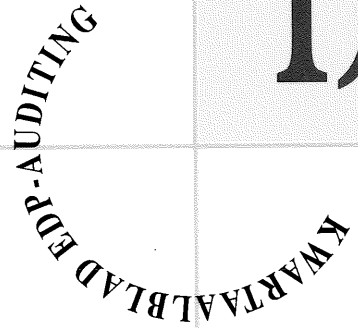
LENTE

COMPACT

EDP-AUDITING EN RECHT

1991/1



Compact ®
Jaargang 18, nummer 1
Een uitgave van KPMG Klynveld EDP Auditors 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 Auditors,
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
Ir. B.A. W.M. Bruns / Prof. mr. drs. J.Th. Degenkamp / Drs. H. van Gils RA / Mw. mr. I.M.A. de Graaf-Hinfelaar / Dr. J.J.C. Kabel / mw. mr. A.M. Ch. Kemna MBA/ P.A.J. van der Knaap / Mr. F.V.B.M. Mutsaerts / 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 tijdschriftuitgeversNOTU

ISSN 0920 - 1645

INHOUDSOPGAVE

2
Redactioneel

3
Geschillenbeslechting in de automatiseringsbranche
Mr. F.V.B.M. Mutsaerts
Talrijke automatiseringsprojecten gaan gepaard met complicaties. Deze bestaan onder andere uit het overschrijden van kosten en tarieven, te late opleveringen en het slecht functioneren van computerapparatuur en/of -programmatuur. Ondanks het feit dat veel van deze problemen aanleiding zouden kunnen geven tot een rechtszaak, is het opvallend hoe onverschillig afnemers en leveranciers in hun contracten omgaan met de wijze waarop automatiseringsproblemen kunnen worden opgelost. Schrijver zet de mogelijkheden voor conflictregulering op een rijtje.

9
De bewijskracht van computermateriaal in de civiele procedure
Mw. mr. I.M.A. de Graaf-Hinfelaar en mw. mr. A.M.Ch. Kemna MBA
Het aandragen van computermateriaal als bewijs in civiele procedures is nog tamelijk nieuw. Vaak is het nog onduidelijk hoeveel waarde de rechter zal hechten aan output, tapes, bestanden, etcetera. Voor partijen bij een potentieel geding is het moeilijk hun proceskansen in te schatten. Dit artikel geeft inzicht in de problematiek van het bewijzen in civiele procedures met behulp van de moderne technieken.

18
Praktische problemen van organisaties bij de implementatie van de Wet Persoonsregistraties
Ir. B.A.W.M. Bruns
De volledige invoering van de Wet Persoonsregistraties (WPR) is op 1 juli 1990 een feit geworden. Welke consequenties heeft deze wet nu voor een organisatie? Dit artikel heeft tot doel de lezer te informeren over een aantal praktijkproblemen bij de implementatie van de WPR, aan de hand van een analyse van de communicatiekanalen die door de WPR worden gereguleerd.

27
Een invulling van de beveiligingseis uit de Wet Persoonsregistraties
P.A.J. van der Knaap
Uit de Wet Persoonsregistraties komt een aantal verplichtingen voort. Eén van de meer in het oog springende verplichtingen is de beveiligingsplicht. In dit artikel wordt aangegeven welke normen hieraan ten grondslag kunnen liggen. Tevens wordt een audit beschreven die in het kader van deze problematiek is uitgevoerd.

35
Computercriminaliteit in Nederland
Mr. V.A. de Pous
Van alle verschijningsvormen van computercriminaliteit komt het illegaal kopiëren en gebruiken van computerprogramma's in Nederland het meeste voor. Slechts vijf procent van de slachtoffers van computercriminaliteit doet aangifte bij politie en justitie. Dat zijn enkele opvallende conclusies uit het rapport "Computercriminaliteit in Nederland", dat eind 1990 door het Platform Computercriminaliteit werd gepresenteerd.

39
EDP Auditorium
Deze rubriek opent met twee deskundige besprekingen van recente publikaties omtrent implicaties van privacy-wetgeving. Verder aandacht voor de uitreiking van de KPMG Klynveld scriptieprijs voor EDP Auditing en voor twee nieuwe hoogleraren op het gebied van informaticarecht en accountancy/EDP-auditing.

47
Cumulatief

REDACTIONEEL

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- systeinen ● 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 Auditors.

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.

"Het beheersen van risico's wordt alsmaar belangrijker. Gevolg is dat EDP-auditing zich mag verheugen in een groeiende belangstelling. Men zou kunnen zeggen dat beheersing van risico's hard op weg is zich te ontwikkelen tot een vijfde produktiefactor."

Met dit citaat uit de vorige Compact leidt de redactie bij haar lezers dit tweede nummer in omtrent de juridische aspecten van automatisering. getiteld "EDP-auditing en recht". Steeds vaker blijkt het recht gehanteerd te kunnen of te moeten worden om risico's bij de geautomatiseerde bedrijfsvoering te beperken of te voorkomen. Het recht heeft op deze wijze direct en ook indirect zijn invloed op het werkveld van de EDP-auditor.

Met de in deze Compact gepresenteerde onderwerpen hoopt de redactie opnieuw aan te geven waar de raakvlakken tussen informaticarecht en EDP-auditing liggen.

Uitvoerig wordt aandacht gegeven aan de praktische consequenties van de Wet Persoonsregistraties voor talrijke organisaties. Dat de wetgeving er is, weet langzamerhand iedereen. De implementatie van de wet geeft echter nog de nodige problemen en vergt veel zorg en kennis van zaken.

Eén onderwerp stippen we op deze plaats extra aan: het NIVRA heeft aan de WPR een geschrift gewijd, dat in deze Compact wordt besproken. De vraag welke risico's bij uitstek samenhangen met verdergaande automatisering, komt naar voren in het recente rapport van het Platform Computercriminaliteit.
Compact behandelt de belangrijkste conclusies en aanbevelingen uit dit rapport.

Risicobeheersing is eveneens een onderwerp dat goed past in het kader van automatiseringsprojecten. De feiten zijn dat nog steeds veel projecten voor betrokkenen op een mislukking uitlopen. Opvallend is het dan te constateren dat er vaak weinig aandacht wordt besteed aan het zorgvuldig invullen van een geschillenclausule.
In deze Compact worden de mogelijkheden voor geschillenbeslechting in de automatiseringsbranche op een rijtje gezet.
Extra aandachtspunt voor auditors: de rol van deskundigen bij bemiddeling in conflicten.

Een onderwerp dat met geschillenbeslechting samenhangt is de bewijsvoering in civiele zaken. De intrede van moderne technieken en media levert voor de rechter nogal eens het probleem op welke waarde hij aan (de betrouwbaarheid van) het bewijs moet hechten. Hier kan een taak liggen voor de EDP-auditor. Of om met een citaat uit de vorige Compact af te sluiten:

"alle reden voor een multidisciplinaire benadering van de vakgebieden informatica en informaticarecht, ofwel: kruisbestuiving".

De redactie bedankt ook deze keer prof.mr. J.M.A. Berkvens voor zijn juridische adviezen en mevrouw mr. A.M.Ch. Kemna MBA voor de coördinatie van dit nummer van Compact.

Prof. A.W. Neisingh RA

Geschillenbeslechting in de automatiseringsbranche

Mr. F.V.B.M. Mutsaerts

Conflicten tussen bijvoorbeeld leveranciers en gebruikers van informatiesystemen hebben naast juridische meestal specifieke technische kanten.
Een advocaat gespecialiseerd in computerrecht geeft inzicht in de mogelijkheden die er zijn om automatiseringsgeschillen deskundig te laten oplossen.

INLEIDING

Talrijke automatiseringsprojecten gaan gepaard met complicaties. Deze bestaan onder andere uit het overschrijden van kosten en tarieven, te late opleveringen en het slecht functioneren van computerapparatuur/programmatuur. Ondanks het feit dat veel van deze problemen aanleiding zouden kunnen geven tot een rechtszaak, is het opvallend hoe onverschillig afnemers en leveranciers in hun contracten aankijken tegen de wijze waarop automatiseringsproblemen kunnen worden opgelost. Automatisering vereist een langdurige betrokkenheid en medewerking van beide partijen. Doordat partijen aan de invulling van de geschillenclausule bij het aangaan van het automatiseringscontract weinig of geen aandacht besteden, komen zij, wanneer zich problemen voordoen bij de uitvoering van het contract, in een patstelling terecht. Procederen wil men niet, maar hoe het geschil dan wel moet worden opgelost weet men ook niet. Een goede invulling van de geschillenclausule kan aan deze impasse een einde maken.

Naast de mogelijkheid het geschil voor te leggen aan de overheidsrechter, bestaan er alternatieve methoden om geschillen te beslechten, zoals problemsolving-onderhandelen, mini-trial en arbitrage. De keuze voor de meest passende vorm voor geschillenbeslechting in de automatiseringsbranche hangt af van diverse overwegingen. Hierna zullen de voor- en nadelen van de verschillende vormen van conflictregulering aan de orde worden gesteld. Vervolgens zal worden nagegaan wat de meest geschikte vorm van geschillenbeslechting voor de automatiseringsbranche is. Daarbij moet rekening worden gehouden met de vaak gemengde (zowel juridische als technische) problemen waarmee men bij het oplossen van automatiseringsgeschillen te maken krijgt.

CONFLICTREGULERING DOOR DERDEN

Wanneer partijen een tussen hen gerezen conflict niet kunnen oplossen, kunnen zij een beroep doen op een derde [Novi88]. Teneinde een antwoord te vinden op de vraag wie de meest geschikte persoon of instantie is om effectief en efficiënt problemen tussen partijen in de automatiseringsbranche op te lossen, zullen we nu de verschillende vormen van conflictregulering en -hantering bezien.

Problemsolving-onderhandelen
De derde spoort de knelpunten op of confronteert de betrokken partijen met hun gedrag en helpt aan te geven hoe de problemen kunnen worden opgelost, zodat partijen onderling tot een vergelijk kunnen komen.

Mini-trial
Een derde tracht partijen tot elkaar te brengen door oplossingsvoorstellen te evalueren of zelf voorstellen te doen. Indien partijen een aanbeveling tot minnelijke schikking niet wensen te accepteren, betekent dit het einde van de mini-trial. De derde blijft een adviseur en kan dus wel drang maar geen dwang uitoefenen.

Bindend advies
Hiervan is sprake wanneer partijen zijn overeengekomen, hetzij naar aanleiding van een gerezen geschil, hetzij met het oog op geschillen die in de toekomst zouden kunnen ontstaan, hun onenigheid te laten beslissen door een derde die daartoe advies uitbrengt. De partijen verklaren dan bij voorbaat zich jegens elkaar gebonden te achten aan dat advies. Een dergelijk advies heeft geen rechtskracht. Indien een partij zich er niet aan wenst te houden, kan men derhalve alsnog naar de rechter stappen.

Arbitrage
Grondslag voor arbitrage is een daartoe strekkende overeenkomst van partijen. In die overeenkomst hebben partijen bepaald dat geschillen aan particuliere scheidslieden (arbiters) worden voorgelegd. De uitspraak die de arbiters voor een geschil geven, heeft de status van een vonnis dat rechtskracht heeft en met behulp van overheidssteun kan worden verwezenlijkt. Arbitrage is geregeld in boek 4, de artikelen 1020 - 1076 Wetboek voor Burgerlijke Rechtsvordering (herziening anno 1988, hierna: Rv).
Bij overeenkomst kunnen partijen incidenteel arbiters aanwijzen (ad hoc-scheidsgerechten) of een verwijzing opnemen naar een arbitrage-instituut, dat beschikt over een door dat instituut opgesteld reglement en geselecteerde arbiters, teneinde een goede afwikkeling van de procedure te waarborgen. In de automatiseringsbranche houden het Nederlands Arbitrage Instituut (NAI) en de nog jonge Stichting Geschillenoplossing Automatisering (SGA) zich met deze geïnstitutionaliseerde arbitrage bezig.

Gewone rechtspraak
Wanneer partijen niet anders zijn overeengekomen, worden geschillen over burgerlijke rechten en over schuldvorderingen door de overheidsrechter beslecht (art. 112 Grondwet).

Welke vorm van conflictregulering?

Vooropgesteld zij dat de lichtst mogelijke vorm van geschillenbeslechting de voorkeur verdient. Deze noodzaak is in de automatiseringsbranche des te meer aanwezig aangezien partijen vaak met elkaar verder moeten.

Wanneer een conflict tussen partijen nog niet is geëscaleerd en partijen de wil hebben om tot een schikking te komen, kan problemsolving-onderhandelen of mini-trial wenselijk en noodzakelijk zijn. Met name als het gaat om technische kwesties, kan een neutrale deskundige de onderhandelingen nog in goede banen leiden. De voordelen van deze vorm van conflicthantering zijn gelegen in de snelheid van de procedure en de lage kosten daarvan. Een nadeel is dat indien partijen een aanbeveling voor een minnelijke schikking niet wensen te accepteren, een procedure voor arbiters of de rechter noodzakelijk is. De derde-deskundige heeft namelijk geen beslissingsbevoegdheid. In dat geval heeft deze conflictregulering slechts tijdverlies tot gevolg.

Doordat partijen aan de invulling van de geschillenclausule bij het aangaan van het automatiseringscontract weinig of geen aandacht besteden, komen zij, wanneer zich problemen voordoen bij de uitvoering van het contract, in een patstelling terecht.

RECHTER OF ARBITER?

Willen partijen hun geschil doen beslechten door een rechter, dan staat de mogelijkheid open om in plaats van de overheidsrechter arbiters te benoemen [Aube88]. Wanneer zich bij de uitoefening van een automatiseringscontract naast problemen van juridische aard tevens problemen van technische aard voordoen, hetgeen meestal het geval is, is het mogelijk één of meer arbiters te benoemen op grond van hun specifieke deskundigheid en inzicht in de automatiseringsbranche. Dit spaart tijd en kosten aangezien een apart deskundigenbericht (art. 1042 en artt. 222 - 226 Rv) achterwege kan blijven [Hano88]. Met name wanneer partijen in het contract zijn overeengekomen dat een tussen hen gerezen geschil zal worden beslecht door arbiters, kunnen zij acuut een geschil aan een scheidsgerecht voorleggen, dat binnen zes maanden of de af-

gesproken termijn uitspraak doet (in geval van arbitrage door het NAI).

Arbitrage is wettelijk geregeld in de artikelen 1020 - 1076 Rv. Daarnaast gelden ook internationale overeenkomsten om te waarborgen dat vonnissen ook tegen buitenlandse rechtspersonen op eenvoudige wijze kunnen worden geëxecuteerd (Verdrag over de Erkenning en Tenuitvoerlegging van Buitenlandse Scheidsrechtelijke Uitspraken, New York 1958.) Bij vonnissen van de overheidsrechter levert dit nogal eens problemen op, omdat met veel landen nog geen executieverdrag is gesloten ten aanzien van "gewone" vonnissen.

Uit artikel 1036 Rv blijkt dat arbiters grote vrijheid hebben het procesverloop te bepalen. De procedure kan daardoor een informeler karakter dragen dan een procedure voor de overheidsrechter. De opstelling van de arbiters is actiever en opener, waardoor een behoorlijke oordeelsvorming wordt bevorderd. Zeker voor partijen die betrokken zijn bij automatisering kan dit informele element een belangrijke rol spelen. Een dergelijk project vereist nauwe samenwerking, hetgeen voor de partijen niet altijd eenvoudig is. Geschillen bestaan in veel gevallen dan ook uit misverstanden en kwesties van ondergeschikt belang. De actieve opstelling van een arbiter zal ertoe bijdragen dat persoonlijke wrevel kan worden weggenomen en de kern van het geschil duidelijk wordt. Tevens heeft de informele procedure tot gevolg dat de sfeer gemoedelijker is. Dit is vooral van belang als partijen na afloop van de procedure nog met elkaar verder moeten.

Kosten

Een bezwaar van arbitrage zou zijn dat de kosten die men maakt om problemen door middel van arbitrage op te lossen, veel hoger zijn dan bij een procedure voor de overheidsrechter, aangezien de partijen de arbiters moeten honoreren [Oost88]. Voor de procedure voor de gewone rechter is slechts een "bescheiden" griffierecht verschuldigd. Vooropgesteld moet worden dat bij een automatisering vaak behoorlijke bedragen omgaan, zodat de kosten die men maakt bij arbitrage maar een klein percentage vormen van de totale kosten. De rechtsgang voor een burgerlijke rechter lijkt goedkoop, maar gezien het feit dat men verplicht is een advocaat in de arm te nemen is dit maar schijn. (Bij arbitrage is bijstand door een advocaat niet vereist, maar wel gangbaar.) Ook het onderzoek door deskundigen moet worden betaald. Tevens kan het feit dat de gerechtelijke procedure veel langer duurt, worden gezien als een kostenpost. Een lange procedure betekent langer stagneren van de bedrijfsuitoefening door de afnemer en een moeilijker planning voor de leverancier voor de inzet van zijn personeel over de verschillende projecten. Tot slot kan het openbaar vonnis van de burgerlijke rechter zowel voor de leverancier als voor de afnemer een negatieve reclame zijn. Het arbitrale vonnis komt alleen in de openbaarheid met toestemming van beide partijen.

Snelle procedure of hoger beroep?

Uitgangspunt van artikel 1050 Rv is dat het niet mogelijk is van een arbitraal vonnis in hoger beroep te gaan. Dit is voor de teleurgestelde afnemer van een computersysteem niet altijd voordelig. In het arbitrale vonnis in de zaak Dolmans - Burroughs BV werd de eis van Dolmans tot ontbinding van de overeenkomst afgewezen [Dolm84]. Dolmans kon tegen dit vonnis geen hoger beroep instellen. In de rechtszaak Hanemaaijer & Van Es tegen dezelfde leverancier, Burroughs BV (Rb. Rotterdam, 7 mei 1982), daarentegen kwamen partijen na het instellen van het hoger beroep nog tot een schikking [Hane85]. Dit terwijl de eis tot ontbinding van de overeenkomst van Hanemaaijer & Van Es in eerste aanleg bij de rechtbank was afgewezen. Wanneer men echter het belang van de snelle afwikkeling van de procedure afweegt tegen het belang van de mogelijkheid van hoger beroep, zal bij automatiseringsgeschillen in veel gevallen het eerste belang zwaarder wegen.

Een lange procedure betekent langer stagneren van de bedrijfsuitoefening door de afnemer en een moeilijker planning voor de leverancier voor de inzet van zijn personeel over de verschillende projecten.

Opgemerkt moet nog worden dat krachtens artikel 1064 Rv tegen een arbitraal vonnis dat niet vatbaar is voor hoger beroep, nog wel de rechtsmiddelen van vernietiging en van request civiel openstaan. De vordering tot vernietiging van het arbitrale vonnis moet binnen drie maanden nadat het in gezag van gewijsde is gegaan bij de Rechtbank worden ingesteld. De vordering tot vernietiging kan slechts worden toegewezen op één of meer van de navolgende gronden:

- Een geldige overeenkomst tot arbitrage ontbreekt (art. 1052 Rv).
- Het scheidsgerecht is in strijd met de daarvoor geldende regelen samengesteld (art. 1052 Rv).
- Het scheidsgerecht heeft zich niet aan zijn opdracht gehouden.
- Het vonnis is niet overeenkomstig het in artikel 1057 bepaalde ondertekend of niet met redenen omkleed.
- Het vonnis, of de wijze waarop dit tot stand kwam, is in strijd met de openbare orde of de goede zeden (art. 1063 Rv).

Herroeping van het arbitrale vonnis wegens request civiel kan blijkens artikel 1068 Rv plaatsvinden op één of meer van de navolgende gronden:

- Het vonnis berust geheel of ten dele op na de uitspraak ontdekt bedrog, door of met medeweten van de wederpartij in de arbitrale procedure gepleegd.
- Het vonnis berust geheel of ten dele op stukken die na de uitspraak vals blijken te zijn.

- Een partij heeft na de uitspraak nog stukken in handen gekregen die op de beslissing van het scheidsgerecht van invloed zouden zijn geweest en door toedoen van de wederpartij zijn achtergehouden.

Het request civiel moet binnen drie maanden nadat het bedrog of de valsheid bekend is geworden of een partij de nieuwe stukken in handen heeft gekregen, worden aangebracht voor het Gerechtshof waar de zaak in hoger beroep zou hebben gediend in geval van een procedure voor de Arrondissementsrechtbank.

Deskundigheid

De snelheid waarmee een particulier scheidsgerecht tot een beslissing kan komen, blijkt uit het eerder genoemde arbitrale vonnis in de zaak Dolmans - Burroughs BV, dat op 18 februari 1985 is gewezen door de Stichting Raad van Arbitrage voor Metaalnijverheid en Handel [Dolm84]. De eiser, Dolmans, heeft op 27 juni 1984 een geschil aanhangig gemaakt. De hoeveelheid schriftelijke bewijsstukken waarmee hij de arbiters confronteerde bij zijn eis was omvangrijk. Dolmans had met gedaagde, Burroughs BV, een koopovereenkomst gesloten, waarbij gedaagde zich verplichtte tot levering van hardware, software, applicaties en diensten ter volledige automatisering van twee apotheken van Dolmans. Hij stelde dat Burroughs BV zich met betrekking tot deze koopovereenkomst aan wanprestatie schuldig had gemaakt en verzocht de Raad van Arbitrage om de koopovereenkomst te ontbinden. Er vonden drie mondelinge behandelingen plaats teneinde partijen de gelegenheid te geven hun standpunten toe te lichten. In de voor zo'n omvangrijke zaak relatief korte periode van nog geen acht maanden kwam het arbitrale college tot een beslissing. De deskundigheid van de arbiters maakte een deskundigenonderzoek overbodig.

De overheidsrechter daarentegen zal zich wegens gebrek aan deskundigheid wel genoodzaakt zien een tussenvonnis te wijzen, zodat hij op basis van artikel 221 Rv een onderzoek door één of meer deskundigen kan gelasten. Een voorbeeld van een geschil waarbij de rechter dat noodzakelijk achtte, teneinde inzicht te verkrijgen in de materie, was de zaak Sijbesma Holding - Wang Nederland e.a. (Rb. Utrecht 30 mei 1984 [Sijb86]). Het Algemeen Applicatie Centrum (AAC) te Woerden had een Wang-computer geleverd aan Sijbesma Holding BV. De door AAC geleverde computer bleek echter niet goed te functioneren. Verschillende reparaties aan de computer konden de storingen niet verhelpen. Teneinde een oordeel te kunnen vormen omtrent de vraag of AAC al dan niet wanprestatie had gepleegd jegens Sijbesma, alsmede omtrent de ernst van de eventuele wanprestatie, achtte de Rechtbank het noodzakelijk een onderzoek door één of meer deskundigen te bevelen. Iedere verdere beslissing werd aangehouden totdat het deskundigenbericht zou zijn uitgebracht. Hierdoor werd de procedure aanzienlijk verlengd.

Bij een snelle afwikkeling van de procedure is zowel de afnemer als de leverancier gebaat. Een bedrijf is in zijn automatiseringsfase bijzonder kwetsbaar. De informatie(re)organisatie beïnvloedt de dagelijkse gang van zaken aanzienlijk. De afnemer ziet dus het liefst dat een geschil met de leverancier zo snel mogelijk wordt opgelost. Ook de leverancier wordt benadeeld wanneer een geschil een oponthoud bij één van zijn afnemers ten gevolge heeft. Hij heeft zijn personeel namelijk al ingedeeld over de verschillende projecten die aangenomen zijn. Een vertraging bij de afronding van een project heeft tot gevolg dat nog niet kan worden begonnen met een nieuw automatiseringsproject.

STANDPUNTEN VAN DE BRANCHE-ORGANISATIES

Hierna wordt ingegaan op de meningen van vertegenwoordigers van de direct betrokkenen, de branche-organisaties voor gebruikers en leveranciers van informatiesystemen.

COMGE

De Nederlandse vereniging van computergebruikers (COMGE) spreekt haar voorkeur uit voor het bindend advies. De COMGE vindt dit de meest vrije en misschien wel de meest volwassen manier van geschillenbeslechting. De derde is niet meer dan een adviseur waaromtrent partijen tevoren hebben afgesproken het oordeel te accepteren. Hierdoor kan de procedure vrij informeel worden gevoerd en dat kan ertoe leiden dat de verhouding tussen partijen niet al te zeer wordt gejuridiseerd. Dit is vooral in de automatisering van belang, omdat partijen daar vaak noodgedwongen een langdurige relatie aangaan. Indien het bindend advies geen haalbare kaart is, acht de COMGE arbitrage een aanvaardbare keuze. Noodzakelijk is dan wel dat in de overeenkomst een clausule wordt opgenomen waarin bepaald is dat geschillen tussen partijen zullen worden beslecht door arbiters. Is dit niet gebeurd, dan moet bij het ontstaan van het geschil een akte van compromis worden opgemaakt. Het is maar de vraag of partijen dan nog tot overeenstemming kunnen komen.

VIFKA

De VIFKA, de brancheverenigingvoor kantoorinformatie- en communicatietechniek, lijkt niet afkerig tegenover arbitrage te staan. Rechtspraak moet efficiënt en kwalitatief goed zijn. Gezien het technische karakter van veel geschillen in de automatiseringsbranche zal een rechter deskundigen moeten inschakelen, hetgeen tot tijdverlies en verhoging van de kosten leidt. Ter zake kundige arbiters kunnen bij technische geschillen sneller tot een oplossing komen.
VIFKA is ervan overtuigd dat een arbitrage-instituut dringend gewenst is. Ze spreekt haar voorkeur uit voor een reeds bestaand instituut, het Nederlands Arbitrage Instituut. Het NAI heeft reeds een goede reputatie opgebouwd waar het

gaat om kwaliteit van uitspraken, geloofwaardigheid en vertrouwen van de verschillende betrokken partijen [Meij88].

COSSO

De Vereniging van Computer Service- en Softwarebureaus (COSSO) pleit voor de mini-trial. De mini-trial voldoet aan alle voorwaarden die van belang zijn voor de geschillenbeslechting in de automatiseringsbranche. De oplossing moet snel, goedkoop, vertrouwelijk, deskundig, vooruitziend, duidelijk en informeel zijn. Echter, omdat de mini-trial in Nederland tamelijk onbekend en dus niet geliefd is, kiest zij tevens voor de mogelijkheid van arbitrage.

De Stichting Geschillenoplossing Automatisering

In mei 1989 is de Stichting Geschillenoplossing Automatisering opgericht door vertegenwoordigers van leveranciers en gebruikers van informatietechnologie, alsook door enkele onafhankelijke instellingen en organisaties. De stichting heeft onder andere van het ministerie van Binnenlandse Zaken, de COMGE en de COSSO adhesiebetuigingen ontvangen. De branche-organisatie VIFKA blijft voor het Nederlands Arbitrage Instituut kiezen.

Volgens artikel 3 van de statuten heeft de stichting als algemene doelstelling het bemiddelen in geschillen op het gebied van de automatisering in de ruimste zin van het woord. Teneinde deze doelstellingen te kunnen realiseren kent de stichting de volgende procedures:

Mini-trial
Vanuit de gedachte dat de minst formele vorm van geschillenoplossing de voorkeur verdient, ontwikkelde de stichting als primair in te roepen procedure de mini-trial [SGAM89]. Het kenmerkende hiervan is dat het conflict na bemiddeling wordt opgelost door partijen zelf. Een actieve medewerking van de betrokken partijen is vereist. Indien partijen niet binnen een door de geschillencommissie of de voorzitter in redelijkheid te bepalen en eventueel te verlengen termijn een minnelijke schikking treffen, betekent dit het einde van de procedure. Iedere partij draagt zijn eigen kosten.

