Zur Strafbarkeit des sog. Computerhackens – Die Problematik des Tatbestandsmerkmals „Verschaffen" in § 202a StGB

Peter-Helge Hauptmann, Hannover

1. Überblick

Die Taten sog. Computerhacker haben in jüngster Zeit großes Aufsehen erregt. Hacker sind u.a. in die Computer wichtiger Institutionen eingedrungen um die dort erlangten Informationen an ausländische Geheimdienste weiter zu geben.[1] Es stellt sich die Frage nach der Legitimität solcher Handlungen, also nach der Strafbarkeit des Hackens.

Zum 01.08.1986 wurde, im Rahmen des zweiten Gesetzes zur Bekämpfung der Wirtschaftskriminalität (2. WiKG), mit dem § 202a StGB (Ausspähen von Daten) eine entsprechende Norm geschaffen. Der Deutsche Bundestag wollte mit dem § 202a StGB alle als Daten dargestellten Informationen in umfassender Weise strafrechtlich gegen Spionage schützen.[2] Die damals schon vorhandenen Normen gewährten nur in Teilbereichen strafrechtlichen Schutz gegen Datenspionage. § 41 des Bundesdatenschutzgesetzes (BDSG) bezieht sich nur auf personenbezogene Daten. Auch ist der Schutzzweck ein anderer; § 41 BDSG dient dem Datenschutz unter dem Gesichtspunkt des Schutzes der Intimsphäre des einzelnen, des Betroffenen und nicht der datenspeichernden Institution.[3] § 17 II Nr. 1 UWG schützt nur materielle Geschäfts- und Betriebsgeheimnisse, soweit diese nicht besonders gesichert sind.[4] Der strafrechtliche Schutz des § 202 III StGB (Briefgeheimnis) bezieht sich zwar auf alle zur Informationsübermittlung bestimmte Träger, so auch auf Magnetbänder, Disketten und Tonbandkassetten, jedoch nur, wenn diese als solche zur Kenntnis genommen werden, etwa durch Entwendung und Abspielung in einem geeigneten Gerät. Daten im Übermittlungsstadium, die etwa durch Anzapfen oder Abhören einer Datenübertragungsleitung beschafft werden, sind somit durch den § 202 III StGB nicht geschützt.[5]

Die gleichzeitig durch das 2. WiKG geschaffenen Normen §§ 303a, 303b StGB befassen sich auch mit Computerkriminalität. Sie ergänzen den Schutzbereich des § 202a StGB in bezug auf Eingriffe in EDV-Anlagen, die zu Störungen des Betriebsablaufes führen. § 303a StGB stellt die rechtswidrige Datenveränderung unter Strafe. Die Vorschrift soll das Interesse an der unversehrten Verwendbarkeit von Daten schützen.[6] § 303b StGB (Computersabotage) schützt die Funktionstüchtigkeit von EDV-Anlagen.[7]

2. Untersuchung des Begriffsfeldes „Hacken"

Es stellt sich vor einer Untersuchung der Strafbarkeit des Hackens gem. § 202a StGB die Frage nach einer konkreten Definition des Begriffs. Zwar wird der Begriff in fast allen Veröffentlichungen über das 2. WiKG[8] und sogar vom Rechtsausschuß des Bundestages[9] benutzt, eine zufriedenstellende Erläuterung wird allerdings nicht angegeben. Sie ist notwendig, da dieser neu geprägte Begriff bis heute nicht ins allgemeine deutsche Sprachgut übernommen wurde, er somit jedem etwas anderes bedeutet, was die Gefahr von weitreichenden Mißverständnissen birgt. Das Wort „Hacker" beschreibt – um das zusammenzufassen, was weithin bekannt ist – den Computerspezialisten, der heimlich, auf elektronischen Wegen, etwa über Datenverbundnetze, in ihm fremde EDV-Anlagen eindringt. Im Augenblick des Eindringens ruft der Hacker schon Daten der Anlage auf seinem Bildschirm auf.[10] Dies läßt sich nicht verhindern, da der Hacker nur mit den Daten auf seinem Bildschirm kontrollieren kann, ob das Eindringen auch tatsächlich gelungen ist. Der Hacker will feststellen, wie weit er in die EDV-Anlage eingedrungen ist und versuchen, durch neues Hacken, tiefer in das System einzudringen. Oft hinterlassen Hacker, nachdem das Eindringen in das System gelungen ist, einen die Benutzung der EDV-Anlage nicht oder fast nicht beeinträchtigenden Hinweis an den offiziellen Benutzer, der ihn auf den Softwarefehler (den vom Hacker gefundenen Weg in die Anlage) hinweist.[11] Dies ist jedoch nicht dem Hacken zuzuordnen. Es ist vielmehr eine darüberhinausgehende Handlung, gedacht als „Service" für den Betreiber.

