteur van de akte te identificeren (identificatiefunctie);
- de handtekening is een uitdrukking van de wil van de ondertekenaar waardoor deze zich de inhoud van de akte a.h.w. toeëigent (animus signandi).

Over de inhoud en de vorm van de handtekening blijft het Burgerlijk Wetboek in het vage. Men neemt aan dat de handtekening de reproductie moet zijn van een naam - een kruisje, een tekening, initialen, e.d. vormen dus geen handtekening - maar de naam moet zeker niet leesbaar zijn. Het is voldoende dat de identificatiefunctie van de handtekening behouden blijft, m.a.w. dat het een middel blijft waardoor de ondertekenaar te onderscheiden is van alle andere personen. Men neemt ook aan dat de handtekening geschreven moet zijn. Volgens het Hof van Cassatie (28/6/82, RCJB, 1985, 57) is de handtekening een geschreven merkteken waardoor de ondertekenaar gewoonlijk zijn persoonlijkheid aan derden meedeelt. De handtekening moet met de hand geschreven zijn ("une marque manuscrite") en er mogen geen supplementaire hulpmiddelen worden gebruikt (bv. een toetsenbord). Tenslotte moet de handtekening ook aangebracht zijn op de akte en ze geldt ook alleen maar voor de akte waarop ze is aangebracht. Dat betekent ook dat op de akte de oorspronkelijke handtekening moet voorkomen. Met de introductie van grafische computerschermen en "pencomputers" - waarbij de gebruiker rechtstreeks op het scherm "schrijft" met een soort elektronisch potlood - kan men zich afvragen of men een handtekening op een computerscherm niet als een geldige handtekening kan aanzien. O.i. moet die gedachte verworpen worden omdat de reproductie- en manipulatiemogelijkheden van dergelijke "handtekeningen" al te aanzienlijk zijn. Indien men dus een onderhandse akte wil, zal men zijn toevlucht moeten nemen tot het traditionele (papieren) geschrift.

3.2.3. Beperkingen aan de noodzaak van een akte

3.2.3.1. De grens van 15.000 frank

De wet van 10 december 1990 veranderde het bedrag van 3000 frank waarvan sprake in art. 1341 BW, in 15.000 frank. Een authentieke of onderhandse akte is dus thans niet meer vereist voor rechtshandelingen waarvan de waarde 15.000 frank niet overschrijdt. Daarmee wordt het probleem van de verrichtingen via de elektronische bankautomaten grotendeels opgelost. De meeste dergelijke verrichtingen betreffen namelijk lagere bedragen. Voor die bedragen is het bewijs in principe vrij. Weliswaar leggen sommige specifieke wetsbepalingen ook onder die grens een geschrift op.

3.2.3.2. Bewijs in handelszaken

Ook in handelszaken is het bewijs vrij en geldt dus niet de dubbele regel van art. 1341 BW. Dat betekent dat tussen handelaars (en ook door een niet-handelaar die een verbintenis wil bewijzen in hoofde van een handelaar) geen enkele juridische beperking bestaat om, in plaats van de onderhandse akte met de handgeschreven handtekening, andere technieken te gebruiken voor zowel de identificatiefunctie als voor de uitdrukking van de "animus signandi". Uiteraard zal men bij eventuele betwistingen, de rechter ervan moeten overtuigen dat deze alternatieve technieken even efficiënt en betrouwbaar zijn als de klassieke onderhandse akte.

3.2.3.3. Begin van schriftelijk bewijs

Art. 1341 BW laat toe dat een begin van schriftelijk bewijs met getuigen en vermoedens kan worden aangevuld. Hoger hebben we al gezien dat, om van een "begin van schriftelijk bewijs" te kunnen spreken, drie voorwaarden vervuld moeten zijn.

De notie "geschrift" wordt zeer ruim opgevat. Van een geschrift is sprake wanneer iemand door middel van tekens op een materiële drager een voor de buitenwereld verstaanbare boodschap overbrengt. Zo werd gesteld dat een telexbericht bv. een geschrift is. Hetzelfde geldt zeker ook voor een telefaxbericht, een telegram of voor een fotocopie. Sommigen (o.m. Ballon, "Het bewijs en de moderne technieken", DAOR, 1990, 87) menen dat een geschrift noodzakelijk een "grafisme" impliceert, dat bovendien "rechtstreeks" afleesbaar moet zijn. Een videoband of een geluidsband zouden in die zin geen geschriften zijn omdat ze "geen grafisch vastgelegde uitdrukking van een gedachte" vormen. Documenten op magnetische of optische schijven zouden volgens die opvatting weliswaar een "grafisch" karakter hebben maar niet direct afleesbaar zijn. Daarom zou men ze ook niet als "geschriften" kunnen beschouwen. Persoonlijk verkiezen wij een soepelere benadering.

3.2.3.4. Onmogelijkheid om zich een geschrift te verschaffen

Vaak zal men aan het vereiste van art. 1341 BW ook kunnen ontsnappen door zich te beroepen

op de uitzondering waarin voorzien is in art. 1348 BW, nl. de onmogelijkheid om zich een geschrift te verschaffen. Dergelijke mogelijkheid kan materieel of moreel zijn. In Frankrijk wordt alvast algemeen de stelling aanvaard dat vast en algemeen gebruik om geen geschrift te eisen als morele onmogelijkheid kan worden gekwalificeerd. Ook in de recente Belgische rechtspraak vond deze visie reeds navolging.

Een goed voorbeeld van een situatie waarbij men zich in de onmogelijkheid bevindt een geschrift te verschaffen, is de videoconferentie. Bij een videoconferentie ontmoeten de partijen elkaar niet fysisch op één plaats maar communiceren ze met elkaar via de uitwisseling van videobeelden. In België stelt bv. Belgacom zowel een vaste als een mobiele studio met het bijhorend technisch personeel ter beschikking van bedrijven die dergelijke videoconferenties willen organiseren. De buitenlandse partner moet van zijn kant uiteraard ook over een opnamestudio beschikken. Via satellieten worden de beelden vanuit de twee studio's uitgewisseld. De partijen zien mekaar dus op een scherm en praten met elkaar via een telefoonverbinding. Er worden ook een aantal bijkomende hulpmiddelen ingeschakeld voor de uitwisseling van documenten, zoals bv. een telefaxapparaat en een computerverbinding. Tijdens dergelijke videoconferenties worden vaak belangrijke contracten gesloten. De partijen bevinden zich echter in de onmogelijkheid om een onderhandse akte op te stellen omdat zij zich niet fysisch op dezelfde plaats bevinden.

3.2.3.5. Bewijsovereenkomsten

Art. 1341 BW is niet van openbare orde. De partijen kunnen er dus van afwijken bij overeenkomst. Via dergelijke "bewijsovereenkomsten" kunnen de partijen:

- een eigen regime m.b.t. de bewijslast ontwerpen;
- zelf vermoedens in het leven roepen (bv. bij het elektronisch geldverkeer wordt in de overeenkomst tussen de bank en de klant gestipuleerd dat de journaalband vermoed wordt weer te geven welke operaties aan het automatisch loket zijn verricht);
- de hiërarchie van de bewijsmiddelen veranderen (bv. aan een vermoeden dezelfde bewijswaarde toekennen als aan een begin van bewijs door geschrift).

Er zijn echter een aantal beperkingen. De wet van 14 juli 1991 op de handelspraktijken laat sommige bedingen niet toe om de consumenten te beschermen. De banken bv. zullen daarmee rekening moeten houden bij het inlassen van bepaalde exoneratieclausules in hun contracten met de klanten. Ook bedingen waarbij aan de partijen de mogelijkheid wordt ontnomen om een bewijsmiddel te betwisten en zich tot de rechter te wenden, zullen als nietig worden aanzien.

Het grote voordeel van de bewijsovereenkomst is dat ze kan aangepast worden aan de specifieke situatie van de partijen en gemakkelijk gewijzigd kan worden als de noodzaak daartoe zich opdringt. Er zijn echter ook een aantal nadelen. Partijen die maar occasioneel met elkaar in aanraking komen, sluiten meestal geen bewijsovereenkomst. Het is eerder een instrument voor partners die op regelmatige wijze met elkaar overeenkomsten sluiten. Ook moet men er rekening mee houden dat men in een bewijsovereenkomst weliswaar een nieuwe techniek als bewijs kan

aanvaarden maar dat bij betwisting uiteindelijk de rechter over de bewijswaarde van die techniek zal moeten oordelen. Tenslotte wordt via de bewijsovereenkomst vaak de bewijslast op de schouders van de economisch zwakkere partij gelegd.

4. INFORMATICAPRODUCTEN EN CONTINUÏTEIT

4.1. INLEIDING

In vele gevallen worden informaticaproducten in een bedrijfsomgeving gebruikt. Meer nog dan bij andere bedrijfsuitrusting zijn hardware en software onderhevig aan de vooruitgang der techniek. De hardware, maar vooral de software, zullen bijna nooit volledig ongewijzigd blijven gedurende hun economische levensduur. Daarnaast is het voor de gebruiker van belang dat de goede werking van de informaticaproducten verzekerd wordt: voor wat met name de software betreft is het noodzakelijk dat voorkomende fouten (zogenaamde 'bugs') kunnen worden hersteld. Vanuit het standpunt van de gebruiker is er dus een grote behoefte aan continuïteit.

Aan de andere kant stellen we vast dat de rechthebbende (meestal de leverancier) van computersoftware op verregaande wijze wordt beschermd door het auteursrecht, dat exclusieve rechten toekent aan de maker van een programma. In principe is elke vorm van exploitatie - gaande van louter gebruik tot vertaling of reproductie - voorbehouden aan de auteur. Derden, waaronder gebruikers, genieten in principe geen toegang tot het programma dan met instemming van de auteur. De leverancier van software zal in de meeste gevallen in de "verkoopsovereenkomst" (in feite een licentieovereenkomst) slechts beperkte gebruiksrechten toestaan (bv. kopiëren verboden, tenzij voor eigen gebruik, en zonder het recht de programmatuur aan te passen). Dit kan een probleem opleveren voor de gebruiker gezien het feit dat de informatica vaak een vitaal deel van zijn bedrijfsvoering uitmaakt en, zoals gezegd, sterk onderhoudsgevoelig is. Geconcludeerd kan worden dat de gebruiker is erge mate afhankelijk is van de leverancier. De vraag stelt zich dan ook hoe hij zich een onafhankelijke positie kan aanmeten en hoe hij zich tegen discontinuïteit kan beschermen.

4.2. OVERDRACHT VAN (EEN AANTAL) EXCLUSIEVE RECHTEN

Het zal eerder uitzonderlijk zijn dat een gebruiker de overdracht van de rechten op de software zal weten te bedingen. In het kader van een softwareontwikkelingsovereenkomst is dit echter niet onmogelijk, zodat de opdrachtgever - voor wie een programma op maat wordt ontwikkeld met het oog op het oplossen van een bepaald probleem - eigenaar wordt van de patrimoniale auteursrechten op de in zijn opdracht en op zijn kosten ontwikkelde software. Deze overdracht moet wel uitdrukkelijk gebeuren, aangezien noch de auteurswet noch de softwarebeschermingswet een vermoeden ten voordele van de opdrachtgever voorziet (zie hoger).

Meestal is dit echter voor de gebruiker niet nodig en door de ontwikkelaar niet gewenst omdat hij het programma of delen ervan nadien nog wil gebruiken c.q. uitbaten. De gebruiker kan als alternatief uitgebreide gebruiksrechten bedingen, die hem toelaten de software te wijzigen,

kopiëren, commercialiseren, enz. (zie lager).

4.3. HANDELINGEN WAARVOOR GEEN TOESTEMMING VEREIST IS

Zoals gezegd voorziet de softwarebeschermingswet van 30 juni 1994 dat alle handelingen omtrent een programma principieel aan de toestemming van de auteur onderworpen zijn. Nochtans voorziet artikel 7 van de richtlijn hierop een aantal uitzonderingen (ook artikel 7 houdt een uitzondering in, namelijk de decompilatie; lees hierover in het onderdeel softwarebescherming).

Tenzij bij overeenkomst uitdrukkelijk anders is bepaald, is voor reproductie en wijziging, onder welke vorm ook, geen toestemming van de rechthebbende vereist, indien reproductie en adaptatie noodzakelijk is om het computerprogramma te kunnen gebruiken voor het beoogde doel (artikel 6, § 1 softwarebeschermingswet). De wet geeft als voorbeeld een aanpassing van het programma om fouten te verbeteren. Dit mag zelfs door derden gebeuren. Deze uitzondering laat echter niet toe dat derden een volledig onderhoud (zie hierna) van de software zouden doen. Bovendien is het zelfs zo dat het in de softwarebeschermingswet opgenomen recht om fouten te verbeteren door de leverancier bij contract kan worden verboden.

Voorts laat de softwarebeschermingswet de rechtmatige gebruiker toe reservekopieën (zogenaamde "back-ups") van het programma te maken indien die copie nodig is voor om het programma te gebruiken (artikel 6, § 2). Zo mag een copie gemaakt worden indien dit nodig is voor het herstel van het originele exemplaar, maar niet om ze te distribueren.

Tenslotte is de (rechtmatige) gebruiker gemachtigd om zonder toestemming van de rechthebbende de werking van het programma te observeren, te bestuderen en uit te testen, teneinde vast te stellen welke ideeën en beginselen aan een element van een programma ten grondslag liggen, indien hij dit doet bij het rechtmatig laden of in beeld brengen, de uitvoering, transmissie of opslag van het programma (artikel 6, § 3 softwarebeschermingswet).

4.4. ONDERHOUDSCONTRACTEN

We hebben gezien dat de softwarebeschermingswet de gebruiker die geen uitgebreide gebruiksrechten in zijn licentie heeft weten te bedingen, enigszins heeft willen beschermen opdat hij van de software gebruik zou kunnen maken in overeenstemming met de doelstelling van zijn aanschaf. Deze bescherming is echter zeer beperkt en omvat geenszins het recht om alle handelingen te stellen die nodig kunnen zijn om een compleet onderhoud van het programma te verzorgen.

Bij wijze van voorbeeld sommen we hierna een aantal handelingen op die essentieel lijken te zijn om software operationeel te houden:

- het vooraf testen van programmatuur teneinde mogelijke negatieve invloed op de computeromgeving te voorkomen;

- het opheffen van storingen die niet door een fout zijn ontstaan maar door andere oorzaken (bv. virussen);
- het testen van uitwijkmogelijkheden naar back-up centra;
- het aanpassen van de programmatuur aan nieuwe versies hardware/besturingssoftware (het zogenaamde 'upgraden');
- het installeren van performance-verbeteringen die de systemen sneller laten werken. - het verrichten van kleine aanpassingen zoals het veranderen van parameters (bv. de belastingspercentages);
- het aanbrengen van grote aanpassingen (bv. wanneer het systeem van de belastingsheffing wijzigt);
- het verrichten van aanpassingen teneinde programmatuur op een andere (vervangende) computer te kunnen gebruiken;
- het toevoegen aan programmatuur van koppelingsmogelijkheden (interfaces) voor apparatuur of andere software.

Of al deze handelingen "noodzakelijk zijn om het programma te kunnen gebruiken voor het beoogde doel" (artikel 6, § 1 softwarebeschermingswet) is een moeilijk te beantwoorden vraag. Indien de gebruiker een goede relatie heeft met zijn leverancier kunnen de handelingen op bevredigende wijze geregeld worden in een goed onderhoudscontract. Al te vaak merk je nog dat slechts in de meeste vage termen (support, maintenance, preventief onderhoud, enz.) afspraken worden gemaakt: het is dan niet duidelijk waartoe de leverancier zich verbindt. Zoals in alle aannemingscontracten moet het voorwerp van een software-onderhoudsovereenkomst precies omschreven worden (zie bv. in Automatiseringscontracten. Modellen voor de praktijk, Kluwer BV, Deventer, 1991: A.H.J. Kuus, Onderhoudsovereenkomst voor standaard- en maatwerkprogrammatuur, E.2.1., inzonderheid artt. 2.1 en 2.12).

Voor het verrichten van de meeste van de bovengenoemde onderhoudshandelingen moet men de beschikking hebben over de source code (en hiermee samenhangende documentatie) van de programmatuur, doch de meeste leveranciers zullen de software slechts in de door de mens niet leesbare machinetaal (object code) leveren. Dit creëert een sterke afhankelijkheid t.a.v. de leverancier die door het verlenen van aanvullende diensten, zoals onderhoud, een supplementaire bron van inkomsten verwerft. Logisch dat over de prijsstelling een verschil van mening kan ontstaan (de onderhoudskost kan hoger oplopen dan het totaal van de kosten van punctuele interventies). Anderzijds kunnen problemen ontstaan wanneer de leverancier niet meer bereid of in staat is om op marktconforme wijze de onderhoudshandelingen te verrichten. Hij kan bijvoorbeeld failliet gaan, zijn activiteit stopzetten, overgenomen worden door een concurrerend bedrijf, enz. De gebruiker moet dan zelf of door inschakeling van derden in het onderhoud kunnen voorzien, zeker wanneer het voor zijn bedrijf gaat om kritische toepassingen. Hoe de gebruiker zich tegen bovenvernoemde gevallen van discontinuïteit kan beschermen bespreken we hierna.

4.5. BESCHIKBAARHEID VAN DE BRONCODE

Het gebeurt dat bij de ontwikkeling van software op maat de broncode ter beschikking gesteld wordt van de klant, wat hem minder afhankelijk maakt van de leverancier voor later aanpassingen en onderhoud.

In de meeste gevallen (van bedrijfskritische software bv. in een bank) beperkt de leverancier zich echter tot het afsluiten van een source code escrow-overeenkomst, waardoor de broncode bij een derde in bewaring wordt gegeven. In het contract wordt voorzien dat in bepaalde omstandigheden (bv. faillissement of contractbreuk) de gebruiker bij een derde-bewaarnemer afgifte van de broncode kan eisen, zodat hij zelf het nodige onderhoud kan (laten) uitvoeren. De leverancier van zijn kant heeft de garantie dat dit toegangsrecht tot de source code beperkt blijft tot welbepaalde omstandigheden.

De escrow-overeenkomst is een ingewikkelde overeenkomst met vele wolffijzers en schietgeweren. In tegenstelling tot de Nederlandse literatuur is hier door Belgische auteurs weinig aandacht aan besteed. Bovendien is er geen wet noch gepubliceerde rechtspraak die houvast kan bieden. Algemeen wordt aangenomen dat een analogische toepassing van de bepalingen uit het BW over de vrijwillige bewaargeving (artt. 1921-1948) mogelijk is.

Een eerste wolffijzer is art. 1944 B.W. dat bepaalt dat de in bewaring gegeven zaak aan de bewaargever moet worden terugggegeven zodra hij zulks vordert, ook al is in het contract een bepaalde tijd voor de teruggave vastgesteld. De drager met daarop de source code is een roerende zaak. Indien de leverancier bijvoorbeeld failliet gaat kan de curator zich op het standpunt stellen dat het gedeponeerde exemplaar van de broncode deel uitmaakt van de faillissementsboedel en als vermogensobject ten gelde dient gemaakt te worden ten voordele van alle schuldeisers van de gefailleerde. Hij zal het gedeponeerde van de derde-bewaarnemer revindiceren.

