Beteugeling van computercriminaliteit

Een terreinverkenning

C. Erkelens*

I. Definiëring en afbakening

Met het toenemend gebruik van de computer gaan ook grote computerisatieproblemen gepaard; de bescherming van de software is momenteel één van de grootste problemen op dit gebied.

Hoewel computercriminaliteit toeneemt, worden nog maar heel weinig gevallen aangegeven. Men moet rekening houden met een groot dark number (80 %).[1]

Bij deze soort criminaliteit heeft men te maken met een specifiek soort dader. Ook het misdrijf zelf is specifiek. Bepaalde aspecten van de computercriminaliteit doen een eventuele toepassing van de bestaande wetgeving erop in vraag stellen:
De wijze waarop het misdrijf gepleegd wordt maakt soms een probleem uit alsook het feit dat de machine in bepaalde gevallen optreedt in plaats van de mens. De specificiteit en de verschillende vormen van de computergegevens maken evenzeer een probleem uit bij de toepassing van de wetgeving op computercriminaliteit, omdat de gegevens niet beantwoorden aan het begrip 'zaak' zoals het door de wetgever bedoeld is.

Een bestudering van de wetgeving, rekening houdend met de verschillende aspecten van computercriminaliteit, is dus zeker nodig.

Hiervoor is eerst en vooral een degelijke en nauwkeurige definitie van het begrip 'computercriminaliteit' vereist.

Verscheidene auteurs hebben gepoogd een zo volledig mogelijke omschrijving te geven. Heel algemeen wordt gesteld dat computermisdrijven alle misdrijven zijn 'waarbij de computer werktuig (middel) of doel van de daad is'.[2] Onder deze brede definitie vallen echter zowel de aanslagen op de software als deze op de hardware, alsook de gevallen van schending van de privacy langs de computer om.

De bescherming van de privacy maakt reeds het voorwerp uit van een aantal studies en zal dan ook hier niet besproken worden.[3]

Voor de bescherming van hardware kan probleemloos de bestaande wetgeving worden toegepast; dit aspect zal hier dan ook terzijde gelaten worden.

---

* Licentiaat in de Rechten en in de Criminologische Wetenschappen, wetenschappelijk medewerkster, Centrum voor Internationaal Strafrecht, V.U.B.

1. U.S. Department of Justice, 'Computer Crime', *Criminal Justice resource manual,* 1979, 381 p.
2. Definitie van VON ZUR MUHLEN, R.A.H., 'Computer-Kriminalität, Gefahren und Abwehrmassnahmen', *Wirtschaftsführung,* nr. 15.
3. Zie daarvoor DE HOUWER, J., 'Privacy and transborder data flows', V.U.B., Centrum voor Internationaal Strafrecht, 1984, 73 p.

Wat hier behandeld wordt is de computerfraude of 'tout acte ou ommission qui nécessite l'utilisation de la technologie informatique dans sa réalisation et porte ou peut porter atteinte à des biens corporels ou incorporels'.[4] Dit is de definitie die we aannemen bij het bestuderen van de toepasselijkheid van onze strafwet op het fenomeen computerfraude.

Toch dient nog opgemerkt te worden dat uiteenlopende definities bestaan. Deze definities vertrekken meestal van een criminologisch concept omdat een alomvattende definitie vanuit juridisch standpunt, volgens sommige auteurs, moeilijk te geven is, aangezien de wetgevers de technologische evolutie achterna hinken.

Herbert Edelherz[5] b.v. gebruikt de term 'computer white collar crime'. Voor hem is er slechts sprake van 'manual routines who have been replaced by E.D.P.' (Electronic Data Processing).

August Bequai[6] stelt dat computercriminaliteit een categorie, een deel is van een ruimere vorm van criminaliteit, de white collar crime. Rainer A.H. von zur Mühlen[7] levert kritiek op de Duitse term 'Computerkriminalität' omdat een computer zelf niet crimineel kan zijn. Daar deze benaming echter algemeen aanvaard wordt, gebruikt hij ze ook en definieert deze 'Computerkriminalität' dan als 'elke criminele daad gericht tegen computers of gepleegd door middel van computers'.

Ulrich Sieber[8] geeft kritiek op de definitie van zijn landgenoot: hij ziet niet in waarom b.v. diefstal van een lege magneetband ook onder deze definitie zou moeten vallen: dit is een gewone diefstal, geen aantasting van software.

