LJN: AO7009, Hoge Raad , 01474/03

Datum uitspraak:	28-09-2004
Datum publicatie:	29-09-2004
Rechtsgebied:	Straf
Soort procedure:	Cassatie
Inhoudsindicatie:	Verspreiding worm-computervirus waardoor mail-servers konden vastlopen. 1. De opvatting dat van “schade” ex art. 350a.3 Sr eerst sprake is indien de betreffende gegevens daadwerkelijk schade aan gegevens in een geautomatiseerd werk hebben aangericht,is onjuist. 2. Voor strafbaarheid o.g.v. art. 350a.3 Sr is vereist dat verdachtes opzet erop is gericht dat de door hem ter beschikking gestelde of verspreide, zichzelf in een geautomatiseerd bestand vermenigvuldigende, gegevens schade kunnen aanrichten.

Uitspraak

28 september 2004
Strafkamer
nr. 01474/03
AGJ/SM

Hoge Raad der Nederlanden

Arrest

op het beroep in cassatie tegen een arrest van het Gerechtshof te Leeuwarden van 28 oktober 2002, nummer 24/000847-01, in de strafzaak tegen:
[verdachte], geboren te [geboorteplaats] op [geboortedatum] 1980, wonende te [woonplaats].

1. De bestreden uitspraak

Het Hof heeft in hoger beroep - met vernietiging van een vonnis van de Arrondissementsrechtbank te Leeuwarden van 27 september 2001 - de verdachte ter zake van "opzettelijk en wederrechtelijk gegevens verspreiden die bedoeld zijn om schade aan te richten door zichzelf te vermenigvuldigen in een geautomatiseerd werk" veroordeeld tot een taakstraf, bestaande uit een werkstraf voor de duur van honderdvijftig uren, subsidiair 75 dagen hechtenis, met onttrekking aan het verkeer en verbeurdverklaring zoals in het arrest omschreven.

2. Geding in cassatie

Het beroep is ingesteld door de verdachte. Namens deze heeft mr. H.A. de Boer, advocaat te Workum, bij schriftuur middelen van cassatie voorgesteld. De schriftuur is aan dit arrest gehecht en maakt daarvan deel uit.
De Advocaat-Generaal Machielse heeft geconcludeerd tot verwerping van het beroep.

3. Beoordeling van het eerste middel

3.1. Het middel keert zich tegen de motivering van de bewezenverklaring. Mede blijkens de toelichting bevat het middel onder meer de volgende klachten. Uit de gebezigde bewijsmiddelen kan niet volgen dat het zichzelf vermenigvuldigende virus bedoeld was om schade aan te richten, welke schade ook niet daadwerkelijk is opgetreden, terwijl uit die bewijsmiddelen evenmin kan volgen dat het opzet van de verdachte was gericht op de omstandigheid dat de desbetreffende gegevens bedoeld waren om schade aan te richten.

3.2. Ten laste van de verdachte is bewezenverklaard dat:
"hij op 10 februari 2001 te en vanuit Sneek, in de gemeente Sneek, opzettelijk en wederrechtelijk gegevens, te weten een zogenaamd Worm-computervirus (het Kournikova-virus), heeft verspreid die bedoeld zijn om schade aan te richten door zichzelf te vermenigvuldigen in een geautomatiseerd werk, immers heeft verdachte opzettelijk en wederrechtelijk een elektronisch bericht, dat die gegevens bevatte, in de (internet)nieuwsgroep alt.binaries.anna-kournikova geplaatst terwijl voornoemd virus bij opening van dit bericht door andere deelnemers/gebruikers van die nieuwsgroep zich, zonder dat daarvoor een nadere handeling was vereist, heeft vermenigvuldigd of kon vermenigvuldigen onder de contactpersonen, voorkomende in het adressenbestand van die deelnemers/gebruikers."