Om dit te vermijden zijn een aantal constructies uitgewerkt met als doel de zakenrechtelijke relatie tussen leverancier en de source code af te snijden. Dat zou kunnen door de gegevensdrager met de broncode over te dragen aan de bewaarder of de gebruiker. De eigendoms-overdracht aan de gebruiker gaat dan gepaard met een gelijktijdige bewaargeving bij een derde, zodat de gebruiker nooit inzaghe heeft in de broncode.

Maar dan blijven er nog twee problemen op te lossen. Wat indien de gebruiker de broncode revindiceert van de bewaarnemer in toepassing van art. 1944 B.W. zonder dat een van de vooraf afgesproken omstandigheden (de zogenaamde 'triggering events') zich heeft voorgedaan. Dit 'misbruik van recht' zou vermeden kunnen worden door in voorkomend geval een onmiddellijk opeisbare hoge boete te laten betalen. Ook kan men voorzien dat de eigendomsoverdracht geschiedt onder ontbindende voorwaarde. Indien de source code wordt opgevraagd of gebruikt in strijd met de contractuele bepalingen, is de voorwaarde vervuld en vervalt de eigendomsoverdracht. Tegen het tweede probleem - het faillissement van de gebruiker - bestaat

geen afdoende bescherming, tenzij preventief : de leverancier zal geen source code in escrow geven t.v.v. een gebruiker die riskeert snel failliet te gaan.

Zoals gezegd wordt in een software-escrowovereenkomst aan de gebruiker een toegangsrecht tot de broncode gewaarborgd. Inzage in de broncode betekent evenwel nog niet dat de begunstigde ermee mag doen wat hij wil, precies omdat de auteursrechthebbende zich tegen ongebreideld gebruik kan verzetten. Teneinde dit te voorkomen is het nodig dat de escrow-overeenkomst uitgebreide gebruiksrechten aan de gebruiker verschaft.

De meest uitgebreide rechten vloeien voort uit de overdracht van het auteursrecht zelf. Dit zal niet vaak voorkomen, tenzij de leverancier oordeelt dat in die omstandigheden (faillissement bv.) hij geen verder belang heeft bij de uitbating van de software. Is dit niet het geval, dan kan er sprake zijn van een partiële eigendomsoverdracht, waarbij de leverancier zich het recht voorbehoudt zelf de software te exploiteren en van de gebruiker geheimhouding t.a.v. derden en een niet-concurrentieverbintenis verlangt.

Een tweede mogelijkheid bestaat erin uitsluitend bepaalde gebruiksrechten aan de begunstigde van de escrow toe te kennen. Te denken valt aan het recht tot het wijzigen, uitbreiden en verbeteren van de software, het recht onderhoud (in de ruime zin : zie supra) en adaptaties ook door derden te doen verrichten, het recht het gebruik van de software binnen de onderneming uit te breiden tot meerdere machines, locaties, toepassingen.

5. INFORMATICAGESCHILLEN

5.1. INLEIDING

Een informaticageschil is een toestand van onenigheid tussen partijen die betrokken zijn bij het ontwerpen, bouwen, verdelen, onderhouden, exploiteren of gebruiken van geautomatiseerde informatiesystemen.

Aldus gedefinieerd is het een zeer ruim begrip. Deze definitie omvat onder meer:

- geschillen over intellectuele eigendomsrechten van softwareontwikkelaars;
- over distributieovereenkomsten tussen fabrikanten en verdelers van informaticaproducten;
- over aansprakelijkheid van een informatica-raadgever tegenover zijn cliënt;
- over de schending van de privacy van een datasubject (d.i. een privé-persoon waarvan persoonsgegevens in een databank worden bewaard);
- over een wanprestatie in de uitvoering van een onderhoudsovereenkomst voor informaticaproducten;
- geschillen tussen een bank en een rekeninghouder die zijn elektronische bankkaart is verloren;
- tussen een verdeler van beursinformatie en een abonnee over de gevolgen van een verkeerd ingevoerde koers.

- enz.

Al die geschillen kunnen als informaticageschillen worden beschouwd omdat in de relatie tussen de geschilpartijen het gebruik van een informaticaproduct een rol speelt. Maar dat is ook het enige gemeenschappelijke criterium, dat als dusdanig geen aanleiding geeft tot een bijzondere behandeling of procedure voor dit soort geschillen. In dit opzicht zijn informaticageschillen zoals alle andere geschillen.

In het domein van de informatica krijgen vooral twee soorten geschillen aandacht. De eerste betreffen misgelopen automatiseringsprojecten, de tweede zijn betwistingen inzake eigendomsrecht op informaticaproducten, met name software.

5.2. MISGELOPEN AUTOMATISERING

Een KMO heeft voor de automatisering van het beheer van zijn productieprocessen een informaticasysteem gekocht dat zowel hardware als software omvat, maar in zijn geheel geconcipieerd en geleverd werd door een software-huis. Terecht of ten onrechte vindt de klant dat de automatisering slecht verloopt.

Eerst tracht de leverancier de problemen die opduiken nog te herstellen, ook al loopt één en ander achter op het geplande tijdschema. De klant is bereid geduld uit te oefenen. Op een gegeven ogenblik blijkt dat de leverancier er niet in slaagt aan de verwachtingen van de klant te voldoen. Deze krijgt meer en meer kritiek te horen van zijn personeel in de productieafdeling dat over het automatiseringsproject niet meer te spreken is. Hij krijgt de raad van een collega die wel tevreden is over zijn systeem of van een op dat ogenblik geraadpleegde onafhankelijke adviseur om een ander systeem aan te schaffen. Hij onderhandelt met de leverancier om de uitvoering van het project te staken maar deze weigert om financiële of andere redenen. Het komt dus niet tot een minnelijke regeling maar tot een procedure.

5.2.1. Procedure ten gronde

De klant beslist de automatiseringsovereenkomst te ontbinden. Ofwel op grond van een uitdrukkelijk ontbindend beding in de overeenkomst, ofwel op grond van artikel 1184 B.W. dat bepaalt dat in wederkerige contracten de ontbindende voorwaarde stilzwijgend begrepen is voor het geval een van de partijen zijn verbintenis niet nakomt. Volgens artikel 1184 moet de ontbinding in rechte gevorderd worden en kan de rechter, naargelang van de omstandigheden, uitstel verlenen aan de verwerende partij. Nochtans heeft de rechtspraak geoordeeld dat in extreme gevallen het aan een partij toegestaan kan zijn de overeenkomst eenzijdig te ontbinden, en nadien deze ontbinding door de rechtbank te laten bevestigen. De partij die ten onrechte de overeenkomst ontbindt, betaalt eventueel schadevergoeding aan de tegenpartij.

De gerechtelijke ontbinding heeft het nadeel dat men op een uitspraak moet wachten en men in die tijd het automatiseringsproject in beginsel niet door een derde kan laten afwerken. Het is zeer

wel mogelijk dat na twee of drie jaar blijkt dat de tussenkomst van een gerechtsdeskundige noodzakelijk is. Men doet er dus goed aan dit eventueel bij het begin van de procedure ten gronde te vragen.

Wanneer men zelfstandig beslist te ontbinden komt in principe een einde aan alle verdere samenwerking, zodat alleen nog sprake kan zijn van betaling van schadevergoeding. Men moet dan wel zeker zijn dat de tekortkomingen van de leverancier ernstig zijn en vaststaan. Aangezien over dit laatste meestal betwisting bestaat, kan men aan een onafhankelijke derde (een expert) vragen de tekortkomingen vast te stellen. Deze deskundige kan men in onderling akkoord aanstellen of men kan de aanstelling aan de rechtbank vragen. Op basis van de vaststellingen van de expert komt men dan meestal tot de oplossing van het conflict. De tekortkomingen van de leverancier staan vast en de klant kan zonder al te groot risico de overeenkomst ontbinden. Of de expert meent dat de grieven niet vaststaan, en dan zal getracht worden een regeling in der minne te bereiken, al dan niet onder impuls van de deskundige die daartoe wettelijk gemachtigd is (art. 972 Ger. W.).

5.2.2. Onderzoeksmaatregel

Het gerechtelijk deskundigenonderzoek is een onderzoeksmaatregel. Het heeft tot doel de werkelijkheid van een feit of toestand na te gaan en te bewijzen. De procedure tot aanstelling is gebaseerd op art. 962 Ger. W. dat bepaalt dat de rechter, ter oplossing van een voor hem gebracht geschil of ingeval een geschil werkelijk en dadelijk dreigt te ontstaan, deskundigen kan gelasten vaststelling te doen of een technisch advies te geven.

Een ontevreden klant kan dus een onderzoek uitlokken op het ogenblik dat nog geen geschil bestaat en wanneer hij meent zich hierdoor een bewijs (van de contractuele tekortkoming van de wederpartij) te kunnen verschaffen. Dit is des te belangrijker wanneer het bewijs met de tijd zou dreigen te verdwijnen.

Meestal is er echter al een geschil, maar wordt de aanstelling gevraagd vooraleer de rechter gevraagd wordt over de grond van het geschil te oordelen. De rechter moet in eerste instantie alleen maar oordelen of een deskundigenonderzoek opportuun is. Meestal is het antwoord hierop positief, ook al omdat de rechters vaak leken zijn in technische materies zoals informatica en hopen dat een expert hun de problemen kan verduidelijken, in voorkomend geval oplossen.

Een eis tot aanstelling van een deskundige kan ingesteld worden hetzij als hoofdvoorwerp van de vordering (bij dagvaarding) hetzij als incidentele vordering (tegeneis bij middel van conclusie). Er is ook nog een derde mogelijkheid die in de praktijk vaak gehanteerd wordt, nl. de procedure in kortgeding (art. 584, vierde lid, 2 Ger. W.). Hiertoe dient dagvaarding te worden uitgebracht voor de voorzitter van de rechtbank van eerste aanleg of de voorzitter van de rechtbank van koophandel. De zaak wordt bij voorrang behandelde en op een periode van 1 tot 4 weken bekomt men de aanstelling van een gerechtsdeskundige.

Voor de ontvankelijkheid van een eis in kortgeding moeten twee voorwaarden voldaan zijn. De zaak dient spoedeisend te zijn d.w.z. van dien aard zijn dat ernstige schade dreigt op te treden. Indien het automatiseringsproject een sleutelfunctie van een bedrijf betreft (productie, boekhouding) is aan deze voorwaarde meestal voldaan. Uit de gepubliceerde rechtspraak blijkt dat de hoogdringendheid in zaken van levering van goederen en diensten in informatica meestal wordt aanvaard. De tweede voorwaarde is dat de vordering voorlopig moet zijn d.w.z. niet vooruitlopen op de behandeling ten gronde. Zoals gezegd is dit voor een deskundigenonderzoek steeds het geval.

5.3. INBREUKEN OP AUTEURSRECHTEN

De inbreuken op het auteursrecht van computerprogramma's (soms software-piraterij genoemd) zijn een gekend probleem voor de uitgevers en distributeurs van computerprogramma's. De procedures waarop benadeelden beroep kunnen doen worden hier in het kort besproken.

5.3.1. Strafrechtelijke procedure wegens namaking

De auteur van een programma kan de namaker van zijn werk strafrechtelijk laten vervolgen (artikel 80 auteurswet). Namaking omvat niet alleen plagiaat (het ongeoorloofd nabootsen) maar ook alle mogelijke aantastingen van de patrimoniale of morele rechten van de auteur : het gebruik van een programma voor een ander doel dan dat waarvoor het uitdrukkelijk vrijgegeven werd; het zonder toestemming van de auteur herwerken en verspreiden van diens programma; enz.

Om strafrechtelijk te worden vervolgd moet de daad kwaadwillig of bedrieglijk zijn gesteld (bijzonder opzet). In geval van goede trouw ontbreekt dus een essentieel bestanddeel van het misdrijf, met name de wil om het te plegen. Soms wordt aan dit bijzonder opzet niet al te veel aandacht besteed. Zo oordeelde de correctionele rechtbank te Verviers dat algemeen opzet volstaat, nl. het wetens en willens inbreuk maken op het auteursrecht (Corr. Rb., 4 oktober 1989, Computerrecht, 1992, 27; J.L.M.B., 1990, 709). Het bewijs van het algemeen opzet kan worden afgeleid uit eenvoudige foutieve nalatigheid, doordat de namaker zich niet voldoende ingelicht heeft over de rechten verbonden aan de beschermde werken.

De auteurswet straft niet alleen de namaker maar ook wie een voorwerp dat niet in orde is met de auteurswet in het handelsverkeer brengt. Onder 'uitbating van namakingen' wordt verstaan elke daad van verkoop, verhuur, tekoop- of tehuurstelling, het in voorraad hebben voor de verkoop of de verhuur of het invoeren in België voor handelsdoeleinden (artikel 80 auteurswet).

5.3.2. Strafrechtelijke procedure wegens inbreuk op de softwarebeschermingswet

Zoals hoger beschreven, bevat artikel 10 van de softwarebeschermingswet specifieke strafsancities voor misdrijven als

- het in het verkeer brengen van onrechtmatige kopieën van softwareprogramma's; daarbij

- is het voldoende dat de betrokkene wist of redenen had om te geloven dat het om een onrechtmatige copie ging;
- het bezitten van onrechtmatige kopieën van softwareprogramma's voor commerciële doeleinden;
 - het in het verkeer brengen of bezitten voor commerciële doeleinden van o.m. programma's die uitsluitend bestemd zijn om de ongeoorloofde verwijdering of ontwijking van de kopiëerbeveiliging van andere programma's mogelijk te maken.

5.3.3. Burgerrechtelijke vordering tot schadevergoeding

Strafrechtelijke vervolging is niet de enige mogelijkheid om inbreuk op auteursrechten te laten gelden. Voor de gevallen waarin het sluitend bewijs van het kwaadwillig of bedrieglijk inzicht moeilijk te realiseren is, biedt een burgerlijke rechtsvordering gebaseerd op art. 1382 BW uitkomst. Opdat een benadeelde - niet noodzakelijk de auteur - schadevergoeding zou kunnen bekomen, volstaat het dat hij bewijst dat een inbreuk gepleegd werd op zijn exclusieve rechten. Opdat de gevorderde schadevergoeding effectief toegekend zou worden, dient de benadeelde echter ook te bewijzen dat de handeling daadwerkelijk schade heeft veroorzaakt ten belope van het gevorderde bedrag. Dit is evenmin een gemakkelijke bewijslast.

5.3.4. Beslag inzake namaak

In sommige gevallen zullen benadeelden niet eens in de mogelijkheid zijn de feitelijkheid van een inbreuk te bewijzen, doordat de makers het materiaal dat de inbreuk juist kan bewijzen, geheim houden. Om hieraan tegemoet te komen voorziet het Ger. W. een procedure van beschrijvend beslag (art. 1481-1488).

Op basis van een eenzijdig verzoekschrift kan de titularis van het auteursrecht aan de beslagrechter toelating vragen om over te gaan tot de beschrijving van de toestellen, machines, werken, voorwerpen en werkwijzen waarvan beweerd wordt dat ze zijn nagemaakt, evenals van de plans, documenten, geschriften waaruit de beweerde namaak kan blijken en van de gereedschappen die rechtstreeks gediend hebben om de aangeklaagde namaking te plegen. Door de beslagrechter wordt een deskundige aangeduid om de beschrijving van de namaking te verrichten.

Omdat het om een eenzijdige procedure gaat (waarvan de tegenpartij niet op de hoogte is tot op het ogenblik dat het beslag wordt uitgevoerd) en dat de loutere bewering van een inbreuk volstaat, behoort misbruik van deze procedure tot de mogelijkheden. Aangezien auteursrecht zonder enige formaliteit ontstaat, is een aanduiding van het bestaan van auteursrechten vaak voldoende. In zoverre de beslagrechter uitsluitend toestaat om een beschrijving van de beweerde nagemaakte producten te maken, is dit geen groot probleem. Indien ook beslag gelegd wordt op de goederen die beweerdelijk zijn nagemaakt of andere blokkeringsmaatregelen worden opgelegd, kan de schade erg groot zijn wanneer na een procedure ten gronde blijkt dat het beslag onterecht was.

5.3.5. Vordering tot staken

Een handelaar (maar ook beroeps- en interprofessionele organisaties en consumentenverenigingen) tenslotte kunnen zich ook tot de voorzitter van de rechtbank van koophandel wenden ten einde een vordering tot staken in te leiden wegens oneerlijke handelspraktijken. De procedure is zoals in kort geding.

Artikel 96 van de Handelspraktijkenwet van 14 juli 1991 sluit daden van namaking die gesanctionneerd worden door de auteurswetgeving uit haar toepassingsgebied uit. Wanneer geargumenteerd wordt dat de beweerde daad van namaking strijdig is met de eerlijke handelspraktijken moet de stakingsrechter zich onbevoegd verklaren om staking van de namaking te bevelen.

De vordering tot staken inzake het pirateren van software wordt daarentegen wel toegewezen wanneer de gewraakte handelswijze enkel als oneerlijk handelsgebruik wordt aangevochten zonder dat enige inbreuk op auteursrechten wordt aangevoerd, of wanneer de daad van namaking gepaard gaat met een oneerlijke handelsdaad.

Bij wijze van voorbeeld : de voorzitter van de rechtbank van koophandel te Brussel kende een vordering tot staken toe in een geschil waar een firma PC's verkocht voorzien van gecopieerde software waarvoor zij geen vergoeding voor het reproduceren van de programma's betaalde. Volgens de voorzitter werd door deze handelswijze de concurrentie vervalst gezien deze firma de mogelijkheid verkrijgt om een PC, met de software, aan zijn cliënten aan te bieden tegen een prijs die abnormaal laag is en dit ten nadele van de eerlijke handelaars die het auteursrecht op de software wel eerbiedigen (Vz. Kh., 2 april 1990, Computerrecht, 1991, 197; J.L.M.B., 1991, 260).

Tot slot nog dit: wat niet in aanmerking komt voor auteursrechtelijke bescherming, kan wel via de vordering tot staken worden beschermd. Dit geldt bijvoorbeeld voor programma's die niet van voldoende originaliteit blijken te geven.

Hoofdstuk 5 Telecommunicatierecht

1. HISTORISCHE INLEIDING

1.1. OPTISCHE TELEGRAFIE

De geschiedenis van de telecommunicatie begint op het einde van de achttiende eeuw met de uitvinding van de optisch-mechanische telegrafie door de Fransman Claude Chappe. Het Chappe-systeem bestond uit een serie torens met seinarmpjes die op gezichtsafstand van elkaar in een lijn werden geplaatst. Met behulp van hendels, wieltjes en touwen werden de seinarmpjes in verschillende posities gedraaid. In totaal werden 98 verschillende posities gebruikt. Elke positie kwam overeen met een teken of een letter. Op die manier werden gecodeerde boodschappen van de ene toren naar de andere doorgeseind. Een dergelijk Chappe-net werd in Frankrijk uitgebouwd vanaf 1793 en bestond in het midden van de negentiende eeuw al in een netwerk van 5000 km aan verbindingen met meer dan 500 torens. Het gebruik van de Chappe-telegraaf was een absoluut monopolie van de Franse Staat. De seincodes waren bovendien geheim omdat ze ook voor militaire doeleinden werden gebruikt. In onze regio ontstonden vanaf het begin van de negentiende eeuw een aantal private telegraafnetten op basis van de Chappe-techniek. Na de onafhankelijkheid van België werd tevergeefs geprobeerd om tot een politieke besluitvorming te komen over het telegrafiedossier¹³².

