Kai Denker

›Big Brother brutal zerhackt‹

Rückblick auf den ersten Hackerparagraphen 1986[1]

Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität (1986):

§ 202a 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.«[2]

Aus der parlamentarischen Diskussion des Gesetzentwurfes (1986):

»[…] Schwerpunkt der Änderungen des Regierungsentwurfs war die Einfügung von Straftatbeständen gegen den Mißbrauch von Computern. Die rasante Entwicklung im Bereich der elektronischen Datenbearbeitung hat zu einer ebenso schnellen Zunahme strafwürdiger Verhaltensformen geführt, denen mit geltendem Recht nicht mehr beizukommen ist. […]
In weitgehender Übereinstimmung sind die Mitglieder des Rechtsausschusses der Überzeugung, daß erhebliche Strafbarkeitslücken besonders in den Fällen des betrügerischen Mißbrauchs bei der Verwendung von Datenbearbeitungsanlagen, in den Fällen der Fälschung oder Unterdrückung von gespeicherten Daten im Rechts- und Beweisverkehr sowie bei Computersabotage und -spionage bestehen. […]
Abschließend möchte ich noch auf den Tatbestand eingehen, der das Ausspähen von Daten zum Inhalt hat. Die Absicht, das Eindringen in fremde Computersysteme unter Strafe zu stellen, hat in der Öffentlichkeit eine breite Diskussion ausgelöst, weil damit auch das Problem der sogenannten Hacker angesprochen wurde. In diesem Zusammenhang waren sich erfreulicherweise alle Fraktionen

1 Diese Analyse greift einige Aspekte auf, die ich in Kai Denker: »Heroes yet Criminals of the German Computer Revolution«, in: Gerard Alberts und Ruth Oldenziel (Hg.): *Hacking Europe. From Computer Cultures to Demoscenes*, London 2013, ausführlicher diskutiert habe.

2 Bundesministerium der Justiz und für Verbraucherschutz (Hg.): »Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. WiKG) vom 15. Mai 1986«, in: *Bundesgesetzblatt* 21 (1986), Teil 1, S. 721–729, hier: S. 721.

darin einig, dass nur eine Regelung in Betracht kommen könne, die nicht gleich jeden jugendlichen Computer-Freak bei der Ausübung seines Hobbys zum Kriminellen stempelt. Der Ausschuss hat deshalb davon abgesehen, schon – wie zunächst von der Bundesregierung angeregt worden war – die Verschaffung unbefugten Zugangs zu besonders gesicherten Daten unter Strafe zu stellen. Vielmehr soll das Strafrecht erst dort eingreifen, wo ein Schaden oder wenigstens eine Rechtsgutbeeinträchtigung – wie die Verletzung des Verfügungsrechts über Informationen u.a. – zu befürchten ist. Sogenannte Hacker, die sich mit dem bloßen Eindringen in ein Computersystem begnügen, sich also nicht unbefugt Daten verschaffen, sollen dagegen von Strafe verschont bleiben. […]«[3]

Während die deutsche politische Öffentlichkeit der frühen 1980er Jahre durch die (ausbleibende?) ›geistig-moralische Wende‹ des Amtsantritts Helmut Kohls, durch NATO-Nachrüstung und Flick-Affäre bewegt wurde, versetzte ein neuer Typus abweichenden Verhaltens Wirtschaft, Rechtswissenschaft und schließlich auch den Gesetzgeber in Unruhe: das ›Hacken‹. Die ›Computer-Hacker‹ nahmen Gestalt an – sowie eine als neu und unbeherrschbar empfundene Computerkriminalität. Unter dem irreführenden Titel der *Bekämpfung von Wirtschaftskriminalität* ging der Gesetzgeber hier nicht so sehr gegen kriminelle Handlungen durch die Wirtschaft als vielmehr *gegen* die Wirtschaft vor.[4] Neben Subventions- und Ausschreibungsbetrug wurde so die von Wirtschaftsvertretern beklagte schlechte Sicherheit teuer angeschaffter Computersysteme parlamentarisches Thema.[5]