3.3. Het in de bewezenverklaring, overeenkomstig de tenlastelegging, voorkomende begrip "bedoeld om schade aan te richten" is daarin klaarblijkelijk gebezigd in de betekenis die daaraan toekomt in art. 350a, derde lid, Sr.

3.4. Blijkens de aanvulling op het verkorte arrest als bedoeld in art. 365a, tweede lid, Sv heeft het Hof de bewezenverklaring doen steunen op de volgende bewijsmiddelen:
"1. Een proces-verbaal, nr. 20010140543, d.d. 22 maart 2001 op ambtsbelofte opgemaakt door G. Bosma, brigadier van politie, taakaccenthouder digitaal rechercheren, eenheid criminaliteitsbeheersing Sneek, (dossierparagraaf 2.1.2. van een dossierproces-verbaal, nr. 2001014054, d.d. 2 april 2001 op ambtsbelofte opgemaakt door Bosma voornoemd), - zakelijk weergegeven - inhoudende:

als verklaring van verbalisant
Op 14 februari 2001 heb ik de computer van [verdachte] onderzocht. De harde schijf bevatte de directory "My virus". Deze directory bevatte een sub-directory "NEW" en in deze sub-directory werd een bestand aangetroffen met de naam
"Anna-Kournikova.jpg.zip". Dit bestand zou op 10 februari 2001 zijn gemaakt. Nadat ik dat bestand had geopend bleek hier een verpakt bestand in te zitten met de naam "Anna Kournikova.jpg.vbs.". Het op het internet verspreide virus had de naam "Anna Kournikova.jpg.vbs." Het virus "Anna Kournikova.jpg.vbs" was op 10 februari 2001 vervaardigd. Verder trof ik op de schijf een html-code aan. In deze code is te zien dat in de nieuwsgroep "alt.binaries.anna-kournikova" het bericht "New Pic" werd geplaatst. Vervolgens blijkt uit deze data dat het bestand "Anna Kournikova.jpg.vbs." als bijlage bij dit bericht werd gevoegd. Verder trof ik gegevens aan waaruit blijkt dat het bericht "New Pic", met hieraan gekoppeld het bestand "Anna Kournikova.jpg.vbs.", op 10 februari 2001 binnen de nieuwsgroep is verspreid.

2. Een schriftelijk stuk, te weten een ongedateerd rapport van A.J. Lamers, inspecteur van politie, digitaalrechercheur, en P. Janssen, internetrechercheur, beiden werkzaam bij het Project Digitaal Rechercheren, (als dossier-paragraaf 2.1.5.1. gevoegd in het sub 1 vermelde dossierproces-verbaal), - zakelijk weergegeven - inhoudende:

als verklaring van verbalisanten, dan wel één hunner
Wij hebben een onderzoek ingesteld naar de werking van het Anna Kournikova-virus. Het Visual Basic Script, bekend onder de naam Kournikova-virus, is in zeer korte tijd wereldwijd over het internet verspreid doordat het gebruik maakte van een veiligheidslek in het veelgebruikte e-mailprogramma Outlook Express van Microsoft. Het script werd geactiveerd wanneer de gebruiker het script opende vanuit zijn e-mailprogramma. Het script verstuurde zichzelf naar alle aanwezige e-mailadressen in het adresboek van de gebruiker. Daardoor was het mogelijk dat mail-servers, zowel pop als smtp, de plotselinge stroom data niet af konden handelen en hierdoor vastliepen (crashten).

3. Een proces-verbaal, nr. 2001014054-6, d.d. 13 maart 2001 op ambtsbelofte opgemaakt door Bosma voornoemd, (dossier-paragraaf 2.1.3.2. van het sub 1 vermelde dossierproces-verbaal), inhoudende - zakelijk weergegeven -:

als verklaring van verdachte
In februari 2001 heb ik het computervirus met de naam "Anna Kournikova.jpg.vbs." vervaardigd met

behulp van het programma Vbs Worm Generator l.5b. Nadat ik het virus gemaakt had heb ik dit geplaatst in de nieuwsgroep "alt.binaries.anna-kournikova". Het bericht zelf heb ik geplaatst met de vermelding "New Pic". Hieraan was het computervirus
"Anna Kournikova.jpg.vbs" gehangen. Ik weet dat een computervirus dat op deze wijze op het Internet wordt gezet zich snel kan verspreiden. Op 12 februari 2001 ben ik op internet gaan zoeken bij diverse newsagency's. Overal waar ik keek zag ik dat er computers besmet waren geraakt door mijn computervirus en overal werd voor dit virus gewaarschuwd.