Spoedarbitrage
De arbitrage geschiedt conform de artikelen 1020 - 1076 Rv. De termijn waarbinnen een uitspraak over het geschil dient plaats te vinden is echter aanmerkelijk korter, namelijk maximaal drie maanden in plaats van zes maanden [SGAA89]. Teneinde aan de eis van snelheid recht te doen is het streven van de stichting erop gericht deze termijn terug te brengen naar negen weken. Tegen het vonnis van de arbiters staat geen hoger beroep open.

Kort-gedingarbitrage
Indien tijdens een automatiseringsproject een geschil ontstaat, maar geen van beide partijen wil het project stopzetten totdat het geschil is opgelost, dan dient soms een voorlopige voorziening te worden getroffen. Het scheidsgerecht doet zo spoedig mogelijk, maar in ieder geval twee weken na de mondelinge behandeling, uitspraak over het al dan niet toewijzen van de voorlopige voorziening.

De mini-trial voldoet aan alle voorwaarden die van belang zijn voor de geschillenbeslechting in de automatiseringsbranche. De oplossing moet snel, goedkoop, vertrouwelijk, deskundig, vooruitziend, duidelijk en informeel zijn.

CONCLUSIE

Op het gebied van de automatisering is het beroep op een gewone rechter niet altijd adequaat. Het gebrek aan deskundigheid van de overheidsrechter en de vaak lange procedures kunnen op onoverkomelijke bezwaren stuiten in de automatiseringsbranche. Informaticaconflicten lenen zich meer voor de alternatieve manieren om geschillen te regelen. Naast onderhandelingstechnieken die het verkrijgen van een minnelijke schikking tot doel hebben, zal arbitrage naar het zich laat aanzien de komende jaren aan populariteit winnen. De in 1989 opgerichte Stichting Geschillenoplossing Automatisering (SGA) zal daar zeker toe bijdragen. Vanuit de automatiseringsbranche heeft de SGA veel ondersteuning gekregen. Alhoewel er in de afgelopen periode slechts een beperkt aantal gevallen bij de stichting is aangemeld, zal, nadat de SGA-clausule in allerlei automatiseringscontracten is opgenomen, dat aantal zeker groeien. Van eminent belang hierbij is de opname van deze clausule in de zojuist vastgestelde, herziene COSSO-voorwaarden, die op 5 december 1990 bij de Rechtbank Den Haag zijn gedeponeerd.

LITERATUUR

[NOVI88] NOVI Conferentie "Geschillenbeslechting in de automatiseringsbranche", Amsterdam 28 januari 1988.

[Aube88] W.G.J.M. van Aubel, *Beslechting van automatiseringsgeschillen en arbitrage, voordelen van arbitrage en het arbitrage-instituut*, Computerrecht 1988/1, pagina 36.

Mr. F.V.B.M. Mutsaerts
Is lid van de maatschap Derks Star Busmann, advocaten, notarissen, belastingadviseurs te Utrecht en hoofd van de sectie Intellectuele Eigendom/Computerrecht.
Het computerrecht wordt door hem beoefend sedert 1982; sindsdien heeft hij over dit onderwerp regelmatig lezingen gegeven en artikelen gepubliceerd.
Hij is juridisch medewerker van de Automatisering Gids en docent Informaticarecht aan de Rijksuniversiteit Utrecht.

[Hano88] B. Hanotiau, *Beslechting van automatiseringsgeschillen en arbitrage; arbitrage en haar alternatieven*, Computerrecht 1988/1, pagina 31.

[Oost88] D. Oosterbaan, *Beslechting van automatiseringsgeschillen en arbitrage, rechter, arbiter of mini-trial*, Computerrecht 1988/2, pagina 81.

[Dolm84] *Dolmans - Burroughs BV*, arbitraal vonnis gepubliceerd in Computerrecht 1984/2, pagina 32.

[Hane85] *Hanemaaijer & Van Es - Burroughs BV*, Rb. Rotterdam, 7 mei 1982, gepubliceerd in Computerrecht 1985/6, pagina 27.

[Sijb86] *Sijbesma Holding - Wang Nederland e.a.*, Rb. Utrecht, 30 mei 1984, gepubliceerd in Computerrecht 1986/1, pagina 34.

[Meij88] A.P. Meijboom, *Arbitrage; rechter of arbiter?*, Computerrecht 1988/2, pagina 109.

[SGAM89] Mini-trial-reglement van de Stichting Geschillenoplossing Automatisering, d.d. 8 juni 1989, 's-Gravenhage.

[SGAA89] Arbitrage-reglement van de Stichting Geschillenoplossing Automatisering, d.d. 8 juni 1989, 's-Gravenhage.

De bewijskracht van computermateriaal in de civiele procedure

Mw. mr. I.M.A. de Graaf-Hinfelaar en
mw. mr. A.M.Ch. Kemna MBA

Past een computertape in een rechtbankvonnis? Wie heeft er gelijk, de bon uit de gelduitgifte-automaat of de gedupeerde cliënt? Ziet u zichzelf of uw cliënt wel eens voor deze vragen van bewijsrechtelijke aard gesteld? Dit artikel geeft u inzicht in waar de haken en ogen kunnen zitten bij het aandragen van computermateriaal als bewijs bij gerechtelijke procedures, ofwel: wat is de relatie tussen een betrouwbaar computersysteem, een tevreden cliënt en een overtuigde rechter?

INLEIDING

"... And if we do rely on this message and carry out our perceived contractual obligations, what is our legal standing if anything is brought into question and we need to furnish evidence?" [Drap90].

Deze verzuchting van een potentiële Electronic Data Interchange (EDI)-gebruiker geeft de vraag weer waarmee steeds meer organisaties en individuen te maken krijgen in onze voortschrijdende informatiemaatschappij. Met het toenemend gebruik van automatiserings- en telecommunicatietechnieken wordt internationaal duidelijk, dat het recht deze nieuwe ontwikkelingen (nog) niet altijd kan volgen. Juristen en meer in het bijzonder rechters zien zich voor de taak gesteld geschillen tussen partijen op te lossen terwijl daarbij steeds minder de vertrouwde bewijsmiddelen van papier en penne-inkt kunnen worden gebruikt. Dit artikel beoogt inzicht te geven in de problematiek van het bewijsrecht in de civiele procedure met behulp van de moderne technieken.

KORTE INTRODUCTIE IN HET PROCES- EN BEWIJSRECHT

Indien partij A met partij B afspreekt dat A een bepaalde hoeveelheid goederen of diensten tegen een bepaalde vergoeding aan B zal leveren op een afgesproken tijdstip, zal B uiteraard graag zien dat A deze overeenkomst ook nakomt. A wil de vergoeding graag tijdig op zijn bankrekening zien verschijnen. Indien de uitvoering van de overeenkomst om een of andere reden niet goed verloopt en er ontstaat een geschil, dan kunnen partijen naar de rechter stappen om "hun recht te halen". De rechter stelt dan in concreto vast wat recht is; indien de uitspraak definitief is hebben partijen zich hieraan te houden.
De wijze waarop partijen zich tot de rechter moeten wenden en de manier waarop de rechter recht moet spreken, is vastgelegd in het burgerlijk procesrecht [Meij88]. Het gaat daarbij om geschillen van burgerrechtelijke (of: civielrechtelijke) aard. Het burgerlijk procesrecht kan worden onderscheiden van het strafprocesrecht, waarbij het niet om geschillen tussen burgers gaat[1], maar waarbij de burger als procespartij tegenover de overheid staat.

Juristen en meer in het bijzonder rechters zien zich voor de taak gesteld geschillen tussen partijen op te lossen terwijl daarbij steeds minder de vertrouwde bewijsmiddelen van papier en penne-inkt kunnen worden gebruikt.

Bewijzen
Onderdeel van het burgerlijk procesrecht is het bewijsrecht. Indien een partij haar gelijk wenst te halen, zal zij haar beweringen met bewijsmiddelen moeten staven. Bewijzen in het burgerlijk proces betekent: voor de rechter de gestelde feiten aannemelijk maken. Doelstelling behoeft dus niet te zijn: het bewijzen van de absolute of materiële waarheid, zoals dat in het strafrecht het geval is. De burgerlijke rechter zoekt naar de processuele waarheid, ofwel: hij stelt vast wat recht is tussen de beide procespartijen op grond van de feiten, zoals die hem door die partijen in het proces worden voorgeschoteld.
Hiermee zijn twee belangrijke onderwerpen aangeboord: het hangt van de partijen af welke feiten er ter discussie staan in een proces (ofwel: de burgerlijke rechter is "lijdelijk", hij bepaalt niet de omvang van het geding en moet voor waar aannemen wat beide partijen voor waar aannemen). Vervolgens dienen partijen de rechter met bewijsmiddelen te overtuigen van die feiten die ter discussie staan. Het gaat er dan om, dat de rechter voldoende kan vertrouwen op het aangedragen bewijs, zodat hij de gestelde feiten aannemelijk kan achten.

Niet alleen in een gerechtelijke procedure zijn bewijsmiddelen van belang; zij werpen hun schaduw meestal al ver vooruit. Een partij zal niet snel een procedure beginnen, indien zij haar "bewijsrechtelijke positie" zwak acht. Voor bovengenoemde partijen A en B betekent dit, dat zij zich reeds bij het aangaan van de overeenkomst dienen bezig te houden met de deugdelijke vastlegging van hetgeen zij afspreken.

Zoals gesteld is bewijzen het aan de rechter een redelijke mate van zekerheid verschaffen met betrekking tot betwiste feiten. In het geval van de koop tussen A en B kunnen beide partijen bijvoorbeeld het contract als bewijs gebruiken, maar ook facturen, orderbevestigingen, brieven, mondelinge afspraken, enz. Hadden zij hun overeenkomst met behulp van EDI, telex of fax afgesloten, dan hadden zij ook de "output" van deze hulpmiddelen kunnen gebruiken. In het Nederlandse bewijsrecht geldt namelijk - in tegenstelling tot enige andere landen, waaronder het Verenigd Koninkrijk - dat het bewijs "vrij" is. In principe zijn alle bewijsmiddelen geoorloofd. In principe, want in een enkel geval bepaalt de wet dat het bewijs alleen met bijvoorbeeld een geschrift kan worden geleverd. Dergelijke bepalingen zijn echter vrij zeldzaam. Er is dus niets op tegen om computermateriaal of bewijs dat met behulp van moderne technieken is totstandgekomen, als bewijsmiddelen aan te dragen.

Bewijskracht
Daar staat wel tegenover, dat deze middelen nog door de rechter *gewaardeerd* ofwel op hun bewijskracht moeten worden getoetst. Op een aantal uitzonderingen na is de rechter vrij in het bepalen van de waarde van een bewijsmiddel. De uitzonderingen betreffen de authentieke, door bijvoorbeeld een notaris opgemaakte akte en in de meeste gevallen ook de onderhandse, door partijen opgemaakte en ondertekende akte; hiervoor geldt dat zij *verplicht bewijs* opleveren. De rechter is dan verplicht de inhoud voor waar aan te nemen of er de volledige bewijskracht aan toe te kennen die de wet eraan verbindt, tenzij er *tegenbewijs* wordt geleverd.
In de andere gevallen bepaalt de rechter in hoeverre het bewijsmiddel voldoende bewijskracht heeft. Naast de overtuiging van de rechter zelf, spelen hierbij ook andere factoren een rol. In zijn verantwoordelijke, openbare functie dient de rechter een moreel verantwoorde beslissing te nemen. Hij dient geen "Weltfremd" persoon te zijn, en dat dient ook ten aanzien van zijn beslissing te gelden. Hier speelt het probleem van de maatschappelijke aanvaardbaarheid c.q. legitimiteit van de rechterlijke beslissing: de rechter is verantwoordelijk voor het zorgvuldig vaststellen van de feiten en het geven van een aanvaardbare oplossing in de maatschappij.

Bewijslastverdeling
De rechter bepaalt eveneens, binnen de grenzen van de wet en naargelang een bewijsaanbod van of een bewijsovereenkomst tussen partijen, welke

1 *Opgemerkt zij, dat de overheid ook als civiele partij geldt (en dus niet als overheid als zodanig) indien zich een civielrechtelijk geschil voordoet, bijvoorbeeld: een geschil omtrent de aankoop van onroerend goed of software door de overheid.*

partij welk gesteld feit moet bewijzen. Het gaat hier om de zogenaamde *bewijslastverdeling*[2]. De verplichting om bewijs te leveren is niet afdwingbaar, maar het niet leveren van bewijs strekt in het nadeel van de bewijslastdragende partij. Bewijslast brengt dus bewijsrisico met zich mee!
Over het algemeen geldt, dat wie stelt moet bewijzen. De rechter kan echter anders bepalen, indien dat volgt uit een wettelijke regeling of indien hij vindt dat op grond van de *redelijkheid en billijkheid* de andere partij de bewijslast heeft te dragen, bijvoorbeeld omdat zij beter in staat is een bepaald feit te bewijzen. Deze billijkheidsregel brengt dan een gedeeltelijke doorbreking van de hoofdregel "wie stelt moet bewijzen" met zich mee. Voor de wederpartij kan dit betekenen, dat deze hierdoor bewijs tegen zichzelf moet leveren!

Voor partijen bij een (potentieel) geding levert de regeling van het bewijsrecht een bepaalde mate van onzekerheid op: hoe zal de rechter bijvoorbeeld de logging van een computersysteem waarderen? Hoe denkt hij over elektronisch opgeslagen berichten? En wie zal straks de gestelde feiten moeten bewijzen? En hoe kan de rechter op een afdoende manier worden overtuigd dat hij kan vertrouwen op het bewijsmiddel? Een vraagstuk waarmee men zich reeds bij het aangaan van een overeenkomst dient bezig te houden.

In het artikel van Mutsaerts elders in deze Compact is aangegeven dat de rechter niet de enige instantie is waar men zijn geschil kan laten beslechten. Andere vormen van geschillenbeslechting zijn over het algemeen aan veel minder procesrechtelijke regels gebonden dan een gerechtelijke procedure. Waar het betreft het bewijzen van het bewijs, ofwel het overtuigen van de beoordelaar van de betrouwbaarheid en de maatschappelijke aanvaardbaarheid van een bepaald bewijsmiddel zodat er rechtsgevolgen aan kunnen worden verbonden, staan partijen bij bedoelde andere vormen voor precies hetzelfde probleem.

GEVOLGEN VOOR COMPUTER-MATERIAAL

In het voorgaande werd aangegeven, dat de wet een open systeem van bewijsmiddelen hanteert. Gezien de huidige stand van de techniek is dat wenselijk, omdat zich steeds nieuwe middelen aandienen. Daarbinnen zullen bestaande en nieuwe computer- en telecommunicatietechnieken steeds een vrije bewijskracht krijgen toebedeeld; het gaat immers niet om authentieke of onderhandse *akten*. Bekijkt men de status van een computeruitdraai, dan gaat het bovendien om een *kopie* van een origineel (namelijk de informatie zoals opgeslagen in het geheugen van de computer). Dat geldt ook indien akten op microfilm worden bewaard; het gaat dan om reprodukties, niet meer om (ondertekende!) akten, met als gevolg: vrije bewijskracht. Eveneens gaat dit op voor transactie-informatie bij gelduitgifte-automaten, elektronisch berichtenverkeer met behulp van EDI, enz.

Terwijl de computersamenleving haar intrede heeft gedaan en computermateriaal nu al een bijna niet meer weg te denken factor is, lijkt de juridische wereld nog steeds de kat uit de boom te kijken. Vooral de rechterlijke macht neemt een afwachtende houding aan. Er is dan ook nog nagenoeg geen Nederlandse jurisprudentie waarin computermateriaal als bewijsmiddel in een civiele procedure wordt gebruikt. Wel is er jurisprudentie met betrekking tot de bewijskracht van bandopnames. Hier wordt verderop in dit artikel op ingegaan.
Over het algemeen blijft het echter nog onduidelijk hoe de rechter computermateriaal of bewijsmiddelen op basis van moderne technieken zal waarderen. Waar het inbrengen ervan in de procedure onvermijdelijk is, blijkt de rechter het direct waarderen van deze bewijsmiddelen veelal te "omzeilen" met de omweg van het deskundigenbericht. Het uiteindelijke beslissingsmoment ligt niettemin nog steeds bij de rechter. Enig inzicht in de materie van betrouwbaarheidsfactoren van moderne bewijsmiddelen en meer in het algemeen van betrouwbaarheidsfactoren van geautomatiseerde informatiesystemen is voor een rechter derhalve een gewenste vaardigheid.

VERBETEREN POSITIE INFORMATICAGEBRUIKER

Hoe zou de bewijsrechtelijke positie van de gebruiker van moderne technieken nu kunnen worden verbeterd? Op deze vraag wordt hieronder nader ingegaan.

De bewijsovereenkomst

Het Nederlandse bewijsrecht geeft aan partijen de mogelijkheid om de bevoegdheid van de rechter bij de waardering van het bewijs en/of bij het verdelen van de bewijslast in te dammen door een *bewijsovereenkomst* te sluiten. In zo'n overeenkomst wordt afgesproken dat een bepaald bewijsmiddel als verplicht en volledig bewijs zal gelden indien zich een geschil voordoet en wie het bewijs moet leveren. Een welbekend voorbeeld hiervan is te vinden in de Algemene Voorwaarden van de banken en van creditcard-maatschappijen, waarin wordt bepaald dat de administratie van de bank als (enig) bewijsmiddel zal gelden. Doel hiervan is het tegengaan van fraude. Ook in EDI-contracten komt een bewijsovereenkomst veelvuldig voor.
De rechter hoeft zich slechts in twee gevallen niet aan een bewijsovereenkomst te houden: indien er door partijen beslist wordt over rechtsgevolgen die niet ter vrije beschikking van partijen staan (maar die dwingend-rechtelijk door de wet worden bepaald) of indien het in strijd zou zijn met de goede trouw om zich op deze overeenkomst te beroepen. Een mogelijk verband kan hier worden gelegd met de toekomstige regeling in het nieuwe Burgerlijk Wetboek met betrekking tot de geldigheid van Algemene Voorwaarden in overeenkomsten met consumenten [Hijm90]. Deze regeling bepaalt, dat

2 *Het verzamelen van de processtof is de taak van partijen en daarom zal elke partij de feiten die voor haar van belang zijn in het geding moeten brengen door ze te stellen. Deze stelplicht gaat vooraf aan de bewijsplicht. Het stellen moet betrekking hebben op de feiten. De eiser geeft zijn visie op de rechtsverhouding, zodat de gedaagde weet waar het om te doen is en zich een oordeel kan vormen. Wat en hoe men in het concrete geval stelt, is een kwestie van procestactiek: niet alleen te weinig, maar ook te veel stellen kan catastrofaal zijn. Als een partij meer heeft gesteld dan zij kan bewijzen, kan zij in moeilijkheden komen, indien de rechter haar het bewijs van al haar stellingen opdraagt. Wanneer echter te weinig wordt gesteld, kan dit voor de rechter onvoldoende gegevens opleveren, wat zeer nadelig voor de desbetreffende partij kan zijn.*

een dergelijke bewijsovereenkomst onder bepaalde omstandigheden "onredelijk bezwarend" is.

Wanneer partijen geen bewijsovereenkomst hebben gesloten, rest hen zich te concentreren op de beïnvloeding van de rechter bij zijn bewijswaardering in het concrete geval.

De overeenkomst is dan vernietigbaar. Aangenomen wordt, dat op deze regeling soms ook een beroep kan worden gedaan door niet-consumenten die ten opzichte van hun wederpartij in een zwakkere positie verkeren; de zogenaamde reflexwerking.

Wanneer partijen geen bewijsovereenkomst hebben gesloten, rest hen zich te concentreren op de beïnvloeding van de rechter bij zijn bewijswaardering in het concrete geval.

Bewijslastverdeling

In het dagelijks leven staan niet altijd partijen met gelijke mogelijkheden tegenover elkaar. Nu de computer doordringt in het dagelijkse leven, komen zogenaamde "leken", vaak de consument, ongewild tegenover sterke geautomatiseerde organisaties met veel know-how te staan. In een procedure levert dit reeds bij aanvang een zwakke tegenover een sterke partij op, op grond van informatievoorsprong. Deze positie zal met name voor een "zwakke eiser" een moeilijke bewijspositie opleveren.
Zoals reeds eerder werd vermeld, kan de rechter hiermee rekening houden bij de verdeling van de bewijslast, op grond van eisen van redelijkheid en billijkheid. Ondanks het feit dat zij gedaagde is, zal de "sterke" partij dan concrete gegevens over het computergebruik moeten verschaffen, aangezien zij de meest gerede partij is. Een dergelijke uitspraak is reeds een keer gegeven, zij het in een ander verband dan een gerechtelijke procedure. De Geschillencommissie Bankbedrijf oordeelde toen in een bindend advies, dat een bank onvoldoende had aangetoond dat een rekeninghoudster haar geheimhoudings- en zorgvuldigheidsverplichtingen ten aanzien van haar PIN-code niet was nagekomen, waardoor een ander met haar (gestolen) pas geld had kunnen opnemen. De stelling van de bank, dat de rekeninghoudster als eiseres onomstotelijk moest bewijzen dat anderen op de gewraakte data niet konden beschikken over haar pas noch over haar PIN-code (voor consumenten tot dan toe veelal een onmogelijke opgave), werd door de Geschillencommissie verworpen.

Wijzigen van het wettelijk stelsel van bewijsrecht?

Aansporingen om de bewijsrechtelijke positie van de gebruiker van onder andere computer-output te verbeteren, komen vooral van internationaal niveau. Een goed voorbeeld daarvan is de aanbeveling nummer R (81)20[3] van het comité van Ministers van de lidstaten van de Raad van Europa, aangenomen op 11 december 1981. Daarin wordt aanbevolen regels betreffende onder andere de bewijskracht van computer-output op te nemen in de regelingen met betrekking tot het bewijsrecht.
Met name wordt aandacht besteed aan waarborgen voor authenticiteit (getrouwe weergave van de oorspronkelijke gegevens, het zonder hiaten tot stand komen van het computermateriaal en het systematisch ordenen, bewaren en beschermen tegen beschadiging).

Een dergelijke regeling in ons wettelijke bewijsrecht valt niet te verwachten om twee redenen. Ten eerste past het niet in het open systeem van bewijsmiddelen en ten tweede is juist sprake van een ontwikkeling naar meer vrijheid voor de rechter bij de waardering van het bewijs. Toch kunnen deze aanbevelingen worden gehanteerd als richtsnoeren bij het toekennen van bewijskracht aan computer-output. Hetzelfde geldt ten aanzien van de aanbevelingen in het UNCITRAL (United Nations Committee on International Trade Law) rapport van 1985. Deze commissie dringt erop aan ten aanzien van de toepassing van materiaal gebaseerd op moderne technieken in een civiele procedure:
- de wet te herzien om zo nodig obstakels ten aanzien van het gebruik van computermateriaal weg te nemen;
- ervoor te zorgen dat deze regels flexibel genoeg zijn in het licht van technologische ontwikkelingen;
- geschikte maatstaven te ontwikkelen waarmee de rechter de betrouwbaarheid van de gebruikte middelen kan inschatten.

Valt een herziening van het wettelijk stelsel niet te voorzien in ons land, de beide rapporten richten zich in bepaalde mate mede tot de rechter en trachten hem "handvatten" te geven bij het bepalen van de waarde van moderne bewijsmiddelen.
Dergelijke maatstaven zullen eveneens de rechtszekerheid voor (potentiële) partijen ten goede komen; men zal zijn proceskansen beter kunnen inschatten. Dat brengt ons wederom bij de taak waar partijen bij een civiel geding zich voor zien gesteld: het aan de rechter aantonen van de authenticiteit ofwel de echtheid c.q. de betrouwbaarheid van deze bewijsmiddelen: het bewijzen van het bewijs.

AANDACHTSPUNTEN TEN BEHOEVE VAN DE BEWIJSKRACHT VAN COMPUTERMATERIAAL

In deze paragraaf wordt de problematiek geschetst van het aantonen c.q. aannemelijk maken voor de rechter van de betrouwbaarheid van moderne bewijsmiddelen. Alvorens daarop in te gaan dient eerst te worden vastgesteld wat "betrouwbaarheid" is. Ten behoeve van dit artikel wordt hiervoor aansluiting gezocht bij NIVRA-geschrift 53, dat ingaat op kwaliteitsoordelen over informatievoorziening.

3 *Recommendation on the Harmonisation of Laws Relating to the Requirement of written Proof and to the Admissibility of Reproductions of Documents and Recordings on Computers.*

"Betrouwbaarheid" kan worden gezien als één van de kwaliteitsaspecten van informatiesystemen[4], naast bijvoorbeeld efficiency en effectiviteit. Indien de betrouwbaarheid van een bepaald (deel van een) systeem wordt onderzocht, wordt volgens het NIVRA-geschrift 53 gekeken naar:

- de controleerbaarheid van de informatie, het informatiesysteem en de informatievoorziening, ofwel de mogelijkheid de structuur van het systeem en de componenten vast te stellen en het proces van gegevensverwerking en informatievoorziening te kunnen controleren;

- de integriteit van de door middel van het systeem gegenereerde en/of verwerkte informatie, ofwel de juistheid, actualiteit en volledigheid van die informatie;

- de exclusiviteit van de informatie, ofwel de mogelijkheid bevoegdheden ten aanzien van de informatie te kunnen definiëren en waar nodig beperken.

Wat is er "anders" aan de moderne materialen?

Aansluitend op deze omschrijving van betrouwbaarheid kan worden vastgesteld, dat de huiver in de juridische wereld ten aanzien van de moderne bewijsmiddelen (mede) wordt veroorzaakt door de volgende factoren:

Manipuleerbaarheid
De informatie op moderne media is in de meeste gevallen manipuleerbaar. Hierdoor kunnen er gemakkelijk wijzigingen op de inhoud worden aangebracht, zonder dat dit direct zichtbaar of controleerbaar behoeft te zijn.
Uiteraard moet hier onderscheid worden gemaakt naar muteerbare en niet-muteerbare media. Voorbeelden van deze laatste zijn een WORM-schijf en niet-manipuleerbare microverfilmingen. In de wetgeving is een tendens te onderkennen, dat deze niet-manipuleerbare media geaccepteerd raken in plaats van het vertrouwde papier. Voorbeeld zijn de hierna nog te bespreken voorschriften van de staatssecretaris van Financiën met betrekking tot het archiveren voor fiscale doeleinden door middel van microverfilming.

Waar het betreft manipuleerbare media dient de inspanning van het aantonen van de authenticiteit van de inhoud niet alleen op de drager betrekking te hebben, maar veeleer op het informatiesysteem waarmee of waardoor de gegevens zijn vervaardigd. Dat brengt ons bij de tweede factor.

Ondoorzichtigheid en onpersoonlijkheid
In het algemeen kan worden gesteld dat met de toenemende automatisering van gegevensverwerkende en informatieverstrekkende processen de mens minder *zichtbare* invloed kan uitoefenen op deze processen. Voor geld halen aan de balie zijn twee personen nodig: de klant en de bankemployé. Beiden kunnen het proces van legitimeren, administreren, ondertekenen en uitbetalen zelf volgen. Bij geldautomaten ligt dat anders: hierbij is slechts één persoon betrokken, die de handelingen van de computer niet kan controleren. In het geval van EDI kan de menselijke factor zelfs helemaal worden uitgeschakeld: hierbij is sprake van twee via gestructureerde berichten met elkaar communicerende computers.