Den wohl bemerkenswertesten Einfluss auf die Verhandlungen zum *2. Gesetz zur Bekämpfung von Wirtschaftskriminalität* hatten aber nicht die Wirtschaft oder die Bundesregierung, sondern, auch wenn sie gar nicht an den Verhandlungstisch geladen worden waren, die Computer-Hacker selbst. Während die offizielle Rechtsgeschichte mit den §§ 202a, 263a und 303a StGB (um die es im Folgenden in ihrer Fassung von 1986 gehen soll) vor allem eine Anpassung an positiv-verheißungsvolle neue Möglichkeiten der Informationstechnik verzeichnet, dokumentieren die Verhandlungen zum 2. WiKG genau das Gegenteil: Technikskepsis. Und eine Sorge um den technischen Status quo. Diese Sorge war es, die es den Hackern erlaubte, zum Prototyp

3 Vgl. Deutscher Bundestag (Hg.): »Rede des Abgeordneten Eicke Götz (CDU/CSU)«, in: *Plenarprotokolle (Stenographischer Bericht)* 10/201 (27.2.1986), S. 15434–15437.

4 Zum Titel des Gesetzes vgl. Fritjof Haft: »Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. WiKG) – Teil 2: Computerdelikte«, in: *Neue Zeitschrift für Strafrecht* 1987, Heft 6, S. 6–10.

5 Vgl. Deutscher Bundestag (Hg.): *Protokolle des Rechtsausschusses* 10/14 (25.1.1984), S. 5ff. Der zentrale Kreditausschuss, der Zusammenschluss der kreditwirtschaftlichen Spitzenverbände in Deutschland (seit 2011 unter dem Namen Die Deutsche Kreditwirtschaft), wird vom Vertreter des Bundesjustizministeriums als Hinweisgeber auf die Strafbarkeitslücken genannt. Auch seitens der Rechtswissenschaft wurde auf die Unzulänglichkeit der bestehenden Regelung hingewiesen. Besonders deutlich hierzu beispielsweise die Expertenanhörung im Rechtsausschuss selbst. Vgl. Deutscher Bundestag (Hg.): *Protokolle des Rechtsausschusses* 10/26 (6.6.1984).

einerseits einer sozialen Technikfolge und andererseits eines Widerstandskämpfers der neuen Zeit aufzusteigen.

I. Zur Vorgeschichte: Rechtliche Probleme der Informationstechnik

Die juristische Diskussion der frühen 1980er Jahre identifizierte drei Typen von möglichen, mit der vor-digitalen Rechtsprechung drohenden Strafbarkeitslücken – und zwar in den Bereichen Urkundenfälschung und Betrug, Sachbeschädigung sowie Briefgeheimnis.[6]

Urkundenfälschung und Betrug

Die Rechtsfigur der Urkunde hat eine lange Geschichte, die eine Urkundendefinition hervorbrachte, welche die beständige und visuell lesbare Verkörperung einer zuordenbaren Gedankenerklärung verlangt. Entscheidend ist, dass die Urkunde ohne Weiteres, d.h. auch ohne technische Hilfsmittel gelesen und als Beweis verwendet werden kann. Die Anfertigung einer falschen Urkunde, der es an der inhaltlichen Wahrheit oder der richtigen Zuordnung zu einem Aussteller mangelt, wird nach § 267 StGB als Urkundenfälschung bestraft. Eine Computerdatei erfüllt diese Bedingungen nicht: Weder ist sie materiell und beständig, noch ist sie ohne Hilfsmittel visuell lesbar. Das Anfertigen von sachlich falschen Dateien, etwa um ein Computersystem zu beeinflussen, kann also keine Urkundenfälschung sein.

