KPMG Klynveld EDP Audit

Samsom BedrijfsInformatie

# COMPACT

## KWARTAALBLAD EDP AUDITING



WINTER

1990 / 4

**Compact ®**
Jaargang 17, nummer 4
Een uitgave van KPMG Klynveld EDP Audit en Samsom BedrijfsInformatie, werkmaatschappij van Wolters Kluwer NV.
Het blad verschijnt 4 x per jaar.

**Redactie**
D. Steeman RA (hoofdredacteur)
Drs. R.G.A. Fijneman RA
Mw. D. Jansen Heijtmajer RI
Prof. A.W. Neisingh RA
Drs. P. Veltman RA

**Redactiesecretariaat**
Mw. A.M.F. Hofland,
KPMG Klynveld EDP Audit,
K.P. van der Mandelelaan 41
3062 MB Rotterdam
Tel.: 010 - 453 47 40
Fax : 010 - 453 47 77

**Vormgeving**
Bureau Karakter, Delft

**Aan dit nummer werkten mee**
Prof. mr. J.M.A. Berkvens
R.A. s'Jacob
Mw.mr. A.M. Ch. Kemna MBA
Prof. A.W. Neisingh RA
Mr. V.A. de Pous

**Abonnementen**
*f* 135,- per jaar incl. BTW.Losse nummers *f* 50,- incl. BTW. Abonnementen kunnen schriftelijk tot uiterlijk één maand voor de aanvang van een nieuw abonnementsjaar worden opgezegd. Bij niet tijdige opzegging wordt het abonnement automatisch met een jaar verlengd.
**Abonnementsadministratie**
Samsom BedrijfsInformatie
Postbus 4
2400 MA Alphen aan den Rijn
Tel.: 01720 - 6 68 00
Fax : 01720 - 7 59 33
Adreswijzigingen - ook tijdelijke - moeten minstens 8 weken voor de verschijningsdatum bekend zijn.

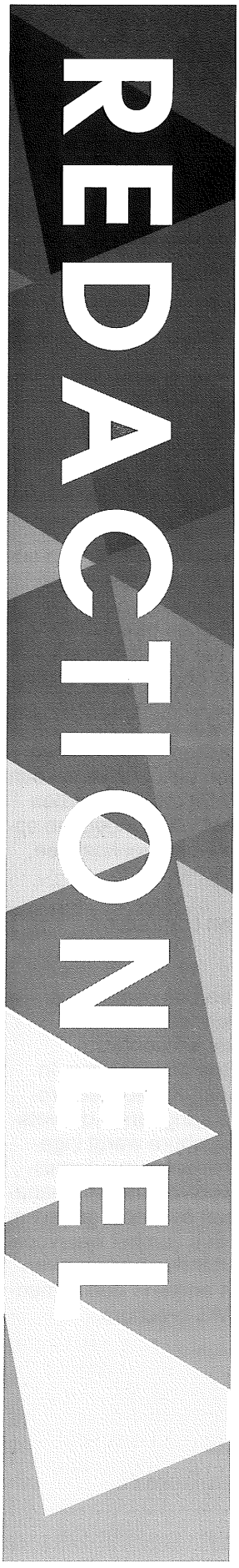


**Uitgever**
J.R.M. Masselink

Lid van de Nederlandse organisatie van tijdschriftuitgevers NOTU

**ISSN 0920 - 1645**

# Inhoudsopgave




# Redactioneel

In de automatiseringsbranche valt een toenemende interesse te bespeuren voor de juridische aspecten van automatisering. Zo worden (toekomstige) software-gebruikers zich steeds meer bewust van hun afhankelijkheden ten aanzien van software-leveranciers en zoeken software-producenten internationaal naar juridische mogelijkheden om hun produkten te beschermen.
Ook krijgen organisaties te maken met wettelijke normen als het gaat om de beveiliging van hun gegevens. De juridische aspecten van automatisering hebben diverse raakvlakken met het vakgebied EDP-auditing. De redactie heeft dan ook besloten een tweetal Compacts te wijden aan het nog jonge vakgebied computerrecht. De beide themanummers geven een overzicht van actuele onderwerpen.

In de voor u liggende Compact wordt in een tweetal artikelen ingegaan op de contractuele kant van automatiseringsprojecten. Het blijkt dat automatiseringscontracten niet alleen het sluitstuk van onderhandelingen zouden moeten zijn, maar dat zij als een instrument kunnen worden gebruikt bij de beheersing van een project.

Daarnaast is een artikel opgenomen over de juridische bescherming van software in een internationaal perspectief. Met name de aanstaande richtlijn van de Europese Gemeenschap omtrent auteursrechtelijke bescherming van software maakt dit artikel actueel en interessant.

Ook aan de op handen zijnde wetgeving op het gebied van de computercriminaliteit wordt in deze Compact aandacht besteed. Beveiliging tegen computercriminaliteit, een aandachtsgebied bij uitstek voor de EDP-auditor, krijgt er door deze wetgeving een dimensie bij.

In het inleidende artikel wordt de connectie tussen EDP-auditing en recht aangegeven. Het artikel maakt duidelijk waarom een EDP-auditor op de hoogte moet zijn van computerrecht, en waar de aandachtspunten van juristen behoren te liggen als zij zich bezighouden met het computerrecht.
De redactie hoopt met de twee themanummers een boeiende en constructieve bijdrage te leveren aan de verrijking van het vakgebied EDP-auditing en de samenwerking tussen EDP-auditors en computerjuristen. Uiteraard werd onderkend dat deskundige bijstand noodzakelijk is om de lezer wederom twee Compacts van hoge kwaliteit te leveren. De redactie dankt mevrouw mr. A.M.Ch. Kemna MBA voor de coördinatie van de beide themanummers. Prof. mr. J.M.A. Berkvens was bereid de redactie vaktechnisch bij te staan, waarvoor zij hem veel dank verschuldigd is.

Prof. A.W. Neisingh RA

---

Het blad wil een bijdrage leveren aan de ontwikkeling van het vakgebied EDP-auditing door het publiceren van actuele artikelen op deelterreinen van EDP-auditing en advies, zoals:

- beoordeling automatiseringsorganisaties en -systemen
- risicobeheersing
- telecommunicatie-adviezen
- beveiligingsonderzoeken
- quality assurance
- opleidingen en trainingen
- privacy-wetgeving
- computercriminaliteit en nieuwe regelgeving

Behalve voor EDP-auditors kan dit blad ook interessant zijn voor EDP-deskundigen en gebruikers van informatiesystemen.

De in dit tijdschrift weergegeven meningen mogen niet worden gezien als officiële zienswijze van KPMG Klynveld EDP Audit.

Het blad Compact is met de meeste zorg samengesteld. Niettemin is het niet geheel uitgesloten dat de geboden informatie enkel en alleen door tijdsverloop en/of andere oorzaken minder juist is.

Noch KPMG Klynveld, KPMG Klynveld EDP Audit, noch de redacteuren persoonlijk, noch uitgeverij Samsom Bedrijfs-Informatie bv, deel uitmakend van Wolters Kluwer NV, aanvaarden enige aansprakelijkheid, hoe ook genaamd, uit welken hoofde dan ook voor enig gevolg rechtstreeks of indirect voortvloeiend uit het gebruik van de informatie.

De redactie stelt gaarne ruimte in Compact beschikbaar voor reacties en/of ervaringen van lezers.

Auteurs die overwegen een bijdrage te leveren, wordt verzocht kennis te nemen van de aanwijzing voor auteurs, die bij het secretariaat verkrijgbaar is.

**Dit inleidende artikel gaat in op de connectie tussen het vak EDP-auditing en het informaticarecht. Aangegeven wordt waarom een EDP-auditor op de hoogte zou moeten zijn van de juridische aspecten van automatisering en een jurist raad moet weten met de technische en organisatorische kant van automatisering.**

**Prof. A.W. Neisingh RA en Mw. mr. A.M.Ch. Kemna MBA**

# Informaticarecht en EDP-auditing in perspectief

## Recht en automatisering

Compact besteedt in twee themanummers aandacht aan de relatie recht en automatisering. De onderwerpen die de revue passeren maken duidelijk waarom een EDP-auditor op de hoogte moet zijn van de juridische aspecten van automatisering en een jurist raad moet weten met de technische en organisatorische kant van automatisering.

Niet omdat alles zo duidelijk is, integendeel zelfs. De voortschrijdende maatschappelijke ontwikkeling maakt de uitbouw van het vakgebied Informaticarecht noodzakelijk teneinde begrippen als privacy, auteursrecht, EDI-contracten en computercriminaliteit een vaste plaats te geven in de automatisering en controleerbaar te maken. Vandaag nog nooit van gehoord, morgen zijn ze al ingeburgerd: escrow en reverse engineering.

## Kruisbestuiving

Iedereen wordt geacht de wet te kennen. Wat daarvan ook waar moge zijn, één ding is zeker: een bedrijf moet ervan op aan kunnen dat een EDP-auditor het recht kent op zijn werkterrein. Een EDP-auditor moet zo gezien alert zijn op en kennis hebben van mogelijke haken en ogen die sluipen in automatiseringscontracten. Tegelijk mag men ook verwachten dat de deskundige man of vrouw op de hoogte is van de ontwikkelingen in op handen zijnde regelgeving. Kortom, een deskundig advies voorkomt vaak veel moeilijkheden achteraf.
In de twee edities worden allerlei thema's besproken die belangrijk zijn bij automatiseren. Er worden mogelijke raakvlakken belicht tussen privaat- en strafrecht enerzijds en informatica anderzijds. Nu komen we meteen aan de tweede reden voor het centrale thema in de twee edities van Compact. Informaticarecht is een jonge discipline. Er moet nog veel in regelgeving worden gegoten, weinig onderwerpen zijn nog grijpbaar. Dus moet worden gesproken en geschreven over de juridische aspecten van automatisering.
Automatiseringsdeskundigen met kennis van de problematiek kunnen op deze wijze mogelijk een bijdrage leveren aan uitbreiding en aanscherping van bestaande regelgeving. Alle reden voor een multidisciplinaire benadering van de vakgebieden Informatica en Informatica-recht, ofwel: kruisbestuiving.

## Nieuwe ontwikkelingen

De samenleving wordt overspoeld door nieuwe ontwikkelingen en mogelijkheden van de informatietechnologie. Netwerken raken steeds meer ingeburgerd. Het koppelen van computer en bestanden biedt enorme mogelijkheden om gegevens te vergelijken en uit te wisselen, met name voor de overheid. Tegelijkertijd dient de koppeling van netwerken voor de samenleving als een signaal te fungeren om attent te zijn waar het gaat om de gevaren voor de privacy van burgers en de noodzaak om dergelijk gebruik van technologie beter te kunnen controleren. Ook op het punt van het in stand houden van de fysieke infrastructuur bestaan er de nodige discussiepunten.
De aansprakelijkheid voor disfunctioneren van concessiehouder PTT Telecom

is slechts beperkt. Voor consumenten houdt dit in dat schade, door het niet kunnen gebruiken van een openbaar netwerk, niet zonder meer te verhalen is op PTT Telecom. Voor VAS-aanbieders (Value Added Services) dient zich hier een potentieel bedrijfsrisico aan.
Ook fysieke barrières - grenzen - vervallen door de internationalisering. Technisch is het mogelijk overal ter wereld aan informatie te komen, waar men zich ook bevindt. Met deze ontwikkelingen begeven we ons op het terrein van het internationaal recht. Een grotendeels nog onontgonnen gebied, bezien vanuit recht en automatisering. Onderzocht moet worden hoe harmonisatie van nationale regelgevingen en internationale standaardisatie te bereiken in relatie tot onder meer grensoverschrijdende informatie.
Mevrouw A.C.M. Nugter promoveerde onlangs op het onderwerp: Transborder flow of personal data within the EC. Zij onderzocht de verschillen tussen enkele nationale privacy-wetten, internationale regelingen en afspraken, en de gevolgen ervan voor bijvoorbeeld de internationale handel. Haar boek wordt besproken in de tweede juridische Compact.

## Misbruik

Er ontstaan veel mogelijkheden om gegevens uit te wisselen én door koppeling nieuwe informatie te verkrijgen. Nu stuiten we al meteen op het terrein van misbruik of zelfs criminaliteit. Wanneer is de privacy in het geding of wordt getornd aan het auteursrecht?
Welke rol is weggelegd voor de wetgeving om computercriminaliteit in te dammen en persoonsgegevens te beschermen? Wat is het belang van het auteursrecht bij gebruik van softwareprogramma's of bij het kopiëren of tijdelijk opslaan van gegevens in een "mailbox"?
Door de stormachtige ontwikkelingen neemt bij bedrijven de interesse voor aspecten als beheersbaarheid, privacy en economische afhankelijkheid toe, juist vanwege de bedrijfsbelangen die ermee zijn gemoeid.

*Door de stormachtige ontwikkelingen neemt bij bedrijven de interesse voor aspecten als beheersbaarheid, privacy en economische afhankelijkheid toe.*

## Vijfde produktiefactor

Het "beheersen van risico" wordt alsmaar belangrijker. Gevolg is dat EDP-auditing zich mag verheugen in een groeiende belangstelling. Een bedrijf moet steeds meer rekening houden met de mogelijke consequenties op termijn van automatisering en de hoge kosten die daarmee gepaard kunnen gaan op effectieve manier indammen. Men zou kunnen zeggen dat "beheersing van risico" hard op weg is zich te ontwikkelen tot een vijfde produktiefactor (naast kapitaal, machines, menskracht en informatie).
En juist kennis van recht is nodig om problemen achteraf te voorkomen. Mislukte automatiseringsovereenkomsten en het niet-nakomen van verplichtingen hebben maar al te vaak als achtergrond gebrek aan deskundigheid, onduidelijke afspraken en een onzorgvuldige uitwerking. Dat komt ook tot uitdrukking bij een ander onderwerp waarmee men vaker in aanraking komt: de bescherming van privacy. In de Wet Persoonsregistraties (WPR) worden eisen gesteld aan de beveiliging van persoonsgegevens en procedures en maatregelen voor het waarborgen van de privacy. Veel organisaties ontbreekt het nog aan de kennis om de wettelijke maatregelen om te zetten in beleid. Wanneer een bedrijf om een advies en een beoordeling van het systeem vraagt, mag het verwachten dat de EDP-auditor op de hoogte is van de wet en de consequenties ervan.

## Privacy

Het voorbeeld van de privacy maakt al veel duidelijk. Een EDP-auditor kan bij een systeembeoordeling privacy als kwaliteitsaspect pas goed behandelen indien hij of zij op de hoogte is van de eisen uit de Wet Persoonsregistraties. Een jurist kan pas invulling geven aan een beveiligingseis zoals verwoord in de Wet Persoonsregistraties wanneer hij of zij op de hoogte is van de organisatorische en technische mogelijkheden bij automatisering. Hetzelfde gaat op voor EDI en telecommunicatie, computercriminaliteit, computercontracten, escrow en intellectuele eigendom.

Een probleem is dat het juridische begrippenapparaat op vele terreinen nog tekort schiet of in de praktijk nog onvoldoende is ingevuld. Een voorbeeld van

dit laatste is de privacy-wetgeving. De aanstaande wetgeving op het gebied van computercriminaliteit laat zien dat de aanvulling van het juridisch arsenaal alléén niet voldoende is. In het wetsontwerp Computercriminaliteit is het "binnendringen in een beveiligd systeem" als een delict omschreven. Opsporing en bewijslast vormen hierbij problemen op zich. Maar het probleem van iedere geautomatiseerde organisatie is: hoe kun je het voorkomen? Op beide terreinen, zowel de opsporingskant als de preventiekant, ligt een mogelijkheid voor samenwerking tussen de jurist en de EDP-auditor.

*Vaak wordt echter een jurist of een EDP-auditor er veel te laat bijgehaald. Zo van: "O ja, er moet nog een contract komen".*

## Multidisciplinaire aanpak

Compact wil door middel van de behandelde onderwerpen de noodzaak onderstrepen van een multidisciplinaire aanpak. Er moet tegelijk rekening worden gehouden met zowel het juridische en technische als het administratieve en organisatorische van automatisering. Kijk naar een automatiseringscontract!
Veel automatiseringsprojecten lijden schipbreuk omdat de "voorkant" van het contract niet goed wordt ingevuld. In een overeenkomst moeten de exacte afspraken, de op te leveren functionaliteit, de implementatieplanning en de afbakening van de verantwoordelijkheden duidelijk staan omschreven. Vaak wordt echter een jurist of een EDP-auditor er veel te laat bijgehaald. Zo van: "O ja, er moet nog een contract komen".
Bij het sluiten ervan zouden niet alle afspraken al vast moeten liggen wanneer de jurist erbij wordt geroepen. Een contract zou ook niet als sluitpost moeten fungeren, als je kijkt naar de belangen die op het spel staan. De overeenkomst moet zorgvuldig worden opgesteld en precies aansluiten bij het te ondernemen project.
Wanneer een bedrijf plannen heeft om te automatiseren moeten als eerste de eisen worden geformuleerd. Welke activiteiten wil men automatiseren; welke hardware en programmatuur is daarvoor noodzakelijk? Wat zijn de kosten en welk tijdpad wordt gevolgd?
De EDP-auditor licht de interne organisatie, het gevolgde keuzeproces en de implementatie van het automatiseringsplan door. In het algemeen moet de overeenkomst klaarheid brengen in de technische en economische afspraken en de juridische regeling. Het contract moet daarbij aansluiten. Wil de EDP-auditor dit toetsen, dan moet hij op de hoogte zijn van de te controleren problemen en het begrippenapparaat. Met andere woorden, afleverdata, acceptatieprocedure, boeteclausule en geschillenregeling - om maar enkele te noemen - moeten duidelijk zijn omschreven.

## Escrow

En last but not least: een regeling voor escrow, in die gevallen waarin dat is gewenst. Indien programmatuur bedrijfseigen is of dusdanig hoge vervangingskosten oplevert, dienen de gevolgen van eventueel stopzetten van het onderhoud c.q. discontinuïteit van de relatie met de leverancier te worden afgedekt. Hiervoor kan escrow, het veilig stellen van de broncode van die programmatuur bij een derde, een oplossing zijn.
Hoe is escrow geregeld? De term is overgenomen uit het Anglo-Amerikaanse recht. Het probleem is vaak hoe de escrow juridisch, technisch en organisatorisch in te vullen.
Juridisch gezien zijn vele constructies mogelijk die echter niet allemaal waterdicht zijn. Het is bovendien moeilijk de rechten en plichten van bewaarder, leverancier en gebruiker precies vast te leggen. Technisch is het moeilijk de broncode bij de derde steeds actueel te houden.
Vanuit organisatorisch oogpunt dient zich ook een aantal vragen aan. Hoe op te treden wanneer de escrow tot effect komt? Wie heeft de kennis, de capaciteit en is tevens op de hoogte van de procedures om het onderhoud uit te voeren? Zijn er alternatieven, bijvoorbeeld reverse engineering, of andere software? Het moge duidelijk zijn: het probleem van escrow is alleen met een multidisciplinaire benadering op te lossen.

## De geschillenregeling: een stiefkindje

De geschillenregeling wordt in automatiseringscontracten vaak behandeld als een stiefkindje. In contracten bestaat er meestal nauwelijks aandacht voor. Toch is geschillenbeslechting vaak de achter-

kant van automatisering. Er zijn vele mogelijkheden om een conflict op te lossen. Maar de weg naar de rechter moet als laatste worden bewandeld. Men verwisselt niet snel van leverancier wanneer er een verschil van mening is, er zijn te hoge bedragen mee gemoeid. Voor beide partijen is het vaak belangrijk om tot een oplossing te komen. In opkomst is de "minitrial" waarbij op directieniveau onder leiding van een onafhankelijke deskundige overleg wordt gevoerd, teneinde tot een oplossing te komen. Deze mogelijkheid biedt bijvoorbeeld de Stichting Geschillenoplossing Automatisering. De EDP-auditor zou hier ook een rol kunnen spelen. Als automatiseringsdeskundige kan hij of zij een rechter of arbiter bijstaan. Men dient dan wel op de hoogte te zijn van het recht: wat mag een deskundige wettelijk wel en wat niet in een proces?

## Conclusie

De informaticajurist en de EDP-auditor kunnen elkaar uitstekend aanvullen. Hun vakgebieden hebben verschillende raakvlakken. Beiden houden zich onder meer bezig met de economische en maatschappelijke kant van de ontwikkelingen binnen automatisering.
Duidelijk is dat men zich als professionele deskundige niet meer kan beperken tot het eigen vakgebied. Een multidisciplinaire aanpak is noodzakelijk om richting te geven aan de ontwikkelingen op het gebied van zowel automatisering als recht.

*Prof. A.W. Neisingh RA*
*Is vennoot bij KPMG Klynveld EDP Audit. Sedert 1971 is hij werkzaam op het terrein van de automatisering en controle. Hij heeft brede ervaring en kennis op het gebied van interne controle, accountantscontrole en dergelijke bij geautomatiseerde gegevensverwerking. Als openbaar accountant is hij in zijn specialistische rol betrokken bij de problematiek van automatisering en controle van vele ondernemingen, waaronder één van de grote Nederlandse banken. Als hoogleraar in de betrouwbaarheidsaspecten van geautomatiseerde informatiesystemen is hij part-time verbonden aan de Economische Faculteit (vakgroep Accountancy) van de Rijksuniversiteit Groningen.*

*Mw. mr. A.M.Ch. Kemna MBA*
*Is werkzaam bij KPMG Klynveld EDP Audit. Zij heeft rechten gestudeerd aan de Katholieke Universiteit Nijmegen en post-doctoraal bedrijfskunde (MBA) aan de Rotterdam School of Management, Erasmus Universiteit Rotterdam. Tot haar werkzaamheden behoort het onderzoeken van de relatie tussen de kwaliteit van de automatisering en het recht. Haar specifieke aandachtsgebieden zijn de beoordeling en begeleiding van computercontracten, de juridische aspecten van netwerken en de consequenties van de Wet Persoonsregistraties. Op dit laatste vlak heeft zij een bijdrage geleverd aan NIVRA-geschrift 58 inzake privacybescherming en de rol van de accountant. Anne-Marie Kemna heeft gepubliceerd en gedoceerd omtrent escrow.*

**De rechtsbescherming van computerprogrammatuur tegen ongeautoriseerd kopiëren en exploiteren staat al zo'n tien jaar in de belangstelling. Momenteel wordt het auteursrecht gezien als de manier om rechtsbescherming te bieden. Schrijver geeft in vogelvlucht een overzicht van een decennium softwarebescherming.**

Mr. V.A. de Pous

# Software-bescherming: tien jaar theorie en praktijk

## 1 Inleiding

De rechtsbescherming van computerprogrammatuur staat al zo'n tien jaar in de belangstelling en het laatste woord is er nog niet over gezegd. Wel worden de lijnen steeds duidelijker. Voor chips is inmiddels speciale wetgeving opgezet en het octrooirecht blijkt om uiteenlopende redenen minder geschikt te zijn om software-juridische protectie te verlenen. Wat overblijft is het auteursrecht. Dat wordt dan ook in Nederland en in de meeste andere landen als de manier aangewezen om een computerprogramma door middel van het recht te beschermen. Ook de Europese Gemeenschap gaat van het auteursrecht uit in de concept-Richtlijn software-bescherming. Op dit moment gaat de discussie dan vooral om de omvang van de auteursrechtsbescherming. Om eens wat te noemen: zijn grafische interfaces juridisch af te schermen tegen nabootsing? En welke rechten heeft de legale gebruiker van een computerprogramma? Mag hij bijvoorbeeld een backup-kopie maken of reverse engineering toepassen, zonder toestemming van de rechthebbende? Een decennium software-bescherming in vogelvlucht.