Onbekendheid
Onbekend maakt onbemind is het gezegde. Dat geldt ook in dit geval: onbekendheid met de wijze waarop de geautomatiseerde informatievoorziening dient te worden beheerst, maakt dat het gebruik van de daaruit voortkomende gegevens niet wordt erkend. Maar ook het omgekeerde komt voor: soms bestaat de neiging meer waarde te hechten aan uitgeprinte informatie dan aan gegevens die digitaal zijn opgeslagen. In werkelijkheid zijn echter beide verschijningsvormen evenzeer of even weinig betrouwbaar, afhankelijk van de kwaliteit van het informatiesysteem waarmee of waardoor ze zijn gegenereerd.

Verschuiven van functies

De manipuleerbaarheid van gegevens op moderne media en de ondoorzichtigheid en onpersoonlijkheid van informatiesystemen lijken aan te geven, dat er wezenlijk andere problemen spelen ten aanzien van de betrouwbaarheid van bewijsmiddelen dan wanneer het gaat om papieren bewijsmiddelen, vervaardigd door of bij een handmatig proces. De vraag is of dit werkelijk waar is. Waar gebruikers van informatiesystemen eerst zélf controle uitoefenden op de voortgang en de uitkomsten van processen, zijn deze controles nu verwerkt in de programmatuur of liggen ze bij anderen dan de gebruikers zelf. Zo gezien kan worden gesteld dat door automatisering er niet zozeer *nieuwe* uitvoerings- en controlefuncties ontstaan, maar veeleer dat er een *verschuiving* optreedt van functies, namelijk van de gebruikersorganisatie (GO) naar de automatiseringsorganisatie (VO, gegevensverwerkende en informatieverstrekkende organisatie en SO, systeemontwikkelings- en onderhoudsorganisatie) en een eventuele transportorganisatie in geval van telecommunicatiesystemen (TO).

Beheersingsconcept

Het uitbesteden van taken van de GO naar aparte functionele organisaties veronderstelt vanuit beheersbaarheidsoogpunt een duidelijke afbakening en omschrijving van de door iedere organisatie uit te voeren functies. Indien de VO, SO (en TO) op zodanige wijze - controleerbaar - zijn georganiseerd, dat de gebruiker erop kan vertrouwen dat de door hem uitbestede functies worden uitgevoerd, kan men spreken van een STOP (STeunen OP)-situatie [Kock90]. Pas in die situatie kan de gebruiker bepaalde aannames maken over bijvoorbeeld de betrouwbaarheid van de output en behoeven minder controles door de GO te worden uitgevoerd. In de STOP-situatie kan onder meer worden gewaarborgd dat:

4 *Informatiesysteem: het samenstel van structuur, middelen, processen en produkten waarmee of waardoor informatie wordt gegenereerd en/of verwerkt.*

– er alleen en bij voortduring wordt gewerkt met door de GO geautoriseerde programmatuur (= volgens specificaties van de GO ontwikkeld, getest, geaccepteerd en daarna overgedragen);

– de VO (en TO) in kan (kunnen) staan voor data-integriteit en voor de integriteit van de in de besturingsprogrammatuur opgenomen bevoegdheidsregels;

– de continuïteit van de verwerking is verzekerd.

De STOP-situatie kan slechts worden geëffectueerd indien gelijktijdig aan de volgende voorwaarden is voldaan:

– De noodzakelijke functiescheidingen tussen de functionele organisaties en tussen functionarissen zijn gerealiseerd en gedocumenteerd, inclusief ondersteunende (controle)procedures.

– Deze functiescheiding en procedures functioneren bij voortduring.

– De informatievoorziening (operationele, beheersings- en verantwoordingsinformatie) kan als voldoende worden aangemerkt.

– De applicatieprogrammatuur in gebruik bij de GO is betrouwbaar ontwikkeld (= bezit voldoende controlefuncties en levert voldoende controle-informatie op) en is voldoende gedocumenteerd.

Is aan één van deze voorwaarden niet voldaan, dan kan men spreken van een NON-STOP-situatie, waarvoor geldt dat de gebruiker niet zonder meer kan steunen op de informatie die door of met het systeem wordt gegenereerd.

Het moge duidelijk zijn, dat een STOP-situatie een ideaalsituatie is die vrij moeilijk is te benaderen. Met name in kleinere organisaties zal bijvoorbeeld de benodigde functiescheiding niet altijd kunnen worden doorgevoerd. In deze situaties dient verder gezocht te worden naar mogelijkheden om betrouwbare gegevens uit het systeem dan wel buiten het systeem op te leveren. Daarnaast speelt het probleem dat een STOP-situatie *bij voortduring* aanwezig dient te zijn, hetgeen uiteraard moeilijk te controleren of aan te tonen is. Overigens is het de vraag of er - in bewijsrechtelijke zin - steeds een STOP-situatie dient te worden aangetoond. Bewijzen in een civiele procedure is immers "aannemelijk maken voor de rechter", niet: "de absolute waarheid ontbloten". Indien een partij voldoende feiten kan aandragen waaruit blijkt dat een STOP-situatie wordt benaderd, kan worden aangenomen dat de output betrouwbaar is.

Overigens is het de vraag of er - in bewijsrechtelijke zin - steeds een STOP-situatie dient te worden aangetoond.

CONCLUSIE

Het voorgaande beoogt slechts een introductie te zijn in de problematiek van de beheersbaarheid van geautomatiseerde informatiesystemen, benodigd bij het waarderen van moderne bewijsmiddelen. Van een rechter mag men begrijpelijkerwijze niet verwachten, dat hij deze beheersbaarheidsproblematiek volledig doorgrondt en kan toepassen zodra bijvoorbeeld computertapes als bewijs worden ingebracht in een civiele procedure. Temeer daar het stelsel van normen dat moet worden aangelegd per situatie kan verschillen. Het is aan de deskundige beroepsgroep in dezen, de EDP-auditors, het stelsel van normen verder uit te bouwen en tot een nadere standaardisatie te komen.
Taak van de procespartij blijft het, haar bewijsmiddelen zodanig te presenteren, dat zij toegankelijk (in de zin van "vertrouwenwekkend") zijn voor de rechter. Enig rechterlijk inzicht in de materie is echter wel vereist; het is immers de taak van de rechter de aangedragen middelen op hun waarde te toetsen. Er zij hier nogmaals op gewezen, dat dat ook kan gelden voor een deskundigenbericht. Deskundigen kunnen duidelijkheid scheppen omtrent de betrouwbaarheidsgraad van moderne bewijsmiddelen, daar waar de kennis van de rechter tekort schiet. EDP-auditors blijken geschikt deze taak uit te voeren, mede gezien de algemeen aan hun beroepsuitoefening gestelde eis van onpartijdigheid. De rechter blijft echter de laatste beslissende instantie.

ENIG VERGELIJKEND PERSPECTIEF

In het hiernavolgende wordt nader ingegaan op enkele bijzondere onderwerpen die mogelijk kunnen bijdragen tot inzicht in de problematiek van het genereren van betrouwbaar bewijs door of met behulp van moderne technieken.

De microfilm

Hierboven werd reeds enige malen de microfilm genoemd als bewijsmiddel. Gesteld werd, dat evenals computer-output ook de microfilm slechts als bewijsmiddel met vrije bewijskracht kan dienen. Voor partijen is het ook hier van belang de film als reproduktie van het origineel zo authentiek mogelijk als bewijs in te brengen. Tegemoetkomend aan de wens van veel organisaties om in het kader van de wettelijke (fiscale) bewaarplicht hun administraties op microfilm te kunnen bewaren, heeft de staatssecretaris van Financiën in 1981 in een resolutie deze mogelijkheid geschapen. Organisaties mogen volgens deze resolutie na twee jaar hun verfilmde originelen vernietigen en de be-

lastinginspectie zal aan de authenticiteit van de verfilmingen niet twijfelen, indien aan een aantal voorschriften is voldaan. Enkele van deze voorschriften zijn:

De microverfilmingsprocedure
a. Er dienen voor het met microverfilming belaste personeel voorschriften te zijn die behelzen dat alle voor microverfilming bestemde bescheiden ook werkelijk op microfilm worden overgebracht en dat de microverfilming op zodanige wijze gebeurt dat de controle ten dienste van de belastingheffing niet moeilijker wordt dan wanneer de originele bescheiden nog aanwezig zouden zijn.

b. Tevens dienen er voor het onder a bedoelde personeel voorschriften te zijn met betrekking tot het juiste gebruik van de apparatuur, alsmede ten aanzien van de controle op volledigheid en goede kwaliteit (met name duidelijkheid) van de filmbeelden.

c. De uitvoering van de onder a en b genoemde werkzaamheden dient te blijken uit een door de ter zake verantwoordelijke functionaris op te maken en te ondertekenen verslag.

De bewaring van de microfilm
a. De microfilms moeten doelmatig worden opgeborgen en er moeten voldoende waarborgen zijn voor beveiliging tegen brand (brandvrije, althans brandvertragende kast) en andere calamiteiten.

b. Om waarborgen te hebben voor de volledigheid van het microfilmarchief dienen voorschriften te worden gegeven met betrekking tot het afgeven en terugontvangen van de microfilms. Deze voorschriften dienen te behelzen wie bevoegd is tot het opvragen van microfilms en het eventueel aanmaken van kopieën, alsmede wie bevoegd is tot het afgeven van microfilms.

Naast eisen ten aanzien van de continuïteit, die uiteraard voor de fiscus van groot belang zijn, zijn er eisen ten aanzien van de betrouwbaarheid op operationeel niveau; laatstgenoemde eisen sluiten aan op het hierboven omschreven beheersingsconcept.

De bandopname

Met een bandopname kan, evenals met de meeste digitale informatiedragers, gemakkelijk worden gemanipuleerd. Uit jurisprudentie blijkt dat onder bepaalde omstandigheden aan bandopnames bewijskracht wordt toegekend. In ieder geval dient er dan geen twijfel te bestaan omtrent de juiste weergave van hetgeen op de band is opgenomen. De rechter houdt ook hier rekening met de technische betrouwbaarheid van het toegepaste procédé en de mogelijkheid van vervalsing van de weergave van het te bewijzen feit.
Met andere woorden: naarmate de mogelijkheid van vervalsing door manipulatie kleiner wordt, neemt de betrouwbaarheid en daarmee de mogelijke bewijskracht toe.

Electronic Data Interchange (EDI)

Het toenemende gebruik van externe elektronische informatie-uitwisseling door middel van EDI is bij uitstek een ontwikkeling die de juridische wereld de nodige hoofdbrekens bezorgt. Bij gestructureerde berichtenuitwisseling van computer naar computer ontbreken zowel schriftelijke (papieren) documenten als direct menselijk handelen (en daarmee directe menselijke controle). Gebruik van EDI zal de komende jaren een steeds grotere vlucht nemen, gezien de gunstige effecten op handel en economie. Deze maatschappelijke realiteit vergt van het recht dan ook, dat er oplossingen worden gevonden voor mogelijke – internationale – juridische obstakels.

EDI levert juridisch gezien een aantal problemen op, waarvan de belangrijkste zijn:

- Hoe weet de ontvanger dat het bericht volledig, tijdig, niet verminkt en niet dubbel is ontvangen (en weet de zender dat het bericht zo is overgekomen)?

- Komt er een overeenkomst tot stand, en zo ja: op welk tijdstip en volgens welke jurisdictie?

- Is de berichtenverzending adequaat beveiligd en is de vertrouwelijkheid gewaarborgd?

- Kunnen de berichten tot bewijs van de overeenkomst c.q. van de wilsuitingen van partijen dienen, en zo ja: wat is de waarde van dit bewijs?

Wij zullen in dit artikel niet op alle bovenstaande problemen ingaan, maar ons beperken tot behandeling in het kader van het bewijsprobleem.

Wetgeving
Nederlandse wetgeving van toepassing op elektronische berichtenuitwisseling ontbreekt nagenoeg geheel. Dit wordt veroorzaakt door de reeds eerder in dit artikel gesignaleerde "huiverigheid" ten aanzien van automatiseringsontwikkelingen waar het betreft de juridische consequenties. Naar onze mening dient wetgeving op dit gebied echter ook in een meer internationaal verband tot stand te worden gebracht, gezien de internationale verwevenheid van de problematiek. Vanuit Nederland wordt er actief deelgenomen aan de activiteiten die de Europese Commissie op het gebied van de ontwikkeling en beheersing van EDI heeft ondernomen, het TEDIS-project.

Controle en certificering door een derde-onafhankelijke partij, die aan professionele regels is gebonden en ter zake kundig is, zullen voor de rechter belangrijke "handvatten" kunnen zijn bij de waardering van elektronisch bewijs.

Eén van de uitkomsten van de juridische werkgroep van TEDIS is tot nu toe een ontwerp-overeenkomst voor (internationale) EDI-projecten, een zogenaamd Interchange Agreement. Vanwege de verschillen in wetgeving tussen de diverse Europese landen dan wel het ontbreken van adequate regelgeving dienen partijen zelf met elkaar af te spreken op welke wijze en onder welke voorwaarden zij door middel van EDI met elkaar zullen handelen. Dit Interchange Agreement is gebaseerd op de "Uniform Rules of Conduct for the Interchange of Trade Data by Teletransmission" (UNCID) van de Internationale Kamer van Koophandel.

Interchange Agreement
Onderdeel van een Interchange Agreement is de bewijsovereenkomst, die in dit artikel reeds is besproken. Ook dient in de overeenkomst te worden afgesproken welke beveiligingsmethode en -maatregelen worden gehanteerd en hoe identificatie van zender en ontvanger dient plaats te vinden om de vertrouwelijkheid en betrouwbaarheid van het berichtenverkeer te waarborgen. Opgemerkt zij, dat hier eveneens een belangrijke rol lijkt weggelegd voor de derde-aanbieder van de VAN (Value Added Network)-diensten, waar EDI-partijen veelal gebruik van zullen maken. Partijen bij een EDI-overeenkomst dienen zich er steeds van te vergewissen, dat de VAN-aanbieder dezelfde hoge maatstaven aanlegt ten aanzien van de beveiliging van het netwerk, zowel fysiek als logisch. De UN-CID-code legt deze derde in dit kader een zorgplicht op. De controle op deze betrouwbaarheid en vertrouwelijkheid van het netwerk is voor EDI-partners niet alleen belangrijk in het kader van hun bedrijfsvoering, zij is eveneens een instrument om de bewijskracht van EDI-berichten in een procedure te versterken. Partijen kunnen in dat kader ook afspreken, dat zij periodiek een onafhankelijke auditor een onderzoek zullen laten uitvoeren.

Elektronische notaris?
Bij het versterken van de bewijspositie past ook het zoeken naar een methode die als elektronische vervanger kan dienen voor de traditionele methoden om de authenticiteit van bewijs aan te tonen. Gedacht wordt hierbij onder andere aan een "elektronisch equivalent" van de "notary public", de notaris. Met name in de Anglo-Amerikaanse jurisdictie is dit aspect van belang, wil men niet-schriftelijk bewijs inbrengen in een procedure. Al speelt dit laatste zoals we gezien hebben niet in Nederland, voor de bewijskracht van computermateriaal heeft een dergelijke methode wel degelijk zin. De notaris speelt van oudsher immers een belangrijke rol in het verzekeren van de betrouwbaarheid van papieren documenten. Onderzoek is er nu op gericht de notaris deze rol ook te laten spelen in de authenticatie of certificering van elektronische documenten.
Afgezien van de mogelijke (internationale) juridische barrières die de wetgeving met betrekking tot het notarisambt kan opwerpen, stelt dit uiteraard de nodige eisen aan de "elektronische bedrijfsvoering" van de notarissen. De problematiek is hier gelijk aan die van de betrouwbaarheid en vertrouwelijkheid bij gebruik van computernetwerken in het algemeen zoals hier aangegeven.
Controle en certificering door een derde-onafhankelijke partij, die aan professionele regels is gebonden en ter zake kundig is, zullen voor de rechter echter belangrijke "handvatten" kunnen zijn bij de waardering van elektronisch bewijs.

SAMENVATTING

Alhoewel geautomatiseerde gegevensverwerking met grote vaart doordringt in de huidige samenleving, is het gebruik ervan in het civiele proces bewijsrechtelijk gezien nog een probleem.
De wet hanteert een open systeem van bewijsmiddelen, maar aan de andere kant is de rechter vrij in zijn waardering van het aangedragen bewijsmateriaal. Op dat moment worden de partijen afhankelijk van de rechter: zijn overtuiging is beslissend. Daar liggen de problemen voor het gebruik van computermateriaal als middel van bewijs. De kennisachterstand binnen de rechterlijke macht leidt ertoe dat de rechter de wereld van de geautomatiseerde gegevensverwerking ervaart als ondoorzichtig. Dit heeft een ongunstig effect op de bewijswaardering door de rechter: hij neemt een afwachtende houding aan, wat meestal leidt tot onderschatting van de bewijskracht van het materiaal als bewijsmiddel of tot een onvoorwaardelijke acceptatie van deskundigenberichten. In wezen loopt de juridische wereld en meer in het bijzonder de rechterlijke macht hiermee achter de maatschappelijke feiten aan.

In dit artikel is getracht de problematiek van de moderne bewijsmiddelen in kaart te brengen en aandachtspunten te geven ten behoeve van de waardering van dat bewijs. De aandachtspunten zijn zowel gericht tot de rechter, die de uiteindelijke verantwoordelijkheid draagt voor een uitspraak op basis van het aangedragen bewijs, als tot de (potentiële) procespartij, die haar bewijsrechtelijke kansen op succes wenst in te schatten.
Het is aan de beroepsgroep die zich bezighoudt met de kwaliteit van de informatievoorziening en van informatiesystemen deze aandachtspunten nadere invulling te geven, onder andere door een verdergaande standaardisatie van het te hanteren stelsel van normen.

LITERATUUR

[Ball90] G.L. Ballon, *Het bewijs en de moderne technieken*, in Computerrecht 1990/5.

[Blen90] *Making Paperless Trade Legally Secure*, Proceedings van de conferentie "EDI and the LAW", Blenheim Online, 1990.

[Drap90] J. Draper, *Security, integrity and legality - barriers to EDI progress in Europe?*, in Update on Computer Audit, Control and Security, volume 2 number 3, 1990.

[Elde90] J.L.M. Elders, *Waardering van bewijs*, Deventer 1990.

[Erke85] C. Erkelens, *Computercriminaliteit en het begrip "vermogensdelict"*, in Soft- en hard-, ware het niet om de fraude, Antwerpen 1985.

[Esch91] R. van Esch, *De UNCID-code*, in Hoofdstukken Informaticarecht, Alphen aan den Rijn, 1991.

[Graa89] F. de Graaf, *Bewijsrecht en bewaarplichten in een geautomatiseerde omgeving*, in Hoofdstukken Informaticarecht, Alphen aan den Rijn 1989.

[Graa90] F. de Graaf e.a., *Juridische aspecten van netwerken*, rapport van de Nederlandse Vereniging voor Informatica en Recht, 1990.

[Hijm90] J. Hijma en M.M. Olthof, *Compendium van het Nederlands vermogensrecht*, 4e druk, Deventer 1990.

[Kock90] H.C. Kocks, *Inzicht in samenhang*, collegedictaat post-doctorale opleiding EDP- auditing EUR, Rotterdam 1990.

[Meij88] P.A.M. Meijknecht, *Kennismaking met het Burgerlijk Procesrecht*, Zwolle 1988.

[NIVR89] *Automatisering en controle, deel VII. Kwaliteitsoordelen over informatievoorziening*, NIVRA-geschrift 53, Deventer 1989.

[Smit85] J. Smits, *Het recht uitgedaagd door de computer*, Deventer/Zwolle 1985.

[TEDI89] *The Legal Position of the Member States with respect to Electronic Data Interchange*, TEDIS Final Report, Europese Commissie, 1989.

Mw. mr. I.M.A. de Graaf-Hinfelaar
Is in 1990 afgestudeerd aan de juridische faculteit van de Katholieke Universiteit van Brabant op het in dit artikel behandelde onderwerp. Momenteel is zij werkzaam bij Loeff Claeys Verbeke, advocaten en notarissen te Rotterdam. Haar werkzaamheden zijn gericht op het automatiseren van de kennis van de sectie Vennootschapsrecht en het ondersteunen van de notariële afdeling.

Mw. mr. A.M.Ch. Kemna MBA
Studeerde rechten aan de Universiteit van Nijmegen en post-doctoraal bedrijfskunde (Master of Business Administration) aan de Rotterdam School of Management, Erasmus Universiteit Rotterdam. Zij werkt sinds 1989 als adviseur informaticarecht bij KPMG Klynveld EDP Auditors. Haar aandachtsgebied omvat de juridische aspecten van automatisering en de connectie met EDP-auditing. Anne-Marie Kemna is betrokken bij een breed scala van consulting en auditing-activiteiten.

Praktische problemen van organisaties bij de implementatie van de Wet Persoonsregistraties

Ir. B.A.W.M. Bruns

De Wet Persoonsregistraties (WPR) heeft administratief-organisatorische gevolgen voor vrijwel elke organisatie. Een EDP-auditor kan de kwaliteit van getroffen privacy-maatregelen toetsen. Kennis van de WPR is hiervoor noodzakelijk. Hoe kan deze wet nu echter praktisch worden ingevuld?
Schrijver zet vanuit zijn EDP-audit- en bedrijfskundige achtergrond de problematiek uiteen.

INLEIDING

De volledige invoering van de Wet Persoonsregistraties is op 1 juli 1990 een feit geworden. Voor organisaties die persoonsregistraties voeren, houdt dit in dat ze vanaf die datum volledig moeten voldoen aan de eisen die de WPR stelt. De organisatie die de zeggenschap heeft over een persoonsregistratie (de houder[1]), is verantwoordelijk en aansprakelijk voor de consequenties die voortvloeien uit het niet-naleven van de WPR (onder andere geldboetes en schadevergoedingen aan geregistreerden die schade hebben geleden door het niet-naleven van de WPR). De WPR vormt een externe invloed op organisaties die – afhankelijk van de aard van de organisatie – de bedrijfsvoering aanzienlijk kan beïnvloeden.

De WPR heeft het karakter van een raamwet. De eisen zijn in globale termen gesteld; organisaties moeten ze zelf verwerken in hun beleid en verder invullen met organisatorische en technische maatregelen (zelfregulering). Daarnaast speelt het feit dat de wet pas relatief kort geheel in werking is, een rol; het referentiekader dat gewoonlijk door jurisprudentie wordt verzorgd, is nog vrij beperkt. De uitvoerige behandeling van de WPR in de Eerste en Tweede Kamer heeft wel meer inzicht verschaft in de inhoud en reikwijdte van in de wet gebruikte termen. Interpretatieproblemen blijven echter nog steeds bestaan. Bij de praktische invulling van de eisen van de WPR stuiten organisaties hier regelmatig op.

Dit artikel tracht de problematiek met betrekking tot de implementatie van de WPR in kaart te brengen aan de hand van een analyse van de communicatiekanalen die door de WPR worden gereguleerd. Als invalshoek bij die analyse is de positie van de persoonsregistraties voerende organisatie gekozen.

IDENTIFICATIE AANDACHTSGEBIEDEN

De doelstelling van de Wet Persoonsregistraties is het beschermen van de persoonlijke levenssfeer van geregistreerde personen. De wet probeert deze doelstelling te bereiken door de communicatie van en over persoonsregistraties te reguleren met de volgende maatregelen:
- het stellen van eisen ten aanzien van de verspreiding van persoonsgegevens;
- het stellen van eisen om de juistheid en de volledigheid van de opgenomen persoonsgegevens te bevorderen;
- het stellen van eisen ten aanzien van de bekendheid van het bestaan en de wijze van gebruik van persoonsregistraties.

Verspreiding van persoonsgegevens
Persoonsgegevens kunnen zowel binnen als buiten de organisatie worden verspreid. Een definitie van het begrip organisatie (van de houder) zal de lezer niet vinden in de wet. Toch is dit begrip van essentieel belang voor de invulling van de WPR. Het begrip organisatie van de houder kan in het kader van de WPR als volgt worden afgebakend: alle medewerkers en organisatorische eenheden die onder de hiërarchische verantwoordelijkheid van de houder vallen. Deze betekenis kan derhalve afwijken van de gangbare organisatiekundige betekenis van functionele eenheid (die in dit artikel wordt gehanteerd). Vooral binnen grote organisaties is het vaststellen van het houderschap in relatie tot de definitie van de organisatie van belang. Hierop zal later in dit artikel nader worden ingegaan.

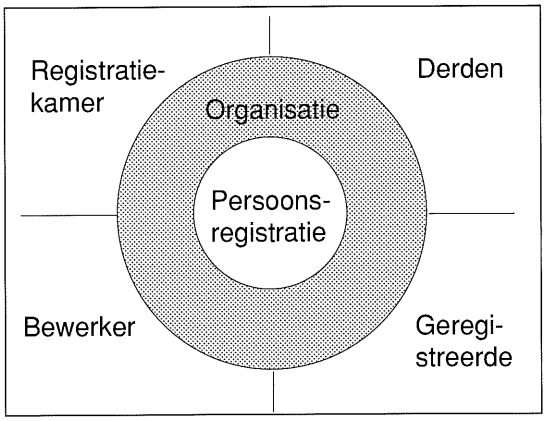
Verspreiding van persoonsgegevens duidt de wet aan als "verstrekkingen". De WPR heeft zowel betrekking op interne als op externe verstrekkingen. Als externe belanghebbenden zijn te onderscheiden de geregistreerden en derden. Binnen de organisatie in functionele zin zijn te onderscheiden de functionarissen die uit hoofde van hun functie gebruik maken van de gegevens uit de registraties en de functionarissen die de persoonsregistraties bewerken en bewaren. Als de laatstgenoemde functionarissen buiten de organisatie van de houder (in termen van de WPR) vallen, spreekt de wet van "bewerker"[2].

Juiste en volledige gegevens
Aangezien onjuistheden en onvolledigheden in persoonsgegevens kunnen leiden tot schade aan de persoonlijke levenssfeer van geregistreerden, stelt de WPR eisen ter bevordering van de juistheid en de volledigheid van de opgenomen persoonsgegevens. De geregistreerden krijgen expliciet rechten waarmee zij de juistheid en de volledigheid van hun persoonsgegevens kunnen controleren en afdwingen. Tevens is de organisatie verplicht zich in te spannen voor de juistheid en volledigheid van de persoonsgegevens.

Bekendheid
De derde wijze waarop de WPR de doelstelling probeert te realiseren, is de bekendheid van het bestaan en de wijze van gebruik van persoonsregistraties te bevorderen. Organisaties moeten hun persoonsregistraties aanmelden bij de bij wet ingestelde Registratiekamer. De aanmelding van een registratie moet worden aangekondigd en bij de organisatie ter inzage liggen voor belanghebbenden. Tevens moet de organisatie een geregistreerde in principe op de hoogte stellen van eerste opname in een persoonsregistratie. Deze maatregelen beogen het bestaan en de wijze van gebruik van een persoonsregistratie bekendheid te geven bij geregistreerden.

SAMENVATTING PARTIJEN WPR

Sinds 1 juli 1990 is de Wet Persoonsregistraties volledig operationeel. De bescherming van de persoonlijke levenssfeer die de wet nastreeft, is van invloed op de bedrijfsvoering van organisaties die persoonsregistraties voeren. De WPR tracht haar doelstelling te bereiken door eisen te stellen aan de communicatie over persoonsgegevens en persoonsregistraties:
- binnen de organisatie;
- tussen organisatie en de Registratiekamer;
- tussen organisatie en derden;
- tussen organisatie en geregistreerden;
- tussen organisatie en eventuele bewerker.