Nicht viel besser die Betrugsvorschrift nach § 263 StGB: Sie verlangt, vorsätzlich durch unrichtige Tatsachenbehauptung oder durch Tatsachenunterdrückung einen Irrtum zu erregen oder zu unterhalten, um sich oder anderen Vermögensvorteile zu verschaffen. Als Irrtum gilt das Auseinanderfallen von Vorstellung und Realität. Wollte man Computersystemen nicht die Eigenschaft zusprechen, Vorstellungen haben zu können, konnte ihnen auch nicht die Fähigkeit zum Irrtum zugesprochen werden. Ist es jedoch nicht möglich, dass Computersysteme sich ›irren‹, kann man sie auch nicht betrügen. Folglich sah sich das Recht außer Stande, den § 263 StGB auf Manipulation von Computerprozessen anzuwenden.[7]

Der Gesetzgeber änderte die bewährten §§ 263 und 267 StGB nicht.[8] Stattdessen wurde eine gesonderte neue Norm eingeführt, § 263a StGB: der Computerbetrug.

6 Ich erlaube mir hier, die Redeweisen des damals federführenden Rechtsausschusses des Bundestags zu übernehmen, ohne die schon hierin vorfindliche ›sprach-strategische‹ Einschreibung zu problematisieren.

7 Vgl. Deutscher Bundestag (Hg.): *Protokolle des Rechtsausschusses* 10/14., a.a.O., S. 8. Dies wurde insbesondere für das elektronische Bezahlen mittels Giralgeld oder Eurocheckkarten als Problem gesehen, da in diesem Fall eine Datenverarbeitungsanlage getäuscht wurde. Vgl. ebd., S. 85. Die zugehörigen *Protokolle des Rechtsausschusses* beziehen sich auch immer wieder auf angeblich gescheiterte Strafverfahren, werden hier aber nie konkret. Vgl. beispielsweise Deutscher Bundestag (Hg.): *Protokolle des Rechtsausschusses* 10/63 (23.10.1985), S. 14ff. Ebendort wird auf S. 31 bemerkt, dass das genaue Ausmaß der Strafbarkeitslücke dem Bundesjustizministerium nicht bekannt sei.

8 Die Gefahr, durch eine Ergänzung einer klassischen Norm unbeabsichtigte Folgen auszulösen, wurde vom Bundesjustizministerium als so groß angesehen, dass es in einem Schreiben an den

§ 263a Computerbetrug:
»(1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, daß er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflußt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.«[9]

Sachbeschädigung und Computersabotage

Ganz ähnliche Probleme treten im Fall der Sachbeschädigung auf: § 303 StGB beschränkt die Norm auf Beschädigungen oder erhebliche, dauerhafte Veränderungen einer Sache. ›Sachen‹ aber sind körperliche Gegenstände (§ 90 BGB), weswegen sich das Verändern oder Löschen von Dateien nicht unter § 303 StGB fassen lassen: Weder sind sie körperliche Gegenstände, noch schädigt oder ändert die Veränderung einer Datei das Computersystem dauerhaft. Die Protokolle einer Expertenanhörung des in der Frage zuständigen Rechtsausschusses verzeichnen die Anekdote eines unzufriedenen Mitarbeiters, der auf dem Weg zu seinem Büro an einem Computersystem vorbei kam und lediglich einige Knöpfe drückte.[10] Die offenbar eher schlecht gesicherte Anlage musste daraufhin neu gestartet werden, was bei damaligen Großrechneranlagen durchaus zwei bis drei Stunden in Anspruch nehmen konnte und daher den Betriebsablauf fühlbar unterbrach. Wir kennen das Motiv des Mitarbeiters nicht, aber die rechtliche Bewertung: Mangels erheblicher und dauerhafter Veränderung einer Sache wurde das Verfahren gegen den Mann eingestellt.[11] Auch hier schuf der Gesetzgeber eine eigene Norm. § 303a StGB bestimmte in seiner Fassung von 1986:

§ 303a Datenveränderung:
»(1) Wer rechtswidrig Daten löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.«[12]

Vorsitzenden des Rechtsausschusses eindringlich darauf insistierte, die bestehenden Normen nicht abzuändern, sondern die Strafbarkeitslücken durch eigene Regelungen zu schließen. Vgl. Schreiben des Bundesjustizministeriums an den Vorsitzenden des Rechtsausschusses vom 11. Juni 1985, dort Anlage 3.