1.2. ELEKTRISCHE TELEGRAFIE

In het begin van de negentiende eeuw ontdekte men dat men electriciteit kon overbrengen langs koperdraden. Een van de eerste toepassingen van deze belangrijke ontdekking was de elektrische telegraaf. In 1832 kwam de Amerikaan Samuel Morse op het idee om een code te gebruiken voor het overseinen van boodschappen. In de Morse-code wordt elke letter of elk cijfer voorgesteld door een reeks punten (dots) of streepjes (dashes). De Morsetelegraaf is een toestel waarmee voor korte (dots) of langere (dashes) tijd een elektrisch circuit wordt onderbroken. De elektrische telegrafie heeft zich vanaf 1845 zeer snel verspreid. In 1850 werd er al een telegraafverbinding geopend tussen Frankrijk en Engeland en in 1866 werd de eerste transatlantische kabel in gebruik genomen.

In België werd de eerste telegraafverbinding in 1845 door een Engelse maatschappij aangelegd langs de spoorweg Brussel-Antwerpen. Het telegraafnet werd uitgebaat door de privé-sector op basis van overheidsconcessies en was vanaf het begin toegankelijk voor het publiek. In 1850 nam de regering het besluit om een openbaar telegraafnet aan te leggen en uit te baten, naar het voorbeeld van Frankrijk en Pruisen. Het beheer werd toevertrouwd aan de administratie van

¹³² Verhoest, P., Vercruysse, J.-P. en Punie Y., Telecommunicatie en beleid in België 1830-1991. Een reconstructie van de politieke besluitvorming vanaf de optische telegraaf tot de oprichting van Belgacom, Amsterdam, Otto Cramwinckel, 1992, p. 30.

spoorwegen en posterijen. Rond 1870 beschikte België over één van de dichtste telgraafnetten van Europa.

1.3. DE START VAN DE TELEFONIE

Al van het begin van de negentiende eeuw had men begrepen dat 'geluid' bestond uit een aantal vibraties. In 1831 slaagde Michael Faraday erin om een vibratie om te zetten in een elektrische impuls. Het was echter Alexander Graham Bell die op het idee kwam om geluid in de vorm van elektrische impulsen langs kabelverbindingen te sturen. Samen met Thomas Watson ontwikkelde hij een apparaat daarvoor en verkreeg van het USA Patent Office een octrooi¹³³.

De eerste telefoonlijnen verbonden uiteraard maar twee telefoontoestellen met elkaar. De uitvinding van Graham Bell werd pas echt interessant door de ontwikkeling van de schakelkasten vanaf 1878. Een aantal telefoonlijnen werden verbonden met één schakelkast die voor de doorschakeling zorgde. Elke telefoongebruiker kon dan verbonden worden met elke andere telefoongebruiker die op de schakelkast was aangesloten. De eerste schakelkasten in de Verenigde Staten konden op die manier een twintigtal telefoonlijnen beheren.

De telefonie verbeterde in de daaropvolgende decennia aanzienlijk door de ontwikkeling van betere schakeltechnieken en nog meer door de uitvinding van de vacuumbuis in 1906, waardoor men over een zeer efficiënte signaalversterker beschikte. In 1915 slaagde men erin een telefoonsignaal van de Oostkust naar de Westkust van de Verenigde Staten te sturen met slechts drie versterkers ('repeaters'). Vanaf de vijftiger jaren werd voor de versterking van telefoonsignalen overgeschakeld op de veel betrouwbaarder transistortechniek. In 1956 werd de eerste transatlantische telefoonkabel aangelegd.

De eerste, voorlopig nog lokale, telefoonlijnen werden in België vanaf 1879 uitgebaat door private maatschappijen. In 1882 waren er ongeveer 2000 telefoonbezitters en werd er geëxperimenteerd met een verbinding van Brussel naar Parijs. De wet van 11 juni 1883¹³⁴ gaf de overheid de mogelijkheid om telefoonlijnen aan te leggen en uit te baten. Voorlopig waren enkel de verbindingen tussen de steden gereserveerd voor de Staat, doch vanaf 1893 werd heel het netwerk onder het overheidsmonopolie gebracht.

Telefonie en telegrafie werden aanvankelijk door gewone Staatsdiensten verzorgd. Pas na de economische crisis van 1926-1930 werd de "Regie des télégraphes et des téléphones" opgericht met de opdracht om, in het algemeen belang, de telefoon- en telegraafdienst uit te baten met

¹³³ Het octrooi sloeg op "the method of, and apparatus for, transmitting vocal or other sounds telegraphically by causing electrical undulations, similar in form to the vibrations of the air accompanying the said vocal or other sounds".

¹³⁴ Loi concernant l'établissement et l'exploitation de réseaux téléphoniques, B.S., 12 juni 1883, Pasinomie 1883, 123-137.

industriële en commerciële methoden¹³⁵. De nieuwe RTT kreeg rechtspersoonlijkheid en een eigen patrimonium, maar werd vertegenwoordigd, geleid en beheerd door een Minister. Aanvankelijk had de RTT een vrij grote autonomie, die echter gaandeweg werd ingeperkt.

Het monopolie van de RTT vond zijn wettelijke basis in artikel 1 van de wet van 13 oktober 1930¹³⁶. Tot aan het einde van de tachtiger jaren werd dit monopolie zeer extensief opgevat zowel op het vlak van de infrastructuur, de transmissie en de schakeling, als op dat van de diensten en de eindapparatuur. Het is pas onder de druk van de Europese Unie dat recentelijk, in de wet van 21 maart 1991, het monopolie van de RTT wordt afgebouwd.

1.4. DRAADLOZE VERBINDINGEN

Rond 1880 experimenteerde de Duitser Heinrich Hertz met antennes waarmee hij electro-magnetische radiogolven kon uitzenden en ontvangen. Deze uitvinding werd verder ontwikkeld door de Italiaan Guglielmo Marconi, die erin slaagde om de Atlantisch Oceaan te overbruggen met radiosignalen.

Eén van de beperkingen van radiotransmissie, die men vanaf het begin had begrepen, bestaat erin dat een ontvangstantenne geen onderscheid kan maken tussen twee radiosignalen op dezelfde frequentie, ook al worden ze door verschillende stations uitgezonden. Om radiosignalen te kunnen onderscheiden, moet men dus verschillende frequenties gebruiken. Het aantal mogelijke frequenties waarop signalen kunnen worden uitgezonden (het zgn. 'spectrum') is uiteraard beperkt¹³⁷. Om te beletten dat iedereen om het even welke frequentie gebruikt en op die wijze elkaars signalen verstoort, is dus een spectrumbeheer nodig. Traditioneel bestaat dit spectrumbeheer in het toewijzen van frequenties.

Het gebruik van radiosignalen voor communicatiedoeleinden is lange tijd relatief beperkt gebleven. Enkel de radio- en televisieontvangers kenden een ruime verspreiding. Uitzend-apparatuur werd buiten de audiovisuele media, o.m. gebruikt voor militaire doeleinden en voor lucht- en scheepvaart. Langzamerhand, door de snelle verspreiding van de mobilfoon, wordt

¹³⁵ Wet van 19 juli 1930 tot oprichting van de Regie van Telegraaf en Telefoon, B.S., 2 augustus 1930. Deze wet werd achteraf herhaaldelijk gewijzigd. Een gecordineerde Nederlandse tekst vindt men o.m. in L. Neels, D. Voorhoof en H. Maertens, Medialex, Kluwer, Antwerpen, 1990, blz. 400-406.

¹³⁶ Wet van 13 oktober 1930 tot samenordering der verschillende wetsbepalingen op de telegrafie en de telefonie met draad, B.S., 20-21 oktober, 1930. Art. 1 luidt als volgt: "Alleen de Regie van Telegrafie en Telefonie heeft het recht telegraaf- en telefoonlijnen en telegraaf- en telefoonkantoren voor het publiek verkeer in te richten en te exploiteren. Zij kan, bij bijzondere overeenkomsten, derden machtigen om aan die exploitatie mede te werken". De facto reikte het monopolie van de R.T.T. veel verder dan de wet expliciet toeliet.

¹³⁷ Deze beperking blijft bestaan ondanks de verbetering van de coderingstechnieken en de uitbreiding van het aantal bruikbare frequenties. Bovendien wordt het radiospectrum vanaf 1935 ook gebruikt voor het transport van televisiesignalen, waarvoor een veel grotere bandbreedte is vereist.

draadloze communicatie echter een massafenomeen.

2. INTERNATIONAAL TELECOMMUNICATIERECHT

2.1. INLEIDING

Toen in het midden van de negentiende eeuw in alle Europese landen telegraafnetwerken werden uitgebouwd, ontstond al snel de vraag naar internationale verbindingen tussen die netwerken. Om dergelijke verbindingen mogelijk te maken moesten de verschillende netwerken vanuit technisch oogpunt ook de nodige compatibiliteit bezitten en daarom waren er internationale afspraken nodig.

Op initiatief van Napoleon III werd in 1856 in Parijs een internationale conferentie bijeenge-roepen. Het resultaat daarvan was de oprichting van de Internationale Unie voor Telegrafie (IUT). Deze organisatie werd vanaf dan het forum waarop internationale afspraken op dit gebied tot stand kwamen.

Vanaf het begin van de twintigste eeuw werd de telefonie dermate complex dat afspraken over standaarden, tarieven en technieken nog tijdens internationale conferenties konden gemaakt worden. Daarom werd op de IUT-conferentie van 1925 in Parijs beslist om een permanent orgaan op te richten dat de internationale afspraken moest voorbereiden in de vorm van technische voorstellen. Uiteindelijk werden twee permanente comités opgericht: de CCIT (Comité Consultatif International pour la Telegraphie) en de CCIF (Comité Consultatif International pour la Téléphonie). In 1956 werden deze twee organen samengesmolten tot de CCITT (Comité Consultatif International pour la Téléphonie et la Télégraphie).

In 1903 kwamen in Berlijn voor de eerste keer een aantal Europese landen samen rond de problematiek van de radioverbindingen. In 1906 leidde een tweede bijeenkomst tot de Internationale Conventie over Radiotelegrafie¹³⁸. In deze Conventie werd de noodzaak erkend van internationale afspraken o.m. op het gebied van maritieme radioverbindingen. Naar het voorbeeld van de IUT werd in 1927 een permanent technisch comité opgericht, nl. de CCIR (Comité Consultatif International pour les Radiocommunications). In 1932 werd de Internationale Unie voor Radiocommunicatie in de IUT geïncorporeerd. Vanaf dat moment werden alle internationale afspraken over telecommunicatie via dezelfde organisatie geregeld.

De belangrijkste opdracht van de internationale organisaties op het gebied van de telecommunicatie is het uitwerken van standaarden. Daarbij geldt het principe dat elke organisatie slechts normen kan opstellen die verenigbaar zijn met de normen van een "hogere" organisatie en daarop afgestemd zijn. Het resultaat is een hiërarchische structuur van internationale normen waarbij de normen van de eerder vernoemde CCI's (CCITT en CCIR) aan de top staan.

¹³⁸ Leive, D.M., *International Telecommunications and International Law: The Regulation of the Radio Spectrum*, Leiden, Sijthoff, 1970, p. 40.

Het werk van de CCITT speelt zich vooral af in de werkgroepen die door de Algemene Vergadering voor een periode van vier jaar worden samengesteld en die belast worden met de studie en de voorbereiding van aanbevelingen. In de regel zijn rond de twintig werkgroepen actief rond o.m. internationale huurlijnen, telefoonnummers, telefoontarieven, pakketgeschakelde datadiensten, ISDN, telefax, videotex, modems, multiplexers, enz...

Tijdens de algemene vergaderingen die om de vier jaar plaatsvinden, beslist de CCITT over de aanbevelingen die in de werkgroepen zijn voorbereid. De CCIR werkt min of meer volgens hetzelfde stamien. De werkgroepen zijn minder talrijk en houden zich o.m. bezig met afspraken over frequentietoewijzing, communicatiesatellieten, ruimtevaart, radioastronomie, e.d.

Zowel aan de werkzaamheden van de CCITT als aan die van de CCIR nemen naast de vertegenwoordigers van de nationale telecommunicatie-organisaties (de "PTT's") ook private telecommunicatiebedrijven en wetenschappelijke instellingen deel. Bovendien zijn er ook vertegenwoordigers van de regionale organisaties, waarover hierna wordt gesproken.

Op Europees vlak bestaat sinds 1959 de Europese Conferentie van de Post- en Telecommunicatie-organisaties ("CEPT"). Deze organisatie verenigt de nationale PTT's van alle West-Europese staten. Hoofdopdracht is het harmoniseren van de telecommunicatienetwerken en -diensten in Europa. Sinds enkele jaren is een nauwe samenwerking ontstaan tussen de CEPT en de Europese Unie. Zoals we hierna zullen zien heeft de Europese Unie desondanks een eigen organisatie opgericht die belast is met het uitwerken van standaarden, nl. ETSI.

Naast deze "gespecialiseerde" organisaties op het gebied van de standaardisering, moet men op telecommunicatiegebied vaak ook rekening houden met normen van de "algemene" standaardorganisaties. Op internationaal vlak is dat de ISO (Internationale Standaardiseringsorganisatie), op Europees vlak de CEN (Comité Européen de la Normalisation) en op Belgisch vlak het BIN (Belgisch Instituut voor Normalisatie). Tenslotte is er ook nog een internationale organisatie die zich bezig houdt met het uitwerken van normen op het gebied van de electronica in het algemeen, nl. de Internationale Commissie voor Electrotechniek (IEC). Op Europees vlak wordt deze rol vervuld door CENELEC. In deze organisaties worden o.m. afspraken gemaakt over netspanning, e.d.

2.2. HET TELECOMMUNICATIEBELEID VAN DE EUROPESE UNIE

2.2.1. Inleiding

De telecommunicatie is één van de belangrijkste uitdagingen geworden van de gemeenschappelijke markt. Tengevolge van de snelle technologische veranderingen en van de deregulering in de Verenigde Staten en in Japan onderging de Europese telecommunicatiesector in de afgelopen jaren een volledige metamorfose.

Met zijn 320 miljoen inwoners, het grote potentiële aan hooggekwalificeerd personeel en recent ook de uitdaging ten gevolge van de ouverture van Oost-Europa, heeft de Europese Unie een essentieel belang in de ontwikkeling van een Communautaire telecommunicatiemarkt. Deze ontwikkeling wordt in belangrijke mate gehinderd door de complexe en uiteenlopende situatie op het vlak van de regelgeving.

Met dit voor ogen heeft de Europese Unie sinds 1984 gestalte gegeven aan haar telecommunicatiebeleid. Het algemeen kader werd vastgelegd in twee belangrijke documenten die nog altijd als basis dienen voor de meeste communautaire beleidslijnen op het vlak van telecommunicatie:

- het communautair actieprogramma van 1984;
- het Groenboek uit 1987.

Sindsdien heeft het telecommunicatiebeleid van de Europese Unie zich ontwikkeld op verschillende vlakken en valt het uiteen in vele facetten: harmonisatie van technische normen en uitwerken van Europese technische normen, harmonisatie en regeling van de procedures voor het plaatsen van overheidsopdrachten in de telecommunicatiesector, het mededingingsbeleid van de Europese Commissie op basis van de artikelen 85 en 86 van het Verdrag, de richtlijnen van de Commissie op grond van artikel 90 over de overheidsmonopolies, de R&D-programma's voor de telecommunicatiesector, zoals RACE e.a., de bevordering van transeuropese netwerken, de inspanningen om te komen tot een onderlinge aanpassing van de wetgevingen over de eindapparatuur, de voorstellen van richtlijnen over de bescherming van de persoonlijke levenssfeer in het domein van de telecommunicatie en de voorstellen inzake ONP (Open Network Provision).

Al deze initiatieven zijn gericht op de ontwikkeling van een eengemaakte en concurrentiële telecommunicatiemarkt. Waarom is dat zo belangrijk?

Eén van de belangrijkste ontwikkelingen in de telecommunicatiesector is de toenadering tussen informatica en telecommunicatie; een belangrijke getuige daarvan is de digitalisering van het telefoonnet. Aan de ene kant worden bij de moderne telecommunicatie meer en meer computers ingeschakeld (zie bijv. de telefooncentrales). Aan de andere kant wordt in de informatica meer en meer op telecommunicatie een beroep gedaan omdat men computers aan elkaar wil koppelen in netwerken.

De informaticasector is een jonge, expansieve en weinig gereguleerde sector. Daarentegen is de telecommunicatiesector een traditionele sector die zeer sterk gereguleerd is. De telecommunicatiesector is lange tijd een exclusief terrein geweest van de nationale "PTT's". Door de intrede van de grote internationale informaticabedrijven is het monopolie van de nationale overheidsinstellingen op de telecommunicatiemarkt aan het wankelen gebracht.

In de Verenigde Staten en in Japan is men al in het begin van de tachtiger jaren begonnen met de afbouw van het overheidsmonopolie op de telecommunicatiemarkt. De introductie van een

regime van vrije concurrentie leidde tot grote competitieve telecommunicatiebedrijven. De vrees bestaat dat met de afbouw van de nationale grenzen in de Unie het terrein geëffend zal worden voor de Amerikaanse en Japanse telecommunicatiemultinationals. Daarom wil de Europese Commissie zeer snel ook in Europa de nationale overheidsmonopolies in de telecommunicatiesector vervangen door een ééngemaakte vrije markt die aan de grote Europese telecommunicatiebedrijven voldoende groeimogelijkheden biedt en hun competitiviteit stimuleert.

Tegen het einde van de eeuw zal meer dan 60% van alle jobs in de Unie te maken hebben met informatievoorziening en dus rechtstreeks of onrechtstreeks afhankelijk zijn van telecommunicatie. Er staat dus heel wat op het spel.

2.2.2. Overzicht van het Europese telecommunicatiebeleid

De belangrijkste onderdelen van het Europese telecommunicatiebeleid zijn o.m.:

- de maatregelen m.b.t. de overheidsopdrachten;
- de ontwikkeling van Europese technische normen;
- individuele procedures in het kader van het mededingingsbeleid;
- de introductie van vrije mededinging m.b.t. eindapparatuur en diensten;
- het verwezenlijken van de onderlinge conformiteit van eindapparaten;
- de maatregelen m.b.t. "open network provision";
- de initiatieven m.b.t. het gebruik van telecommunicatiesatellieten;
- het streven naar een Europees mobilofoonnetwerk;
- de stimulering van een Europees ISDN-netwerk;
- de bescherming van persoonsgegevens bij het gebruik van digitale telecommunicatienetwerken, in het bijzonder ISDN en mobilofonie.

2.2.2.1. Overheidsopdrachten

De belangrijkste opdrachten voor leveringen van telecommunicatieprodukten en -diensten komen nog altijd van de nationale overheden. Decennia lang waren de overheidsopdrachten inzake telecommunicatie in de Lid-Staten van de Unie de facto gereserveerd voor de nationale telecommunicatiebedrijven. De toekenning van een belangrijk telecommunicatiecontract voor de Belgische RTT aan een onderneming buiten België was zo goed als ondenkbaar.