Donn B. Parker[9] baseert zich op de fenomenologische factoren van computercriminaliteit waarbij hij een verschil met white collar crime opmerkt: 'Computer abuse is any intentional act involving a computer where one or more perpetrators made or could have made gain and one or more victims suffered or could have suffered a loss. Computer crime is a common term used to identify illegal computer abuse; however it implies direct involvment of computers in committing a crime. Computer-related crime conveys the broader meaning of any illegal act for which knowledge of computer technology is essential for succesful prosecution'.

Hier worden alleen de gevallen van *aantasting van software* besproken. Volgens de type-voorstellen van de W.I.P.O. (World Intellectual Property Organization)[10] is 'software' te definiëren als behorende tot één van de volgende drie categorieën:

a. een computerprogramma, wat betekent een geheel van instructies dat, eenmaal omgezet op een machinaal leesbare drager, een functie, een taak of een be-

---

4. Definitie voorgesteld door de V.U.B. in het antwoord op de O.E.S.O.-vragenlijst van oktober 1982.
5. Deze definitie van H. Edelherz komt uit: SIEBER, U., *Computerkriminalität und Strafrecht,* München, Heymans, 1980, 364 p.
6. BEQUAI, A., *Computer crime,* U.S.A., Lexington Books, 1978, 207.
7. VON ZUR MUHLEN, R.A.H., 'Computer-Kriminalität, Gefahren und Abwehrmassnahmen', *Wirtschaftsführung,* nr. 15.
8. SIEBER, U., *Computerkriminalität und Strafrecht,* München, Heymans, 1980, 364 p.
9. PARKER, Donn B., *Crime by computer,* New York, Scribner, 1976.
10. *La propriété industrielle,* W.I.P.O., 1977, 277.

paald resultaat kan doen aanduiden, uitvoeren of bekomen, bij middel van een toestel geschikt voor informatieverwerking;
b. een beschrijving van een programma, hetzij een volledige voorstelling van werkzaamheden, onder de vorm van woorden, schema of anders, voldoende gedetailleerd om een geheel van instructies vast te stellen die leiden tot een overeenstemmend computerprogramma;
c. hulpdocumentatie, zijnde iedere documentatie andere dan een programma of een beschrijving van een programma, gemaakt om de begrijpelijkheid of de toepassing van een computerprogramma te vergemakkelijken, b.v. probleembeschrijvingen en gebruiksaanwijzingen.

De hier behandelde computermisdrijven zijn dus: de vormen van vermogensdelicten waarbij computergegevens onrechtmatig *veranderd* worden (computermanipulatie), onrechtmatig *verkregen* en/of *gebruikt* worden (computerspionage), *vernietigd* worden (computersabotage), of waarbij *computertijd* onrechtmatig gebruikt wordt (tijddiefstal).[11]

II. Fenomenologische factoren

Om de specificiteit van computercriminaliteit te kennen en om de graad van aangepastheid van de wetgeving daaraan te bepalen, is een onderzoek van de fenomenologische factoren onmisbaar. De wetgeving moet namelijk niet alleen aangepast zijn aan het beeld van de misdrijven, maar ook aan het beeld van de misdadiger.

De computerproblematiek heeft een 'onzichtbaar' karakter. Het is tevens een vorm van 'white collar crime', wat men als één van de voornaamste kenmerken van de computercriminaliteit kan beschouwen.

De computerfraude wordt meestal *toevallig* ontdekt.[12] Het is steeds ten gevolge van één of ander incident dat een onderzoek leidt tot de ontdekking van het feit. De fraude kan slechts ontdekt worden door deskundigen. Een ander probleem is het relatief ongeorganiseerd publiek ressentiment: de 'intelligente' computercriminaliteit wordt niet echt als 'misdadigheid' ervaren, de daders worden niet als echte criminelen beschouwd door het publiek.

Verder zijn de slachtoffers zelden in staat zich te verweren, dikwijls wensen ze zelf de fraude geheim te houden omwille van hun eigen reputatie. Een sensibilisering op dit vlak is nodig.

Men heeft ook te maken met het Robin Hood-syndroom. In hun rationalisatieproces stellen de daders het zelf voor alsof ze enkel schade berokkenen aan de machine en niet aan mensen. De anonimiteit speelt hierbij een grote rol: er is geen fysisch contact met het slachtoffer. De daders ervaren hun gedrag wel als deviant maar niet als delinquent.

---

11. Deze vierdelige indeling komt uit de Duitse rechtsleer. Ze wordt gebruikt door: LENCKNER, Th., *Computerkriminalität und Vermogensdelikte,* Heidelberg, Karlsruhe, C.F. MULLER, 1981, 51 p.; SIEBER, U., *o.c.* Daarnaast is er de Amerikaanse indeling: direct financial fraud and theft, unauthorised use or sale of services, vandalism, information or property theft: uit: PARKER, Donn B., *o.c.*
12. Zie: DAUDIER DE CASSINI, P., 'L'effet Serendip et la fraude informatique', *Banque,* 1982, 192.