Figuur 1. Communicatiekanalen op basis van de WPR.

Een en ander is in figuur 1 schematisch weergegeven. Het vervolg van dit artikel zal worden gepresenteerd aan de hand van de communicatiekanalen die hierboven zijn genoemd.

COMMUNICATIEKANALEN BINNEN DE ORGANISATIE

De eisen die de WPR stelt aan communicatie over persoonsgegevens binnen de organisatie, zijn beschreven in de algemene bepalingen van de wet. Opgemerkt moet worden, dat ook de eisen die de

1 Definitie "houder" uit artikel 1 WPR: degene die de zeggenschap heeft over een persoonsregistratie.

2 Definitie "bewerker" uit artikel 1 WPR: degene die het geheel of een gedeelte van de apparatuur onder zich heeft, waarmee een persoonsregistratie waarvan hij niet de houder is, wordt gevoerd.

WPR stelt aan de communicatie tussen de organisatie en derden, gevolgen kunnen hebben voor de interne organisatie van de houder. De belangrijkste onderwerpen zijn hierbij de beveiliging van de registratie en de zorg voor de juistheid en de volledigheid van de gegevens. Deze onderwerpen zullen derhalve in deze paragraaf worden behandeld.

Een drietal in de praktijk gesignaleerde problemen komt hier aan de orde. De eerste twee problemen hebben betrekking op de interpretatie van bepaalde artikelen uit de wet (art. 8 en art. 49 lid 1: beveiligingsplicht, en art. 5: zorgplicht); het derde probleem ontstaat doordat de interne organisatie ofwel (nog) niet bestaat (eisen aan communicatie met externen) ofwel niet aansluit bij de eisen van de WPR (doelbinding uit de artt. 5 en 6).

Welk niveau van beveiliging eist de WPR?

Om ongecontroleerde verspreiding van persoonsgegevens tegen te gaan en de juistheid en volledigheid te bevorderen stelt de WPR in artikel 8 dat de houder zorg moet dragen voor de nodige voorzieningen van technische en organisatorische aard ter beveiliging van een persoonsregistratie tegen verlies of aantasting van de gegevens en tegen onbevoegde kennisneming, wijziging of verstrekking daarvan. Voor de bewerker geldt dezelfde plicht voor het gedeelte van de apparatuur dat hij onder zich heeft, waarmee de registratie wordt gevoerd.

De interpretatie van de beveiligingsplicht is in de literatuur een heet hangijzer. De een gaat uit van het feit dat een absolute beveiliging wordt bedoeld (in de praktijk onmogelijk), terwijl de ander ervan uitgaat dat het artikel naar redelijkheid van de situatie moet worden geïnterpreteerd. Voor organisaties vormt de verwarring omtrent de beveiligingsplicht derhalve een probleem.

Duidelijk is wel dat de beveiligingsplicht voor organisaties een externe invloed op hun beveiligingsbeleid vormt. Tot voor kort bepaalde het interne bedrijfsbeleid in belangrijke mate het beveiligingsbeleid. De beveiliging van bedrijfseigendommen was de belangrijkste doelstelling. Momenteel vormen externe invloeden als de WPR (beveiligingsplicht) en de in aantocht zijnde Wet Computercriminaliteit (binnendringen in een onbeveiligd computersysteem is niet strafbaar) steeds meer een factor van betekenis. Heroverweging van het beveiligingsbeleid is derhalve noodzakelijk voor organisaties. Ook voor EDP-auditors is deze constatering van belang: ten aanzien van de beoordeling van het kwaliteitsaspect vertrouwelijkheid dient rekening te worden gehouden met deze wettelijke, externe vereisten bij het opstellen van de toetsingsnormen.

Welk intern gebruik van persoonsgegevens staat de WPR toe?

Organisaties leggen (persoons)registraties aan om hun bedrijfsprocessen te ondersteunen. De WPR legt aan het interne gebruik van persoonsregistraties beperkingen op om de informationele privacy van de geregistreerden te beschermen. Twee delen van de wet die betrekking hebben op intern gebruik zijn artikel 6 lid 2 (taakbinding[3]) en artikel 5 lid 2 (zorgplicht[4]).
De taakbinding houdt in dat binnen de organisatie slechts persoonsgegevens worden verstrekt aan functionarissen die ingevolge hun taak die gegevens mogen ontvangen. De strekking van de taakbinding is duidelijk en gezien het feit dat veel organisaties het principe "informatie naar behoefte" toepassen, levert de taakbinding weinig problemen op.
De interpretatie van het artikel over de zorgplicht veroorzaakt meer onduidelijkheden. Onduidelijk is welke voorzieningen de organisatie moet treffen om de juistheid en volledigheid van de persoonsgegevens voldoende te verzorgen. Uit jurisprudentie zal moeten blijken wanneer organisaties voldoen aan de door de WPR geëiste inspanningsverplichting.

De taakbinding, de zorgplicht en de beveiligingsplicht hebben als gemeenschappelijk doel te bewerkstelligen dat persoonsgegevens binnen de organisatie worden behandeld met zorgvuldigheid en onder geheimhouding. Deze "privacy-mentaliteit" is niet in alle organisaties aanwezig. Afhankelijk van de cultuur van de organisatie kan de invoering van de benodigde mentaliteitsverandering moeizaam verlopen.

Is aanpassing van de interne organisatie nodig?

De restricties die de WPR oplegt aan het interne gebruik van persoonsregistraties, hebben in sommige organisaties tot gevolg dat de huidige werkwijze aanpassing dan wel aanscherping behoeft. Vooral de doelbinding uit artikel 5 lid 1[5] en artikel 6 lid 1[6] formaliseert de restricties aan het gebruik van persoonsregistraties, die voorheen slechts waren gebaseerd op jurisprudentie.
De eisen die de WPR stelt aan de communicatie tussen organisatie en externen, vragen daarnaast om uitbreiding van de interne organisatie. Om te voldoen aan de eisen zijn veelal nieuwe procedures nodig.

Aanpassing en uitbreiding van de interne organisatie kan op weerstand stuiten binnen de organisatie. Problemen bij de verandering en uitbreiding van de interne organisatie zijn echter niet specifiek voor de invoering van de WPR. In dit artikel zal hierop dan ook niet nader worden ingegaan.

Conclusie

De WPR stelt eisen aan het gebruik van persoonsregistraties (en de gegevens erin) binnen organisaties. Voor een deel zijn deze eisen globaal gesteld en zal de organisatie ze "naar eer en geweten" moeten invullen op basis van de beschikbare wetgeving, jurisprudentie en literatuur (onder andere kamerstukken). Aanpassing en uitbreiding van de interne organisatie kan een gevolg zijn. Tevens beoogt de WPR een privacy-mentaliteit te bewerkstelligen. De implementatie van de wet kan binnen

3 *Artikel 6 lid 2: Binnen de organisatie van de houder worden uit een persoonsregistratie slechts gegevens verstrekt aan personen die ingevolge hun taak die gegevens mogen ontvangen.*

4 *Artikel 5 lid 2: De houder treft de nodige voorzieningen ter bevordering van de juistheid en de volledigheid van de opgenomen persoonsgegevens.*

5 *Artikel 5 lid 1: Een persoonsregistratie bevat slechts gegevens die rechtmatig zijn verkregen en in overeenstemming zijn met het doel waarvoor de registratie is aangelegd.*

6 *Artikel 6 lid 1: De opgenomen persoonsgegevens worden slechts gebruikt voor doeleinden die met het doel van de persoonsregistratie verenigbaar zijn.*

de organisatie dus zowel organisatorische als mentaliteitsvraagstukken opleveren.

COMMUNICATIE TUSSEN ORGANISATIE EN REGISTRATIEKAMER

De communicatie tussen de organisatie en de Registratiekamer bestaat voornamelijk uit het aanmelden van persoonsregistraties en het wijzigen van eerdere aanmeldingen. Daarnaast beantwoordt de Registratiekamer vragen van organisaties omtrent de WPR en controleert zij naleving van de wet.

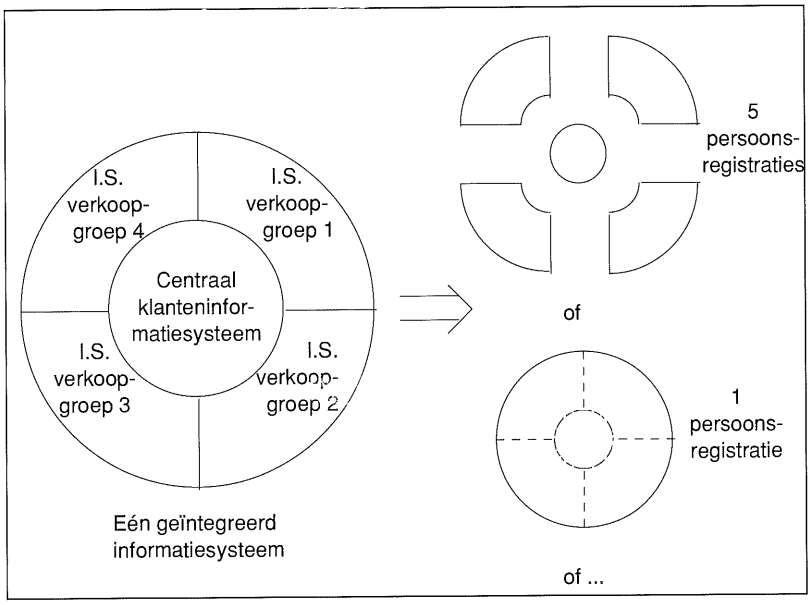
Momenteel vergt voornamelijk de communicatie van organisaties richting de Registratiekamer de aandacht. In principe moet het bestaan van een persoonsregistratie volgens de artikelen 19 en 24 worden aangemeld bij de Registratiekamer (meldingsplicht). Aanmelden van persoonsregistraties en wijzigen van aanmeldingen gebeuren met door de wet vastgestelde - en bij Algemene Maatregel van Bestuur nader gespecificeerde - reglementen en formulieren. Reglementen zijn volgens de wet van toepassing voor "persoonsregistraties op het gebied van de overheid en het onderwijs, de gezondheidszorg en de maatschappelijke dienstverlening"; formulieren voor "persoonsregistraties op het gebied van bedrijf en beroep en op overige gebieden".

In de reglementen en formulieren moeten organisaties met name beschrijven:
- wie verantwoordelijk is voor de persoonsregistratie;
- wat het doel van de persoonsregistratie is;
- wat de inhoud van de persoonsregistratie is;
- hoe de persoonsregistratie werkt.

Bij het aanmelden van persoonsregistraties en het wijzigen van aanmeldingen kan een aantal problemen optreden. Hieronder volgt er een drietal dat in de praktijk regelmatig wordt gesignaleerd.

Wat is een persoonsregistratie?

Het begrip persoonsregistratie is in de WPR omschreven als een samenhangende verzameling van op verschillende personen betrekking hebbende persoonsgegevens, die langs geautomatiseerde weg wordt gevoerd of met het oog op een doeltreffende raadpleging van die gegevens systematisch is aangelegd. In de kamerstukken en de overige literatuur over dit onderwerp is het begrip nader toegelicht. In de praktijk levert de interpretatie echter nog wel eens problemen op, vooral wanneer het (deels) handmatige registraties betreft. Het definiëren van omvang en inhoud van een persoonsregistratie laat de WPR over aan de houder (binnen de grenzen van de wet). Wanneer de houder echter meerdere persoonsregistraties voert, die zijn gekoppeld en geïntegreerd – zoals in moderne informatiesystemen gebruikelijk is –, dan kan het opdelen van de geïntegreerde informatiesystemen in afzonderlijk aan te melden persoonsregistraties problematisch worden.



Figuur 2. Het opdelingsprobleem.

Als voorbeeld kan worden gedacht aan een verkooporganisatie met meerdere produktgroepen. De organisatie heeft een geïntegreerd informatiesysteem met een gezamenlijk klanteninformatiesysteem en voor elke verkoopgroep een eigen verkoopsysteem, dat gebruik maakt van (een deel van) het klanteninformatiesysteem (zie figuur 2). Bestaat het geïntegreerde systeem uit één of vijf persoonsregistraties of zijn nog andere opdelingen mogelijk? De oplossing zal steeds per geval moeten worden gevonden. Zij is onder andere afhankelijk van een mogelijke vrijstelling voor delen van de registratie.

Is aanmelding van de persoonsregistratie verplicht?

Alle persoonsregistraties die niet zijn uitgezonderd in artikel 2 van de WPR of tijdelijk uitgezonderd op basis van artikel 54, vallen onder het regime van de WPR. Aanmelding bij de Registratiekamer is echter niet in alle gevallen noodzakelijk. In de artikelen 22 en 27 van de WPR wordt de mogelijkheid geschapen bepaalde - bij Algemene Maatregel van Bestuur nader vast te stellen - persoonsregistraties vrij te stellen van de aanmeldingsplicht. In het "Besluit genormeerde vrijstelling" van 2 januari 1990 zijn de voorwaarden voor vrijstelling nader uitgewerkt.

De genormeerde vrijstelling is bedoeld voor persoonsregistraties die veel voorkomen, daardoor een zeker standaardkarakter hebben en waarvan het bestaan en de werking bij de geregistreerden doorgaans wel bekend is. De voorwaarden voor vrijstelling hebben betrekking op:
- de soort persoonsregistratie;
- de inhoud van de persoonsregistratie;
- het doel van de persoonsregistratie;

- de werking van de persoonsregistratie (onder meer de verstrekkingen).

Bij de interpretatie van de voorwaarden en daarmee bij de bepaling of een persoonsregistratie onder de genormeerde vrijstelling valt, worden in de praktijk regelmatig fouten gemaakt. Met name de normering van het doel en de werking veroorzaken interpretatieproblemen. Vaak worden de wettelijke bepalingen onvoldoende zorgvuldig beoordeeld.

Een voorbeeld van dit laatste is de misinterpretatie die een financiële dienstverlenende organisatie deed. De vrijstelling van de debiteurenadministratie werd verondersteld op basis van het "Besluit genormeerde vrijstelling" (art. 9: "Boekhoudingen of daarmee gelijk te stellen administraties van debiteuren en crediteuren"). Op het eerste gezicht leek deze administratie inderdaad te zijn vrijgesteld. In lid 2 van het desbetreffende artikel is het doel van de vrijgestelde registraties echter zodanig ingeperkt dat de debiteurenadministratie van de voorbeeldorganisatie niet zou zijn vrijgesteld. De organisatie had dit over het hoofd gezien. Gevolg: verzaking van de meldingsplicht.

Bij de interpretatie van de voorwaarden en daarmee bij de bepaling of een persoonsregistratie onder de genormeerde vrijstelling valt, worden in de praktijk regelmatig fouten gemaakt.

Hoe moet de aanmelding geschieden?

Indien aanmelding van een persoonsregistratie verplicht is, dient de houder hiertoe een formulier c.q. reglement in te vullen. De bescheiden (het formulier of het beperkte formulier voor aanmelding van een zelfgemaakt reglement) zijn bij de Registratiekamer te verkrijgen. Bij het invullen van de aanmeldingsbescheiden realiseert de houder zich regelmatig dat de in het formulier gewenste informatie niet beschikbaar of niet voldoende expliciet is (bijvoorbeeld het doel van de registratie). Het ontwikkelen van de gewenste informatie stuit vervolgens vaak op problemen, omdat men geen inzicht heeft in de (wettelijke) consequenties van de informatie. Hieronder is een aantal aandachtspunten beschreven dat tot verwarring kan leiden.

Struikelblokken
Een eerste struikelblok bij het invullen van een formulier c.q. reglement is dat deze bescheiden termen bevatten die een speciale betekenis hebben en niet intuïtief duidelijk zijn (houder, verstrekking, etc.). De verwarring die hierdoor kan ontstaan, hebben de opstellers voorzien. Een toelichting is aanwezig bij het formulier. Gebruik hiervan kan een aantal misverstanden en vragen voorkomen.

In het reglement moet worden aangegeven wie de houder van de persoonsregistratie is. Zoals eerder is gesteld, bepaalt het houderschap de omvang van de organisatie van de houder en daarmee wie derde is. In grote organisaties (denk bijvoorbeeld aan een holding met werkmaatschappijen) zou het houderschap op topniveau (holding) kunnen worden gelegd, maar ook op een lager niveau (bijvoorbeeld bij een werkmaatschappij).
Het bedrijfsleven is over het algemeen voorstander van houderschap op het hoogste niveau, omdat dit de beperkingen bij en de kosten van het voeren van een persoonsregistratie vermindert (denk onder andere aan verstrekkingen en vrijstellingen). De Registratiekamer is echter van mening dat voor een goede privacy-bescherming het houderschap (zo mogelijk) op een lager niveau hoort te liggen. Deze controverse is momenteel nog niet opgelost. Voor grote organisaties is een goede afweging derhalve van groot belang.

Een belangrijk punt bij het invullen van een aanmelding is de doelomschrijving. Gebruik van persoonsgegevens voor doeleinden die niet verenigbaar zijn met de doelomschrijving, is volgens de WPR niet toegestaan. Voor een flexibel gebruik van persoonsregistraties is het derhalve van belang de doelomschrijving goed te overwegen, zodat deze niet te nauw is voor het uitvoeren van bestaande of toekomstige activiteiten.
Anderzijds moet de doelomschrijving ook niet te ruim zijn. Op grond van artikel 31 (correctierecht geregistreerde) van de WPR kan de geregistreerde de organisatie bij een te ruime doelomschrijving verzoeken aanvullende gegevens op te nemen in de persoonsregistratie omdat de gegevens gezien de doelstelling onvolledig zouden zijn. Zo'n verzoek tot opname van extra gegevens kan bij een volledig geautomatiseerde persoonsregistratie problemen veroorzaken en is vanuit de organisatie gezien over het algemeen niet gewenst (anders waren de gegevens immers reeds opgenomen).

Om redenen van economische aard en flexibiliteit is een goede (her)overweging van de doelomschrijving van een persoonsregistratie derhalve van belang.

Aanpassing interne procedures?
In de aanmelding dient de organisatie vast te leggen hoe de persoonsregistratie werkt. Daartoe moet worden bepaald:
- welke categorieën personen worden geregistreerd;
- hoe de persoonsgegevens worden verkregen;
- welke functionarissen binnen de organisatie toegang hebben tot welke gegevens;
- onder welke voorwaarden welke gegevens worden verstrekt aan derden;
- welke verbanden de persoonsregistratie heeft met andere registraties.

Bij invulling van het formulier of reglement blijkt soms dat deze zaken binnen de organisatie niet volledig duidelijk zijn of niet geheel in de lijn van de doelomschrijving liggen. Aanpassing van de interne procedures omtrent de persoonsregistratie is in die gevallen noodzakelijk.

Opgemerkt dient te worden dat volgens de artikelen 19 en 25 van de WPR elke wijziging in een formulier of reglement dient te worden gemeld aan de Registratiekamer, bekend te worden gemaakt aan geregistreerden en ter inzage te worden gelegd voor belanghebbenden. Deze onderhoudsgevoeligheid kan voor de organisatie een reden zijn de persoonsregistratie zodanig in te richten dat deze onder een (genormeerde) vrijstelling valt.

Conclusie

Zoals uit de geschetste problemen blijkt, is communicatie met de Registratiekamer moeilijker dan het op het eerste gezicht lijkt. Evalueren, uitvoeren en onderhouden van de aanmeldingsplicht doe je niet "even". Het vereist ten eerste een zorgvuldige voorbereiding en (her)overweging en ten tweede een goede interne organisatie.

COMMUNICATIE TUSSEN DE ORGANISATIE EN DERDEN

Voor het verstrekken van gegevens aan derden zal de organisatie over het algemeen een beweegreden hebben. Structurele (periodieke) verstrekkingen zullen plaatsvinden in het kader van de bedrijfsvoering (bijvoorbeeld het aanmelden van nieuwe personeelsleden bij een bedrijfsgezondheidsdienst).
Bij incidentele verstrekkingen (indien het een niet voorziene uitzonderingssituatie betreft) zal een verzoek van een derde de beweegreden vormen voor de verstrekking.

De WPR maakt bij derdenverstrekkingen onderscheid tussen organisaties die bedrijfsmatig persoonsgegevens verzamelen en verstrekken (art. 13), en organisaties die andere redenen daarvoor hebben (artt. 11, 12, 14 en 18). Hier wordt slechts ingegaan op de laatste categorie.
Onder het bewind van de WPR mogen slechts persoonsgegevens worden verstrekt om de volgende redenen:

- De verstrekking valt binnen de doelomschrijving van de persoonsregistratie.
- De geregistreerde geeft toestemming voor de verstrekking.
- De verstrekking is wettelijk verplicht.
- De persoonsgegevens worden verstrekt ten behoeve van wetenschappelijk onderzoek of statistiek dan wel om een dringende andere reden en de persoonlijke levenssfeer van de geregistreerde wordt niet onevenredig geschaad.
- De verstrekking omvat slechts gegevens benodigd voor communicatie.

De eisen die de WPR stelt aan derdenverstrekkingen, zijn – waarschijnlijk mede door de doelstelling van de wet – vrij eenduidig interpreteerbaar. De implementatie in de organisatie is echter nadere aandacht waard.

Wanneer verstrekken we persoonsgegevens aan derden?

Structurele verstrekkingen aan derden kan de organisatie mogelijk maken door de verstrekking op te nemen in de doelomschrijving van de persoonsregistratie. Voor dergelijke verstrekkingen is dan geen toestemming van de geregistreerde nodig.

Voor incidentele verstrekkingen is het van belang het verzoek van de derde te toetsen aan de eisen van de wet. Bij een beperkt aantal verzoeken kan een functionaris worden geïnstrueerd de verzoeken op dat punt te beoordelen. Bij grotere aantallen verzoeken zullen meerdere functionarissen moeten worden ingeschakeld. Een eenduidig beleid ten aanzien van verstrekkingen is dan van belang. In deze situatie is het zinvol de eisen van de wet nader uit te werken in richtlijnen voor derdenverstrekkingen.

De organisatie is volgens artikel 32 verplicht te registreren aan wie gedurende het laatste jaar persoonsgegevens zijn verstrekt (protocolplicht). De geregistreerden kunnen inzicht in het protocol verlangen. Als een geregistreerde gebruik maakt van zijn correctierecht, is de organisatie volgens artikel 35 tevens verplicht de wijzigingen door te geven aan derden aan wie gedurende het laatste jaar gegevens zijn verstrekt. Het mag duidelijk zijn dat de protocolplicht voor de organisatie veel extra werk kan inhouden. De definitie van het houderschap (waaruit voortvloeit wie derde is) is mede hierom belangrijk en kan de hoeveelheid werk in verband met de protocolplicht sterk beïnvloeden.

Conclusie

De problemen bij de communicatie tussen de organisatie en derden zijn gering omdat de wet in dezen vrij duidelijk is. Afhankelijk van het karakter van de verstrekkingen (structureel/incidenteel) en de hoeveelheid verzoeken bestaan er verschillende mogelijkheden voor de inrichting van de communicatie tussen de organisatie en derde.

COMMUNICATIE TUSSEN DE ORGANISATIE EN GEREGISTREERDE

De communicatie tussen de organisatie en geregistreerden wordt door de WPR gereguleerd om de geregistreerden in staat te stellen de juistheid en volledigheid van de opgenomen persoonsgegevens te controleren en af te dwingen. Hiertoe moet de geregistreerde het bestaan van de persoonsregistratie kennen en de middelen hebben om zijn gegevens in de registratie te beïnvloeden. De WPR regelt deze zaken door plichten op te leggen aan de organisatie en expliciet rechten toe te kennen aan de geregistreerden.

De organisatie is verplicht het bestaan van (niet-vrijgestelde) persoonsregistraties kenbaar te maken aan geregistreerden door het bekend maken en

ter inzage leggen van het formulier c.q. reglement (art. 24 respectievelijk art. 19). Tevens dient de organisatie aan de geregistreerde te melden dat deze voor de eerste maal is opgenomen in de registratie, tenzij de geregistreerde de opname redelijkerwijs kon weten (art. 28). Deze twee plichten van de organisatie dienen te waarborgen dat de geregistreerden op de hoogte zijn van het feit dat ze zijn geregistreerd, van het doel van de registratie en van de werking ervan.

Inzage- en correctierecht
Om het de geregistreerde mogelijk te maken zijn gegevens in een registratie te beïnvloeden voorziet de WPR in een inzagerecht (art. 29), recht tot kennisname van de gedane incidentele verstrekkingen (art. 32) en een correctierecht (art. 31). Het correctierecht kan de geregistreerde gebruiken om zijn persoonsgegevens te laten corrigeren, te laten verwijderen of te laten aanvullen indien ze niet in overeenstemming zijn met de doelomschrijving van de registratie of indien ze feitelijk onjuist zijn. Met behulp van deze rechten en de benodigde rechtsmiddelen om naleving af te dwingen (art. 34) kan de geregistreerde de organisatie ertoe bewegen de persoonsregistratie conform de doelomschrijving aan te wenden. Een belangrijk punt is dat de rechten van de geregistreerden niet contractueel zijn uit te sluiten; de organisatie is derhalve in alle gevallen gebonden aan de wet.

Bovengenoemde plichten en rechten vormen een leidraad voor het inrichten van de communicatie tussen organisatie en geregistreerden. Zoals reeds eerder gezegd kan wijziging van de interne organisatie noodzakelijk zijn. Op de organisatie- en mentaliteitsproblemen wordt hier echter niet nader ingegaan. Een aantal onduidelijkheden bij de invulling van de communicatie wordt hieronder behandeld.

Hoe dient een geregistreerde zich te legitimeren?

Indien een geregistreerde het inzage- of correctierecht wil uitoefenen, dient de organisatie volgens de wet "zorg te dragen voor een deugdelijke vaststelling van de identiteit van de verzoeker". Nadere invulling van deze bepaling laat de WPR over aan de organisatie.

Momenteel is onvoldoende duidelijk wat "deugdelijke vaststelling" inhoudt. In de praktijk wordt bijvoorbeeld wel gevraagd zich persoonlijk met een legitimatiebewijs aan de balie te komen melden, maar ook het enkel opsturen van een (kopie van een) legitimatiebewijs wordt ter vaststelling van de identiteit gehanteerd.

De inhoud van de identificatieplicht is onduidelijk. Derhalve is het aan te raden zorgvuldig te werk te gaan. Deze zorgvuldigheid kan blijken uit het vragen van advies aan de Registratiekamer of andere deskundigen en uit het aansluiten bij de gedragscodes[7]. Gedragscodes zijn een middel tot zelfregulering en worden vereist door de WPR (artt. 15 en 16). Ze kunnen branchegewijs worden opgesteld en ter beoordeling worden voorgelegd aan de Registratiekamer.

Wanneer mag de organisatie uitvoering van de rechten van de geregistreerde weigeren?

De wet maakt het in artikel 30 mogelijk dat de organisatie kan weigeren te voldoen aan verzoeken tot inzage of correctie van persoonsgegevens, indien belangen van derden daartoe aanleiding geven. Weigering is toegestaan voor zover dit noodzakelijk is in het belang van:
- de veiligheid van de staat;
- de opsporing en vervolging van strafbare feiten;
- economische en financiële belangen van de staat en andere openbare lichamen;
- inspectie, controle en toezicht door of vanwege overheidsorganen of andere organen met een publiekrechtelijke taak;
- gewichtige belangen van anderen dan de verzoeker, de houder daaronder verstaan.