4. De verklaring van verdachte ter 's hofs terechtzitting d.d. 14 oktober 2002, inhoudende - zakelijk weergegeven -:
Ik heb het wormvirus onder de naam Anna Kournikova op 10 februari 2001 vanuit mijn ouderlijke woning te Sneek verspreid. Ik beschikte destijds over meer dan 7000 virussen. Ik had verwacht dat het virus zich op grote schaal zou verspreiden. Ik las in die tijd veel computerbladen. Ik kende het "I love you"-virus. Ik had ten tijde van de verspreiding van het virus behoorlijk veel verstand van computers."

3.5. Art. 350a, derde lid, Sr luidt als volgt:
"Hij die opzettelijk en wederrechtelijk gegevens ter beschikking stelt of verspreidt die bedoeld zijn om schade aan te richten door zichzelf te vermenigvuldigen in een geautomatiseerd werk, wordt gestraft met gevangenisstraf van ten hoogste vier jaren of geldboete van de vijfde categorie."

3.6.1. Voorzover aan de desbetreffende klachten van het middel de opvatting ten grondslag ligt dat van "schade" als bedoeld in art. 350a, derde lid, Sr eerst sprake is indien de in die bepaling bedoelde ter beschikking gestelde of verspreide gegevens daadwerkelijk schade aan gegevens in een geautomatiseerd werk hebben aangericht, is deze opvatting onjuist (vgl. Kamerstukken II 1990-1991, 21 551, nr. 7, blz. 5). In zoverre falen de klachten.

3.6.2. Voor het overige is blijkens de inhoud van de door het Hof gebezigde, onder 3.4 weergegeven, bewijsmiddelen - welke onder meer inhouden dat door het onderhavige computervirus mail-servers konden vastlopen - de bewezenverklaring wat betreft het schadelijke karakter van de desbetreffende door de verdachte verspreide, zichzelf vermenigvuldigende, gegevens voldoende met redenen omkleed. In zoverre falen de klachten eveneens.

3.7. De klacht van het middel dat het opzet van de verdachte niet uit de bewijsmiddelen kan worden afgeleid, stelt de rechtsvraag aan de orde of het opzet van de dader mede daarop gericht moet zijn dat de verspreide gegevens bedoeld zijn om schade aan te richten of dat daarvoor voldoende is dat het opzet is gericht op het zichzelf vermenigvuldigende karakter van de desbetreffende gegevens. Daaromtrent geldt het volgende. Voor strafbaarheid op grond van art. 350a, derde lid, Sr is vereist dat het opzet van de verdachte erop is gericht dat de door de verdachte ter beschikking gestelde of verspreide, zichzelf in een geautomatiseerd bestand vermenigvuldigende, gegevens schade kunnen aanrichten. Die uitleg strookt met de tekst van deze bepaling, waarin het begrip "opzettelijk" voorafgaat aan het bestanddeel "bedoeld om schade aan te richten", terwijl de wetsgeschiedenis geen aanknopingspunten biedt voor de andere opvatting. In deze zaak kan dat opzet uit de gebezigde bewijsmiddelen worden afgeleid.

3.8. De overige klachten die het middel behelst kunnen evenmin tot cassatie leiden. Dit behoeft, gezien art. 81 RO, geen nadere motivering, nu die klachten niet nopen tot beantwoording van rechtsvragen in het belang van de rechtseenheid of de rechtsontwikkeling.