Aan de basis van de computercriminaliteit liggen zes fenomenologische factoren:

1. De omgeving waarin het misdrijf tot stand komt

In één databank worden een enorme hoeveelheid gegevens opgeslagen, waarbij het gevaar voor fraude en dus ook de 'opbrengst' van de misdrijven enorm groot is. Eén enkele chip bevat een zeer groot aantal gegevens. Door de technologische evolutie stijgt die hoge waarde van de chip nog steeds. In Duitsland spreekt men van de sterke 'Komprimierung' van de gegevens.[13] Men is reeds in staat een heel klein computertje aan te brengen op een chip van hooguit een halve vierkante centimeter: de zogenaamde microprocessorchip. Een normaal moduul van vier geheugenchips bevat in totaal ruim 32.000 tekens. Geheugenchips zijn daarbij ook zeer snel toegankelijk. In enkele miljoensten van een seconde haalt de centrale verwerkingseenheid er programma-instructies en andere gegevens uit te voorschijn. De snelheid van moderne verwerkings- en geheugenchips brengt mee dat de verwerkingssnelheden van grote moderne computers al worden uitgedrukt in de eenheid MIPS (Miljoenen Instructies Per Seconde).[14]

Vraag is of men met deze uitermate hoge waarde rekening kan houden bij een eventuele toepassing van traditionele wetsbepalingen.

Ook grijpen er datatransfers plaats tussen geografisch van elkaar verwijderde gebruikers. De misdrijven richten zich op computercentra, terminals, telefoon en telex, gegevensdragers zoals ponskaarten, magneetbanden, geheugenschijven ...

Het grootste aantal misdrijven wordt gepleegd door mensen die rechtstreeks contact hebben met de computer.[15]

2. De modi operandi

Deze zijn specifiek. Ze zijn te verklaren door de automatische routines in de computersystemen.

Men heeft een apart jargon om de verschillende technieken aan te duiden: data diddling, trojan horse, salami technique, superzapping, trap doors, logic bombs, asynchronous attacks, scavenging, data leakage, piggy backing, impersonation wire tapping, simulation ....[16]

3. Het nagestreefde voordeel

In essentie komt dit overeen met dat van de klassieke vermogensdelicten. Toch worden de electronische pulsen en gegevens in andere vorm, die het voorwerp uitmaken van computermisdrijven, minder beveiligd dan het geld en de goederen die voorwerp zijn van de klassieke vermogensdelicten.

---

13. SIEBER, U., *o.c.*, LENCKNER, Th., *o.c.*
14. Zie: I.B.M., *Computers, gereedschap van deze tijd,* Nederland N.V., 1980, 46 e.v.
15. Zie b.v. WHITESIDE, T., *Computercapers,* U.S.A., New American Library, 1979, 165.
16. Voor de uitleg hiervan zie: U.S. Department of Justice, 'Computer Crime', *Criminal justice resource manual,* 1979, 55.

4. De tijdsfactor

De tijd nodig om een computermisdrijf te plegen, verschilt van diegene die nodig is bij klassieke misdrijven. Voor sommige informaticamisdrijven volstaan reeds drie milliseconden. Hierdoor is de kans om ontdekt te worden ook kleiner.[17]

5. De ruimtefactor

Door de telecommunicatie en de groei van de netwerken bestaat er geen 'afstand' meer tussen de computer en zijn gebruikers. Een misdrijf kan vanop duizend kms. gepleegd worden.[18]

6. De dader zelf

De daders beantwoorden niet aan het traditionele beeld van een misdadiger. Ze zijn tussen de 18 en 46 jaar oud, met een gemiddelde leeftijd van 25 jaar. De jongsten zijn bijna allen universitair geschoolden. Vaak zijn ze nog niet lang werkzaam bij het bedrijf of de instelling dat hun slachtoffer wordt, ze voelen zich niet meer met hun werk verbonden en er is nog geen positieve identificatie met het bedrijf. De studies die ze volgden maken dat ze dikwijls overgekwalificeerd zijn voor het werk dat ze moeten verrichten: hun creatieve energie gebruiken ze dan voor criminele doeleinden. De meeste misdrijven worden gepleegd in de eigen werksfeer.

Vaak zijn er ook medeplichtigen of mededaders. Dikwijls gaat het om de computerspecialist die het technische aspect voor zijn rekening neemt en een tweede persoon die niets met de computer te maken heeft, maar de technische ingreep omzet in werkelijk gewin.

