LARRY LEFFER VOR GERICHT
HAFTUNG FÜR COMPUTERVIREN

Vortrag auf dem 1. Computerviren-Symposium in Neuss am 11. April 1991

I. Einleitung

Die CeBIT hat eben in Hannover ihre Tore geschlossen. Schon weit vor ihrem Beginn beherrschte die Messe das Geschehen in deutschen Zeitungen und Zeitschriften, und das nicht nur im Bereich der EDV-spezifischen Fachpresse. Dass dies so war, stellt gegenüber den Vorjahren kein Novum dar.

Bei der Lektüre fiel mir allerdings in diesem Jahr auf, dass mehr denn je von Computerviren die Rede war. Von der Wirtschaftswoche bis hin zur CHIP widmeten die Redaktionen den (meist) bösartigen Programmutanten Leitartikel und Aufmacher. Unser Gastgeber befindet sich mit seiner Entscheidung für die Einladung zu einem »Computer-Viren Symposium« mithin in guter Gesellschaft. Die Zeiten, in denen sich allein der Computer Chaos Club in Hamburg mit Computerviren befasste, sind angesichts des Umfangs der bislang festgestellten Infektionen endgültig vorbei.

a) Wachsende Zahl von Infektionen

Die Frankfurter Allgemeine Zeitung meldete in Ihrer Ausgabe vom 12. März 1991[1], dass die Anzahl der Computerviren beständig steigt. Zur Zeit sind rund 400 verschiedene Arten bekannt.[2] Nach Einschätzung der großen Mehrheit der Teilnehmer der Europäischen Konferenz über Computerviren im Dezember 1990 in Hamburg werden es innerhalb von nur 18 Monaten 1.000 sein.[3] Die Zahl der allein in Deutschland infizierten Personalcomputer erreicht 200.000.[4] Untersuchungen der Zeitschrift CHIP zufolge soll auf der CeBIT 1990 jeder neunte Rechner befallen gewesen sein.[5] Die Viren treten dabei in den unterschiedlichsten Spielarten auf. Eines der jüngsten Exemplare der Spezies, ein sogenanntes »music-bug« namens »Ohropax«,

1 Fischer in: F.A.Z. v. 12.3.91, Beilage CeBIT '91, S. B 34.
2 Thoms in: »Epidemie im Computer«, Wirtschaftswoche v. 15.3.1991, S. 105; nach anderen Quellen (Sabetzki in: »Hoffentlich wurden die Daten gesichert«, Handelsblatt v. 13.3.91, Beilage »Computer und Kommunikation«, S. B 25) sind es erst 250.
3 Fischer in: »Gefahr erkannt, Gefahr gebannt«, F.A.Z. v. 12.3.91, Beilage CeBIT '91, S. B 34.
4 Brunnstein, zit. in Thoms, »Epidemie im Computer«, Wirtschaftswoche v.15.3.91, S. 105.
5 Thoms in: »Epidemie im Computer«, Wirtschaftswoche v. 15.3.91, S. 105.

zeichnet sich dadurch aus, dass es nicht nur den Zugriff auf die Diskettenlaufwerke verlangsamt, sondern dabei auch noch Musik spielt.[6]

b) Ursachen der Verbreitung

Schuld an dieser sprunghaften Entwicklung sind zunächst natürlich diejenigen, die neue Viren bewusst kreieren und darauf aus sind, diese anschließend zu verbreiten.

Hierzu zählen keineswegs nur lichtscheue Hacker, sondern durchaus auch angesehene Softwarehäuser, die auf diese Weise ihre Produkte vor Raubkopierern zu schützen suchen.[7] Nur aus diesem Beweggrund heraus wurden Anfang der siebziger Jahre überhaupt die ersten Viren geschaffen.[8] Man vermutet, dass im gerade beendeten Golfkrieg in die militärischen Computersysteme des jeweiligen Gegners vorsätzlich eingebrachte Computerviren eine ausschlaggebende Rolle gespielt haben oder jedenfalls spielen sollten. Und im vergangenen Jahr versprach gar das Pentagon öffentlich demjenigen, der ein akzeptables Konzept für einen militärisch nutzbaren Computervirus vorlegt, eine Belohnung von 50.000 Dollar und stellte darüber hinaus bei Funktionieren einen Auftrag in Höhe von 500.000 Dollar in Aussicht.[9] Niemand kann die Zahl der Hobbyprogrammierer schätzen, die sich aufgrund dieser Ausschreibung daranmachten, Viren zu schreiben – und sie auf fremden Zielsystemen zu testen. Experten wundern sich, dass sich der Schaden bislang in Grenzen hielt. Sie halten es angesichts dieser Entwicklung nur für eine Frage der Zeit, bis eine Welle von Computerkriminalität über uns hereinbrechen wird.[10]

Neben dieser vorsätzlichen Art, Viren zu verbreiten, trägt aber andererseits vor allem das sorglos fahrlässige Verhalten von Herstellern, Vertreibern und Anwendern von Software zu deren rascher Ausbreitung bei. In jüngerer Zeit tauchen immer mehr Viren aus dem Osten Europas auf. Der Boom, der vor etwa zwei Jahren in Bulgarien zu verzeichnen war, scheint nun in der UDSSR eine Wiederholung zu finden, weil viele Hersteller in osteuropäischen Ländern Software in Lohnarbeit erstellen lassen. Selbst führende Softwarehäuser haben bereits Pannen erlebt und verseuchte Software an ihre Kunden ausgeliefert, obwohl schon seit geraumer Zeit Empfehlungen existieren, deren Beachtung die meisten dieser Vorkommnisse hätten verhindern können. Zwischenhändler übertragen die Viren auf die Rechner ihrer Kunden, weil sie nicht die notwendige Sorgfalt bei Kopieroperationen beachten. Und schließlich ist es der Anwender selbst, der eigene und fremde Systeme dadurch verseucht, dass er mit Kopien von Originalprogrammen arbeitet, die aus dubiosen Quellen stammen. Hierzu zählt die sogenannte Public Do-