De verwezenlijking van een eengemaakte Europese telecommunicatiemarkt veronderstelt echter dat de Europese ondernemingen, ongeacht tot welke Lid-Staat zij behoren, gelijke kansen krijgen bij alle belangrijke overheidsopdrachten.

In de schoot van de Europese Commissie (DG III: Interne Markt en Industrie) is er een Directoraat F dat zich bezig houdt met de Europese regeling voor het plaatsen van overheidsopdrachten. De belangrijkste zorg van dat directoraat bestaat erin aan alle bedrijven van de Unie, ongeacht in welke Lidstaat ze gevestigd zijn, gelijke kansen te geven wanneer in één van

de Lidstaten een overheidsopdracht wordt uitgeschreven. Allerlei obstakels (gebrekkige publiciteit, uiteenlopende procedures, enz...) staan een dergelijke gelijke toegang in de weg.

Om die reden heeft de Raad van Ministers in de zeventiger jaren twee belangrijke richtlijnen uitgevaardigd over de coördinatie van de procedures voor het plaatsen van overheidsopdrachten voor de uitvoering van werken¹³⁹ en voor het plaatsen van overheidsopdrachten voor leveringen¹⁴⁰. Op 14 juni 1993 werd van beide teksten een nieuwe gecoördineerde tekst aangenomen¹⁴¹. Inmiddels was in 1992 een richtlijn uitgevaardigd betreffende de coördinatie van de procedures voor het plaatsen van opdrachten van dienstverlening¹⁴².

De sectoren water- en energievoorziening, vervoer en telecommunicatie werden van de toepassing van deze richtlijnen uitgesloten. De belangrijkste reden voor deze uitsluiting is dat de diensten in deze sectoren soms onder het publiekrecht en in andere gevallen onder het privaatrecht vallen. Die sectoren kenmerken zich bovendien door een nauwe betrokkenheid van de overheid, bijvoorbeeld doordat exclusieve rechten worden toegekend en/of door een belangrijke aanwezigheid van de overheid in de beheersstructuren. Om aan deze moeilijkheid tegemoet te komen, werd voor de nutssectoren in september 1990 een aparte richtlijn uitgevaardigd¹⁴³. Door een richtlijn van 14 juni 1993 werden ook bepalingen voor de gunning van opdrachten van dienstverlening in de nutssectoren in deze richtlijnen geïncorporeerd¹⁴⁴.

¹³⁹ Richtlijn 71/305/EEG van de Raad van 26 juli 1971 betreffende de coördinatie van de procedures voor het plaatsen van overheidsopdrachten voor de uitvoering van werken (PB nr. L 185 van 16/8/1971, blz. 5), laatst gewijzigd bij Richtlijn 89/440/EEG (PB nr. L 210 van 21/7/1989, blz. 1).

¹⁴⁰ Richtlijn 77/62/EEG van de Raad van 21 december 1976 betreffende de coördinatie van de procedures voor het plaatsen van overheidsopdrachten voor leveringen (PB nr. L 13 van 15/1/1977, blz. 1), laatst gewijzigd bij een Richtlijn van 22 maart 1988 (PB nr. L 127 van 20/5/1988, blz. 1).

¹⁴¹ Richtlijn 93/36/EEG van de Raad van 14 juni 1993 betreffende de coördinatie van de procedures voor het plaatsen van overheidsopdrachten voor de uitvoering van leveringen, PB nr. L 199/1 van 9 augustus 1993; Richtlijn 93/37/EEG van de Raad van 14 juni 1993 betreffende de coördinatie van de procedures voor het plaatsen van overheidsopdrachten voor de uitvoering van werken, PB nr. L 199/54 van 9 augustus 1993.

¹⁴² Richtlijn 92/50/EEG van de Raad van 18 juni 1992 betreffende de coördinatie van de procedures voor het plaatsen van overheidsopdrachten voor dienstverlening, PB nr. L 209 van 24 juli 1992, blz. 1.

¹⁴³ Richtlijn 90/531/EEG van de Raad van 17 september 1990 betreffende de procedures voor het plaatsen van opdrachten in de sectoren water- en energievoorziening, vervoer en telecommunicatie, PB nr. L 291 van 29/10/1990, blz. 1.

¹⁴⁴ Richtlijn 93/38/EEG van de Raad van 14 juni 1993 houdende coördinatie van de procedures voor het plaatsen van opdrachten in de sectoren water- en energievoorziening, vervoer en telecommunicatie, PB nr. L 199 van 9 augustus 1993, blz. 84.

2.2.2.2. Normalisatie

Een tweede belangrijke hindernis voor de verwezenlijking van de Europese telecommuni-
catiemarkt wordt gevormd door de verschillende technische normen die in elke Lid-Staat inzake
telecommunicatie worden gehanteerd. Om een Europese telecommunicatiemarkt te
verwezenlijken zijn er Europese normen nodig.

Binnen DG III van de EG-Commissie is er nog een ander Directoraat, B, dat zich bezig houdt
met technische harmonisatie en normalisatie. Het algemeen kader van de Europese normalisatie
is opgebouwd rond een richtlijn van 1983¹⁴⁵, waardoor de Lid-Staten verplicht worden om hun
ontwerpen van technische voorschriften voor te leggen aan de Commissie en aan de andere Lid-
Staten, en rond de resolutie van 7 mei 1985 over de "nieuwe aanpak" op het gebied van de
technische harmonisatie en normalisatie. De uitvoering van dit beleid gebeurt in samenwerking
met de Europese Normalisatieorganisaties CEN en CENELEC, en, voor wat de telecommu-
nicatie betreft, sinds 1988, vooral met het Europees Instituut voor Normalisatie op het gebied
van de Telecommunicatie (ETSI).

ETSI werd in 1987 opgericht na de publicatie door de Europese Commissie van het Groenboek
over de ontwikkeling van de gemeenschappelijke markt voor telecommunicatiediensten en -
apparatuur. De zetel van ETSI bevindt zich in de Franse Provence (in Sophia-Antipolis).

2.2.2.3. Mededingingsbeleid

Een derde onderdeel van het Europees telecommunicatiebeleid situeert zich op het vlak van het
mededingingsrecht. DG IV (Concurrentie) waakt over de toepassing van de artikelen 85 e.v. van
het E.E.G.-Verdrag. De ambtenaren van deze DG sporen concurrentiebeperkende afspraken
tussen ondernemingen, misbruiken van machtspositie en, sinds kort, ook concurrentiebeperkende
concentraties van ondernemingen op. DG IV treedt dus op als een soort concurrentie-politie. Zij
stellen vooral individuele procedures in tegen private ondernemingen op basis van de artikelen
85 en 86 van het Verdrag. Ten aanzien van de overheidsbedrijven, wordt in DG IV erover
gewaakt dat de Lid-Staten de concurrentieregels van het Verdrag en het discriminatieverbod
(artikel 7) respecteren. Voor zover nodig kunnen daarvoor in DG IV ook richtlijnen of
beschikkingen tot de Lid-Staten gericht worden (artikel 90, 3.). Deze richtlijnen mag men zeker
niet verwarren met de richtlijnen die door de Raad van Ministers worden uitgevaardigd. Richt-
lijnen van de Commissie moet men eerder zien als een soort politionele maatregelen die tegelijk
naar alle Lid-Staten worden gestuurd, omdat de ambtenaren van de Commissie menen dat in al
die Lid-Staten toestanden bestaan die concurrentiebeperkend of discriminerend zijn. Hierna
zullen we zien dat de Commissie in verband met de telecommunicatie reeds tweemaal van deze
mogelijkheid gebruik gemaakt heeft, namelijk in 1988 met de richtlijn over de liberalisatie van
de eindapparatuur en in juni 1990, met de richtlijn over de liberalisatie van de
telecommunicatiediensten.

¹⁴⁵ Richtlijn 83/189/EEG van de Raad van 28 maart 1983 betreffende een informatieprocedure op het
gebied van normen en technische voorschriften.

2.2.2.4. Vrije mededinging op het vlak van de eindapparatuur en de telecommunicatiediensten

Inzake de eindapparatuur wordt door de Europese Commissie vooral gewerkt aan de onderlinge aanpassing van de wetgevingen van de Lid-Staten en aan de onderlinge erkenning van de conformiteit van die apparatuur. Wat de infrastructuur en de diensten aangaat, wordt het Europees telecommunicatiebeleid vooral opgebouwd rond de richtlijn van de Raad van 28 juni 1990 over "Open Network Provision"¹⁴⁶

Hierna wordt eerst aandacht besteed aan het Europese mededingingsbeleid op de telecommunicatiemarkt. Daarna komt dan het eigenlijke telecommunicatiebeleid aan de orde. De accenten liggen daarbij op de harmonisatie van de voorschriften voor de eindapparatuur en op de uitvoering van de ONP.

2.2.3. Individuele procedures op de telecommunicatiemarkt

In het kader van de artikelen 85 en 86 heeft de Commissie al herhaaldelijk op de telecommunicatiemarkt tegen individuele ondernemingen of administraties ingegrepen. Het meest bekende geval is de zaak "British Telecom"¹⁴⁷. De aanleiding voor deze zaak was een door een Brits agentschap neergelegde klacht. Het ging om verbodsbepalingen van het Post Office en, na de Telecommunications Act van 1981, British Telecom, met betrekking tot het doorzenden van telexberichten afkomstig uit of bestemd voor derde landen. Om allerlei redenen was het goedkoper om voor berichten tussen de Verenigde Staten en het Europese vasteland een omweg te maken via Groot-Brittannië. Enkele Britse bedrijven hadden zich hierop toegelegd en boden deze dienst aan maar werden door de Britse telecommunicatie-administratie teruggefloten. Hun klacht daartegen werd zowel door de Commissie als achteraf door het Hof gegrond verklaard.

Ook meer recent is de Commissie voor de handhaving van de mededingingsregels in de telecommunicatiesector opgetreden. Zo is o.m. de klacht tegen de Belgische RTT bekend, betreffende het verbod om huurlijnen te gebruiken voor de levering van telecommunicatiediensten met toegevoegde waarde aan derden. In september 1988 diende een private leverancier van telecommunicatiediensten bij de Europese Commissie een klacht in tegen de Belgische RTT om dit verbod te betwisten. De betrokken leverancier wou van de RTT een internationale lijn huren om gegevens van Franse klanten over het Belgisch grondgebied door te

¹⁴⁶ Richtlijn 90/387/EEG van de Raad van 28 juni 1990 betreffende de totstandbrenging van de interne markt voor telecommunicatiediensten door middel van de tenuitvoerlegging van Open Network Provision (ONP), PB nr. L 192 van 24 juli 1990, blz. 1.

¹⁴⁷ Beschikking van de Commissie van 10 december 1982, PB L 360 van 21/12/1982, blz. 36; zie ook het 12de Mededingingsverslag (1982), punt 94; de zaak wordt uitvoerig besproken in het Groenboek over de ontwikkeling van de gemeenschappelijke markt voor telecommunicatiediensten en -apparatuur, COM(87) 290 def., blz. 122 e.v.

sturen naar een verwerkingscentrum in Nederland. In deze procedure werd uiteindelijk tussen de partijen een minnelijke schikking getroffen. De RTT verbond er zich toe vanaf januari 1990 het gebruik van internationale huurlijnen voor de transmissie van gegevens van derden (third-party data traffic) toe te laten. Ondertussen is dit principe wettelijk bevestigd door de wet van 21 maart 1991 (zie hierna).

Een ander bekende en recente procedure is deze over de CEPT-Aanbeveling over de tarieven voor internationale huurlijnen. Op initiatief van de Commissie heeft de CEPT (de Europese Conferentie van de Post- en de Telecommunicatie-administraties) deze aanbeveling moeten intrekken. De door de CEPT aanbevolen harmonisatie van de tarieven beperkte uiteraard de concurrentie tussen de nationale PTT's en viel dus onder het verbod van artikel 85 van het Verdrag. Een gelijkaardige actie werd in 1990 door de Commissie ondernomen m.b.t. een Aanbeveling van de CCITT (de *internationale* consultatieve commissie voor telefonie en telegrafie) over de tarieven en gebruiksvoorwaarden van internationale huurlijnen.

Daarnaast is de Commissie ook opgetreden n.a.v. de oprichting van "joint ventures" in de telecommunicatiesector. Twee voorbeelden zijn de actie m.b.t. "MDNS" (een joint venture tussen 22 nationale PTT's met als doel de ontwikkeling van gestandaardiseerde telecommunicatiediensten met o.m. "one-stop shopping", netwerkbeheer, enz.) en de actie m.b.t. "EIRPAGE" (een joint venture tussen de Ierse PTT, Irish Telecom, en Motorola met het oog op de ontwikkeling van een Iers mobilfoonnetwerk).

Eveneens in 1990 onderzocht de Commissie de regelingen in de verschillende Lid-Staten betreffende de "access charges" voor het internationaal telefoonverkeer. De Commissie vermoedde dat de Europese telecommunicatie-administraties bij de aanrekening van deze "access charges" misbruik maakten van hun economische machtspositie. "Access charges" zijn lasten die door de nationale PTT's aan elkaar worden aangerekend voor het internationaal telefoonverkeer. Wie naar het buitenland belt, betaalt namelijk enkel aan zijn eigen PTT; het land van de bestemming ontvangt van de abonnee geen cent, hoewel het ook een deel van de verbinding verzorgt. Ter compensatie daarvan is het systeem van de "access charges" ingevoerd. De Europese Commissie verdacht er de Europese nationale PTT's van dat ze overdreven "access charges" oplegden aan de Amerikaanse telefoonmaatschappijen.

Om de transparantie van haar mededingingsbeleid in de telecommunicatiesector te bevorderen, heeft de Europese Commissie in de zomer van 1990 een document gepubliceerd met "Richtsnoeren voor de toepassing van de EEG-mededingingsregels op de telecommunicatiesector"¹⁴⁸. Deze richtsnoeren moeten de marktdeelnemers toelaten om hun strategieën en voorzieningen voor netwerken en diensten op Europese schaal van bij de planning in een vorm te gieten die een volledige overeenstemming met die regels toelaat.

Vaak wordt ook vergeten dat de artikelen 85 en 86 van het E.E.G.-Verdrag rechtstreekse

¹⁴⁸

Document IV/403-1/90 van juli 1990, 53 blz.

werking hebben in de Belgische rechtsorde. Ze kunnen dus ook door de Belgische hoven en rechtbanken worden toegepast. Als voorbeeld kan verwezen worden naar het vonnis van de Rechtbank van Koophandel te Brussel, waarbij de RTT-regeling betreffende de levering van PABX-centrales werd afgekeurd¹⁴⁹. Eventueel kan de Belgische rechter, aan wie een geschil wordt voorgelegd betreffende de Europese mededingingsregels, over de toepassing van deze regels een prejudiciële vraag stellen aan het Hof van Justitie. Dat is bijvoorbeeld gebeurd door de Voorzitter van de Rechtbank van Koophandel te Brussel bij wie de RTT een vordering tot staking had ingeleid tegen een grote warenhuisketen die niet gehomologeerde, uit Hong Kong ingevoerde telefoontoestellen verkocht. Deze toestellen werden verkocht aan gevoelig lagere prijzen dan deze die door de RTT werden gevraagd¹⁵⁰. In een arrest van 13 december 1991 (RTT v. GB-Inno-BM, Zaak 18/88) heeft het Europees Hof van Justitie geoordeeld dat de wijze waarop in België de homologatie van telefoontoestellen gebeurde, in strijd was met art. 30 en 90 van het Verdrag. Ondertussen is de reglementering over de homologatie van telefoontoestellen en andere eindapparaten door de wet van 21 maart 1991 volledig veranderd.

2.2.4. De concurrentierichtlijnen over de telecommunicatiemarkt

2.2.4.1. Artikel 90 van het E.E.G.-Verdrag

Naast de artikelen 85 (overeenkomsten, verenigingen en onderling afgestemde gedragingen) en 86 (misbruik van economische machtspositie) is ook artikel 90 van het E.E.G.-Verdrag zeer belangrijk voor de telecommunicatiesector. Het eerste lid van artikel 90 zegt dat de Lid-Staten, met betrekking tot de openbare bedrijven en de ondernemingen waaraan zij bijzondere of uitsluitende rechten verlenen, geen enkele maatregel mogen nemen of handhaven die in strijd is met de regels van het verdrag, met name die bedoeld in de artikelen 7 (discriminatieverbod) en 85 tot en met 94 (de concurrentieregels van het Verdrag). Deze bepaling verbiedt dus niet het verlenen van bijzondere of uitsluitende rechten aan openbare bedrijven. Er mogen alleen geen maatregelen genomen worden die discriminerend zijn of in strijd met de mededingingsregels van het Verdrag.

In het derde lid van artikel 90 staat dan de bepaling waarrond zoveel te doen is in de telecommunicatiesector. Ze voorziet: "De Commissie waakt over de toepassing van dit artikel en richt, voor zover nodig, passende richtlijnen of beschikkingen tot de Lid-Staten". Uit dit artikel volgt dus dat de Commissie ook richtlijnen kan uitvaardigen. Lange tijd heeft men getwijfeld aan de precieze juridische kracht van dit soort richtlijnen. Men stelde dat de richtlijnen die de Commissie uitvaardigt in het kader van artikel 90 van het Verdrag, niet dezelfde draagwijdte kunnen hebben als de richtlijnen van de Raad, die op voorstel van de Commissie, en na advies van het Europees Parlement worden uitgevaardigd.

¹⁴⁹ Rechtbank van Koophandel Brussel, 31 juli 1986, LT, 1987, 345, met noot B. De Crombrughe.

¹⁵⁰ Voorz. Kh., 11 januari 1988, R.T.T. t./ GB-Inno-BM, samengevat in "Handelspraktijken - Jaarboek", 1988, blz. 37.

Het Hof van Justitie heeft deze stelling echter niet gevolgd en besliste dat de richtlijnen en de beschikkingen van de Commissie in toepassing van artikel 90 behoren tot de algemene categorie van richtlijnen en beschikkingen zoals ze worden gedefinieerd in artikel 189 van het Verdrag¹⁵¹.

2.2.4.2. De concurrentierichtlijn over de eindapparatuur

In 1988 heeft de Commissie, in toepassing van artikel 90, een eerste richtlijn uitgevaardigd over de mededinging op de markten van telecommunicatie-eindapparatuur¹⁵². Artikel 1 van deze richtlijn definieert als eindapparatuur "de apparaten die voor overbrenging, verwerking of ontvangst van informatie direct of indirect op de eindpunten van een openbaar telecommunicatienet zijn aangesloten".

Artikel 2 is het centrale artikel van deze richtlijn. Het bepaalt dat de Lid-Staten die aan ondernemingen bijzondere of uitsluitende rechten verlenen van invoer, afzet, aansluiting, opstarten en/of onderhoud van telecommunicatie-eindapparatuur, moeten zorgen voor de opheffing daarvan. De Commissie verplicht m.a.w. de Lid-Staten ertoe om het monopolie van de nationale PTT's op de markt van de eindapparatuur op te heffen en de vrije mededinging toe te laten.

Volgens artikel 3 moeten de Lid-Staten ervoor zorgen dat alle economische subjecten het recht hebben eindapparatuur in te voeren, in de handel te brengen, aan te sluiten, op te starten en te onderhouden. Voor het aansluiten en het opstarten moet de apparatuur wel voldoen aan technische specificaties, en mag verder de noodzakelijke technische kennis opgelegd worden volgens objectieve, niet-discriminerende en openbaar gemaakte criteria.