4. Beoordeling van het tweede middel

Het middel kan niet tot cassatie leiden. Dit behoeft, gezien art. 81 RO, geen nadere motivering nu het middel niet noopt tot beantwoording van rechtsvragen in het belang van de rechtseenheid of de rechtsontwikkeling.

5. Slotsom

Nu de middelen niet tot cassatie kunnen leiden, terwijl de Hoge Raad ook geen grond aanwezig oordeelt waarop de bestreden uitspraak ambtshalve zou behoren te worden vernietigd, moet het beroep worden verworpen.

6. Beslissing

De Hoge Raad verwerpt het beroep.

Dit arrest is gewezen door de vice-president F.H. Koster als voorzitter, en de raadsheren A.J.A. van Dorst, W.A.M. van Schendel, J.W. Ilsink en J. de Hullu, in bijzijn van de griffier S.P. Bakker, en uitgesproken op 28 september 2004.

Conclusie

Nr. 01474/03
Mr Machielse
Zitting 30 maart 2004

Conclusie inzake:

[verdachte]

1. Het Gerechtshof te Leeuwarden heeft op 28 oktober 2002 verdachte voor het opzettelijk en wederrechtelijk gegevens verspreiden die bedoeld zijn om schade aan te richten door zichzelf te vermenigvuldigen in een geautomatiseerd werk veroordeeld tot een werkstraf van 150 uren en tot onttrekking aan het verkeer en verbeurdverklaring zoals in het arrest aangegeven.
Het betreft degene die in 2001 het zgn. Kournikova-virus heeft gemaakt en op het internet gezet.

2. Mr. H.A. De Boer, advocaat te Workum, heeft cassatie ingesteld en een schriftuur ingezonden, houdende twee middelen van cassatie.

3.1. Het eerste middel komt op tegen de bewezenverklaring, die als volgt luidt:

"(dat) hij op 10 februari 2001 te en vanuit Sneek, in de gemeente Sneek, opzettelijk en wederrechtelijk gegevens, te weten een zogenaamd Worm-computervirus (het Kournikova-virus), heeft verspreid die bedoeld zijn om schade aan te richten door zichzelf te vermenigvuldigen in een geautomatiseerd werk, immers heeft verdachte opzettelijk en wederrechtelijk een elektronisch bericht, dat die gegevens bevatte, in de (internet)nieuwsgroep alt.binaries.anna-kournikova geplaatst, terwijl voornoemd virus bij opening van dit bericht door andere deelnemers/gebruikers van die nieuwsgroep zich, zonder dat daarvoor een nadere handeling was vereist, heeft vermenigvuldigd of kon vermenigvuldigen onder de contactpersonen, voorkomende in het adressenbestand van die deelnemers/gebruiker."

De steller van het middel bestrijdt dat de inhoud der gebezigde bewijsmiddelen toelaat bewezen te verklaren dat het zichzelf verspreidende virus bedoeld was om schade aan te richten door dit verspreiden.
Voorts zouden de bewijsmiddelen niet de conclusie kunnen dragen dat het opzet van verdachte erop was gericht om schade toe te brengen.
Tenslotte zou niet kunnen bewezen worden dat het virus automatisch verspreid werd, omdat de gebruiker nog de bijlage moest aanklikken om verspreiding te bewerkstelligen.

3.2. Het misdrijf waarvoor verdachte is veroordeeld is dat van het derde lid van art. 350a Sr.
Het hof heeft de volgende bewijsmiddelen gebezigd waarin de karakteristieken van het door verdachte verspreide virus zijn opgetekend:

- Als verklaring van verbalisanten (bewijsmiddel 2):

"Het Visual Basic Script, bekend onder de naam Kournikova-virus, is in zeer korte tijd wereldwijd over het internet verspreid doordat het gebruik maakte van een veiligheidslek in het veelgebruikte e-mailprogramma Outlook Express van Microsoft. Het script werd geactiveerd wanneer de gebruiker het script opende vanuit zijn e-mailprogramma. Het script verstuurde zichzelf naar alle aanwezige e-mailadressen in het adresboek van de gebruiker. Daardoor was het mogelijk dat mail-servers, zowel pop als smtp, de plotselinge stroom data niet af konden handelen en hierdoor vastliepen (crashten)."