6 CHIP, Heft 3/91, S. 6; WDR-Radio-Sendung v. 15.3.91, 19-20 Uhr.
7 Vgl. hierzu die Nachweise bei Rombach, CR 1990, 101, Fn. 5 und Dehn/Paul, Vorbeugung bei Computerviren, CR 1989, 68, 69.
8 Fausten/Rompel, Aktenzeichen Computer, S. 111.
9 Randow in: CHIP, Heft 3/91, S. 25.
10 BSI-Chef Leiberich, zit. in: Randow, CHIP, Heft 3/91, S. 24.

main Software, deren Anteil an den Infektionsquellen inzwischen bei 33% liegt.[11] Infiziert sind häufig auch die Programme, die in Mailboxen bereit gehalten werden. Vor allem in größeren Unternehmen kommt es dann immer wieder vor, dass die Mitarbeiter nicht darauf verzichten wollen, die derart erlangten Computerspiele zur Freude der Kollegen und zum Leidwesen der Firmenleitung ins Netz einzubringen, ohne an die Folgen zu denken. Wie heißt es in einem Werk zur Computerkriminalität so schön: »Der 'Erfinder' von Computerviren kann noch immer mit der Dummheit seiner Opfer rechnen.«[12]

Auf diese Weise finden Computerviren idealen Nährboden für ihre Fortpflanzung. Die damit einhergehenden Schäden sind erheblich. Wege zu ihrer Vermeidung, Begrenzung und Behebung aufzuzeigen, Verantwortliche haftbar zu machen, ist Aufgabe auch der Juristen. Ich will mich heute bemühen, Ihnen einige wenige Ansätze näher zu bringen.

II. Computer im Recht

Juristen stehen in dem Ruf, mit Elektronischer Datenverarbeitung auf Kriegsfuß zu stehen. Aus meiner eigenen Erfahrung heraus kann ich diese Einschätzung nicht uneingeschränkt bestätigen, gebe aber zu, dass sich vor allem ältere Kollegen auch heute noch schwer tun im täglichen Umgang mit Textverarbeitung und Tabellenkalkulation. Gerade deshalb entwickelte sich erst nach und nach das Verständnis dafür, dass so manches Problem, das sich im Zusammenhang mit dem Einsatz von Computern ergibt, mit herkömmlichen juristischen Maßstäben nicht ohne weiteres in den Griff zu bekommen war. Software ist keine »bewegliche Sache«, die wie ein Auto gestohlen werden kann; sie ist aber auch nicht ohne weiteres eine geistige Schöpfung wie das Buch, dem das Urheberrecht Schutz verschafft.

Rechtsprechung und Lehre bemühten (und bemühen) sich daher oft erfolglos, mit dem vorhandenen rechtlichen Instrumentarium zurechtzukommen.

Im Jahre 1986 wurde dann schließlich auch der Gesetzgeber aktiv und schuf neue strafrechtliche Vorschriften, die sich nun erstmals auch mit dem Computerumfeld befassen. Sie gab dem Rechtsanwender damit ein Werkzeug im Kampf gegen die Computerkriminalität an die Hand, dessen Effizienz sich allerdings erst noch erweisen muss.

Im zivilrechtlichen Bereich steht eine Kodifizierung bislang aus. Es bereitet daher nach wie vor vielfach Schwierigkeiten, neue Konstellationen im EDV-Bereich in das Korsett normierter Vertragstypen zu zwängen, wobei die Spannweite vom Kauf- über das Werk- bis hin zum Lizenzvertragsrecht reicht.

[11] Sabetzki in: Handelsblatt v. 13.3.91, Beilage »Computer und Kommunikation«, S. B 25.
[12] Fausten/Rompel, Aktenzeichen Computer, S. 139.

III. Strafrecht und Zivilrecht

Bei der rechtlichen Beurteilung des Einsatzes von Computerviren sind die strafrechtlichen von den zivilrechtlichen Aspekte zu trennen.

a) Strafrecht

Wenn der Jurist auf dem Gebiet des Strafrechts tätig wird, tut er das, was die große Öffentlichkeit, medienbeeinflußt (und -beeindruckt!) von amerikanischen Gerichtsepen und königlich-bayerischen Amtsgerichts-Tragikomödien, von ihm erwartet: Er führt Straftäter als Richter oder Staatsanwalt ihrer gerechten Strafe zu – oder versucht gerade dies als Verteidiger zu verhindern. Strafrechtliche Normen bestimmen somit, was die Allgemeinheit für strafbar hält und deshalb mit Geldstrafe oder Gefängnis bestraft sehen möchte. Solche Regeln finden sich, soweit sie hier von Interesse sind, in erster Linie im Strafgesetzbuch (StGB), aber auch in anderen Gesetzen, wie etwa dem Urhebergesetz (UrhG).

b) Zivilrecht

Von der Bestrafung des Übeltäters haben der virengeschädigte Anwender oder der redliche Vertriebshändler allerdings herzlich wenig. Sie möchten ihr Geld wiedersehen, dass sie durch Datenverlust und Programmzerstörung verloren haben. Die Frage, inwieweit ihnen ihr Schaden zu ersetzen ist, regelt vor allem das Zivilrecht. Hier finden sich Vorschriften zum Schadensersatz vor allem im Bürgerlichen Gesetzbuch (BGB).