## 2 Software outlaws en pirates

Een computerprogramma is voor de auteur/producent zonder twijfel een belangrijk economisch goed. Het terugverdienen van investeringen in de zin van know-how en tijd is immers mede afhankelijk van het feit of het software-produkt op grote schaal zonder toestemming wordt gekopieerd en verkocht. Toch was er eens een tijd dat de vraag naar de juridische status van een computerprogramma en de manier waarop software door middel van het recht kon worden beschermd tegen onrechtmatig gebruik nauwelijks relevant was, terwijl software al wel bestond. Computersystemen werden namelijk in het verleden letterlijk als één systeem geleverd: programmatuur was in feite niet los verkrijgbaar. Daar heeft fabrikant van kantoormachines IBM in 1969 een einde aan gemaakt met de zogenoemde "unbundling". Hardware en software konden vanaf dat moment dus afzonderlijk worden aangeschaft en dat maakte de rechtsvragen die betrekking hadden op een computerprogramma actueler dan voorheen. Toch zou het nog bijna tien jaar duren voordat de nood echt aan de man kwam. Anders geformuleerd: voordat er regelmatig een beroep op het recht werd gedaan om software te beschermen.

Met de introductie van personal computers eind jaren zeventig was de beer definitief los. Computerprogramma's voor verschillende toepassingen, dat wil zeggen zowel zakelijke administratieve produkten als allerlei computerspelletjes, en in verschillende verschijningsvormen, zoals weggeschreven op een magnetische diskette maar ook vastgelegd in een micro-elektronische schakeling (ROM, EPROM en dergelijke), werden op grote schaal nagebootst of klakkeloos overgenomen. Software-piraterij was een feit. Met name het Amerikaanse pioniersbedrijf Apple Computers werd slachtoffer van deze illegale praktijken, maar Apple beet fel van zich af en een harde, wereldwijde rechtsstrijd tegen de handelwijze van piraten en kloners bracht uiteindelijk uitkomst. Software bleek in veel gevallen goed door het auteursrecht te kunnen

worden beschermd. In andere gevallen bracht een beroep op oneerlijke concurrentie uitkomst.

Door het optreden van Apple Computer is de software-industrie zich bewust geworden van de problematiek en de discussie brak los. Zo heeft een Belgische jurist in zijn dissertatie geopperd dat het auteursrecht niet geëigend is om aan technische produkten zoals computersoftware juridische protectie te verlenen, zag een Amsterdamse advocaat meer heil in een Amerikaansachtig "copyright", waarbij het deponeren van het auteursrechtelijk beschermde werk een rol speelt, en meende een bedrijfsjurist in de stellige overtuiging te zijn een gat in onze Auteurswet 1912 te hebben ontdekt, omdat programmatuur in "objectcode" niet voor auteursrechtsbescherming in aanmerking komt, omdat het produkt als zodanig niet (direct) voor menselijke waarneming vatbaar is.

*Creativiteit wordt aangenomen wanneer twee mensen met dezelfde opdracht statistisch bezien tot een verschillend resultaat dienen te komen.*

Deze argumenten hebben niet mogen baten. Rechterlijke uitspraken in binnen- en buitenland hebben laten zien dat auteursrecht, algemeen gesproken, een redelijke manier blijkt te zijn om software juridische protectie te verlenen tegen onrechtmatig gebruik in de meest brede zin van het woord.

## 3 Nederland

Op juridisch terrein is het geschut reeds lang in stelling gebracht en er is ook al flink mee geschoten. Hoofddoel: het auteursrecht. Sinds het begin van de tachtiger jaren heeft onze lagere rechter auteursrechtsbescherming voor software erkend, net zo als de juridische doctrine. Een computerprogramma kan namelijk auteursrechtelijk worden beschermd, indien het aan de eisen van de Auteurswet 1912 voldoet. Het produkt moet origineel zijn, dat wil zeggen niet het idee moet van creativiteit getuigen, maar de uitwerking, de vormgeving ervan. Daarnaast kent ons auteursrechtssysteem nog een wat afgezwakte beschermingsvorm voor geschriften zonder eigen of persoonlijk karakter.

In beginsel zal computersoftware echter gemakkelijk aan de eis van originaliteit voldoen. Creativiteit wordt aangenomen wanneer twee mensen met dezelfde opdracht statistisch bezien tot een verschillend resultaat dienen te komen.

Sedert het begin van de jaren tachtig zijn er in Nederland ten minste tien *civielrechtelijke* procedures gevoerd met betrekking tot rechtsbescherming voor computerprogramma's. In verreweg de meeste uitspraken is auteursrecht op software met een eigen en persoonlijk karakter door de rechter toegewezen. Hoewel de Hoge Raad zich hierover (nog) niet heeft uitgesproken, neemt vrijwel iedereen aan dat een computerprogramma van enige omvang met succes aanspraak kan maken op de bescherming die onze Auteurswet 1912 de rechthebbende biedt.

Ten aanzien van een print met componenten (transponder) heeft de Zwolse rechtbankpresident in 1983 gesteld dat het als een bekend feit moet worden beschouwd "dat in de elektronika vele wegen naar Rome leiden, waarbij de ene weg niet meer voor de hand ligt dan de andere en het derhalve wel gemakkelijk doch geenszins noodzakelijk is de door een andere ontwerper gekozen weg te volgen".
De rechtbank Den Bosch formuleerde een en ander in de zaak HIC vs. BAS (1981/1982) als volgt: "waar vaststaat dat een idee op zich geen auteursrechtelijke bescherming geniet, een computerprogramma kan worden beschouwd als een werk in de zin van het auteursrecht".

En indien het aan oorspronkelijkheid van een computerprogramma schort, dan staan de programmeur wiens werk wordt gekopieerd altijd rechtsmiddelen op grond van de slaafse nabootsing ten dienste, naast een beroep op de geschriftenbescherming.
Toch zal er in Nederland wetswijziging plaatsvinden. Een interdepartementale werkgroep zal hierover begin 1991 rapporteren; het resultaat hangt af van de ontwikkelingen in Brussel, in het kader van de harmonisatie van de auteurswetgeving in de twaalf lidstaten van de Europese Gemeenschap (zie paragraaf 4).

Tot zover de civielrechtelijke bescherming voor computerprogramma's. Wat zegt ons strafrecht ervan? Allereerst zijn er in de afgelopen tien jaar ten minste twee *strafrechtelijke* vonnissen gewezen, waarin de rechter vaststelde dat een computerprogramma een auteursrechtelijk beschermd werk is. Het gaat hier om

*Openbaar Ministerie vs. R.S.* (strafkamer Rechtbank Amsterdam, 1984) en *Openbaar Ministerie vs. W.S.* (strafkamer Rechtbank Arnhem, 1985), waarbij veroordelingen hebben plaatsgevonden op grond van schending van het auteursrecht (artikel 31 AW 1912: het opzettelijk inbreuk maken op auteursrechten).
Eerder heeft het Hof Arnhem het kopiëren van computerprogramma's op grond van verduistering (dus het gemene strafrecht) strafbaar gesteld, in het veel bekritiseerde arrest waarin wordt gesteld dat computergegevens en programma's het karakter hebben van "overdraagbaarheid, reproduceerbaarheid en beschikbaarheid, terwijl ze bovendien economisch waardeerbaar zijn" (*Openbaar Ministerie vs. W.A.R.*, strafkamer Gerechtshof Arnhem, 1983).

Verder is er in verband met de bestrijding van piraterij van auteursrechtelijk beschermde werken op 1 oktober 1989 de Wet van 3 juli 1989 (Staatsblad 1989, 282 en 1989, 316) in werking getreden. Deze wetswijziging omvat zowel civielrechtelijke (mogelijkheid tot afdracht genoten winst, mogelijkheid tot het leggen van revindicatoir beslag) als strafrechtelijke maatregelen. Zo wordt het opzettelijk ter verspreiding aanbieden, ter verspreiding of met het oog op invoer voorhanden hebben of uit winstbejag bewaren, tegenwoordig strafbaar gesteld. Een en ander brengt met zich mee dat opsporingsorganen niet meer hoeven te wachten tot de verspreiding of het openlijk te koop stellen daadwerkelijk plaatsvindt. Men kan al eerder ingrijpen. Bijvoorbeeld wanneer het auteursrechtelijke werk ter verspreiding wordt aangeboden of wanneer de dader met het oog op de verspreiding het werk voorhanden heeft.
Dit verspreidingsdelict wordt aangemerkt als misdrijf, met een strafbaarstelling van zes maanden gevangenisstraf of een geldboete van de vierde categorie, dat wil zeggen ƒ25.000.

*Als het aan het Europees Parlement ligt, mogen legale gebruikers reverse engineering toepassen om onderhoud en compatibiliteit te realiseren, indien hiervoor geen andere mogelijkheden aanwezig zijn.*

Vervolgens wordt de maximumstraf verhoogd tot vier jaar gevangenisstraf of een geldboete van de vijfde categorie, in casu ƒ100.000, indien de dader van het plegen van de delicten in art. 31 (het opzettelijk inbreuk maken op auteursrechten) en art. 31a (het opzettelijk ter verspreiding aanbieden of met dat doel voor ogen voorhanden hebben) een beroep maakt of het plegen van deze delicten als zijn bedrijf uitoefent. Bij rechtspersonen geldt alleen de maximum geldboete van ƒ100.000. Door de hoogte van de strafbaarstelling is voorlopige hechtenis mogelijk.

In een ander nieuw artikel gaat het ook om hetzelfde verspreidingsdelict, maar dan met schuld in plaats van opzet als bestanddeel. Er moet dan bewezen worden dat de dader redelijkerwijs kon vermoeden dat het werk waar het om gaat, is gemaakt met inbreuk op een andermans auteursrecht. Strafbaarstelling: maximaal een geldboete van ƒ10.000 (derde categorie). Verder wordt in de nieuwe wet bepaald dat opsporingsambtenaren die bevoegd zijn tot het opsporen van in de Auteurswet 1912 gestelde werken, vanaf 1 oktober 1989 de mogelijkheid hebben inzage te vorderen in alle bescheiden en informatiedragers, waarvan inzage voor de vervulling van hun taak redelijkerwijs nodig is. Van deze inzagebevoegdheid kunnen opsporingsambtenaren alleen gebruik maken tegen daders die op commerciële basis betrokken zijn bij auteursrechtelijk beschermde werken.

## 4 Europese ontwikkelingen

Als het aan het Europees Parlement ligt, mogen legale gebruikers reverse engineering toepassen om onderhoud en compatibiliteit te realiseren, indien hiervoor geen andere mogelijkheden aanwezig zijn. Bij reverse engineering gaat het om het technische proces om de "structure, sequence en organization" van een computerprogramma te analyseren op basis van de programmatuur in objectcode.
Het Europees Parlement staat nu onder voorwaarden reverse engineering toe. Daarnaast krijgen legale gebruikers een wettelijk recht om een backup-kopie van een computerprogramma te maken. Aldus staat in de door het Europees Parlement gewijzigde en op 11 juli jl. aangenomen ontwerp-Richtlijn software-bescherming. Het voorstel gaat uit van auteursrecht als beschermingsvorm en merkt software aan als een werk van letterkunde in de zin van de Berner Conventie tot bescherming van literaire en artistieke werken. Als de Raad alsnog ingrijpende wijzigingen van plan is aan te brengen, wil het Europees Parlement op-

nieuw worden geraadpleegd. In het geamendeerde voorstel wordt ervan uitgegaan dat de nationale wetgeving in de lidstaten uiterlijk op 1 januari 1993 aan de voorschriften van de Richtlijn voldoet. De Raad kwam op 12 april 1989 met de concept-Richtlijn als vervolg op het aan software en databanken gewijde hoofdstuk van het EG-Groenboek over auteursrechten.

Met deze richtlijn probeert de Europese Gemeenschap het wettelijk kader aan te geven waarbinnen leverancier en gebruiker van computerprogramma's dienen te functioneren. Enerzijds worden er exclusieve rechten voor de duur van vijftig jaar aan de software-auteur gegeven; anderzijds zijn er op deze rechten uitzonderingen geformuleerd, waardoor de gebruiker de mogelijkheid krijgt in redelijkheid met de programmatuur te werken. Hoewel het voorstel uitgaat van het auteursrecht op computerprogramma's, adresseert de regeling ook onderwerpen die niet in de nationale auteurswetten van de twaalf lidstaten van de Europese Gemeenschap voorkomen.
Voorbeelden hiervan zijn een geclausuleerde mogelijkheid tot reverse engineering, het begrip onderhoud op software, en artikelen die de contractvrijheid van leverancier en gebruiker op sommige punten aanzienlijk beperken.

Onder computerprogramma verstaat de ontwerp-Richtlijn vanaf heden: "iedere instructiereeks die bestemd is voor rechtstreeks of indirect gebruik in een informatiesysteem, met als doel een functie te verrichten of een bepaald resultaat te verkrijgen". De exclusieve rechten van de auteur zijn in tweeën gesplitst. Hij krijgt allereerst het uitsluitende recht zijn computerprogramma geheel of ten dele te verveelvoudigen. Daarnaast zijn het vertalen, aanpassen, bewerken en dergelijke van de software handelingen die louter aan hem zijn voorbehouden. Op beide rechten zijn ook uitzonderingen geformuleerd. Zo mag de legale gebruiker, indien hierover niets in het contract wordt gezegd, de kopieer- en bewerkingshandelingen zonder toestemming van de auteur verrichten, "indien zij noodzakelijk zijn voor het gebruik van het programma voor de beoogde doeleinden". Daarnaast bepaalt de gewijzigde Richtlijn dat het maken van een backup-kopie, opnieuw voor zover dat voor het beoogde gebruik noodzakelijk is, niet contractueel mag worden verboden.

Wat betekent de door het Europees Parlement goedgekeurde Richtlijn nu voor reverse engineering? Het kopieerverbod blijft weliswaar overeind staan, maar de wettige bezitter van een kopie van een programma kan "zonder toestemming van de rechthebbende de werking van het programma observeren, bestuderen of testen ter bestudering van de onderliggende ideeën, beginselen en andere aspecten die niet door het auteursrecht worden beschermd, voor zover het betrekking heeft op het laden, het bekijken, de uitvoering, de transmissie of de opslag". Software mag dus op allerlei manieren worden geanalyseerd, maar niet wanneer dat met zich meebrengt dat de programmatuur geheel of gedeeltelijk wordt gekopieerd.
Het voorstel gaat echter nog verder. In een door het Europees Parlement toegevoegd artikel wordt namelijk gesteld dat, tenzij contractueel anders bepaald is, de auteur zich niet op de verveelvoudigings- en bewerkingsverboden kan beroepen, wanneer een gebruiker deze handeling verricht, omdat die "absoluut noodzakelijk is voor het onderhoud en de opstelling en gebruik van compatibele computerprogramma's". Aan reverse engineering worden dus voorwaarden gekoppeld. De legale gebruiker mag de software alleen kopiëren en bewerken wanneer voor de verwezenlijking van de compatibiliteit noodzakelijke gegevens nog niet gepubliceerd of beschikbaar zijn gesteld. Ook mag het onderzoek van de programmatuur alleen die onderdelen betreffen die hiervoor noodzakelijk zijn. Verder mogen de aldus verkregen gegevens niet aan derden worden meegedeeld, "indien dit niet noodzakelijk is voor het gebruik van het tweede programma". Daarnaast mogen deze gegevens eveneens niet worden gebruikt voor het ontwikkelen van nieuwe programmatuur en het op de markt brengen van een computerprogramma "dat de auteursrechten van de maker van het oorspronkelijke programma schaadt".

## 5 User interface

Ging de eerste generatie jurisprudentie in casu over de vraag of software juridisch beschermd kan worden door het auteursrecht, de tweede generatie rechterlijke uitspraken heeft betrekking op de omvang van de rechtsbescherming voor computerprogramma's. Anders gezegd:

hoe ver reikt de wet? Een zeer belangrijk vonnis in dit kader betreft de juridische status, de "look-and-feel" van een computerprogramma. Hierbij gaat het met name om de (grafische) interface van software, de manier waarop de gebruiker met de software kan omgaan. Deze zomer heeft een Amerikaanse rechter een heel belangrijke uitspraak ter zake gedaan in de zaak *Lotus Development Corp. vs. Paperback Software International.*

Toen het software-bedrijf Lotus begin 1987 concurrent Paperback, samen met de oorspronkelijke auteur dr. James Stephenson van het computerprogramma dat door Paperback op de markt wordt gebracht, VP-Planner, voor de rechter daagde op grond van schending van auteursrechten en ongeoorloofde mededinging, werd in de dagvaarding gesteld dat het compatibele programmapakket VP-Planner van Paperback met enkele eenvoudige aanpassingen niets anders is dan een kopie van het rekenprogramma Lotus 1-2-3. Volgens eiser Lotus zijn de "look-and-feel" en de "user interface" van Lotus-programmatuur domweg gekloond en dat zou onder meer blijken uit de benaming van de functies, het scala en de opzet van keuzes in menu's en sub-menu's, de manier waarop en volgorde waarin de gebruiker deze keuzes in beeld krijgt en de macro-taal van het programma.

Dat VP-Planner inderdaad nauwkeurig is afgeleid van Lotus 1-2-3, spreekt niemand tegen. Ook Paperback niet. In de handleiding van het VP-Planner-programma wordt namelijk aangegeven dat de software "a feature-for-feature work-alike" is en dat het alles doet wat Lotus 1-2-3 doet. Ook gedraagt het zich en werkt het programma "just like 1-2-3", aldus de begeleidende tekst van Paperback. Aan de Amerikaanse District Court-rechter Robert R. Keeton werd de vraag voorgelegd of dat allemaal maar mag. Nee, dat is onrechtmatig, aldus Keeton in een 113 pagina's tellend vonnis in de zaak Lotus Development vs. Paperback Software. Paperback heeft zich schuldig gemaakt aan "overwhelming and pervasive" nabootsing van het zo succesvolle spreadsheet-programma Lotus 1-2-3.

*De uitspraak in de zaak Lotus vs. Paperback zet originele software-ontwikkelaars steviger in het zadel en verslechtert de rechtspositie van producenten van gekloonde computer-programma's.*

Rechter Keeton zegt in het Lotus/Paperback-vonnis het volgende over het begrip originaliteit in relatie tot menu's van computerprogramma's, zoals deze zich op het beeldscherm manifesteren: "Ik concludeer dat het mogelijk is dat een menucommandostructuur op verschillende en wellicht zelfs ongelimiteerde manieren kan worden vormgegeven, en dat de commandostructuur van Lotus 1-2-3 een originele en niet voor de hand liggende manier van vormgeven van een commandostructuur is." De rechter baseert zijn zienswijze op de vormgeving van andere spreadsheet-programma's, waaronder Multiplan, Framework II, Supercalc 4 en Excel. Daaruit blijkt tevens dat de structuur van het "Lotus-menu als één geheel" (het menusysteem) niet terugkomt in de vormgeving van de andere reken-software".
Verder stelt Keeton zichzelf de auteursrechtelijke vraag of de "structure, sequence and organization" (SSO) van het menucommandosysteem een substantieel deel uitmaakt van het vermeende auteursrechtelijk beschermde werk Lotus 1-2-3. "Ja", luidt zijn antwoord. "De gebruikersinterface is het meest unieke element van 1-2-3, en het is dit aspect dat 1-2-3 zo populair heeft gemaakt."

Op deze gronden neemt de rechter aan dat de gebruikersinterface van het computerprogramma Lotus 1-2-3 auteursrechtelijk beschermd is. De volgende stap betreft de positie van VP-Planner: gaat het om een toegestaan afgeleid produkt of een onrechtmatige nabootsing? Stephenson begon in 1982 het spreadsheet-programma FIPS te ontwikkelen, dat een jaar later voor een groot deel klaar was. In februari 1983 zag Stephenson echter een versie van Lotus 1-2-3 draaien, paste vervolgens FIPS aan en veranderde de naam in VP-Planner. Adam Osborne begon in die dagen net met Paperback Software International, een software-bedrijf dat programmatuur voor lage prijzen wilde aanbieden. Hij wilde VP-Planner graag uitgeven. Tijdens de procedure zeiden gedaagden dat VP-Planner huns inziens alleen een commercieel succes zou kunnen worden, als het compatible zou zijn met Lo-tus 1-2-3. De enige manier om dat te bereiken, was volgens hen ervoor te zorgen dat "arrangements and names of commands and menus in VP-Planner are conformed to that of Lotus 1-2-3". Files kunnen op deze wijze worden uitgewisseld en VP-Planner-gebruikers hoeven niet opnieuw te worden opgeleid.