- Als verdachtes eigen tegenover verbalisanten afgelegde verklaring (bewijsmiddel 3):
"In februari 2001 heb ik het computervirus met de naam "Anna Kournikova.jpg.vbs." vervaardigd met behulp van het programma Vbs Worm Generator 1.5b. Nadat ik het virus gemaakt had heb ik dit geplaatst in de nieuwsgroep "alt.binaries.anna-kournikova". Het bericht zelf heb ik geplaatst met de vermelding "New Pic" . Hieraan was het computervirus "Anna Kournikova.jpg.vbs" gehangen. Ik weet dat een computervirus dat op deze wijze op het internet wordt gezet zich snel kan verspreiden. Op 12 februari 2001 ben ik op internet gaan zoeken bij diverse newsagency's. Overal waar ik keek zag ik dat er computers besmet waren geraakt door mijn computervirus en overal werd voor dit virus gewaarschuwd."

- Als verdachtes in hoger beroep afgelegde verklaring (bewijsmiddel 4):
"Ik heb het wormvirus onder de naam Anna Kournikova op 10 februari 2001 vanuit mijn ouderlijke woning te Sneek verspreid. Ik beschikte destijds over meer dan 7000 virussen. Ik had verwacht dat het virus zich op grote schaal zou verspreiden. Ik las in die tijd veel computerbladen. Ik kende het "I love you"-virus. Ik had ten tijde van de verspreiding van het virus behoorlijk veel verstand van computers."

3.3. In het oorspronkelijk voorstel voorzag art. 350a Sr enkel in een strafbaarstelling van manipulatie van gegevens die door middel van een geautomatiseerd werk zijn opgeslagen. De voorgestelde tekst had de volgende inhoud:

"Hij die opzettelijk en wederrechtelijk gegevens die door middel van een geautomatiseerd werk zijn opgeslagen, worden verwerkt of overgedragen, verandert, wist, onbruikbaar of ontoegankelijk maakt, dan wel andere gegevens daaraan toevoegt, wordt gestraft met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie."

De memorie van toelichting liet weten dat onder meer bedoeld was de invoering van een computervirus onder de strafwet te brengen.(1) In de memorie van antwoord verwees de minister naar een rapport van het Landelijk Platform Computercriminaliteit, waarin justitie en het bedrijfsleven samenwerkten, in welk rapport werd aanbevolen de verspreiding van computervirussen strafbaar te stellen.(2) Tevens gaf de minister aan dat de voorgestelde bepaling slechts vergde dat bepaalde aanwijsbare gegevens gewijzigd waren.(3) Bij nota van wijziging bracht de minister een aanvulling op het voorgestelde art. 350a Sr aan en wel door toevoeging van een tweede en derde lid met de volgende inhoud:

"2. Hij die opzettelijk gegevens ter beschikking stelt of verspreidt die geschikt zijn om in geautomatiseerd werk zichzelf te vermenigvuldigen, wordt gestraft met gevangenisstraf van ten hoogste vier jaren of geldboete van de vijfde categorie.
3. Niet strafbaar is degeen die het feit, bedoeld in het tweede lid, pleegt met het oogmerk om schade als gevolg van deze gegevens te beperken."