Die technische Realisierung dieser Handlungen ist für eine Abgrenzung von Bedeutung. Nur durch die Untersuchung der tatsächlich vorgenommenen Handlungen lassen sich konkrete Aussagen über das Hacken machen. Beim Hacken ist die technische Realisierung in einer fortlaufenden Entwicklung begriffen und eine beschränkte Betrachtung unter dem heutigen Stand der Technik wird schon bald überholt sein. Derzeit sind sog. „Trojanische Pferde"[12] der Stand der Technik in der Problematik der Datensicherung und ihrer Umgehung. Die ersten in Computern eingesetzten Sicherungen bestanden in der Vergabe von Paßwörtern.[13] Der Benutzer mußte sich mit einem meist acht Buchstaben langen Codewort als berechtigt ausweisen. Durch das nächtelange Ausprobieren[14] aller theoretisch

1 Mit weiteren Fällen: Wirtschaftswoche, 10/1989, S. 48ff; Michael Birnbaum, Gefangen in der kalifornischen Sonne, Süddeutsche Zeitung 4.3.1989, S. 3; DER SPIEGEL, 10/1989, S. 122ff.

2 Bundestagsdrucksache, 10/5058, S. 28 (28).

3 Vgl. Lenckner/Winkelbauer, Computerkriminalität – Möglichkeiten und Grenzen des 2. WiKG, CR 1986, S. 483 (483).

4 Bundestagsdrucksache, a.a.O., S. 29; Granderath, Das zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität, DB 1986, Beilage Nr. 18, S. 1 (1); Leicht, Computerspionage – Die „besondere Sicherung gegen Zugang" (§ 202a StGB), IuR 1987, S. 45 (45).

5 Bundestagsdrucksache, a.a.O., S. 28; Granderrath, a.a.O., S. 1; Haft, Das zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. WiKG), NStZ 1987, S. 6 (9).

6 Möhrenschlager, Das neue Computerstrafrecht, Wistra 1986, S. 128 (141).

7 Möhrenschlager, a.a.O., S. 142.

8 statt vieler: Haft, a.a.O., S. 9.

9 Bundestagsdrucksachen. a.a.O., S. 28

10 Diese Tatsache wird auch von Lenckner/Winkelbauer, a.a.O., S. 488, festgestellt.

11 Vgl. DER SPIEGEL, a.a.O.

12 Der Begriff wurde in Anlehnung an eine alte Sage Homers gewählt, wonach die Einwohner der Stadt Troja, nach einer langen Belagerung durch die Griechen, ein Geschenk dieser, ein großes hötzernes Pferd, in die Stadt holten. Im Pferd sollen sich sieben Männer versteckt gehalten haben, die dann im Schutze der Nacht von innen die Stadttore öffneten und damit den Griechen die Gelegenheit zum Sieg über Troja gaben.