De erg competitief ingestelde computertechnici zijn er ook op uit om hun superioriteit te bewijzen. De uitdagingen binnen de eigen firma of tussen concurrerende bedrijven kunnen leiden tot crimineel gedrag, b.v. binnendringen in systemen van de concurrentie om boekhoudkundige gegevens te bemachtigen, aftappen van lijnen, binnendringen bij de concurrentie om hun programma's te vernietigen ...

Naast het Robin Hood-syndroom is er ook een elitair syndroom: de daders vinden dat ze het recht hebben om de computer te gebruiken voor persoonlijke doeleinden omdat zij het privilege hebben van ermee te werken.

De daders zijn meestal mensen met een blanco-strafregister en met hoge inkomens.[19]

Bij de analyse van de verschillende computermisdrijven moet men bovendien nog het onderscheid maken tussen de misdrijven gepleegd door gespecialiseerd personeel en de misdrijven gepleegd door buitenstaanders. Zo ook kunnen de misdrijven gepleegd worden binnen het systeem en de instelling, maar ze kunnen ook gepleegd worden van buitenuit.

---

17. Zie: I.B.M., *o.c.*, 143.
18. Ibid., 99 e.v.
19. U.S. Department of Justice, *l.c.*, 53-55.

Met al deze factoren dient rekening gehouden te worden bij de behandeling van computercriminaliteit.

Daarnaast dient dan onderzocht te worden in hoeverre onze wetgeving erop van toepassing is.

III. Wetgeving

We kennen geen wetten, wetsontwerpen of wetsvoorstellen die uitsluitend de informaticacriminaliteit betreffen en deze materie globaal pogen te regelen.

De rechtbanken proberen in de mate van het mogelijke de bestaande strafwetgeving toe te passen, maar zien zich in een aantal gevallen genoodzaakt tot vrijspraak wegens de onaangepastheid van de wetgeving.[20] Het legaliteitsbeginsel mag namelijk niet uit het oog verloren worden, analogie moet vermeden worden. Feiten die niet voorzien zijn door de wet mogen niet bestraft worden, zelfs indien ze moreel of sociaal af te keuren zijn. Men ondervindt wel dat het legaliteitsbeginsel meer en meer wordt aangetast en meer in het bijzonder in het domein van de vermogensdelicten.[21] Vooral op dit vlak heeft men te maken met de snel evoluerende technologie. Men ziet dat het toepassingsveld van de vermogensdelicten zich uitbreidt. Dit betekent echter niet dat het legaliteitsbeginsel verdwijnt. Het betekent alleen dat de interpretatiebevoegdheid van de rechters vergroot, maar deze bevoegdheid is zeker niet onbeperkt.

Niet alleen het soort misdadiger is specifiek, maar ook de aard van het gepleegde feit. Dit leidt tot een aantal moeilijkheden bij een eventuele bestraffing ervan.

In een computersysteem onderscheidt men namelijk verschillende *'etappes'* in de verwerking van de data, en elke etappe is vatbaar voor een specifieke criminele manipulatie[22]:

- Men heeft als eerste stadium de *gegevensinvoer (input)* en het *vertalen van gegevens in computertaal (compiling).*

Hier kan een persoon valse gegevens inbrengen, met alle gevolgen vandien. De data kunnen ook vernietigd worden.

- De computer antwoordt op de manier die door het *programma* gedicteerd wordt. Het programma kan wederrechtelijk gebruikt worden ten gevolge van diefstal, indiscretie, ongeluk of verlies. Het personeel kan programma's doorspelen aan de concurrentie.
- De *central processing unit (C.P.U.) of centrale verwerkingseenheid (C.V.E.)* die de computer richt en leidt om de nodige functies te vervullen volgens de richtlijnen van het programma, is ook vatbaar voor verschillende vormen van manipulatie.

---

20. Welke gevallen dit zijn, vindt men verder in het artikel. Er zijn voorbeelden van vrijspraak inzake misbruik van elektronisch geldverkeer, hoewel de strafwet hierop wel kan toegepast worden: Corr. Namen, 26 mei 1982, niet uitgegeven; Corr. Namen, 26 september 1982, niet uitgegeven.
21. Zie: COUSIN-HOUPPE, M.S., 'Vers une continuité de la loi pénale dans le domaine des principales infractions portant atteinte juridique aux biens (vol, abus de confiance, escroquerie)', *Rev. sc. crim.*, 1977, 780-781.
22. Zie: *Inleiding tot de informatica,* V.U.B., 1980, 127.

