

Juridische consequenties van misbruik van informatie

Prof. Mr. H. Franken

1 Inleiding

Is computercriminaliteit realiteit of fictie? De kranten geven van tijd tot tijd het relaas van een geslaagde 'kraak'. Ook een fraudeur haalt wel eens de kolommen van een dagblad. Uit deze enkele publikaties blijkt evenwel bij lange na niet de ernst en de omvang van het misbruik dat wordt gemaakt van de moderne middelen van informatietechniek. Deze middelen scheppen niet alleen kansen voor nieuwe vormen van schadelijk gedrag zoals het inbreken in informatiesystemen en het afluisteren van telecommunicatie, maar leveren ook bijzonder krachtige instrumenten om bestaande delictsvormen als fraude en oplichting te plegen met aanzienlijk grotere gevolgen dan tot voor kort mogelijk was. Fraude met behulp van computers blijkt in de Verenigde Staten gemiddeld 25 keer zo lucratief te zijn als een bankoverval en bracht vijf jaar geleden al gemiddeld 670.000 dollar op. Het gaat steeds om grote bedragen, waarbij de dader niet wordt beperkt door de hoeveelheid geld die in de kas aanwezig is. Een bankinstelling in Nederland verloor in 1986 f 87 miljoen ten gevolge van manipulaties door computerprogrammeurs en een ambtenaar uit Rotterdam wist deze gemeente f 8,6 miljoen lichter te maken door te knoeien in de rekeningbestanden. De meest recente gegevens, die aanspraak kunnen maken op betrouwbaarheid, komen uit Frankrijk.¹ Zij geven aan, dat de in 1990 bij verzekeringsmaatschappijen geclaimde schadebedragen flink zijn gestegen als het gaat om schade, die opzettelijk is toegebracht bij het gebruik van computers en programmatuur. Dit cijfer staat in contrast met de schade ten gevolge van fouten in overmachtssituaties. De grotere gebruikersvriendelijkheid en betere organisatie van back-up fa-

ciliteiten verklaren een daling van de schade ten gevolge van schuld. De schade ten gevolge van het opzettelijk misbruik bedroeg echter in 1990 in Frankrijk meer dan f 1,5 miljard.

We weten, dat kennis macht is. Kennis – beter gezegd informatie – kan ook ten nadele van anderen worden gebruikt. We denken daarbij dan in het bijzonder aan

- schending van geheimen;
- manipuleren van gegevens (diverse vormen van fraude) en
- verstoring van de overdracht van informatie.

2 Een pakket van maatregelen

Het bestrijden van dit schadeveroorzakend gedrag dient op verschillende manieren plaats te vinden. In de eerste plaats is het aan de burger zelf om schade ten gevolge van informatiemisbruik te voorkomen. Hiertoe kan hij voor de hand liggende fysieke beschermingsmaatregelen nemen en waarborgen inbouwen in de organisatie van zijn onderneming (functiescheiding is een eerste vereiste). Ook is het noodzakelijk om een beveiliging aan te brengen in de te gebruiken programmatuur. Daarna komen juridische maatregelen aan de orde. Het is te vergelijken met de beveiliging van een huis. Vóór iemand met vakantie gaat, sluit hij zijn woning af. Men volstaat niet met te vertrouwen op een wettelijk verbod van inbraak.

Prof. Mr. H. Franken is hoogleraar in de Inleiding tot de rechtswetenschap en het Informatierecht aan de Rijksuniversiteit te Leiden en in de Juridische Informatica aan de Rijksuniversiteit te Groningen. Hij was voorzitter van de Commissie Computercriminaliteit en is vice-voorzitter van de Stichting Geschillenoplossing Automatisering.

De juridische maatregelen kunnen liggen in de preventieve sfeer, zoals het deponeren van broncode bij een onafhankelijke persoon of instantie, zoals een notaris of een uitwijkinginstelling. We denken dan evenwel voornamelijk aan de overdracht van het risico op schade aan anderen door het uitdrukkelijk regelen van licenties, het opnemen van een concurrentiebeding in arbeidsovereenkomsten (volgens gegevens uit de praktijk vormen werknemers de grootste risicogroep) en het sluiten van verzekeringsovereenkomsten.

Daarnaast kan de overheid hulp bieden door middel van wetgeving zowel op het gebied van het strafrecht als op het terrein van het privaatrecht. Bij het nemen van zulke maatregelen dient de overheid evenwel terughoudend te zijn. Wij erkennen immers de free flow of information als grondrecht.² Bescherming van gegevens vormt een uitzondering op dit grondrecht en daarvan mag daarom slechts op beperkte schaal gebruik worden gemaakt.