Volgens de rechter gaat dit echter niet

op. Allereerst laat Excel zien dat succes mogelijk is, zonder honderd procent uitwisselbaar met Lotus 1-2-3 te zijn. Ten tweede kan compatibiliteit ook op een andere manier worden gerealiseerd dan door de menustructuur over te nemen, aldus Keeton. Hij denkt hierbij aan de macro-conversiemogelijkheid van Excel. Door VP-Planner bewust in de richting van Lotus 1-2-3 te ontwikkelen, hebben gedaagden juist die vormgegeven elementen overgenomen, die auteursrechtelijke status hebben. Dat is onrechtmatig.

Met dit vonnis is het laatste woord over de juridische status van "look-alike"-computerprogramma's nog niet gezegd. Onder de rechter is ook nog de zaak *Apple vs. Microsoft en Hewlett Packard*, waarop deze uitspraak zeker van invloed is. Daarnaast heeft Paperback te kennen gegeven tegen het deelvonnis in hoger beroep te gaan. De uitspraak in de zaak *Lotus vs. Paperback* zet originele software-ontwikkelaars dus steviger in het zadel en verslechtert de rechtspositie van producenten van gekloonde computerprogramma's. De organisatie en layout van een menu kunnen, evenals de menucommando's, in de Verenigde Staten auteursrechtelijk worden beschermd. Zoals hierboven al is gesteld, is er geen reden om aan te nemen dat de Nederlandse rechter er anders over zou denken.

*Mr. V.A. de Pous*
*Houdt zich sinds zijn studie Nederlands recht aan de Vrije Universiteit Amsterdam (doctoraal examen in 1983) bezig met advies en informatievoorziening inzake juridische aspecten van de informatietechnologie. Hij is onder meer juridisch commentator en columnist van het automatiseringsvakblad Computable en geeft de maandelijkse nieuwsbrief NewsWare uit.*

**Automatiserings projecten vergen over het algemeen naast een goede technische en organisatorische voorbereiding en invulling de nodige aandacht voor de juridische consequenties. Dit artikel geeft een overzicht van juridische aandachtspunten bij de ontwikkeling van software. Tevens is een checklist opgenomen voor een offerte-aanvraag.**

**Prof.mr. J.M.A. Berkvens**

# Juridische aandachtspunten bij software-ontwikkeling

## 1 Algemeen

Bij de ontwikkeling van software zijn er ook voor de jurist de nodige onderwerpen die de aandacht verdienen. Zo zal bij de ontwikkeling van software rekening moeten worden gehouden met de mogelijkheid dat de wet specifieke eisen stelt aan die software. Men denke bijvoorbeeld aan de eisen inzake beveiliging zoals die uit de Wet Persoonsregistraties voortvloeien. Een bijzonder aandachtspunt vormt de mogelijkheid van auteurs- of zelfs octrooirechtelijke bescherming van de software. Als de software in chips is belichaamd, geldt de Wet inzake de bescherming van topografieën van halfgeleiderprodukten. Fiscalisten kunnen zich bezighouden met waarderingsvraagstukken. Bankjuristen kunnen zoeken naar wegen om te financieren met software als zekerheid. Als de ontwikkeling van de software wordt uitbesteed, ontstaat een reeks van contractuele aandachtspunten. Het gaat daarbij om de juridische relevantie van de precontractuele fase (offerte-aanvraag, behandeling offertes, onderhandelingen) en eventuele intentieverklaringen. Daarnaast moet er worden gezorgd voor de opstelling van contracten inzake advisering alsmede de ontwikkeling, de implementatie en het onderhoud van de software. In dit artikel wordt met name ingegaan op de eisen die de wet stelt aan software alsmede aan het realiseren van adequate juridische bescherming rondom de externe ontwikkeling van de software.

### Maatwerk

Als er geautomatiseerd gaat worden, betekent dat niet dat steeds opnieuw het wiel moet worden uitgevonden. Veel organisaties kampen met dezelfde problemen. Voor grote groepen van toepassingen is derhalve op ruime schaal standaard-software beschikbaar. Een organisatie kan dan, desnoods met externe ondersteuning, een passende oplossing selecteren uit het bestaande aanbod. Dat is echter niet altijd mogelijk. Zo zullen bijvoorbeeld unieke processen, bedrijfsspecifieke randvoorwaarden, systeemintegratieproblemen en nieuwe vraagstukken een maatwerkbenadering vereisen.

## 2 Interne fase

De lange weg naar het in gebruik nemen van nieuwe software begint met een intern onderzoek naar de aard van de problemen en de mogelijke oplossingsrichtingen. Als besloten wordt tot automatisering, dient een nadere uitwerking te worden gemaakt van de eisen die men aan die automatisering stelt. Dergelijke eisen krijgen vorm in functionele specificaties. Soms kunnen ook technische specificaties worden opgesteld. Men denke aan de protocollen die nodig zijn om de software in samenhang met andere software of hardware te laten functioneren.
Een ander punt van aandacht zijn de operationele eisen. Welke piekbelasting moet de software aankunnen? Welke functies dienen gelijktijdig beschikbaar te zijn? Welke reactietijden zijn nog acceptabel? Wat zijn de eisen die de software mag stellen aan de scholingsgraad van personeel, welke computercapaciteit is beschikbaar? Welke gevolgen mag de automatisering hebben voor de interne organisatie? Moet er een opleidingsprogramma beschikbaar komen; hoe zit het met documentatie?
Ook ten aanzien van het onderhoud

dient een en ander op papier te staan. Hoe snel dient een storing te kunnen worden verholpen, zijn er stand by-eisen, welke soorten onderhoud wil men zelf verrichten? Welke eisen moet men stellen ten aanzien van de continuïteit van de software: beschikbaarheid onderhoud, ondersteuning bij calamiteiten, beschikbaarheid van broncodes, toekomstige uitbreidingsmogelijkheden.
Een ander punt van aandacht is de specificatie van de beschikbare financiële ruimte, te differentiëren naar de kosten van software-ontwikkeling, software-onderhoud en gebruikskosten.
Het uitwerken van het pakket van eisen kan in eigen beheer gebeuren of onder inschakeling van een externe adviseur. In dat laatste geval is het nuttig de voorwaarden waaronder de advisering plaatsvindt schriftelijk vast te leggen. Daarbij is met name van belang in welke mate de adviseur verantwoordelijk kan worden gesteld voor eventuele gebreken in zijn advies. Als de adviseur bijvoorbeeld een bepaalde combinatie van hardware en (te ontwikkelen) software adviseert die achteraf niet blijkt te werken, is het voor de opdrachtgever prettig als hij zijn schade kan verhalen. Adviseurs kunnen hun risico ter zake afdekken in een algemene beroepsaansprakelijkheidsverzekering.

**Wetgeving**
Bij de opstelling van het pakket van eisen wordt het in toenemende mate belangrijk na te gaan of in het licht van bestaande of komende wetgeving specifieke eisen aan de software moeten worden gesteld. Het aantal wetten dat zich direct of indirect met de inhoud van de automatisering bezighoudt, neemt namelijk alleen maar toe. Daarnaast zijn er wetten die invloed hebben op de beschikbaarheid van software. Voorts kunnen uit bestaande overeenkomsten met derden nadere eisen ten aanzien van de software voortvloeien. Hieronder volgen enkele voorbeelden:

-- De Wet Persoonsregistraties heeft gevolgen voor de wijze waarop computerprogramma's moeten worden gestructureerd. Veel computerprogramma's worden immers gebruikt om gegevens over personen (personeel, cliënten, relaties) te genereren, te transporteren, op te slaan of te bewerken. Men dient aandacht te besteden aan invoervalidatie, functiescheidingen in programmatuur, rapportage- en mutatiemogelijkheden alsmede zorg te dragen voor beveiligingsprocedures. Soms kan het achterwege laten van de opneming van bepaalde gegevens vrijstelling van formulier- of reglementsplicht tot gevolg hebben. Dus is het nuttig alle op te nemen gegevenssoorten nog eens op relevantie te screenen.

-- Het voorstel tot aanpassing van het Wetboek van Strafrecht stelt als randvoorwaarde voor strafbaarheid van computervredebreuk, dat er sprake was van een voldoende niveau van beveiliging.

-- Er ligt een voorstel bij de Tweede Kamer om het Burgerlijk Wetboek te voorzien van een bepaling die bedrijven verplicht een uitspraak over de kwaliteit van de automatisering in het jaarverslag op te nemen.

-- De Wet Telecommunicatievoorzieningen stelt nadere voorwaarden ten aanzien van het opzetten van telecommunicatie-infrastructuren, de aan te sluiten randapparatuur en het gebruik van faciliteiten.

-- In belastingwetgeving wordt geleidelijk meer aandacht besteed aan het faciliteren van het geautomatiseerd opbergen van informatie die krachtens deze wetgeving soms wel tien jaar bewaard moet blijven. De wet geeft randvoorwaarden.

-- Op diverse andere terreinen is de wetgever actief. Men denke aan produktaansprakelijkheid voor gebrekkige software, bewijsregels in EDI-systemen, toepassing van het mededingingsrecht ten aanzien van het gebruik van grote exclusieve geautomatiseerde systemen (banken, luchtvaartreserveringssystemen), etc.

-- Financiële instellingen worden geconfronteerd met eisen van de Europese Commissie ten aanzien van de standaardisatie van informatiesystemen ten behoeve van het betalingsverkeer.

-- Grensoverschrijdend gegevensverkeer wordt in toenemende mate aan formaliteiten onderhevig. In juli 1990 maakte de Europese Commissie nieuwe initiatieven bekend.

-- Ten aanzien van de beschikbaarheid van software zijn er eveneens wettelijke regels. Zo kan de aanschaf van bepaalde soorten programmatuur vallen onder exportbeperkende maatregelen. Met name in de sfeer van beveiliging en

encryptie kan sprake zijn van dergelijke belemmeringen.

-- Als de te ontwikkelen software gebruik maakt van modulen van derden of als de intellectuele eigendom bij de ontwikkelaar zal berusten, is het auteursrecht van belang. Binnen de Europese Commissie zijn voorstellen in voorbereiding voor een richtlijn die enerzijds software expliciet onder de werking van het auteursrecht brengt, maar anderzijds beperkingen oplegt in het operationele gebruik van die software. Het gaat om de beperking van aantallen backup-kopieën en beperkingen ten aanzien van bepaalde vormen van reverse engineering die noodzakelijk zijn om storingen in software te verhelpen, onderhoud door derden te laten verrichten en de software in een multi-vendor-omgeving te installeren (voorstel voor een richtlijn van de Raad betreffende de rechtsbescherming van computerprogramma's, Com (88) 816 def\-SYN 183, Publicatie-blad C 91/4 van 12 april 1989). In het Europees Parlement zijn inmiddels enkele verzachtende amendementen geaccepteerd (17 juli 1990), welke slechts ten dele zijn terug te vinden in het Consolidated Amended Proposal van 8 november 1990.

*De opdrachtgever zal in ieder geval een standpunt moeten innemen ten aanzien van de vertrouwelijkheid van de aan de ontwikkelaar te verstrekken informatie, de vraag wie auteursrechthebbende wordt, of de ontwikkelaar bepaalde exploitatierechten verkrijgt en zo ja, op welke voorwaarden.*

-- Indien systemen worden gebruikt als ondersteuning in de uitvoering van overeenkomsten met derden, dient te worden nagegaan welke eisen ten aanzien van de systemen voortvloeien uit die contracten. Maar ook moet worden nagegaan welke schade kan voortvloeien uit wanprestatie als gevolg van de uitval van geautomatiseerde systemen: moet dergelijke schade worden afgewenteld op de leverancier van het systeem, is verzekering mogelijk, draagt de organisatie de schade zelf of dient de schade te worden geëxonereerd.

-- Als te ontwikkelen software wordt geïntegreerd in een bestaand geautomatiseerd systeem, dient te worden nagegaan of in de licentiecontracten met de desbetreffende leveranciers ruimte wordt geboden om de integratie tot stand te brengen. Worden de noodzakelijke specificaties ter beschikking gesteld, is reverse engineering toegestaan, mogen derden worden ingeschakeld?

**Intellectuele eigendom**
Als duidelijk is welke eisen aan de software gaan worden gesteld en nadat de eisen eventueel zijn bijgesteld in het licht van wettelijke randvoorwaarden, komen de overige juridische randvoorwaarden aan de orde.
Allereerst is er de vraag of de te ontwikkelen software volledig eigendom zal moeten worden van de opdrachtgever. Het is denkbaar dat de ontwikkelaar van de software de bij de ontwikkeling opgedane kennis commercieel wil benutten. Mogelijk wil hij zelfs de programmatuur gaan distribueren onder derden. Daar staat tegenover dat de specificaties die ten grondslag hebben gelegen aan de ontwikkeling van de programmatuur een vertrouwelijk karakter kunnen hebben en wellicht zelfs een voorsprong op concurrenten betekenen. De opdrachtgever zal in ieder geval een standpunt moeten innemen ten aanzien van de vertrouwelijkheid van de aan de ontwikkelaar te verstrekken informatie, de vraag wie auteursrechthebbende wordt, of de ontwikkelaar bepaalde exploitatierechten verkrijgt en zo ja, op welke voorwaarden.
Soms doet zich het probleem voor dat in de te ontwikkelen software bestaande standaardroutines worden ingebouwd waarvan het gebruiksrecht bij de leverancier of diens toeleverancier blijft berusten. Als de ontwikkelaar de intellectuele eigendomsrechten verkrijgt, komt de vraag aan de orde of de opdrachtgever de beschikking krijgt over de broncode van de programmatuur. Die is van belang als er problemen ontstaan waardoor de ontwikkelaar niet meer bereid of in staat is onderhoud te verrichten. Als de broncode bij de ontwikkelaar blijft berusten, is het aan te bevelen een escrow-regeling te treffen, waarbij de broncode op een veilige plaats wordt gedeponeerd en beschikbaar is bij problemen.

**Garanties**
Een volgend onderwerp vormen de gewenste garanties:

-- Is de leverancier bereid de totale verantwoordelijkheid voor het project te dragen? Hij is degene die een bepaalde oplossing heeft geoffreerd. Hij is degene die daarbij mogelijk derden/onderaannemers betrekt.
Hij is beter dan de opdrachtgever in staat een en ander onder controle te houden. Indien delen van de software niet blijken te kunnen functioneren, neemt hij dan eventueel speciaal aangeschafte hardware ook terug?

-- Garandeert de leverancier dat het eindresultaat ook geschikt is voor de door de opdrachtgever kenbaar gemaakte doelstellingen? Fitness for purpose.

-- Staat de leverancier in voor het halen van het door hem geoffreerde tijdschema? Is er een sanctie in de vorm van een boete bij ernstige aan hem te wijten vertragingen?

-- Indien toekomstige uitbreidingsmogelijkheden in het vooruitzicht zijn gesteld, kan de leverancier hier dan een garantie voor geven (bijvoorbeeld een bankgarantie)?

-- Garandeert de leverancier dat de software na oplevering gedurende de economische levensduur kan worden onderhouden? Geldt die garantie ten aanzien van alle functies? Omvat het onderhoud upgrades, verhelpen van storingen, aanpassing van programmatuur aan externe ontwikkelingen? Wat zijn de sancties bij gebrekkig onderhoud? Zijn er criteria vastgesteld voor de kwaliteit van het onderhoud? Wat zijn de reactietijden ten aanzien van het onderhoud?

-- Maakt de geoffreerde oplossing geen inbreuk op wetten of op rechten van derden? Er kan sprake zijn van inbreuken op rechten van intellectuele eigendom van derden in Nederland of andere landen.

-- Indien er sprake is van een zogenaamde multi-vendor-omgeving (de te ontwikkelen software wordt gebruikt op hardware van andere leveranciers of aan andere software gekoppeld) dient bij voorkeur van iedere leverancier de bereidheid te zijn vastgelegd dat hij op verzoek van de afnemer onvoorwaardelijk medewerking zal verlenen aan het detecteren van storingsoorzaken. De kosten kunnen naderhand worden verhaald op de veroorzaker of de afnemer.

-- Garandeert de leverancier dat de software vrij is van virussen?

-- Welke garanties zijn er ten aanzien van het risico van discontinuïteit van het bedrijf van de leverancier? Is er een parent guarantee of is een hardware-leverancier bereid garant te staan? Is alle software beschikbaar in broncodevorm of moet er een escrow-arrangement worden opgezet?

**Aansprakelijkheid**
Ten aanzien van de aansprakelijkheid van de ontwikkelaar voor schade als gevolg van mislukking van het project zou een analyse kunnen worden gemaakt van het totaal van de mogelijke schade. Daarbij kan worden gedacht aan de kosten van het opnieuw opstarten van een selectieproces, de eigen personeelskosten, onkosten van apparatuur en ruimte gedurende het project en de vooraf aan de leverancier betaalde bedragen. Daarnaast zijn er kostencategorieën in de meer indirecte sfeer, bijvoorbeeld gederfde winst of claims van derden. Kan van de leverancier worden gevraagd bij mislukking alle kosten te vergoeden; is er een maximum? Hier speelt een rol of de leverancier een beroepsaansprakelijkheidsverzekering heeft afgesloten.

**Projectorganisatie**
Ten aanzien van de organisatie van het ontwikkelwerk kunnen randvoorwaarden worden opgesteld met betrekking tot de opsplitsing van het project in min of meer zelfstandige onderdelen, het definiëren van verantwoordelijkheden, het specificeren van procedures tot wijziging van de specificaties en het inbouwen van breekpunten waarop het project nog kan worden geannuleerd. Zeer belangrijk is een procedure die kan worden gevolgd als er onenigheid zou zijn ten aanzien van de uitleg van specificaties.
Het verdient aanbeveling ervoor te zorgen dat onenigheid niet leidt tot het vertragen van het project. Het is beter af te spreken dat als regel het project conform de wensen van de opdrachtgever doorgaat. Men zoekt naderhand uit wie de kosten draagt, eventueel met inschakeling van derden.

**Selectiecriteria leverancier**
Een aandachtspunt vormen de eisen ten aanzien van de ontwikkelaar zelf. Naarmate het belang van de te ontwikkelen programmatuur voor de opdrachtgever groter wordt, dient hij meer aandacht te besteden aan de ontwikkelaar. Wat is de rechtsvorm; wat is de financiële positie; wat is de ervaring; zijn er vergelijkbare systemen ontwikkeld; is de kritische kennis over voldoende personen gespreid; kunnen onvriendelijke prioriteitenstellingen (een andere cliënt krijgt voorrang bij het toewijzen van capaciteit) het onderhoud vertragen?

**Modelcontracten**
Een laatste punt is ten slotte de vraag van de contracten. De opdrachtgever

doet er verstandig aan zelf een idee te hebben van de inhoud van de uiteindelijke overeenkomst.
De overeenkomst heeft een tweeledige indeling. Enerzijds zal veel ruimte (veelal in bijlagen) worden besteed aan een beschrijving van het onderwerp van de overeenkomst. Anderzijds worden formele regels vastgelegd. De opdrachtgever kan kiezen uit een groot aantal bestaande contractmodellen. Zowel leveranciersorganisaties (VIFKA, COSSO) als gebruikers (COMGE, RKMC, BIZA) hebben modellen ontwikkeld. Ook de grotere leveranciers en afnemers alsmede advocatenkantoren en adviesbureaus hebben eigen standaards. Die dienen enerzijds een antwoord te geven op specifieke juridische vraagstukken (toepasselijk recht, overmacht, overdracht rechten en plichten, aansprakelijkheden) en anderzijds ruimte te geven voor een gedetailleerde weergave van de te verrichten werkzaamheden.

*Grote leveranciers zullen kleine afnemers hun voorwaarden proberen op te leggen. Voorwaarden die de risico's van die leveranciers beperken. Voorwaarden waaringaranties ontbreken enwaarin aansprakelijkheden worden uitgesloten.*

**Opstellen Request For Proposal (RFP)**
Als de opdrachtgever gereed is met het uitwerken van de beschrijving van het gewenste produkt en de bijbehorende randvoorwaarden, kan worden aangevangen met het zoeken van een geschikte leverancier. Een pragmatische werkwijze is daarbij het uitlokken van offertes die, volgens een vooraf bepaald formaat, de voor de opdrachtgever relevante informatie verschaffen. Daartoe wordt door de opdrachtgever een Request For Proposal (RFP) opgesteld. Dit document verschaft potentiële leveranciers zoveel mogelijk gedetailleerde informatie over de opdrachtgever, diens probleem alsmede de gewenste oplossing. Vervolgens wordt de leverancier uitgenodigd informatie te verschaffen over zichzelf (soliditeit, organisatiestructuur, ervaring), de te leveren oplossing, de financiële aspecten van de oplossing alsmede de juridische randvoorwaarden.
Ten slotte geeft het RFP aan volgens welke procedure en onder welke voorwaarden de opdrachtgever eventuele offertes zal evalueren. Daarbij denke men onder andere aan de minimale geldigheidsduur van een offerte en geheimhoudingsaspecten.
Als bijlage is aan het slot van dit artikel een checklist RFP met honderd vragen opgenomen.

## 3 Externe fase

De opdrachtgever distribueert zijn RFP onder in aanmerking komende softwareontwikkelaars. Nadat de offertes zijn binnengekomen, vindt evaluatie plaats en worden nadere gesprekken gevoerd met enkele serieuze gegadigden. Naarmate RFP en offerte beter op elkaar aansluiten, zal op een zeker moment de definitieve keuze voor een bepaalde leverancier kunnen worden gemaakt. Op dat moment zou een overeenkomst moeten worden opgesteld, waarin de wederzijdse verplichtingen worden bevroren. Als de onderhandelingen goed zijn voorbereid, zou het contract kunnen bestaan uit het door de opdrachtgever geselecteerde standaardcontract, waarbij RFP en offerte als bijlagen fungeren. In de praktijk zullen, zeker als het gaat om software-ontwikkeling, gedurende de onderhandelingen nog de nodige aanpassingen worden aangebracht.