- De *gegevensuitvoer (output)* kan gestolen worden en eventueel aanleiding geven tot chantage. De uitvoergegevens kunnen eveneens veranderd of vernietigd worden.
- Tenslotte is de *overdracht van gegevens* naar andere gebruikers of computers *(netwerken)* kwetsbaar, men denke maar aan het aftappen van telefoonlijnen.

Men kan de computermisdrijven indelen in vier grote groepen[23]: *computermanipulatie, computerspionage, computersabotage, tijddiefstal.*

De toepassing van de strafwet hierop, brengt een aantal kwalificatieproblemen met zich mee.

1. Computermanipulatie

De computermanipulatie bestaat uit misdrijven, waarbij de dader gedeeltelijk gegevensveranderingen in de computer aanbrengt met het doel de verwerking en de output van de gegevens te veranderen, en hierdoor (meestal) een persoonlijk vermogensvoordeel te bekomen.[24] Er zijn verschillende manipulatievormen, telkens te situeren in één van de verschillende etappes van dataverwerking. Men spreekt over inputmanipulaties, manipulaties in het stadium van de eigenlijke gegevensverwerking (programma manipulaties en klaviermanipulaties), outputmanipulaties.

De input en output kunnen door derde personen beïnvloed worden, de manipulaties in het stadium van eigenlijke gegevensverwerking maken echter werkelijk 'intelligente' misdadigheid uit. De dader kan b.v. het verloop van een programma veranderen, maar daarvoor kan het nodig zijn een volledig deel van het programma te herschrijven. Dergelijke manipulaties zijn moeilijk uit te voeren, maar daardoor ook moeilijk te ontdekken.

Er zijn geen voorbeelden van computermanipulatie terug te vinden in de Belgische rechtspraak.

Trouwens, wanneer men de strafwet analyseert, komt men tot de vaststelling dat ze slechts zeer uitzonderlijk op deze feiten kan toegepast worden. De rechter zou dus in een aantal gevallen van computermanipulatie moeten vrijspreken.

Er is namelijk slechts sprake van *oplichting* (artikel 496 Sw.) in enkele zeer uitzonderlijke gevallen: wanneer iemand zich wederrechtelijk *een bepaald goed,* een som geld, laat *overmaken* via een computermanipulatie, indien men de manipulatie als *'bedrieglijk middel'* kan beschouwen waardoor men doet geloven aan een denkbeeldig krediet of indien men een vermeend vertrouwen daardoor schept waarvan de dader misbruik zal maken om het goed te bekomen. B.v. de persoon die door toevoeging van fictieve namen aan een lijst onrechtmatig geld verkrijgt (hij verkrijgt dus door de computermanipulatie *afgifte* van de som, constitutief bestanddeel van het misdrijf 'oplichting'), kan veroordeeld worden wegens oplichting: hij maakt gebruik van een valse naam, één van de mogelijke bedrieglijke middelen.[25]

---

23. Dit is de indeling uit de Duitse rechtsleer.
24. Definitie van: SIEBER, U., *o.c.,* 42 e.v.
25. B.v. in Duitsland: Kindergeldzaak: beschreven door SIEBER, U., *o.c.,* 42 e.v.

- De input- en outputmanipulatie *zelf* kunnen als listige kunstgreep, als bedrieglijk middel beschouwd worden: de manipulatie zelf is het uitwendig element dat een leugenachtige bewering (vervat in de gegevens) een bepaald krediet toekent.[26]

Dit is echter niet zo voor programmamanipulaties: de instructies van het programma kunnen geen (leugenachtige) bewering bevatten.

- Tevens is voor de toepassing van artikel 496 Sw. vereist dat op de manipulatie ook daadwerkelijk een afgifte of een levering volgt: poging tot oplichting is in ons land niet strafbaar. Misschien zou het wel nuttig zijn om de poging tot oplichting te beteugelen zoals men dat in Frankrijk heeft gedaan; daar worden dan ook zekere computermanipulaties aan de hand van deze bepaling bestraft.[27]

Maar in elk geval zou dergelijke aanpassing van de wetgeving niet volstaan, aangezien het doel van een computermanipulatie *niet noodzakelijk* een afgifte van een goed, een vermogensvermeerdering is. Zo kunnen b.v. gegevens omtrent de solvabiliteit van personen gewijzigd worden om andere redenen, kan de samenstelling van een produkt gewijzigd worden zodat fouten ontstaan in de fabrikatie, kunnen gegevens uit medische dossiers gewijzigd worden en verkeerde behandelingen toegepast worden.