13 Vgl. Leicht, a.a.O., S. 50.

14 Aufgrund dieses stundenlangen Herumhackens auf der Tastatur des Computers hat sich der Begriff „Hacker" herausgebildet.

möglichen Paßwortkonstellationen, bis zum Erfolg, wurden diese Sperren schnell überwunden. Später übernahmen Computer selbst das Ausprobieren aller denkbaren Codewörter und erleichterten so die Arbeit der Hacker. Ein Eindringen auf diesem Wege wurde durch den Einbau einer Zeitsperre verbaut. Wer nicht innerhalb von z. B. einer Minute das richtige Paßwort eingegeben hat, wird automatisch aus dem EDV-System verwiesen. Auch diese Sicherungen wurden durch geeignete Wege zur Findung des richtigen Paßwortes umgangen.[15] Als Zwischenergebnis ist festzustellen, daß bei den beschriebenen Wegen der Datenbestand bis zum Zeitpunkt des Eindringens nicht verändert wurde. Erst später, zur Benachrichtigung des offiziellen Benutzers, wurde der Datenbestand leicht erweitert, also verändert.

An dem Grundprinzip, der Vergabe eines Code- oder Paßwortes hat sich bis heute nichts geändert, jedoch an den Wegen der Hacker, sich diese zu beschaffen. Die aktuelle Methode der Hacker, an Paßwörter fremder EDV-Systeme zu gelangen, besteht in der Einbringung von sog. Trojanischen Pferden. Bei wichtigen und komplizierten EDV-Systemen, wie etwa die Computer von NASA und anderen wissenschaftlichen Instituten, bestehen immer einige Datenbibliotheken (Dateien), die für die Allgemeinheit, also für Gäste, abrufbar sind. Solche Bibliotheken sind allgemein üblich und dienen dem Fortschritt der Wissenschaft. Zunächst erfolgt der Rechnerzugang des Hackers unter der Eintragung als Gast in eine der öffentlichen Dateien. Dort installiert der Hacker ein Trojanisches Pferd. Es wird von den anderen Benutzern nicht bemerkt. Dieses Programm kommuniziert mit allen nachfolgenden Benutzern der Bibliothek in gleicher Weise. Es untersucht die Daten des Benutzers nach seinem Paßwort und speichert dies. Da die nachfolgenden Benutzer oft keine Gäste sind, sondern bedeutende Zugriffsberechtigungen haben, gelangt das Trojanische Pferd schnell in den Besitz von wichtigen Paßwörtern. Diese braucht der Hacker nur auf geeignete Weise abzufragen. Er hat sich somit alle Zugriffsberechtigungen verschafft. Dabei ist es unwichtig, ob er selbst vormals das Trojanische Pferd installiert hatte, oder ob ihm nur der Schlüssel zur Öffnung des Pferdes bekannt war.[16] Das Installieren von Trojanischen Pferden ist also nicht die Hackerhandlung, sondern das Finden, Ausnutzen und Aufdecken solcher.
Ist der Hacker erst einmal im EDV-System, so stehen ihm alle Möglichkeiten offen. Er kann das gesamte System, einzelne Dateien und Daten löschen, er kann Daten manipulieren, er kann Mitarbeiter von der Benutzung aussperren, er kann, falls dies im System vorgesehen ist, sich oder anderen Geldbeträge überweisen. Er hat sogar die Möglichkeit, sich das gesamte System oder interessante Einzelheiten zu kopieren. Diese Tätigkeiten haben jedoch mit dem Hacken nichts mehr zu tun.
An dieser Stelle läßt sich nun unter Bezug auf das oben Dargestellte eine geeignete Definition für den Begriff „Hacken" festlegen. Da die Handlungen mit der größeren kriminellen Energie auszugrenzen sind, aber andererseits auf die technischen Notwendigkeiten Rücksicht zu nehmen ist, kommt folgende Definition in Betracht:

Hacken ist zu verstehen als

- Eindringen in fremde Computernetze (oder in höhere, nicht für Gäste zugelassene Ebenen eines EDV-Systems)

und

- Ansehen der dort gespeicherten Programme, Dateien und Daten durch Aufruf auf dem Bildschirm des Handelnden.

Nicht umfaßt ist also das Hinterlassen einer Nachricht an den offiziellen Benutzer sowie das Installieren von Trojanischen Pferden oder ähnliche Handlungen, da diese zu einer erweiternden Veränderung des Datenbestandes führen, mit z.T. unübersehbaren Folgen, wie etwa der Möglichkeit für viele, in das System einzudringen. Hacken läßt sich also als unberechtigtes Eindringen und Umsehen in EDV-Systemen definieren.