Tenslotte is ook nog artikel 6 van de richtlijn van belang. Daarin wordt bepaald dat het voortaan niet meer de nationale PTT's zelf mogen zijn die bepalen aan welke normen de eindapparatuur moet voldoen en die de keuringen uitvoeren. De vaststelling van de normen en de keuringsregels, en de controle op de toepassing daarvan moet worden uitgevoerd door een onafhankelijke instantie. Op die manier moet vermeden worden dat de nationale PTT's, die hun eindapparaten in concurrentie met andere leveranciers aanbieden, tegelijk rechter en partij zouden zijn.

Richtlijn 88/301 is voor het Hof van Justitie aangevochten door Frankrijk. Vier andere Lid-Staten (België, Griekenland, Italië en Duitsland) hebben zich bij de klacht van Frankrijk aangesloten. Volgens deze Lid-Staten had de Commissie met deze richtlijn haar bevoegdheid overschreden. De zaak is door het Europees Hof van Justitie beslecht in een arrest van 19 maart

¹⁵¹ Arrest van 30 juni 1988, Commissie t./ Griekenland, Zaak 226/87, Jur. Hof van Justitie, 1988, blz. 3611

¹⁵² Richtlijn 88/301/EEG van de Commissie van 16 mei 1988 betreffende de mededinging op de markten van telecommunicatie-eindapparatuur, PB nr. L 131 van 27/5/1988, blz. 73.

1991. Het Hof bevestigde grotendeels het standpunt van de Commissie maar vernietigde niettemin sommige artikelen van de richtlijn omdat de Commissie haar interventie onvoldoende had gemotiveerd. In de praktijk heeft deze vernietiging niet veel gevolgen meer. Het beroep van de Lid-Staten tegen de richtlijn heeft niet de uitvoering ervan geschorst; alle Lid-Staten hebben de regels van de Richtlijn intussen in hun nationale wetgeving opgenomen. In België gebeurde dit door de wet van 21 maart 1991 (zie hierna).

2.2.4.3. De concurrentierichtlijn over de diensten

Ondertussen heeft de Commissie al werk gemaakt van een tweede richtlijn voor de telecom-municatiesector op grond van artikel 90 van het Verdrag. Ditmaal handelt de richtlijn over de mededinging op de markten voor telecommunicatiediensten¹⁵³.

Rekening houdende met de kritiek tegen de richtlijn over de eindapparatuur, is de Commissie met de richtlijn over de diensten veel voorzichtiger te werk gegaan.

Dat blijkt in de eerste plaats uit de zeer uitvoerige motivering. In niet minder dan 33 zorgvuldig geformuleerde overwegingen duidt de Commissie thans aan op welke punten de huidige stelsels van de Lid-Staten die uitzonderlijke en exclusieve rechten toekennen aan openbare bedrijven met betrekking tot de telecommunicatiediensten, onverenigbaar zijn met artikel 90, lid 1 van het Verdrag, in samenhang met artikel 86. Verder is de Commissie ook zo voorzichtig geweest om haar richtlijn, hoewel dat eigenlijk niet hoefde, vooraf voor te leggen aan de Raad. De bespreking van de richtlijn van de Commissie gebeurde daar samen met de bespreking over de ONP-kaderrichtlijn, waarover hierna nog in detail wordt gesproken.

De richtlijn van de Commissie over de telecommunicatiediensten is niet van toepassing op radio-omroep en televisie. Ze is verder ook niet toepasselijk op de telexdienst, de mobiele radiotelefonie en de semafoon. Oorspronkelijk was ze ook niet van toepassing op satelliet-communicatie, maar dit veranderde door de wijzigingen aangebracht door de richtlijn 94/46/EG van 13 oktober 1994.

Artikel 2 bepaalt dat de Lid-Staten de bijzondere of uitsluitende rechten voor het aanbod van andere telecommunicatiediensten dan de spraaktelefoondienst moeten afschaffen en de maatregelen moeten nemen die nodig zijn om het recht te waarborgen van alle marktdeelnemers om deze telecommunicatiediensten aan te bieden.

Het begrip "spraaktelefoondienst" wordt eng gedefiniëerd als "de commerciële exploitatie ten behoeve van het publiek van direct transport en schakeling van spraak in real-time van en naar aansluitpunten van het geschakelde openbaar netwerk, waar van iedere gebruiker van op een dergelijk aansluitpunt aangesloten apparatuur gebruik kan maken om met een ander aansluitpunt

¹⁵³ Richtlijn nr. 90/388/EEG van de Commissie van 28 juni 1990 betreffende de mededinging op de markten voor telecommunicatiediensten, PB. nr. L 192 van 24/7/1990, blz. 10.

te communiceren". Uit deze definitie volgt dat o.m. "voice messaging" systemen, telefoondiensten voor een gesloten gebruikersgroep, "voice refiling/low-cost routing (het opslaan van een gesprek om vervolgens de goedkoopste route te berekenen), audiotex, e.a. niet onder het begrip "spraaktelefoon dienst" vallen.

Het moeilijkste punt is natuurlijk wat onder "diensten" (met toegevoegde waarde) moet worden verstaan. In geen enkele wetgeving vindt men daarvan een bevredigende definitie. De grondidee is de levering van diensten die "iets" toevoegen aan het basistransport zoals dat wordt verzorgd door de telecommunicatie-administratie. Waar echter het basistransport eindigt en de toegevoegde waarde begint, is een groot discussiepunt. Uit de richtlijn kan men opmaken dat volgende diensten als "diensten met toegevoegde waarde" worden aanzien: protocol-conversie, informatiediensten als instrument voor de toegang tot databanken, gegevensverwerking op afstand, elektronische post, transactiediensten zoals bijvoorbeeld voor het elektronisch geldverkeer of EDI, teleshopping, telereservatie en telebesturing.

Volgens het tweede lid van artikel 2 van de richtlijn kunnen de Lid-Staten het aanbieden van telecommunicatiediensten doen afhangen van de naleving van een vergunnings- of aanmeldingsprocedure, maar de vergunningen moeten worden verleend volgens objectieve, niet-discriminerende en duidelijke criteria. De eventuele weigering van een vergunning moet gemotiveerd zijn en er moet worden voorzien in een procedure om tegen dergelijke weigeringen in beroep te gaan.

Artikel 3 bevat de bepalingen over de pakket- en circuitgeschakelde datadiensten (regeling over de doorverkoop van capaciteit en lastencohier van openbare dienstverlening).

Betreffende de infrastructuur, bepaalt artikel 4 dat, overal waar nog bijzondere of uitsluitende rechten blijven bestaan voor de aanleg en de exploitatie van openbare telecommunicatienetten, de nodige maatregelen moeten genomen worden om de voorwaarden voor de toegang tot de netwerken openbaar, objectief en niet-discriminerend te maken. De gebruikers die een aanvraag indienen, moeten binnen een redelijke termijn huurlijnen krijgen. Bij elke verhoging van het tarief voor huurlijnen moeten de Lid-Staten aan de Commissie de gegevens meedelen aan de hand waarvan de gegrondheid van deze verhoging kan worden beoordeeld.

In artikel 5 van de richtlijn staat dat de kenmerken van de technische interfaces die nodig zijn voor het gebruik van de openbare telecommunicatienetten uiterlijk op 31 december 1990 moeten worden gepubliceerd.

Artikel 6 zegt dat ten aanzien van het verlenen van telecommunicatiediensten, alle bestaande beperkingen met betrekking tot de verwerking van signalen voorafgaand aan hun transmissie via het openbaar net of na hun ontvangst, moeten afgeschaft worden, tenzij wordt aangetoond dat deze beperkingen noodzakelijk zijn om de openbare orde of essentiële eisen te doen naleven. Verder moeten de Lid-Staten er ook voor zorgen dat de dienstenverleners, telecommunicatie-organisaties inbegrepen, ten aanzien van de gebruiksvoorwaarden, noch ten aanzien van de

tarieven worden gediscrimineerd. Ook hiervoor geldt 31 december 1990 als uiterste datum.

Op te merken valt dat de zojuist vermelde artikelen 4, 5 en 6 van de richtlijn eigenlijk de volledige problematiek dekken van de ONP. Zij handelen namelijk over de toegangsvoorwaarden, de publicatie van de kenmerken van de interfaces en de tariefbeginselen. In die zin overlapt de concurrentierichtlijn over de diensten derhalve de ONP-richtlijn van de Raad, waarover later in dit cursusonderdeel wordt gesproken.

Vanaf 1 juli 1991 geldt de verplichting om de toekenning van exploitatievergunningen, de controle op de typegoedkeuringen en op de verplichte specificaties, de toekenning van frequenties en het toezicht op de gebruiksvoorwaarden toe te vertrouwen aan een instantie die onafhankelijk is van de telecommunicatieorganisaties (artikel 7). De combinatie van regelgevende bevoegdheden met de exploitatie-activiteiten van de administraties, maakt een misbruik van economische machtspositie uit in de zin van artikel 86 van het Verdrag (overweging 25). De Commissie heeft evenwel de graad van onafhankelijkheid die vereist is om aan de richtlijn te voldoen, niet gespecificeerd. Dat wordt door velen terecht betreurd.

In artikel 8 staat dat, zodra de betrokken bijzondere of uitsluitende rechten zijn afgeschaft, de telecommunicatieorganisaties hun klanten die door een overeenkomst voor het aanbieden van telecommunicatiediensten voor langer dan één jaar zijn gebonden, de mogelijkheid moeten geven om deze overeenkomst met een termijn van zes maanden op te zeggen. Artikel 9 legt aan de Lid-Staten op om aan de Commissie alle informatie door te spelen voor het maken van een jaarverslag over de toepassing van de richtlijn. Verder zegt artikel 10 dat er in 1992 vanwege de Commissie een globale evaluatie komt van de situatie in de sector van de telecommunicatiediensten. De reeds vermelde herzieningsclausule sluit deze richtlijn af.

2.2.5. Onderlinge erkenning van eindapparatuur

2.2.5.1. De richtlijn van 1986

In juli 1986 heeft de Raad op voorstel van de Commissie een richtlijn betreffende de eerste fase van de wederzijdse goedkeuringen van eindapparatuur voor telecommunicatie goedgekeurd¹⁵⁴.

Het probleem is bekend. Door de verschillende technische vereisten in elke Lid-Staat wordt de handel in eindapparatuur voor telecommunicatie tussen de Lid-Staten erg bemoeilijkt. Aanpassingen aan eindapparatuur, noodzakelijk om conform te zijn met de vereisten in een andere Lid-Staat dan die van de fabricant, kunnen zeer vaak enkel door die fabricant zelf uitgevoerd worden, en leveren daardoor voor eventuele invoerders bijna onoplosbare problemen op.

¹⁵⁴ Richtlijn nr. 86/361/EEG van de Raad van 24 juli 1986 betreffende de eerste fase van de wederzijdse erkenning van goedkeuringen van eindapparatuur voor telecommunicatie, PB. nr. L 217 van 5/8/1986, blz. 21.

Nog zwaarder weegt het feit dat elke Lid-Staat - voor de Unie dus vijftien maal - aparte en verschillende erkenningsprocedures heeft. Een fabricant die zijn eindapparatuur in de ganse Unie wil verhandelen moet dus vijftien keer in de rij gaan staan om een erkenning te bekomen.

Deze barrières zijn zodanig in strijd met de idee van een Europese gemeenschappelijke markt, dat de Commissie reeds vanaf 1985 zich over dit probleem aan het werk heeft gezet.

De richtlijn van 1986 was een eerste, zeer schuchtere stap om op dit vlak de regelingen in de Lid-Staten dichterbij elkaar te brengen. De richtlijn beperkt zich tot de wederzijdse erkenning van de "resultaten van de conformiteitsproeven voor eindapparatuur". Aan de Lid-Staten werd dus gevraagd om, wanneer een eindapparaat in een andere Lid-Staat reeds aan conformiteitsproeven was onderworpen, met de resultaten daarvan rekening te houden. Op die manier hoopte men minstens te vermijden dat een eindapparaat in verschillende Lid-Staten aan identieke testen zou worden onderworpen.

Omdat de vereisten en de procedures van de Lid-Staten zover uiteen lopen, komt de situatie van identieke testen en het nut van overname van resultaten van testen, uitgevoerd in andere Lid-Staten niet zoveel voor. Het praktisch belang van de richtlijn van 1986 is dan ook zeer gering gebleven.

2.2.5.2. Naar een volledige wederzijdse erkenning?

Overeenkomstig artikel 9 van de richtlijn van 1986, moest de Commissie bij de Raad een voorstel indienen om de wederzijdse erkenning van goedkeuringen van eindapparatuur, verder uit te werken. De Commissie heeft daaraan gevolg gegeven met een voorstel voor een richtlijn van de Raad, ingediend in juli 1989. Dit leidde tot de richtlijn van 29 april 1991 (PB L128, 23/5/91).

De richtlijn heeft twee strategische beleidspunten op het oog, die in de Resolutie van de Raad van 30 juni 1988 inzake de ontwikkeling van de gemeenschappelijke markt voor telecommunicatiediensten en -apparatuur tot 1992¹⁵⁵, werden vastgesteld.

- "1. Het tot stand brengen of waarborgen van de integriteit van de netwerkinfrastructuur in de gehele Unie als een van de essentiële factoren voor een gemeenschappelijke markt voor telecommunicatiediensten en -apparatuur, waarbij wordt uitgegaan van het beginsel van volledige interconnectiviteit van alle betrokken netten in de Unie."
- "2. Verdere ontwikkeling van een open Communautaire markt voor eindapparatuur. Hiertoe moet spoedig overeenstemming worden bereikt over de volledige wederzijdse erkenning van typegoedkeuring van eindapparatuur op basis van gemeen-

155

PB nr. C 257 van 4/10/1988, blz. 1.

schappelijke conformiteitsspecificaties."

De belangrijkste elementen van de richtlijn zijn de volgende:

- eindapparatuur mag op de markt worden gebracht, indien de conformiteit met bindende technische voorschriften ten aanzien van een aantal essentiële eisen is gecontroleerd; deze technische voorschriften worden gebaseerd op normen die binnen het communautaire normalisatiesysteem zijn ontwikkeld en waarvan de bindende status wordt bereikt via een nieuw op te richten comité (ACTE);
- de conformiteit van een terminal met relevante technische voorschriften kan worden gecontroleerd volgens twee procedures: de EG-type-onderzoeksprocedure of de procedure van de EG-verklaring van overeenstemming; in beide gevallen dient een derde partij als controlerend orgaan te fungeren; de keuze tussen de beide procedures wordt overgelaten aan de fabrikant die de eindapparatuur op de markt wil brengen;
- de EG-type-onderzoeksprocedure resulteert in het afgeven van een EG-type-onderzoekscertificaat dat in de gehele Unie geldig is; op de terminals kan dan een CE-merkteken worden aangebracht;
- de EG-verklaring van overeenstemming is gebaseerd op een door een derde partij goedgekeurd kwaliteitssysteem, voor ontwerp, fabricage, eindcontrole en testen; via die weg wordt dus een horizontale integratie van de controleprocedures in alle fabricagestappen mogelijk;
- eindapparatuur voorzien van het CE-merkteken wordt toegelaten op de gehele Communautaire markt en er zijn geen verdere procedures vereist voor aansluiting op de openbare netwerken.

2.2.6. Open Network Provision ("ONP")

2.2.6.1. Begrip

Het begrip "ONP" is opgedoken bij de voorbereiding van het Groenboek. In dat Groenboek staat over ONP het volgende:

"Wil men voorkomen dat er een grote reeks geschillen ontstaat (tussen de "PTT's" en de private dienstenleveranciers), dan zal de Unie gemeenschappelijke principes moeten opstellen voor de algemene voorwaarden waaronder de netwerkinfrastructuur door de telecommunicatie-administraties ter beschikking van gebruikers en aanbieders van concurrerende diensten wordt gesteld"¹⁵⁶.

Hoewel dat vaak zo gesteld wordt, heeft ONP op communautair vlak minder te maken met garanties voor private dienstenleveranciers tegenover de telecommunicatie-administraties, om te beletten dat deze laatsten misbruik zouden kunnen maken van het feit dat zij enerzijds het monopolie hebben over de infrastructuur, maar anderzijds ook aanbieder zijn van concurrerende

¹⁵⁶

Groenboek blz. 69.

diensten. Het is natuurlijk niet denkbeeldig dat de telecommunicatie-administraties zichzelf bij de toegang tot de infrastructuur en de gebruiksvoorwaarden van het openbaar netwerk zouden bevoordelen.

ONP heeft echter meer te maken met harmonisatie. Vanuit het oogpunt van de Unie is het van zeer groot belang dat de toegangsprincipes voor de openbare netwerken niet te veel verschillen, omdat dat een ééngemaakte telecommunicatiemarkt in de weg staat. Tè grote verschillen in die toegangsprincipes vormen namelijk een belangrijke barrière voor het aanbieden van grensoverschrijdende diensten.

Daarom wordt reeds in Groenboek voorgesteld om hierover richtlijnen uit te werken. In deze richtlijnen zou dan moeten worden omschreven welke toegangsvoorwaarden de telecommunicatie-administraties dienen te hanteren voor het gebruik van het netwerk door aanbieders van grensoverschrijdende diensten.

De belangrijkste uitgangspunten van "ONP" zijn de volgende:

- geharmoniseerde ONP-voorwaarden moeten op objectieve criteria zijn gebaseerd, doorzichtig en voldoende publiek zijn en gelijkheid van toegang waarborgen;
- de uitwerking van de ONP-voorwaarden moet geleidelijk gebeuren en de nadruk moet liggen op harmonisatie;
- in het kader van de globale communautaire aanpak van de Europese normalisatie, moeten er Europese normen uitgewerkt worden voor een open netwerk.

De drie hoofdgebieden voor de ontwikkeling van geharmoniseerde ONP-voorwaarden zijn de volgende:

- definitie van geharmoniseerde technische interfaces ;
- definitie van geharmoniseerde gebruiksvoorwaarden, zoals leveringstermijnen, contractduur, kwaliteit van de dienstverlening, voorwaarden voor gedeeld gebruik, doorverkoop van capaciteit, enz...;
- definitie van geharmoniseerde tariefbeginselen, gebaseerd op de kosten, duidelijk bekendgemaakt en zonder discriminatie toegepast.

Reeds in 1988 werd een aanvang gemaakt met het definiëren van ONP-voorwaarden voor huurlijnen. Dit heeft tot een voorstel van richtlijn geleid, dat hierna nog ter sprake komt. Tegelijk werd door de Commissie voorgesteld om over ONP een kaderrichtlijn uit te werken¹⁵⁷. De bedoeling van deze kaderrichtlijn zou erin bestaan het geleidelijke harmonisatieproces voor de ONP-voorwaarden te omschrijven en een tijdschema vast te stellen voor de realisatie ervan.

¹⁵⁷ Mededeling van de Commissie over de stand van de definitie van Open Network Provision, COM(88) 718 def., blz. 8.