- Het is nodig dat er *een bepaald slachtoffer* is van de oplichting, iemand die misleid wordt en die daardoor tot de afgifte of levering gedreven wordt. Slachtoffer van de computermanipulatie is in geval van oplichting de instelling, het bedrijf of de bank die de computer gebruikt. Het is deze instelling die misleid wordt door de manipulatie van de computer die dan als passief instrument voor de oplichting dient. Het gaat hier dus niet om een 'te slim af zijn' van de computer zelf.[28]

Geen andere bepalingen uit onze strafwet komen in aanmerking voor de beteugeling van computermanipulatie, tenzij *'valsheid in geschriften'*, wanneer men de gegevens als 'geschrift' kan beschouwen. Men maakt namelijk een onderscheid tussen 'source code' en 'object code'.[29] 'Source code' is geschreven in een hogere programmeertaal en zou als geschrift aan te merken zijn; 'object code' of machinetaal is de voor de mens niet verstaanbare en alleen door de machine leesbare vorm waarin een computerprogramma zich bevindt op het ogenblik waarop het gebruikt wordt, en zou geen geschrift uitmaken.

---

26. Het gebruik van documenten die een leugenachtige bewering bevatten, werd reeds vroeger beschouwd als uitwendig element dat volstaat om onder artikel 496 Sw. te vallen, zelfs indien dit niet gepaard ging met verbale leugens: Cass., 26 september 1955, *Pas.*, 1956, I, 49. Wanneer men de lijn doortrekt, kan men dus stellen dat het gebruik van gegevensdragers die 'een leugenachtige bewering' bevatten evenzeer dat uitwendig element uitmaakt.
27. Trib. Gr. Inst., Paris, 9 februari 1982, *Expertises,* 1982, nr. 38.
28. Dit probleem wordt namelijk gesteld in de Duitse rechtsleer: zij achten dan ook de oplichting in deze gevallen niet mogelijk – LENCKNER, Th., *o.c.* – of slechts mogelijk t.o.v. het personeel dat de gemanipuleerde gegevens in handen krijgt en op deze wijze misleid wordt: SIEBER, U., *o.c.*
29. Zie: VAN HOECKE, K., 'Software piraten', rede uitgesproken op de plechtige openingsvergadering van de Vlaamse Conferentie bij de balie te Gent op 22 oktober 1983, *R.W.*, 1983-84, 1649.

Aldus blijven de manipulaties van data die niet als geschrift kunnen beschouwd worden, waarbij geen vermogensvoordeel wordt bekomen en/of waarbij geen gebruik gemaakt wordt van bedrieglijke middelen in de zin van artikel 496 Sw., onbeteugeld.

Men zou de ongeoorloofde verandering van de gegevens op zichzelf als een misdrijf moeten beschouwen indien men wil vermijden dat de daders vrijuit gaan.

Een aangepaste bepaling is op dit vlak derhalve welkom.

2. Computerspionage

Dit is de onrechtmatige verkrijging en/of het onrechtmatig gebruik van data. Het gaat om speciale vormen van bedrijfsspionage.[30] Tot nu toe is hiervan slechts één voorbeeld terug te vinden in onze rechtspraak.[31]

Voorwerp voor het misdrijf zijn enerzijds de input- en outputgegevens, anderzijds de programma's. Ook moet het onderscheid gemaakt worden tussen de onrechtmatige verkrijging van data en het onrechtmatig gebruik ervan.

De *onrechtmatige verkrijging* kan op verschillende manieren plaatsvinden: men kan de gegevensdragers ontvreemden, men kan de gegevensdragers copiëren, men kan de spionage plegen door enkel onrechtmatige toegang tot de gegevens: door lezing ervan of onrechtmatige verkrijging van op afstand.

Elke vorm leidt tot eigen moeilijkheden voor de toepassing van onze strafwet erop.

Eerst en vooral dient de vraag gesteld te worden of de gegevens als een 'zaak' in de zin van artikel 461 Sw., *diefstal,* kunnen beschouwd worden. Diefstal kan namelijk *niet* slaan op abstracte informatie. De materiële gegevensdrager kan wél gestolen worden, maar bij de toepassing van artikel 461 Sw. dient principieel abstractie gemaakt te worden van de inhoud ervan, ongeacht de bedoeling van de dader.[32]

Onze strafwet kan zonder probleem toegepast worden op de aantastingen van de hardware. Het zijn de eigenlijke computermisdrijven, de aantastingen van de software, die grotendeels onbeteugeld blijven.