De toelichting op dit voorstel van wijziging is summier en luidt als volgt:

"Het voorgestelde tweede lid van artikel 350a ziet op de strafbaarstelling van de verspreiding van virussen, ook wanneer deze nog niet daadwerkelijk schade heben aangebracht in een geautomatiseerd werk. In het derde lid is een strafuitsluitingsgrond opgenomen voor degeen die maatregelen tegen de schadelijke gevolgen van een virus onderneemt, bij voorbeeld door deze ter beschikking te stellen van een externe deskundige opdat deze kan onderzoeken hoe schade kan worden tegengegaan."(4)

Leden van de vaste Commissie voor justitie vroegen zich af of het voorgestelde tweede lid niet beter kon worden toegesneden op het effect van de manipulatie der gegevens en stelden de minister voor het tweede lid als volgt in te kleden:

"Hij die gegevens, bestemd voor de verwerking in een geautomatiseerd werk, ter beschikking stelt, verspreidt of ter verspreiding in voorraad heeft, wetende dat 1 deze gegevens:
1. andere in een geautomatiseerd werk aanwezige gegevens kunnen wissen, onbruikbaar maken of ontoegankelijk maken, hetzij;
2. stoornis in de gang of werking van een geautomatiseerd werk kunnen veroorzaken, wordt gestraft met..."(5)

De Nota naar aanleiding van het eindverslag ging in op de vraag van leden van de Tweede Kamer of het niet gewenst was een culpoze variant van art. 350a Sr te introduceren. De minister wees deze suggestie van de hand. Zo een uitbreiding zou niet stroken met het bestaande niveau van strafrechtelijke bescherming. De minister wees op de reikwijdte van het voorwaardelijk opzet en verklaarde dat het voorgestelde art. 350a Sr zowel degene die opzettelijk een geautomatiseerd werk met een virus besmet strafbaar stelde als degene die gegevens ter beschikking heeft dan wel verspreidt waarvan hij weet dat zij geschikt zijn om zich in een geautomatiseerd werk te vermenigvuldigen.(6) Naar aanleiding van opmerkingen van de Tweede Kamer werd overigens het voorgestelde art. 350a Sr weer gewijzigd en kwamen het derde en vierde lid als volgt te luiden:

"3. Hij die opzettelijk gegevens ter beschikking stelt of verspreidt die geschikt zijn om schade aan te richten door zichzelf te vermenigvuldigen in een geautomatiseerd werk, wordt gestraft met gevangenisstraf van ten hoogste vier jaren of geldboete van de vijfde categorie.
4. Niet strafbaar is degeen die het feit, bedoeld in het derde lid, pleegt met het oogmerk om schade als gevolg van deze gegevens te beperken."(7)

De toelichting op deze wijziging luidt als volgt:
"Het nieuwe derde lid heeft betrekking op virussen. Deze bepaling moet bij nader inzien stringenter worden omschreven. Niet alleen moet het gaan om gegevens die geschikt zijn om zichzelf te vermenigvuldigen. Dergelijke gegevens kunnen nodig zijn voor bepaalde noodzakelijk te verrichten functies. Bijkomend bestanddeel is dat zij geschikt zijn om schade aan te richten. Verder moet er een causaal verband zijn tussen het zich vermenigvuldigen en het aanrichten van schade."(8)
Maar sommige leden van de Tweede Kamer waren nog niet tevreden en stelden een amendement op art. 350a Sr voor waardoor het derde lid de volgende inhoud zou krijgen:

"3. Hij die opzettelijk en wederrechtelijk gegevens ter beschikking stelt of verspreidt die bedoeld zijn om schade aan te richten door zichzelf te vermenigvuldigen in een geautomatiseerd werk, wordt gestraft met gevangenisstraf van ten hoogste vier jaren of geldboete van de vijfde categorie."