**De praktijk**
Hoewel het de voorkeur verdient over een goed contract te onderhandelen, zal dat in de praktijk niet altijd mogelijk blijken te zijn. Grote leveranciers zullen kleine afnemers hun voorwaarden proberen op te leggen. Voorwaarden die de risico's van die leveranciers beperken. Voorwaarden waarin garanties ontbreken en waarin aansprakelijkheden worden uitgesloten. Daarbij zal men zich soms beroepen op interne voorschriften die door (buitenlandse) moeders worden voorgeschreven. Of men wijst op het tijdrovende karakter van onderhandelingen. Met name als het contractsbelang gering is of als de risico's klein zijn, valt hier enig begrip voor op te brengen. Voordat men echter klakkeloos de leveranciersvoorstellen dan maar accepteert kunnen nog enkele varianten worden overwogen.

1. Men kan een lijst van knelpunten opstellen met de wenselijke oplossing (toptien). Als bijvoorbeeld de opleverdatum van cruciaal belang is, kan een garantie met boete op overschrijdingen gewenst zijn. Of een bankgarantie (performance bond) ten aanzien van het inderdaad gerealiseerd worden van beloofde toekomstige uitbreidingsmogelijkheden. Het contract kan dan bestaan uit de algemene voorwaarden van de leverancier aangevuld met een bijlage waarin op de desbetreffende punten wordt afgeweken van die voorwaarden.

2. Bij een eenvoudige opdracht kan

worden volstaan met een summier document waarin de toepasselijkheid van algemene voorwaarden (van beide par-tijen) wordt uitgesloten en waarin slechts enkele essentialia worden vermeld. Bijvoorbeeld een verwijzing naar functionele specificaties, een opleverdatum en een prijs of een nacalculatiesysteem.

3. Bij een confrontatie tussen algemene voorwaarden van leverancier en afnemer kan wellicht worden uitgeweken naar door veel leveranciers geaccepteerde evenwichtige standaardcontracten. Men denke aan de RKMC-overeenkomst voor de ontwikkeling van software. Of men neme de in opdracht van de minister van Binnenlandse Zaken ontwikkelde software-contracten.

4. Conflicten over de bevoegde rechter c.q. het toepasselijk recht kunnen worden opgelost door "naar een neutraal land uit te wijken". Ook kan het zijn dat bemiddeling door de Stichting Geschillenoplossing Automatisering (minitrial, bindend advies, arbitrage) is te prefereren.

5. Een contract kan in Nederlandse ogen onvriendelijk overkomen als het is opgesteld voor een Angelsaksisch rechtssysteem. Als een met een Neder-landse rechtspersoon gesloten contract onderworpen is aan de interne fiattering door een buitenlandse moeder, kan een tussen leverancier en opdrachtgever geldende interpretatieve side letter enkele scherpe kanten weghalen.

6. Ten slotte zij opgemerkt, dat in de jurisprudentie criteria zijn ontwikkeld die kunnen verhinderen dat in geval van onredelijk bezwarende voorwaarden een beroep op een dergelijke contractbepaling kan worden gedaan.

## 4 Conclusie

Helaas gebeurt het maar al te vaak dat in een zeer laat stadium juristen worden betrokken bij een automatiseringsproject. In het voorgaande is aangegeven dat al bij het intern opstellen van functionele specificaties software-juridische invalshoeken van belang kunnen zijn. Uit de bij dit artikel behorende checklist voor de RFP blijkt dat er een groot aantal vragen is dat bij de selectie van de leverancier van belang is. Daarnaast zijn er nogal wat onderwerpen die van het grootst mogelijke belang zijn voor de opdrachtgever in het kader van de sturing en de beheersbaarheid van het project. Een RFP kan ertoe bijdragen dat de selectie van de leverancier op een meer verantwoorde wijze plaatsvindt. Als de positie van de leverancier ten aanzien van de diverse vragen bekend is, worden de contractbesprekingen vereenvoudigd. Er wordt voorkomen dat moeizame onderhandelingen volgen, waarbij de opdrachtgever het risico loopt dat zijn sturingsmogelijkheden sterk worden beperkt onder gelijktijdige toename van zijn financiële risico's.

*Prof.mr. J.M.A. Berkvens*
*Is hoofd van de afdeling Juridische Adviezen Informatica, Stafgroepen & Diensten en Logistiek binnen de Juridische en Fiscale Dienst van de Rabobank Nederland.*
*Hij is tevens als bijzonder hoogleraar Informatica & Recht verbonden aan de Juridische Faculteit van de Katholieke Universiteit Nijmegen. Hij is lid van de redactie van het blad Computerrecht en publiceert regelmatig over onderwerpen als elektronisch betalingsverkeer, privacy en computercontracten.*

*Bijlage*
## Checklist Request For Proposal (RFP) (100 vragen)

### RFP en offerte

1. Vrijblijvendheid offerte.
2. Geldigheidsduur offerte.
3. RFP en offerte worden deel van het contract.
4. Kosten opstellen offerte zijn voor leverancier.
5. RFP vertrouwelijk behandelen.
6. Opgenomen specificaties blijven eigendom opdrachtgever en mogen niet door leverancier worden gebruikt.
7. Relatie met opdrachtgever geheim houden.
8. Copyright RFP voorbehouden aan opdrachtgever.

### Opdrachtgever

9. Rechtsvorm.
10. Organisatiebeschrijving.
11. Probleemomschrijving.
12. Omschrijving gewenste oplossing.
13. Samenhang met andere systemen.

### Leverancier

14. Rechtsvorm.
15. Financiële gegoedheid (jaarverslagen).
16. Aantal werknemers; aantal vestigingen.
17. Verspreiding know-how over de werknemers.
18. Professionele ervaring.
19. Afhankelijkheid van know-how bij prioriteitenstelling door andere concern-onderdelen of overige derden.
20. Wie is auteursrechthebbende van eventueel te integreren standaardmodulen.
21. Heeft leverancier een beroepsaansprakelijkheidsverzekering.
22. Heeft leverancier ervaring met vergelijkbare projecten, zijn er referenties.
23. Is leverancier lid van een beroepsvereniging die kwaliteitseisen stelt (bijvoorbeeld COSSO).
24. Heeft leverancier invloed op de relevante hardware-leveranciers.

### Algemeen

25. Toepasselijkheid gekozen standaardcontract opdrachtgever.
26. Order of precedence: contract, RFP, offerte en overige bijlagen.
27. Toepasselijkheid Nederlands recht.
28. Bevoegdheid Nederlandse rechter.
29. Uitsluiting internationaal privaatrecht.
30. Geschillenbeslechtingsprocedures (minitrial).
31. Specifieke geheimhoudingsregels.
32. Bereidheid projectverantwoordelijkheid te dragen.
33. Omvang eventuele beperking aansprakelijkheid uit wanprestatie of uit wet.
34. Bereidheid tot redelijke schadevergoeding bij vertragingen.

### Intellectuele eigendomsrechten

35. Bereidheid tot overdracht auteursrechten van ontwikkelde software.
36. Status gebruikte modulen van derden.
37. Licentievoorwaarden standaardmodulen.
38. Bereidheid tot levering sources; escrow-regeling.
39. Overdraagbaarheid systeem aan derden.
40. Afspraken over exploitatierechten voor leverancier.

**Garanties**

41. Garantieverklaring moedermaatschappij leverancier mogelijk.
42. Bereidheid bankgarantie af te geven ten aanzien van toekomstige uitbreidingsmogelijkheden.
43. Garantie dat geen inbreuk op rechten van derden wordt gemaakt.
44. Fitness for purpose-garantie.
45. Virusvrij-garantie.
46. Conformiteitsgarantie (software zal voldoen aan specificaties).
47. Tijdigheidsgarantie (oplevering zal niet vertraagd zijn).
48. Integratiegarantie (software functioneert in samenhang met hardware en andere software) ook indien meer dan één leverancier betrokken is.

**De ontwikkeling van het systeem**

49. Gedetailleerde beschrijving technische en functionele karakteristieken per onderdeel.
50. Change request-procedures; regeling meerwerk.
51. Projectorganisatie, beslissingsbevoegdheden beide partijen.
52. Voortgangsrapportage ontwikkelwerk; melding vertragingen; inzet extra-capaciteit bij vertragingen.
53. Vervanging slecht functionerende personen.
54. Procedure voor inschakeling derden.
55. Gefaseerde oplevering, vaste tijdstippen per onderdeel.
56. Breekpunten; kosten bij tussentijdse beëindiging; eigendom onvoltooide werken; voltooien door derden.
57. Acceptatieprocedure per opgeleverd onderdeel; integratietest totaal systeem.
58. Gebruikmaking van bestaande software.
59. Is leverancier verplicht de relevantie en volledigheid van door opdrachtgever verstrekte informatie te verifiëren.
60. Verantwoordelijkheid voor configuratiekeuzes.
61. Gebruikmaking van formele ontwikkelmethodieken.
62. Certificatie van software.
63. Voorziet het ontwikkelproces in viruspreventie en -detectie (checksum, scanners, overige controles).

**Onderhoud**

64. Indeling in soorten mogelijk onderhoud (storingen, parameters, uitbreidingen, structuurveranderingen, upgrading hardware, upgrading besturingssysteem).
65. Beschikbaarheid onderhoud buiten kantooruren, stand by-faciliteiten, telefonische ondersteuning (helpdesk).
66. Beschikbaarheid onderhoud gedurende levensduur systeem.
67. Informatie over release-beleid (aard, frequentie).
68. Storingsprocedures, prioriteitenstelling, responstijden bij melding.
69. Coördinatie storingshandling in multi-vendor-omgeving.
70. Compatibiliteitsgarantie applicaties bij wijzigingen in hardware.
71. Compatibiliteitsgarantie applicaties bij wijzigingen in operating systeem.
72. Calamiteitenregeling mogelijk.
73. Afwijkende regels voor standaardmodulen, onderhoud standaardmodulen door derden.
74. Beschikbaarheidsregeling mogelijk.
75. Bereidheid tot conversie-applicatie bij migratie naar andere hardwareomgeving.
76. Facilitering onderhoud in eigen beheer.
77. Sancties bij slecht onderhoud.
78. Beschikbaarheid structuurgegevens standaardmodulen.

**Kosten**

79. Gedetailleerd overzicht van de kosten van het systeem: schatting kosten manuren ontwikkelwerk, kosten gebruik ontwikkelapparatuur, invoeringskosten (documentatie, opleidingen, kosten schaduwdraaien), operationele kosten (manjaren, apparatuur, onderhoud, afschrijving).
80. Betalingsschema.
81. Specificatie dagtarieven van alle soorten medewerkers.
82. Specificatie onderhoudskosten.
83. Specificatie invloed interne promoties op tarieven ingeschakelde medewerkers.
84. Specificatie indexmechanismen tarieven.
85. Project op basis van nacalculatie, fixed price of mengvorm.
86. Berekening eventuele fixed price-offerte op basis van betaling achteraf.
87. Welke valuta; welke verrekeningsregels.
88. Toepasselijke kortingen.

**Documentatie en opleidingen**

89. Welke documentatie is beschikbaar (soort, taal).
90. Aantal gratis exemplaren; kopieer- en gebruiksrestricties.
91. Presentatievorm (paperbased of machine-readable); update-procedures.
92. Welke cursussen worden gegeven (soort, taal, individueel of klassikaal).
93. Kosten; kortingsregeling.

**Escrow**

94. Is de software onderhoudbaar door opdrachtgever.
95. Is er een "bankruptcy proof"-constructie.
96. Wordt reeds tijdens ontwikkelproces gedeponeerd.
97. Depot van standaardmodulen van derden, documentatie, compilers.
98. Is voorzien in updating van sources.
99. Omvatten de "triggering events" faillissement, wanprestatie, overmacht, virusproblemen.
100. Is inschakeling van derden bij completering ontwikkeling of onderhoud toegestaan.

Mw. mr. A.M.Ch. Kemna MBA

# Escrow. Het depot van de broncode: fopspeen of panacee?

**Het begrip "software escrow" heeft in automatiseringskringen inmiddels enige bekendheid verworven. Met name bij software-ontwikkeling en bij licentiëring van specifieke of dure standaardsoftware kan escrow uit oogpunt van continuïteit gewenst zijn. Escrow is echter een vlag die nogal wat lading dekt. Of een escrowovereenkomst slechts een fopspeen of juist een uitkomst is, zal dan ook steeds inhoudelijk moeten worden getoetst.**

## 1 Inleiding

De woorden "software escrow" en "source code depot" hebben in automatiseringskringen inmiddels de nodige bekendheid verworven. Menig auditor weet dat de begrippen te maken hebben met de continuïteit van de geautomatiseerde gegevensverwerking en daarmee met de bedrijfscontinuïteit.
De inhoudelijke uitwerking van een escrow is voor velen echter nog onduidelijk. Geen wonder, want het betreft een complex juridisch vraagstuk, maar ook en vooral een aangelegenheid die zorgvuldige technische en organisatorische voorbereiding en kennis vergt van de gebruiker van de software. Escrow is een vlag die momenteel nogal wat lading dekt. Die lading kan niet altijd waarmaken wat een gebruiker van een escrow verwacht, namelijk dat deze erop kan vertrouwen dat hij in noodgevallen de beschikking zal krijgen over de broncode, en dat hij er dan ook daadwerkelijk mee uit de voeten kan. Of een escrow-overeenkomst slechts een fopspeen of juist een uitkomst is, zal dan ook steeds inhoudelijk moeten worden getoetst. In dit artikel wordt ingegaan op de diverse aspecten van Nederlandse escrow-overeenkomsten.

## 2 Source code escrow: het kader

Binnen de automatiseringswereld is een groeiende aandacht te constateren voor de juridische aspecten van automatisering. De branche is in een fase gekomen waarin klanten mondiger en ter zake kundiger worden. Organisaties ontdekken dat "automatisering" niet een black box is, die met bedrijfskundige, juridische en economische instrumenten nauwelijks te beheersen is. Binnen veel bedrijven is het reeds ingeburgerd naast het algemeen bedrijfsbeleid een specifiek informatie- en automatiseringsplan op te stellen en daarbij eveneens aandacht te schenken aan de beveiligings- en continuïteitsaspecten van automatisering.

Source code escrow ofwel het depot van de broncode van software dient te worden gezien als een onderdeel van dat beveiligings- en continuïteitsbeleid en is als zodanig een onderwerp dat aandacht van het management verdient. Centraal bij "escrow" staat namelijk de continuïteit van de geautomatiseerde organisatie van de gebruiker van software, voor het geval de leverancier van die software met name zijn onderhoudsverplichtingen niet (meer) nakomt. Het is in veel gevallen (of zou in veel gevallen moeten zijn) een belangrijk onderwerp bij het opstellen van en onderhandelen over contracten bij automatiseringsprojecten.

## 3 Wat is escrow: probleemstelling

**De leverancier**
De broncode, te zamen met de technische documentatie, vormt de sleutel tot de know-how die door de programmeur in het programma is verwerkt, bijvoorbeeld in de vorm van speciale programmeeroplossingen. Het software-huis, dat zich de moeite van de investering in ervaring en onderzoek heeft moeten getroosten, geeft zijn know-how niet graag vrij aan anderen buiten de onderneming. Kopiëren van een computerprogramma

is immers eenvoudig en het gevaar van nabootsing is groot. Om deze reden geeft een software-huis meestal niet de broncode van een programma af, maar slechts de objectcode. Ook hiervan is het kopieergevaar groot, maar de verwerkte kennis is beter "afgeschermd" voor potentiële concurrenten.

Een tweede reden voor een software-huis om alleen de objectcode uit te leveren is het feit, dat met behulp van de sources en de documentatie de structuur van het programma begrepen en gewijzigd kan worden. Onderhoud en aanpassingen van software, hetzij om software-fouten te herstellen, hetzij om functionele aanpassingen of uitbreidingen uit te voeren op de software in verband met uitbreiding of aanpassing van het systeem of de organisatie van de gebruiker, vergt de beschikking over de broncode. Dit betekent derhalve een aardige klantenbinding en bron van inkomsten voor het software-huis.

**De gebruiker**
Deze laatste reden geeft ook direct het belang aan van de broncode voor de klant, de gebruiker van het computerprogramma. Indien een bedrijf in belangrijke mate geautomatiseerd is, of als strategische of essentiële bedrijfsprocessen zijn geautomatiseerd, is de continuïteit van het bedrijf in belangrijke mate verbonden met de continuïteit van de software. Een onderhoudsovereenkomst met de leverancier is dan ook vaak noodzakelijk. Wat echter indien de leverancier wanprestatie pleegt of niet meer in staat is aan zijn onderhoudsverplichtingen te voldoen? Faillissement van het software-huis is in de "snelle" wereld van de automatisering, waarin toetreden tot de markt met weinig middelen kan geschieden, helemaal niet ondenkbaar! Gebrekkig onderhoud of inflexibele software kan een geautomatiseerd bedrijf zich onmogelijk veroorloven. Een gebruiker zal dan ook voor die gevallen de beschikking over de broncode dienen te hebben, om zelf (of een derde) het onderhoud uit te (laten) voeren.

*Source code escrow ofwel het depot van de broncode van software dient te worden gezien als een onderdeel van het beveiligings- en continuïteitsbeleid.*

**Belangentegenstelling**
De belangentegenstelling tussen software-leverancier en software-gebruiker, geheimhouding van de source versus bedrijfscontinuïteit, is de reden voor het bedenken van escrow-constructies bij de aanschaf van software.

De gebruiker zal hierbij uiteraard een kosten/baten-afweging moeten maken. Gaat het om relatief goedkope standaardpakketten of gemakkelijk vervangbare programmatuur, dan is het eenvoudiger en goedkoper indien nodig nieuwe software aan te schaffen. Gaat het echter om dure standaard- dan wel unieke software, waarvan de klant niet de broncode en het auteursrecht heeft verkregen, dan dient hij escrow in serieuze overweging te nemen.

**Virussen**
Een bijkomende reden om tot deponering van de broncode van software over te gaan, welke niet direct met het onderhoud van de software te maken heeft, maar wel alles met de continuïteit van het geautomatiseerde systeem, is een bewijsrechtelijke. In toenemende mate worden gebruikers en leveranciers van software geconfronteerd met het verschijnsel "virus" in de software. De desastreuze gevolgen die dergelijke virussen mogelijk hebben, kunnen aanleiding zijn voor hoge schadeclaims van gebruikers jegens hun software-leveranciers.
Leveranciers zullen zich hiertegen willen indekken, onder andere door te bewijzen dat het virus niet van hen (via de door hen geleverde software) afkomstig is. Deponering van een "schone", verzegelde versie bij een derde, direct bij aanvang van het gebruik van de software, levert de software-leverancier een bruikbaar bewijsmiddel op. Bovendien is de leverancier nu steeds verzekerd van een "schone" versie voor het geval ook zijn systeem is aangetast.

## 4 Wat is escrow: definitie

De term "escrow" duidt op een soort bewaargevingsovereenkomst en is afkomstig uit het Anglo-Amerikaanse recht (voor het gemak wordt deze term hier gebruikt; in wezen bestaan er uitgebreide verschillen tussen het Amerikaanse en het Britse rechtsstelsel).
Escrow betekent daarin zoveel als: de overeenkomst waarbij een escrower (de bewaargever) akten, geld of goederen aan een escrowee (de bewaarnemer) ter bewaring overhandigt, die deze materialen slechts dan aan een escrow beneficiary (de begunstigde) zal uitleveren, als een bepaalde, van tevoren contractueel omschreven voorwaarde in vervulling is gegaan.

Bij een source code escrow is de software-leverancier degene die de te deponeren materialen overhandigt aan de escrowee. Deze bewaarnemer is bij voorkeur iemand die zich als escrow agent heeft gespecialiseerd in de uitvoering van zulke afspraken.

## 5 Escrow: juridische vorm

De vorm waarin een escrow-overeenkomst in ons Nederlandse rechtsstelsel kan worden gegoten, is divers. Er wordt onder andere gebruik gemaakt van de juridische vorm bewaargeving, maar ook van beheersconstructies, waarbij de escrow-agent een rechtspersoon (NV, BV, vereniging of stichting) is. Ten slotte wordt gebruik gemaakt van notarieel depot, dat wil zeggen het onderbrengen van de sources bij een notaris met behulp van een notariële akte. Deze vormen zullen hieronder aan de orde komen.

Escrow is geen eenvoudig produkt.
Een complicerende factor is bovendien vaak ook nog eens het feit dat veel van de in Nederland gebruikte software afkomstig is uit het buitenland. Degene van wie de gebruiker de software "koopt" (ofwel degene die een gebruiksrecht geeft) kan slechts een distributeur zijn van de werkelijke buitenlandse eigenaar. Zo kan er een hele keten van gebruiksrechten ontstaan, waarbij verschillende rechtsstelsels betrokken zijn.
Het juridisch juist structureren van een escrow wordt hierdoor nog ingewikkelder. In dit artikel wordt op deze buitenlandse factoren niet verder ingegaan. Het is voor een gebruiker in een dergelijke situatie raadzaam steeds deskundigen te raadplegen op het gebied van de betrokken rechtsstelsels.

## 6 Escrow: randvoorwaarden

Allereerst zal echter worden ingegaan op de randvoorwaarden voor escrow, waaraan aandacht moet worden besteed ongeacht de juridische constructie waarvoor wordt gekozen. Het betreft hier de persoon, kennis en verplichtingen van de bewaarder, de in bewaring te geven materialen en het up-to-date houden daarvan, en ten slotte de omschrijving van de uitleveringssituaties waaronder de gebruiker de broncode tot zijn beschikking zal krijgen en de situatie "after depot".

### De materialen

Allereerst moeten partijen goed afspreken wat er nu eigenlijk in bewaring moet worden gegeven en in welke vorm. Uiteraard moet dit de source code van de programmatuur zijn.
Daarnaast zal ook de volledige technische documentatie, voor zover niet opgenomen in de sources, gedeponeerd moeten worden. Indien er een specifieke compiler nodig is, die niet eenvoudig elders verkrijgbaar is of niet tegen redelijke kosten, zal ook deze bij het materiaal moeten worden gevoegd.
Ten slotte dient de vorm waarin de software gedeponeerd wordt - in listings of op andere informatiedragers - duidelijk te worden afgesproken. Daarbij moet worden opgemerkt, dat de listing van een uitgebreid software-pakket vaak een omvangrijke opslagcapaciteit zal vereisen.