2.2.6.2. De kaderrichtlijn van 28 juni 1990

De belangrijkste elementen van de kaderrichtlijn van 28 juni 1990¹⁵⁸ zijn de volgende:

- In het Publikatieblad van de Europese Unie zullen verwijzingen worden gepubliceerd naar voor ONP geschikt geachte normen, opgesteld i.s.m. het ETSI, om als grondslag te dienen voor geharmoniseerde technische interfaces en/of geharmoniseerde kenmerken van diensten. Deze normen hebben geen verplichtend maar enkel een facultatief karakter. Evenwel zullen de dienstenleveranciers die deze normen hanteren, de betrokken diensten in de ganse Unie kunnen aanbieden. De telecommunicatie-organisaties die deze normen hanteren, worden verondersteld daarmee aan de eis inzake open en efficiënte toegang te voldoen (artikel 5).
- Indien het hierboven beschreven systeem in de praktijk niet voldoende blijkt om de interoperabiliteit van grensoverschrijdende diensten in de Unie te waarborgen, kan de verwijzing naar de Europese normen verplicht worden gesteld, voor zover zulks strikt nodig is om deze interoperabiliteit en de verbetering van de vrije keuze van de gebruiker te waarborgen (echter zonder afbreuk te doen aan de toepassing van de artikelen 85 en 86 van het Verdrag). Het is zeer onwaarschijnlijk dat er dergelijke verplichte normen zullen komen voor diensten met toegevoegde waarde. Het systeem is vooral bedoeld voor basisdiensten zoals pakketgeschakelde datatransmissie en ISDN.
- Er zal een strikt tijdschema gehanteerd worden voor de invoering van ONP-voorwaarden. Op dit moment zijn er reeds ONP-richtlijnen voor huurlijnen en voor spraaktelefonie. Over ISDN en pakketgeschakelde datadiensten werden Aanbevelingen uitgevaardigd¹⁵⁹.

2.2.6.3. De richtlijn over de toepassing van ONP op huurlijnen

Op 5 juni 1992 werd door de Raad een richtlijn over de toepassing van ONP op huurlijnen uitgevaardigd¹⁶⁰. De richtlijn handelt over de harmonisatie van niet-discriminerende voorwaarden voor een open en efficiënte toegang tot (en gebruik van) huurlijnen in openbare telecommunicatienetwerken. Ze wil tegelijk ook voorzien in de beschikbaarheid van minstens één geheel van geharmoniseerde huurlijnen dat gans het grondgebied van de Unie bestrijkt (artikel 1).

In de eerste plaats legt de richtlijn aan de Lid-Staten op om een aantal gegevens betreffende huurlijnen te publiceren: de technische kenmerken van de aangeboden huurlijnen en de

¹⁵⁸ Richtlijn nr. 90/387/EEG van de Raad van 28 juni 1990 betreffende de totstandbrenging van de interne markt voor telecommunicatiediensten door middel van de tenuitvoerlegging van Open Network Provision (ONP), PB nr. L 192 van 24/7/1990, blz. 1.

¹⁵⁹ Aanbeveling 92/383 van 5 juni 1992 over ISDN en Aanbeveling 92/382 van dezelfde datum over pakketgeschakelde datadiensten, beide gepubliceerd in Pub. E.G. nr. L 200 van 18 juli 1992.

¹⁶⁰ PB nr. L 165 van 19 juni 1992, blz. 27

verwijzingen naar de toegepaste normen, de tarieven, voorwaarden voor de aansluiting van eindapparatuur en algemene leveringsvoorwaarden, zoals de leveringstermijn, de contractduur en de interventietijd bij storingen. Al deze informatie moet voldoende kenbaar gemaakt worden zodat ze voor alle potentiële gebruikers gemakkelijk toegankelijk is.

Betreffende nieuwe aanbiedingen van huurlijnen door de telecommunicatie-organisaties, moeten de Lid-Staten erover waken dat voor de toegankelijkheid van de informatie hierover, geen discriminatie ontstaat tussen de TO's, als gebruiker van huurlijnen voor de aanbieding van concurrerende telecommunicatiediensten, en andere huidige of potentiële gebruikers. Het is nog niet duidelijk hoe de naleving van dergelijke verplichting kan gecontroleerd worden.

In het kader van de algemene voorwaarden zullen specifieke leveringsvoorwaarden deel uitmaken van de overeenkomst voor de huur van lijnen. Als er een wijziging komt in de algemene leveringsvoorwaarden moeten die minstens twee maanden vooraf meegedeeld worden aan de gebruikers. De specifieke voorwaarden moeten, behoudens toestemming van de gebruiker, onveranderd blijven tot het einde van de contractperiode (artikel 4).

In artikel 5 van de richtlijn wordt het begrip "essentiële vereisten" nader omschreven op het terrein van de huurlijnen. Dit begrip komt in zeer vele richtlijnen van de Europese Unie voor, niet alleen op het domein van de telecommunicatie. Het begrip komt uit de rechtspraak van het Hof van Justitie en met name uit het bekende arrest "Cassis de Dijon"¹⁶¹. Volgens dat arrest zijn er overeenkomstig de verdragsbepalingen over het vrij verkeer van goederen, geen hinderpalen voor het goederenverkeer mogelijk, wanneer het gaat om produkten die aan de "essentiële vereisten" (te specificeren in elke sector) voldoen. Deze rechtspraak is gesteund op het principe dat produkten in de verschillende Lid-Staten vaak aan andere voorschriften onderworpen zijn, maar dat deze voorschriften nooit een hinderpaal mogen vormen voor het vrij goederenverkeer, tenzij daardoor essentiële belangen in het gedrang komen. Het typisch voorbeeld van een dergelijk essentieel belang is de bescherming van de gezondheid. Thans probeert men voor verschillende sectoren te komen tot Europese definities van deze "essentiële vereisten".

In de ONP-kaderrichtlijn worden de "essentiële eisen" voor de telecommunicatiesector gedefiniëerd als volgt:

"redenen van algemeen belang en van niet-economische aard die een Lid-Staat ertoe kunnen bewegen de toegang tot het openbare telecommunicatienetwerk of de openbare telecommunicatiediensten te beperken. Deze redenen zijn de veiligheid van het functioneren van het netwerk, het behoud van netwerkindegriteit en, in gerechtvaardigde gevallen, de interoperabiliteit van de diensten en de bescherming van gegevens.

Gegevensbescherming kan bestaan uit de bescherming van persoonlijke gegevens, het vertrouwelijk karakter van informatie die wordt doorgegeven en/of

¹⁶¹

Zaak 120/78.

opgeslagen, alsmede de bescherming van de persoonlijke levenssfeer."¹⁶².

De bijlage 2 van de kaderrichtlijn voorziet in de concretisatie ervan naar bepaalde domeinen toe door specifieke richtlijnen. De Richtlijn 92/44/EEG van de Raad van 5 juni 1992 betreffende de toepassing van Open Network Provision (ONP) op huurlijnen (PB. L. 165, 19 juni 1992, 27) geeft hieraan een eerste uitvoering. Bij elke beperking van de toegang of het gebruik van het openbaar netwerk of van publieke diensten waarbij deze essentiële belangen worden ingeroepen moeten specifieke procedures gevolgd worden (informatie aan de gebruiker, aan het publiek en aan de Commissie, enz...). Voor de bescherming van persoonsgegevens wordt verwezen naar de voorgestelde richtlijn die de Commissie hierover heeft ingediend.

Artikel 6 van de richtlijn bepaalt dat er geen technische beperkingen mogen opgelegd of gehandhaafd worden voor de interconnectie van huurlijnen onderling of voor de interconnectie van huurlijnen met het openbaar telecommunicatienetwerk.

In artikel 7 wordt aan de Lid-Statens opgelegd dat hun telecommunicatie-organisaties afzonderlijk of samen een minimum set van huurlijnen zouden aanbieden, om in heel de Unie een minimum aanbod te waarborgen. Als boven dit minimum aanbod nog andere types van huurlijnen aangeboden worden, dan mag dit toch geen afbreuk doen aan de verplichting om de minimumset aan te bieden (artikel 8).

In géén geval mogen de telecommunicatie-organisaties de huurlijnen onderbreken of het gebruik ervan beperken omdat een gebruiker de bijzondere of exclusieve rechten of het verbod van eenvoudige doorverkoop van capaciteit met de voeten getreden zou hebben.

2.2.6.4. Perspectieven

In de schoot van de Commissie wordt gewerkt aan de ONP-voorwaarden voor publieke datanetwerken, voor spraaktelefonie en voor ISDN.

De Commissie verwacht dat de Europese eenheidsmarkt de vraag naar trans-Europese telecommunicatiediensten zal doen toenemen. Daarom wil men zo snel mogelijk uniforme trans-Europese telecommunicatienetwerken realiseren.

Op het domein van de telecommunicatie via satellieten vermeldt het Groenboek dat een zekere mate van vrije mededinging noodzakelijk is, indien dit niet de overige functies van de satellieten in de weg staat en de financiële leefbaarheid van de leveranciers van de infrastructuur niet in het gedrang brengt. Ondertussen is er een specifiek groenboek over

¹⁶² Artikel 2, punt 6 van de Richtlijn nr. 90/387/EEG van de Raad van 28 juni 1990 betreffende de totstandbrenging van de interne markt voor telecommunicatiediensten door middel van de tenuitvoerlegging van Open Network Provision, PB nr. L 192 van 24/7/1990, blz.2.

satellietcommunicatie verschenen. Daarin wordt een verregaande liberalisering van het "aarde-segment" (ontvangstterminalen, zendapparaten, vrije toegang tot het "ruimtesegment") voorgesteld.

Op het domein van ISDN (Integrated Services Digital Networks) wordt naar een gecoördineerde invoering op Europees vlak gestreefd (eenvormige interfaces, definitie van trans-Europese diensten, eenvormige tarifieringssystemen, eenvormige abonneenummers,...). In dezelfde richting wordt ook aan een Europees *mobilofoonnetwerk* gewerkt. De moeilijkheden die men daarbij ondervindt worden wellicht best geïllustreerd met de vermelding dat er in 1986 in de Unie nog zes verschillende, onderling volstrekt incompatibele autotelefoonsystemen werden gebruikt.

Er werd een actieplan 1993-1998 opgesteld, dat de liberalisering van de spraaktelefoniedienst voorziet tegen uiterlijk 1 januari 1998.

2.3. DE HERVORMING VAN DE BELGISCHE TELECOMMUNICATIEMARKT

2.3.1. Inleiding

De wetgeving over de telecommunicatiesector moet in België thans gezocht worden in de wet van 21 maart 1991 "betreffende de economische overheidsbedrijven".

2.3.1.1. De "autonome overheidsbedrijven"

Titel I van de wet van 21 maart 1991 bevat een nieuw statuut voor de "autonome overheidsbedrijven". Deze hervorming is vooral ingegeven door de groeiende concurrentie van privé-bedrijven op terreinen die traditioneel voorbehouden waren voor de overheid (men denke bijv. aan de concurrentie tussen de Post en de private koerierdiensten). Het afschermen van deze terreinen wordt steeds moeilijker, vanwege de verplichtingen, opgelegd door de Europese Unie, om werk te maken van de afbouw van concurrentievervalsende subsidiëring aan overheidsbedrijven en van de exclusieve rechten van deze bedrijven. De Belgische overheid wil dus snel wat meer efficiëntie en dynamiek in de overheidsbedrijven krijgen, zodat ze de concurrentie met de privé-sector en, in het licht van de Europese eenheidsmarkt, ook met buitenlandse overheidsbedrijven, kunnen doorstaan. Bovendien zal de kwaliteit van de overheidsdiensten, vooral op het gebied van communicatie en vervoer steeds meer een belangrijke rol gaan spelen bij investeringsbeslissingen.

Om al deze redenen wilde men aan een reeks overheidsbedrijven die actief zijn in commerciële of industriële sectoren, meer armslag geven. Dat is gebeurd in de wet van 21 maart 1991 door aan deze bedrijven een grotere autonomie te verlenen op het vlak van tarieven, beheer, sluiten van samenwerkingsakkoorden, personeelsbeleid, enz... Om, tegenover het winstbejag van de nieuwe overheidsbedrijven, toch nog enige bescherming

te bieden aan de individuele gebruikers, worden inspraakorganen en "ombudsdiensten" in het leven geroepen.

Elke instelling van openbaar nut die over beheersautonomie moet beschikken om te kunnen functioneren in een industriële of commerciële sector, kan, na aanpassing van haar statuut door de wetgever, de nieuwe autonomie verkrijgen door het sluiten van een beheerscontract met de Staat. Het beheerscontract is een overeenkomst waarbij de "opdrachten van openbare dienst" worden gedefiniëerd en waarbij de uitvoeringsmodaliteiten van deze opdrachten worden overeengekomen. Een autonoom overheidsbedrijf sluit een beheerscontract derhalve uitsluitend voor zijn opdrachten van openbare dienst. Voor het overige kan het onder de regels van het gemeen recht alle overeenkomsten sluiten die nodig worden geacht.

Voor vier specifieke instellingen wordt de eerste stap naar het nieuwe statuut reeds in de wet van 21 maart 1991 zelf gezet: 1) de Regie van telegraaf en telefoon (RTT), 2) de Regie der Posterijen, 3) de Nationale Maatschappij der Belgische Spoorwegen en 4) de Regie der luchtwegen. In wat volgt, richten we onze aandacht enkel op de hervorming van de RTT.

2.3.1.2. Een nieuwe telecommunicatiereglementering

De Titels II en III van de wet van 21 maart 1991 houden, naast de hervorming van de RTT in een "autonoom overheidsbedrijf", tevens een nieuwe regeling in voor de telecommunicatiesector in zijn geheel. De Belgische reglementering van de telecommunicatiemarkt was namelijk nog niet aangepast aan de richtlijnen van de Europese Unie. Het overheidsmonopolie van de RTT, zowel inzake infrastructuur en eindapparatuur, als inzake telecommunicatiediensten, was nog vrijwel onaangeroerd.

Hierna overlopen we de belangrijkste bepalingen over de telecommunicatiemarkt uit de bovengenoemde wet. Achtereenvolgens behandelen we de hervorming van de instellingen en de hervorming van de spelregels op de Belgische telecommunicatiemarkt.

2.3.2. De hervorming van de instellingen

2.3.2.1. Overzicht

Vanuit het oogpunt van de institutionele hervorming van de telecommunicatiesector diende de wet van 21 maart 1991 verschillende doeleinden tegelijk te realiseren. In de eerste plaats was het de bedoeling om aan de RTT nieuwe mogelijkheden te geven om concurrentiëel te blijven op de - binnenkort eengemaakte - Europese telecommunicatiemarkt. Tegelijk diende de rol van de RTT als openbare dienst te worden beveiligd, zonder dat dit de vrije concurrentie mocht in de weg staan. In de derde plaats moesten, overeenkomstig de Europese richtlijnen, de functies van de RTT enerzijds als leverancier

en dus mededinging op de telecommunicatiemarkt, anderzijds als regulerende instantie van diezelfde markt, van elkaar gescheiden te worden.

Om aan deze verschillende doelstellingen te voldoen, heeft de wetgever een institutionele constructie met de volgende acteurs bedacht:

- de Minister van PTT houdt de belangrijkste touwtjes van het telecommunicatiegebeuren in handen, o.m. door het onderhandelen en sluiten van het beheerscontract, door het toezicht op Belgacom (de nieuwe benaming van de RTT) via een regeringscommissaris en, vooral, via het beheer van het B.I.P.T. (Belgisch Instituut voor Postdiensten en Telecommunicatie);
- Belgacom is het nieuwe autonome overheidsbedrijf dat het operationele en commerciële deel van de vroegere Regie overneemt; het bedrijf is, enerzijds, verantwoordelijk voor de openbare telecommunicatiediensten, anderzijds speelt het ook mee op de telecommunicatiemarkt als gewone leverancier, in concurrentie met de privé-bedrijven; binnen Belgacom vinden we de volgende organen:
- het directiecomité, met aan het hoofd een gedelegeerd-bestuurder, voor het dagelijks beheer;
- de raad van bestuur, met aan het hoofd een voorzitter, oefent toezicht uit op het directiecomité;
- de regeringscommissaris oefent, in naam van de Minister, het administratief toezicht uit op Belgacom;
- een college van commissarissen controleert de financiële toestand en de jaarrekening;
- een paritair comité, dat voor de helft is samengesteld uit leden van de raad van bestuur en voor de andere helft uit personeelsleden aangeduid door de representatieve vakorganisaties (art. 30);
- een dienst "ombudsman", bestaande uit twee leden (een Nederlandstalige en een Franstalige), bevoegd voor de contacten met de gebruikers.
- het "Belgisch Instituut voor Postdiensten en Telecommunicatie" wordt de regulerende instantie voor de telecommunicatiemarkt; het blijft echter volledig onder de controle van de Minister; bij het Instituut vinden we een Raadgevend Comité, samengesteld uit vertegenwoordigers van de diverse partijen op de telecommunicatiemarkt.

2.3.2.2. Inrichting van Belgacom

Om de breuk met het verleden goed in de verf te zetten, wordt de RTT door de wet van 21 maart 1991 omgedoopt in "Belgacom" (art. 55).

Belgacom krijgt twee bestuursorganen: een raad van bestuur en een directiecomité. Hun leden worden voor een beperkte duur van zes jaar benoemd. De hernieuwing van hun mandaat moet, volgens de wet, afhangen van hun verwezenlijkingen inzake de uitvoering van het beheerscontract en het ondernemingsplan.

Het **ondernemingsplan** is een document dat jaarlijks door de raad van bestuur wordt opgesteld en waarin de doelstellingen en de strategie op middellange termijn worden beschreven. Het is een meerjarenplan dat jaarlijks kan worden bijgestuurd op basis van de ondernemingsresultaten. Enkel de onderdelen van het ondernemingsplan die de taken van openbare dienst betreffen, moeten goedgekeurd worden door de Minister. De andere onderdelen worden enkel ter informatie aan de Minister meegedeeld (art. 26).

Het beheerscontract is een overeenkomst tussen Belgacom en de Belgische Staat over de uitvoering van de taken van openbare dienst. Het zou een echte overeenkomst moeten zijn, die gesloten wordt voor een termijn van tenminste drie en ten hoogste vijf jaar. Tijdens de parlementaire debatten stelde de regering dat, hoewel het om een contract gaat tussen publiekrechtelijke personen (Belgacom en de Belgische Staat) betreffende de uitoefening van opdrachten van openbare dienst, het beheerscontract niettemin door de regels van het gemeen recht wordt beheerst. Artikel 1184 van het Burgelijk Wetboek is echter niet van toepassing (art. 3, § 3, lid 2), zodat noch de Staat, noch Belgacom de ontbinding van het beheerscontract kunnen vorderen. Bovendien worden ook alle uitdrukkelijke ontbindende voorwaarden uitgesloten. In geval van gebrekkige uitvoering riskeert Belgacom dus enkel schadevergoeding of eventueel een specifieke sanctie die echter dan wel in het beheerscontract voorzien moet zijn.

Het beheerscontract is dus geen "administratief contract". Het is geen "concessie-overeenkomst", waarop volgens het Hof van Cassatie niet uitsluitend de regels van het Burgerlijk Wetboek maar tevens de algemene beginselen van behoorlijk bestuur toepasselijk zijn.