Bei der Durchsetzung seiner Ansprüche muss der Geschädigte, anders als dies etwa im anglo-amerikanischen oder romanischen Rechtskreis der Fall ist, deshalb regelmäßig die Zivilgerichte anrufen. Der Strafrichter verurteilt den Täter zwar und kann ihm auferlegen, eine Geldstrafe in die Staatskasse zu zahlen. Der Geschädigte aber sieht nur dann etwas von seinem Geld wieder, wenn er aus dem Urteil eines Zivilgerichts vollstrecken kann.

Meine Ausführungen möchte ich aus diesem Grund auf die zivilrechtlichen Aspekten des Einsatzes von Computerviren beschränken.

IV. Definition: Virus

Die Zahl der Beispiele für den Einsatz von Sabotageprogrammen zur Schädigung von EDV-Systemen ist Legion. Die immer wieder zitierten Fälle reichen zurück bis in die sechziger Jahre. All diesen Sabotageprogrammen ist dabei gemeinsam, dass sie einen Auslöser für einen Zerstörungserfolg enthalten.

In der Familie der Sabotagegruppe zeichnen sich die Computerviren durch zwei Eigenschaften aus: Sie können Kopien ihres eigenen Programmcodes erzeugen und ihn in andere Computerprogramme einpflanzen, ohne die auf diese Weise »infizierten« Programme damit zu zerstören.

Daneben können sie zusätzliche, exakt vorherbestimmbare Funktionen wahrnehmen. Alle bisherigen Versuche, den Begriff »Computervirus« zu beschreiben oder zu umschreiben gehen dabei auf den Amerikaner Fred Cohen zurück. Frei übersetzt definierte er schon 1983:

> *»Der Computervirus ist ein Programm, das andere Programme durch Einbringung seiner eigenen Kopie infizieren kann.«*

Aus dieser Definition ergibt sich, dass Virusprogramme selbst neutral sind; ihre Existenz verursacht noch keine Schäden in den »Wirtsprogrammen«. Viren können vielmehr auch zu nützlichen Zwecken Verwendung finden und verschiedene Hilfsfunktionen wahrnehmen (wie etwa das Komprimieren von Programmen zum Zwecke der Speichereinsparung). Zum Sabotageprogramm wird ein Virus erst dadurch, dass ihm als Zusatzfunktion ein »Sabotageauftrag« erteilt wird, indem es mit einem aktiven oder passiven Auslöser gekoppelt wird. Nun kann der Virus – in der EDV-Welt hat sich zur Unterscheidung vom medizinischen Virus die maskuline Schreibweise durchgesetzt[13] – als Trägermittel für jede erdenkliche Sabotagefunktion in allen Bereichen eines Rechnersystems dienen.

In Personal-Computern werden Viren zumeist durch die Verwendung von Datenträgern übertragen, auf denen sich infizierte Programme befinden. Werden diese gestartet, so breitet sich das Virus im System aus. Daneben ist im Zuge zunehmender Vernetzung von PCs auch die Übertragung von Viren über Datenfernleitungen zu befürchten. An die eingangs erwähnte Ansteckung durch Gratisprogramme aus Mailboxen sei erinnert.

IV. Zivilrechtliche Beurteilung

Nach dem ersten Auftreten von Computerviren dachten die Betroffenen sowohl in den USA als auch in Deutschland zunächst nicht an Schadensersatzansprüche im weiteren Sinne. Es ging ihnen vielmehr meist nur um die Beseitigung der Virenprogramme und die Wiederherstellung des alten Datenbestandes. Das Gesetz geht weiter. Es erlaubt es dem Geschädigten, vorausgesetzt, die grundsätzliche Haftung des Vireneinbringers steht fest, in vielen Fällen, Ersatz seines gesamten Schadens zu fordern. Hierzu gehören neben den Kosten einer Rekonstruktion des Datenbestandes auch die Aufwendungen für die Schadensermittlung, der durch die Infizierung bedingte Verdienstausfall und schließlich die Gerichts- und Anwaltskosten.

Bei der zivilrechtlichen Erfassung und Beurteilung des Einsatzes von Computerviren sind zweckmäßigerweise unterschiedliche Fallkonstellationen zu unterscheiden, je nachdem, ob die Viren vorsätzlich oder fahrlässig verbreitet werden.

---

[13] Dehn/Paul, CR 1989, 68.

a) Vorsätzliche Verbreitung von Viren

Dazu ein erstes Fallbeispiel:

Der Softwarehersteller S möchte ein von ihm geschaffenes Programm wirksam gegen Raubkopierer schützen. Er verfällt deshalb auf die Idee, eine seiner Neuschöpfungen mit einem Virus zu versehen, der ab der zweiten – unautorisierten – Kopie übertragen wird. Der Anwender A kauft bei S das Programm, stellt eine Kopie her und infiziert in der Folgezeit damit unwissentlich seine Festplatte. Hierdurch werden Daten zerstört; dem A entsteht ein erheblicher Schaden. Es fragt sich, ob er den S auf Ersatz in Anspruch nehmen kann.

aa) Vertragliche Ansprüche

Hier kann A zunächst versuchen, vertragliche Anspruchsgrundlagen heranzuziehen, da zwischen ihm und dem S ein Vertragsverhältnis besteht. In Betracht kommen Ansprüche wegen sogenannter Schlechterfüllung, die der Jurist »positive Forderungsverletzung« nennt. Gemeint ist damit, dass der S den Vertrag zwar grundsätzlich erfüllt hat, weil das verkaufte Programm als solches voll funktionstüchtig ist. S hat aber Nebenpflichten aus dem Vertrag verletzt, da durch sein Verhalten ein Schaden an den Rechtsgütern des A entstanden ist. Solche Schäden müssen die Vertragspartner voneinander fernhalten. Hier hat der S gegen diese Pflicht verstoßen, weil er vorsätzlich die Ursache für einen – im Übrigen vorhersehbaren – Schaden des A gesetzt hat.