Wil het depot van enig nut zijn voor de gebruiker, dan zal het dynamisch moeten zijn en voortdurend de actuele broncode moeten betreffen. Dit betekent dat de gedeponeerde materialen telkens na een uitgevoerde aanpassing, verbetering of vernieuwing vervangen dienen te worden door de leverancier.
Het vervangen van de broncode zal niet altijd gladjes gaan. Het kan zijn dat de bewaargevingsprocedure uiterst traag verloopt, bijvoorbeeld door allerlei tests. Hierdoor kan er een achterstand optreden. Het is bovendien niet ondenkbaar dat juist indien de leverancier in moeilijkheden raakt, hij aan de vernieuwing een lagere prioriteit gaat geven dan wenselijk is voor de gebruiker. Dit probleem is mogelijk één van de grootste praktische bedreigingen voor de werking van escrow in welke vorm dan ook! Een zorgvuldige contractuele regeling is zeker vereist.

### De bewaarder

Het in bewaring geven van materialen kan in principe gebeuren bij iedere derde die partijen daarvoor geschikt achten. In de praktijk wordt wel gekozen voor banken, advocaten, accountants of notarissen. Sinds een tijdje zijn er ook, net als in de Verenigde Staten, escrow-agents op de markt, die zich hebben gespecialiseerd in source code escrow. Het is met name voor de gebruiker van belang dat de bewaarder als persoon of instelling onafhankelijk en onpartijdig is, om tegenstrijdige belangen bij het uitvoeren en af-

handelen van de escrow zoveel mogelijk te voorkomen. De notaris is in ieder geval een persoon van wie men die kwaliteiten mag verwachten, en als zodanig een aantrekkelijk bewaarder.
Dit geldt ook ten aanzien van de eis van continuïteit, die aan de bewaarder gesteld moet worden. Het is voor de gebruiker belangrijk dat hij voor langere tijd op de escrow aan kan. Voor de opvolging van een notaris als publiekrechtelijk functionaris wordt altijd gezorgd, bij een escrow-bedrijf is dat meestal niet het geval!

Het bewaren van sources brengt nog een aantal specifieke problemen met zich mee. De materialen moeten op een zodanig veilige plaats kunnen worden bewaard, dat onbevoegden, zowel extern als intern, er geen kennis van kunnen nemen.
De bewaarder dient bovendien een zorgvuldige administratie te voeren, opdat hij de juiste source aan de juiste gebruiker kan uitleveren.
Vervolgens dienen de bewaringsfaciliteiten geschikt te zijn om de in bewaring gegeven materialen in bruikbare vorm te houden.

*Een enkele omschrijving als "De klant krijgt de beschikking over de broncode en de documentatie als de leverancier ophoudt met het uitvoeren van onderhoud" is te vaag en teveel omvattend.*

Als de software op magnetische gegevensdragers is vastgelegd, zal dit uiteraard andere eisen stellen aan de depotomgeving dan wanneer de programmatuur in listings is aangeleverd. Hier is al enig technisch inzicht vereist van de bewaarder, maar nog meer is dit van belang bij de eventuele controle en verificatie van de materialen. De gebruiker wil immers zeker weten dat datgene wat in bewaring wordt gegeven en hetgeen hij ontvangt bij uitlevering, exact die source code is, die hoort bij de objectcode van het programma zoals dat bij hem in gebruik is. Een afwijkende source is waardeloos voor hem. Als de gebruiker zelf een dergelijke test niet kan of mag doen, dient de bewaarder deze op verzoek te kunnen uitvoeren. Zeker geen eenvoudig karwei.
Veel bewaarders in Nederland kunnen of willen niet aan al deze eisen voldoen. De deskundigheid om technische tests uit te voeren zal bij velen ontbreken. Beschadiging of ontvreemding van de waardevolle source code zou tot hoge schadeclaims kunnen leiden. In veel escrow-overeenkomsten wordt dan ook iedere aansprakelijkheid van de bewaarder jegens leverancier of gebruiker ten aanzien van de aanwezigheid, juistheid en volledigheid van de broncode uitgesloten. De keuze van een bewaarder is gezien de hier besproken punten met name voor de gebruiker van groot belang en daarom voor hem een belangrijk punt van onderhandeling.

**Uitleveringsvoorwaarden**
De partijen bij escrow dienen goed af te spreken wanneer een gebruiker van de software precies de beschikking mag krijgen over de broncode, de zogenaamde "triggering events". Een enkele omschrijving als "de klant krijgt de beschikking over de broncode en de documentatie als de leverancier ophoudt met het uitvoeren van onderhoud" is te vaag en te veel omvattend. Stopzetting van onderhoud kan immers ook gebeuren doordat de relatie met de klant beëindigd wordt omdat de klant wanprestatie pleegt (contractuele afspraken niet nakomt).

Doelstelling bij de vaststelling van de uitleveringsvoorwaarden moet zijn: duidelijke, redelijke en haalbare voorwaarden, om vertragingen of onterechte uitlevering te voorkomen. Daarnaast dient er een geëigende vorm van geschillenbeslechting te zijn afgesproken, zodat onnodige vertraging kan worden voorkomen.

De uitleveringsvoorwaarden die in escrow-overeenkomsten voorkomen, hebben meestal betrekking op de volgende situaties:

a. De leverancier beëindigt de onderhoudsovereenkomst (zonder aanwijsbaar tekortschieten, bijvoorbeeld omdat hij een bepaalde versie niet langer wil ondersteunen).

b. De leverancier schiet aanwijsbaar tekort in de uitvoering van de onderhoudsovereenkomst.

c. De leverancier gaat failliet of dreigt failliet te gaan.

d. Er is sprake van overmacht bij de leverancier.

Situatie c, het faillissement van de leverancier, kan in de praktijk tot de grootste problemen leiden. Met name zal niet altijd duidelijk zijn of uitlevering wel haalbaar is. De curator die zorgt voor de afwikkeling van het faillissement van de leverancier, zal in sommige gevallen de uitlevering willen verhinderen. Aan situatie c zal hierna dan ook de meeste aandacht worden besteed.

**"After depot"**
Het is al even kort aangegeven: een deugdelijke juridische constructie is weliswaar conditio sine qua non voor escrow, van even zo groot belang is het dat de gebruiker van tevoren aandacht besteedt aan de technische en praktische kant van de zaak. Wat kan een gebruiker immers met de sources van de software, als hij ze eenmaal rechtsgeldig in handen heeft gekregen? Hij zal van tevoren degelijk nagedacht moeten hebben over de vraag of hij zelf het onderhoud kan plegen, of dat hij hiervoor een derde moet inschakelen. En welke derde moet dit dan zijn? En kan die derde ook daadwerkelijk dat onderhoud op zich nemen, als de sources bij hem op tafel worden gelegd? Met andere woorden, is het programma qua structuur wel onderhoudbaar, of is het spaghetti? Vaak is het bovendien ook nog maar de vraag of de technische documentatie wel goed is bijgehouden.

*Een deugdelijke juridische constructie is weliswaar conditio sine qua non voor escrow, van even groot belang is het dat de gebruiker van tevoren aandacht besteedt aan de technische en praktische kant van de zaak.*

Men zou er natuurlijk op kunnen vertrouwen dat als de nood aan de man komt er wel één of twee programmeurs van de software-leverancier kunnen worden "weggekocht", maar dat mag een bedenkelijk uitgangspunt voor continuïteitsbeleid worden genoemd. Het moge duidelijk zijn hoe belangrijk het is een juiste afweging te maken bij het aangaan van een broncodedepot, niet alleen juridisch maar ook praktisch.

## 7 Rechten ten aanzien van de broncode

Tussen leverancier en gebruiker van de software moet geregeld worden welke rechten de gebruiker krijgt op de in bewaring te geven materialen. Onderscheid dient te worden gemaakt tussen de eigendomsrechten op de dragers van de software (de tapes of diskettes of het papier) en de auteursrechten die rusten op de software zelf.

**Eigendomsrecht**
De source code van software is op zich niets anders dan informatie. Zij moet dan ook worden vastgelegd op een drager, al dan niet magnetisch, om te kunnen worden gebruikt en ook om in bewaring te kunnen worden gegeven. Die dragers kunnen in eigendom toebehoren aan ofwel de leverancier of de gebruiker van de software, of wel de escrow-agent.

**Auteursrecht**
Op de door de software-leverancier ontwikkelde software rust in het algemeen, zo wordt aangenomen, het auteursrecht van die leverancier, ook al wordt software nog niet met zoveel woorden genoemd in onze Auteurswet 1912. Ook op de bijbehorende documentatie is in de regel het auteursrecht van toepassing.

Als een gebruiker software aanschaft krijgt hij van de leverancier over het algemeen alleen een (beperkt) gebruiksrecht op die software, een zogenaamde licentie. Hij krijgt daarmee niet het (op het eigendomsrecht lijkende) auteursrecht. Dit is zelfs het geval indien de software in zijn opdracht is ontwikkeld, en er geen nadere afspraken zijn gemaakt omtrent het auteursrecht. Het is dus meestal aan de software-leverancier om te bepalen wat de gebruiker wel en niet mag doen met zijn software. Ook bij escrow krijgt de gebruiker vaak alleen een licentie om de sources in de toekomst te gaan gebruiken, niet het volledige auteursrecht.

## 8 Escrow: bewaargeving

Na de behandeling van de algemene zaken rondom een escrow-overeenkomst wordt nu ingegaan op enkele vormen waarin een escrow kan worden gegoten. Overigens moeten hierna voor "source code" ook steeds de bijbehorende documentatie en overige in escrow gegeven materialen gelezen worden.
Allereerst de gewone bewaargeving.

Zoals reeds eerder aangegeven, komt het in bewaring geven van de broncode neer op het bij een onafhankelijke persoon in bewaring geven van de dragers waarop de broncode is vastgelegd. Ten behoeve van de gebruiker wordt een licentie opgenomen, waarbij hij het recht verkrijgt na uitlevering zijn software en de daarbij behorende documentatie te (laten) onderhouden en aan te passen.
Bewaargeving wordt geregeld in het Burgerlijk Wetboek, de artikelen 1731 en volgende. Een bewaarder moet volgens de wet zorgvuldig met de in bewaring gegeven goederen omgaan, zeker indien hij (zoals bij escrow gebruikelijk is) voor zijn inspanningen wordt betaald.

**Problemen**
Indien de leverancier failliet gaat, kan zich bij bewaargeving een aantal problemen voordoen. De bewaargevingsovereenkomst zal in principe bij een faillissement gewoon blijven bestaan. Vraagt de bewaarder of de gebruiker echter aan de curator of hij de overeenkomst wil nakomen, dan kan deze besluiten om dat niet te doen, als dat gunstig is voor de failliete boedel. Dat kan bijvoorbeeld zo zijn als de curator de source code wil verkopen. De dragers vallen immers in het faillissement van de leverancier, en het auteursrecht kan in de meeste gevallen wel te gelde worden gemaakt.
Maar eigenlijk hoeft niet de curator de escrow-overeenkomst meer na te komen, maar de bewaarder. De curator hoeft alleen nog maar te "dulden". Slimme bewaarders en gebruikers vragen dan ook niet of de curator de overeenkomst wil nakomen.

Wat de curator echter nog wel kan doen, is het opvorderen van de dragers waarop de software is vastgelegd en die afkomstig zijn van de leverancier. Escrow-overeenkomst of niet, die dragers behoren tot de failliete boedel en mogen daarom verkocht worden aan de hoogste bieder. Ook dan hoeft er nog geen man overboord te zijn voor de gebruiker van de software, indien de derde die de software koopt ook de onderhoudsverplichtingen mee overneemt.
Dat zal in de meeste gevallen wel gebeuren, omdat het onderhoud immers een bron van inkomsten is. Het gaat hier echter om persoonlijke verplichtingen, afgesproken tussen de failliete leverancier en de gebruiker. De derde is nooit verplicht die ook over te nemen!

Stel echter, dat de slimme bewaarder en gebruiker er bij aanvang van de escrow voor hebben gezorgd dat de dragers waarop de sources vastliggen, niet meer in eigendom toebehoren aan de leverancier. Gevolg: de dragers behoren niet tot het vermogen van de failliete leverancier. De curator kan ze dan in de meeste gevallen niet opvorderen en verkopen! De gebruiker krijgt gewoon zijn sources van de bewaarder. Ook dan kan zich helaas nog een zelfde probleem voordoen als hierboven vermeld: is de derde die de software koopt uit de failliete boedel wel gebonden aan de rechten die de vorige eigenaar heeft gegeven in het kader van de escrow?
Volgens het huidige recht is het nog niet zeker of degene die het auteursrecht overneemt, ook gehouden is al uitgegeven licenties te erkennen.
Een soortgelijke situatie, die overigens wel door de wetgever geregeld is, doet zich voor wanneer iemand een huis koopt dat verhuurd is. Zoiets als "huurbescherming" voor software-gebruikers bestaat echter (nog) niet.

**Schadevergoeding**
Gaat het fout met de escrow en krijgt de gebruiker zijn sources niet, dan heeft hij nog wel steeds het recht om een vordering in te dienen in het faillissement van de leverancier. Hij lijdt immers schade doordat de overeenkomst niet is nagekomen. Maar van een kale kip is het slecht plukken. Bovendien gaat het de gebruiker in eerste instantie niet om een geldelijke vergoeding, maar juist om de broncode!

Samenvattend moet van de bewaargeving gezegd worden, dat de gebruiker op zijn qui-vive dient te zijn. Het gaat vaak om wankele constructies, waarbij de nodige twijfel bestaat of de gebruiker voldoende mag vertrouwen op de goede werking van de escrow. Een belangrijke verbetering is het al, indien de dragers van de source code direct bij aanvang van de escrow al in eigendom worden overgedragen aan de gebruiker of de bewaarder. Het probleem blijft echter dat de rechten die de gebruiker krijgt op de source code alleen maar persoonlijke rechten jegens de software-leverancier zijn. Een derde is daar in de meeste gevallen niet aan gebonden. Dit kan eigenlijk alleen worden opgelost, indien ook het auteursrecht al bij aanvang van de escrow wordt overgedragen aan de gebruiker. Voor de leverancier zal dit echter meestal onbespreekbaar zijn. Bovendien zou een escrow dan in principe ook niet meer nodig zijn!

Overigens kan een curator, ook als hij besluit de afgifte van de source code te frustreren, nog besluiten de onderhoudswerkzaamheden van de failliet voort te zetten. Inkomsten uit onderhoud kunnen immers een belangrijk deel van de omzet van software-huizen uitmaken, zodat zo'n voortzetting nog wel lucratief kan zijn. In dat geval is er voor de klant ook nog geen directe reden de source code in handen te krijgen; het onderhoud aan zijn software zal dan immers worden gecontinueerd.

## 9 Escrow: notarieel depot

De volgende te behandelen juridische constructie is het depot van de broncode bij de notaris.
Een belangrijke reden voor de keuze voor de notaris als bewaarder van de broncode is voor veel partijen het aanzien dat de notaris geniet als vertrouwensman. Daarnaast worden er in de Wet op het Notarisambt eisen gesteld aan de uitoefening van het ambt van notaris. De akten die de notaris opmaakt, hebben volledige bewijskracht. De notaris heeft ook de verplichting van "titelonderzoek", ofwel hij moet kijken of de leverancier ook werkelijk het recht heeft de broncode in escrow te geven en erover te beschikken[1]. De notaris is vervolgens verplicht iedere akte die onder hem berust te bewaren. Hij mag ze niet uit handen geven, bijvoorbeeld aan de curator van de software-leverancier. Notariële akten zijn als het ware onttrokken aan het rechtsverkeer. Wel moet hij aan iedere belanghebbende bij de akte op verzoek een afschrift verstrekken.
Ten slotte is de continuïteit van de notaris als escrow-agent in belangrijke mate gewaarborgd, omdat er altijd een opvolger voor zijn taak zal worden aangewezen.

**Notarieel sausje?**
De gang naar de notaris geeft de afspraak tussen leverancier en gebruiker een "officiële tint", wat de door hen beoogde werking van de escrow lijkt te kunnen waarborgen. Ook hier is echter oplettendheid nodig ten aanzien van de gekozen juridische vorm! Als de broncode bij de notaris als *private persoon* in bewaring wordt gegeven, eventueel bezegeld met een notariële akte van overeenkomst, dan gaat het in wezen om een gewone bewaargeving met een notarieel sausje. De beperkingen zoals hierboven werden beschreven, gelden dan ook hier.

Een minder waterdoorlatende constructie is echter het *depot voor minuut* van de broncode. Artikel 40 van de Wet op het Notarisambt spreekt van akten die zijn neergelegd als minuut en van akten die aan andere akten zijn vastgehecht. Het gaat dan om akten die niet door de notaris zelf zijn opgemaakt. Uitgaande van de veronderstelling dat het begrip "akten" zo ruim mag worden uitgelegd, dat hieronder ook de broncode van de software kan vallen, kan de broncode dus gedeponeerd worden als een minuutakte, aangehecht aan een akte van depot, die de notaris opstelt ten behoeve van partijen. De veronderstelde ruime uitleg van het begrip "akte" is in notarisland echter nogal omstreden!

Aangenomen dat zo'n depot mogelijk is (en in de praktijk gebeurt het ook al), dan gelden de hierboven genoemde voordelen van het notarieel depot. Met name de onttrekking aan het rechtsverkeer is van groot belang: de curator in het faillissement van de leverancier kan de akte (ofwel de broncode) immers niet terugvorderen! De gebruiker daarentegen is verzekerd van een afschrift van de broncode, mits hij in de begeleidende akte als begunstigde is aangemerkt.

**Problemen**
De hier genoemde constructie is echter niet gemakkelijk voor de notaris. Oorzaak hiervan zijn enkele bepalingen uit de Wet op het Notarisambt. Zo dienen akten op "deugdelijk materiaal" te zijn vastgelegd. De drager van de broncode mag dus niet al te kwetsbaar zijn, een probleem dat vooral speelt bij magnetische dragers. Daarnaast stelt de wet dat de notaris zijn akten verplicht dertig jaren onder zich moet houden. Aangezien het depot van aangepaste software regelmatig moet geschieden om de broncode actueel te houden, kan dit de notaris voor opslagproblemen stellen. Dit geldt zeker als de sources in de vorm van listings worden gedeponeerd!

De notaris dient zijn akten ook op een adequate en veilige plaats te bewaren. Depot van magnetische dragers stelt hem, in dit licht gezien, eveneens voor een opslagprobleem.

De notaris moet vervolgens in staat zijn een afschrift van de broncode te maken. Weer een probleem voor de notaris, dat met name speelt bij het depot van magnetische dragers!

Ten slotte vereist de wet dat de akten worden aangehecht aan een notariële akte van depot. Voorkomen moet uiter-

1 In de praktijk is overigens gebleken dat men van dit titelonderzoek niet te veel mag verwachten. Het is voor de notaris moeilijk te achterhalen wie de rechten op de sources nu werkelijk heeft. Complicerend is vaak het feit dat rechthebbende een buitenlands bedrijf is, of dat de rechten in een aparte rechtspersoon zijn ondergebracht. Ook is het vaak niet duidelijk of het auteursrecht op bepaalde stukken van de programmatuur bij anderen dan de leverancier berust.

aard worden dat de notaris hiervoor een traditioneel nietje gebruikt! Menig notaris zal dit tegenwoordig wel inzien, en andere oplossingen bedenken, bijvoorbeeld een verzegelde envelop waarin de dragers worden bewaard.

Duidelijk zal zijn dat het notarieel depot nogal omgeven is met praktische en interpretatieproblemen. Velen zijn van mening dat de bepalingen van de Wet op het Notarisambt te veel moeten worden opgerekt voor deze vorm van zekerheidsverschaffing. Menig notaris is dan ook nog huiverig deze vorm van depot toe te passen, zeker als hij niet over de nodige technische kennis ter zake beschikt.

Ondanks de bezwaren lijkt het depot voor minuut echter een aantrekkelijke vorm van escrow voor zowel gebruiker als leverancier, niet in de laatste plaats omdat de taakuitoefening van de notaris wettelijk is omschreven. Een relativerende opmerking is echter op zijn plaats. Als de gebruiker een afschrift heeft verkregen van de akte, met andere woorden een kopie van de broncode (en de documentatie), zal hij hiervan gebruik willen maken. Voor dit geval moet de gebruiker een gebruiksrecht voor het uitvoeren van onderhoud hebben gekregen. Het betreft hier weer een persoonlijk recht, waarvoor dezelfde bezwaren gelden als genoemd zijn bij de gewone bewaargeving. Al met al geldt ook weer ten aanzien van de notariële deponering: bezint eer ge begint!

*Al met al klinkt de trust-constructie ideaal voor het depot van de source code van software. Helaas is het echter naar Nederlands recht niet mogelijk een dergelijke trust te vestigen.*

## 10 Broncode depot: het beheer

Een laatste vorm van depot van de broncode die hier zal worden behandeld, is het beheer van de broncode door middel van een beheersconstructie. Model hiervoor staat de trust-figuur uit het Anglo-Amerikaanse recht. De trust is het centrale leerstuk uit het deel van het Anglo-Amerikaanse recht dat Equity wordt genoemd en dat te onderscheiden is van de Common law. Met name het naast elkaar bestaan van deze twee rechtsgebieden onderscheidt het Anglo-Amerikaanse recht van het continentale rechtsstelsel waaronder ook het Nederlandse valt.

**Dual ownership**
Kenmerkend voor de trust is het zogenaamde dual ownership ofwel een gesplitst eigendom.
Trustproperty wordt in beheer gegeven aan een trustee (de beheerder) die als "eigenaar" naar common law wordt aangemerkt. De begunstigden bij de beheersconstructie, de beneficiaries, zijn eigenaar volgens equity. Het ownership naar dit recht is van een geheel andere orde dan ons begrip "eigendom"! Belangrijk is dat de trustproperty (dat zou in casu de broncode en de documentatie, alsmede de rechten daarop omvatten) een soort "afgescheiden vermogen" vormt van het eigen vermogen van de trustee-beheerder. Dit houdt dan grofweg in dat de beneficiaries (de gebruikers-begunstigden) sterkere rechten op de sources kunnen uitoefenen dan de crediteuren van de trustee-beheerder.