Voor praktisch gebruik binnen organisaties zijn deze eisen echter niet voldoende specifiek. Uitwerking van de eisen voor de desbetreffende organisatie is dan ook noodzakelijk. Het nog beperkte referentiekader (onder andere de kamerstukken) vormt hierbij een probleem.

Net als bij de identificatieplicht is het ook hier van belang een eventuele gedragscode, de Registratiekamer of andere deskundigen te raadplegen om de door de wet nagestreefde zorgvuldigheid te bewerkstelligen.

Conclusie

Naast de zorgplicht legt de WPR nog een aantal andere plichten op aan de organisatie om de juistheid en volledigheid van de opgenomen persoonsgegevens te bevorderen. Deze andere plichten zijn gericht op het aan de geregistreerde kenbaar maken dat hij is opgenomen in een registratie. De geregistreerde kan dan zijn inzage- c.q. correctierecht uitoefenen ter verhoging van de juistheid en volledigheid van de over hem geregistreerde persoonsgegevens.

De deels vage wettelijke bepalingen ten aanzien van de communicatie tussen organisatie en geregistreerden leveren in de praktijk moeilijkheden op. De organisatie doet er goed aan bij invulling van deze communicatie te letten op een eventuele gedragscode. Advies van de Registratiekamer of andere deskundigen is tevens een mogelijkheid om de (interne) richtlijnen te ontwikkelen. Een zorgvuldige handelwijze is gezien de onduidelijkheden bij de interpretatie van de WPR gewenst.

7 *Definitie "gedragscode" uit artikel 1 WPR: Een besluit van één of meer organisaties, representatief voor de sector waarop het besluit betrekking heeft, houdende in het belang van de bescherming van de persoonlijke levenssfeer gestelde regels of gedane aanbevelingen ten aanzien van persoonsregistraties.*

COMMUNICATIE TUSSEN ORGANISATIE EN BEWERKER

Zoals reeds vermeld is de bewerker een rechtspersoon die buiten de organisatie van de houder (in termen van de WPR) valt en in opdracht van de houder een persoonsregistratie bewerkt. Een voorbeeld van een bewerker is een servicebureau dat voor andere organisaties de salarisadministratie voert. Bij de uitbesteding van de salarisadministratie draagt de houder persoonsgegevens over aan de bewerker die de administratie verder zal voeren op basis van opdrachten en gegevens uit de organisatie van de houder.

Aan de communicatie tussen organisatie en bewerker stelt de WPR slechts indirect eisen. Zo wordt in de artikelen 8 en 50 gesteld dat de beveiligingsplicht zowel geldt voor de houder als voor de bewerker (voor het deel van de apparatuur dat hij onder zich heeft). In de artikelen 9 en 10 wordt de bewerker mede-aansprakelijk gesteld voor schade bij de geregistreerde ten gevolge van overtreding van de WPR, voor zover deze voortvloeit uit zijn werkzaamheden. Globaal gesteld is de bewerker medeverantwoordelijk en mede-aansprakelijk voor de persoonsregistraties die hij voert voor andere organisaties. De eisen die de WPR aan de bewerker stelt zijn derhalve dezelfde als die welke aan de houder worden gesteld, met dien verstande dat de bewerker niet verantwoordelijk is voor de inhoud van de persoonsregistratie.

Wie doet wat?

Zoals hierboven vermeld zijn de eisen aan de communicatie tussen organisatie en bewerker indirect gesteld. Voor nadere invulling hiervan dient de organisatie zorg te dragen. De verdeling van de taken tussen organisatie en bewerker zal duidelijk moeten geschieden om geschillen in de toekomst te voorkomen.

In de praktijk geeft de houder aan de bewerker richtlijnen voor de uitvoering van de bewerkingstaak. De richtlijnen dienen bij voorkeur te worden opgenomen in het contract tussen de houder en de bewerker.

Hoe kan de organisatie haar verantwoordelijkheid dragen?

Omdat de houder de bewerkingstaak heeft gedelegeerd aan een organisatie die buiten de directe invloedssfeer van de houder valt, is het belang van controle op de uitvoering van de bewerkingstaak groot. In veel organisaties bestaat echter het probleem dat de (organisatorische en technische) deskundigheid voor het uitvoeren van de controle of de macht tot controleren ontbreekt.

Bij het ontbreken van de deskundigheid binnen de organisatie kan een externe persoon of instantie de controle uitvoeren. Hierbij kan met name aan de EDP-auditor worden gedacht. De controle kan zowel namens de houder als namens de bewerker geboeren. De bewerker zal een dergelijke controle laten uitvoeren om een onafhankelijke "verklaring van goed gedrag" te verwerven voor commerciële doeleinden. De houder zal zijn controlerecht via zijn contract met de bewerker moeten bewerkstelligen.

Conclusie

De bewerker is medeverantwoordelijk en mede-aansprakelijk voor de persoonsregistraties die hij voert voor de houder. De communicatie tussen de organisatie van de houder en de bewerker zal derhalve worden beheerst door richtlijnen voor de uitvoering van de bewerkingstaak en verantwoordingsinformatie ter controle op de juiste uitvoering. Het is zinnig de richtlijnen contractueel vast te leggen[8]. Omdat de houder verantwoordelijk blijft voor de uitvoering van de bewerkingstaak jegens de geregistreerde, dient de bewerker te worden gecontroleerd. Bij gebrek aan deskundigheid daartoe kan aan de inzet van externen worden gedacht.

De onzekerheid omtrent de eisen van de WPR vraagt van de organisatie de zorgvuldigheid om zich intensief met de problematiek bezig te houden.

SAMENVATTING

Om de persoonlijke levenssfeer van geregistreerden te beschermen is de Wet Persoonsregistraties ontworpen en ingesteld. De wet legt beperkingen op aan het gebruik van en de communicatie over persoonsgegevens. Afhankelijk van de aard van de organisatie kan de wet aanzienlijke consequenties hebben voor het beleid en de werkwijze van de organisatie.

In dit artikel is een aantal problemen aangestipt dat kan optreden bij de implementatie van de WPR binnen organisaties. De problemen ontstaan voornamelijk door onduidelijkheden in de wetgeving (zelfregulering en het ontbreken van jurisprudentie). Daarnaast kunnen de door de WPR opgelegde eisen organisatie- en mentaliteitsproblemen doen ontstaan of tevoorschijn doen komen bij de invoering van de gewenste veranderingen.

Om de genoemde problemen het hoofd te kunnen bieden (of nog beter: te voorkomen) zijn de volgende punten van belang bij de implementatie van de WPR binnen de organisatie:

– Een gedegen inventarisatie van de binnen de organisatie aanwezige persoonsregistraties en hun doelstellingen is een eerste vereiste om te kunnen voldoen aan de WPR.

8 *Zie hierover onder andere: Achter de schermen van automatiseringscontracten, J.M.A. Berkvens e.a., Samsom H.D. Tjeenk Willink, 1989.*

Ir. B.A.W.M. Bruns
Is sinds 1989 werkzaam bij KPMG Klynveld EDP Auditors. Hij studeerde Informatica en Bedrijfskunde aan de Technische Universiteit Eindhoven. Momenteel volgt hij de post-doctorale opleiding EDP-auditing aan de Erasmus Universiteit Rotterdam. Speciale aandachtsgebieden in zijn audit-werk zijn informatieplanning, begroten en beheersen van automatiseringsprojecten en de Wet Persoonsregistraties.

– De onzekerheid omtrent de eisen van de WPR vraagt van de organisatie de zorgvuldigheid om zich intensief met de problematiek bezig te houden. De door de wet gewenste zorgvuldigheid bij de behandeling van persoonsgegevens kan blijken uit het raadplegen van een eventuele gedragscode, de Registratiekamer en externe deskundigen bij de implementatie van de wet.

– Indien sprake is van een bewerker, zijn (contractueel vastgelegde) richtlijnen over de gewenste handelwijze van de bewerker van belang voor de organisatie. Een (externe) controle op de naleving is – als bij iedere andere delegatie – belangrijk.

– Naleving van de WPR vraagt om een kwalitatief goede en bekende interne organisatie. Om de bekendheid te bevorderen kunnen organisaties zogenaamde interne "privacy-reglementen" met beschrijvingen van de procedures en de richtlijnen gebruiken.

Samenvattend kan worden gesteld dat het inrichten van een organisatie om aan de Wet Persoonsregistraties te voldoen, kennis vereist op juridisch, organisatiekundig en (automatiserings)technisch gebied. Wanneer een organisatie dergelijke kennis bezit, is zij in principe bij machte om de Wet Persoonsregistraties naar behoren in te vullen.

LITERATUUR

[Berk89] *Achter de schermen van automatiseringscontracten*, J.M.A. Berkvens e.a., Samsom H.D. Tjeenk Willink, 1989.

[WetP] *Wet Persoonsregistraties, leidraad voor de praktijk*, prof.mr. J.M.A. Berkvens e.a., losbladige uitgave, Kluwer.

[Priv89] *Privacy en Computers*, brochure over de Wet Persoonsregistraties, KPMG Klynveld, 1989.

[Ende88] *Privacy en kwaliteitsaspecten van informatiesystemen*, drs. P.C.M. van der Enden RI, Samsom 1988.

Een invulling van de beveiligingseis uit de Wet Persoonsregistraties

P.A.J. van der Knaap

Gaf het vorige artikel inzicht in de problematiek bij implementatie van de WPR, dit artikel gaat in op het specifieke audit-aspect in dit kader: de beveiligingsplicht. Een spraakmakend en qua inhoud nog onduidelijk onderwerp.
Schrijver illustreert hoe door middel van de risico-analysemethode de kwaliteit van de beveiliging integraal kan worden getoetst.

INLEIDING

De Wet Persoonsregistraties (WPR) stelt weliswaar in artikel 8 dat de houder zorg moet dragen voor de nodige voorzieningen van technische en organisatorische aard – ter beveiliging van een persoonsregistratie, tegen verlies of aantasting van de gegevens en tegen onbevoegde kennisneming, wijziging of verstrekking daarvan –, maar geeft niet aan op welke wijze dit dient te geschieden.
Opgemerkt kan worden dat de wetgever aan de WPR een deregulerend karakter heeft gegeven. De WPR kent veel globale termen. Organisaties zullen de uit de WPR voortkomende verplichtingen zelf moeten verwerken in hun beleid en zullen zelf de te treffen organisatorische en technische maatregelen moeten vaststellen.

Een onderzoek waarbij het onderzoeksobject is na te gaan of een organisatie voldoet aan de eisen die de WPR stelt, kan op verschillende wijzen worden uitgevoerd en kan zich op verschillende aspecten van de WPR richten (beveiligingsplicht, formulierplicht, meldingsplicht en protocolplicht).
Dit artikel richt zich specifiek op de beveiligingsplicht.
Aan de hand van een stappenplan wordt een methodiek uiteengezet die kan worden gebruikt voor het opstellen en implementeren van een beveiligingsbeleid.

Ingegaan wordt op de normen die kunnen worden gebruikt om na te gaan of aan de beveiligingsplicht wordt voldaan. Het artikel wordt afgesloten met de behandeling van een in het kader van de WPR uitgevoerde audit. Het betreft hier een onderzoek naar de wijze waarop een organisatie de beveiligingsplicht heeft ingevuld. Hierbij werd niet alleen aangegeven of men wel of niet aan de WPR voldeed, maar tevens is geprobeerd in het oordeel bepaalde nuances aan te geven. Voor de evaluatie van de onderzoeksresultaten werd hierbij gebruik gemaakt van de risico-analysemethode. Het doel van de evaluatie was een systematische afweging mogelijk te maken tussen de kosten die de invoering van een bepaalde maatregel met zich meebrengt ten opzichte van de opbrengst die deze maatregel oplevert in de zin van het verminderen van een bepaalde bedreiging.

Aan het einde van het artikel wordt in de vorm van een schema een aanzet gegeven voor een methode om een gebeurtenissenanalyse uit te voeren. In dit schema zijn de mogelijke consequenties aangegeven indien bepaalde bedreigingen manifest worden.

HET HANTEREN VAN NORMEN IN EDP-AUDITING

Het beoordelen van de betrouwbaarheid en de kwaliteit van de geautomatiseerde gegevensverwerking behoort tot het vakgebied EDP-auditing.
Dit vakgebied is relatief jong, langzamerhand begint er consensus te ontstaan bij de mensen die het vak uitoefenen over de wijze waarop dit dient te geschieden. Echter, een eenduidig en algemeen aanvaard normstelsel dat hierbij kan worden toegepast, is nog niet aanwezig en het is zelfs de vraag, gezien de verwachte complexiteit en veelzijdigheid van dit normstelsel, of dit er ooit zal komen.
Niet alleen het ontbreken van een eenduidig normstelsel maakt toetsing van een gegeven situatie moeilijk, ook speelt het probleem dat de evaluatie zelf problematisch is.

Voor het toetsen van een aangetroffen situatie aan een gewenste situatie zal door degene die deze toetsing uitvoert, gebruik worden gemaakt van de kennis waarover hij of zij op dat moment beschikt.

Beveiliging in het algemeen en privacy-bescherming in het bijzonder zijn voor een belangrijk deel een kwestie van mentaliteit en organisatiecultuur.

Het is dan ook zeer wel mogelijk dat door een ander persoon tot een ander resultaat zou zijn gekomen. Natuurlijk geldt dit voor alle processen waarbij evaluatie dient plaats te vinden. Echter, omdat degene die de evaluatie uitvoert niet beschikt over eenduidige toetsingscriteria die hem aangeven wat in een bepaalde situatie als een bevredigende maatregel mag worden beschouwd en wat niet, is het risico van interpretatieverschillen versterkt aanwezig.

DE VERPLICHTING TOT BEVEILIGING

De effectiviteit van privacy-bescherming wordt in belangrijke mate bepaald door de kwaliteit van de beveiliging.

Artikel 8 WPR draagt houder en bewerker (voor het deel van de apparatuur waarmee de registratie wordt gevoerd dat hij onder zich heeft) op ter beveiliging van de registratie de nodige technische en organisatorische voorzieningen te treffen, teneinde verlies of aantasting van de gegevens alsmede onbevoegde kennisneming, wijziging of verstrekking daarvan te voorkomen.

Artikel 49 lid 1 geeft nog een aanvullende eis, namelijk de verplichting tot beveiliging van de toegang tot een zich in het buitenland bevindende – niet onder de WPR vallende – persoonsregistratie en van de daaruit verkregen gegevens.

Gezien het belang van de geautomatiseerde gegevensverwerking voor organisaties kennen vele daarvan reeds een beveiligingsbeleid. Nagegaan zal moeten worden of de eisen uit hoofde van de WPR invloed hebben op het beveiligingsbeleid en of deze aanvullende eisen tevens zullen leiden tot aanvullende beveiligingsmaatregelen.

De beveiligingsmaatregelen die reeds zijn geformuleerd op basis van een aanwezig beveiligingsbeleid, zullen zich in het algemeen hoofdzakelijk richten op de geautomatiseerde gegevensverwerking. Aanvullende maatregelen uit hoofde van de invoering van de WPR kunnen worden verwacht ten aanzien van het gebruik van informatie uit geautomatiseerde persoonsregistraties en ten aanzien van de input (brondocumenten) van en de output (lijsten, microfiches, etc.) uit deze persoonsregistraties.
Daarnaast zullen dergelijke maatregelen zijn vereist voor bepaalde onder de WPR vallende handmatige registraties.
Beveiligingsmaatregelen betreffende de bescherming van de privacy moeten het resultaat zijn van een zorgvuldige afweging, hetgeen een integrale aanpak vraagt.
Beveiligingsbeleid, waarvan de bescherming van de privacy een onderdeel is, vraagt om sturing door het management.
Beveiliging in het algemeen en privacy-bescherming in het bijzonder zijn daarnaast voor een belangrijk deel een kwestie van mentaliteit en organisatiecultuur [Nivr91].

STAPPENPLAN

Beveiliging uit hoofde van de WPR is geen doel op zich. Men dient te komen tot een integrale beveiliging waarvan de privacy-bescherming een geïntegreerd onderdeel dient te zijn. Om te komen tot een geïntegreerd beveiligingsbeleid kan gebruik worden gemaakt van een stappenplan [Nivr91].
Dit stappenplan bestaat uit de volgende fasen:

Fase 1: Probleemverkenning en probleemdefinitie

Gestart wordt met een inventarisatie van het huidige informatie- en beveiligingsbeleid en nagegaan wordt of hierin tekortkomingen zijn te onderkennen.
Tevens zal worden nagegaan wat de consequenties zijn van het gebruik van een bepaalde informatietechnologie voor de beheersing van de organisatie, bijvoorbeeld welk risico een onderneming loopt indien zij voor haar bedrijfsvoering veelvuldig gebruik maakt van extern dataverkeer over een openbaar (telefoon)netwerk.

Fase 2: Risico-analyse

Risico-analyse kan worden gedefinieerd als het geheel van activiteiten gericht op het onderzoeken dan wel bepalen van de bedreigingen, de getroffen (en mogelijk te treffen) maatregelen en de optimale set van maatregelen [Giel89]. Door toepassing van deze methode wordt een inventarisatie gemaakt van bedreigingen waaraan een organisatie bloot staat.

Fase 3: Formuleren van een beveiligings-beleid en de keuze van de beveiligingsmaatregelen

Aan de hand van de resultaten van de vorige fase kan nu een aantal beleidsalternatieven worden voorgesteld waaruit een keuze moet worden gemaakt. Het management moet aangeven met welke intensiteit en op welke wijze de bedreigingen tegemoet moeten worden getreden.
Maatregelen zijn naar hun aard te onderscheiden in preventieve, repressieve en correctieve maatregelen. Een dusdanige mix van maatregelen dient te worden samengesteld dat voldaan wordt aan de eisen zoals vastgelegd in het beveiligingsbeleid.
Een duidelijke verschuiving zal plaatsvinden van repressieve en correctieve maatregelen naar preventieve maatregelen; immers, slechts preventieve maatregelen kunnen waarborgen dat zich geen inbreuk op de privacy van personen heeft voorgedaan.
De volgende zaken dienen in het beveiligingsbeleid aan de orde te komen [Sche89]:

– Overall-doelstelling:
Duidelijk dient naar voren te worden gebracht waarom het beleid wordt gevoerd.
Informatie wordt tegenwoordig vaak gezien als een strategisch goed waarmee een bepaald concurrentievoordeel kan worden behaald. Om dit concurrentievoordeel te behouden zal men ervoor zorg dienen te dragen dat de informatie niet ongeautoriseerd kan worden gebruikt door derden.

– Verantwoordelijke manager:
Binnen het hoogste management dient een functionaris verantwoordelijk te zijn gesteld voor het beveiligingsbeleid. Deze functionaris geldt tevens als aanspreekpunt voor de lagere echelons in de organisatie die zich met beveiliging bezighouden.

– Toekomstvisie:
Zowel een korte-termijn- als een lange-termijnvisie dient te worden aangegeven.

– Middelen die ter beschikking worden gesteld:
Aangegeven dient te worden welke middelen (geld, personeel en resources) ter beschikking worden gesteld om het beleid ten uitvoer te kunnen brengen.

– Doelstellingen, normen en verantwoordelijkheden ten aanzien van de sleutelgebieden organisatie, apparatuur, besturingsprogrammatuur, applicatieprogrammatuur, gegevens en omgeving dienen te worden vastgesteld.

Aansluitend op laatstgenoemd punt is onderstaand per sleutelgebied een aantal relevante attentiepunten vermeld.

Organisatie
– Het management dient betrokken te zijn bij de automatisering. Deze betrokkenheid dient onder andere te blijken uit expliciete beveiligingsrichtlijnen en een expliciete automatiseringsstrategie. Deze strategie is een afgeleide van de informatiseringsstrategie.

Beveiliging uit hoofde van de WPR is geen doel op zich. Men dient te komen tot een integrale beveiliging waarvan de privacy-bescherming een geïntegreerd onderdeel dient te zijn.

Apparatuur
– De wijze waarop apparatuur wordt geïnstalleerd en gebruikt, mag niet leiden tot het doorbreken van de vereiste functiescheidingen, noch binnen de automatiseringsorganisatie, noch binnen de gebruikersorganisatie.

– De uitwisseling van gegevens via telefoonverbindingen dient beschermd te zijn tegen ongeautoriseerde beïnvloeding en kennisname van gegevens. Er dienen waarborgen te zijn getroffen om ongeautoriseerde toegang tot het systeem via datacommunicatieverbindingen te voorkomen.

Besturingsprogrammatuur
– Mogelijkheden tot controle en beveiliging dienen buiten applicaties te worden gehouden, dat wil zeggen binnen de aanwezige apparatuur of standaardbesturingsprogrammatuur te worden geïmplementeerd.
Wanneer van additionele beveiligingspakketten gebruik wordt gemaakt, dienen de daardoor geboden beveiligingsmogelijkheden te worden getoetst aan de gestelde beveiligingseisen.

– Het gebruik van privileged user identifiers (dan wel interfaces waarmee een geprivilegieerde status kan worden bereikt) dient tot een minimum te worden beperkt.

Applicatieprogrammatuur
– Produktiegegevens mogen slechts met door gebruikers geautoriseerde programmatuur worden verwerkt.

– Wijzigingen of nieuwe programma's mogen slechts tot stand worden gebracht na een opdracht van een daartoe geautoriseerde gebruiker.

– Vastgesteld dient te kunnen worden of het object (het door de computer uit te voeren programma) dat door de gebruiker is geaccepteerd, overeenstemt met het source-programma (het door de mens leesbare programma) dat door applicatiebewaring wordt bewaard.

Gegevens
– Toegang (inclusief wijzigen en verwijderen) tot gegevens mag slechts plaatsvinden via geautoriseerde applicaties en door (of in opdracht van) geautoriseerde functionarissen.

– Er dient een beveiligingsmechanisme te zijn geïmplementeerd dat bewerkstelligt dat:
  – de toegang tot het systeem op beheerste wijze plaatsvindt;
  – processen behorend tot verschillende domeinen elkaar niet op onbeheerste wijze kunnen beïnvloeden;
  – toegang tot en het door meerdere gebruikers gelijktijdig gebruik maken van programmatuur en gegevens op een beheerste manier plaatsvindt.

– Intern en extern dienen (voldoende) kopieën te worden bewaard van programmatuur (inclusief besturingsprogrammatuur en job control streams), bestanden en documentatie (zowel gebruikers- als operators-handleidingen) in een tegen stof, brand, water, extreme temperaturen, magnetisme en dergelijke beschermde omgeving.

De wijze waarop door verschillende organisaties een stelsel van maatregelen wordt opgesteld en geïmplementeerd om te voldoen aan de beveiligingsplicht, zal iedere keer anders zijn.

Omgeving
– Teneinde storingen door het fysiek in ongerede raken van apparatuur en de risico's van diefstal of verminking van apparatuur, programmatuur en/of gegevens zoveel mogelijk te beperken, dient een computercentrum fysiek te worden beveiligd.

Fase 4: Implementatie van de beveiligingsmaatregelen

De beveiligingsmaatregelen zoals deze uit het beveiligingsbeleid voortvloeien, dienen met behulp van de resources zoals gedefinieerd in fase 3 tot uitvoering te worden gebracht in de organisatie.

Fase 5: Evaluatie en bijstelling

In principe is dit een continu proces dat voortdurend zal plaatsvinden. Continu wordt nagegaan of maatregelen blijven voldoen aan de eisen zoals deze in het beveiligingsbeleid zijn vastgesteld en of veranderende omstandigheden (bijvoorbeeld nieuwe bedreigingen) noodzaken tot aanvullende maatregelen. Dit houdt in dat met een zekere regelmaat de risico-analyse uit fase 2 opnieuw dient te worden uitgevoerd en dat aanpassing van het beveiligingsbeleid op basis van de opgeleverde gegevens dient plaats te vinden.

NORMEN

In artikel 8 van de WPR wordt gesteld dat de houder (en bewerker) *de nodige voorzieningen* van technische en organisatorische aard dient te treffen ter beveiliging van zijn registratie. Dit geeft een zeer globale norm, waarmee men in de dagelijkse praktijk slecht uit de voeten kan. Wat onder *de nodige voorzieningen* moet worden verstaan, is niet duidelijk.

Onder de opsomming welke zaken in het beveiligingsbeleid aan de orde dienen te komen werd in de voorgaande paragraaf een aantal normen gegeven.
Veelvuldig wordt door EDP-auditors gebruik gemaakt van checklists, bijvoorbeeld de checklist Computerbeveiliging van het NGI [Chec89]. Deze checklist richt zich in het bijzonder op de fysieke beveiligingsmaatregelen en in veel mindere mate op organisatorische maatregelen.

Ten aanzien van gegevensbeveiliging kan een onderscheid worden gemaakt in:
– de fysieke toegangsbeveiliging;
– de logische toegangsbeveiliging.

Voor logische toegangsbeveiliging wordt vaak gerefereerd aan een tweetal beveiligingsmodellen, namelijk het Bell-LaPadula-model (en zijn verdere aanvulling in het zogenaamde "Orange book" van het American Department of Defence [Tsec85]) en het Clark-Wilson-model.
Het Bell-LaPadula-model richt zich met name op de geheimhouding van de informatie, het Clark-Wilson-model beschrijft niet alleen uitspraken over bevoegdheden ten aanzien van gegevens, maar ook regels waarmee de integriteit kan worden afgedwongen [Brin89].
Een verder uitgebreid normstelsel kan worden gevonden in het draft report "Information Technology Security Evaluation Criteria" [Itse90]. In dit draft report wordt een classificatie voorgesteld die bestaat uit zeven categorieën (E0 tot en met E6). Het TOE (Target Of Evaluation = object van onderzoek) van categorie E0 is dusdanig slecht beschermd dat aan de kwaliteit en de betrouwbaarheid van de gegevensverwerking van dit object geen waarde mag worden gehecht. De classificatie E1 geeft aan dat aan een minimumniveau wordt voldaan; de classificatie E6 geeft aan dat aan een maximumniveau wordt voldaan. Toetsing van een TOE kan plaatsvinden ten aanzien van het ontwikkelingsproces en het verwerkingsproces. Na-deel van deze evaluatiemethode is dat zij zo formalistisch is opgesteld (hetgeen noodzakelijk is om te

kunnen komen tot eenduidige evaluaties) dat de toepasbaarheid ervan bijzonder gecompliceerd is. Daarnaast is toetsing van een object op bovenstaande wijze bijzonder kostbaar.
Voor het toetsen van een hardware-systeem dan wel een operating systeem kan nog naar voren worden gebracht dat deze kosten kunnen worden verdeeld over het aantal af te zetten exemplaren en dat mag worden gesteld dat toetsing van één exemplaar uit een reeks een oordeel geeft over alle exemplaren van deze reeks. Dit kan echter moeilijk worden volgehouden indien dient te worden getoetst of aan de beveiligingsplicht wordt voldaan. De wijze waarop door verschillende organisaties (zelfs indien vergelijkbare hardware en software worden gebruikt) een stelsel van maatregelen wordt opgesteld en geïmplementeerd om te voldoen aan de beveiligingsplicht, zal immers iedere keer anders zijn.

Beter dan van de hiervoor genoemde methoden kan gebruik worden gemaakt van de ideeën zoals deze worden aangetroffen in het stelsel uit Bijlage 3 van het rapport *Privacy-bescherming; de gevolgen voor organisaties en de rol van de accountant* [Nivr91]. In deze bijlage worden de te treffen maatregelen verdeeld in een drietal categorieën, namelijk:
- technische maatregelen;
- organisatorische maatregelen;
- programmeerbare maatregelen.