Fraglich ist, ob sich an diesem Zwischenergebnis deshalb etwas ändert, weil der A selbst gegen seine vertragliche Verpflichtung, von Kopien abzusehen, verstoßen hat. Hinzukommt, dass § 53 Abs. 4 S. 2 bestimmt, dass »die Vervielfältigung eines Programms für die Datenverarbeitung ... oder wesentlicher Teil davon stets nur mit Einwilligung des Berechtigten« zulässig ist. Manche Autoren in der juristischen Fachwelt schließen hieraus, dass auch das Anfertigen einer bloßen Sicherungskopie gegen den Willen des Herstellers einen Verstoß gegen das geltende Urheberrecht darstellt.[14] Andere halten dem entgegen, dass die Vorschrift weit zu interpretieren sei.[15] Sie wolle nämlich lediglich verhindern, dass die Kopie parallel mit dem Originalprogramm auf weiteren Computeranlagen zum Einsatz kommt. Bei einer Sicherungskopie sei dies aber gerade nicht der Fall, so dass der Anwender immer das Recht habe, solche Archivexemplare zu erstellen. Eine solche Ansicht deckte sich im Übrigen mit der geltenden Rechtslage in den USA.

Während die Rechtsprechung bislang keine Gelegenheit hatte, sich mit der Frage auseinanderzusetzen, tendiere ich selbst dazu, noch weiter zu gehen. Selbst dann, wenn der Anwender vertragswidrig und unter Verstoß gegen das Urheberrechtsgesetz dazu übergeht, Raubkopien

[14] Nachweise bei Rombach, CR 1990, 101, 103, Fn. 27.
[15] Nachweise bei Rombach, CR 1990, 101, 103, Fn. 28.

zu erstellen, entbindet das den Hersteller nicht von seiner Haftung. Dazu muss man wissen, dass es keinen allgemeinen Rechtsgrundsatz gibt, wonach nur derjenige Rechte erfolgreich geltend machen kann, der sich selbst rechtstreu verhalten hat.[16] Solche eigenen Rechtsverstöße begründen unter den im Gesetz vorgesehenen Voraussetzungen ihrerseits Schadensersatzansprüche und geben dem anderen Teil die Befugnis zur Zurückbehaltung, führen aber nicht zu einem Wegfall eigener Rechte.[17] Nur in besonders krass liegenden Ausnahmefällen hat die Rechtsprechung bisher den Anspruch entfallen lassen.[18] Ein so gewichtiger Verstoß gegen die Interessen des S liegt sicher selbst dann nicht vor, wenn A das Programm im Freundeskreis verbreitet.

Eine Besonderheit gegenüber anderen Arten von Schadensverursachungen liegt allerdings hier darin, dass nicht der S, sondern der A selbst die letzte Ursache für den Schadenseintritt setzt, indem er Kopien herstellt und möglicherweise verbreitet. In der Rechtsprechung ist das Fehlverhalten Dritter als Grenze der Zurechenbarkeit anerkannt. Eine Einstandspflicht ist trotzdem nicht ausgeschlossen, wenn der Schaden durch eine Handlung verursacht worden ist, die nicht allein auf dem Fehlverhalten des Verletzten oder eines Dritten beruht.[19] Fehlt eine Warnung hinsichtlich der Gefahren, die von einer unautorisierten Kopie des Originalprogramms für Datenbestände einer Computeranlage ausgehen, so nutzt der Softwarehersteller den Raubkopierer quasi als Werkzeug der Schadensherbeiführung. Eine Unterbrechung des Ursachenzusammenhangs durch das Fehlverhalten des Raubkopierers, der ohne Kenntnis um die Gefahren virenverseuchte Programmkopien verbreitet, scheidet somit grundsätzlich aus.

Der Raubkopierer, der eine Kopie des Originalprogramms hergestellt hat und diese nicht als Sicherungskopie verwendet, muss sich allerdings sein Mitverschulden auf die Höhe des entstehenden Schadens anspruchsreduzierend anrechnen lassen.

Bei einer ausdrücklichen Warnung vor der Wirkung unautorisierter Kopien des Originalprogramms gestaltet sich die Rechtslage komplizierter. Führt der Verletzte in Kenntnis der Warnung an eigenen Sachen die Schädigung herbei oder billigt er den Einsatz raubkopierter Programme in Kenntnis der Warnung, ist die Kausalität zu bejahen, wenn zu dieser schädigenden Handlung durch das haftungsbegründende Ereignis herausgefordert worden ist.[20] In diesen Fällen ist trotz des Willensentschlusses des Verletzten zur schädigenden Handlung die Verantwortlichkeit des Auslösers der

[16] BGH NJW 1971, 1747; BAG Betr 1974, 2357.
[17] Teichmann in: Soergel, § 242 Rdnr. 287.
[18] Nachweise bei Heinrichs in: Palandt, § 242 Rdnr. 44.
[19] Heinrichs in: Palandt, vor § 259 Rdnr. 77.
[20] BGH, Urteil vom 13.9.1971, BGHZ 57, 25, 31; Urteil vom 29.10.1974, BGHZ 63, 189, 191 f.

