De Wet Computercriminaliteit een feit

Dr. K.IJ. Mollema

Inleiding

Op 1 maart 1993 is de Wet Computercriminaliteit in werking getreden. Dit is van belang, omdat de wet zowel voor bedrijven als voor accountants van grote betekenis zal zijn. De wet is het resultaat van het werk van de Commissie Franken, die in 1987 zo'n 29 aanbevelingen tot wetswijziging rapporteerde.[1]
De wet heeft drie implicaties:
- wijziging van het Wetboek van Strafrecht;
- wijziging van het Wetboek van Strafvordering en
- wijziging van het Burgerlijk Wetboek.

Alvorens in te gaan op de inhoud van de wet en de maatschappelijke betekenis daarvan, is het nuttig eerst even stil te staan bij een van de kernproblemen die bij het ontwerpen van de wet een rol hebben gespeeld, namelijk het begrip 'gegevens'. Hoewel dit begrip al zo oud is als de mens zelf, heeft de automatisering de potentie van gegevens enorm verruimd en is ook het misbruik ervan op een veel grotere schaal mogelijk geworden. Zoals altijd, ijlt wetgeving na op maatschappelijke ontwikkelingen. Het is pas vrij laat geweest dat de wetgever tot de conclusie is gekomen dat er een hiaat in de wet zat met betrekking tot het begrip 'gegeven'.

Zo is bijvoorbeeld in een arrest over de verduistering van een computerprogramma door het Hof Arnhem[2] geprobeerd om het begrip 'gegeven' onder het begrip 'goed' te laten vallen, in analogie van een oud elektriciteitsarrest[3]. Deze poging is echter weinig vruchtbaar gebleken en heeft veel kritiek ontmoet. Terecht, want de kenmerken van gegevens zijn zeer afwijkend van de kenmerken van goederen. Denk bijvoorbeeld aan de dupliceerbaarheid van gegevens, het op verschillende plaatsen tegelijkertijd beschikbaar zijn, de instabiliteit van gegevens in vergelijking met goederen en men vindt voldoende redenen om geen verband te leggen. In de Wet Computercriminaliteit is de hiervoor gesignaleerde leemte ondervangen door een wettelijke definitie van het begrip 'gegeven'[4], waardoor het gegeven object kan worden van zowel civielrechtelijke als strafrechtelijke als strafvorderlijke bepalingen. Dat is een wezenlijke stap voorwaarts.

Maatschappelijke gewenstheid van de wet

Over het al of niet invoeren van de Wet Computercriminaliteit is veel te doen geweest. Vóór- en tegenstanders hebben elkaar met argumenten bestookt in de literatuur, maar uiteindelijk is het er toch van gekomen.
Argumenten vóór waren uiteraard dat de ontwikkeling van de computertechnologie de definitie van een nieuwe wet nodig maakt. Ook het maatschappelijke fenomeen computercriminaliteit, computermisbruik, 'hacking' gaf daaraan een sterke impuls. De computerhacker die werd betrapt kon strafrechtelijk nauwelijks worden aangepakt; iets wat het rechtsgevoel tekort deed. Voorstanders van de wet bepleitten dan ook

Dr. K.IJ. Mollema, registeraccountant, studeerde Bedrijfseconomie en Accountancy (RUG), in 1990 gepromoveerd (VU). Hij is thans controller van Fortis en verbonden als docent aan de postdoctorale edp audit-opleiding aan de Vrije Universiteit van Amsterdam.

bescherming van bedrijven en organisaties door de overheid tegen criminele inbreuken.
Tegenstanders echter brengen daartegenin dat bedrijven en organisaties zichzelf maar adequaat moeten beveiligen tegen computermisbruik, door het introduceren van een goed beveiligingssysteem. Een ander argument tegen invoering van de wet is de problematiek van het constateren van het delict, het opsporen van de dader, het vaststellen van de plaats van het misdrijf (iets wat in de tijd van grensoverschrijdende netwerken niet eenvoudig is) en de capaciteit en prioriteit bij politie en justitie. Als al vast te stellen valt dat iemand een systeem is binnengedrongen, dan is het nog zeer moeilijk om te zien wie dat gedaan heeft. De vraag lijkt gerechtvaardigd of een politie- en justitie-apparaat, dat onvoldoende succesvol lijkt in de bestrijding van veel hardere vormen van criminaliteit zoals gewapende overvallen, milieudelicten en andere, voldoende prioriteit en capaciteit kan toewijzen aan de opsporing van de computercriminaliteit (zie bijvoorbeeld de jaarlijkse rapportage van de Centrale Recherche Inlichtingendienst).