3. Die Problematik des Tatbestandsmerkmals „verschaffen" (§ 202a StGB)

Da, wie dargestellt, durch Hacken weder Daten verändert noch sabotiert werden, somit weder eine Strafbarkeit nach § 303a noch § 303b StGB vorliegt, und für eine Strafbarkeit nach anderen Gesetzen wie etwa dem Fernmeldegesetz oder dem UWG beim Regelfall des Hackens keine konkreten Anhaltspunkte vorliegen, ist § 202a StGB (Ausspähen von Daten) die entscheidende Strafbarkeitsnorm.

Für die Frage der Strafbarkeit des Hackens ist das Tatbestandsmerkmal „Verschaffen" von hervorzuhebender Bedeutung. Die weiteren Tatbestandsmerkmale liegen in der Regel unzweifelhaft vor. Der Geheimnischarakter der Daten ist im Normalfall vorhanden, genauso wie die Daten nicht für den Hacker bestimmt sind. Die Tatsache, daß die Daten gegen unberechtigten Zugang besonders gesichert waren, ist wohl vorauszusetzen, wenn der Zugang nur mit besonderen datentechnischen Methoden möglich war.[17] [18]

Es stellt sich also die Frage, ob der Hacker sich regelmäßig Daten im Sinne des § 202a StGB verschafft. Der Ausdruck „Verschafft" wird im StGB noch an einer weiteren Stelle, im § 96 StGB (Landesverräterische Ausspähung), im Zusammenhang mit Informationen benutzt. Körperliche Gegenständen verschafft sich der Täter, indem er sie in Gewahrsam nimmt (ohne Kenntnis zu erlangen).[19] In allen übrigen Fällen dadurch, daß er Kenntnis erlangt. Da Daten keine körperlichen Gegenstände sind, lassen sie sich nicht in Gewahrsam nehmen. Wollte man den Begriff in beiden Normen gleich anwenden, so ist also auf die Kenntnis abzustellen. Dies ist jedoch problematisch. Da Daten sich beliebig kopieren lassen, könnte ein Täter sich ein geschütztes Computerprogramm kopieren, es sich aber nicht ansehen. Er hätte es somit zwar zur Verfügung, jedoch hätte er keine Kenntnis vom Inhalt. Auch diese Konstellation sollte jedoch - so die Ansicht des Rechtsausschusses - vom Tatbestandsmerkmal „Verschaffen" umfaßt werden. Im Rechtsausschuß wurde daher versucht eine datenbezogene Auslegung zu erschaffen.[20]

15 Mehr über die technische Realisierung der Datensicherungsmethoden bei Leicht, a.a.O., S. 47ff.
16 Sehr genaue Erklärungen über die sog. Trojanischen Pferde finden sich bei Bernau/Vogler, Trojanische Pferde im Computer-Netz, CHIP, 2/1988, S. 32ff.
17 Vgl. die ausführliche Diskussion zur Frage der besonderen Sicherung bei Leicht, a.a.O., S. 45.
18 Eine ausführliche Diskussion aller Tatbestandsmerkmale findet sich bei Lenckner/Winkelbauer, a.a.O., S 483f.
19 Lackner, Kommentar zum Strafgesetzbuch, 17. Auflage, München 1987, § 96, Nr 2.
20 Bundestagsdrucksachen, a.a.O., S. 28.

Es wurde daher die Auffassung vertreten, daß in den Fällen, in denen sich der Täter nicht mit dem unbefugten Zugang begnügt, sondern darüber hinaus Daten abruft, eine Strafbarkeit gem. § 202a StGB vorliegen soll.[21] Ein Täter, der in EDV-Systeme nicht nur eindringt, sondern auch Daten abruft, verschafft sich demnach diese Daten. Auch eine breite Meinung in der Literatur ist dieser Ansicht gefolgt. So soll das bloße Eindringen in einen Datenspeicher oder Datenübermittlungsvorgang nicht zur Strafbarkeit ausreichen. Ein bloßes Wahrnehmen der Daten soll andererseits schon zur Strafbarkeit führen.[22]

