Computercriminaliteit

M. WLADIMIROFF*

Krakers nemen kennis van vertrouwelijke gegevens van ziekenhuis, gratis telefoneren met het buitenland via het Deense telefoonnet, computercriminelen kraken bankrekening, personeelslid steelt software. De laatste jaren worden we steeds meer met dit soort berichten geconfronteerd. Computersystemen zijn te weinig beveiligd en de juridische aspecten van automatisering zijn nog onvoldoende opgelost. We kunnen constateren dat de vooruitgang van de techniek sneller is geweest dan die van de maatschappelijke inpassing daarvan.

De technische ontwikkelingen op het gebied van de informatica zijn sinds de jaren zeventig zo stormachtig snel verlopen dat de computer inmiddels een niet meer weg te denken plaats in de maatschappij heeft verworven. Automatisering is niet meer voorbehouden aan (grote) bedrijven. Door de komst van de personal computer met een hoge gebruiksvriendelijkheid en een relatief lage prijs zal binnen afzienbare tijd de homecomputer in brede lagen van de bevolking zijn intrede doen. De door velen toegejuichte komst van de informatiemaatschappij heeft echter ook zijn schaduwzijden. De geautomatiseerde opslag, verwerking en overdracht van gegevens leidt nu eenmaal ook tot misbruik.

Een aantal vormen van misbruik wordt op dit moment reeds aangepakt, zoals bijvoorbeeld inbreuken op de persoonlijke levenssfeer bij geautomatiseerde gegevensbestanden. Bij de Tweede Kamer is thans in behandeling het wetsontwerp persoonsregistraties. Daarnaast liggen er wetsontwerpen (nummers 19 919 en 19 921) gereed ter regeling van de bescherming van (besturings)programmatuur. Het wachten is thans op regelingen op strafrechtelijk gebied.

Internationale dimensie

In landen die ons voor zijn gegaan, zoals de Verenigde Staten van Amerika blijkt de strafrechtelijke wetgeving zich brokkelig ontwikkeld te hebben. Vanaf 1978 hebben ongeveer 40 Amerikaanse staten wettelijke maatregelen genomen ter bestrijding van specifiek computermisbruik. Op federaal niveau werd in 1984 de Counterfeit Access Device and Computerfraud and Abuse Act aangenomen, terwijl in 1986 een federale wet werd aangenomen waarin onder andere onbevoegde toegangsverschaffing en computersabotage strafbaar werd gesteld. De ontwikkeling in andere landen is navenant. In 1973 werd in Zweden de Data Lag aangenomen die hoofdzakelijk betrekking heeft op de bescherming van privacy en een enkele strafbaarstelling van hacken (gluren in een anders bestand) en sabotage kent. In Groot Brittannië werd in 1981 de Forgery and Counterfeiting Act aangenomen. Denemarken volgde in 1985 met de Datakriminalitet-wet en Canada in datzelfde jaar met de Criminal Law Amendment Act. In 1986 tenslotte werd in West-Duitsland het Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität aangenomen.

De in de diverse landen getroffen wettelijke maatregelen zijn niet goed met elkaar te vergelijken omdat het bereik van de strafrechtelijke bepalingen zeer verschillend is. Daarnaast zijn de oplossingen ook technisch van verschillende aard, namelijk enerzijds betreft het geheel nieuwe wetgeving en anderzijds gaat het om 'oplappen' van bestaande strafrechtelijke regels. Door het samengaan van informatica en telecommunicatie (welke combinatie ook wel wordt aangeduid als telematica) heeft de geautomatiseerde gegevensoverdracht een sterk internationaal karakter gekregen. Daarom bestaat er grote behoefte aan afstemming van strafrechtelijke bescherming van schadelijke gedragingen op internationaal niveau. De Organisatie voor Economische Samenwerking en Ontwikkeling (OESO) heeft daarom een werkgroep ingesteld, die in 1986 een rapport heeft uitgebracht onder de titel Computer-related crime: analyses of legal policy. Het rapport van de werkgroep van de OESO komt met een aantal aanbevelingen, inhoudende dat iedere lidstaat ervoor zorgdraagt dat tenminste een vijftal gedragingen strafbaar wordt gesteld. Deze gedragingen zijn enerzijds het opzettelijk inbrengen, wijzigen, wissen of uit functie plaatsen van computergegevens of computerprogramma's met het oogmerk om 1. een onrechtmatige overdracht van gelden of van een andere zaak van waarde te bewerkstelligen (oplichtingsdelicten), of 2. een en ander te vervalsen (valsheidsdelicten), of 3. de functie van een en ander te belemmeren (sabotage) en anderzijds 4. inbreuken op exclusieve rechten op programmatuur (copyrights) of 5. het onrechtmatig verschaffen van toegang tot systemen (computervredebreuk).