Kausalkette weiterhin gegeben. Für eine Herausforderung zur schädigenden Handlung durch den Softwareproduzenten liegen keine Anhaltspunkte vor. Ein Anspruch des Raubkopierers selbst scheidet somit aus.

Dagegen unterbricht die Handlung eines Raubkopierers den Kausalzusammenhang nicht ohne weiteres, wenn ein Dritter ohne Kenntnis um die Gefahren eines Einsatzes der Raubkopie Schaden erleidet. Es widerspricht der Wertung des zivilrechtlichen Deliktsrechtes, den Erzeuger einer erheblichen Gefahrenquelle für die Rechtsposition anderer von der Haftung zu verschonen. Die mit Computerviren verseuchten Kopien bilden aber eine erhebliche Gefahr für das Eigentum Dritter. Das Typische der weiten Verbreitung von Raubkopien ist, dass ein Bezug zur Originalsoftware, insbesondere der Beschreibung mit der in ihr enthaltenen Warnung vor den Folgen der Erstellung einer Raubkopie nicht mehr besteht. Gerade bei kommerziell eingesetzten Computern kann häufig in größeren Unternehmen vom Nichtwissen des Eigentümers der Anlage um die Verwendung von Raubkopien ausgegangen werden.

Nach allem bleibt eine Verantwortung des Softwareherstellers, der das Verhalten des Verbreiters von Raubkopien wesentlich mitbestimmt hat. Er darf sich nicht darauf verlassen, dass sich der Raubkopierer von der Warnung hinsichtlich der Gefahren einer unautorisierten Kopie von deren Einsatz auf anderen Computeranlagen abhalten lassen.

Die haftungsbegründende Kausalität ist damit zu bejahen, so dass S dem A gegenüber – von der Sondersituation einmal abgesehen, dass dieser trotz Warnung Raubkopien zum Einsatz auf andern Anlagen anfertigt – haftet. Geschädigte Dritte können sich darüber hinaus, dessen Solvenz vorausgesetzt, natürlich auch am unmittelbaren Schädiger schadlos halten.

ab) Deliktische Ansprüche

Sofern A das infizierte Programm nicht unmittelbar von S sondern über einen Zwischenhändler erworben hat, scheiden vertragliche Ansprüche gegenüber S mangels vertraglicher Sonderverbindung von vornherein aus.

Schutzlos ist der Anwender aber auch in diesem Fall nicht, weil er auf sog. deliktische Anspruchsgrundlagen zurückgreifen kann. Hierunter versteht der Jurist all diejenigen gesetzlichen Bestimmungen, die Ansprüche auf Schadensersatz auch dann gewähren, wenn zwischen dem Geschädigten und dem Schädiger kein Vertragsverhältnis besteht. Schlage ich einem anderen die Fensterscheibe ein, hafte ich »aus Delikt«.

Ebenso verhält es sich bei der Infektion mit Computerviren. Nach § 823 Abs. 1 BGB, der zentralen Vorschrift im Bereich der deliktischen Anspruchsgrundlagen, haftet für den entstandenen Schaden, »wer vorsätzlich oder fahrlässig ... das Eigentum ... eines anderen widerrechtlich verletzt.« Objekt der Schadenswirkung können allerdings nur Sachen sein, da nur an solchen Ei-

gentumsrechte bestehen können. Unproblematisch ist dieses Erfordernis in Fällen von Hardwarezerstörungen durch das Wirken von Computerviren erfüllt, da hier die Sacheigenschaft eindeutig vorliegt. Fraglich ist eine Eigentumsverletzung dagegen, wenn die Virenroutine spätestens im Zeitpunkt der Ausführung des Aufgabenteils auf anderen Datenträgern des Verwenders (nur) die Funktionsuntauglichkeit der Programme bis hin zum Verlust von Daten herbeiführt. Bei der Frage nach der Sacheigenschaft von Programmen kann das Strafrecht Hilfestellung leisten. Auch der Tatbestand der Sachbeschädigung des § 303 StGB setzt den Eingriff auf eine Sache voraus. Danach sind Kräfte und Energien keine Sachen, wohl aber ihre Trägersubstanzen. Übertragen auf die Software und ihre Existenzabhängigkeit von ihrem jeweiligen Trägermedium (Diskette, Festplatte, Bandgerät oder Eprom) wird vertreten, dass der physikalische Zustand der Magnetisierung der jeweiligen Trägermedien auf die bestimmungsgemäße Brauchbarkeit keinen Einfluss nimmt.[21] Eine Diskette etwa ist auch nach der Zerstörung der auf ihr gespeicherten Informationen noch einsatzfähig. Auf der anderen Seite entscheidet allein der Eigentümer über die bestimmungsgemäße Brauchbarkeit einer Sache, er erst gibt der eingesetzten Diskette ihre neue Bestimmung. So wird in der Rechtsliteratur überwiegend eine Sachbeschädigung durch Löschen eines Tonbands bejaht.[22] Diese Wertung ist auf Software und gespeicherte Daten übertragbar.[23] Damit steht fest, dass S auch aus § 823 Abs. 1 BGB haftet, wenn dem A ein Schaden entsteht.