3 Strafrechtelijke maatregelen

In verband met het grensoverschrijdende karakter van misbruik van informatie (-systemen) heeft de Organisatie van Economische Samenwerking en Ontwikkeling in 1986 aan de lidstaten een programma aanbevolen om te komen tot nationale wettelijke regelingen. Hiertoe behoren de volgende onderwerpen:

- a het invoeren, veranderen, wissen of storen van computerdata of programma's met het oog op de illegale overdracht van geld of iets van waarde;
- b het veranderen, wissen of storen van computerdata of programma's met de opzet om een valsing te bewerkstelligen;
- c het veranderen, wissen of storen van computerdata of programma's met het oog op het storen van een computer of telecommunicatiesysteem;
- d de inbreuk op het exclusieve recht van de houder van een beschermd computerprogramma met de opzet om dat programma commercieel te exploiteren en op de markt te brengen;
- e het zich onbevoegd toegang verschaffen tot een computer of telecommunicatiesysteem of (1) door schending van veiligheidsmaatregelen of (2) met andere onfatsoenlijke intenties.

Voor wat betreft het onderwerp sub d is een wetsvoorstel aanhangig tot regeling van het auteursrecht of software³ en is een chipswet⁴ tot stand gekomen. Met betrekking tot de overige onderwerpen is een opdracht gegeven aan de Commissie Computercriminaliteit (Commissie Franken)⁵, die zich met name moest richten op een wijziging en/of aanvulling van het Strafrecht. Deze commissie heeft eind 1987 aan de minister van Justitie rapport uitgebracht met daarin een voorstel tot herziening van het Wetboek van Strafrecht en het Wetboek van Strafvordering.

Er zijn in dit rapport diverse redenen genoemd waarom het huidige Strafrecht niet meer voldoet. In de eerste plaats heeft het gebruik van andere gegevensdragers dan papier een leemte in de wet veroorzaakt ten aanzien van de valsheidsdelicten waarvoor men zich volgens de wet nog steeds van 'geschriften' zou moeten bedienen.⁶

In de tweede plaats betekent het feit, dat menselijke handelingen vaak worden vervangen door computerhandelingen dat oplichting kan plaatsvinden zonder dat *iemand* wordt bewogen tot de afgifte van enig goed. Oplichting kan alleen menselijke handelingen betreffen en geen handelingen van een machine. Daarmee is strafbaarheid van bijvoorbeeld gratis tanken door middel van manipulatie van een chipkaart via artikel 326 Wetboek van Strafrecht onmogelijk.

In de derde plaats geldt, dat economische waarden steeds meer worden belichaamd in immateriële goederen, terwijl het Wetboek van Strafrecht is gericht op de bescherming van rechten ten opzichte van stoffelijke voorwerpen. Het moge zo zijn, dat het Gerechtshof te Arnhem⁷ met een impliciete verwijzing naar het elektriciteitsarrest⁸ verduistering van gegevens met behulp van artikel 321 Wetboek van Strafrecht strafbaar heeft geacht. Deze uitspraak is evenwel hevig bekritiseerd. Het gaat ook niet aan om 'gegevens' te beschouwen als stoffelijke voorwerpen. Immers gegevens zijn te definiëren als een weergave van feiten, begrippen of instructies op een overeengekomen wijze die ze geschikt maakt voor overdracht, interpretatie of verwerking door personen of door automatische middelen. Computerprogrammatuur of software vormt in deze omschrijving een bijzondere categorie van gegevens. Thans is wel algemeen erkend, dat eigendom van

gegevens niet mogelijk is. De Hoge Raad heeft in 1921 ook uitdrukkelijk gezegd, dat gegevens als vrucht van geestelijke arbeid anders moeten worden behandeld dan stoffelijke voorwerpen die als producten van lichamelijke arbeid zijn te beschouwen. Voor dit onderscheid is het stelsel van intellectuele en industriële eigendomsrechten in het leven geroepen.

Ten slotte mogen we aannemen, dat de maximum strafmaat voor oplichting (3 jaar) en diefstal (4 jaar) niet afschrikwekkend genoeg lijkt nu het misbruik van informatietechnieken vele miljoenen guldens voordeel kan opleveren.