**Nederlandse vertaling**
Al met al klinkt de trust-constructie ideaal voor het depot van de source code van software. Helaas is het echter naar Nederlands recht niet mogelijk een dergelijke trust te vestigen. Wij kennen geen echt gesplitst eigendom. De uitgebreide rechten zoals die toekomen aan de gebruikers-beneficiaries kent ons recht niet. Juridisch gezien betekent dit dat de trust "vertaald" moet worden naar het Nederlandse recht.
Consequentie hiervan is dat de rechten van de gebruikers-beneficiaries naar Nederlands recht weer alleen maar persoonlijke rechten zijn, die niet tegenover derden gelden. Ook mogen de schuldeisers van de trustee-beheerder in Nederland zich weer verhalen op de goederen die hij in beheer heeft. Kortom, voor de gebruiker een aanzienlijk minder goede constructie dan het Anglo-Amerikaanse equivalent.
Toch zijn er wel mogelijkheden om deze vorm aan te passen aan de wensen van de partijen bij een escrow-overeenkomst. Zo kan men een aparte rechtspersoon oprichten (NV, BV, vereniging of stichting), waarin de eigendomsrechten op de source code worden ondergebracht. Het beste kan daarvoor een stichting worden gebruikt, met strikt omschreven doelstelling en statuten. Het feitelijke beheer kan gebeuren door een afzonderlijke beheerder, bijvoorbeeld een notaris. Hoewel de gebruikers-beneficiaries nu nog steeds alleen maar een persoonlijk recht op het trust-goed of op een kopie daarvan hebben, zal hun recht toch op deze wijze veel minder snel doorkruist kunnen wor-

den door schuldeisers. Die zullen er namelijk door de beperkte taak en doelomschrijving van de trustee-rechtspersoon niet of nauwelijks zijn.
Deze constructie is zowel goed toe te passen als er maar één gebruiker is als wanneer er meerdere gebruikers zijn. Al met al een aardige mogelijkheid, die zeker het overwegen waard is.

## 11 Interpretable programma's en escrow

Al eerder werd beschreven onder welke voorwaarden escrow in overweging zou moeten worden genomen. Uitzonderingen zijn echter ook mogelijk, zoals het volgende praktijkgeval laat zien.

Een bedrijf overwoog bij de aanschaf van een omvangrijk en voor de bedrijfsvoering essentieel standaardpakket-met-aanpassingen de opname van een escrow-clausule in het contract.
Nader overleg wees uit dat de programmatuur geschreven was in een basic-taal en met behulp van een interpreter door de computer werd uitgevoerd. Vanwege deze werkwijze werden de sources door de leverancier geleverd in plaats van een versie in objectcode. Gevolg: een daadwerkelijke escrow was niet nodig, de sources waren immers reeds beschikbaar bij de gebruiker. Er behoefde alleen, en dat is in dergelijke gevallen overigens wél essentieel, een regeling te worden getroffen voor gebruik van de sources voor onderhoud en aanpassing in geval van faillissement en/of het staken van het onderhoud door de leverancier[2].

*Er wordt wel gezegd dat het Nederlandse recht eigenlijk het Amerikaanse beginsel van "fair use" zou moeten kennen, waarmee de rechter de mogelijkheid krijgt "redelijk gebruik" te onderscheiden van "misbruik" van auteursrechtelijk beschermde werken.*

## 12 Maakt reverse engineering escrow overbodig?

Men krijgt de neiging om voor een zo ingewikkeld en omvangrijk produkt als een escrow naarstig op zoek te gaan naar alternatieven. Zo wordt momenteel reverse engineering wel als vervanger geopperd voor escrow. Een originele gedachte, maar helaas met de nodige haken en ogen.
Reverse engineering of wel het onderzoeken van de objectcode van programmatuur om de achterliggende structuur te achterhalen is een term waaronder vele handelingen kunnen vallen. In het kader van dit artikel wordt met reverse engineering bedoeld: het decompileren van de objectcode en in combinatie met het testen van de werking van de software op deze wijze verkrijgen van een zo compleet mogelijke geordende specificatie aan de hand waarvan een inhoudelijk gelijkluidend programma zou kunnen worden gebouwd[3].

Twee vragen zijn er in dit kader interessant:
Mag reverse engineering volgens ons auteursrecht, en zo ja, is er werkelijk sprake van een alternatief voor escrow?

De eerste vraag staat momenteel ook internationaal in de belangstelling, nu er een EG-richtlijn op stapel staat met betrekking tot auteursrechtelijke softwarebescherming. Naar huidig Nederlands recht is het nog onduidelijk of reverse engineering is toegestaan. De specifieke kanten van software-bescherming worden nog niet beschreven door onze Auteurswet 1912. Interpretatie van de wet levert argumenten op voor zowel voorals tegenstanders. Voorstanders bepleiten overigens dat het in bepaalde gevallen onredelijk zou zijn als reverse engineering niet zou mogen. Te denken valt dan met name aan gebruikersbelangen, zoals onderhoud of renovatie van verouderde, slecht gedocumenteerde systemen. In dit kader wordt wel gezegd dat het Nederlandse recht eigenlijk het Amerikaanse beginsel van "fair use" zou moeten kennen, waarmee de rechter de mogelijkheid krijgt "redelijk gebruik" te onderscheiden van "misbruik" van auteursrechtelijk beschermde werken.
Het lijkt erop dat de Europese richtlijn, onder andere onder druk van lobbyende software-leveranciers van compatible software en van grootgebruikers, gedeeltelijk een dergelijk beginsel zal gaan bevatten. Het ontwerp staat de legale bezitter van software toe een programma te analyseren, zonder dat het programma daarbij gekopieerd wordt. Als het voor de gebruiker "absoluut noodzakelijk is voor het onderhoud en de opstelling en ge-

2 NB: Hier dient wel verwezen te worden naar de mogelijke consequenties van faillissement voor deze rechten, zoals beschreven in paragraaf 8.

3 Definitie van J.E. Dommering, *Reverse engineering: een softwarepuzzel*, Computerrecht 1990/3.

bruik van compatible computerprogramma's", mag hij onder voorwaarden ook kopiëren en zelfs bewerken, zonder toestemming van de auteursrechthebbende. Indien de huidige ontwerp-richtlijn in 1991 wordt overgenomen, is reverse engineering ten behoeve van onderhoud van programmatuur dus ook zonder daadwerkelijke toestemming van de auteursrechthebbende - zij het onder voorwaarden - mogelijk binnen Europa[4].

**Kennis, tijd, geld**

Betekent dit nu het einde van escrow? Dat mag betwijfeld worden. Reverse engineering heeft nadelen vergelijkbaar met die van escrow.

Weliswaar behoeven de sources niet reeds in een vroeg stadium gedeponeerd te worden bij een derde met alle kosten van dien. Maar voor het overige blijven ook bij reverse engineering de knelpunten: kennis, tijd en geld.

Reverse engineering is een tijdrovende bezigheid, waarvoor veel deskundigheid vereist is. De uitkomst van het reverse engineeren van de load-module van de gebruiker zal bovendien nooit de originele, volledige broncode zijn. Belangrijke toevoegingen aan de source, het commentaar en de naamgeving van functies en variabelen, ontbreken. Dit betekent dat de structuur van het programma onbekend blijft. Essentieel voor het uitvoeren van onderhoud is verder bovenal het hebben van de volledige technische documentatie. Die is echter nu niet beschikbaar! Waarlijk een hels en daardoor kostbaar karwei om met een reverse engineered objectcode onderhoud te plegen!

Het mag worden betwijfeld of de kosten hiervan opwegen tegen een juridisch, technisch en organisatorisch goed geregelde escrow. Reverse engineering zal mogelijk wel een goede aanvulling kunnen zijn van een escrow, bijvoorbeeld als de gedeponeerde source niet geheel up-to-date of onvolledig is.

4 Een relativerende opmerking: de ontwerp-richtlijn bevat omtrent het recht van reverse engineering tevens de clausule 'tenzij contractueel anders is bepaald'. Volgens de CIAD, de Europese gebruikersvereniging, zal dit mogelijk betekenen, dat leveranciers dit standaard in hun contracten zullen opnemen. Met andere woorden: terug naar af. Elders in deze Compact gaat mr. V.A. de Pous nader in op software-bescherming en de Europese richtlijn.

## 13 De markt van deponering: enkele voorbeelden

Na de juridische en technische theorie zal nu worden ingegaan op de praktijk: de ontwikkelingen die zich inmiddels op de escrow-markt hebben voorgedaan. Met het in de belangstelling komen van escrow, zijn verschillende beroepsgroepen zich gaan bezighouden met de problematiek.

Van verscheidene kanten is inmiddels reeds een beroep op het notariaat gedaan om zich meer als escrow-agent beschikbaar te stellen, onder meer door de Raad van de Centrale Ondernemingsorganisaties en de COSSO. Tot nu toe heeft het notariaat zich echter nogal afwijzend opgesteld in escrow-zaken, met name vanwege de hierboven al genoemde obstructies in de Wet op het Notarisambt. Inmiddels gaan er echter wel stemmen op vanuit het notariaat om een onafhankelijke escrow-beheersstichting op te zetten, die dienst kan doen voor het gehele notariaat. Een enkele vooruitstrevende notaris experimenteert bovendien met het depot voor minuut.

Ook diverse advocatenkantoren hebben niet stilgezeten en zich, zij het nog schoorvoetend, geworpen op de escrow. In korte tijd zijn er bovendien enkele professionele aanbieders van escrow-diensten, escrow-agents, op de markt verschenen. Dit zijn het Computer Uitwijk Centrum te Lelystad en Escrow Europe te Maarssen. Binnenkort wil ook het Engelse NCC (National Computing Centre) zijn diensten gaan aanbieden op de Nederlandse markt, door middel van bewaargeving volgens Brits recht.

Dat de escrow-markt nog onzeker en moeilijk benaderbaar is moge blijken uit het feit dat er inmiddels ook al weer een aanbieder ter ziele is, Escrow Trust & Security International. Deze agent bood als één van de eersten "full service". Dat wil zeggen: een gebruiker kon ieder onderdeel van een escrow afnemen, van verschillende depotmogelijkheden tot aan verificatie en "after depot service" (het daadwerkelijk voor de gebruiker uitvoeren van het onderhoud). Meer zekerheid voor de gebruiker dus dat hij ook daadwerkelijk iets had aan de escrow. Uiteraard hing aan dit ingewikkelde samenstel van diensten ook een prijskaartje, dat kennelijk nog te duur was voor potentiële escrow-klanten. Een bescheiden prijskaartje zal voor het hierboven

genoemde Engelse NCC dan ook de belangrijkste troef worden in de slag om de escrow-klant.

**Computer Uitwijk Centrum**
Per 1 oktober 1989 is in Lelystad het CUC van start gegaan met het aanbieden van escrow-diensten. Deze kunnen zowel passief als actief zijn. Volgens het CUC is escrow steeds maatwerk, en het escrow-contract is dan ook modulair van opbouw. Afhankelijk van de uiteindelijke contractueel bepaalde dienstverlening varieert ook de prijs van het depot.

*Juridisch blijft het probleem bij escrow dat nog geen enkele constructie bij de rechter is uitgetest op duurzaamheid. Aangezien dit ook niet direct in het belang is van de aanbieders, zal een dergelijk "proefproces" nog wel op zich laten wachten.*

De basis voor het contract vormt de bewaargeving. De dragers waarop de source code is vastgelegd, worden echter wel in eigendom overgedragen aan het CUC. Ze zullen dus niet in het faillissement van de leverancier noch in dat van de gebruiker vallen. De gebruiker (afhankelijk van het soort contract partij of derde bij de overeenkomst) krijgt bij uitlevering van de sources een gebruiksrecht. De triggering events zijn grondig omschreven.

De gebruikers en de leverancier hebben het recht jaarlijks de gang van zaken bij het CUC te controleren. Daarnaast verplicht het CUC zich jaarlijks bij de gebruiker en de leverancier na te gaan of het depot nog wel up-to-date is.
Ook kan controle worden uitgeoefend op de juistheid en volledigheid van de software. Standaard is dat een checklist wordt afgewerkt, waarop onder andere de omvang van de files wordt aangegeven (controle op aantal en omvang van de records van het programma), alsmede de aanwezige documentatie. Gekeken wordt ook naar de bruikbaarheid van de dragers van de sources en documentatie. Wil men echter volledige zekerheid omtrent de juistheid en volledigheid van de sources, dan kunnen uitgebreide technische tests worden aangeboden, uiteraard tegen meerprijs.
De standaardovereenkomst van het CUC (één gebruiker, één leverancier) kost ƒ7.000 entrance fee en ƒ1.500 jaarlijks, exclusief BTW. Uitbreiding van de modulaire overeenkomst brengt extra kosten met zich mee. Wel inbegrepen in de standaardsituatie zijn onder andere het maken van de overeenkomst, juridisch advies, twee keer per jaar een updatemogelijkheid en de afwikkeling van de afgifte van het gedeponeerde.

**Escrow Europe**
Ook sinds vorig jaar biedt Escrow Europe escrow-diensten aan. Gebruikers en leveranciers kunnen ook hier weer kiezen voor enkel een passief depot of ook voor actieve escrow-dienstverlening. De basis is een gewone bewaargevingsovereenkomst, maar er kan daarnaast aandacht worden besteed aan wat het bedrijf noemt "programmatuur consultancy" en aan uitwijk- en backup-services. Hiervoor is samenwerking gezocht met enkele bedrijven in de automatiseringsbranche. Een nieuwe en originele dienst is een speciaal ontworpen software-escrow-verzekeringspolis. Deze polis moet de gebruiker die geen eigen automatiseringsafdeling bezit of onvoldoende kennis in huis heeft, verzekeren van het ook daadwerkelijk kunnen gebruiken van de source code indien deze uit de escrow is verkregen. De broncode (en de documentatie) wordt dan aan technische tests onderworpen, waarbij de onderhoudbaarheid van de structuur wordt beoordeeld. Aan de hand hiervan wordt de premie bepaald.
Ten aanzien van de escrow-activiteiten kan, eveneens in verband met de modulaire structuur, hier slechts een indicatie worden gegeven. Standaard passieve software-escrow (= louter deponeren) kost de leverancier een eenmalig bedrag van ƒ5.000. Hiervoor mag drie keer per jaar het depot worden vernieuwd. De gebruiker betaalt vervolgens een bepaald jaarlijks bedrag, afhankelijk van de hoogte van de licentieprijs, de looptijd van het licentiecontract en het aantal gebruikers. Voor het testen van de programmatuur rekent Escrow Europe een uurtarief.

## 14 Conclusie

De standaard-escrow-diensten van de respectievelijke aanbieders zullen elkaar in prijs en prestatie niet veel ontlopen, zij het dat sommige juridische constructies vertrouwenwekkender lijken dan andere. Wat de komst van het Engelse NCC op de markt voor invloed zal hebben, moet nog worden afgewacht.
Juridisch blijft het probleem bij escrow echter, dat nog geen enkele constructie bij de rechter is uitgetest op duurzaamheid. Aangezien dit ook niet direct in het belang is van de aanbieders, zal een dergelijk "proefproces" nog wel op zich laten wachten.
Een deugdelijke juridische constructie is

weliswaar onmisbaar voor escrow, van even zo groot belang is het dat de gebruiker aandacht besteedt aan de technische en praktische kant van de zaak. Hij zal zich van tevoren degelijk bedacht moeten hebben of hij zelf onderhoud kan plegen, of dat hij hiervoor een derde moet inschakelen.
Die derde zou ook de escrow-agent kunnen zijn. Hoe het prijsverschil tussen de escrow-agenten ligt indien men de respectievelijke kale escrow-overeenkomsten gaat optuigen met aanvullende actieve diensten, is onduidelijk. De prijs/prestatie-verhouding moet in dat geval uiteraard worden meegewogen.

*Mw. mr. A.M.Ch. Kemna MBA*
*Is werkzaam bij KPMG Klynveld EDP Audit. Zij heeft rechten gestudeerd aan de Katholieke Universiteit Nijmegen en post-doctoraal bedrijfskunde (MBA) aan de Rotterdam School of Management, Erasmus Universiteit Rotterdam. Tot haar werkzaamheden behoort het onderzoeken van de relatie tussen de kwaliteit van de automatisering en het recht. Haar specifieke aandachtsgebieden zijn de beoordeling en begeleiding van computercontracten, de juridische aspecten van netwerken en de consequenties van de Wet Persoonsregistraties. Op dit laatste vlak heeft zij een bijdrage geleverd aan NIVRA-geschrift 58 inzake privacybescherming en de rol van de accountant. Anne-Marie Kemna heeft gepubliceerd en gedoceerd omtrent escrow.*

**Op 16 mei 1990 heeft de minister van Justitie aan de Tweede Kamer der Staten-Generaal het wetsontwerp Computercriminaliteit aangeboden. In dit artikel wordt ingegaan op het verschijnsel computermisbruik, worden de wetsvoorstellen geanalyseerd en wordt een overzicht gegeven van de consequenties van het wetsvoorstel voor het Nederlandse bedrijfsleven en de overheid.**

R.A. s'Jacob

# Een analyse van het wetsvoorstel Computercriminaliteit

## 1 Inleiding

De voortschrijdende ontwikkelingen van de informatietechnologie hebben de vraag doen rijzen of het huidige strafrecht nog toereikend is om bescherming te bieden tegen nieuwe vormen van misbruik van deze informatietechnologie. In 1985 deed de Organisatie voor Europese Samenwerking en Ontwikkeling (OESO) een aanbeveling waarin de lidstaten (waaronder Nederland) in overweging werd gegeven een aantal nader omschreven vormen van computermisbruik strafbaar te stellen. In het kader van de Raad van Europa is het werk van de OESO voortgezet.

In november 1985 gaf de toenmalige minister van Justitie een commissie opdracht een onderzoek in te stellen naar de toereikendheid van het strafrecht op het gebied van informatietechnologie. In april 1987 bracht deze commissie (naar haar voorzitter de "Commissie Franken" genoemd) haar eindrapport uit. Dit rapport heeft in diverse kringen, van juristen tot en met deskundigen op het gebied van automatisering en controle, vele reacties opgeroepen. Nu, ruim drie jaar later en nadat vele discussies hebben plaatsgevonden, heeft de minister van Justitie Hirsch Ballin aan de Tweede Kamer der Staten-Generaal het wetsontwerp Computercriminaliteit aangeboden waarbij het rapport van de Commissie Franken en de daaropvolgende discussies als uitgangspunt hebben gediend.

Alvorens de consequenties van het wetsontwerp worden weergegeven, wordt in dit artikel ingegaan op het verschijnsel computermisbruik en worden de voorgestelde (wijzigingen van) wetsartikelen geanalyseerd.

## 2 Het verschijnsel computer criminaliteit

Voor het begrip computercriminaliteit zijn in de literatuur verschillende definities te vinden. In het kader van dit artikel wordt computermisbruik gedefinieerd als:

*Het gedrag met een voor anderen (potentieel) schadelijk karakter waarbij geautomatiseerde systemen ter opslag, verwerking of uitwisseling van gegevens zijn betrokken.*

Geautomatiseerde systemen kunnen op tweeërlei wijze betrokken zijn bij (potentieel) schadelijk gedrag. Ten eerste kan het systeem object van gedraging zijn. Zulke handelingen hoeven geen strafbaar feit naar de huidige strafrechtelijke stand van zaken op te leveren. Daarnaast kan het systeem worden misbruikt als hulpmiddel om enig ander delict te plegen. Dit type gedrag levert op zich wel reeds een strafbaar feit op, maar kan met behulp van de computer tot veel grotere schadebedragen leiden. Beide vormen van computermisbruik (het systeem als object of als middel) hoeven elkaar niet uit te sluiten. Het begrip geautomatiseerd systeem moet ruim worden opgevat; van zakcomputer tot internationale netwerken waaraan vele duizenden apparaten zijn gekoppeld.

De volgende vier typen misbruik zijn te onderscheiden:

1. het zich onbevoegd toegang verschaffen tot een systeem of het onbevoegd gebruik maken ervan;

2. het verhinderen of bemoeilijken van de goede werking van een systeem, op zich onder te verdelen in:

a. computersabotage;
b. manipulatie van apparatuur, programmatuur of gegevens;
c. wegnemen van apparatuur, programmatuur of gegevens;

3. het onbevoegd kennis nemen of kopiëren van gegevens;

4. het onbevoegd namaken van apparatuur of programmatuur.

Zodra de hierboven genoemde gedragingen een strafbaar feit opleveren, wordt gesproken van computercriminaliteit. Het gebruik van deze term duidt op een wettelijke strafbaarstelling, zoals mede besproken in de volgende paragrafen.

## 3 Algemene kenmerken van het wetsvoorstel

Het wetsvoorstel Computercriminaliteit gaat, in navolging van de Commissie Franken, uit van een zodanige aanvulling van de bestaande rechtsregels dat zoveel mogelijk aansluiting wordt gezocht bij het bestaande niveau van strafrechtelijke bescherming en de bestaande mogelijkheden van waarheidsvinding en de in dat verband geboden rechtsbescherming in het strafproces. Het wetsvoorstel bestaat uit drie artikelen:

I. Wijziging van het Wetboek van Strafrecht;
II. Wijziging van het Wetboek van Strafvordering;
III. Wijziging van het Burgerlijk Wetboek.

In het Wetboek van Strafrecht is het materiële strafrecht geregeld: een omschrijving van de strafbare gedragingen en de daarbij behorende maximale straffen. In het Wetboek van Strafvordering is het formele strafrecht geregeld: het instrumentarium waarmee organen belast met de opsporing, vervolging en berechting moeten opereren. Daarbij is aangegeven hoe ver hun bevoegdheden strekken en welke beperkingen voor het handelen van deze instanties gelden.

De artikelen I en II zijn verdeeld in onderdelen. Per onderdeel worden voorstellen gedaan om bestaande wetsartikelen te wijzigen, te laten vervallen of nieuwe artikelen toe te voegen.
De wijziging van het Burgerlijk Wetboek betreft Titel 9 van Boek 2: de jaarrekening en het jaarverslag. Voorgesteld wordt dat het bestuur van een onderneming, voor zover Titel 9 van Boek 2 van toepassing is, in het jaarverslag een mededeling doet omtrent de *"maatregelen in verband met de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking"*.