Men kan ook spreken over *diefstal van elektriciteit*[33] aangezien de gegevens door de input worden omgezet in elektronische pulsen die dan verder door de computer verwerkt worden. Strikt genomen slaat de bepaling echter ook weer niet op de abstracte gegevens, slechts op de elektriciteit waarin de gegevens vervat zijn.[34]

Ook is er bij de onrechtmatige verkrijging van computergegevens niet altijd sprake van een materiële wegneming, constitutief bestanddeel van artikel 461

---

30. Definitie van SIEBER, U., *o.c.*
31. De zaak werd echter niet strafrechtelijk behandeld: Kh. Brussel, 14 september 1982, *T.B.H.,* 1983, 641, noot VANDENBERGHE, G.
32. *R.P.D.B.,* v° Vol, nr. 148; CHARLES, R., *Introduction à l'étude du vol,* Brussel, Bruylant, 1961, 43.
33. Zie: BRAHY, A., 'Les vols d'eau et d'énergie. Le vol d'usage', *J.T.,* 1975, 597-602.
34. De gegevens worden namelijk *onrechtstreeks* overgedragen, via de elektriciteit. Ze zitten vervat in de elektriciteit zoals ze in een materiële gegevensdrager kunnen vervat worden.

Sw. Een gegevens*drager* kan materieel weggenomen worden, maar zoals gezegd slaat de diefstal slechts op die gegevensdrager zelf. Het copiëren van gegevens kan niet als materiële wegneming beschouwd worden, tenzij een gegevensdrager eerst weggenomen wordt en daarna pas terugbezorgd.[35] Op onrechtmatige toeëigening van data door loutere lezing ervan, kan de strafwet niet worden toegepast.

In enkele uitzonderlijke gevallen van computerspionage kan van *oplichting* gesproken worden: wanneer iemand door gebruik van bedrieglijke middelen (b.v. een valse naam) zich onrechtmatig een gegevensdrager laat overhandigen. De gegevens kunnen het voorwerp uitmaken van artikel 496 Sw., maar er is afgifte of levering vereist.

In bepaalde gevallen kan artikel 491 Sw., *misbruik van vertrouwen,* worden toegepast op de gegevensdragers of op de elektrische stroom, wanneer er afgifte is met precair karakter.[36] Onlichamelijke goederen maken echter ook niet het voorwerp uit van artikel 491 Sw.: strikt genomen slaat het artikel dus niet op eigenlijke computerspionage.

Een aanpassing van de wetgeving is dus zeker nodig: wanneer men daarbij de onrechtmatige verkrijging van data beschouwt als een vermogensdelict, als een onrechtmatig verwerven van eigendom, dient zowel rekening gehouden te worden met de aard van het ontvreemde als met de waarde, de sterke 'Komprimierung' van de gegevens.

Voor het *onrechtmatig gebruik* van data gaat men eerder zijn toevlucht zoeken in specifieke bepalingen.

Zo kan artikel 309 Sw., bedrieglijk meedelen van fabrieksgeheimen, worden toegepast zo de dader (gewezen) werknemer is van de betrokken onderneming en het meegedeelde gegeven een geheim procédé bevat dat industrieel, origineel en eigen aan de onderneming is, en indien het niet het voorwerp is geweest van een octrooi dat in het openbaar domein is gevallen.[37]

Tevens kan men hier spreken over daden strijdig met de eerlijke handelspraktijken.

In plaats van tot strafrechtelijke bepalingen gaat men zich voor het onrechtmatig gebruik van computerprogramma's eerder wenden tot de bescherming geboden door het auteursrecht en het octrooirecht.[38]

Ook wat onrechtmatig gebruik van data betreft, is de wettelijke bescherming ontoereikend.

---

35. Dit is de stelling aangenomen door de Franse rechtsleer: zie: VOLLIN, R., 'Le recel et la détention de la chose', *D. Sirey,* 1972, Chron., 281-284. Zie ook: CORLAY, P., 'Réflexions sur les récentes controverses relatives au domaine et à la définition du vol', *S.J.,* 1984, 3160.
36. Bepaalde contracten lenen zich tot verduistering in de zin van artikel 491 Sw., andere niet. Zie: LINANT DE BELLEFONDS, X., *L'informatique et le droit,* Que sais-je?, P.U.F., 1981, 127.
37. Zie: CORBET, J., *Intellectuele rechten,* V.U.B., 1983-84, 107.
38. Octrooirecht zou van toepassing zijn als voldaan wordt aan de vereisten van nieuwheid en industrieel karakter. Auteursrecht zou slechts op 'source code' van toepassing zijn: zie: VAN HOECKE, K., *l.c.*

3. Computersabotage

Dit is de vernietiging van computergegevens, van software. Hiervan kent men nog geen voorbeelden in de Belgische rechtspraak. Deze vormen van sabotage kunnen *niet* gerangschikt worden onder de gewone sabotagemisdrijven.