Diese Ansicht führt jedoch zu Problemen. In der durchgeführten Untersuchung wurde dargestellt, daß das normale Hacken grundsätzlich aus Eindringen und Aufrufen der Daten besteht. Eine Trennung der beiden Handlungen ist technisch nicht möglich. Mit dem Eindringen nimmt der Hacker automatisch die ersten Daten auf seinem Bildschirm war. Das vom Gesetzgeber geförderte Begnügen „mit dem unbefugten Zugang"[23] ist also technisch nicht realisierbar. Es ist also festzustellen, daß das normale Hacken durch diese Auffassung, nur das bloße Eindringen sei straffrei und jede Form des Aufrufens von Daten sei ein „sich verschaffen" im Sinne des § 202a StGB, strafbar wird.[24] Dies war vom Gesetzgeber jedoch nicht gewollt, „sog. „Hacker" ... sollen von Strafen verschont bleiben"[25]. Auch die oben dargestellte Literatur vertritt die Ansicht, daß das einfache Hacken nicht gem. § 202a StGB strafbar sei.[26]

Die Tatsachen und der Wunsch des Gesetzgebers und der ihm folgenden Literatur fallen demnach auseinander. Der Wille, das Hacken nicht unter Strafe zu stellen, ist in der Ausformulierung des Gesetzes und der Beratungen nicht verwirklicht worden.[27] Möglicherweise hat also die Unwissenheit darüber, daß das Eindringen in Computersysteme und das Aufrufen derselben in einem Schritt geschieht, dazu geführt, daß eine wirklichkeitsfremde Auffassung den Beratungen zugrundegelegt wurde.

4. Überlegungen zu einer neuen Auslegung des Tatbestandsmerkmals „verschaffen"

Es stellt sich an dieser Stelle die Frage, ob dem ursprünglichen Willen des Bundestages, den Hacker straffrei zu lassen, nicht doch gefolgt werden soll. Sollte nicht besser die Anpassung des Tatbestandsmerkmals „Verschaffen" an die technische Realität zur Vermeidung einer ursprünglich nicht erwünschten Strafbarkeit führen?[28]

Der Rechtsausschuß des Bundestages zur Beratung des 2. WiKG wollte, entgegen der Anregung der Bundesregierung, davon absehen, den bloßen unberechtigten Zugang unter Strafe zu stellen. Der Gefahr einer Überkriminalisierung sollte damit vorgebeugt werden. Für eine Kriminalisierung des bloßen Eindringens wurde kein strafwürdiges Verhalten entdeckt. Zwar werde mit dem erfolgreichen Eindringen in fremde Datenbanken das Integritätsinteresse von Betreibern und Benutzern gefährdet. Ein solches Verhalten stelle jedoch eine so geringe Gefährdung dar, daß sie als Ansatzpunkt für einen neuen Straftatbestand nicht ausreiche.[29] Durch die Kriminalisierung einer oft vorgenommenen vormals legalen Handlung, wie hier das Hacken, werden Täter in den Untergrund gedrängt. Handlungen, die vorher in aller Öffentlichkeit vorgenommen und diskutiert wurden, werden im Geheimen und ohne die notwendige Diskussion über Sinn und Zweck vorgenommen. Dies ist hinlänglich aus dem Problemkreis des Schwangerschaftsabbruchs bekannt. Die Hacker geraten so in einen Computeruntergrund. Die Verbreitung der Erkenntnisse und Erfahrungen der Hacker in der Öffentlichkeit wird unterbunden. Sie können nicht mehr in den gesellschaftlichen Entwicklungsprozeß einfließen. Dies hätte unerwünschte Folgen. Da die Informationen über Softwarefehler (Eindringungsmöglichkeiten in wichtige Computernetze) nicht mehr allgemein bekannt werden würden, sondern nur im Geheimen - immer unter der Angst der Strafandrohung - weitergereicht würden, gelängen diese nicht an den Betreiber, der sie schnell abstellen könnte. Die Softwarefehler werden auf diese Weise, sozusagen als Geheimwissen, einer immer größer werdenden Zahl von Menschen bekannt. Es wächst die Gefahr, daß das Wissen zur Datenveränderung oder sogar zur Datenspionage benutzt wird. Den schwerwiegenden Computerstraftaten, etwa gem. § 303a oder § 303b StGB wird somit durch die Abdrängung der Hacker in den Computeruntergrund Vorschub geleistet.