4 Nieuwe wettelijke bepalingen.

In navolging van de conclusies van de Commissie Franken is bij de Tweede Kamer een wetsontwerp ingediend tot wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering: de Wet Computercriminaliteit.⁹ De voorgestelde wijzigingen hebben zowel betrekking op het gebruik van de middelen van informatietechniek als op de bescherming van gegevens. Als uitgangspunt daarvoor heeft de Commissie een drietal abstracte criteria of typen van belangen geformuleerd die het rechtsgoed aanduiden dat door de wet bescherming verdient. Deze criteria zijn: beschikbaarheid, integriteit en exclusiviteit van zowel middelen (hardware) als gegevens (software).

Het eerste belang betreft de *beschikbaarheid* van de middelen van opslag, verwerking en overdracht van gegevens en de beschikbaarheid van die gegevens zelf. Vanwege het feit, dat de samenleving in grote mate afhankelijk is van deze middelen en gegevens, dient het ongestoord gebruik daarvan te worden gegarandeerd. Deze beschikbaarheid kan in gevaar worden gebracht door rampen, stroomuitval of menselijke fouten maar ook door kwaadwillig handelen, zoals sabotage, vernieling, onbruikbaar maken en wegnemen van hardware en software componenten en door de verandering en verstoring van datacommunicatie.

Voor het bereiken van juiste resultaten en het kunnen nemen van de juiste beslissingen met behulp van gegevens in geautomatiseerde systemen is het van groot belang dat die systemen op de juiste

wijze functioneren en dat bovendien de gegevens en programma's correct en volledig zijn. Hiermee hebben we het oog op de *integriteit* van systemen en de daarin vervatte gegevens.

Ten slotte noemt de commissie het belang, dat bedrijven, instellingen en personen kunnen hebben om middelen en gegevens een *exclusief* karakter toe te kennen, bijvoorbeeld omdat men niet wenst dat onbevoegden kennisnemen van als geheim of vertrouwelijk aangemerkte gegevens, of omdat men de exclusieve zeggenschap wil hebben over de wijze waarop en de personen door wie de middelen en gegevens mogen worden gebruikt.

Aan de hand van de genoemde criteria wordt voorgesteld de vernieling, beschadiging, onbruikbaarmaking dan wel het veroorzaken van storing in de werking van middelen van informatietechniek strafbaar te stellen, indien daardoor

- aan het functioneren van de openbare infrastructuur schade wordt toegebracht en/of
- een gemeen gevaar voor goederen of de levering van diensten te duchten is, en/of
- levensgevaar voor anderen te duchten is.¹⁰

Dit voorstel is bedoeld om aanslagen op de continuïteit van het functioneren van informatietechnische processen waaraan algemene belangen zijn verbonden te kunnen tegengaan. Tevens dient het om aanslagen op informatietechnische middelen welke mogelijk zeer ernstige gevolgen zullen hebben, te kunnen bestraffen. Te denken valt aan vluchtleidingscentra en kapitaalverkeer.

Daarnaast is voorgesteld om in een nieuw artikel 138a Wetboek van Strafrecht 'computervredesbreuk' strafbaar te stellen. Het betreft het zich wederrechtelijk toegang verschaffen tot geautomatiseerde gegevens verwerkende systemen. Hierbij zal alleen van strafbaarheid sprake zijn, indien bij het 'wederrechtelijk binnendringen' een beveiliging daartegen wordt doorbroken. De plaats waar de beveiliging is aangebracht is te beschouwen als de grens tussen het 'privé-terrein' en het voor een ieder toegankelijk gebied. De achtergrond van dit voorstel is gelegen in de opvatting dat strafbaarstelling wenselijk is omdat computervredesbreuk als zodanig onbehoorlijk is. Het betreft het ongenood binnendringen in het privé-domein van een ander.

Tevens speelt een rol dat met strafbaarstelling een drempel kan worden opgeworpen tegen eventuele op het binnendringen volgende schadelijke handelingen, zoals het wijzigen en wissen van gegevens en de kennisneming of het kopiëren van vertrouwelijke gegevens.

Andere voorstellen hebben direct betrekking op de bescherming van gegevens. Daarbij gaat het steeds om gegevens (waaronder ook programma's) die zijn opgeslagen, worden verwerkt of overgedragen door middel van een geautomatiseerd werk. De bepalingen betreffen het wissen, onbruikbaar of ontoegankelijk maken van gegevens, de manipulatie daarvan en het tegengaan van de verspreiding van virussen.¹¹

Met het totaal van de voorstellen is een afgerond geheel ontworpen waarmee strafbaar wordt gesteld:

- 1e dat personen zich wederrechtelijk toegang verschaffen tot beveiligde gegevens;
- 2e dat wederrechtelijk verkregen gegevens worden bekendgemaakt of uit winstbejag gebruikt, en
- 3e dat niet wederrechtelijk verkregen gegevens met een geheim karakter wederrechtelijk worden bekendgemaakt.