Per categorie worden voorbeelden genoemd, zoals bijvoorbeeld:
- er is een mogelijkheid om ruimten af te sluiten (technische maatregel);
- fysieke toegangscontrole (technische maatregel);
- screening van personeel (organisatorische maatregel);
- plausibiliteitscontrole op resultaten met melding van geconstateerde fouten (programmeerbare maatregel).

AUDIT IN HET KADER VAN DE WPR

In het vervolg van dit betoog zal worden ingegaan op een audit die mede stof heeft aangeleverd voor dit artikel. Het betreft een audit waarbij onderzocht is of ten aanzien van het persoonsregistratiesysteem werd voldaan aan de eisen zoals deze voortvloeien uit de WPR. De beoordeling werd zowel uitgevoerd ten aanzien van de geautomatiseerd bijgehouden registratie als ten aanzien van de gegevens die niet op geautomatiseerde wijze werden vastgelegd, zoals bijvoorbeeld de brondocumenten en de door het systeem opgeleverde fysieke output (microfiches en papier). Door het gebruik van computersystemen wordt de opslag van (persoons)gegevens vereenvoudigd. Hierdoor neemt de mogelijkheid tot systematisering en onderlinge vergelijking van de gegevens toe. De nadruk bij het onderzoek lag derhalve vooral op het geautomatiseerde gedeelte van het persoonsregistratiesysteem.

RISICO-ANALYSEMETHODE

Bij het onderzoek werd voor de kwantificering van de risico's gebruik gemaakt van ideeën uit de risico-analysemethode. Een risico-analyse wordt in een aantal stappen uitgevoerd.

De eerste stap bestaat uit het identificeren, analyseren en kwantificeren van bedreigingen. Bedreigingen kunnen worden gedefinieerd als ongewenste gebeurtenissen, die op zich kunnen worden veroorzaakt door ongewenste (sub)gebeurtenissen.

In de tweede stap van de risico-analyse worden de getroffen en mogelijk te treffen maatregelen geïdentificeerd, geanalyseerd en gekwantificeerd. De kwantificering betreft het beoordelen in hoeverre door de uitvoering van een bepaalde maatregel een bepaalde bedreiging wordt afgedekt.

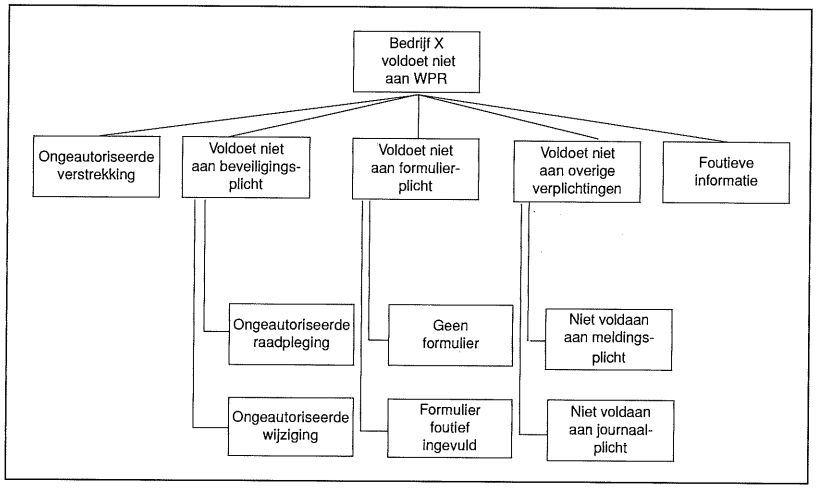
Beveiligingsbeleid, waarvan de bescherming van de privacy een onderdeel is, vraagt om sturing door het management.

De laatste stap van de risico-analyse betreft het bepalen van de optimale set van maatregelen. Optimaal betekent hier het zo hoog mogelijk afdekken van de bedreiging tegen de laagst mogelijke kosten. In deze fase wordt nagegaan of kostbare maatregelen kunnen worden vervangen door minder kostbare maatregelen die hetzelfde dan wel meer effect hebben. Deze laatste fase van de risico-analyse is bij dit specifieke onderzoek niet uitgevoerd.

Als eindresultaat van de audit werd een rapport opgeleverd, waarin aanbevelingen werden gedaan ter verbetering van het stelsel van maatregelen in de automatiseringsorganisatie en ten aanzien van het geautomatiseerde persoonsregistratiesysteem. Tevens werd in de vorm van een risico-analysemodel kwantitatief aangegeven in hoeverre het bedrijf effectief was in het zich te weer stellen tegen de hoofdbedreiging (hier gedefinieerd als het niet voldoen aan de eisen zoals deze voortvloeien uit de WPR). De hoofdbedreiging werd opgesplitst in een aantal subbedreigingen (zie figuur 1 op blz. 32).
De aspecten formulierplicht, meldingsplicht en journaalplicht werden niet verder onderzocht.
Wel werd het aspect beveiligingsplicht nader geanalyseerd, zoals onderstaand is aangegeven.

Subbedreigingen en oorzaken

De bedreiging "Het niet kunnen voldoen aan de beveiligingsplicht" is afhankelijk van de subbedreigingen:
- het onbevoegd kennis kunnen nemen van informatie;
- het onbevoegd wijzigen van informatie.



Figuur 1. Overzicht hoofd- en subbedreigingen.

De subbedreiging "Onbevoegd kennis kunnen nemen van informatie" wordt veroorzaakt doordat niet-geautoriseerde personen:
- kennis nemen van de input;
- kennis nemen van de gegevens tijdens het verwerkingsproces;
- kennis nemen van de opgeslagen gegevens;
- kennis nemen van de output.

Het onbevoegd kennis nemen van informatie kan plaatsvinden:

- aan de bron, doordat: gebruikers bescheiden niet opbergen, de fysieke beveiligingsprocedures in de gebruikersorganisatie niet van voldoende niveau zijn of er geen procedures zijn ter vernietiging van input die niet meer wordt gebruikt;

- met behulp van terminals, doordat: geen time-out voor kritische terminals (in de zin van terminals waarmee toegang kan worden verkregen tot gevoelige data) is geïnstalleerd, de gebruiker de terminal onbeheerd achterlaat, de gebruiker de terminal dusdanig heeft geplaatst dat onbevoegden kunnen meelezen;

- door onbevoegd kennis nemen van input op papier tijdens transport van de ene naar de andere afdeling, doordat de input eenvoudig te onderscheppen is en doordat verzending naar een foutieve bestemming plaatsvindt;

- door onbevoegd kennis nemen van in/output bij transport over het netwerk, doordat de logische beveiliging van het netwerk tegen het vrijkomen van berichten onvoldoende is en doordat de fysieke beveiliging van het netwerk onvoldoende is (waardoor het op eenvoudige wijze mogelijk is berichten af te tappen).

Tabel 1. Risicomatrix.

Omschrijving Hoofdbedreiging level 1:		Ongeautoriseerde raadpleging					
Omschrijving bedreiging level 2:		Onbevoegd kennisnemen van input					
		level 3		level 4		level 5	
	Waarde	Norm	Score	Norm	Score	Norm	Score
3. Onbevoegd kennis nemen van input bij de bron	61	40	24				
.....	.....						
3. Onbevoegd kennis nemen input transport op papier	61	40	24				
.....	.....						
3. Onbevoegd kennis nemen in/output bij transport over het netwerk	18	20	4				
4. Logische beveiliging netwerk tegen vrijkomen berichten-inhoud voldoende	0			65	0		
5. Gegevens via netwerk encrypted	0					80	0
5. Gegevens in knooppunt encrypted	0					20	0
4. Fysieke beveiliging netwerk voldoende	52			35	18		
5. Knooppunten in netwerk fysiek beveiligd	25					40	10
5. Dial-in-lijnen fysiek beveiligd	70					60	42
		100	52				

RISICOMATRIX

Om een beeld te geven van de berekeningssystematiek zijn de gegevens uit de vorige paragraaf ingevoerd in de in tabel 1 weergegeven risicomatrix.

De risicomatrix bestaat uit een vijftal lagen, namelijk: hoofdbedreiging (level 1), bedreigingen (level 2), subbedreigingen (level 3), kwaliteitseisen (level 4) en maatregelen (level 5). Subbedreigingen kunnen worden afgedekt door te voldoen aan een samenstel van kwaliteitseisen. Aan een kwaliteitseis kan worden voldaan door één of meer maatregelen te treffen. De kwaliteitseisen en maatregelen worden per subbedreiging weergegeven.

Per subbedreiging wordt een totaal van honderd punten verdeeld over een set van kwaliteitseisen. Onder het kopje norm is de verdeling gegeven. Naarmate de kwaliteitseis zwaarder telt om de subbedreiging af te dekken, ontvangt hij meer punten. De normatieve waarde is bepaald door het uitvoeren van een groot aantal gelijksoortige onderzoeken door medewerkers van KPMG Klynveld EDP Auditors en wordt voor elke specifieke situatie opnieuw aangepast.

Ter illustratie het volgende voorbeeld.
Voor de maatregel "Gegevens via netwerk encrypted" is de normatieve waarde 80, hetgeen betekent dat indien deze maatregel naar behoren is geïmplementeerd, de kwaliteitseis "Logische beveiliging netwerk tegen vrijkomen berichteninhoud voldoende" voor 80% is afgedekt.

Door een beoordeling van de daadwerkelijk getroffen maatregelen wordt vastgesteld in welke mate feitelijk aan de kwaliteitseis wordt voldaan. De feitelijke waarde wordt bepaald door de afzonderlijke maatregelen te beoordelen op een schaal van 0 tot en met 100 (zie de kolom onder het kopje Waarde). Aan de maatregel "Dial-in-lijnen beveiligd" is de beoordeling 70 gegeven. De EDP-auditor heeft bij de evaluatie van de effectiviteit van deze maatregel bijvoorbeeld de volgende aspecten

laten meewegen, waarbij zijn oordeel positief werd beïnvloed door het feit dat:
- er slechts een beperkt aantal dial-in-lijnen aanwezig is;
- er procedures aanwezig zijn die voorschrijven dat dial-in-lijnen pas mogen worden gebruikt na tussenkomst van de operators, dus de modems staan niet op auto-answer;
- degene die verzoekt om een dial-in-verbinding zich op een vast omschreven wijze dient te identificeren;
- de operators goed op de hoogte zijn met de inhoud van deze procedure;
- de verbinding na het afloggen automatisch wordt verbroken, waardoor geen dial-in-verbindingen "open" blijven staan.

Zijn oordeel werd negatief beïnvloed door het feit dat:
- er geen dial-back-faciliteiten aanwezig zijn;
- de aangetroffen maatregelen ongunstig worden beïnvloed doordat de laatste tijd veelvuldig gebruik wordt gemaakt van uitzendkrachten die niet goed bekend zijn met de in gebruik zijnde procedure.

Berekening van de behaalde score, bijvoorbeeld ten aanzien van de kwaliteitseis "Fysieke beveiliging netwerk voldoende", geschiedt nu als volgt:

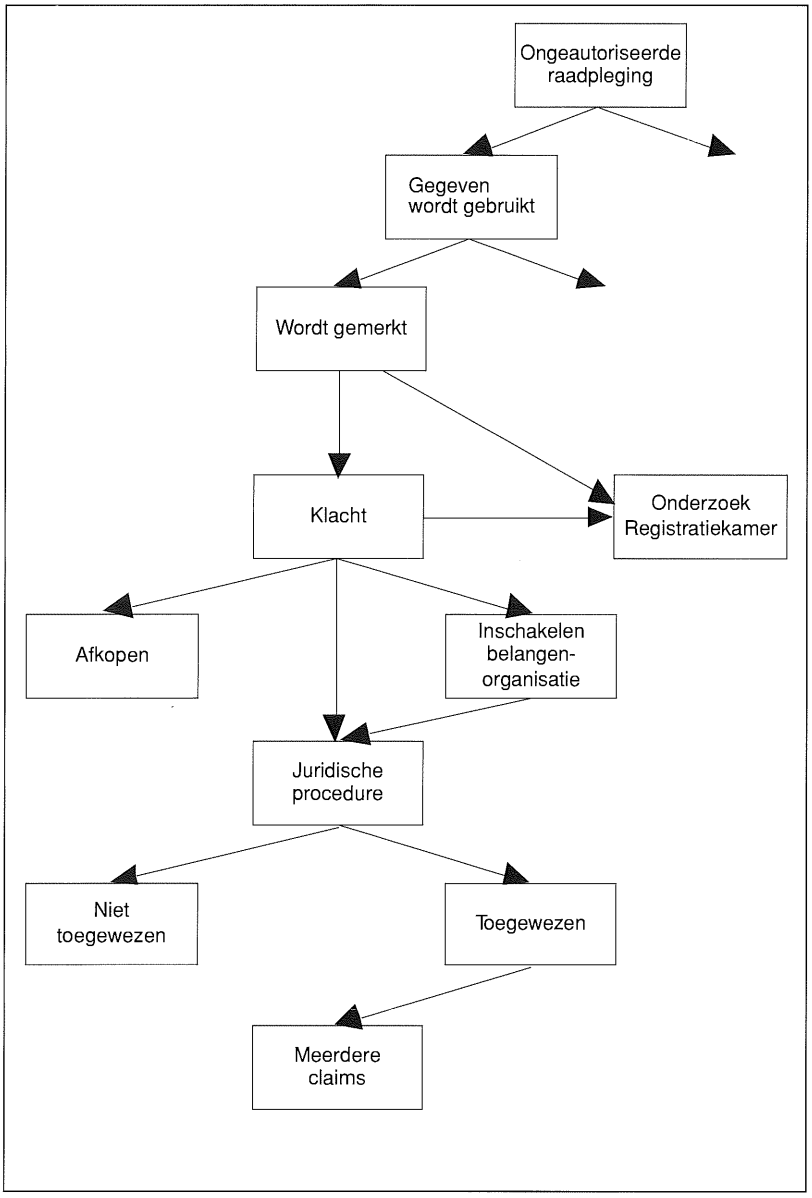
$$(25/100 * 40) + (70/100 * 60) = 10 + 42 = 52.$$

Het dekkingspercentage van de kwaliteitseisen vermenigvuldigd met de normen leidt tot de dekking van de subbedreiging. Bijvoorbeeld voor de subbedreiging "Onbevoegd kennis nemen in/output bij transport over het netwerk" is de dekking

$$(0/100 * 65) + (52/100 * 35) = 0 + 18 = 18.$$

De risicomatrix geeft inzicht in de kans op het optreden van bedreigingen (combinatie van de geschatte kans van optreden en de aanwezige dekking). Een gebeurtenissenanalyse geeft inzicht in de gevolgen indien een bedreiging tot werkelijkheid zou worden.

Naast de foutboomanalyse met behulp van de risicomatrix is voor de hier besproken audit tevens een begin van een gebeurtenissenanalyse uitgevoerd. Hierbij is geanalyseerd wat de consequenties zijn indien de bedreiging "Ongeautoriseerd raadplegen van tot personen herleidbare gegevens door onbevoegden" daadwerkelijk heeft plaatsgevonden.
Een volgende fase in het onderzoek zou zijn te bepalen wat de verwachte vervolgschaden zijn indien de acties uit de gebeurtenissenanalyse zich voordoen; deze onderzoeksfase is in deze audit niet uitgevoerd.



Figuur 2. Overzicht gebeurtenissenanalyse.

SAMENVATTING

In dit artikel is beschreven hoe de beveiligingsplicht uit hoofde van de WPR kan worden ingevuld. Aangegeven is dat er momenteel nog geen sprake is van een formeel stelsel van normen dat kan worden gebruikt om te bepalen of wordt voldaan aan de beveiligingsplicht. Aan de hand van een stappenplan is gepoogd aan te geven hoe een coherent beveiligingsbeleid kan worden opgezet. Onderdeel van dit stappenplan vormt de risicoanalyse.
Ter illustratie is het artikel afgesloten met de beschrijving van een audit waarbij de doelstelling van het onderzoek was na te gaan in hoeverre een persoonsregistratiesysteem naar behoren was beveiligd. De kwantificering van het onderzoeksresultaat werd daarbij in de vorm van een risicomatrix vastgelegd.

P.A.J. van der Knaap
Is sinds 1981 werkzaam bij KPMG Klynveld EDP Auditors. Hij heeft een breed scala van audit-opdrachten uitgevoerd, waaronder de beoordeling van geautomatiseerde informatiesystemen, rekencentra-onderzoeken en de uitvoering van risico-analyses.
Binnen KPMG Klynveld EDP Auditors is Van der Knaap betrokken bij research-projecten ten behoeve van het ontwikkelen van methoden voor risico-analyse, en efficiency- en effectiviteitsonderzoeken bij rekencentra.

LITERATUUR

[Brin89] J. Brinkman, *Logische toegangsbeveiliging*, in Compact 1989/49.

[Chec89] *Checklist Computerbeveiliging*, rapport van het NGI sectie beveiliging, 1987.

[Giel89] C.J.M. Gielen, *Een praktische methode voor de analyse van risico's bij automatisering*, in Compact 1989/49.

[ITSE90] *Criteria voor de evaluatie van Informatie Beveiligingstechnologie (ITSEC)*, Der Bundesminister des Innern, Bonn 1990.

[NIVR89] NIVRA-geschrift 53, *Automatisering en controle, deel VII. Kwaliteitsoordelen over informatievoorziening*, Kluwer Bedrijfswetenschappen, 1989.

[Priv89] *Privacy en Computers*, brochure over de Wet Persoonsregistraties, KPMG Klynveld, 1989.

[NIVR91] NIVRA-geschrift 58, *Privacy-bescherming; de gevolgen voor organisaties en de rol van de accountant*, Kluwer Bedrijfswetenschappen, 1991.

[Sche89] R. Schenk, *Beveiligingsbeleid formuleren*, in Compact 1989/49.

[Tsec85] *Trusted Computer System Evaluation Criteria*, DOD 5200.28-STD, Department of Defence, United States of America, 1985.

Computercriminaliteit in Nederland

Mr. V.A. de Pous

Juridisch commentaar in automatiseringsland. De Pous belicht opvallende conclusies uit het rapport van het Platform Computercriminaliteit.
"Software-piraterij is als het fietsen zonder licht in Amsterdam". En: "Een groot deel van de organisaties heeft onvoldoende zorg voor de beveiliging tegen computercriminaliteit".

INLEIDING

Van alle verschijningsvormen van computercriminaliteit komt het illegaal kopiëren en gebruiken van computerprogramma's in Nederland het meeste voor. Daarna volgen het schade toebrengen aan gegevens of programma's, meestal door virussen, hacken, spionage en computergerelateerde valsheden en fraude. Verder doet slechts vijf procent van de slachtoffers aangifte bij politie en justitie, en is uit onderzoek gebleken dat veel misbruik kan worden voorkomen door een goede beveiliging van informatiesystemen.
Dat zijn enkele opvallende conclusies uit het rapport "Computercriminaliteit in Nederland", dat eind 1990 door het Platform Computercriminaliteit werd gepresenteerd.

GESCHIEDENIS

Ruim twee jaar na de publikatie van de studie "Informatietechniek en strafrecht" van de Commissie Franken werd het Platform Computercriminaliteit geïnstalleerd. De toenmalige minister van Justitie mr. F. Korthals Altes en de voorzitter van de Raad van Centrale Ondernemingsorganisaties (RCO) mr. C.J.A. van Lede ondertekenden hiertoe in juni 1989 een convenant. Daarin is vastgelegd dat de werkzaamheden van het Platform moeten resulteren in meer inzicht in de omvang en de verschijningsvormen van computercriminaliteit, in de factoren die de aangiftebereidheid beïnvloeden en in de juridische mogelijkheden en beperkingen bij de bestrijding van computercriminaliteit.

In 1988 vond slechts in achttien gevallen strafrechtelijk vooronderzoek plaats naar aanleiding van computerfraude, terwijl een door de VIFKA in Nederland gedaan onderzoek aangaf dat 82 procent van de respondenten geen aangifte van computerfraude zou doen.

Minister Korthals Altes wees er toen nadrukkelijk op dat het samenwerkingsverband tussen overheid en bedrijfsleven onder voorzitterschap van prof. J. van Oorschot niet als een opsporingsdienst moest worden beschouwd. "Het Platform heeft tot doel door middel van analyse van – desnoods anoniem – door het bedrijfsleven gemelde gevallen van computercriminaliteit een vergroting van inzicht in mogelijke vormen van computercriminaliteit te bewerkstelligen", aldus de bewindsman.

Maatschappelijk belang

Volgens RCO-voorzitter Van Lede geven Amerikaanse cijfers een exponentiële toename van computercriminaliteit aan en er is geen enkele reden om aan te nemen dat dit verschijnsel zich in Nederland in mindere mate zou voordoen. Van Lede: "In cijfers van aangifte is dat echter niet terug te vinden. In 1988 vond slechts in achttien gevallen strafrechtelijk vooronderzoek plaats naar aanleiding van computerfraude, terwijl een door de VIFKA in Nederland gedaan onderzoek aangaf dat 82 procent van de respondenten geen aangifte van computerfraude zou doen."

Ook signaleerde Van Lede dat verschillende handelingen die maatschappelijk onaanvaardbaar worden geacht, zoals hacking, nog niet strafrechtelijk kunnen worden aangepakt. Daarnaast uitte Van Lede zijn bezorgdheid over de relatieve ondeskundigheid bij de politie en het Openbaar Ministerie op automatiseringsgebied en de vrees dat het stilleggen van computersystemen voor het bedrijfsleven ernstige gevolgen heeft.
Hoewel algemeen bekend is dat de aangiftebereidheid bij het bedrijfsleven in geval van computermisbruik gering is, hoopt het Platform deze tendens juist te doorbreken. Onder meer door de onderzoekers van het Computer Law Institute van de Vrije Universiteit, mevrouw drs. F. Charbon en mr. R. Kaspersen, de gemelde zaken te laten anonimiseren.

Activiteiten

Het Platform ging in eerste instantie voor een experimentele periode van een jaar van start. Het tot stand komen van het Platform Computercriminaliteit is een rechtstreeks gevolg van het werk van de Commissie Franken, die in haar rapport van april 1987 de instelling van een dergelijk overlegorgaan bepleitte.

Het rapport van het Platform heeft naar schatting *f* 450.000 gekost, hetgeen werd gesubsidieerd door de ministeries van Justitie en Economische Zaken alsmede door het georganiseerde bedrijfsleven. Of er geld is voor vervolgstudies is niet bekend. Behalve met dit rapport is het Platform al eerder in de openbaarheid getreden met bliksemacties om schade door computercriminaliteit te voorkomen. Voor de afloopdatum van het computervirus Datacrime, 13 oktober 1989, heeft het Platform een anti-virusdiskette op de markt gebracht. Daarvan zijn er uiteindelijk dertigduizend verkocht voor *f* 5 per stuk. Deze actie bracht het Platform landelijke bekendheid.

SOFTWARE-PIRATERIJ, HET MEEST GEPLEEGDE DELICT

Begin 1990 had het Platform Computercriminaliteit ongeveer 2600 organisaties in Nederland schriftelijk geënquêteerd. De respons bedroeg 34,5 procent, dat wil zeggen 910 organisaties hebben de formulieren ingevuld en teruggestuurd. Uit de formulieren bleek dat de software-piraterij – in de zin van het Platform het illegaal verveelvoudigen, verspreiden of aan het publiek ter beschikking stellen van beschermde computerprogramma's, inclusief het onbevoegd gebruiken van software – "verreweg" de meest voorkomende vorm van computercriminaliteit is.

140 organisaties (16,6 procent van de totale respons) zijn volgens eigen zeggen "op enigerlei wijze" met software-piraterij in aanraking gekomen. Daarvan geven 23 organisaties aan dat zij als ontwikkelaar of rechthebbende het slachtoffer van onrechtmatig gebruik van software zijn geworden. In de andere gevallen gaat het om organisaties (134) die als gebruiker, bijvoorbeeld door middel van handelingen van personeel, zich schuldig hebben gemaakt aan illegaal kopiëren, verspreiden en gebruiken van computerprogramma's.

Omvang en schade
Hoeveel er in Nederland illegaal wordt gekopieerd, weet ook het Platform niet, maar het wijst als referentie in dit kader op verschillende buitenlandse cijfers. Zo maakte de Spaanse branche-organisatie SEDISI naar aanleiding van een onderzoek uit mei 1990 bekend dat in Europa per honderd verkochte personal computers maar vijftig software-pakketten zijn verkocht. In ons land zou dat cijfer lager liggen, namelijk 41 computerprogramma's per honderd PC's.
De hoogte van de schade die de software-industrie door illegaal kopiëren lijdt is onduidelijk. Volgens het Platform lopen de schattingen nogal uiteen. In Engeland heeft de Federation Against Software Theft (FAST) gesteld dat Britse ondernemingen in 1989 voor minimaal 300 miljoen pond (dat is ruim *f* 1 miljard) illegaal software hebben gekopieerd.
Hoewel een aantal software-leveranciers regelmatig te kennen geeft dat ze niet overtuigd zijn van hun rechtspositie in ons land, laat het Platform Computercriminaliteit hierover geen misverstand bestaan. "Onder de bestaande wet is het zonder toestemming vervaardigen van kopieën van beschermde programma's en het in circulatie brengen daarvan een strafbaar feit. Ook degene die gebruik maakt van een illegale programmakopie is strafbaar onder de huidige Auteurswet."

COMPUTERMISBRUIK, GROOT GEVAAR VOOR DE SAMENLEVING

In de rij van vormen van computercriminaliteit volgen na software-piraterij: het schade toebrengen aan gegevens en programma's, hacken, spionage en computergerelateerde vervalsingen en fraude. Computersabotage en "diefstal" van geautomatiseerde diensten komen minder voor, terwijl piraterij van chips en het onbevoegd onderscheppen van gegevensverkeer nauwelijks is geregistreerd.
De lijst van verschijningsvormen van computercriminaliteit, in volgorde van voorkomen, ziet er dus als volgt uit:

1. software-piraterij;
2. het schade toebrengen aan gegevens of programma's (meestal door virussen);
3. het onbevoegd inbreken in informatiesystemen, het zogenoemde "hacken";
4. spionage;
5. computergerelateerde vervalsingen en fraude;
6. computersabotage;
7. "diefstal" van geautomatiseerde diensten;
8. piraterij van chips;
9. het onbevoegd onderscheppen van gegevensverkeer.

Volgens het Platform Computercriminaliteit blijkt uit het onderzoek dat "computercriminaliteit een serieuze bedreiging vormt voor iedere organisatie waar processen zijn geautomatiseerd, vooral gezien de grote risico's die eraan zijn verbonden." Het Platform waarschuwt dan ook dat computercriminaliteit niet mag worden "veronachtzaamd". Daarnaast verwacht het Platform dat misbruik van computersystemen in ons land in de toekomst verder zal toenemen en geeft het daarvoor verschillende oorzaken aan.
Allereerst zal het gebruik van informatietechnologie toenemen, er zullen meer gebruikers komen en de gebruikersvriendelijkheid van apparatuur en programmatuur zal groter worden. Bovendien vergroten de technologische ontwikkelingen de bereikbaarheid van computersystemen.

53 organisaties gaven aan dat zij in de afgelopen jaren één of meer gevallen van schade hebben gehad. Meestal was de schade ontstaan door computervirussen, Trojaanse paarden of logische bommen. Organisatorische en technische maatregelen kunnen in dit kader uitkomst bieden.