Na alle voors en tegens te hebben afgewogen, heeft de minister toch gemeend om de wet te moeten voorstellen aan de Kamer, die na enige wijziging de wetsvoorstellen grosso modo conform de oorspronkelijke voorstellen heeft goedgekeurd. Zodoende is op 1 maart jongstleden de wet in werking getreden. Omdat de wet een feit is heeft het weinig zin om nog lang te discussiëren over de nuttigheid daarvan; de tijd zal het leren. De vraag is nu wat de maatschappelijke betekenis van de wet zal zijn voor bedrijven en organisaties, maar ook voor accountants, die daar een rol in spelen.

De betekenis van wet voor bedrijven en organisaties

Bij het analyseren van de betekenis van de wet voor bedrijven en organisaties moet men een onderscheid maken tussen de strafvorderlijke, strafrechtelijke en civielrechtelijke bepalingen.
De strafvorderlijke bepalingen betreffen een uitbreiding van de bevoegdheden van politie en justitie in het kader van de fraudebestrijding. Het gaat hierbij niet om computercriminaliteit, maar om opsporingsbevoegdheden in het kader van onderzoeken tegen verdachte organisaties waar op één of andere manier de computer toegang kan gaan geven tot bewijsmateriaal. De organisatie is dus hierbij niet de benadeelde, maar degene die onder justitiële verdenking staat. Belangrijk is dat een aantal bevoegdheden van politie en justitie die al reeds bestonden nu ook betrekking kunnen hebben op gegevens. Het gaat daarbij onder andere om bevel tot uitlevering en huiszoeking.

Hierbij zijn enige kanttekeningen te plaatsen. Het lijdt geen twijfel dat de fraudebestrijding door politie en justitie de sympathie moet hebben van alle Nederlandse burgers en organisaties. Evenwel moet er ook tegen worden gewaakt dat een overijverig justitieel apparaat onevenredige schade toebrengt. Met name het doen van huiszoeking in computercentra bergt het gevaar in zich een grote schade toe te brengen aan partijen die niet verdacht zijn. Immers veel rekencentra werken voor meer dan één opdrachtgever en omdat bij een huiszoeking weinig anders overblijft dan het stilleggen van het hele computercentrum om een effectieve bewijsgaring mogelijk te maken, valt te vrezen dat ook grote schade kan worden toegebracht aan partijen die met het vergrijp niets van doen hebben. Rechtsbeginselen als het proportionaliteitsbeginsel (het middel moet evenredig zijn met het vergrijp) of het subsidiariteitsbeginsel (bij een keuze uit middelen moet het lichtste gekozen worden) bieden onvoldoende bescherming. Immers men kan op deze beginselen slechts achteraf een beroep doen in een juridische procedure en dan is het leed reeds geleden. Overigens is deze bevoegdheidsverruiming ook niet zonder gevaar voor justitie, daar waar zij het risico gaat lopen om met grote schadeclaims te maken te krijgen. In een van de stellingen bij mijn proefschrift[5] heb ik een pleidooi gevoerd voor een convenant tussen justitie en computercentra (in analogie met het convenant tussen justitie en banken), waar het gaat om het vrijwillig uitleveren van gegevens die noodzakelijk zijn voor juridische bewijsgaring.

Tenslotte zij nog opgemerkt over dit onderwerp, dat het beter was geweest om deze uitbreiding van bevoegdheden in een apart wetje te regelen. Zij heeft namelijk veel verwarring gesticht over wat precies onder computercriminaliteit moet worden verstaan. Duidelijk is dat het onderwerp 'computercriminaliteit' weinig te maken heeft met de verruiming van bevoegdheden van politie en justitie als hiervoor beschreven.

De materieel-strafrechtelijke kant

Het grootste gedeelte van de wet heeft betrekking op strafrechtelijke bepalingen, die grosso modo betrekking hebben op het misbruik maken van gegevens danwel van computersystemen en op het binnendringen van een computersysteem. Daarnaast zijn er nog specifieke technische bepalingen die voor het belang van dit artikel buiten beschouwing worden gelaten. De wet stelt een aantal handelingen ten aanzien van computergegevens of computersystemen strafbaar (Artikel 1 van de wet, inhoudende een aantal wijzigingsbepalingen op het Wetboek van Strafrecht). Daarbij wordt heel systematisch te werk gegaan vanuit de criteria integriteit, exclusiviteit en beschikbaarheid en dat steeds op het niveau van computersysteem of van gegevens, waarbij een tamelijk sluitende opsomming wordt gegeven van handelingen die in het vervolg strafbaar zullen zijn. De vraag komt op waarom naast deze strafbepalingen ten aanzien van ongewenste handelingen ook bepalingen moet worden opgenomen van computervredebreuk. Computervredebreuk is (analoog aan huisvredebreuk) het verboden wederrechtelijk binnendringen in een computersysteem, ongeacht wat men daar uitspookt. De wetgever heeft gemeend om de computervredebreuk strafbaar te moeten stellen, waarschijnlijk omdat vaak moeilijk te bewijzen valt wat iemand die is binnengedrongen in een systeem allemaal gedaan heeft.