Een aantal typen computermisbruik is onder de huidige wetgeving al strafbaar. Getracht wordt bestaande delictsomschrijvingen, zoals van valsheid in geschrifte, zodanig uit te leggen dat bepaalde typen computermisbruik hieronder vallen. Het bekendste voorbeeld is de zaak Rotterdam waarin het Hof heeft geoordeeld dat in bepaalde gevallen een computerbestand een geschrift is met bewijsbestemming. De Hoge Raad heeft zich hierover overigens nog niet uitgelaten. Eén van de criteria bij het opstellen van het wetsvoorstel is geweest dat het toepassen van de huidige rechtsregels op het verschijnsel computermisbruik resulteert in een ongewenste overspanning van bestaande juridische begrippen als "geschrift" of "goed".

In het wetsontwerp wordt overigens geen aandacht besteed aan strafrechtelijke sancties op het onbevoegd namaken van programmatuur of apparatuur. Deze problematiek wordt tot het terrein van het intellectueel eigendomsrecht gerekend. Derhalve wordt in dit artikel aan dit onderwerp ook geen aandacht besteed.

## 4 Wijziging van het Wetboek van Strafrecht

Artikel I van het wetsontwerp betreft wijzigingen van het Wetboek van Strafrecht (Sr.). De belangrijkste daarvan hebben betrekking op:

-- inbreken in computers, zowel door personen binnen als door personen buiten de organisatie;

-- het aftappen en/of opnemen van gegevensverkeer;

-- het verstoren van de geautomatiseerde gegevensverwerking;

-- het maken en gebruiken van valse betaalpassen en waardekaarten;

-- het manipuleren van gegevens (toevoegen, wijzigen en verwijderen).

De overige wetsvoorstellen betreffen wijzigingen uit een oogpunt van uniformiteit met andere reeds bestaande bepalingen. In het kader van dit artikel volstaan wij met de opmerking dat in een aantal artikelen het begrip "gegevens met geldswaarde in het handelsverkeer" (bijvoorbeeld programmatuur of adressenbestanden) wordt geïntroduceerd, naast het begrip "goed". Daar-mee vervalt voor deze artikelen de juridische vraag of onder goederen tevens gegevens moeten worden verstaan. Voor-beeld hiervan is het met winstoogmerk bekend maken of gebruiken van door misdrijf verkregen gegevens ("helen").

*De minister erkent dat het niveau van minimale beveiliging geen statisch begrip is, maar afhangt van de ontwikkelingen in de informatietechnologie.*

In aansluiting op het bestaande artikel 138 Sr. wordt in het nieuw toe te voegen artikel 138a Sr. in het wetsontwerp voorgesteld dat *"Hij die wederrechtelijk binnendringt in een daartegen beveiligd geautomatiseerd werk voor de opslag of verwerking van gegevens, of in een daartegen beveiligd deel daarvan, wordt gestraft met ..."*. In aanvulling daarop wordt in het tweede lid gesteld dat *"Hij die zich de toegang heeft verschaft door middel van het aannemen van een valse hoedanigheid, listige kunstgrepen of een valse sleutel, wordt geacht te zijn binnengedrongen"*.

De kernvraag in de discussie rondom dit artikel is de vraag wanneer sprake is van *"een daartegen beveiligd geautomatiseerd werk"*.
In de Memorie van Toelichting gaat de minister van Justitie hierop in. Volgens de minister verlangt artikel 138a Sr. voor het ontstaan van strafbaarheid van de indringer niet meer dan een minimale maar wel een daadwerkelijke beveiliging. Er kan bijvoorbeeld niet worden volstaan met de waarschuwing "verboden toegang" op het beeldscherm. De minister voegt hieraan toe dat het voldoende is als het slachtoffer van een computerinbraak kan aantonen dat er sprake is van *enige reële beveiliging*. Het is niet nodig dat deze beveiliging ook adequaat was in het licht van de te beveiligen, aan de gegevens verbonden belangen. Het gaat er volgens de minister om dat *degeen die de computer binnendringt door het doorbreken van de beveiliging, heeft blijk gegeven de wetenschap te hebben gehad dat hij een beveiligd systeem binnendringt en doelbewust enige inspanning heeft gedaan de beveiliging te doorbreken.*

De minister erkent dat het niveau van minimale beveiliging geen statisch begrip is, maar afhangt van de ontwikkelingen in de informatietechnologie.

De strafrechtelijke bescherming van het transport van gegevens vormt een complex geheel van wetsvoorstellen dat in samenhang met de Wet op de Telecommunicatievoorzieningen moet worden gezien. In het kader van dit artikel volstaan wij met de niet limitatieve opsomming van voorgestelde strafbare feiten:

-- het aftappen van gegevens die via de (openbare) telecommunicatie-infrastructuur of daarop aangesloten randapparatuur worden getransporteerd;

-- het aftappen van gegevensoverdracht tussen bijvoorbeeld terminal en centrale verwerkingseenheid en het verkeer via private netwerken;

-- het aftappen van straalverbindingen door middel van het plaatsen van een ontvanginrichting in het straalpad;

-- het aftappen van autotelefoonverbindingen slechts indien daartoe een *heel stelsel van ontvanginrichtingen die op elkaar zijn afgestemd* wordt gebruikt;

-- het aftappen van residustraling van beeldschermen.

Het storen van de geautomatiseerde gegevensverwerking wordt in de volgende gevallen strafbaar gesteld:

-- *"...indien daardoor verhindering of bemoeilijking van de opslag of verwerking van gegevens ten algemene nutte of stoornis in de telecommunicatie-infrastructuur ontstaat";*

-- *"...indien daarvan gemeen gevaar voor goederen of voor de verlening van diensten te duchten is";*

-- *"...indien daarvan levensgevaar voor een ander te duchten is";*

-- *"...indien daarvan levensgevaar voor een ander te duchten is en het feit iemands dood ten gevolge heeft"*.

In de Memorie van Toelichting wordt niet ingegaan op het begrip "ten algemene nutte" omdat dit begrip al een rol speelt in reeds bestaande strafrechtelijke bepalingen. De computers van de deltawerken vallen hier bijvoorbeeld onder, de com-

puters van een eenvoudige produktieonderneming zeer waarschijnlijk niet.

De minister stelt in de Memorie van Toelichting dat ook *tijdens eventuele stakingen de strafrechtelijke aansprakelijkheid voor het ongestoord functioneren van de desbetreffende voorzieningen overeind blijft.* Hij noemt daarbij met name PTT Telecom. Ons inziens geldt dit ook voor personeel werkzaam bij een rekencentrum (onder dezelfde voorwaarden zoals genoemd bij de strafbaarstelling). De meeste creditcards zijn evenwel ook geschikt voor gebruik in geldautomaten!

De minister stelt vervolgens voor dat *"hij die opzettelijk een betaalpas of waardekaart bedoeld voor het verrichten van betalingen langs geautomatiseerde weg, valselijk opmaakt of vervalst, met het oogmerk zichzelf of een ander te bevoordelen, wordt gestraft met...".* Het tweede lid bepaalt dat ook het opzettelijk gebruik van een dergelijke betaalpas of waardekaart *"als ware hij echt en onvervalst"* strafbaar is.
Voorbeeld van een betaalpas is de smartcard, voorbeeld van een waardekaart is de telefoonkaart waarmee in bepaalde telefooncellen kan worden getelefoneerd. Kaarten waarbij later wordt betaald, bijvoorbeeld door toezending van een rekening, vallen volgens de Memorie van Toelichting niet onder het begrip waardekaart. Dit soort creditcards valt ons inziens ook niet onder het begrip betaalpas, waardoor het vervalsen daarvan derhalve niet strafbaar is gesteld.

Ten slotte stelt de minister voor dat *"hij die opzettelijk en wederrechtelijk gegevens die door middel van een geautomatiseerd werk zijn opgeslagen, worden verwerkt of overgedragen, verandert, wist, onbruikbaar of ontoegankelijk maakt, dan wel andere gegevens daaraan toevoegt, wordt gestraft met ...".*
Deze bepaling stelt volgens de Memorie van Toelichting onder meer het invoeren van een computervirus, *indien daardoor andere gegevens worden veranderd, gewist, onbruikbaar of ontoegankelijk gemaakt*, strafbaar.
Naast het vernielen of beschadigen van gegevens wordt overigens ook het vernielen en beschadigen van geautomatiseerde systemen als zodanig strafbaar gesteld. Evenals dat voor het verstoren van de gegevensverwerking het geval is, worden hier alleen systemen bedoeld die ten behoeve van het algemene nut worden gebruikt.

Ten slotte merken wij op dat de voorwaarde van beveiliging alleen voorkomt in het artikel over het inbreken in computers. Dit is des te opmerkelijker als we de (maximale) strafmaat in beschouwing nemen. Voor het inbreken in computers geldt een lagere strafmaat dan voor het manipuleren met gegevens of het verstoren van de geautomatiseerde gegevensverwerking. De reden daarvoor is dat in de voorgestelde strafmaat met de mogelijke schadelijke gevolgen rekening is gehouden. De neiging zou echter kunnen ontstaan dat geen aangifte wordt gedaan van het inbreken maar wel van de daaropvolgende handelingen. De minister ziet de voorgestelde artikelen namelijk niet in relatie tot elkaar. Wat te doen indien wordt ingebroken in een computer, deze wordt besmet met een computervirus dat vervolgens de computer lam legt? Volgen we de letter van de wet dan blijkt daaruit dat deze drie strafbare feiten onafhankelijk van elkaar moeten worden gezien. Ook al is er geen sprake geweest van een minimaal niveau van beveiliging, dan nog levert het besmetten van de computer en het lamleggen daarvan - dit laatste alleen in bepaalde gevallen - ons inziens twee afzonderlijke strafbare feiten op waarvan aangifte kan worden gedaan.

## 5 Wijziging van het Wetboek van Strafvordering

In voorgaande paragraaf is een aantal wetswijzigingen ten aanzien van het Wetboek van Strafrecht besproken. Deze wijzigingen hebben alle betrekking op specifiek genoemde strafbare gedragingen. De voorgestelde wetswijzigingen ten aanzien van het Wetboek van Strafvordering hebben daarentegen betrekking op alle strafbare feiten die met behulp van een computer worden verricht. De voorstellen omvatten in hoofdlijnen de volgende onderwerpen:

-- de verplichting van de houder van een concessie voor de telecommunicatie-infrastructuur aan de officier van Justitie of de rechter-commissaris op diens vordering bepaalde inlichtingen te verschaffen;

-- het uitbreiden van de bevoegdheid van de rechter-commissaris tijdens het gerechtelijk vooronderzoek telefoonge-

sprekken af te luisteren tot de bevoegdheid het gegevensverkeer via de telecommunicatie-infrastructuur af te tappen;

-- het verrichten van onderzoek in een geautomatiseerd systeem tijdens de huiszoeking;

-- het uitbreiden van de rechtsbescherming die geldt ten aanzien van het gebruik van door politie of justitie opgenomen gegevens;

-- het gevolg geven aan verzoeken uit andere landen die zijn aangesloten bij het Europees Verdrag aangaande de wederzijdse rechtshulp in strafzaken;

-- de vergoeding van kosten die derden (waaronder in een aantal gevallen de gewezen verdachte) moeten maken ten behoeve van de opsporing.

In het kader van dit artikel volstaan wij met het toelichten van het onderzoek in een geautomatiseerde omgeving.

Het verrichten van een huiszoeking dient mede ter inbeslagname van gegevens die als bewijsmiddel kunnen dienen. De huidige wetgeving staat toe dat huiszoeking in een rekencentrum wordt verricht. Huiszoeking ter inbeslagname is beperkt tot een (vooraf bepaalde) fysieke locatie. Kenmerk van een geautomatiseerd systeem, opgenomen in een wijd verbreid netwerk, is dat de fysieke locatie waar gegevens zijn opgeslagen, niet steeds op voorhand duidelijk is. Gegevens die zich niet op de fysieke locatie van de huiszoeking bevinden, kunnen derhalve bij de huidige wetgeving niet in beslag worden genomen.

Teneinde het in beslag nemen van gegevens die voor de bewijsvoering noodzakelijk zijn, mogelijk te maken, wordt voorgesteld een afzonderlijke bevoegdheid tot het vergaren van gegevens in het Wetboek van Strafvordering op te nemen. Deze bevoegdheid is vastgelegd in een zestal wetsartikelen.

Allereerst wordt de mogelijkheid geopend, dat de rechter-commissaris tijdens het gerechtelijk vooronderzoek beveelt dat *"...hij van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot bepaalde gegevens die kunnen dienen om de waarheid aan de dag te brengen, deze gegevens, voor zover deze zijn opgeslagen, worden verwerkt of overgedragen met gebruikmaking van een geautomatiseerd werk, zal vastleggen, hem daartoe toegang zal verlenen of naar de griffie van de rechtbank zal overbrengen ...".*

De meest vergaande bevoegdheid tot onderzoek in een geautomatiseerd systeem bevat het daaropvolgende artikel. Het eerste lid van dit artikel luidt als volgt: *"In geval van een huiszoeking kan in een elders aanwezig geautomatiseerd werk onderzoek worden gedaan naar gegevens die kunnen dienen om de waarheid aan de dag te brengen. Worden dergelijke gegevens aangetroffen, dan kunnen zij worden vastgelegd".* In de Memorie van Toelichting wordt gesteld dat het begrip onderzoek tevens inhoudt dat *"groepen gegevens met elkaar kunnen worden vergeleken of anderszins aan bewerkingen onderworpen".* Het tweede lid van het artikel bepaalt dat het onderzoek slechts kan worden gedaan, *"indien een dergelijk geautomatiseerd werk vanaf de plaats waar de huiszoeking wordt gedaan op rechtmatige wijze toegankelijk is voor de personen die aldaar wonen, plegen te werken of te verblijven".* Het derde lid ten slotte bepaalt dat slechts met uitdrukkelijk verlof van de rechtbank, de rechter-commissaris ook gegevens die niet het voorwerp van het strafbaar feit uitmaken of tot het begaan daarvan hebben gediend, kan zoeken en opnemen.

Als aanvulling op bovenstaande twee artikelen wordt vervolgens bepaald dat *"...tot degeen van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de wijze van beveiliging van een geautomatiseerd werk, het bevel kan worden gericht toegang te verschaffen tot de aanwezige geautomatiseerde werken of delen daarvan. Degeen tot wie het bevel is gericht, kan hieraan gevolg geven door de kennis omtrent de beveiliging ter beschikking te stellen".* In de Memorie van Toelichting wordt de systeembeheerder genoemd als een zodanig persoon; vermoedelijk worden hier ook degenen bedoeld die de betrokken organisatie hebben geadviseerd. Deze kunnen ook worden geacht over dergelijke kennis te beschikken.

In aansluiting op de bestaande wetgeving wordt aan bovenstaande bepalingen toegevoegd dat geen onderzoek mag plaatsvinden naar *"gegevens die zijn ingevoerd door of vanwege personen met bevoegdheid tot verschoning"* en *"voor zover daartoe hun plicht tot geheimhouding zich uitstrekt".* Tevens wordt be-

paald dat een bevel tot medewerking niet kan worden gericht aan de verdachte. Indien de verdachte een rechtspersoon is, kan volgens de Memorie van Toelichting het bevel niet worden gericht aan de rechtspersoon als zodanig, maar wel aan de personen die in dienst zijn van deze rechtspersoon. Uiteraard kunnen deze zich verschonen indien zij zich bij medewerking blootstellen aan een strafrechtelijke vervolging.

Gaat het om een kennelijk in het buitenland zich bevindend systeem, dan zal degene die het onderzoek verricht, behoudens een uitdrukkelijk verdragrechtelijke grondslag, zich van het onderzoek dienen te onthouden. Een dergelijke verdragrechtelijke grondslag bestaat momenteel nog niet. De vraag is overigens of bij onderzoek in een netwerk dat internationaal vertakt is, in alle gevallen zichtbaar is dat onderzoek in een zich in het buitenland bevindend systeem wordt verricht. Indien achteraf blijkt dat gegevens zijn opgenomen uit een systeem in een land waarmee (nog) geen verdrag hieromtrent is gesloten, dan worden deze gegevens beschouwd als onrechtmatig verkregen bewijs, hetgeen impliceert dat ze niet als bewijsmateriaal kunnen worden gehanteerd.

## 6 Wijziging van het Burgerlijk Wetboek

Artikel III van het Wetsvoorstel Computercriminaliteit betreft wijziging van artikel 391 Titel 9 van Boek 2 van het Burgerlijk Wetboek: het door het bestuur van een onderneming, voor zover Titel 9 van toepassing is, in het jaarverslag opnemen van een mededeling "*omtrent de maatregelen in verband met de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking*".

De Memorie van Toelichting vermeldt dat *dit voorstel tot uitdrukking brengt dat de verantwoordelijkheid voor de mate en kwaliteit van beveiliging bij de directie van de vennootschap ligt. Het dwingt de directie zich rekenschap te geven van dit onderdeel van de gang van zaken binnen de onderneming*. In de Memorie van Toelichting wordt niet ingegaan op de aard en diepgang van deze mededeling.

De nadere invulling wordt aan de praktijk overgelaten. Naar onze mening kan een dergelijke mededeling onder andere de volgende vorm hebben:

-- een feitelijke mededeling dat maatregelen zijn getroffen;

-- een (al dan niet globale) feitelijke opsomming van de getroffen maatregelen;

-- één van bovenstaande mededelingen met daarbij een uitspraak over de kwaliteit van het getroffen stelsel van maatregelen, al dan niet met verwijzing naar de normen waaraan de getroffen maatregelen zijn getoetst.

Consequentie van dit voorstel is mede dat de accountant die belast is met de wettelijke controle van de jaarrekening (conform artikel 393 BW) deze mededeling hierbij moet betrekken. Artikel 393 BW schrijft voor dat de accountant moet nagaan of:
-- het jaarverslag, voor zover hij dat kan beoordelen, overeenkomstig de wet is opgesteld;
-- het jaarverslag met de jaarrekening verenigbaar is.

Artikel 393 BW schrijft niet voor dat de accountant de mededeling inhoudelijk toetst. Indien de mededeling echter geheel ontbreekt, zal de accountant hiervan in ieder geval in zijn verklaring melding moeten maken.

## 7 Consequenties van het wetsvoorstel

Beschouwen we bovenstaande wetsvoorstellen, dan kunnen we concluderen dat deze geen directe consequenties, anders dan die ten aanzien van de accountantscontrole, met zich meebrengen. In de wet is geen eis tot beveiliging vastgelegd. Wel is voor slechts één artikel, het inbreken in computers, beveiliging als voorwaarde voor strafbaarheid geïntroduceerd. Voor de overige artikelen geldt deze voorwaarde niet.

Indien er een vermoeden bestaat dat zich één van de voorgestelde strafbare feiten heeft voorgedaan, kan worden overwogen hiervan aangifte te doen. Het tijdstip waarop dit geschiedt, is uitermate belangrijk. Aangifte kan direct na het ontdekken van het vermeende strafbare feit geschieden. Het is ook mogelijk dat eerst zoveel mogelijk bewijsmateriaal wordt

vergaard, zodat de aangifte goed voorbereid kan worden gedaan. Criteria voor de keuze zijn:

-- de mate waarin een goed voorbereide aangifte noodzakelijk is teneinde Justitie in staat te stellen de juiste beslissingen te nemen;

-- de tijdigheid die het geval vereist: indien de dader op het punt staat naar het buitenland te vertrekken (hetgeen bij een greep uit de kas meer regel dan uitzondering is), dan kan hij na aangifte onmiddellijk worden aangehouden;

-- de kans dat door het doen van aangifte de vermoede dader hiervan op de hoogte komt en zijn acties staakt waardoor betrapping op heterdaad niet meer mogelijk is.

Per concreet geval zal door het verantwoordelijke management een afweging moeten worden gemaakt. Het doen van aangifte is, met uitzondering van strafbare feiten waarbij levensgevaar is ontstaan, niet verplicht. Overigens heeft het Openbaar Ministerie de bevoegdheid de strafbare feiten ambtshalve te vervolgen.

De bewijsvoering van de vermoede strafbare feiten vereist bijzondere aandacht. Ter terechtzitting zal niet alleen moeten worden aangetoond dat de vermeende gedraging heeft plaatsgevonden, ook zal moeten worden bewezen dat de verdachte dat feit heeft gepleegd. Daarbij kan niet worden volstaan met de redenering dat de verdachte de enige van een aantal verdachten is die het strafbaar feit zou kunnen hebben gepleegd. Het is daarentegen noodzakelijk dat een directe relatie kan worden gelegd tussen de dader en het delict.

*Gezien de vluchtigheid van informatie op elektronische gegevensdragers kunnen sporen eenvoudiger worden gewist dan in een conventionele omgeving waar geen sprake is van het gebruik van computers.*

Derhalve is het noodzakelijk in een zeer vroeg stadium (bijvoorbeeld direct na het ontstaan van een vermoeden dat een of meer strafbare feiten zijn gepleegd) bewijsmateriaal te verzamelen. Daarbij zijn twee situaties te onderscheiden:

1. Het is niet waarschijnlijk dat dezelfde dader hetzelfde strafbare feit nogmaals zal plegen (bijvoorbeeld een onrechtmatige overboeking van een groot bedrag naar het buitenland).

2. Het is zeer waarschijnlijk dat dezelfde dader hetzelfde strafbare feit nogmaals zal plegen (bijvoorbeeld een hacker die probeert vertrouwelijke gegevens te achterhalen).

Indien wordt vermoed dat hetzelfde strafbare feit niet zal worden herhaald, zal moeten worden getracht zoveel mogelijk bewijsmateriaal veilig te stellen. Hierbij valt te denken aan de logging, invoer- en verwerkingsverslagen en backup-bestanden. Indien echter wordt vermoed dat het strafbare feit zal worden herhaald zonder dat directe schade van onacceptabele omvang aan de organisatie wordt toegebracht, dan kan worden overwogen de dader te gaan observeren. In de meeste gevallen zal het in een dergelijk geval gaan om iemand die probeert in de computer in te breken. Alle acties die worden verricht, dienen te worden vastgelegd zonder dat de dader dit in de gaten krijgt, bij voorkeur op papier. Zodra het fysieke terminal-adres bekend is, kan de dader op heterdaad worden betrapt. Samen met de logging vormt dit naar alle waarschijnlijkheid voldoende bewijsmateriaal.