LAGE AANGIFTEBEREIDHEID

Organisaties in Nederland die het slachtoffer worden van één van de verschijningsvormen van computercriminaliteit blijken nauwelijks bereid te zijn dit bij politie en justitie te melden. Slechts in vijf procent van de gevallen wordt aangifte gedaan. Met dit cijfer, dat uit het onderzoek van het Platform Computercriminaliteit naar voren is gekomen, zijn niet alleen politie en justitie zeer ongelukkig, ook het georganiseerde bedrijfsleven is niet blij met deze uitkomst. Volgens RCO-voorzitter Van Lede lijkt het erop dat ondernemers ten aanzien van *alle* vormen van criminaliteit de ogen sluiten. "Toch moet een eventueel taboe op beveiligingsbewustzijn en criminaliteitsbeheersing worden doorbroken. Doen ondernemers dat niet, dan zullen zij eerder vroeg dan laat hardhandig wakker worden geschud. Het is denkbaar dat de computercriminaliteit hierbij als wekker gaat werken", aldus Van Lede.

In de meeste gevallen van computercriminaliteit heeft de dader gebruik gemaakt van het onvoldoende toepassen van beveiligings- en controlemaatregelen door het slachtoffer. Minder is door de daders gebruik gemaakt van technische kennis om beveiliging te omzeilen of buiten werking te stellen.

Van Lede tekende hierbij aan dat over schade door computercriminaliteit nog steeds weinig bekend is. Wel zijn er cijfers beschikbaar van Franse verzekeraars. Daaruit blijkt dat de veertienhonderd in 1989 gemelde gevallen van computercriminaliteit in totaal voor *f* 1,4 miljard schade hebben veroorzaakt. "Dat is dus *f* 1 miljoen per schadegeval", aldus

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.

Van Lede. "Naar verhouding zou het in Nederland dan gaan om zo'n driehonderd gevallen van computercriminaliteit met een schade van al snel enkele honderden miljoenen guldens."

AANBEVELINGEN

In zijn rapport doet het Platform Computercriminaliteit een aantal aanbevelingen. Omdat blijkt dat beveiliging schade die door computercriminaliteit is ontstaan, in veel gevallen kon beperken of zelfs voorkomen, is computerbeveiliging in de ogen van het Platform een absolute noodzaak. Voorzitter prof. J. van Oorschot: "In de meeste gevallen van computercriminaliteit heeft de dader gebruik gemaakt van het onvoldoende toepassen van beveiligings- en controlemaatregelen door het slachtoffer. Minder is door de daders gebruik gemaakt van technische kennis om beveiliging te omzeilen of buiten werking te stellen. Uit de enquête blijkt dat een groot deel van de organisaties onvoldoende zorg heeft voor de beveiliging tegen computercriminaliteit".

Volgens het Platform moet er ook meer aangifte worden gedaan. Dat kan best, omdat de bestaande vooroordelen ten aanzien van ondeskundigheid bij politie en justitie en de risico's van het uitlekken van informatie niet door het onderzoek worden bevestigd.
Verder wil het Platform onder meer dat de verspreiding van computervirussen zelfstandig strafbaar wordt gesteld.
Daarnaast moet er een landelijk aanspreekpunt voor slachtoffers van computercriminaliteit komen en acht het Platform het noodzakelijk verder onderzoek naar deelaspecten van computermisbruik te doen.
Bovendien verdient het aanbeveling meer voorlichting te geven. Zo vindt het Platform het "een niet onbelangrijke maatregel" om het bewustzijn van met name werknemers te vergroten, in het bijzonder ten aanzien van het illegaal kopiëren van computerprogramma's. Uit interviews is namelijk gebleken dat het met illegaal kopiëren en gebruiken van computerprogramma's "net is als met fietsen zonder licht in Amsterdam", aldus het Platform. "Men weet dat het niet mag, maar het wordt massaal gedaan, er is geen (sociale) controle en er wordt niet of nauwelijks tegen opgetreden".

EDP AUDITORIUM

In dit nummer van Compact wordt veel aandacht besteed aan privacy. Ook de boekbesprekingen behandelen dit onderwerp. Onlangs verscheen NIVRA-geschrift 58 omtrent privacy en de rol van de accountant. Verder promoveerde de informaticajuriste A.C.M. Nugter op een onderzoek naar de Europese aspecten en barrières voor geautomatiseerd persoonsgegevensverkeer. De beide werken worden uitvoerig besproken door privacy-deskundigen van het eerste uur. Verder in EDP Auditorium aandacht voor de KPMG Klynveld scriptieprijs voor EDP Auditing. Tot slot volgt een korte bespreking van de oraties uitgesproken door twee pas aangetreden hoogleraren op het gebied van informaticarecht en accountancy/EDP-auditing.

BOEKBESPREKING

A.C.M. Nugter, *Transborder Flow of Personal Data within the EC. A Comparative analysis of the privacy statutes of the Federal Republic of Germany, France, the United Kingdom and The Netherlands and their impact on the private sector*, dissertatie Utrecht, handelseditie, Kluwer Law and Taxations Publishers, Deventer, 1990 (XVIII/434 blz.).

Inleiding

Met de toeneming van het internationale handelsverkeer – Europa 1992 is dichtbij – krijgt ook de EDP-auditor steeds meer belangstelling voor de internationale invloeden op de kwaliteit van de geautomatiseerde informatieverwerking. Een belangrijk kwaliteitsaspect in dit kader is privacy, dat veelal op gespannen voet staat met de vrije uitwisseling van gegevens. Het hier besproken boek geeft aan de geïnteresseerde jurist, EDP-auditor en overige beroepsmatig bij geautomatiseerd gegevensverkeer betrokken personen op unieke wijze inzicht in deze spanning.
Voor de goede verstaander: recensent was lid van de zogenaamde leescommissie die het besproken werk vóór de promotie heeft moeten beoordelen. Laat ik al dadelijk mijn oordeel van toentertijd geven: een voorbeeldige methode van onderzoek. De privacy-problematiek wordt benaderd met een duidelijk eigen uitgangspunt en ordelijk op een rij gezet. Het rechtsvergelijkend overzicht van de privacy-wetgevingen van vier EG-lidstaten dat Nugter presenteert is verheugend beknopt.

Focus van het onderzoek

Nugter concentreert zich op grensoverschrijdend dataverkeer in de particuliere sector, op "firms doing business" om het in haar eigen woorden te zeggen. Dat in de particuliere sector ook instanties voorkomen die geen business bedrijven (de particuliere non-profitsector), is een gebied dat in het boek niet voorkomt. Het straks nog te noemen voorstel voor een EG-Richtlijn inzake data protection bevat een uitzonderingsclausule voor die sector. Ledenlijsten van verenigingen behoeven niet aan de subtiliteiten van privacy-bescherming te worden onderworpen als er –paradoxaal genoeg – met betrekking tot die lijsten maar géén inbreuk op de privacy wordt gemaakt. Volgens artikel 3 lid 2 sub b van de concept EG-Richtlijn zijn de bepalingen van de richtlijn niet van toepassing op ledenlijsten van verenigingen zonder winstoogmerk indien de leden toestemming hebben gegeven op de lijst te worden opgenomen én hun gegevens niet aan derden worden verstrekt.
Naast gegevensverkeer bij "firms doing business" gaat het Nugter voorts om persoonsgegevens die geautomatiseerd worden verwerkt én om gerichte, niet-openbare dataverspreiding. Dossiers, kaartenbakken en dergelijke vallen derhalve buiten haar onderzoek, evenals verspreiding van gegevens via massamedia.
Zij behandelt, in het voetspoor van de classificatie van de OECD grensoverschrijdend dataverkeer binnen de onderneming, data die internationale handelstransacties begeleiden, grensoverschrijdende handel in persoonsgegevens en grensoverschrijdende diensten van computerbureaus.
Eerdere net zo veel omvattende publikaties over dit onderwerp ontbraken tot nu toe in ons land. Het enige rechtsvergelijkende overzicht van Nederlandse auteurs op dit gebied tot nu toe was dat van Slagter. Hij schreef ten behoeve van de direct marketing-sector het rapport *International comparison of data protection and privacy protection*[1].

Vergelijking privacy-regelingen

Naast de vier in de titel genoemde landen worden twee internationale systemen afzonderlijk besproken: de Conventie van de Raad van Europa inzake de bescherming van individuen met betrekking tot de automatische verwerking van persoonsgegevens (Straatsburg, 1981) en de toepassing van het EG-Verdrag op grensoverschrijdend gegevensverkeer. De OECD-Richtlijnen worden in enkele bladzijden kort beschreven, maar niet afzonderlijk behandeld. Dat is toch jammer: er is geen fraaiere collectie beginselen te bedenken dan die van de OECD. Wie informationele privacy – en zelfs het ruimere privacy-begrip – goed wil doordenken, heeft die beginselen als een soort van bijbel nodig.
Nugter bespreekt de privacy-wetgeving van de genoemde vier EG-lidstaten telkens afzonderlijk. Dat vind ik niet echt handig: om te weten te komen hoe het bijvoorbeeld met de regeling voor derdenverstrekking zit in ieder land, moeten al de desbetreffende vier hoofdstukken worden nagelopen. Zij hanteert daarbij overigens wel steeds dezelfde systematiek en dat verzacht de bladerpijn ietwat. Beter is wat dat betreft haar behandeling

1 *W.J. Slagter, International comparison of data protection and privacy protection, Services Postaux Européens, Montreux, 1986. De Graaf's (red.) losbladige uitgave Handboek Privacybescherming en Persoonsregistratie bevat overigens ook teksten van buitenlandse wetgeving en ander rechtsvergelijkend materiaal. Daarnaast is in september 1990 gepubliceerd Douwe Korff, Data Protection and Direct Marketing. A Study of the National and International Legal Framework of Data Protection Rules Applicable to the Direct Marketing Industry, including a First Assessment of a Proposed EC Council Directive on Data Protection, commissioned by EDMA, The European Direct Marketing Association, 34 Rue du Gouvernement Provisoire, B-1000 Brussels, Belgium, September 1990, 54 blz. prijs 3000 Bfr.*

van het echte onderwerp: een rechtsvergelijkend overzicht van de bepalingen omtrent grensoverschrijdend dataverkeer in hoofdstuk 7. Hier worden telkens per onderdeel (territoriale reikwijdte, export en import van data) de verschillende nationale systemen achter elkaar gezet. Aan de hand van schematische overzichten worden de bevindingen geïllu-streerd en in een conclusie worden de verschillen duidelijk gemaakt. Dit is een hoofdstuk om enthousiast van te worden, hetgeen overigens ook geldt voor hoofdstuk 8 (over de Conventie van de Raad van Europa van Straatsburg). Dat soort werk is de basis voor haar conclusie: er is een harmonisatierichtlijn nodig, en dan op het hoogste niveau van bescherming. Nugter toont overtuigend aan dat wij ons heil voor een goede regeling van grensoverschrijdend gegevensverkeer niet in het Verdrag van Straatsburg moeten zoeken. Uitgaande van de hypothese dat de vier onderzochte lidstaten alle de Conventie hebben ondertekend, weet ze waar te maken dat de Conventie slechts een theoretische en zeker geen praktische betekenis heeft voor het harmonisatieprobleem.

Belemmeringen door nationale wetgeving

De lezer zal zich afvragen of er in dit boek eigenlijk geen twee verschillende onderwerpen worden behandeld: een rechtsvergelijkend overzicht van de informationele privacy-wetgeving in vier EG-lidstaten en de problematiek van het grensoverschrijdend dataverkeer. De hoofdtitel van het boek betreft het laatste, de ondertitel het eerste gebied. Inderdaad is het de vraag of analyse van louter interne, nationale wetgeving noodzakelijk is voor een beter begrip van de problematiek van het grensoverschrijdend gegevensverkeer. Dat klemt temeer wanneer men ziet hoe schrijfster haar onderwerp beperkt tot de behandeling van "point to point delivery of messages based on contractual relationships between parties" in de particuliere sector, uitsluitend betrekking hebbend op geautomatiseerd verwerkte data. Had het niet meer voor de hand gelegen alleen de nationale en internationale bepalingen inzake grensoverschrijdend gegevensverkeer te beschrijven? Dat had vier hoofdstukken (op de tien) gescheeld die alleen de nationale privacy-wetgevingen behandelen, niet specifiek de problematiek van grensoverschrijding (die wordt immers per land afzonderlijk behandeld in het reeds geprezen hoofdstuk 7).

Toch is schrijfsters behandeling wel juist: er bestaan, ook bij de meer fundamentele begrippen als subject en object van privacy-wetgeving, aanzienlijke verschillen in de wetgeving van de vier behandelde lidstaten. Die verschillen zijn op hun beurt als even zovele belemmeringen op een vrij gegevensverkeer te beschouwen. De verschillen in wetgeving maken de rechtspositie van de geregistreerde onoverzichtelijk en moeilijk verdedigbaar. Ik noem hier als voorbeeld de uitzonderingspositie die Nederland inneemt bij de bepaling van het object: het statische begrip "persoonsregistratie" in plaats van het dynamische begrip "processing" zoals dat in de overige drie landen wordt gebruikt en overigens ook in de komende EG-Richtlijn.

Wat vindt de lezer niet in dit boek

De problematiek rondom data protection is omvangrijk. Schrijfster heeft zich uiteraard moeten beperken in haar behandeling ervan. Zonder dat altijd als omissies te beschouwen, meld ik enige onderwerpen in verband met data protection die de lezer niet in dit boek aantreft.

Een kritische analyse van het privacy-begrip zelf
De beroemdste definitie van privacy is die van Alan Westin: "privacy is the claim of individuals (...) to determine for themselves, when, how and to what extent information about them is communicated to others". Nugter neemt Westins definitie voor lief. Die definitie heeft nogal wat consequenties, die echter niet op basis van de definitie verder zijn uitgewerkt. Nugter zet alleen en terecht een kanttekening bij Westins incorporatie van groepen en instituten onder het subject van het recht op privacy ("the individual").
Overigens wordt de definitie bij mijn weten door niemand letterlijk genomen. Wat dat betreft is vermelding van deze definitie meer een ritueel dansje dat eerlijk gezegd bij de meeste beschouwingen over privacy voorkomt - dan een serieuze beschouwing over het begrip.

De context van het privacy-begrip
Informationele privacy-wetgeving (wetgeving met betrekking tot het gebruik van persoonsgegevens) is een onderdeel van de bescherming van het bredere begrip "persoonlijke levenssfeer". Deze constatering is van belang om de principes en de beperkingen van specifiek informationele privacy-wetgeving beter te begrijpen. Gebreken in informationele privacy-wetgeving zouden wel eens met behulp van meer algemene regels inzake de bescherming van de persoonlijke levenssfeer kunnen worden opgevangen. Een Nederlands voorbeeld hiervan is de ontwikkeling in de jurisprudentie omtrent het inzagerecht van een geregistreerde in zijn gegevens toen de WPR nog niet van kracht was. Voor die situaties die buiten de WPR vallen blijft het voor een geregistreerde overigens ook nu nog mogelijk om op dit algemene recht bij de rechter een beroep te doen.
Ook in deze en dergelijke gevallen zijn uiteraard verschillen per land te constateren. Die verschillen kunnen op hun beurt van invloed zijn op het bijzondere regime voor de informationele privacy dat in dat land geldt, zelfs als er een EG-harmonisatierichtlijn bestaat. Men denkt maar aan een Franse, Zweedse, Spaanse of Nederlandse uitleg van het begrip "redelijk belang van de geregistreerde" bij bijvoorbeeld inzage in zijn eigen gegevens. Een onderwerp dat helaas niet nader wordt behandeld in het boek van Nugter.

Bescherming van gegevensbestanden op basis van intellectuele eigendomsrechten
Impliciet in Nugters betoog is dat dataverkeer steeds met toestemming geschiedt van de dataverzamelaar. Van de wetgeving met betrekking tot de inhoud van gegevens worden software-bescherming en exportbeperkingen op technologie-overdracht in Nugters boek dan ook niet behandeld.
In de rechtspraak wordt tegenwoordig erkend, dat er op databestanden auteursrecht kan rusten, ook

indien de bestanden persoonsgegevens[2] bevatten. Dit betekent mijns inziens dat er tegenwoordig op zijn minst vier afzonderlijke wijzen van zeggenschap bestaan met betrekking tot databestanden die persoonsgegevens bevatten:

1. die van de economisch eigenaar die de bestanden als vermogensbestanddeel op de balans zet;
2. die van de houder in de zin van (bijvoorbeeld) de WPR die zeggenschap uitoefent over het omgaan met registraties;
3. die van de intellectuele eigenaar aan wie een auteursrecht toekomt op zijn creatieve verzamelaarsprestatie; en ten slotte
4. die van degene om wie het allemaal gaat: de geregistreerde. Deze moet naar mijn mening ook en vooral worden gezien als de economisch eigenaar van waardevolle gegevens.

Terecht verdedigde Nugter overigens tijdens de promotie dat de visie van de geregistreerde als "economisch belanghebbende" in de praktijk weinig verschil zal maken. Dit omdat behartiging van de economische belangen van geregistreerden bijna per definitie gegevensverstrekking aan derden (lees: aan bureaus die optreden als makelaar in persoonsgegevens) zal impliceren.
De eerste drie categorieën zullen in de praktijk vaak in één persoon zijn verenigd, maar noodzakelijk is dat niet. Gaat het om meerdere personen, dan zijn mogelijke conflicten tussen de verschillende wijzen van zeggenschap en de bijbehorende aansprakelijkheid niet uitgesloten. Ook kan dit nadelige consequenties hebben voor de privacybescherming en voor de "free flow of information", de twee beginselen die Nugter op hun verzoenbaarheid beproeft.

Uitsluiting van aansprakelijkheid
Verkade heeft in het blad Computerrecht[3] zeer precies aangegeven dat uitsluiting van aansprakelijkheid die de WPR oplegt aan de houder (en aan de bewerker van een registratie) eigenlijk niet mogelijk is. Dit vanwege het dwingendrechtelijke karakter van de regeling. "Exoneration" of iets dergelijks treft de lezer in het trefwoordenregister van Nugter echter niet aan. Toch valt aan te nemen dat dit Nederlandse systeem niet op dezelfde wijze in andere EG-lidstaten geldt. Ook dat is een factor die bij overigens gelijke inhoudelijke privacy-wetgeving verschillen tussen de privacy-regimes van de lidstaten kan veroorzaken.
En dan ga ik nog maar voorbij aan juridische constructies om privacy-wetgeving te ontduiken die ook per land verschillend kunnen zijn. In de Nederlandse praktijk is het bijvoorbeeld mogelijk gebruik te maken van gegevensbestanden terwijl de gebruiker niet als houder kan worden aangemerkt omdat hij geen zeggenschap heeft over de gegevens. Houder is namelijk een nogal misleidend begrip in de WPR. Daarmee wordt niet bedoeld degene die – zoals dat in ons privaatrecht geldt – goederen houdt voor de eigenaar, maar degene die eigendomsbevoegdheden mag uitoefenen met betrekking tot de persoonsgegevens. Welnu, ieder die op de een of andere wijze naast de eigenaarhouder de beschikking krijgt over persoonsgegevens, zonder over opslag van die gegevens, doel van de registratie, beëindiging daarvan, etc. te mogen beslissen, valt niet als houder te beschouwen. Hij heeft dus ook niet de verplichtingen zoals de WPR die aan de houder oplegt. Dat is bijvoorbeeld zo als hij een gegevensbestand voor eenmalig gebruik "huurt" voor geadresseerde direct mail-acties, zonder dat hij als huurder de gegevens zelf onder zich krijgt. De resultaten (de geregistreerde ontvangt aanbiedingen als had de huurder zelf over de adressen beschikt) zijn echter identiek aan een actie door de houder!

Infrastructuur van telecommunicatie
Nugter sluit van behandeling in haar boek uit de zogenaamde *conduit regulations*, dat wil zeggen de regelingen met betrekking tot het telecommunicatieverkeer zelf dat wordt gebruikt voor gegevensverzending. De definitieve versie van een voorstel voor een Richtlijn van de Raad inzake data protection is gepubliceerd te zamen met een voorstel voor een Richtlijn van de Raad betreffende privacy en telecommunicatie[4]. Het laatste voorstel is om een aantal redenen nodig naast een algemene Richtlijn voor de informationele privacy (data protection). De algemene Richtlijn heeft nu eenmaal geen betrekking op de infrastructuur van digitale telecommunicatievoorzieningen. Er ontstaan echter door de inrichting van die infrastructuur wel degelijk situaties waarmee de persoonlijke levenssfeer gemoeid is, zelfs in ruimere zin dan alleen de informationele privacy.
Vooralsnog heeft de ontwerp-Richtlijn in hoofdzaak betekenis voor het openbare telefoonverkeer, voor PTT Telecom dus. Onder openbaar telefoonverkeer valt overigens ook telefonische werving, telewinkelen en het raadplegen van videotekst. De ontwerp-Richtlijn bevat dan ook bepalingen die de telecommunicatie-organisatie verplichten toezicht te houden op dienstverleners die van haar voorzieningen gebruik maken. Tante Pos dus als hoedster van de privacy.

Naar een harmonisatierichtlijn

Hoe kunnen de begrippen "optimale bescherming van de geregistreerde" en een "vrij dienstenverkeer van gegevens" nu op één lijn worden gebracht? Volgens Nugter zijn de Conventie van de Raad van Europa, eventuele contractuele oplossingen of een optionele harmonisatie niet bruikbaar. Haar proefschrift bevat een krachtig en gemotiveerd pleidooi voor een totale harmonisatie van de nationale privacy-wetgevingen op basis van artikel 100A van het EG-Verdrag. Op 24 september van dit jaar is dit pleidooi gehonoreerd met de publikatie van het voorstel voor een Richtlijn betreffende de bescherming van personen in verband met de behandeling van persoonsgegevens, gebaseerd op artikel 100A en gericht op een hoog beschermingsniveau. Op dit hoge beschermingsniveau is van de kant van het bedrijfsleven al de nodige kritiek geuit[5]. Deze kritiek is inhoudelijk en gaat niet in op de vraag wat een economisch orgaan als de Europese Commissie eigenlijk van doen heeft met de bescherming van mensenrechten, zoals dat van de bescherming van de persoonlijke levenssfeer. Het is immers een lange weg van douane-unie naar behartiger van "human rights" die de commissie hier aflegt.

2 *In Nederland bijvoorbeeld Rb. Amsterdam 17 mei 1989, gepubliceerd in Informatierecht/AMI, 1990/3, blz. 51-52; Pres. Rb. Haarlem 5 december 1989, gepubliceerd in Informatierecht/AMI, 1990/3, blz. 54-56; Pres. Rb. Arnhem 19 januari 1990, gepubliceerd in Informatierecht/AMI, 1990/3, blz. 57-59. Zie voor het probleem in het algemeen: P.B. Hugenholtz, Auteursrecht op informatie, Kluwer Deventer, 1989.*

3 *D.W.F. Verkade, Afwijken van de Wet Persoonsregistraties bij (standaard) contract?, Computerrecht, 1988/1, blz. 17-20.*

4 *Voorstel voor een Richtlijn van de Raad betreffende de bescherming van personen in verband met de behandeling van persoonsgegevens, COM (90) 314 def. - SYN 287, Brussel, 24 september 1990; Voorstel voor een Richtlijn van de Raad betreffende de bescherming van persoonsgebonden gegevens en van de persoonlijke levenssfeer in het kader van openbare digitale telecommunicatienetten met name in het kader van het digitaal netwerk voor geïntegreerde diensten (ISDN) en van openbare digitale mobiele netwerken, COM (90) 314 def. - SYN 288, Brussel, 24 september 1990.*

5 *Zie hierover het bij noot 1 genoemde rapport van Korff en de reactie van het European Advertising Tripartite, d.d. 12 oktober 1990, in Nederland verspreid door het Direct Marketing Instituut Nederland (DMIN) te Amsterdam.*

De meest fundamentele inbreuken op privacy vinden vaak plaats op terreinen die niet binnen de werkingssfeer van de Gemeenschap vallen: bij bestanden uit de openbare sector die uitsluitend worden aangehouden ter vervulling van publieke taken. Nugter pleit er dan ook voor dat een harmonisatierichtlijn eveneens onverkort geldt voor die publieke sector. Zij reikt daarbij niet het instrument aan om dat te bewerkstelligen. De Commissie doet dat wel: bij het voorstel voor een Richtlijn heeft zij een ontwerp-resolutie gevoegd van de vertegenwoordigers van de lidstaten van de EG, in het kader van de Raad bijeen. De ontwerp-resolutie heeft tot doel de beginselen van de algemene Richtlijn uit te breiden tot de openbare sector. De burgerkoopman die én handel wil én maximale bescherming van zijn niet-commerciële levenssfeer is hiermee geboren. De discussie over deze politiek van de Commissie is nog niet beëindigd.

Aanpassen WPR vereist?

Nugter geeft in haar slothoofdstuk alleen maar zeer globaal aan wat de inhoud van een richtlijn zou moeten zijn. Dat is jammer: een gedetailleerdere conclusie had ons materiaal verschaft om het huidige voorstel voor een Richtlijn goed tegen het licht te houden. Dat is nodig, omdat de Richtlijn zoals zij er nu ligt aanpassing van onze nog jonge Wet Persoonsregistraties noodzakelijk maakt. Ik noem enkele voorbeelden.
Het ontwerp voor een Besluit Gevoelige Gegevens[6] verbiedt in een aantal gevallen het houden van registraties met gevoelige gegevens zelfs al zou de geregistreerde daarvoor toestemming hebben gegeven. De ontwerp-Richtlijn staat het houden van die bestanden altijd toe als de geregistreerden daarvoor zeer welbewust toestemming hebben gegeven. Hier lijkt de Nederlandse wet te streng.
Over verstrekkingen van zijn gegevens aan derden moet een geregistreerde in het Nederlandse systeem worden bericht, als hij daarom verzoekt; de ontwerp-Richtlijn verplicht tot spontane mededeling. De ontwerp-Richtlijn introduceert voorts een blokkeringsrecht voor geregistreerde ten aanzien van verstrekking aan derden: het systeem dat wij kennen bij het zogenaamde antwoordnummer 666 voor brievenbusreclame. Dit 666-systeem dient dus over de gehele linie te worden ingevoerd.
Ten slotte: de regeling voor grensoverschrijdend dataverkeer in paragraaf 9 van de WPR moet volgens de ontwerp-Richtlijn geheel op de helling. De bevoegdheid om te beslissen of gegevens naar een derde land mogen worden geëxporteerd, komt grotendeels bij de Commissie te liggen. Grensoverschrijdend gegevensverkeer binnen de lidstaten wordt uitputtend geregeld door de Richtlijn.

Conclusie

Nugter heeft een goede hand gehad bij de keuze van haar onderwerp en dat degelijk uitgediept. Er zijn wat schoonheidsfoutjes: ik zou niet zo gauw een samenvatting ná het trefwoordenregister verwachten en word altijd wat hels van het notenkolenkitsysteem[7]. Van de andere kant verheldert Nugter haar betoog met zeer illustratieve schema's. Als voorbeeld noem ik dat op blz. 193-194, waar in één klap de complexe materie van de toepasselijkheid van wetgeving in de vier lidstaten duidelijk wordt gemaakt. Zij zet de lezer aan het denken over de eigenaardigheid van de dienstverlening die het verschaffen van persoonsgegevens is: inbreuk op privacy is inherent aan de dienstverlening zelf, ofwel door de dienstverlening wordt inbreuk gepleegd.
De toepassing van het bekende EG-principe: "wat in land A legaal op de markt is gebracht, mag vrijlijk door de gehele EG worden gedistribueerd", stuit als het om persoonsgegevens gaat op zeer specifieke problemen. Immers, ook de verdere distributie van gegevens kan een afzonderlijke inbreuk op de persoonlijke levenssfeer opleveren. Er valt nog veel te onderzoeken.