Met de introductie van de termen "wederrechtelijk" en "bedoeld" zou volgens de schriftelijke toelichting op het amendement worden voorkomen dat het opzettelijk, maar te goeder trouw een besmet programma ter beschikking stellen onder deze bepaling valt. Te denken zou bijvoorbeeld zijn aan het gebruik van een besmet programma ten behoeve van studiedoeleinden.(9)

3.4. Ik betwijfel of het aldus toevoegen van het bestanddeel 'wederrechtelijk' en de vervanging van het bestanddeel 'geschikt' door 'bedoeld' meer aan de delictsinhoud toevoegt dan een zekere mate van onzekerheid.(10) Door de scheiding tussen 'opzettelijk' en 'wederrechtelijk' behoeft het opzet van de dader niet op de wederrechtelijkheid te zijn gericht. Degene die te goeder trouw aan een ander een virus ter beschikking stelt voor studiedoeleinden kan geacht worden niet wederrechtelijk te handelen, maar mij dunkt dat ook al veel uitzonderingen door het vierde lid worden afgevangen. Het 'bedoeld zijn om schade aan te richten' zal niet aldus uitgelegd moeten worden dat verdachte bij het verspreiden de bedoeling moet hebben om schade aan te richten. Dan had het voor de hand gelegen als het amendement anders zou hebben geluid; bijvoorbeeld: "Hij die opzettelijk en wederrechtelijk gegevens ter beschikking stelt of verspreidt om schade aan te richten (etc.)." De bedoeling om schade aan te richten door zichzelf te vermenigvuldigen lijkt mij een eerder objectief gegeven te zijn waarin

de werking van het virus tot uitdrukking komt. Steun voor deze uitleg is ook te vinden bij de inhoud van de culpoze variant van art. 350b Sr. Het tweede lid van die bepaling spreekt óók van 'gegevens die bedoeld zijn om schade aan te richten door zichzelf te vermenigvuldigen'. Een subjectieve bedoeling is niet gemakkelijk met de culpa te rijmen. Kaspersen heeft dan ook bepleit het woord 'bedoeld' in de bepaling door 'bestemd' te vervangen.(11) Maar ook als men de zinsnede zo uitlegt dat het opzet wordt geaccentueerd en dat de kwade trouw van maker of verspreider aldus wordt benadrukt zal deze uitleg verdachte niet kunnen baten omdat toch moeilijk kan worden beweerd dat de kwade trouw van verdachte niet uit de gebezigde bewijsmiddelen is af te leiden.

3.5. Dat het virus dat verdachte heeft ontwikkeld bedoeld was om schade aan te richten door zichzelf te vermenigvuldigen - hoe ook te verstaan - is af te leiden uit de hiervoor aangehaalde bewijsmiddelen. Het gaat om een wormvirus dat zich nestelt in andermans computer en zich via de mail verspreidt. De schade bestaat erin dat servers verstopt kunnen raken, dat aldus computers niet meer bereikbaar of onbruikbaar worden(12) en dat besmette computers weer van het virus moeten worden ontdaan, hetgeen tijd en geld kost. Dat verdachte als verzamelaar van virussen en ontwerper van het Koernikova-virus opzet had op het veroorzaken van dat soort schade heeft het hof kunnen afleiden uit de eigen verklaring van verdachte (bewijsmiddel 4), die zegt het virus te hebben gecreëerd en op het internet te hebben gezet in de verwachting dat het zich op grote schaal zou verspreiden. Ik sluit mij aan bij de opmerking van Kaspersen dat een maker en verspreider van virussen toch geen andere bedoeling kan hebben dan schade aan te richten.(13) Dat het virus werkelijk schade heeft aangericht behoeft de rechter niet vast te stellen.(14) De steller van het middel tracht verdachte voor te stellen als een soort digibeet die niet zou weten wat een virus doet als dat eenmaal op het internet is geplaatst, maar verdachtes eigen verklaring (bewijsmiddel 4) spreekt andere boekdelen. Ik bestrijd de stelling in het middel dat het feit dat verdachte wist dat het virus zich op grote schaal zal verspreiden en dat hij verstand heeft van computers niet toereikend zou zijn om het opzet op de aard van het virus te vestigen, zeker in combinatie met de uitlating van verdachte dat hij een grote verzameling virussen heeft aangelegd en bekend was met het "I love you"-virus.
Eveneens kan uit de bewijsmiddelen worden afgeleid dat het virus zichzelf vermenigvuldigde. Bewijsmiddel 2 houdt immers in dat het virus zichzelf naar alle adressen in het adresboek van de computergebruiker verstuurde als het eenmaal was geactiveerd. Daaraan doet niet af dat de computergebruiker dat mechanisme in gang moest zetten door het bestand te openen; het was immers niet de gebruiker die het virus door eigen handelen naar alle adressen verzond, maar dit automatisme was in het virus ingebouwd.
Het eerste middel faalt in al zijn onderdelen.