Bij het verzamelen van bewijsmateriaal bestaan de volgende additionele problemen:

-- Gezien de vluchtigheid van informatie op elektronische gegevensdragers kunnen sporen eenvoudiger worden gewist dan in een conventionele omgeving waar geen sprake is van het gebruik van computers.

-- Bij computercriminaliteit kan de dader vaak anoniemer blijven dan bij "gewone" criminaliteit: er zou eventueel nog kunnen worden aangetoond dat bepaalde gedragingen zijn verricht onder een bepaalde user identity en password; dat wil echter nog niet zeggen dat daarmee de dader (de persoon) kan worden aangetoond. Civielrechtelijk kan iemand verantwoordelijk worden gesteld voor alle acties die onder zijn of haar user identity en password zijn geschied; strafrechtelijk is dit niet mogelijk.
Uit het voorgaande kan niet anders worden geconcludeerd dan dat het krachtigste bewijsmiddel bij computercriminaliteit het betrappen op heterdaad is. Het is uitermate moeilijk op een andere wijze de identiteit van de dader vast te stellen. Het aantonen van het wederrechtelijk aftappen van verbindingen vormt zo mogelijk een nog groter probleem; de technische mogelijkheden zijn daarbij zeer beperkt en het is de vraag of het in een concreet geval überhaupt mogelijk is.

Voor het gebruik van valse betaalpassen geldt hetzelfde als hiervoor geschetst. Als het fysieke adres van de betaal- of geldautomaat bekend is, zou de dader op heterdaad kunnen worden betrapt. Technisch onderzoek van in beslag genomen betaalpassen of waardekaarten kan in principe uitwijzen dat deze valselijk zijn opgemaakt of vervalst.

*Eén van de eerste maatregelen die tijdens een huiszoeking zal worden getroffen, is het stilleggen van de geautomatiseerde gegevensverwerking.*

Ik merk op dat indien op onrechtmatige wijze gebruik wordt gemaakt van automatische betaalsystemen, het waarschijnlijk niet voldoende is om te bewijzen dat het geld naar een rekening van de betrokkene is geboekt. Nog steeds is daarmee niet vastgesteld dat de overboeking door hem is verricht. Aanvullend bewijsmateriaal blijft ook in een dergelijk geval noodzakelijk.
In het voorgaande is kort aangegeven dat het verrichten van een huiszoeking ter inbeslagname één van de dwangmiddelen is die Justitie kan hanteren bij de vervolging van strafbare feiten. In principe kan iedere organisatie te maken krijgen met een dergelijke huiszoeking. Het Openbaar Ministerie kan bepaalde strafbare feiten ambtshalve vervolgen zonder dat door de benadeelde aangifte is gedaan. Indien daarbij onvoldoende informatie beschikbaar is over de dader, kan worden besloten om zonder vooraf overleg te plegen met de directie of het bestuur over te gaan tot huiszoeking. Daarbij zal het rekencentrum zeer zeker plaats van onderzoek zijn.

De huidige rechtsregels ten aanzien van het verrichten van een huiszoeking zijn ook voor een huiszoeking in een rekencentrum van toepassing. Dit impliceert dat zowel apparatuur als gegevensdragers in beslag kunnen worden genomen, indien deze voor het onderzoek van belang zijn, ook indien daarmee de continuïteit van de geautomatiseerde gegevensverwerking in gevaar komt. Dit belang zal door Justitie worden afgewogen tegen het belang van een continue gegevensverwerking. Onzorgvuldig optreden kan namelijk leiden tot het betalen van een schadevergoeding aan degenen die schade hebben geleden zonder zelf betrokken te zijn geweest bij het gepleegde feit.

Eén van de eerste maatregelen die tijdens een huiszoeking zal worden getroffen, is het stilleggen van de geautomatiseerde gegevensverwerking. Om schade te voorkomen is het verstandig om zoveel mogelijk hieraan mee te werken. De voorgestelde wetswijzigingen impliceren overigens dat deze medewerking kan worden afgedwongen op bevel van onder andere de rechter-commissaris (zie paragraaf 5). Een andere consequentie van de voorgestelde wetswijzigingen is dat mede op bevel van de rechter-commissaris hem medewerking moet worden verleend bij het verschaffen van de toegang tot het geautomatiseerde systeem en tot geautomatiseerde systemen op andere locaties, voor zover deze toegang op normale wijze kan worden verkregen en deze systemen zich niet in het buitenland bevinden. Het niet opvolgen van een dergelijk bevel levert op zich een strafbaar feit op.
Een andere consequentie van de wetsvoorstellen is dat Justitie nu de bevoegdheid heeft om gegevens te kopiëren op gegevensdragers en deze mee te nemen in plaats van de oorspronkelijke gegevensdragers in beslag te nemen. De geautomatiseerde gegevensverwerking zou na afloop van de huiszoeking in principe weer kunnen worden voortgezet.

Voor service centres geldt een geheel eigen problematiek. Het is mogelijk dat één van de cliënten wordt verdacht van het plegen van strafbare feiten en dat Justitie overgaat tot het verrichten van huiszoeking bij het service centre. Daarbij is het van belang dat geen gegevens van andere cliënten in beslag worden genomen. Het stilleggen van de geautomatiseerde gegevensverwerking heeft direct gevolgen voor de verwerking van gegevens van niet-verdachte cliënten, waardoor het service centre haar verplichtingen jegens die cliënten niet meer kan nakomen. Naar onze mening is er in een dergelijk geval sprake van overmacht, tenzij het service centre zich bewust was van mogelijk strafbare activiteiten. Ten aanzien van het strafbare feit van artikel 50 Wet Persoonsregistraties heeft het service centre een eigen verantwoordelijkheid. Het is zelf ook strafbaar. Indien gegevensdragers of zelfs apparatuur in beslag worden genomen, is de kans groot dat ook na het verrichten van de huiszoeking de verwerking niet kan worden voortgezet. Het is de verantwoordelijkheid van de rechter-commissaris om slechts gegevens van verdachte cliënten in beslag te nemen en de verwerking van gegevens van niet-verdachte cliënten van het service centre zo min mogelijk te storen. Desondanks is het voor het management van het service

centre verstandig mee te werken, nog afgezien van het feit dat medewerking kan worden afgedwongen. Overigens dient erop te worden toegezien dat de belangen van de verdachte cliënt mede in beschouwing worden genomen; een verdachte cliënt is nog geen schuldige cliënt!

*R.A. s'Jacob*
*Is sinds 1987 werkzaam als junior EDP-auditor bij KPMG Klynveld EDP Audit. Hij is momenteel bezig met het vak Controleleer van de NIVRA-opleiding. Gedurende zijn opleiding heeft hij onder andere stage gelopen bij de Fraude Centrale van de Centrale Recherche Informatiedienst.*
*René André s'Jacob heeft met name ervaring opgedaan in het beoordelen van administratieve organisaties en complexe financiële informatiesystemen bij banken en bij de overheid en bij het inrichten van de organisatie rondom deze systemen. Zowel intern als extern doceert hij de KPMG Klynveld-cursussen Basiskennis Automatisering en Interne Controle (BAIC) en Systeembeoordeling (CASA).*
*Daarnaast verricht hij onderzoek op het gebied van juridische aspecten van automatisering, waaronder de ontwikkelingen op het gebied van automatiseringscontracten en informatietechnologie en strafrecht.*

EDP AUDITOR

# EDP Auditorium

## Boekbespreking
## *Achter de schermen van automatiseringscontracten*

*Mr. V.A. de Pous*

De tijd dat op het nog relatief jonge rechtsgebied computerrecht eenoog koning is, lijkt voorgoed voorbij. Verschillende juristen beschouwen tegenwoordig de automatische verwerking en communicatie van gegevens in juridisch perspectief en leggen het resultaat van hun noeste arbeid vast op papier. Een goede zaak, want juridische doctrine draagt in zeer belangrijke mate bij aan de rechtsontwikkeling.

Computerrechtliteratuur dient als rechtsbron voor juristen en als richtsnoer voor informatici, EDP-auditors en het management van geautomatiseerde organisaties. In tegenstelling tot andere rechtsgebieden kan men in het licht van computerrecht nog niet van een "informatiecrisis" spreken, maar de hoeveelheid artikelen, rapporten en boeken groeit gestaag. Gelukkig wordt er niet *alleen* voor rechtsgeleerden geschreven. Ook anderen die betrokken zijn bij aanschaf en gebruik van informatietechnologie, komen zo nu en dan aan bod.

*Achter de schermen van automatiseringscontracten* is zo'n publikatie, geschreven door en voor mensen in de wereld van geautomatiseerde gegevensverwerking, waarmee niet-juristen heel goed uit de voeten kunnen. En dat is een verdienste. De *hoofd*auteurs van dit boek zijn prof.mr. J.M.A. Berkvens (afdelingsdirecteur Juridisch Fiscale dienst Rabobank Nederland/bijzonder hoogleraar Informatica en Recht Katholieke Universiteit Nijmegen), drs. J.J.M.F. Borking (directeur branche-organisatie voor informatietechnologie COSSO), mr. C.F. van Geest (contractmanager IBM), mr. N.J. Rinkel (adjunct-directeur technische computergebruikersvereniging CIAD) en mr. H.A. van der Schraaf (medewerker Stafgroep Strategie Rabobank Nederland) en de vorig jaar overleden prof.dr. G.P.V. Vandenberghe (hoogleraar Informatica en Recht Vrije Universiteit Amsterdam), aangevuld met mr. R.E. van Esch (senior bedrijfsjurist Rabobank Nederland), drs. R. van den Hoven van Genderen (wetenschappelijk medewerker Universiteit Utrecht) en mw. mr. E.P.M. Thole (wetenschappelijk medewerkster Universiteit Utrecht).

Deze auteurs zijn erin geslaagd licht te brengen in het duistere, maar vooral complexe terrein van computercontracten. *Achter de schermen van automatiseringscontracten* bevat namelijk een veelheid aan waardevolle informatie, die betrekking heeft op de aanschaf en het gebruik van informatietechnologieprodukten en -diensten. Die informatie wordt verstrekt in de vorm van essays, wetgeving, (model)contracten en algemene voorwaarden en een aantal checklists. Dat maakt het voor de praktijk van alledag een zeer bruikbare publikatie.

De gekozen vorm, een gebonden boek en niet een losbladige editie, versterkt de bruikbaarheid. Daar ben ik blij om, want losbladige publikaties zijn vaak minder toegankelijk en vereisen van de gebruiker bovendien een haast ijzeren discipline om de supplementen in te brengen. Daarnaast is een losbladige editie verre van compact.

De auteurs van *Achter de schermen van automatiseringscontracten* hebben in dit verband niet zozeer de kool en de geit gespaard, dan wel eerder een goed evenwicht bereikt door zo volledig mogelijk op de brede en complexe problematiek van computercontracten in te gaan, zonder de voorwaarde van compactheid tekort te doen. Dat is het knappe van deze publikatie. Maar het gevaar, mede gelet op de omvang van de eerste druk (410 pagina's), ligt op de loer dat de volgende druk opnieuw meer pagina's gaat bevatten dan de huidige 503. Ik zou dat jammer vinden.

Verder teken ik bewaar aan tegen de titel. Het begrip "automatiseringscontract" wordt mijns inziens hoofdzakelijk gebruikt in de sfeer van de sociale partners

en niet of nauwelijks in de verhouding tussen leverancier en gebruiker van computer-gerelateerde produkten en diensten. Zo sluiten werkgevers en vertegenwoordigers van werknemers nogal eens een automatiseringscontract, waarin allerlei materiële (onder andere arbeidsvoorwaarden en werkgelegenheid) en formele afspraken (inspraakprocedures bij de aanschaf van automatiseringssystemen) worden vastgelegd. Wellicht dat de term computercontracten niet helemaal de lading dekt, maar hij is mijns inziens zuiverder.

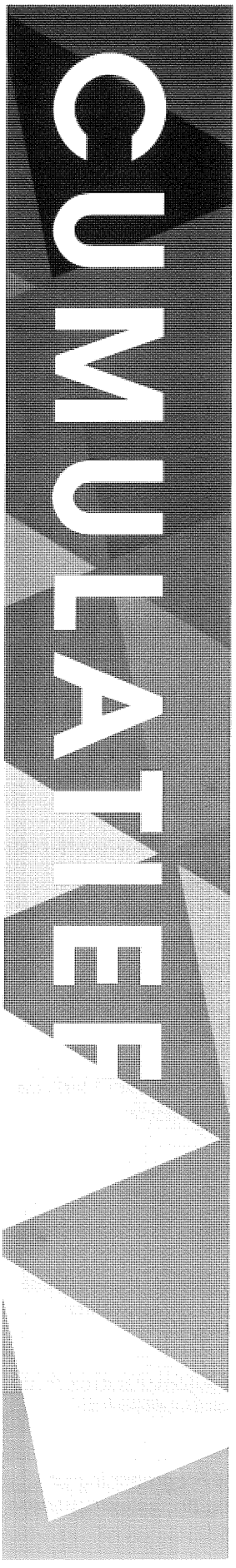
Maar wat daarvan zij, voor wat betreft de inhoud het volgende. Na enkele opmerkingen over de informaticamarkt (hoofdstuk I), gaan de auteurs op een heldere wijze in op het bijzondere van computercontracten (hoofdstuk II) en wordt de lezer aan de hand en stap voor stap meegenomen hoe je van een automatiseringsproject tot een contract komt (hoofdstuk III). Voor mij is dit de essentie van de publikatie, maar dat komt, bijvoorbeeld in de inhoudsopgave, er wellicht te weinig uit. Dat geldt in zekere mate ook voor de structuur van het boek. Die is weliswaar zonder meer aanwezig, maar voor niet in de problematiek ingevoerden niet meteen duidelijk.

In hoofdstuk IV wordt ingegaan op internationale aspecten en dat ziet voor een groot deel toe op contracten met Amerikaanse leveranciers. Vervolgens zijn er twee hoofdstukken (V en VI) met capita selecta. De eerste over wettelijke regelingen die van invloed zijn op aanschaf van informatietechnologieprodukten en -diensten, zoals de Auteurswet, de Wet Persoonsregistraties en telecommunicatiewetgeving; de tweede over bijzondere onderwerpen, waaronder turnkey-projecten, juridische aspecten van netwerken en geschillenbeslechting.

Twaalf contractmodellen, een begrippenlijst, een literatuurlijst, een trefwoordenregister en een overzicht van de door het boek opgenomen checklists besluiten *Achter de schermen van automatiseringscontracten.* Een indrukwekkende hoeveelheid informatie.

Dat de publikatie ook haar nut heeft voor niet-juristen, is uiteraard de bedoeling van de auteurs geweest. Er werd pas later bedacht daar uiting aan te geven. Zo bood men de eerste druk aan een jurist aan, te weten de vorige minister van Justitie; het eerste exemplaar van de tweede druk daarentegen werd met opzet aan twee niet-rechtsgeleerden overhandigd. Wie zijn publikatie over recht aan de president van de Algemene Rekenkamer F.G. Kordes en de oud-directeur van de Rijkskantoormachinecentrale prof. J. van Oorschot aanbiedt, moet sterk in zijn schoenen staan. Dat doen de auteurs dan ook en zij hebben wat mij betreft gelijk. Het boek is zonder twijfel de moeite van het lezen waard voor iedereen die betrokken is bij aanschaf en gebruik van computers.

*Het boek van mr. J.M.A. Berkvens e.a., Achter de schermen van automatiseringscontracten, wordt uitgegeven door Samsom H.D. Tjeenk Willink in Alphen aan den Rijn (tweede druk, 1989, 503 pagina's; ISBN 9060923596).*




# Cumulatief

**Overzicht van eerder verschenen artikelen in Compact**

Een selectie van geactualiseerde artikelen uit de 12 1/2 jaar Compact 1974 - 1986 is opgenomen in het boek *24 over EDP-auditing.* 24 auteurs over EDP-auditing in theorie en praktijk: visies, ontwikkelingen, werkwijzen en oplossingen. Het boek is verkrijgbaar via de boekhandel onder nummer: ISBN 90 14 03648 5.

**___45 14e jaargang 87/3**
**HERFST 1987**

Escrow-depot voor computersoftware in Nederland / *mr. V.A. de Pous*

Beveiligen tegen computermisbruik / *A.W. Neisingh RA en drs. J. Vossen*

Geïntegreerde gegevensverwerking: Structuur van controle- en beveiligingsmaatregelen in een ADR/DATACOM DB-DC-omgeving / *J.A.W. Winterink RA en drs. R.G.A. Fijneman*

Belangrijke functies van een toegangsbeveiligingspakket / *M.C. Duijm*

**___46 14e jaargang 88/1**
**WINTER 1987 / 1988**

SKE, Structured Knowledge Engineering *ing. A. van der Vlist*

Beveiliging bij datatransmissie / *ing. H.A.J.M. Spape*

Electronic Funds Transfer: het elektronisch uitvoeren van betalingen - literatuurstudie / *mw. ing. I.M. van Duin*

**___47 15e jaargang 88/2**
**LENTE / ZOMER 1988**
**Special van de sectie Software Engineering**

De sectie Software Engineering, een inleiding / *H. Veenman*

Software Engineering / *H. Veenman en ing. L.J.M.W. Gielen*

Het testen van software / *O. Kluyt*

UNIX / *ing. A. van der Vlist en ing. J.C. van Winkel RI*

Computervirussen / *ing. J.C. van Winkel RI*

Objects / *ing. L.J.M.W. Gielen*

HyperCard / *J. Schalk*

Programmeertheorie / *J. Schalk*

Het Apple Talk netwerk, een beschouwing / *J.L. Ramos Najera*

PS/2 - OS/2 / *ir. J. de Graaff en drs. D.J.P. Witte*

Elektronisch betalen, de betaalpas / *ing. J. Rotteveel*

**___48 16e jaargang 89/1**
**LENTE 1989**

Het uitvoeren van een transactie-analyse / *M.C. Duym*

Software escrow / *R.A. s'Jacob*

Computervirussen. Worm in groot netwerk / *drs.ing. J.C. van Winkel RI*

Beheersaspecten bij gebruik van microcomputers / *J.F.C. van Epen CISA*

The IBM AS/400. A concern to the EDP Auditor? / *H.J. Lijnes*

AS/400 security / *mw. V. Six*

Internationale gegevensstromen: abstract en moeilijk te controleren / *mr. V.A. de Pous*

**___49 16e jaargang 89/2 ZOMER 1989**

Beveiliging, noodzaak? / *J.L.H. Kooijman RA*

Beveiligingsbeleid formuleren / *drs. R. Schenk*

Informatiebeveiliging in het kader van automatisering / *drs. H.C. Kocks RA en drs.ing. H.A.J.M. Spape RA*

De keuze van beveiligingsmaatregelen in een geautomatiseerde omgeving / *drs. J. Kuipers RA*

De praktische methode voor de analyse van risico's bij automatisering / *ing. C.J.M. Gielen*

Organisatorische beveiliging van de geautomatiseerde gegevensverwerking / *J.C. Boer RA*

Fysieke beveiliging / *J.F.C. van Epen CISA*

Beveiligingsaspecten van computernetwerken / *drs.ing. H.A.J.M. Spape RA*

Logische toegangsbeveiliging / *J. Brinkman*

Beveiliging van de informatie in geautomatiseerde personeelsregistratiesystemen / *J.F.C. van Epen CISA*

**___50 16e jaargang 89/3 WINTER 1989**

De gevolgen van toepassing van informatietechnologie voor banken / *S. Lelieveldt*

Electronic Data Interchange (EDI) en Elektronisch Betalingsverkeer / *M. Groesz*

Vernieuwing geautomatiseerd verwerkingsproces van het betalingsverkeer bij de Postbank / *drs. C.P. Aland RA en A.H. Kuijlaars RA*

Mogelijkheden tot standaardisatie van de beveiliging van geautomatiseerd giraal betalingsverkeer / *drs. A. Hemelaar RA*

Geautomatiseerd uitgaand geldverkeer en het frauderisico / *drs. H.C. Kocks RA*

Cryptografische beveiliging van elektronisch berichten- en betalingsverkeer *drs. T.P. de Vries*

S.W.I.F.T. en Controle / *drs. P.M. Knuvers en ing. G.H.M. Meijer*

**Met ingang van 1990 wordt Compact uitgegeven in samenwerking met Samsom BedrijfsInformatie.**
**In Compact nieuwe stijl verschenen de volgende artikelen:**

**___1 17e jaargang 90/1 LENTE 1990**

De audit van operating systems / *drs. P. Veltman RA*

Het Virtual Machine concept van IBM / *A.A.J. Breed*

Betrouwbaarheid en beveiliging van het MVS-besturingssysteem / *ing. G.H.M. Meijer*

UNIX-beveiligingsaspecten / *drs.ing. J.C. van Winkel RI*

Aandachtsgebieden bij een AS/400 security audit / *ing. J.F. Kuperus*

Beveiligingsaspecten van VAX/VMS-systemen / *mw. G.J.C. Heikamp*

**___2 17e jaargang 90/2 ZOMER 1990**

Kwaliteitsbeheersing bij systeemontwikkeling / *ing. L.J.M.W. Gielen RI en drs. ing. G.J.P. Swinkels*

Het gebruik van geautomatiseerde hulpmiddelen bij systeemontwikkeling / *ir. J.A. Verstelle*

Jackson Structured Programming en kwaliteitsbeheersing bij systeemontwikkeling / *mw. V. Six*

Beoordelen betrouwbaarheid geautomatiseerde informatiesystemen op basis van de risico-analysemethode /
*drs. R.G.A. Fijneman RA,*
*drs. E.P.R. van Vroenhoven en*
*J.A..W. Winterink RA*

**___3 17e jaargang 90/3**
**HERFST 1990**

FunctiePunt Analyse voor de begroting van software-ontwikkeling /
*ir. B.A.W.M. Bruns*

Effect van software-kwaliteit op de kostenbegroting van systeemontwikkeling /
*drs. M.J. van der Vos*

Qualify: beoordeling effectiviteit en efficiëntie van informatiesystemen /
*drs.ing. G.J.P. Swinkels en*
*P.P.M.G.G. Brouwers*

An approach to Data Centre Efficiency Auditing / *D. Hall*