De ontwikkeling in Nederland is niet wezenlijk anders dan die in andere landen. In de praktijk blijken de strafrechtelijke regels onvoldoende houvast te bieden voor een adequate bestrijding van vormen van computercriminaliteit. De sedert 1984 aarzelend op gang gekomen jurisprudentie heeft nogal wat kritiek ontmoet. De vraag op welke wijze voldoende strafrechtelijke bescherming in Nederland zou kunnen worden geboden leidde in november 1985 tot de instelling

* De auteur is hoogleraar economisch strafrecht in Utrecht en advocaat in Den Haag.

Honderden Amerikaanse tieners, waaronder deze 14-, 15- en 17-jarige computerfreaks, hebben ingebroken in belangrijke computersystemen in de VS, bijvoorbeeld bij de NASA. De FBI heeft hieraan een eind gemaakt.

van de Commissie Computercriminaliteit. De discussie werd vervolgens structureel op gang gebracht door het symposium Strafrecht in de informatie-maatschappij in april 1986 aan de Vrije Universiteit te Amsterdam. Tijdens dat symposium werd duidelijk dat ook Nederland een dringende behoefte heeft aan anti-computermisbruik wetgeving. De Commissie Computercriminaliteit, onder voorzitterschap van prof. Franken heeft snel werk geleverd en reeds in dit voorjaar het rapport informatietechniek en strafrecht aan de minister van Justitie aangeboden.

Afhankelijkheid en kwetsbaarheid

In onze gecompliceerde samenleving vragen vele belangen onze aandacht. Niet alle belangen behoeven echter bescherming van het recht, of dit nu civiel-, administratief- of strafrecht is. Om welke belangen gaat het nu bij informatietechniek. In de eerste plaats kan gewezen worden op de toenemende afhankelijkheid van de samenleving van de computer. De invoering van automatiseringssystemen in bedrijven en instellingen vervangt de klassieke administratie en gegevensopslag.

De aard van de informatietechniek brengt met zich mee dat organisaties juist door deze vorm van geautomatiseerde opslag, verwerking en overdracht van gegevens extra kwetsbaar zijn. Het gaat hier dan ook om het belang van de integriteit, exclusiviteit, betrouwbaarheid en beschikbaarheid van essentiële gegevens. Dergelijke belangen spelen niet alleen in het bedrijfsleven maar ook bij de overheid (de veiligheid van de staat) of bij particulieren (bijvoorbeeld in de persoonlijke levenssfeer). De afhankelijkheid en kwetsbaarheid van informatietechniek betreft dan ook individuele en collectieve belangen.

Deze belangen kunnen weer onderscheiden worden in het belang van de beschikbaarheid van de middelen van opslag, verwerking of overdracht van gegevens en de beschikbaarheid van die gegevens zelf. Daarnaast kan het belang worden onderscheiden van de integriteit van systemen en de daarin vervatte gegevens, dat wil zeggen dat bij vernieling van de hardware of vervalsing of verandering of ontregeling van de software niet alleen nadelen ontstaan voor rechthebbenden, maar ook ongeoorloofde voordelen voor degenen die de integriteit van systemen en gegevens aantast. Tenslotte kan nog gewezen worden op het belang van de exclusiviteit, dat wil zeggen dat gegevens niet ter kennis van onbevoegden komen. Daarbij gaat het niet alleen om gegevens in de persoonlijke levenssfeer maar ook om bedrijfsgegevens welke bescherming behoeven uit oogpunt van concurrentiepositie of staatsgeheimen. Dit belang heeft een divers karakter, het kan gaan om de gegevens zelf, of om de programmatuur en soms om de besturingsprogrammatuur.

Bezien wij al deze belangen dan is duidelijk dat het hier gaat om belangen die met behulp van het recht behoren te worden beschermd. Niettemin is strafrecht niet een panacee; strafrecht is toch een ultimum remedium, een sluitstuk van de hierbedoelde bescherming. Het stellen van strafrechtelijke normen zal dan ook aansluiting moeten zoeken bij het strafrechtelijke klimaat in ons land, dat gebaseerd is op 'een strafrecht met mate'.

Bezien we deze ontwikkelingen dan kan worden vastgesteld dat een strafrechtelijke regeling van computercriminaliteit zowel nieuwe (technologische) vormen van computermisbruik zal moeten omvatten als de klassieke delicten door middel van computers. OESO spreekt van computercrimes en computer-related crimes. De commissie-Franken heeft deze strafrechtelijke implicaties van informatietechniek in zijn rapport 'vertaald' in een groot aantal (29) voorstellen tot wetswijziging. Afgezien van de technische merites van deze voorstellen verdienen ook twee andere vragen onze aandacht. Computercriminaliteit moet niet alleen bestreden worden door middel van strafrechtelijke regels, minstens even zo belangrijk is het beveiligen van computersystemen.