Um den ursprünglichen Wunsch der Bundesregierung nach der Straffreiheit des Hackens zu entsprechen, ist es, wie oben dargestellt, notwendig, eine andere Auslegung des Tatbestandsmerkmals „Verschaffen" zu wählen. Eine Auslegung, die der technischen Realisation des Hackens entspricht und somit auch tatsächlich geeignet ist, die negativen Auswirkungen der Abdrängung in den Untergrund abzuwenden.

Es wird daher vorgeschlagen, daß als „Verschaffen" im Sinne von § 202a StGB ein Verhalten anzusehen ist, bei dem der Täter außer das er sich Zugang zu den Daten bewirkt, diese a u c h auf einen Datenträger überträgt.[30] Die Folge der Strafbarkeit gem. § 202a StGB soll also erst eintreten, wenn der Täter in ein Computersystem eindringt, und, unabhängig davon ob er sich umsieht, Daten, also Programme oder Dateien, auf ein eigenes Medium abspeichert. Zum Eindringen soll noch zusätzlich das Abspeichern zum Ausfüllen des Tatbestandsmerkmals notwendig werden. Dies ist technisch durchaus realisierbar. Das Abspeichern von Daten ist ein gesonderter Schritt, auf den beim Hacken verzichtet werden kann. Nachdem der Täter in ein Computersystem eingedrungen ist, erscheinen, wie dargestellt, die ersten Daten auf dem Bildschirm des Täters. Er ruft die Daten also auf seinen Bildschirm und sieht sie sich an. Nachdem er neue Daten aufgerufen hat, etwa eine neue Datei, sind die alten Daten nicht mehr im Computer des Täters vorhanden. Damit er diese behält, muß er sie etwa auf einer Diskette oder auf einem anderen geeigneten Medium abspeichern.

21 Bundestagsdrucksachen, a.a.O., S. 29.
22 Systematischer Kommentar-Samson, 21. Lieferung, Frankfurt 1987, § 202a, RN 11; Dreher-Tröndle, Kommentar zum Strafgesetzbuch, 44. Auflage, München 1988, § 202a, RN 2; Lackner, a.a.O., Nr. 4; Lenkner/Winkelbauer, a.a.O., S. 488; Granderath, a.a.O., S. 2
23 Bundestagsdrucksachen, a.a.O., S. 29.
24 so Bühler, Ein Versuch, Computerkriminellen das Handwerk zu legen, MDR 1987, S. 448 (453).
25 Bundestagsdrucksachen, a.a.O., S. 28
26 Siehe Fußnote 22.
27 Zur gleichen Schlußfolgerung kommt Tiedemann, Die Bekämpfung der Wirtschaftskriminalität durch den Gesetzgeber, JZ 1986, S. 866 (868).
28 Auch Tiedemann, a.a.O., S. 868, und Bühler, a.a.O., S. 453, forderen eine Klärung bzw. die Klarstellung des Begriffs „Verschaffen".
29 Bundestagsdrucksachen, a.a.O., S. 28f
30 Ähnlich Haft, a.a.O., S. 10, jedoch ohne Begründung.

Auf eine solche Tätigkeit kann der Hacker sehr wohl verzichten. Da er nur ein Interesse an dem Aufbau und nicht an den konkreten Daten hat, braucht er die im fremden Computersystem gefundenen Daten nicht zu speichern. Solange er die gefundenen Daten nicht nutzen will, macht es für ihn keinen Sinn, diese abzuspeichern und teuere Speicherplätze dafür aufzuwenden. Es kann also gefordert werden, daß der Hacker, um straffrei zu bleiben, auf ein Abspeichern der gefundenen Daten verzichtet.