Wat staat er in het beheerscontract? Vooreerst de opsomming van de taken die Belgacom op zich neemt ter vervulling van zijn opdrachten van openbare dienst. Vervolgens de principes voor de tarifiering van de prestaties van openbare dienst die door Belgacom worden geleverd, de gedragsregels ten aanzien van de gebruikers van de openbare dienst, de subsidie die Belgacom van de Staat ontvangt voor de uitvoering van de taken van openbare dienst, de eventuele vergoedingen die Belgacom aan de Staat moet betalen in ruil voor de exclusieve concessies, de inhoudstafel van het ondernemingsplan en eventuele sancties bij gebrekkige uitvoering van het beheerscontract. Daarnaast vermeldt de wet ook een reeks bepalingen die op facultatieve wijze in het beheerscontract kunnen worden opgenomen, zoals bijvoorbeeld de bestemming van de netto-winst (art. 3, § 2).

De Minister onder wiens bevoegdheid Belgacom ressorteert, is volgens de wet ook degene die het beheerscontract met Belgacom onderhandelt en sluit (art. 4, § 1). Op het eerste gezicht lijkt dus de betrokken Minister met zichzelf moet onderhandelen. In de praktijk is het beheerscontract een beleidsdocument dat door de afgevaardigde-bestuurder en zijn directiecomité wordt opgesteld, en waarover vervolgens, via onderhandelingen, het fiat van de regering moet bekomen worden. Van de zijde van Belgacom wordt over

het beheerscontract weliswaar onderhandeld door het directiecomité maar het is de raad van bestuur die uiteindelijk bij tweederde meerderheid beslist. Het contract treedt pas in werking na goedkeuring bij Koninklijk besluit dat in Ministerraad moet zijn overlegd. De inhoud ervan - behalve de bepalingen die industriële of commerciële geheimen bevatten - wordt in het Staatsblad gepubliceerd (art. 6, lid 2).

De hierboven uiteengezette bepalingen over het beheerscontract hebben o.i. niet als gevolg dat er in de praktijk van een echte overeenkomst sprake is. Een overeenkomst zou veronderstellen dat de partijen vrij kunnen onderhandelen. Indien de onderhandelingen mislukken, gaan de partijen uiteen en komt er geen akkoord. In de wet van 21 maart 1991 is deze situatie echter niet voorzien. Belgacom heeft de wettelijke verplichting om de taken van openbare dienst inzake telecommunicatie op zich te nemen. De Regeringscommissaris moet, in naam van de Minister, over de naleving van deze verplichting waken. In de praktijk kan Belgacom bij de onderhandelingen over het beheerscontract niet anders dan de voorwaarden van de Minister aanvaarden. De reële inspraak van Belgacom is vooral afhankelijk van het persoonlijk gewicht van de gedelegeerde-bestuurder. Overigens moet deze laatste niet alleen de Minister overtuigen. Het beheerscontract moet, zoals vermeld, goedgekeurd worden door de raad van bestuur. Ook het paritair comité, het B.I.P.T. en het raadgevend comité hebben hun zeg.

Een belangrijke vraag is ook welke rechten de gebruikers uit het beheerscontract kunnen putten. De gedragsregels ten aanzien van de gebruikers worden weliswaar in het beheerscontract opgenomen, maar kunnen de gebruikers de naleving van die regels ook afdwingen? De wet zegt dat het beheerscontract geen akte of reglement is in de zin van artikel 14 van de wetten op de Raad van State en dat alle clausules worden geacht contractueel te zijn (art. 3, § 5). Dat zou betekenen dat de gebruikers t.a.v. het beheerscontract tussen Belgacom en de Staat als "derden" moeten beschouwd worden.

Ook buiten het kader van het beheerscontract - en dus buiten de taken van openbare dienst - reikt de autonomie van Belgacom niet altijd zo ver als soms wel wordt beweerd. Beslissingen over de verwerving of de vervreemding van onroerende goederen moeten, boven een bepaald bedrag, voorafgaandelijk door de Minister worden goedgekeurd. Beleggingen in vreemde munt zijn onderworpen aan de voorafgaande machtiging van de Minister van Financiën (art. 12, § 3). Het belangrijkste is echter dat de leden van de raad van bestuur benoemd worden bij een in Ministerraad overlegd Koninklijk Besluit. Iedereen weet wat dat in België betekent. Ook de voorzitter wordt op die manier (politiek) benoemd en hetzelfde geldt voor de benoeming van de gedelegeerd-bestuurder. De benoemingen van de overige leden van het directiecomité gebeuren door de raad van bestuur op voordracht van de gedelegeerd-bestuurder, mits goedkeuring van de Minister van PTT (art. 20, § 2, in fine).

In de praktijk zal de autonomie van Belgacom zeer sterk bepaald worden door de persoonlijkheid van de gedelegeerd-bestuurder en door de welwillendheid van de

Minister, van zijn regeringscommissaris en van de voorzitter van de raad van bestuur.

Onder bepaalde voorwaarden kan Belgacom rechtstreeks of onrechtstreeks belangen nemen in dochterondernemingen (art. 13, § 1). Een dergelijke dochteronderneming kan eventueel betrokken worden bij de uitvoering van taken van openbare dienst. Zo kan Belgacom dus bijvoorbeeld de uitbating van de mobilifoondienst overdragen aan een private dochteronderneming. Stukken van de openbare telecommunicatie zouden op die manier toch in private handen kunnen komen. Deze "sluipende privatisering" heeft men willen vermijden. Niet alleen is er een machtiging nodig bij een in Ministerraad overlegd Koninklijk besluit. Bovendien mag de dochteronderneming slechts taken van openbare dienst uitvoeren, als de overheid meer dan 50% van de aandelen en 75% van de stemmen en de mandaten bezit. De wet voorziet ook in de mogelijkheid dat een dochteronderneming van Belgacom zelf het statuut van "autonoom overheidsbedrijf" verwerft (art. 13, § 4).

Het personeel van Belgacom blijft onder het ambtenarenstatuut maar er kunnen in een aantal beperkte gevallen ook contractuelen worden aangeworven (art. 29, § 1). Van de wet van 19 juli 1930 werd de bepaling overgenomen dat vijf procent van de jaarlijkse winst zal worden uitgekeerd aan het kader en het personeel. Er wordt voor Belgacom, zoals voor de andere overheidsbedrijven, een paritair comité opgericht, waarvan de samenstelling en de bevoegdheden in de wet gedetailleerd worden geregeld (art. 30). Op het niveau van alle autonome overheidsbedrijven samen, komt er een sectoriel Comité Overheidsbedrijven. Op dat niveau worden de collectieve arbeidsovereenkomsten gesloten die voor alle autonome overheidsbedrijven gelden (art. 31).

Ofschoon Belgacom in de wet voorlopig nog een overheidsbedrijf blijft, kan de raad van bestuur later beslissen tot de omzetting in een naamloze vennootschap van publiek recht. De omzetting heeft evenwel slechts uitwerking na goedkeuring bij een in Ministerraad overlegd Koninklijk besluit. Aanvankelijk zijn alle aandelen dan nog in handen van de Staat. Bij een eventuele kapitaalsverhoging, kunnen ook andere personen aandelen van Belgacom verwerven, met een voorkeursrecht voor het personeel. Er is in elk geval voor gezorgd dat de Staat altijd minstens 50% van de aandelen en 75% van de stemmen en de mandaten moet behouden (art. 39).

2.3.2.3. De activiteiten van Belgacom

Belgacom heeft, volgens de wet van 21 maart 1991, drie doelstellingen:

1. het ontwikkelen van telecommunicatiediensten in binnen- en buitenland,
2. het verrichten van alle handelingen die, rechtstreeks of onrechtstreeks haar activiteiten kunnen bevorderen of een optimaal gebruik van haar infrastructuur mogelijk maken,
3. het deelnemen in reeds bestaande of nog op te richten openbare of private, Belgi-

sche, buitenlandse of internationale instellingen, vennootschappen of verenigingen (art. 56).

Daarnaast krijgt Belgacom een "opdracht van openbare dienst". Deze opdracht bestaat in de terbeschikkingstelling aan het publiek van de openbare telecommunicatie én in taken van sociale of humanitaire aard inzake de openbare telecommunicatie (art. 58). Laatstgenoemde taken moeten in het beheerscontract gepreciseerd worden.

2.3.2.4. Het B.I.P.T.

Naast het autonoom overheidsbedrijf Belgacom wordt door de wet van 21 maart 1991 een nieuwe (klassieke) instelling van openbaar nut opgericht, onder de benaming "Belgisch Instituut voor Postdiensten en Telecommunicatie", afgekort "B.I.P.T." Deze instelling wordt vertegenwoordigd en beheerd door de Minister, die de bevoegdheid krijgt om alle daden van beheer te stellen. Het dagelijks beheer van het B.I.P.T. wordt waargenomen door een leidend ambtenaar, waarvan de bevoegdheid door de Minister wordt vastgesteld (art. 72). Het B.I.P.T. heeft hoofdzakelijk een adviserende bevoegdheid. De echte regulerende bevoegdheid blijft in handen van de Minister. Hij is het die bijvoorbeeld goedkeuringen voor eindapparaten kan verlenen of intrekken op voorstel van het B.I.P.T. (art. 94 en 95).

Men kan zich terecht afvragen of dit wel in overeenstemming is met de Europese richtlijnen. Volgens Richtlijn 88/301 moet, inzake eindapparatuur, met ingang van 1 juli 1989 de formele vastlegging en publicatie van de specificaties en de keuringsregels, alsmede de controle op de toepassing ervan, worden uitgevoerd door een eenheid die "onafhankelijk is van de particuliere en overheidsondernemingen die goederen en/of diensten op telecommunicatiegebied aanbieden". Men kan toch bezwaarlijk stellen dat de Minister onder wie Belgacom ressorteert, "onafhankelijk" van Belgacom is. Het argument dat de Minister toch niet de "beheerder" is van Belgacom, houdt geen steek. Elke band is namelijk, volgens de Europese Richtlijn, al voldoende. Ook het argument dat de andere Lid-Staten eveneens de regulerende bevoegdheid inzake telecommunicatie in de handen van de overheid laten, is niet ernstig. In sommige van die landen is de uitbating van de openbare telecommunicatie namelijk geprivatiseerd. Dat de andere Lid-Staten ook Richtlijn 88/301 met de voeten treden, is bovendien een zwak juridisch argument.

2.3.2.5. Het Raadgevend Comité

Naast Belgacom en het B.I.P.T. wordt door de wet tenslotte nog een "Raadgevend Comité" opgericht. Dit comité is samengesteld uit vertegenwoordigers van Belgacom, van de aanbieders van telecommunicatiediensten, van residentiële en professionele gebruikers, van de producenten van telecommunicatie-uitrustingen en uit onafhankelijke telecommunicatie-experten (art. 81). Het comité kan adviezen verlenen inzake

telecommunicatie, hetzij op eigen initiatief, hetzij op vraag van het B.I.P.T. of van de Minister. Het moet in elk geval geraadpleegd worden over de bepalingen van het beheerscontract die de gebruikers aanbelangen (art. 80).

2.3.3. De hervorming van de spelregels: overzicht

Het basisprincipe van de nieuwe telecommunicatiewetgeving vindt men in art. 69 van de wet. Daarin staat dat, met uitzondering van de "openbare" telecommunicatie, alle activiteiten inzake telecommunicatie **vrij** zijn. Onder "telecommunicatie" wordt verstaan: "elke overbrenging, uitzending of ontvangst van tekens, seinen, geschriften, beelden, klanken of gegevens van alle aard, per draad, radio-electriciteit, optische seingeving of een ander electromagnetisch systeem" (art. 68, 4). Deze omschrijving stemt overeen met de definitie die opgenomen is in de bijlage 2 van het internationaal verdrag betreffende de televerbindingen dat op 6 november 1982 werd gesloten en dat in België werd goedgekeurd bij de wet van 28 augustus 1986¹⁶³.

Het resultaat van de vermelde basisregel is dat de telecommunicatiemarkt in twee domeinen wordt verdeeld: het domein van de openbare telecommunicatie en het domein van de vrije mededinging. Deze twee domeinen worden hierna nader bekeken.

2.3.3.1. De openbare telecommunicatie

Het begrip "openbare telecommunicatie" wordt in artikel 82 omschreven. Het omvat 1) de aanleg, het onderhoud, de modernisering en de werking van de openbare telecommunicatieinfrastructuur, 2) de uitbating van de gereserveerde diensten ten behoeve van derden en 3) de aanleg, het onderhoud en de werking van de voor het publiek toegankelijke en op het openbaar domein geplaatste inrichtingen, die bestemd zijn voor telecommunicatie. Deze drie categorieën van activiteiten worden in exclusieve concessie toegekend aan Belgacom.

2.3.3.1.1. De openbare infrastructuur

De exclusieve concessie van Belgacom omvat in de eerste plaats de openbare telecommunicatie-infrastructuur. De reikwijdte van dit monopolie is natuurlijk volledig afhankelijk van de definitie die men aan "openbare telecommunicatie-infrastructuur" geeft. Deze definitie vindt men in art. 68, 5: "het geheel van uitrustingen met daarbij horende middelen, die het openbaar domein overschrijden en die bestemd zijn voor de telecommunicatie met uitzondering van deze bestemd voor de radio-omroepdienst en de radio- en teledistributienetten. Dit geheel wordt begrensd door daartoe behorende aansluitpunten, met inbegrip van de aansluitingen op buitenlandse telecommunicatie-infrastructuur". Een "aansluitpunt" is een eindpunt van de telecommunicatie-in-

¹⁶³

Memorie van Toelichting, Gedr. St., Kamer, 1287/1 - 89/90, 46.

frastructuur dat dient voor de aansluiting van een eindapparaat (art. 58, 6).

Veel wijzer wordt men met dit soort definities niet. De grens tussen de openbare telecommunicatie-infrastructuur, die tot het overheidsmonopolie behoort, enerzijds, en de eindapparatuur, die het voorwerp is van vrije concurrentie, anderzijds, zal bij elke applicatie in concreto bepaald moeten worden. Vereenvoudigend kan men echter stellen dat tot de openbare infrastructuur alles behoort dat op het openbaar domein de aansluitpunten verbindt voor het aanbieden van gereserveerde diensten of gehuurde lijnen.

Het aansluitpunt zelf behoort tot de infrastructuur. In de meeste gevallen is het aansluitpunt een stopcontact binnenshuis bij de gebruiker. De zaak is echter ingewikkelder in het geval van mobiele telecommunicatie. Uit praktische overwegingen neemt men aan dat, bijvoorbeeld in het geval van de mobilfoon, het aansluitpunt op een hypothetisch punt "in de ether" ligt.

De protocollen zijn niet in de infrastructuur begrepen. Zij maken in principe deel uit van de eindapparatuur en vallen dus in het domein van de vrije concurrentie. De enige uitzondering vormen de zogenaamde "essentiële vereisten".

Eindapparaten zijn inrichtingen die rechtstreeks op de telecommunicatie-infrastructuur kunnen aangesloten worden via het aansluitpunt. Waar precies de functies van de eindapparatuur aan de grens van het toelaatbare komen of overgaan in de aan Belgacom voorbehouden functies van de openbare infrastructuur, zal in elk geval steeds aanleiding blijven geven tot discussies. De leveranciers van eindapparatuur zullen uiteraard zoveel mogelijk additionele functies in hun apparaten willen inbouwen om meer electronica kwijt te kunnen, terwijl Belgacom, van zijn kant, een aantal van deze functies zal willen reserveren om de integriteit van het netwerk te bewaren.

Om iedere leverancier van eindapparatuur, inclusief Belgacom zelf, op gelijke voet te plaatsen voor de toegang tot de openbare telecommunicatie-infrastructuur, is het noodzakelijk dat de specificaties van de aansluitpunten voor iedereen op dezelfde wijze toegankelijk zijn. In het jargon van de Europese Commissie noemt men dit "Open Network Provision". Artikel 86 van de wet bepaalt dat de Minister, op voorstel van het B.I.P.T., voor elke gereserveerde dienst het aansluitpunt enkel op grond van de volgende criteria mag bepalen: 1) de "integriteit", d.w.z. de afwezigheid van storingen in en de mogelijkheid tot het controleren van de goede werking van de gereserveerde diensten en de openbare telecommunicatie-infrastructuur, 2) de "interoperabiliteit", d.w.z. de mogelijkheid tot verbindingen binnen of tussen gereserveerde diensten, en 3) de mogelijkheid tot aansluiting van goedgekeurde eindapparaten op de openbare telecommunicatie-infrastructuur. Via deze limitatieve lijst van criteria wil men de private eindapparatuurleveranciers geruststellen dat de overheid, wanneer ze bepaalt waar het aansluitpunt moet komen en hoe het aansluitpunt er technisch uit zal zien, nooit

Belgacom (zelf leverancier van eindapparaten) of een andere leverancier zal bevoordelen.

Naast de afgrenzing tussen de openbare telecommunicatie-infrastructuur en de eindapparatuur, is er nog een andere afgrenzing van belang. De exclusieve concessie van Belgacom voor het aanleggen van de openbare telecommunicatie-infrastructuur betekent namelijk niet dat men zelf, thuis of in een bedrijf, geen stukje telecommunicatie-infrastructuur kan aanleggen. Op het eerste gezicht zou men denken dat de grens hier samenvalt met deze tussen het openbare en het private domein. In werkelijkheid liggen de zaken niet zo simpel. Hierop komen we hierna terug, bij de bespreking van de gereserveerde diensten en meer bepaald in de paragraaf over de vaste verbindingen.

2.3.3.1.2. De gereserveerde diensten

Het tweede element van de exclusieve concessie die door de wet aan Belgacom wordt verleend, is de uitbating van de "gereserveerde diensten" ten behoeve van derden. De gereserveerde diensten bestaan uit: 1) de telefoondienst, 2) de telex-, de mobilfoon- en semafoondiensten, 3) de dienst voor gegevensschakeling tot zeven maanden na de inwerkingtreding van het lastenboek bedoeld in artikel 126 en uiterlijk tot en met 31 december 1992, 4) de telegraafdienst en 5) de terbeschikkingstelling van vaste verbindingen.

"Telefoondienst" wordt in de wet gedefiniëerd als "de telecommunicatiedienst bestemd voor het rechtstreekse transport in real-time en de schakeling van vocale signalen van en naar aansluitpunten, in de mate dat hij enkel de functies omvat die nodig zijn voor de exploitatie" (art. 68, 10). Uit deze definitie volgt dat diensten als "voice mail" of "telesecretariaten" niet onder het monopolie van Belgacom vallen. Ze beperken zich namelijk niet tot het rechtstreeks transport in real-time, maar hebben ook een opslagfunctie. Uit de voorbereidende werken blijkt dat "rechtstreeks transport in real-time" niet al te letterlijk mag worden opgevat. "Real-time" komt in zuivere vorm haast nooit voor. De normale, onvermijdelijke tijdsdecalage die bij het transport van telefoonsignalen onvermijdelijk is, heeft niet als gevolg dat er niet meer van "telefoondienst" sprake zou zijn.