§ 823 Abs. 2 BGB erweitert die Schadensersatzpflicht auf schuldhafte Verletzungen eines sogenannten Schutzgesetzes. Dies ist ein Tatbestand vor allem des Strafrechts, der gerade dem Schutz des Verletzten dienen soll. Hier kommen insbesondere die §§ 303, 303a und 303b StGB in Betracht. Diese Vorschriften stellen die Sachbeschädigung und deren spezielle Ausformungen im Bereich der Computersabotage unter Strafe. § 303b schützt dabei das Interesse von Wirtschaft und Verwaltung am störungsfreien Ablauf ihrer Datenverarbeitung durch eine gegenüber dem allgemeinen Sachbeschädigungs-Tatbestand des § 303 StGB höhere Strafdrohung besonders. Die Norm umfasst in ihrer Tatbestandsalternative in Abs. 1 Nr. 2 auch die Manipulation eines Datenträgers durch die Veränderung seines Speicherzustandes. § 303b StGB ist dabei deshalb als Schutzgesetz im Sinne des § 823 Abs. 2 BGB zu werten, weil er eine besondere Ausprägung des Rechtsschutzes von Unternehmen darstellt.

Daneben kann der geschädigte Softwarekonsument möglicherweise Rechte aus § 826 BGB herleiten. Voraussetzung ist aber insbesondere, dass ein Verstoß gegen die guten Sitten nachgewiesen werden muss. Angesichts der erheblichen, teilweise existenzbedrohenden Einnah-

[21] Lampe, »Die strafrechtliche Behandlung der sogenannten Computer-Kriminalität«, GA 1975, 1, 16.
[22] Merkel, »Ist rechtswidriges Löschen von Tonbändern Sachbeschädigung?«, NJW 1956, 778; Schönke/Schröder, § 303 Rdnr. 8 b m.w.N.
[23] Rombach, CR 1990, 101, 104.

meverluste durch Raubkopien fällt es schwer, der Softwareindustrie einen solchen Verstoß zur Last zu legen. Im einzelnen sollte eine Differenzierung anhand der Aufgabenbestimmung des jeweiligen Virustyps vorgenommen werden. Beschränkt sich die Aufgabe des Virus auf die zeitweilige Lahmlegung der anderen Computeranlage, entfällt der Sittenwidrigkeitsvorwurf. Die Intensität erreicht nicht die Stärke, um die legitime Zielrichtung der Verfolgung eigener Interessen vollständig zu überlagern.[24] Die völlige Zerstörung fremder Datenbestände auf allen erreichbaren Datenträgern einer Computeranlage ist hingegen als sittenwidrige vorsätzliche Schädigung zu werten. Der Softwarehersteller, der sich dieses Abwehrmittels zur Verfolgung seiner Schutzinteressen bedient, ist sich bewusst, dass bei der Auslösung der Zerstörungsroutinen auf einer kommerziell verwendeten Computeranlage katastrophale Folgen verursacht werden können.

Im Ergebnis ist daher festzuhalten, dass der Softwarehersteller, der seine Produkte bewusst mit Viren versieht, für entstehende Schäden fast immer haftet. Ein solcher Softwareschutz ist, ganz abgesehen von der wenig werbewirksamen Wirkung einer solchen Aktion, nicht anzuraten.

b) Fahrlässige Infektion

Wie sieht es aber nun aus, wenn der Virus nicht (mehr oder minder) vorsätzlich, sondern lediglich fahrlässig verbreitet wurde? Hierzu ein weiteres Beispiel:

Dem Anwender A sind aufgrund eines Bedienerfehlers wichtige Programmdaten verlorengegangen. Weil vom Hersteller des Programms Ersatz nicht rasch genug herbeigeschafft werden kann, wendet er sich an das Softwarehaus S mit der Bitte, die verlorenen Programmteile zu restaurieren. Die Techniker des S kommen dieser Bitte nach, benutzen hierbei aber Disketten, die – ohne ihr und das Wissen des S – von einem Virus befallen sind. Dieser gelangt bei der Installation auf die Festplatte des Rechners des A und zerstört dort in der Folgezeit wichtige Daten. Es fragt sich, wie S in diesem Fall haftet.

Auch hier kommen vertragliche und deliktische Ansprüche in Betracht. Da die zivilrechtliche Haftung, anders als dies häufig im Strafrecht der Fall ist, grundsätzlich sowohl bei vorsätzlichem wie auch bei bloß fahrlässigem Verhalten eingreift, konzentriert sich die Fragestellung darauf, wann dem S ein solcher haftungsbegründender Fahrlässigkeitsvorwurf zu machen ist.

Das Gesetz definiert in § 276 Abs. 1 S. 2 BGB Fahrlässigkeit als die Außerachtlassung der »im Verkehr erforderlichen Sorgfalt«. Maßgeblich ist dabei kein individueller, sondern ein auf die allgemeinen Verkehrsbedürfnisse ausgerichteter objektiver Sorgfaltsmaßstab.[25] im Rechtsverkehr muss jeder darauf vertrauen dürfen, dass die anderen die für die Erfüllung ihrer Pflichten erforderlichen Fähigkeiten und Kenntnisse besitzen. Für S bedeutet dies, dass er sich nicht auf

[24] Rombach, CR 1990, 101, 105.
[25] Heinrichs in: Palandt, § 276 Rdnr. 15 m.w.N.

seine eigene Unkenntnis berufen kann. Dies gilt – jedenfalls im vertraglichen Bereich – auch, soweit er sich zur Erfüllung seiner Verbindlichkeiten, wie regelmäßig, der Mithilfe seiner Techniker bedient. Für deren Verschulden haftet er nach dem Gesetz wie für eigenes Fehlverhalten.

Welches ist aber nun der Haftungsmaßstab, den S konkret beachten muss, um einer Haftung für die Folgen eines Befalls mit Computerviren aus dem Weg zu gehen?