Dr. J.J.C. Kabel
Is directielid en hoofdonderzoeker bij het Instituut voor Informatierecht van de Universiteit van Amsterdam. Promoveerde in 1981 op reclamerecht. Kabel geeft onderwijs in het recht van de intellectuele eigendom, het mededingingsrecht en het informatierecht. Daarnaast is hij onder andere deskundige bij het Commissariaat voor de Media en (plaatsvervangend) voorzitter van de Direct Marketing Kamer Codecommissie. Hij publiceert regelmatig omtrent onderwerpen op het gebied van intellectuele eigendom, reclame- en privacy-recht.

BOEKBESPREKING

***Privacy-bescherming; de gevolgen voor organisaties en de rol van de accountant*, NIVRA-geschrift 58, Kluwer Bedrijfswetenschappen, 1991.**

Inleiding

De voorzitter van de Registratiekamer gaat weg, de registratietrein rolt voort. Persoonsregistraties nemen in tal en last toe, burgers vragen zich af waar zij al niet geregistreerd staan en wat er zoal met "hun gegevens" gebeurt.
"Vertrouwen is goed, controle is beter" was niet alleen de slagzin van president Reagan, maar is als het ware de lijfspreuk van accountants. Het is dan ook niet verwonderlijk dat vanuit het NIVRA de ontwikkelingen rondom de privacy-wetgeving – de wetgeving met betrekking tot de bescherming van de persoonlijke levenssfeer – nauwlettend zijn gevolgd. Die wetgeving is niet zonder hindernissen tot stand gekomen, maar de Wet Persoonsregistraties (verder WPR) is op 1 juli 1990 volledig in werking getreden.
Onder auspiciën van de Com-missie van Advies inzake Automatiseringsvraag-stukken van het NIVRA heeft de Werkgroep Pri-vacy het rapport met de in de kop van dit artikel genoemde titel vervaardigd. De materie is zowel vanuit algemeen als vanuit beroepsoogpunt voor accountants van groot belang. Het NIVRA heeft dan ook besloten het rapport uit te brengen als een NIVRA-geschrift, nummer 58. Op 14 januari jl. is het eerste exemplaar hiervan aangeboden aan de plaatsver-

6 *Dit ontwerp-Besluit is gebaseerd op art. 7 van de WPR en werd gepubliceerd in de Staatscourant van woensdag 6 juni 1990, nr. 107.*

7 *Zie bijvoorbeeld blz. 321, noot 63: zie supra noot 45; noot 45: ibidem; noot 44: X, o.c., zie noot 9; noot 9: eindelijk het briefje in de kolenkit gevonden.*

vangend voorzitter van de Registratiekamer.
Het geschrift richt zich tot een zeer brede doelgroep, maar beoogt vooral een handreiking te zijn voor accountants in hun controlerende en adviserende functie.
De basisbegrippen uit de WPR, "persoonsgegevens" en "persoonsregistraties", worden nauwkeurig omschreven, de maatschappelijke betekenis van controle op privacy-bescherming wordt aangeduid en ten slotte wordt in het rapport de (mogelijke) rol van de accountant bij de bescherming van privacy aangegeven.

Inhoud van het geschrift

Ik geef eerst een verkorte samenvatting van de inhoud:
hoofdstuk 1 Inleiding en samenvatting;
hoofdstuk 2 WPR en andere privacy-beschermende bepalingen;
hoofdstuk 3 Privacy-bescherming en organisatie;
hoofdstuk 4 De rol van de accountant;
hoofdstuk 5 Mededelingen omtrent privacy-onderzoek door accountants.

Bijlagen: Toepasselijke rechtsregels, beveiligingsmaatregelen en procedures, checklist-overeenkomst houder-bewerker, model privacy-statuut en een literatuurlijst.
Met opzet noem ik de bijlagen, omdat deze voor de praktijk uiterst nuttige informatie bevatten.

Maatschappelijke betekenis
"Informatie is macht" zou men kunnen zeggen en "ongecontroleerde informatie is supermacht"; reden waarom – zoals in het rapport ook terecht wordt gesteld (paragraaf 1.3) – de maatschappelijke betekenis van controle op privacy-bescherming vanuit zowel macro- als microstandpunt groot is.
Gesteld wordt dat de kwaliteit van de bescherming van privacy in hoge mate wordt bepaald door de kwaliteit van de beveiliging van de (vaak geautomatiseerde) persoonsregistraties. Omdat het bij persoonsregistraties over mensen en niet over guldens gaat, liggen ook de afwijkingstoleranties anders dan bij de financieel-economische administratie. Maar het gaat om administraties en daarom is het "natuurlijk" dat accountants dit gat willen vullen. Gesteld wordt dat het bij de beveiliging van persoonsregistraties gaat om het stellen van normen aan de informatieverzorging en met name aan de interne controle-aspecten daarvan.
De administratieve organisatie wordt dus mede beïnvloed door datgene wat op basis van de WPR moet en kan!
Hoofdstuk 3 van het rapport behandelt daarom de gevolgen van de WPR cum annexis voor de organisatie van degenen die verantwoordelijk en aansprakelijk zijn voor persoonsregistraties (houders, bewerkers en beheerders).
Accountants kunnen een nuttige "derden"-functie vervullen bij controle en advies ten aanzien van persoonsregistraties; op de mogelijkheden van inschakeling van accountants hierbij en de beperkingen die hierbij gelden, gaat het rapport uitvoerig in. De reikwijdte van het accountantsonderzoek en mededelingen omtrent de uitkomsten komen in hoofdstuk 5 aan de orde.

De WPR en aanpalende regelingen
Hoofdstuk 2 van het rapport behandelt de WPR. De hoofdlijnen van de wet plus uitvoeringsregelingen worden duidelijk uiteengezet. Trefwoorden bij de WPR zijn "raamregeling" en "zelfregulering". Duidelijk wordt aangegeven wat wel en wat niet onder de WPR valt en voorts dat het onderscheid (semi-)overheid/bedrijfsleven ook voor persoonsregistraties van belang is.
De bezetter van de Belle van Zuylen-leerstoel in Utrecht – F. Kuitenbrouwer – is verre van tevreden over de manier waarop dit onderscheid in de wet gestalte heeft gekregen. Hij signaleert een groot lek in artikel 18 van de wet. Dit artikel maakt het mogelijk dat gegevens uit persoonsregistraties op het gebied van de overheid, het onderwijs, de gezondheidszorg en de maatschappelijke dienstverlening kunnen worden verstrekt aan andere "overheidsinstanties" voor zover die andere instanties die gegevens nodig hebben voor hun taakuitoefening en de privacy van de geregistreerden niet onevenredig wordt geschaad.
Dit doorgeven van informatie behoeft niet te worden meegedeeld aan geregistreerden en over het "nodig hebben" en het "niet onevenredig schaden" beslist de houder van het bestand zelf. Een situatie die ook mijns inziens schreeuwt om inschakeling van onafhankelijke controleurs die hieromtrent in het openbaar verklaringen afleggen. Aan deze –vooral bij de overheid bestaande – "objectieve behoefte" wordt jammer genoeg in het rapport slechts terloops (in paragraaf 2.3.4) aandacht besteed. In het rapport wordt kort vermeld dat ook op internationaal niveau regulering bestaat c.q. wordt voorbereid.

Privacy-bescherming en (administratieve) organisatie
Privacy is een "kwetsbaar" goed en organisaties die onder andere steunen op informatieverwerkende apparatuur zijn dat vaak ook. De combinatie is derhalve in beginsel "onveilig". Beveiliging is daarom kernwoord in het hoofdstuk dat de rol van de houder van persoonsregistraties beschrijft. Met behulp van een driedimensionaal model (de "beveiligingskubus") – dat in een bijlage handen en voeten krijgt – worden beveiligingsmaatregelen beschreven. Een model voor ontwerp en uitvoering is eveneens in het rapport opgenomen.

De rol van de accountant
In hoofdstuk 4 wordt aangegeven waarom aan de accountant moet worden gedacht bij controle en advies in het kader van privacy-bescherming. Genoemd worden onafhankelijkheid en onpartijdigheid, de bestaande vertrouwensrelatie als gevolg van jaarrekeningonderzoek en de daaruit voortvloeiende kennis van de administratieve organisatie zowel in het algemeen als ten aanzien van het relatiebestand.
In het kader van controle en advies zijn vooral de exclusiviteit, de integriteit en de controleerbaarheid van gegevens van belang; deze dimensies kunnen naar mijn mening door accountants inderdaad goed worden beheerst, als tenminste aan enkele randvoorwaarden is voldaan.
Het rapport stelt terecht dat op basis van een "klassiek" jaarrekeningonderzoek geen mededelingen kunnen worden gedaan ten aanzien van "de stand van de privacy-bescherming".

Van de accountant mogen geen wonderen worden verwacht, dat geldt trouwens ook ten aanzien van jaarrekeningen; wel kan een oordeel worden gegeven over de structuur en het functioneren van de organisatie van de bescherming van privacy.
Het rapport geeft een voorbeeld van een mededeling omtrent uitgevoerde accountantsarbeid in het kader van de privacy-bescherming, waarbij dus vooral de reeds hiervoor genoemde criteria – exclusiviteit, integriteit en controleerbaarheid – centraal staan.

Conclusie

Een overzichtelijk rapport dat de accountant handvatten verschaft en de gebruiker inzicht geeft in wat hij van "zijn" accountant mag en kan verwachten. Eén slotopmerking: in het voorgaande heb ik het gehad over randvoorwaarden waaraan accountants moeten voldoen. Men zal het mij als jurist niet kwalijk nemen dat ik een grondige kennis van de van toepassing zijnde rechtsregels als randvoorwaarde nog eens expliciet noem, doch dit zal voor zich spreken.

Prof.mr.drs. J.Th. Degenkamp
Studeerde economie en rechten aan de Universiteit van Amsterdam. Is hoogleraar inleiding Rechtswetenschap, Burgerlijk Recht en Handelsrecht aan de Rijksuniversiteit Groningen. Sinds 1978 is prof. Degenkamp voorzitter van de VERA-stuurgroep Recht.

UITREIKING KPMG KLYNVELD PRIJS 1990 VOOR EDP AUDITING

Op 22 januari jl. heeft de officiële uitreiking plaatsgevonden van de door KPMG Klynveld ingestelde prijzen voor de beste scripties op de werkterreinen van KPMG. De categorieën betreffen Accountancy, Management Consultancy en EDP Auditing. Voorzitter van de jury van de KPMG Klynveld Prijs 1990 voor EDP Auditing was mevrouw mr. J.C.M. Couzijn. Zij overhandigde de prijs in deze categorie aan de heer ir. M.J.M. van Wonderen, voor zijn afstudeerscriptie aan de faculteit der Technische Wiskunde en Informatica van de Technische Universiteit Delft. Titel van zijn scriptie is: "Definitie en controle van een security policy bij het GAK".
De scriptie geeft op een overzichtelijke wijze een belangrijke aanzet voor de uitwerking van een security policy bij het GAK, gevolgd door een realistische benadering van de informatie die nodig is om de naleving van beveiligingsmaatregelen te toetsen. In het juryrapport is onder meer te lezen dat "Van Wonderen met name een brug heeft geslagen tussen de meer theoretische benadering van computerbeveiliging als deel van het totale beveiligingsbeleid en de praktische uitwerking daarvan. Door het definiëren van programmatuur geeft de scribent duidelijk de praktische waarde aan van de bevindingen van de scriptie".
De scriptie is goed leesbaar, mede doordat achterliggende theoretische verhandelingen en specifieke apparatuurkenmerken naar de bijlagen zijn gebracht.
De jury heeft een bijzondere vermelding in haar rapport opgenomen voor de heer drs. E.M. Peeters (Erasmus Universiteit, Rotterdam) voor zijn afstudeerscriptie getiteld: "Electronic Mail Reliability". Zijn op praktische waarnemingen gebaseerde scriptieconclusie geeft een beeld van de huidige situatie inzake de mate van falen van E-mail voor zover het de transportfunctie op openbare (wetenschappelijke) netwerken betreft. Het is te hopen dat dezelfde conclusie niet ook voor het bedrijfsleven kan worden getrokken.
De scriptie geeft zinvolle aanbevelingen voor het verbeteren van de betrouwbaarheid van netwerken. De redactie van Compact is verheugd dat zij de heer Peeters bereid heeft gevonden om een beknopt artikel uit zijn omvangrijke scriptie voor dit blad samen te stellen. In een van de volgende nummers zult u met dit artikel kennis maken.
De dag werd besloten met een lezing van de heer J. Wilsing, directeur van de CRI (Centrale Recherche Informatiedienst), inzake de rol die hij ziet voor EDP-auditors in het kader van het recherchewerk van de CRI. Over dit onderwerp, ook wel aangeduid als "forensische EDP-auditing", zult u de komende jaren naar verwachting nog het nodige vernemen. *H.v.G.*

ORATIES PROF. A.W. NEISINGH RA EN PROF. MR. J.M.A. BERKVENS

Sinds enige tijd is Nederland twee bijzondere leerstoelen rijker, die in EDP Auditorium niet onbesproken mogen blijven. Aan de Rijksuniversiteit Groningen is de leerstoel "Betrouwbaarheidsaspecten Geautomatiseerde Informatiesystemen" ingesteld, die bezet wordt door prof. A.W. Neisingh RA. Aan de Katholieke Universiteit Nij-megen is prof. mr. J.M.A. Berkvens aangetreden als bijzonder hoogleraar "Recht en In-formatica, in het bijzonder het Informaticarecht". Hierna volgt een korte bespreking van de oraties van de beide hooggeleerde heren, welke zij onlangs uitspraken.

Neisingh

Op 19 maart jl. aanvaardde Neisingh zijn ambt als bijzonder hoogleraar met een rede getiteld *"Betrouwbaarheid en continuïteit van geautomatiseerde gegevensverwerking in het bankwezen: een kritische beschouwing van het Memorandum van de Nederlandsche Bank"*. Naast dit onderwerp gaf Neisingh, vennoot bij KPMG Klynveld EDP Auditors en redacteur bij dit blad, een toelichting op de invulling die hij aan zijn nieuwe leerstoel zal geven. In dit kader beschreef hij, hoe de automatisering van de informatieverzorging het beheersinstrumentarium van het management van ondernemingen en overige huishoudingen beïnvloedt. Hij merkte op, dat ten gevolge van de ontwikkelingen in de informatietechnologie de consequenties voor het stelsel van maatregelen van interne controle zelfs ingrijpend zijn. Voor het accountantsvak heeft dit uiter-

aard eveneens gevolgen van ingrijpende aard. Een accountant zal in een dergelijke geautomatiseerde omgeving zijn zelfstandigheid en onafhankelijkheid moeten kunnen behouden. Het mag volgens Neisingh niet zo zijn, dat de accountant "voor de meest elementaire onderzoeken naar de kwaliteit van de administratieve organisatie een beroep zou moeten doen op specialisten". Slechts waar automatisering zo is doorgevoerd, dat de complexiteit van de organisatie onevenredig toeneemt, zal hij een beroep dienen te doen op de specialisten: de EDP-auditors.

CAAT
Behalve aan de implicaties van automatisering van huishoudingen op de aanpak van de accountantscontrole, zal de nieuwe hoogleraar eveneens aandacht besteden aan de ontwikkelingen op het gebied van de automatisering van die controle zelf, ofwel Computer Assisted Audit Techniques.
De leerstoel zal een geïntegreerd deel gaan uitmaken van het doctoraal-curriculum van de accountancy-opleiding. Neisingh merkte op, dat de RuG zich door instelling van deze leerstoel een belangrijke voorsprong heeft verworven ten opzichte van andere universiteiten.

Kritisch gebruiker
In het tweede deel van zijn oratie gaf Neisingh een kritische bespreking van het Memorandum van De Nederlandsche Bank van 1988 omtrent de betrouwbaarheid en continuiteit van geautomatiseerde gegevensverwerking in het bankwezen. Een goed gekozen onderwerp, het handelt immers in feite over de problematiek zoals die tot uitdrukking komt in het onderzoeksgebied van zijn leerstoel. Neisingh schetste de ontstaansgeschiedenis van het Memorandum, waarbij hij zelf als "kritisch gebruiker" betrokken was. Na aandacht te hebben besteed aan de plaats van het Memorandum in het toezicht van DNB en te hanteren normen en beheersingsconcepten ten aanzien van de kwaliteit van de informatievoorziening bij banken, formuleerde Neisingh een aantal voorstellen voor verbetering. Indien de doelstelling van DNB was met het Memorandum een betere aandacht voor de kwaliteit van de automatisering bij banken te bewerkstelligen, dan is zij hierin naar de mening van Neisingh wel geslaagd. Op een aantal punten heeft men de plank naar zijn mening echter niet goed vastgeslagen. Kort gezegd komt het erop neer, dat het Memorandum te weinig is 'geïndividualiseerd" naar de vorm en de positie van de verschillende banken. De bruikbaarheid van het Memorandum verbetert, indien DNB zich zou richten op specifieke (soorten) banken met het voor hen geldende beheersingsconcept. Verder tast het in de huidige vorm de beleidsvrijheid van banken binnen de vereisten van solvabiliteit en liquiditeit te veel aan.

Tot slot merkte Neisingh op, dat het aanwijzen van de management letter als medium om leiding, raad van commissarissen en DNB te informeren over de kwaliteit van de automatisering, zoals is gebeurd in het Memorandum, dit medium wel erg van karakter doet veranderen. Een rapportage aan maar ook over de leiding is nooit de intentie van de management letter geweest, aldus Neisingh.

Berkvens

Bijzonder hoogleraar Berkvens aanvaardde zijn ambt op 1 maart jl. met het uitspreken van de rede *"Congestie op data-highways"*. Berkvens, in het dagelijks leven afdelingsdirecteur juridische en fiscale dienst bij de Rabobank, levert reeds vele jaren een kritische en uiterst produktieve bijdrage (de publikaties die op zijn naam staan zijn respectabel, zowel qua inhoud als qua aantal) aan de ontwikkeling van allerlei aspecten van het vak informaticarecht. Het interessante van zijn oratie was, dat hij nu een aantal van deze onderwerpen bijeen bracht, om aan te geven dat informaticarecht in de fase is gekomen waarin het dient te worden behandeld als een integratievak.

Overregulering
Het wordt steeds duidelijker dat ontwikkelingen in de informatietechnologie een samenhangend cluster van maatschappelijke en juridische vraagstukken oproept, die in wezen niet afzonderlijk van elkaar kunnen worden opgelost. Daarnaast is het volgens de hoogleraar zo, dat de oplossing van deze vraagstukken niet altijd gezocht moet worden in nieuwe wetgeving. Opgepast moet worden voor (nationale en Europese) overregulering, waardoor toekomstige ontwikkelingen in de informatietechnologie niet kunnen worden gevolgd. Zijn stelling is, dat naarmate het aantal wetten op een bepaald terrein toeneemt, de effectiviteit ervan exponentieel afneemt. Onverwachte samenlopen doen zich voor, met als gevolg een reeks van reparatiewetjes.
Opgepast moet ook worden voor het uit het oog verliezen van de samenhang tussen deelvraagstukken en van het doel dat men nastreeft met regulering. Zo moet wetgeving geen onnodige barrières oproepen voor het internationale gegevensverkeer, niet alleen binnen Europa, maar ook niet met landen buiten de EG. Het gevaar van overregulering en van het uit het oog verliezen van samenhang en doelstelling is volgens Berkvens niet gering: het leidt tot congestie op internationale data-highways, en daarmee tot hoge kosten en gemiste kansen.

Data-highways
De data-highways die Berkvens, getrouw aan zijn bancaire afkomst, centraal stelde in zijn oratie, zijn die van het Europese betalingsverkeer, ofwel het stelsel van netwerken dat binnen Europa wordt gerealiseerd. In een kort bestek beschreef hij de aspecten van het opzetten en beheren van beta-lingsverkeersystemen. Aan de orde kwamen de realisatie van de infrastructuur, de relaties tussen betrokken partijen (banken, consumenten, telecommunicatie-exploitanten, nationale en Europese overheden) en de juridische inkadering van de netwerken (onder andere systeemeisen, consumentenvoorwaarden, privacy-bescherming en antimisbruikwetgeving). Twee gebieden waarmee Berkvens zijn stellingen vervolgens treffend toelichtte waren de regulering van de bescherming van de privacy en van software. Allereerst de privacy.

Hondenkennel = persoonsregistratie
De Europese Commissie heeft een tweetal ont-

werprichtlijnen gepubliceerd; de een inzake gegevensbescherming in het algemeen en de ander inzake gegevensbescherming in ISDN (zie voor een nadere aanduiding de boekbespreking van Kabel elders in deze EDP Auditorium). Verontrustend is het volgens Berkvens dat het voorstel voor een algemene privacy-richtlijn zulke algemene en vage definities bevat, dat misbruik of verkeerd gebruik voor de hand lijkt te liggen. Als voorbeeld gaf hij aan, dat op basis van die definities zelfs een hondenkennel als persoonsregistratie kan worden aangemerkt, terwijl het blaffen van de daarin aanwezige honden (persoonsgegevens volgens de richtlijn!) als ongeautoriseerde verstrekking van persoonsgegevens zou kunnen worden aangemerkt.
Berkvens noemde een aantal consequenties van de algemene richtlijn voor het betalingsverkeer: een kostbare investering in administratieve verplichtingen, een verbod op bijvoorbeeld selectieve marketing op basis van geautomatiseerd tot stand gekomen persoonsprofielen (iets waarover overigens consumentenorganisaties zich wellicht weer wel zullen verheugen), de verplichting om "state of the art" beveiligingstechnologie te gebruiken en de onmogelijkheid om tot zelfregulering te komen door middel van een privacy-gedragscode.

Middeleeuwen
Het tweede voorstel voor een richtlijn omtrent de bescherming van persoonsgegevens bij gebruik van openbare digitale communicatienetten bevat eveneens de nodige knelpunten met betrekking tot het betalingsverkeer. Deze ontwerp-richtlijn legt een toestemmings- en controletaak op de nationale PTT's (telecommunicatie-organisaties) ten aanzien van financiële instellingen (dienstverleners/gebruikers van de netten): bij misbruik van gegevens door de dienstverlener wordt de PTT gestraft. Volgens Berkvens "een middeleeuwse benadering die ervoor zorgt dat de boodschapper van het slechte nieuws in de kasteelgracht wordt gegooid"! De richtlijn maakt het zelfs mogelijk, dat dit principe niet alleen op PTT's wordt toegepast, maar ook op bancaire netwerkdienstverleners.

Naar een ander model van gegevensbescherming
Toch staat de systematiek van deze laatste richtlijn ook aan de basis van de voorstellen van Berkvens tot verbetering van privacy-regulering: een ander model van gegevensbescherming. Men dient, aldus Berkvens, onderscheid te maken naar de verschillende fasen van het informatieverwerkingsproces, waarbij uitgangspunt is, dat het gebruik van de gegevens de basis voor regulering dient te zijn, niet de enkele aanwezigheid. Berkvens maakt in dit kader onderscheid tussen gebruiksbestemmingen die zijn gerelateerd aan het individu en gebruiksbestemmingen die zijn gerelateerd aan het informatieverwerkingsproces zelf. Voorbeeld van het eerste is het bijwerken van een abonnementenadministratie of van een rekening-courantverhouding tussen de bank en een individu. Voorbeelden van het tweede zijn het maken van backups of het verzamelen van betalingsopdrachten door de bank en het doorgeven van de opdrachten aan de bank van de begunstigde, maar ook het wettelijk verplicht bewaren van persoonsgegevens voor de fiscus. Dergelijke verzamelingen zijn hulpbestanden, waarvoor (slechts) een meer algemeen regime, gericht op beveiliging van de hulpbestanden dient te bestaan. Berkvens pleit hiermee voor een normatieve benadering in plaats van de administratieve, die tot nu toe gebruikelijk is.

Accountants
Berkvens staat overigens niet alleen in zijn kritiek op de ontwerp-privacy-richtlijnen van de Europese Commissie. Reeds diverse organisaties hebben hun kritiek geuit op de ontwerpen, waaronder The Institute of Chartered Accountants in England and Wales (januari 1991). De kritiek is met name gericht op het feit dat de richtlijnen onnodig restrictief zijn, een enorme administratieve last leggen op met name kleine organisaties en dure investeringen in beveiligingsbeleid noodzakelijk maken. Het laatste woord over de beide richtlijnen is klaarblijkelijk nog niet gesproken.

Softwarebescherming
Op het gebied van de Europese initiatieven te komen tot een richtlijn voor software-bescherming, gebaseerd op het auteursrecht, levert Berkvens eveneens de nodige kritiek. De ontwerp-richtlijn heeft ingrijpende wijzigingen ondergaan onder druk van een omvangrijke internationale lobby van software-exploitanten. Het is de vraag of daarbij de gerechtvaardigde belangen van de gebruikers van die software voldoende in het oog zijn gehouden.
Aan de hand van een aantal voorbeelden stelt hij, dat onder andere in de bancaire sector de eisen ten aanzien van de gebruiks- en onderhoudsmogelijkheden van programmatuur hoog zijn. De voorgestelde richtlijn behoudt het merendeel van de bevoegdheden, nodig om deze behoeften uit te kunnen voeren, echter voor aan de auteursrechthebbende. Dit is niet bevorderlijk voor de continuïteit en flexibiliteit van de gebruiker.
Enkele verbeteringsvoorstellen die hij doet zijn:
- Het gebruiksrecht dient alle niet bij contract uitgesloten gebruiks- en onderhoudshandelingen te omvatten.
- De (vaak zeer ondoorzichtige) eigendomsrelatie met betrekking tot de software dient gesystematiseerd te worden vastgelegd.
- Het deponeren van de sources van de software, ofwel *escrow*, dient wettelijk te worden geregeld.

Conclusie
Berkvens concludeert dat er een tendens te bespeuren valt naar een steeds verder gaande regulering, waardoor de contractsvrijheid dreigt te worden beperkt. De Europese Commissie ontplooit diverse initiatieven die direct of indirect het betalingsverkeer raken, en die veel overlapping vertonen. Partijen verliezen steeds meer de mogelijkheid tot zelfregulering, terwijl zij hiertoe volgens Berkvens op diverse gebieden zeer wel in staat zijn. Het gevaar van te sterke regulering is, dat toekomstige technische en maatschappelijke ontwikkelingen in de kiem worden gesmoord. Zijn advies aan de nationale en Europese overheden is dan ook: benader een nieuw vraagstuk met respectievelijk niets regelen, dereguleren en dan pas met reguleren, in die volgorde. *A.M.Ch.K.*

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.

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
ir. 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

4 17e jaargang 90/4 winter 1990

Informaticarecht en EDP-auditing in perspectief
prof. A.W. Neisingh RA en mw. mr. A.M. Ch. Kemna MBA

Software-bescherming: tien jaar theorie en praktijk
mr. V.A. de Pous

Software-ontwikkelingscontracten
prof.mr. J.M.A. Berkvens

Escrow. Het depot van de broncode: fopspeen of panacee?
mw. mr. A.M.Ch. Kemna MBA

Strafbaarstelling van computermisbruik
R.A. s'Jacob