De telefoondienst omvat natuurlijk meer dan het louter tot stand brengen van de telefoonverbinding. Ook de verbindingsoopbouw, de routing en de tarifiering vallen er onder, alsmede het beheer van de telefoongidsen en het verrekenen van aansluit- en gebruikskosten. Bij routing denkt men bijvoorbeeld aan een dienst die ervoor zorgt dat een grote telefoongebruiker met verschillende vestigingen over heel het land, slechts één landelijk uniform telefoonnummer heeft, waarbij de gebruiker automatisch van de ene naar de andere vestiging kan doorverbonden worden. Dergelijke diensten horen bij de telefoondienst en vallen dus onder het monopolie van Belgacom.

Wat met andere telecommunicatievormen dan het directe transport van spraak, die met

gebruik van de telefoondienst gerealiseerd worden? Men denke maar aan telefax of datatransport via modems? Inzoverre men bij de telefax gebruik maakt van het geschakeld telefoonnetwerk, is deze dienst niet te scheiden van de telefoondienst. Indien men daarentegen voor het faxen andere netwerken gebruikt, zoals het geval is voor de telefax van de CCITT-groep IV, zit men op het terrein van de vrije concurrentie.

Bij telefoonverbindingen denkt men voorlopig vooral nog aan de transmissie van "vocale" en dus analoge signalen. Men mag echter niet vergeten dat het telefoonverkeer progressief wordt geïntegreerd in het dataverkeer en dat spraak meer en meer in digitale vorm over de lijnen gaat. Zodra de huidige telefoon-infrastructuur volledig gedigitaliseerd zal zijn, is dat voor de hele telefoondienst het geval. Het wordt dan moeilijk om nog een onderscheid te maken tussen spraak, beelden, tekst en andere gegevens. Alles resumeert zich in datatransport. Op middellange termijn is daarom de aparte status van de telefoondienst niet houdbaar.

Naast de telefoondienst houdt de Belgische wetgever ook de telex-, de mobilfoon- en de semafoondienst binnen het overheidsmonopolie. Dat kan omdat de Europese Richtlijn over de telecommunicatiediensten niet van toepassing is op de radio-omroep, de televisie, de telexdienst, de mobiele radiotelefonie, de semafoon en de satellietdiensten. Het behoud van het monopolie over het mobilfoonnet wordt gerechtvaardigd met de overweging dat België te klein is voor meer dan één operator.

"Diensten voor gegevensschakeling" zijn "telecommunicatiediensten waarvan de functies zich beperken tot het transport en de schakeling van gegevens via pakket- of circuitschakeling, met inbegrip van de functies die nodig zijn voor zijn exploitatie (art. 68, 9)". Deze diensten (in België verzorgd door de dienst "D.C.S.") bleven, overeenkomstig de Europese Richtlijn 90/388, tot 31 december 1992 voorbehouden aan Belgacom. Sedert die datum is de dienst echter niet volledig vrij. De uitbating van een dienst voor gegevensschakeling kan onderworpen worden aan een "lastenboek voor openbare dienstverlening". De voorwaarden vervat in dat lastenboek moeten objectief en doorzichtig zijn, en ze mogen niet discriminerend werken. Ze mogen enkel tot doel hebben de naleving te waarborgen van de "essentiële vereisten" en van minimumvoorwaarden van gelijke en regelmatige beschikbaarheid, geografische spreiding en betrouwbaarheid.

De laatste gereserveerde dienst, tenslotte, is "het ter beschikking stellen van vaste verbindingen". Een vaste verbinding is "een verbinding die het openbaar domein overschrijdt en die rechtstreekse telecommunicatie toelaat tussen, enerzijds, een aansluitpunt of een aansluiting op een buitenlandse telecommunicatie-infrastructuur en, anderzijds, één of meer aansluitpunten of aansluitingen op een buitenlandse telecommunicatie-infrastructuur en waarbij de gebruiker het totstandkomen of verbreken van de verbinding niet via zijn aansluitpunt kan beïnvloeden"(art. 68, 8). Dat laatste maakt het verschil uit tussen een vaste verbinding en de openbare infrastructuur. Bij een vaste

verbinding is het voor de gebruiker niet mogelijk een bestemming te kiezen. Het staat vast tussen welke punten de dienst zal worden verleend.

Alleen Belgacom kan vaste verbindingen ter beschikking stellen. Dit moet gebeuren binnen een redelijke termijn na het verzoek. De terbeschikkingstelling mag ook niet gekoppeld worden aan andere beperkingen dan deze die in de wet zijn bepaald (art. 85, lid 1 en lid 2). Belgacom dient alle aanvragers op gelijke wijze te behandelen en mag ook zichzelf niet bevoordelen (art. 107, § 1 en § 2). Op deze laatste verplichtingen, die aan Belgacom worden opgelegd, komen we later nog terug n.a.v. het probleem van de eerlijke mededinging op de telecommunicatiemarkt.

Wie van Belgacom een vaste verbinding verkrijgt, mag deze in geen geval gebruiken voor het louter leveren van gereserveerde diensten aan derden (art. 85, lid 3). Men mag dus geen vaste verbinding gebruiken om een parallelle telefoondienst op te zetten. Op deze manier wil men "afroming" vermijden. Belgacom is verplicht om heel het land onder gelijke voorwaarden telefoondiensten te verstrekken. Een private leverancier zou daaruit enkel de meest winstgevende geografische zones kunnen uitkiezen. Uit de wet of uit de voorbereidende werken is het niet duidelijk wat precies met het "louter" leveren van gereserveerde diensten wordt bedoeld. Het leveren van een gereserveerde dienst (telefoon bijv.) als geïntegreerd onderdeel van een totaalpakket van telecommunicatiediensten zou met deze beperking wel toegelaten zijn. Ook het doorverhuren van bijvoorbeeld een gedeelte van de lijncapaciteit van de vaste verbinding is onder de wet van 21 maart 1991 mogelijk.

Mag men zelf geen vaste verbindingen aanleggen als men met die verbindingen het openbaar domein niet overschrijdt? De wet van 21 maart 1991 bepaalt in dit verband: "er moet rechtstreeks of onrechtstreeks gebruik gemaakt worden van een gereserveerde dienst voor de onderlinge verbinding van telecommunicatie-inrichtingen, hetzij gelegen in twee of meer gebouwen die geheel of gedeeltelijk gebruikt worden door verschillende personen, hetzij indien het openbaar domein wordt overschreden" (art. 92, § 1). Leden van hetzelfde gezin (in het Frans: une même famille) worden als één persoon beschouwd. Ook als men niet op openbaar domein komt, moet men dus in vele gevallen op Belgacom beroep doen voor een verbinding. Het volstaat dat men twee "gebouwen" met elkaar moet verbinden, die niet door dezelfde personen gebruikt worden. Voor de verbinding van verschillende gebouwen op hetzelfde bedrijfsterrein zal er dus meestal geen probleem zijn. Ook de verbindingen tussen verschillende verdiepingen in een flatgebouw kunnen zonder tussenkomst van Belgacom worden aangelegd. Voor sommige "gebouwen-complexen" zal het overigens niet steeds eenvoudig zijn om uit te maken of men met afzonderlijke gebouwen te maken heeft. Er zijn op dit punt boeiende juridische discussies in het vooruitzicht!

De bedoeling van de wettelijke beperking op het aanleggen van telecommunicatie-verbindingen, zelfs buiten het openbaar domein, bestaat er opnieuw in het ontstaan van

parallelle netwerken te verhinderen die de activiteit van Belgacom zouden kunnen "afromen". Men denke bijvoorbeeld aan besloten netwerken met verschillende bedrijven in grote industrieparken.

Afwijkingen zijn mogelijk voor de Staat, de Gemeenschappen, de Gewesten, de provincies, de gemeenten, de Nationale Maatschappij der Belgische Spoorwegen, de maatschappijen voor het gemeenschappelijk stads- en streekvervoer, de gas- en electriciteitsmaatschappijen, de uitbaters van de radio- en teledistributienetten. Deze instellingen en organisaties kunnen, voor eigen gebruik, hun eigen netwerken kunnen blijven benutten, ook wanneer die het openbaar domein overschrijden.

Ook aan anderen kan door de Minister een dergelijke afwijking verleend worden (art. 92, § 2). Dat laatste is in principe echter niet mogelijk indien Belgacom de verbintenis aangaat om, aan het normale tarief en binnen een redelijke termijn die zij vaststelt, een verbinding ter beschikking te stellen die technisch gelijkwaardig is als deze waarvoor de afwijking wordt gevraagd. Op voorstel van het B.I.P.T. kan de Minister evenwel een voorwaardelijke afwijking toekennen voor het geval waarin de door Belgacom aangegane verbintenis niet zou worden nagekomen binnen de vastgestelde termijn (art. 92, § 3). Bovendien kan een dergelijke afwijking gekoppeld worden aan een vergoeding voor Belgacom, behalve wanneer laatstgenoemde niet in staat is om tijdig voor een gelijkwaardig alternatief te zorgen.

2.3.3.1.3. De openbare telecommunicatie-inrichtingen

Naast de openbare telecommunicatie-infrastructuur en naast de gereserveerde diensten (cfr. supra), omvat de openbare telecommunicatie - voorbehouden terrein voor Belgacom - ook nog "de aanleg, het onderhoud en de werking van de voor het publiek toegankelijke en op het openbaar domein geplaatste inrichtingen die bestemd zijn voor telecommunicatie". Hierbij wordt vooral aan de uitbating van publieke telefooncellen gedacht. De automatische bankklokken worden hier expliciet niet mee bedoeld omdat deze inrichtingen niet bestemd zouden zijn voor telecommunicatie.

2.3.3.2. De vrije mededinging op de telecommunicatiemarkt

2.3.3.2.1. Overzicht

Eerder werd er al op gewezen dat de wet van 21 maart 1991 de Belgische telecommunicatiemarkt in twee stukken verdeelt: het domein van de openbare telecommunicatie en het domein van de vrije concurrentie. Buiten het domein van de openbare telecommunicatie, dat exclusief voor Belgacom is gereserveerd, kunnen voortaan door iedereen niet-gereserveerde diensten worden aangeboden. Daarbij dient benadrukt dat vanaf 1 januari 1993 ook de diensten voor gegevensschakeling daarbij horen. Ook de verdeling, de installatie en het onderhoud van alle eindapparaten behoort voortaan tot het

domein van de vrije concurrentie. Omdat Belgacom, naast zijn taken van openbare dienst, ook als "gewone" mededinger meespeelt op de telecommunicatiemarkt, zijn in de wet een aantal waarborgen voor vrije concurrentie ingebouwd. Deze waarborgen moeten vooral verhinderen dat Belgacom op de vrije markt vanuit een bevoorrechte positie kan opereren.

2.3.3.2.2. De niet-gereserveerde diensten

Alle niet-gereserveerde diensten zijn in principe vrij (art. 89, § 1). Ze kunnen door iedereen worden uitgebaat, ook door Belgacom (art. 87). Toch zijn er een aantal beperkingen: het verplicht gebruik van de openbare telecommunicatie op openbaar domein en de verplichting tot voorafgaandelijke aangifte vooraleer met de uitbating te starten.

Voor het uitbaten van een niet-gereserveerde dienst die het openbaar domein overschrijdt, moet rechtstreeks of onrechtstreeks gebruik gemaakt worden van de openbare telecommunicatie (art. 88). De Minister kan evenwel, op voorstel van het B.I.P.T., bepalen in welke gevallen en onder welke voorwaarden van deze regel kan worden afgeweken (art. 92, § 2).

Wie een niet-gereserveerde dienst wenst uit te baten, moet hiervan ten laatste twee maanden voor het begin van de uitbating van de dienst, aangifte doen bij het B.I.P.T. met een aangetekende brief (art. 89, § 3, lid 1). Het B.I.P.T. kan zich binnen deze termijn tegen de uitbating verzetten indien de wettelijke bepalingen niet zijn nageleefd. Indien de aanvrager na twee maanden geen beslissing van het B.I.P.T. heeft ontvangen die hem verbiedt de betrokken dienst uit te baten, mag met de uitbating worden gestart (art. 89, § 5). Indien de uitbating niet wordt toegestaan, is een beroep mogelijk bij de Minister.

De overdracht van een niet-gereserveerde dienst is vrij, voor zover ze wordt aangegeven bij het B.I.P.T. ten laatste zeven "vrije" dagen na de overdracht.

Indien de leverancier van een niet-gereserveerde dienst zijn wettelijke verplichtingen niet nakomt, kan het B.I.P.T. hem een ingebrekestelling sturen om de leverancier alsnog tot de orde te roepen. Als dat niet lukt, kan de Minister de verzorging van de dienst schorsen of verbieden voor een periode die hij aanduidt.

2.3.3.2.3. Eindapparatuur

Iedereen mag eindapparaten ter beschikking stellen, op de openbare telecommunicatie-infrastructuur aansluiten, in dienst stellen of onderhouden (art. 93). De rechtstreeks op de openbare telecommunicatie-infrastructuur aangesloten eindapparaten moeten goedgekeurd zijn door de Minister, op voorstel van het B.I.P.T. (art. 94, § 1).

Onrechtstreeks aangesloten eindapparaten, bijvoorbeeld telefoontoestellen die aan een PABX zijn gekoppeld, hoeven niet te worden goedgekeurd. De goedkeuring kan worden

ingetrokken als het apparaat niet meer overeenstemt met het oorspronkelijk goedgekeurde type, als het niet meer beantwoordt aan de technische specificaties, als de voorwaarden waaronder de goedkeuring is verleend, niet worden nageleefd en, tenslotte, als het eindapparaat storing of schade veroorzaakt aan de openbare infrastructuur of gevaarlijk is voor de gebruikers of voor het personeel van Belgacom (art. 95).

2.3.3.2.4. Waarborgen voor de eerlijke mededinging

In de "vrije zone" van de telecommunicatiemarkt is Belgacom een leverancier die in concurrentie staat met de andere, meestal private, binnenlandse en buitenlandse leveranciers van apparatuur en diensten. Laatstgenoemden zijn echter van Belgacom afhankelijk omdat ze voor het leveren van hun diensten de infrastructuur en de verbindingen van Belgacom moeten gebruiken.

Om te beletten dat Belgacom in een voordeliger concurrentiepositie zou komen omdat het aan zichzelf goedkope verbindingen kan leveren en aan de concurrenten daarentegen hoge tarieven zou kunnen opleggen, bepaalt artikel 106 van de wet dat het tarief van de vaste verbindingen gebaseerd moet zijn op de kostprijs, "verhoogd met een redelijke winstmarge". Indien de vaste verbinding wordt aangesloten op een gereserveerde dienst, kan dit tarief worden verhoogd met een redelijke toegangsvergoeding. Het is evident dat deze bepalingen slechts efficiënt zijn indien de boekhouding van Belgacom voor iedereen volstrekt transparant is. Ook dan nog zal de bepaling van wat als "redelijk" moet beschouwd worden, zeker stof voor discussie bieden.

Vrije concurrentie veronderstelt ook dat iedereen gelijke toegang heeft tot de gereserveerde diensten en dat Belgacom aan zijn concurrenten geen willekeurige voorwaarden oplegt om de toegangsdrempel wat hoger en duurder te maken. Dit is het voorwerp van de Europese Richtlijn 90/387 over "Open Network Provision". Volgens artikel 107 kan de toegang tot de gereserveerde diensten slechts geweigerd worden op grond van "essentiële eisen": 1) de operationele veiligheid van netwerken, 2) het behoud van de netwerkintegriteit, 3) de interoperabiliteit van diensten en netwerken in gegronde gevallen en 4) de bescherming van de overgebrachte gegevens in gegronde gevallen. Deze lijst stemt overeen met deze van artikel 3, 2 van de ONP-Richtlijn.

Een derde mogelijke concurrentievervalsing tussen Belgacom en andere dienstenleveranciers zou kunnen voortvloeien uit het feit dat Belgacom veel eerder dan zijn concurrenten op de hoogte is van nieuwe technische kenmerken van bijvoorbeeld vaste verbindingen. Door vroeger dan de concurrenten over die informatie te beschikken, heeft Belgacom een voorsprong bij het leveren van diensten. Dit probleem wordt in de nieuwe wet niet echt opgelost. Artikel 108 bepaalt enkel dat de precieze technische kenmerken, die het gebruik mogelijk maken van de gereserveerde diensten, door het B.I.P.T. gepubliceerd worden, en dat, bij een wijziging, Belgacom het B.I.P.T. vooraf op de hoogte moet brengen.

Tenslotte zou Belgacom de concurrentie met de andere leveranciers van diensten en eindapparatuur ook nog kunnen vervalsen door financiële middelen over te sluizen vanuit de openbare telecommunicatie. Opbrengsten van de telefoondienst of van de mobilfoondienst zouden op die manier kunnen gebruikt worden om niet-gereserveerde diensten van Belgacom te subsidiëren. Deze vorm van kruissubsidiëring wordt door artikel 109 verboden. Om dit min of meer te kunnen controleren, moet Belgacom zijn boekhouding zodanig organiseren dat de exploitatieresultaten uit de openbare telecommunicatie gescheiden blijven van deze uit de andere activiteiten.

Men kan zich terecht afvragen of de waarborgen die in de wet vervat zijn om Belgacom in dezelfde concurrentiepositie te plaatsen als de andere leveranciers van niet-gereserveerde diensten, enig effect kunnen hebben. De dubbelrol van Belgacom blijft hoe dan ook problematisch omdat de concurrenten van Belgacom tegelijk ook van Belgacom afhankelijk zijn. Belgacom blijft tenslotte één bedrijf en er zal dus steeds kennis en informatie van de ene activiteit naar de andere doorstromen. Dit lijkt een onvermijdelijk gevolg van de institutionele constructie waarvoor de Belgische wetgever heeft gekozen.

2.3.4. Besluit

Onder de druk van de Europese Unie wordt in België zeer aarzelend afgestapt van het overheidsmonopolie inzake telecommunicatie. In zoverre het door de Europese richtlijnen nog toegelaten is, wordt dat monopolie zoveel mogelijk in stand gehouden. Het is een hervorming die "willens nillens" moest doorgevoerd worden en wellicht hadden velen het liever bij het oude gelaten.

De openbare telecommunicatie, die exclusief in handen blijft van de overheid, bestrijkt een gebied dat zo ruim gedefiniëerd is als door de Europese richtlijnen enigszins wordt toegelaten. Telecommunicatie wordt in België, misschien niet ten onrechte, zeer sterk als een openbare dienst beschouwd, die niet louter volgens economische principes mag geleid worden.

België is een klein landje. Het volledig vrijgeven van de telecommunicatiemarkt zou ongetwijfeld als gevolg hebben dat grote buitenlandse bedrijven de Belgische markt zouden overspoelen. Ook om die reden is men liever voorzichtig.

Een zeer essentieel punt komt in de wet van 21 maart 1991 niet aan de orde. België heeft een zeer uitgebreid kabelnet dat momenteel uitsluitend voor radio- en teledistributie wordt gebruikt. Velen koesteren grote ambities met betrekking tot het gebruik van dat net voor nieuwe telecommunicatiediensten. Bovendien is het kabelnet aan modernisering toe, op een moment dat ook het telefoonnetwerk naar glasvezelverbindingen wil overstappen. Kan België zich een "dubbel" geavanceerd fysisch netwerk veroorloven? Een bijkomende complicatie hierbij is dat, sinds de Staatshervorming, de nationale wetgever

geen bevoegdheid meer heeft inzake radio en televisie, maar dat deze kwestie thans door elke Gemeenschap afzonderlijk wordt geregeld...