De artikelen uit het strafwetboek kunnen slechts betrekking hebben op vernieling van hardware, niet op eigenlijke computersabotage (behalve valsheid in geschriften wanneer men opzettelijk gegevens uitwist die men als geschrift kan beschouwen, met het oogmerk te schaden en met mogelijk nadeel voor iemand).

Bij de eigenlijke computersabotage is niet alleen het voorwerp van de handeling specifiek (zowel wegens de aard ervan: input- en outputgegevens en de programma's, als wegens de sterke 'Komprimierung' van de gegevens, waardoor de schadebedragen ook zeer hoog liggen), maar is ook de handeling zelf specifiek.

Men kan te maken hebben met klassieke bedrijfssabotage (b.v. lossnijden van kabels), maar de dader kan ook anders te werk gaan: met een magneet voor het elektromagnetisch geheugen; met bepaalde terminalopgaven of bepaalde overeenkomende programma's mits programmeer- en systeemkennis; de netwerken geven ook specifieke mogelijkheden, enz.

Vernietiging van software gaat vaak gepaard met vernietiging van hardware. Met al deze aspecten dient rekening gehouden te worden bij een eventuele incriminatie van computersabotage.

4. Tijddiefstal

Het gaat om het ongeoorloofd gebruik van de computer zelf, om een loutere gebruiksaanmatiging. Hiervan zijn evenmin voorbeelden gekend in onze rechtspraak. Buiten diefstal van elektriciteit, wat dan alleen op die elektriciteit slaat, komt geen enkele bepaling ter beteugeling van dit feit in aanmerking.

We kennen slechts een zeer ontoereikende, gelimiteerde strafrechtelijke bescherming tegen computerfraude: computermanipulatie wordt slechts zeer uitzonderlijk beteugeld door de bepaling van oplichting en/of door deze van valsheid in geschriften, computerspionage door deze van diefstal of diefstal van elektriciteit (maar die bepalingen slaan strikt genomen niet op de abstracte inhoud van het gestolene) als er materiële wegname is, in enkele gevallen door de bepaling van oplichting. Computersabotage wordt slechts zeer uitzonderlijk door 'valsheid in geschriften' beteugeld, tijddiefstal blijft onbeteugeld. Nieuwe bepalingen zijn nodig alsook de aanpassing van zekere bestaande bepalingen.

Tot slot dient in verband hiermee nog opgemerkt te worden dat inzake *misbruik van automatische geldverdelers* de traditionele bepalingen van toepassing zijn.

In tegenstelling tot de Franse rechtspraak[39] en rechtsleer[40] heeft de Belgische jurisprudentie de bepaling van diefstal aangepast bevonden aan geldopna-

39. Cass., Fr., 24 november 1983, *D. Sirey,* 1984, 165.
40. Zie: CORLAY, P., *l.c.,* 3160.

me zonder dekking uit een bankbiljettenautomaat.[41] Wordt gebruik gemaakt van een valse of een gestolen legitimatiekaart, dan is dit diefstal met behulp van valse sleutels.[42] Wordt door een verkeerde programmatie van de computer meer geld afgeleverd dan volgens de provisie voorradig is en de malafide rekeninghouder verbergt het, is dit bedrieglijke verberging.[43]

IV. Besluit

Computercriminaliteit maakt duidelijk een groeiend probleem uit. De beveiliging van software kent verschillende aspecten waarmee rekening gehouden moet worden, een interdisciplinaire samenwerking is nodig. In elk geval dient de wetgever op te treden. Het informaticamisdrijf in de strafwet introduceren veronderstelt echter wel voorafgaandelijk een weloverwogen opportuniteits- of beleidsbeslissing, alsmede een daarmee gepaard gaande keuze inzake wetgevende techniek.

Men kan er dan over twisten of bijstelling van het bestaande normenstelsel voldoende is, dan wel of een revolutionair-nieuwe aanpak vereist is. In elk geval staat het vast dat wanneer de computer problemen van dergelijke afmetingen schept, er iets aan gedaan moet worden.

---

41. Corr. Antwerpen, 29 april 1971, *R.W.*, 1971-72, 482, noot LIEBAERT, J.; Gent, 21 december 1981, *R.W.*, 1981-82, 2561, noot VANDEPLAS, A.; Corr. Luik, 22 maart 1982, *Jur. Liège,* 1982, 319, noot PIEDBŒUF, F.
42. Brussel, 22 maart 1973, *J.T.*, 1974, 65, noot VANDERVEEREN, P.; Corr. Hasselt, 26 oktober 1984, niet uitgegeven.
43. Cass., 16 mei 1979, *R.D.P.*, 1979, 688.