Van de strafbaarheid van computervredebreuk moet een hoge preventieve werking uitgaan. De strafbepaling is dan ook niet mals, men kan hiervoor zelfs gevangenisstraf krijgen. Omtrent de computervredebreuk is veel discussie geweest, omdat de wetgever heeft gemeend de dader te moeten vrijwaren van rechtsvervolging in geval er sprake is van een onvoldoende beveiligd systeem. In geval van huisvredebreuk is wel denkbaar dat, indien een huisbezitter achteloos met zijn woning omspringt, justitie besluit om af te zien van vervolging. Het delict op zich blijft echter strafbaar! In geval van de computervredebreuk gaat de wetgever zo ver dat het doorbreken van enige beveiliging voorwaarde is voor strafbaarheid. Dit is iets nieuws en heeft dan ook onder juristen veel teweeggebracht. Een mogelijk nadelige bijkomstigheid is dat de gearresteerde computervredebreker zich altijd zal beroepen op de bepaling dat het systeem onvoldoende beveiligd was. Het bedrijf dat het slachtoffer werd van de computervredebreuk kan daardoor gedwongen worden zijn beveiligingssysteem breed uit te meten in de rechtszaal. Te verwachten valt dat dit risico afschrikkend zal werken voor aangiftebereidheid inzake computervredebreuk.

De wetgever heeft niet willen volstaan met een aantal strafvorderlijke en een aantal strafrechtelijke bepalingen. De wet voorziet namelijk ook in een wijziging van het Burgerlijk Wetboek.

Civielrechtelijke bepaling

Artikel 2:393, lid 4 BW, dat handelt over de accountant, krijgt de volgende toevoeging: 'Hij (de accountant) maakt daarbij tenminste melding van zijn bevindingen met betrekking tot betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking.' De strekking van deze bepaling is die van een stok achter de deur. De wetgever wil als het ware de ondernemer aansporen tot beveiliging en heeft gezocht naar wegen om de accountant daarin een rol te laten spelen. Aanvankelijk werd gekozen voor het jaarverslag als vehikel, waar in het directieverslag melding moest worden gemaakt van de informatiebeveiliging door de directie. Omdat de accountant onwaarheden in het directieverslag niet kan tolereren zou zijn verklaring bij de jaarrekening impliciet iets zeggen over de staat van beveili-

ging. Hierop is van de kant van de Raad van de Centrale Ondernemingsorganisaties (RCO),[6] maar ook van de Commissie Vennootschapsrecht[7] negatief gereageerd naar de minister toe. Met name het argument van laatstgenoemde dat op deze manier de jaarrekening nog voor vele andere doeleinden oneigenlijk te gebruiken zou zijn heeft de doorslag gegeven.

De wetgever heeft een andere keuze gemaakt, namelijk dat de accountant melding moet maken van zijn bevindingen over de beveiliging. Merkwaardig is alleen dat hier niet meer gesproken wordt over beveiliging, maar over betrouwbaarheid en continuïteit, wat een veel ruimere strekking heeft.

De gevolgen van de Wet Computercriminaliteit voor ondernemingen en organisaties

De gevolgen zijn in de eerste plaats in positieve zin dat er meer rechtsbescherming is ontstaan. Een organisatie die een hacker betrapt kan zijn geschonden rechtsgevoel genoegdoen door aangifte en mag verwachten dat er tot een behoorlijke strafvervolging wordt overgegaan. Ook in preventieve zin mag worden verwacht dat hiervan een beschermende werking uitgaat.