Bij de laatste categorie hebben we het oog op gegevens die berusten bij zogenaamde geheimhouders en bedrijfsgeheimen.

Naast de voorstellen tot wijziging van het materiële strafrecht zijn aanpassingen van de strafvordering aan de orde met betrekking tot het gebruik van een aantal dwangmiddelen.¹² Op grond van de huidige bepalingen kunnen immers alleen *voorwerpen* in beslag worden genomen, terwijl gegevens als zodanig, dat wil zeggen onafhankelijk van een gegevensdrager, niet ter beschikking van de justitie kunnen komen. Aangezien het niet steeds mogelijk is door inbeslagneming van een gegevensdrager de noodzakelijke gegevens ter beschikking te krijgen of omdat onder omstandigheden het in beslag nemen van een drager een disproportioneel middel vormt, is voorgesteld een afzonderlijke bevoegdheid te creëren tot het vergaren en opnemen van gegevens. Dit betekent, dat de mogelijkheid wordt geschapen om gegevens te selecteren en bijeen te brengen en om deze tevens vast te leggen op een drager die door de politie of justitie kan worden meegenomen.

5 Zuinig met strafrecht

Het strafrecht vormt weliswaar een noodzakelijke aanvulling op preventieve maatregelen, doch het uiteindelijk effect kan niet anders dan beperkt zijn. Dit houdt in, dat men terughoudend moet zijn bij het hanteren van het strafrecht. In de huidige voorstellen is van deze terughoudendheid op twee manieren blijk gegeven. In de eerste plaats door niet alle gedragingen strafbaar te stellen, die als onoirbaar worden aangemerkt en in de ons omringende landen soms wel strafbaar zijn of worden gesteld. In Nederland is bijvoorbeeld voorgesteld om het onbevoegd gebruik van informatietechnische middelen niet strafbaar te stellen. In de tweede plaats door sommige onoirbaar geachte handelingen slechts strafbaar te stellen wanneer aan bepaalde voorwaarden is voldaan. Zo is in het voorstel tot strafbaarstelling van computervredebreuk een belangrijke beperking aangebracht door deze alleen te richten op het inbreken in beveiligde systemen.

Met deze eis wordt aangegeven, dat de beveiligingsmaatregel een grens van het computersysteem aangeeft. Om deze grens te overschrijden is opzet van de dader nodig, zodat een 'per ongeluk' binnenkomen in een computersysteem, buiten de strafwet valt. Verder geldt, dat van binnendringen in de voorgestelde bepaling alleen sprake kan zijn indien men zich toegang verschafft tegen de onmiskenbare wil van de rechthebbende. Deze wil zou kunnen blijken uit de woorden 'verboden toegang' of iets dergelijks. In het wetsvoorstel is gesteld, dat woorden alleen (bijvoorbeeld op het beeldscherm) niet voldoende zijn, want de kennisneming daarvan valt moeilijk te bewijzen, terwijl daarmee een 'toegang per ongeluk' niet wordt voorkomen. Dit gevaar is in veel mindere mate aanwezig wanneer een hogere drempel wordt aangebracht, die bestaat uit bepaalde tegen het wederrechtelijk binnendringen gerichte beveiligingsmaatregelen. Het is als met een woonhuis: de deur moet niet alleen dicht zijn, maar ook op slot.

6 Rechtspersonenrecht

Bij de strafbaarstelling van computervredebreuk blijkt zelfwerkzaamheid van het potentiële slachtoffer een *conditio sine qua non*. Een dergelijke eis moge

nieuw zijn, maar deze sluit aan bij de gewone gang van zaken in het handelsverkeer. Immers ook bij betrekkelijk kleine vorderingen voorziet een crediteur zich van zekerheden. Daarbij rekent men niet uitsluitend op bescherming door de rechter bij het niet nakomen van een verbintenis, maar men vestigt een pand- of hypotheekrecht of vraagt bij voorbaat een garantie of borgstelling. Ten aanzien van vele door het strafrecht bestreken handelingen – vooral in de vermogenssfeer – blijft het potentiële slachtoffer evenwel passief. Hij wacht af of hem niets zal overkomen en als dat onverhoopt wel het geval is dan moet de overheidsrechter genoegdoening of compensatie geven. Nu blijkt die overheidsrechter dat werk niet meer aan te kunnen. Vooral dit verschijnsel vormt een reden om te bezien of er in het civiele recht mogelijkheden zijn om maatregelen tegen het misbruik van informatie te stimuleren. Een belangrijke aanzet om drempels op te werpen tegen nonchalance ten aanzien van de beveiliging van gegevensstromen bestaat uit het stellen van regels dienaangaande voor rechtspersonen. Een regeling in Boek 2 titel 8 BW is denkbaar. Daarbij laten zich de volgende varianten onderscheiden:

- a als onderdeel van de controle van de jaarrekening zou door de registeraccountant een oordeel moeten worden gegeven over de beveiliging van de geautomatiseerde gegevensverwerkende systemen waarvan de onderneming zich bedient;
- b een deskundige zal een oordeel moeten uitspreken met betrekking tot de betrouwbaarheid en de continuïteit van de geautomatiseerde gegevensverwerking;
- c een verklaring betreffende de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking wordt door de directie opgenomen in het jaarverslag van de onderneming, over welke verklaring de accountant zich dient uit te laten.¹³

Variant a verdient – althans voorlopig – geen aanbeveling. De accountantsverklaring bij de jaarrekening is gericht op de vraag of deze een getrouw beeld geeft van het vermogen en het resultaat van de vennootschap. Daarbij worden geautomatiseerde gegevensverwerkende systemen alleen in de controle betrokken voor zover zulks dienstig is aan

het doel van de jaarrekeningcontrole. Men zou in deze variant veel meer van de accountant gaan vragen, namelijk een oordeel over het totale stelsel van geautomatiseerde systemen in het bedrijf.

Bij variant b is gedacht aan een afzonderlijk oordeel over de mate van beveiliging van de geautomatiseerde gegevensverwerkende systemen door een specifieke deskundige. Hiervoor valt te denken aan een accountant, die is gespecialiseerd op het gebied van automatisering en controle (AC-accountant of EDP-auditor). Zolang er nog geen sprake is van reglementering van de opleiding voor deze specialisten, kan een verklaring van een AC-accountant of EDP-auditor niet het gewicht hebben, dat aan een accountantsverklaring ten aanzien van de jaarrekening toekomt. Het zal dan meer gaan om een onderhandelnde verklaring – een management letter – waarvoor evenwel het probleem geldt, dat deze niet buiten de kring van de bestuurders van de vennootschap komt.

Variant c houdt in, dat het bestuursorgaan van de rechtspersoon een verklaring moet opnemen in zijn jaarverslag over de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking. Hieruit blijkt uitdrukkelijk dat de verantwoordelijkheid voor de mate en kwaliteit van beveiliging bij de directie ligt. Deze zou in de eerste plaats, analoog aan het voorschrift in de Wet persoonsregistraties op grond waarvan bepaalde houders van persoonsregistraties verplicht zijn een reglement op te stellen, schriftelijk moeten aangeven aan welke eisen de beveiliging in het betrokken bedrijf moet voldoen. Vervolgens zou in het jaarverslag moeten worden aangegeven dat de beveiliging conform het reglement is uitgevoerd, zodat het bestuur instaat voor de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking. Tenslotte kan de accountant door deze verklaring van het bestuur te toetsen aan het reglement publiekelijk uitspreken of deze verklaring van de directie al dan niet terecht is gegeven.

Hoewel de vergadering van de Nederlandse Juristen Vereniging in 1988 zich ten aanzien van een wijziging van het rechtspersonenrecht inhoudend opstelde, heeft het NlvRA zich als een voorstander

daarvan uitgesproken. In geschrift nr. 53 'Automatisering en controle'¹⁴ wordt een uitwerking gegeven van kwaliteitsoordelen over de informatievoorziening in aansluiting op voorgenoemd voorstel in de variant b. De minister van Justitie heeft deze keuze gehonoreerd door een wijziging op artikel 393 lid 4 van Boek 2 BW voor te stellen, waarin de controlerende accountant wordt opgedragen bij zijn verslag aan de raad van commissarissen en het bestuur melding te maken van zijn bevindingen met betrekking tot de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking. Dit voorstel sluit aan bij het memorandum dat De Nederlandsche Bank¹⁵ op 20 september 1988 heeft uitgegeven waarbij zij op grond van haar toezichthoudende taak op het bankwezen de verplichting oplegt aan de externe accountant op te dragen zich periodiek een oordeel te vormen 'omtrent de betrouwbaarheid en continuïteit van voor de bedrijfsprocessen essentiële geautomatiseerde gegevensverwerking'.