4.1. Het tweede middel klaagt dat het hof niet heeft gerespondeerd op het verweer dat ontkende dat het bestanddeel 'wederrechtelijk' zou zijn vervuld.

4.2. Het betreft een bewijsverweer dat gewoonlijk zijn weerlegging in de bewijsconstructie vindt. Dat is ook hier het geval. Verdachte heeft, zo blijkt uit de bewijsmiddelen, een virus ontwikkeld en dat vermomd als nieuwe foto van Anna Kournikova in de nieuwsgroep "alt.binaries.anna-kournikova" geplaatst. Aldus is het virus niet verspreid ter bestudering of met een ander, geoorloofd doel. Integendeel, uit het feit dat verdachte het virus in een andere gedaante op zó een wijze heeft gelanceerd dat hij rekening moest houden met verspreiding op grote schaal volgt al dat er geen sprake is geweest van een gedraging waarvoor de strafbaarstelling niet bedoeld kan zijn en welke gedragingen door de eis van 'wederrechtelijkheid' van strafbaarheid zijn uitgesloten.
Het tweede middel faalt.

5. Beide middelen falen en kunnen met de aan art. 81 RO ontleende motivering worden verworpen. Ambtshalve heb ik geen grond gevonden die tot vernietiging aanleiding behoort te geven.

6. Deze conclusie strekt tot verwerping van het beroep.

De Procureur-Generaal
bij de Hoge Raad der Nederlanden

1 Kamerstukken II 1989-1990, 21551, nr. 3, p. 24.
2 Kamerstukken II 1990-1991, 21551, nr. 6, p. 1.
3 Kamerstukken II 1990-1991, 21551, nr. 6, p. 39.
4 Kamerstukken II 1990-1991, 21551, nr. 7, p. 5.
5 Kamerstukken II 1991-1992, 21551, nr. 10, p. 11.
6 Kamerstukken II 1991-1992, 21551, nr. 11, p. 10/11.
7 Kamerstukken II 1991-1992, 21551, nr. 12, Tweede nota van wijziging.
8 Kamerstukken II 1991-1992, 21551, nr. 12, p. 6.
9 Kamerstukken II 1991-1992, 21551, nr. 18, Amendement van de leden Koffeman en Jurgens.
10 Tijdens de mondelinge beraadslaging lichtte het lid Koffeman het amendement nog als volgt toe: "Waar het derde lid van artikel 350a spreekt van "opzettelijk gegevens ter beschikking stellen of verspreiden, die geschikt zijn om schade aan te richten, virussen en dergelijke" wordt over het hoofd gezien dat er in bepaalde situaties, bijvoorbeeld ten behoeve van studiedoeleinden of opsporingsactiviteiten, legitiem kan worden gehandeld en dat er toch strafbaarheid op grond van de wettekst kan ontstaan. Om deze goede trouw te beschermen, dient het element van wederrechtelijkheid in het derde lid te worden geïntroduceerd, terwijl de opzet tegelijkertijd wordt geaccentueerd als de brede term "geschikt" wordt
vervangen door "bedoeld". Ook wat dit betreft verwijs ik naar het amendement op stuk nr. 18." Handelingen II 93-5871.
11 Prof. mr. H.W.K. Kaspersen, De Wet computercriminaliteit is er - nu de boeven nog, in Computerrecht 1993, p. 137.
12 Vgl. HR NJ 1999, 251
13 Ibidem, p. 138.
14 NLR 3a/350a.