Een consequentie van de wet is dat de ondernemer min of meer gedwongen wordt tot een adequate beveiliging van zijn informatiesystemen. Er zijn twee impulsen daarvoor. De eerste is het feit dat de computervredebreker ontslag van rechtsvervolging krijgt in geval van het ontbreken van enige beveiliging. Een andere impuls is dat de accountant hierover iets zou moeten rapporteren in zijn brief aan bestuur en commissarissen. Uit verschillende onderzoeken komt naar voren dat het er met de beveiliging van de informatiesystemen in de Nederlandse bedrijven niet optimaal voorstaat. Impulsen om tot een betere beveiliging te komen mogen dan ook positief worden beoordeeld. Een probleem blijft de aangiftebereidheid van ondernemingen en organisaties. Onderzoek door het Platform Computercriminaliteit[8] heeft uitgewezen dat deze bereidheid vermoedelijk laag zal zijn. Dit valt te begrijpen waar het binnendringen van een computersysteem toch iets in zich heeft van aan de schandpaal genageld worden wegens een onvoldoende beveiliging. Ook het risico dat de details van een beveiligingssysteem in een rechtszaal breed uitgemeten zouden moeten worden zal drempelverhogend werken voor de aangiftebereidheid.

Een van de vragen die bij bedrijven en organisaties zal opkomen is de vraag wat de organisatie eigenlijk mag verwachten van zijn accountant op het gebied van het beoordelen van de beveiliging als onderdeel van betrouwbaarheid en continuiteit. Daarover straks meer.

Gevolgen van de wet voor accountants

Ten tijde van de totstandkoming van de Wet op de Privacybescherming heeft de wetgever nauwelijks gedacht aan de accountant en zijn deskundigheid op het gebied van informatiebeveiliging.

Bij de Wet Computercriminaliteit ligt dat anders. Aan de accountant wordt een belangrijke rol toebedeeld, daar waar wordt verondersteld dat hij, in zijn beoordeling van betrouwbaarheid en continuïteit, zwakheden kan rapporteren aan bestuur en commissarissen inzake onder andere de informatiebeveiliging.

Merkwaardig is dat de minister een bezwaar van de zijde van de RCO dat dit een inhoudelijke uitbreiding van de opdracht aan de accountant zou zijn, heeft weggewuifd. De minister stelt in de memorie van antwoord dat het gaat om een rapportageverplichting inzake bevindingen die de accountant normaliter in zijn jaarrekeningcontrole opdoet en heeft dus *geen* uitbreiding van de opdracht aan de accountant op het oog.[9]
Dit vergt enige nadere bezinning. De minister zegt hier namelijk impliciet mee dat de accountant de betrouwbaarheid en continuïteit van de gegevensverwerking tot op zekere hoogte beoordeelt. (Anders immers zou hij een lege bepaling hebben voorgesteld.)

De vraag of dit waar is valt niet zonder meer positief te beantwoorden. In een analytisch controleconcept, zoals dat bij de meeste financiële instellingen wordt gehanteerd door de accountant, zal onmiskenbaar in belangrijke mate naar betrouwbaarheid en continuïteit worden gekeken en ook de beveiligingsaspecten zullen aan een zekere beoordeling worden onderworpen. Buiten de financiële instellingen echter, is er een richtingenstrijd aan de gang, waarbij de een zich baseert op een zogenaamde systeemgerichte controle en de ander op een gegevensgerichte controle. De accountant die traditioneel gegevensgericht controleert hoeft maar betrekkelijk weinig te zien van de betrouwbaarheid en continuïteit van de gegevensverwerking. Of dat juist is, is een onderwerp van vaktechnische discussie, dat in dit artikel verder niet behandeld wordt. Daarover heeft ondergetekende in eerdere publikaties[10] duidelijk stelling genomen.

De vraag is nu of de accountant, die in zijn accountantscontrole gegevensgericht controleert en dus weinig te melden heeft aan bestuur en commissarissen, niet in de problemen gaat komen. Immers, als hij niets of weinig rapporteert dan kan dat even goed betekenen dat hij niets gevonden heeft als dat hij nergens naar gekeken heeft. En de geadresseerden van zijn brief hebben niet veel houvast om te weten wat zij eigenlijk van de accountant op dit punt mogen verwachten. Dit schept een situatie van onzekerheid, die vervelend is voor de organisaties, de onderneming, en die voor de accountant een verhoogd aansprakelijkheidsrisico zou kunnen herbergen. Het verdient aanbeveling om aan deze situatie van onzekerheid een einde te maken. Omdat de wetgever artikel 393 heeft uitgebreid verdient het dan ook aanbeveling dat de accountant en zijn opdrachtgever om de tafel gaan zitten om tot een nieuwe gezamenlijke vaststelling van de opdracht aan de accountant te komen. De opdrachtgever moet daarbij duidelijk maken aan zijn accountant wat hij van hem verwacht op het gebied van beoordeling van betrouwbaarheid en continuïteit, inclusief de beveiliging. De accountant op zijn beurt moet aan zijn opdrachtgever kenbaar maken wat hij in zijn jaarrekeningcontrole doet aan het beoordeling van betrouwbaarheid en continuïteit, met andere woorden wat de opdrachtgever van hem mag verwachten. Op grond van deze beide beelden dienen opdrachtgever en accountant tot een nieuwe definitie te komen voor de toekomst van de taak van de accountant bij de onderneming.