5. Schlußbetrachtung

Damit läßt sich zusammenfassend feststellen, daß die hier vorgeschlagene Auslegung, das Tatbestandsmerkmal „Verschaffen" des § 202a StGB bestehe aus dem Eindringen u n d dem Abspeichern von Daten, der von weiten Teilen der Literatur und des Rechtsausschusses aus guten Gründen gewünschten Straffreiheit des Hackens Rechnung trägt, ohne dabei jedoch das Ausspähen von Daten ausufernd straffrei zu lassen. Sie sollte deshalb zur Anwendung gelangen.

Das Epos von Silicon und die Barden des Binären

Zur Bestimmung der korrekten Reichweite des urheberrechtlichen Schutzes für Computer-Programme

Anthony L. Clapes/Patrick Lynch/Mark R. Steinberg *

Vorbemerkung

Einer der bemerkenswertesten Beiträge, den ein Meister auf dem Gebiet des Rechts leisten kann, besteht darin, das Recht mit Verstand so ruhig wie möglich durch die oft rauhen Gewässer des sozialen Wandels zu steuern. Auf dem Gebiet des Urheberrechts sind in den letzten Jahren die rauhesten Gewässer diejenigen gewesen, in denen die See ihr Verhalten in Abhängigkeit von der Verfügbarkeit neuer Technologie geändert hat. Vervielfältigungstechnik, Audio- und Videotapes und Computersoftware haben das Urheberrecht vor ernste Herausforderungen gestellt, indem sie neue Aktivitäten erleichterten (in manchen Fällen sogar dazu ermutigten), die mit den Ausschließlichkeitsrechten des Urheberrechtsinhabers unvereinbar sind.

Mel Nimmer hat in vielen Fällen seine besondere Erfahrung nutzbar gemacht und so geholfen, die Entwicklung des amerikanischen Urheberrechts durch solche rauhen Gewässer zu steuern. Er arbeitete als stellvertretender Vorsitzender der nationalen Kommission für neue technische Formen der Nutzung urheberrechtsgeschützter Werke (National Commission on New Technological Uses of Copyrighted Works - „CONTU"). Diese Kommission war von Präsident Ford eingesetzt worden um zu prüfen, welche Änderungen gegebenenfalls im Urheberrecht angezeigt seien, um die Folgerungen aus der breiten Verfügbarkeit dieser neuen Technologien zu ziehen. Durch seine Arbeit in der Kommission spielte er eine wichtige Rolle bei der Ausarbeitung der Ergänzungen des Jahres 1980 zum Urheberrechtsgesetz. Dadurch, daß er seine maßgebliche Abhandlung nicht nur um Zusammenfassungen und Synthesen von Fällen ergänzte, die sich mit den neuen technologischen Formen des Gebrauches beschäftigen, sondern seine eigene Perspektive zu der Frage einbrachte, wie (und welche) Prinzipien des Urheberrechts auf diese Gebrauchsformen Anwendung finden sollten, brachte er das breitest mögliche Publikum mit seinem Verständnis der Dinge in Berührung. Indem er die harten Fragen, die durch die neuen Technologien gestellt wurden, vor seinen Studenten zusammen mit der traditionellen Lehre des Urheberrechts ausbreitete, rüstete er eine Gruppe junger Anwälte in einer Weise aus, die es ihnen erlaubte, mit den neuen Fragestellungen umzugehen, ohne dem Rechtssystem Gewalt anzutun, das unserer Gesellschaft so lange in so geeigneter Weise gedient hatte.

* Der Beitrag ist mit dem Titel „Silicon Epics and Binary Bards: Determining the Proper Scope of Copyright Protection for Computer Programs" zuerst im UCLA Law Review (vol. 34, no. 5 & 6) erschienen. Wir danken für die freundliche Erlaubnis, ihn hier in deutscher Übersetzung bringen zu dürfen. - Anthony L. Clapes ist "Senior Corporate Counsel" bei IBM (Armonk, N.Y.), Patrick Lynch und Mark R. Steinberg sind Partner der Kanzlei Melveny and Myers (Los Angeles, CA).