Het moge zo zijn, dat hiermee een nieuwe last op het bedrijfsleven wordt gelegd, deze last is gerechtvaardigd door het grote belang, dat aandeelhouders en crediteuren hebben bij een expliciete zorg van het management voor een ongestoorde informatieverwerking in de onderneming.

7 Conclusie

De nieuwe wetsvoorstellen zijn afgestemd op de praktijk. Over de handhaafbaarheid ervan is diepgaand overleg geweest. Zij sluiten bovendien aan bij de tendens, dat ook verzekeraars steeds meer clausules in polissen opnemen, die inhouden, dat beveiligingsmaatregelen verplicht zijn. We mogen daarom stellen, dat men zich thans alleen op bescherming door anderen (verzekeraars, overheid) kan beroepen als de benadeelde-eigenaar zelf zich ook voorzichtig heeft gedragen. Voor bescherming van gegevens geldt, dat de houder daarvan moet handelen met de zorgvuldigheid, die in het maatschappelijk verkeer ten aanzien van zijn 'eigen' gegevens betaamt.

Literatuur

Commissie Computercriminaliteit (Commissie Franken). *Informatietechniek en Strafrecht*. 's-Gravenhage 1987.

- Stichting Beheer Platform Computercriminaliteit. *Computercriminaliteit in Nederland*. 's-Gravenhage 1990.
- De Nederlandsche Bank. *Memorandum omtrent de betrouwbaarheid en continuïteit van geautomatiseerde gegevensverwerking in het bankwezen*. 20-9-1988.
- Nederlands Instituut van Registeraccountants. *Automatisering en controle*. Deventer 1989.
- Organisatie voor Economische Samenwerking en Ontwikkeling. *Computer Related Crime: Analysis of Legal Policy*. Parijs 1986.
- Parker D., *Fighting Computer Crime*. New York 1983.
- Franken H. Kaspersen H. W. K., de Wildt A. H., *Recht en Computer*. Deventer 1992.
- Sieber U., *The International Handbook of Computer Crime*. New York 1986.

Noten

- 1 Gegevens ontleend aan een publikatie van CLUSIF (CLUB de la Sécurité Information Français), de Franse vereniging van organisaties met belangen in informatiebeveiliging.
- 2 Vergelijk artikel 7 Grondwet en artikel 10 Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (Verdrag van Rome 1950).
- 3 Wetsontwerp 19 921. Voor wat betreft de auteursrechtelijke regeling van computerprogrammatuur is dit ontwerp teruggenomen in afwachting van een Richtlijn van de Europese Gemeenschappen. Deze is inmiddels in een tweede versie verschenen: Commissie E.G. (90) 509 def. SYN 183. Brussel 18 oktober 1990.
- 4 Wet van 28 oktober 1987, houdende regelen inzake de bescherming van oorspronkelijke topografieën van halfgeleiderprodukten. Een voorstel tot wijziging c.q. vereenvoudiging van deze wet is thans aanhangig bij de Tweede Kamer onder nr. 21 640.
- 5 *Informatietechniek en Strafrecht*. Rapport van de Commissie Computercriminaliteit. 's-Gravenhage 1987.
- 6 Artikel 225 Wetboek van Strafrecht.
- 7 Hof Arnhem 27-10-83 NJ 1984-80.
- 8 HR 23-5-21 NJ 1921 p. 564.
- 9 Wijziging van het Wetboek van Strafrecht en van het Wetboek van Strafvordering in verband met de voortschrijdende toepassing van informatietechniek (Wet computercriminaliteit), 21551.
- 10 Vergelijk de ontwerp artikelen 161 sexies en 161 septies Wetboek van Strafrecht.
- 11 Vergelijk artikel 350a lid 2 Wetboek van Strafrecht.
- 12 Vergelijk de artikelen 125f, 125g, 125i tot en met 125n Wetboek van Strafvordering.
- 13 Vergelijk hieromtrent Informatietechniek en Strafrecht t.a.p. p. 98 e.v.
- 14 Nivra-geschrift, nummer 53. Deventer 1990. Vergelijk ook K.Y. Mollema en H. Franken: Jaarrekening en computerbeveiliging, in *De Accountant* 98e jrg. 1991 p. 177 e.v.
- 15 Memorandum omtrent de betrouwbaarheid en continuïteit van geautomatiseerde gegevensverwerking in het bankwezen.