Nun, er muss all das tun, was ihm nach dem aktuellen Stand der Technik zur Vermeidung eines Virenbefalls möglich ist. An der Konkurrenz kann er sich dabei nicht unbedingt ausrichten. Soweit diese schlampig arbeitet, gibt ihm das noch keinen Freibrief, ebenso zu verfahren. Etwa eingerissene Verkehrsunsitten und Nachlässigkeiten bei der Handhabung möglicherweise virenverseuchter Datenträger entschuldigen ihn nämlich ebenso wenig wie das Bestehen eines »verbreiteten Brauchs«.[26]

Maßstab ist damit die größtmögliche Sorgfalt: Bis zur Grenze des wirtschaftlich Zumutbaren muss der S alles tun, um einen Virenbefall zu verhindern. Schon aus lizenzrechtlichen Gründen wird er daher grundsätzlich nur die beim Anwender – hoffentlich – vorhandenen schreibgeschützten Originaldisketten benutzen. Bei Großkunden ist zudem denkbar, dass das betreuende Softwarehaus Sicherungskopien jeder installierten Originaldiskette in den eigenen Geschäftsräumen aufbewahrt. Wirtschaftlich unvertretbar und damit unzumutbar dürfte es dagegen sein, grundsätzlich von jedem installierten Programm eine ungeöffnete Originalversion für den Notfall bereitzuhalten.

Nur wenn die Originaldisketten bzw. hiervon unmittelbar hergestellte Sicherungskopien nicht verfügbar sind, darf S ausnahmsweise auf eigene Sicherungsdisketten aus anderen Quellen zurückgreifen. Dabei sollte er peinlichst darauf achten, dass die benutzten Datenträger nach jedem Einsatz von den übrigen Disketten getrennt werden und auf Virenbefall hin gescannt werden. Am Rande sei in diesem Zusammenhang darauf hingewiesen, dass auch das regelmäßige Überprüfen der Programme auf ihre Länge hin nicht letzte Sicherheit bietet, obwohl dies immer wieder empfohlen wird. Es sind inzwischen Viren bekannt, die dem Anwender durch entsprechende Änderung im File Allocation Table, also im Inhaltsverzeichnis, eine falsche Länge der Programme vortäuschen.

Bei der Installation selbst sollte es selbstverständlich sein, dass nur mit Schreibschutz auf den Quelldisketten gearbeitet werden, soweit das Programm dies zulässt. Auf diese Weise wird vermieden, dass die Einrichtungsdisketten ihrerseits von verseuchten Festplatten infiziert werden und bei späteren Installationen den Virus weitertragen.

[26] Heinrichs in: Palandt, § 276 Anm. 4 B b.

Als Arbeitgeber wird S endlich mit Stichproben darauf achten, dass die Sicherheitsanforderungen tatsächlich beachtet werden. Bei solchen Routinekontrollen entdeckte Sicherungskopien ohne Schreibschutz sollten – auch aus erzieherischen Gründen – ausnahmslos gelöscht werden. Beachtet S diese Anforderungen, minimiert er das Risiko einer von ihm verursachten Infektion. Ein Haftungsvorwurf kann ihm dann nicht gemacht werden.

V. Praktische Konsequenzen

Welche praktischen Konsequenzen sind nun aus so viel juristischer Theorie zu ziehen?

Leider obliegt es regelmäßig dem Geschädigten, nicht nur den Schaden nachzuweisen, den er durch Computerviren erlitten hat, sondern auch den Beweis für die Urheberschaft des Viren-Einbringers an seinem Schaden zu erbringen. Die Beweislage ist dabei gerade hier, wo verdeckt operierende Programme im Spiel sind, oft sehr schwierig. Hinzu kommt das Problem, dass häufig zwar der Geschädigte und erst recht der Beklagte, nicht aber immer der Richter hinreichend sachkundig ist, diese Vorgänge richtig zu beurteilen. Selten kann daher der Viren-Programmierer überhaupt benannt, geschweige denn belangt werden.

Selbst wenn man aber Personen benennen kann, die für die Virus-Infektion verantwortlich zu machen sind, so bieten heutige PC-Systeme praktisch keine Informationen, mit denen der Ablauf und die Umstände einer Infektion belegt werden können. Beweisträger, also die infizierten Programme selbst, sollte man daher auf keinen Fall löschen, bevor sie nicht zu Beweiszwecken gesichert wurden. Ansonsten wird der Geschädigte häufig auf Geständnisse oder auf den Zufall angewiesen sein.

Schwierig ist es auch, den Schaden hinreichend präzise und schlüssig zu belegen und zu bewerten. Wer kann schon den Nutzen der verseuchten Daten, den Zeitverlust, den Ärger im Personalbereich substantiiert in Zahlen umsetzen?

Schließlich ist das Interesse des Betroffenen an einer öffentlichen Verfolgung oft begrenzt, sei es wegen eines befürchteten Rufschadens oder weil dabei rechtlich relevante Faktoren zum eigenen Nachteil (etwa illegale Programmnutzung) zur Sprache kommen würden oder weil man sonst wie mitschuldig an dem Vorfall sein könnte.

Selbst wenn die Fakten eines Virus-Vorfalls einwandfrei festgestellt und »gerichtsverwertbar« belegt sind, ist damit nach heutiger Rechtslage ein Gerichtsverfahren wenig aussichtsreich.