Beveiliging

Met de beveiliging van computersystemen is het droevig gesteld in Nederland; en niet alleen in Neder-

land, ook in andere landen blijkt uit onderzoek dat het ontbreken van een deugdelijke beveiliging strafbare gedragingen faciliteert. De commissie-Franken heeft ook laten onderzoeken hoe het in Nederland met de beveiliging van computers is gesteld. Uit een op verzoek van de commissie door Kleynveld, Kraayenhof en co. uitgebracht rapport blijkt dat van de onderzochte bedrijven slechts 35% over voldoende beveiligde systemen beschikten, 47% onvoldoende beveiligd was en dat ten aanzien van 18% geen oordeel kon worden gegeven. Het predikaat 'goed' kon aan geen der onderzochte bedrijven worden toegekend. Kortom er blijkt sprake te zijn van een ongelooflijke nonchalance bij het bedrijfsleven, wellicht omdat men de kwetsbaarheid en de risico's van informatietechniek onvoldoende beseft.

Dit leidt tot de vraag of het algemeen belang niet met zich meebrengt dat er van de zijde van de overheid regels moeten worden gesteld welke verplichtingen tot beveiliging met zich meebrengen. Te denken valt aan wettelijke maatregelen waarin niet alleen beveiligingseisen worden gesteld maar ook nadere eisen worden geformuleerd waaraan een beveiliging zou moeten voldoen, wil er sprake zijn van een aanvaardbaar beveiligingsniveau. Omdat geautomatiseerde gegevensbestanden onderdeel uitmaken van administraties liggen er ook aanknopingspunten voor controle van het beveiligingsniveau voor accountants. In de accountantswereld is thans een ontwikkeling gaande waarbij zich een nieuwe deskundige aandient, de AC-accountant of EDP-auditor. Deze deskundige kan een oordeel uitspreken over de beveiliging, de betrouwbaarheid en de continuïteit van de geautomatiseerde gegevensverwerking. Een apart probleem is de vraag wie als AC-accountant kan worden aangemerkt, kortom welke eisen aan dergelijke deskundigheid moet worden gesteld wil men bevoegd hiervoor bedoelde verklaring kunnen afgeven.

Een bijzonder probleem bij de bestrijding van computercriminaliteit is de geringe bereidheid van slachtoffers om aangifte te doen. Uit onderzoek, met name in de Verenigde Staten blijkt dat de bereidheid om aangifte van computercriminaliteit te doen minstens de helft is van de aangifte-bereidheid bij gewone criminaliteit. Sommige onderzoeken, zoals onlangs in Nederland (VIFKA) tonen aan dat ruim 80% van de ondervraagden verklaarde geen aangifte te zullen doen in geval van diefstal van programmatuur. Bij een dergelijke stand van zaken heeft het stellen van strafrechtelijke regels alleen weinig zin. Opsporing en vervolging van computercriminaliteit hangt toch af van het ter kennis van politie en justitie brengen van dergelijke misdrijven. Aldus dreigt er een neergaande spiraal te ontstaan: bij weinig vervolging gaat er ook weinig generale preventie uit van het stellen van strafrechtelijke normen. Immers als de pakkans gering is, is de normerende werking van strafbepalingen ook gering. Bovendien brengt een lage aangiftebereidheid met zich mee dat de toch al geringe deskundigheid bij politie en justitie op een laag niveau zal blijven. De eventuele wettelijke verplichting tot aangifte lost niets op; het zal een voos voorschrift blijven. Een oplossing dient eerder gezocht te worden in een mentaliteitsverandering bij gebruikers van informatietechniek. De overheid zal daartoe naast het treffen van wettelijke maatregelen ook een informatiecampagne moeten voeren om een dergelijke mentaliteitsombuiging te bewerkstelligen.

Conclusie

De snelle ontwikkeling van de techniek noopt tot een dienovereenkomstige ontwikkeling van het computerrecht. De strafrechtelijke implicaties van automatisering zullen ook in Nederland geregeld moeten worden. Toch moet computercriminaliteit niet alleen met strafrecht bestreden worden. Een hogere graad van beveiliging van geautomatiseerde systemen dient gemeengoed te worden. De overheid kan daarbij door middel van regelgeving en treffen van andere maatregelen de aanzet geven. Bestrijding van computercriminaliteit kan niet alleen van de zijde van de overheid komen, ook het bedrijfsleven en gebruikers van informatiesystemen zelf zullen het nodige moeten doen, daarbij hoort ook een grote bereidheid om aangifte te doen. Het woord is thans aan de overheid om de nodige wetgeving te realiseren en aan het bedrijfsleven om de nodige maatregelen te treffen.