Dit gedaan hebbende, zijn er twee interessante consequenties. Ten eerste is het nieuw dat de accountant expliciet maakt wat hij in zijn jaarrekeningcontrole doet aan beoordeling van betrouwbaarheid en continuïteit, met andere woorden hoe zijn methode van controle is. Tot nu toe heeft dit zich aan het oog van de opdrachtgever in belangrijke mate onttrokken.

Het tweede gevolg is dat de accountant met zijn opdrachtgever om de tafel zit over deze problematiek en zo een gemakkelijk aanknopingspunt heeft voor aanbieding van adviesdiensten die kunnen leiden tot een bijzondere opdracht. Dit zou de informatiebeveiliging aanzienlijk kunnen verbeteren, waardoor computercriminaliteit bemoeilijkt wordt.
Bovendien geeft het een mooie gelegenheid om de zogenaamde 'expectation gap' te dichten ten aanzien van de verwachting van de ondernemer over de automatiseringscompetentie van zijn accountant.[11] De accountant gewapend met een herziene opdracht kan zich ook veiliger voelen voor wat betreft zijn aansprakelijkheidsrisico, omdat er duidelijkheid bestaat over wat zijn opdrachtgever van hem mag verwachten.[10]

Conclusies

De Wet Computercriminaliteit is een wet van grote maatschappelijke betekenis. Voor justitie, voor ondernemingen en voor de accountant. Justitie ziet zijn bevoegdheden verruimd, de onderneming is beter beschermd, maar wordt gedwongen tot betere beveiliging en nuttigheid van accountantscontrole neemt toe doordat een bijprodukt wordt geleverd dat wezenlijk kan bijdragen aan verbetering van de informatiebeveiliging.

Interessant is nog hoe de Nederlandse nieuwe wet zich verhoudt tot wetgeving in de overige EG-landen. Geconstateerd kan worden dat er grote verschillen zijn. Iets wat ongewenst is, omdat computercriminaliteit moeiteloos landsgrenzen passeert. Europese harmonisatie van de wetgeving, of liever nog in bijvoorbeeld OESO-verband, lijkt daarom de enige effectieve manier om de mondiale computercriminaliteit te weerstaan.

Voor degenen die geïnteresseerd zijn in meer details over dit onderwerp wordt verwezen naar een nieuw NIVRA-geschrift no. 62[12] dat in april is verschenen over de computercriminaliteit, de wetgeving, de gevolgen voor bedrijven en de accountant. In dit 75 pagina tellende boekje vindt men een handzame uitwerking van de problematiek.

Noten

1 H. Franken e.a., *Informatietechniek & Strafrecht*, Staatsuitgeverij 1987.
2 Hof Arnhem, 27 oktober 1983, NJ 1984, 80.
3 HR 23 mei 1921, NJ 1921, 564.
4 WCC artikel 1, inhoudende toevoeging WvS art. 80 quinquies.
5 K.IJ. Mollema, *Zichtbaarheid van Informatiekwaliteit*, Samsom Alphen a/d Rijn 1991.
6 Tweede Kamer der Staten-Generaal, *MvA 21551*, nr. 6, 15 juli 1991.
7 Brief Commissie Vennootschapsrecht aan de minister van Justitie d.d. 11 december 1990.
8 F.H. Charbon en H.W. Kaspersen, *Computercriminaliteit in Nederland*, Stichting Beheer Platform Computercriminaliteit, RCO Den Haag 1990.
9 Tweede Kamer der Staten-Generaal, *Nota n.a.v. eindverslag* nr. 11, 13 april 1992.
10 K.IJ. Mollema, EDP audit, vak met een toekomst?, *de Accountant* nr. 8, april 1989.
11 Limperg Instituut, *Opvattingen over accountants*, 1990.
12 K.IJ. Mollema, H. Franken e.a., Computercriminaliteit, *NIVRA-geschrift 62*, reeks Automatisering & Controle, Kluwer 1993.