Nicht unerheblich ist zudem der Kostenfaktor beim gerichtlichen Verfahren. Hat man das Glück, einen vorsätzlich handelnden mutmaßlichen »Anstecker« dingfest machen zu können, sollte man sich deshalb nicht scheuen, zunächst den Ausgang eines etwaigen Strafverfahrens abzuwarten. Der Vorteil einer solchen Verfahrensweise besteht darin, ohne eigenes Kostenrisiko

abklären lassen zu können, ob der Beschuldigte als Urheber für den erlittenen Schadens verantwortlich ist. Die Entscheidung des Strafrichters ist für den Richter im späteren Zivilrechtsstreit zur Durchsetzung des Schadensersatzanspruchs zwar nicht verbindlich. Durchaus denkbar ist, dass dieser im Zivilprozess hinsichtlich der Verursachung des Schadens zu einem gänzlich anderen Urteil gelangt als sein Kollege in der strafrechtlichen Abteilung. Es ist aber ein offenes Geheimnis, dass er sich regelmäßig der Ansicht des Strafrichters anschließen wird. Dies machen sich seit langem die Geschädigten bei Verkehrsunfällen zu Nutze, die zunächst den Ausgang des Strafverfahrens abwarten, um dann mit ihren eigenen Forderungen nachzuhaken.

Der Inhaber S des Softwarehauses aus unseren Beispielsfällen schließlich kann versuchen, durch geschickte Vertragsgestaltung seine Haftung angemessen auf Fälle grober Fahrlässigkeit zu beschränken. Dies bedeutet, dass er nur dann haftet, wenn seine Techniker die notwendige Sorgfalt in besonders schwerem Maße außer Acht lassen, also das nicht beachten, was jedem auch nur halbwegs sorgfältigen Zeitgenossen als notwendig eingeleuchtet hätte. Einen formularmäßiger Haftungsausschluss in Allgemeinen Geschäftsbedingungen auch für grob fahrlässiges Verhalten lässt dagegen das Gesetz zur Regelung des Rechts der Allgemeinen Geschäftsbedingungen nicht zu.

Ich hoffe, Ihnen mit meinem kurzen Vortrag einen kleinen Eindruck davon verschafft zu haben, welchen Fragestellungen sich der Jurist, aber auch der Geschädigte, ausgesetzt sieht, wenn Viren ihr zerstörerisches Werk getan haben. Einen Rat möchte ich Ihnen und jedem, der sich mit Computerviren beschäftigt, deshalb noch auf den Weg geben. Er stammt von Steffen Wernery, dem Pressesprecher des Chaos Computer Club in Hamburg, der 1987 mahnte:[27]

> *»Wer mit Viren experimentiert, sollte sich der rechtlichen Konsequenzen bewusst sein. Nicht nur der höfliche, sondern auch der vorsichtige Mensch behält seine Viren daher vielleicht besser für sich.«*

Dem ist nichts hinzuzufügen. Ich danke Ihnen für Ihre Aufmerksamkeit!

Wichtige gesetzliche Bestimmungen

A. Zivilrecht

§ 276 BGB. Haftung für eigenes Verschulden

(1) Der Schuldner hat, sofern nicht ein anderes bestimmt ist, Vorsatz und Fahrlässigkeit zu vertreten. Fahrlässig handelt, wer die im Verkehr erforderliche Sorgfalt außer acht lässt. (...)

[27] In einem Bericht über den Chaos Communication Congress 1987 - PC-Virenforum - in der »Datenschleuder«, dem »wissenschaftlichen Fachmagazin für Datenreisende«, Heft Nr. 18, Februar 1987.

(2) Die Haftung wegen Vorsatzes kann dem Schuldner nicht im Voraus erlassen werden.

§ 823 BGB. Schadensersatzpflicht

(1) Wer vorsätzlich oder fahrlässig das Leben, den Körper, die Gesundheit, die Freiheit, das Eigentum oder ein sonstiges Recht eines anderen widerrechtlich verletzt, ist dem anderen zum Ersätze des daraus entstehenden Schadens verpflichtet.

(2) Die gleiche Verpflichtung trifft denjenigen, welcher gegen ein den Schutz eines anderen bezweckendes Gesetz verstößt. (...)

§ 826 BGB. Sittenwidrige vorsätzliche Schädigung

Wer in einer gegen die guten Sitten verstoßenden Weise einem anderen vorsätzlich Schaden zufügt, ist dem anderen zum Ersätze des Schadens verpflichtet.

B. Strafrecht

§ 202 a StGB. Ausspähen von Daten

(1) Wer unbefugt Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, sich oder einem anderen verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

§ 303 a StGB. Datenveränderung

(1) Wer rechtswidrig Daten (§ 202 a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

§ 303 b StGB. Computersabotage

(1) Wer eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, dadurch stört, dass er

1. eine Tat nach § 303 a Abs. 1 begeht oder
2. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert,

wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) der Versuch ist strafbar.

§ 303 c StGB. Strafantrag

In den Fällen der §§ 303 bis 303 b wird die Tat nur auf Antrag verfolgt, es sei denn, dass die Strafverfolgungsbehörde ein Einschreiten von Amts wegen für geboten hält.

§ 53 Abs. 4 UrhG. Vervielfältigung zum privaten Gebrauch

(4) Die Vervielfältigung

a) graphischer Aufzeichnungen von Werken der Musik,

b) eines Buches oder einer Zeitschrift, wenn es sich um eine im wesentlichen vollständige Vervielfältigung handelt,

ist, soweit sie nicht durch Abschreiben vorgenommen wird, stets nur mit Einwilligung des Berechtigten zulässig oder (...) zum eigenen Gebrauch, wenn es sich um ein seit mindestens seit zwei Jahren vergriffenes Werk handelt. Ebenso ist die Vervielfältigung eines Programms für die Datenverarbeitung (...) oder wesentlicher Teile davon stets nur mit Einwilligung des Berechtigten zulässig.