9 § 263a (1) StGB, Fassung vom 1. August 1986, in Bundesministerium der Justiz und für Verbraucherschutz (Hg.): »Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. WiKG) vom 15. Mai 1986«, in: *Bundesgesetzblatt* 21, a.a.O, S. 722.

10 Vgl. dazu ausführlich Deutscher Bundestag (Hg.): *Protokolle des Rechtsausschusses* 10/26., a.a.O., in dem der Vorsitzende den geladenen ›Experten‹ mehrfach für ihre Geduld dankt und sich für das eigene Unwissen entschuldigt. Vgl. ebd., S. 189 und 195.

11 Vgl. ebd., S. 179–180. Wurde der Mann entlassen? Ein Vertreter der betroffenen Firma bedauerte jedenfalls, dass der Vorgang ›strafrechtlich nicht fassbar‹ gewesen sei.

12 § 303a (1) StGB, Fassung vom 1. August 1986, in Bundesministerium der Justiz und für Verbraucherschutz (Hg.): »Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. WiKG) vom 15. Mai 1986«, in: *Bundesgesetzblatt* 21, a.a.O, S. 723–724.

Briefgeheimnis und Datenausspähung

Damit zum Briefgeheimnis, geschützt durch § 202 StGB (sowie Art. 10 GG). Die Strafnorm bezieht sich ausdrücklich auf Schriftstücke, für die sie eine besondere Sicherung durch einen Umschlag oder ein verschlossenes Behältnis verlangt.[13] Strafbewehrt sind unbefugtes Öffnen des Umschlags oder Behältnisses oder dessen Umgehung durch technische Hilfsmittel. Die Übertragung oder Speicherung von Daten hingegen wird durch § 202 StGB nicht geschützt und die Rechtsprechung sah keine Möglichkeit für einen Analogieschluss.[14] Eine auf einem Computersystem gespeicherte Datei ist weder ein Schriftstück noch durch Umschlag/Behältnis geschützt. Der neu eingeführte Tatbestand des ›Ausspähens‹, § 202a StGB, erweitert den Schutz auf Daten, allerdings nur auf solche, die gegen Zugriffe besonders gesichert sind.[15] § 202a (2) StGB in der Fassung von 1986 setzt einen Datentyp voraus, der sich durch eine elektronische, magnetische oder auf andere Weise nicht direkt wahrnehmbare Speicherung oder Übermittlung auszeichnet. Diese Einschränkung zeigt erneut die Absicht des Gesetzgebers, den flüchtigen Daten zwar einen rechtlichen Schutz zuzugestehen, sie aber dennoch von Sachen und Urkunden zu unterscheiden.

2. Täter oder Widerstandskämpfer

Soweit liest sich die Geschichte des Computer-Strafrechts in Deutschland als eine Geschichte der bloßen Anpassung des Rechts an technische Entwicklungen. Akzeptiert man die Position, dass es sich bei der Computertechnik um etwas grundlegend Neues handelt, sie aber dennoch (oder gerade deshalb?) keinen Anlass bieten soll, eine bereits etablierte Rechtsprechung in traditionellen Feldern durch Integration neuer Fallverläufe in die Judikatur zu alten Normen zu beseitigen, scheint die vorgestellte – ergänzende – Gesetzgebung nebst ihrer frühen Kommentierung plausibel. Die politische Entscheidung, Eingriffe auf unzureichend gesicherte Systeme mittels (neuer) Strafrechtsnormen gegen Angreifer zu beantworten und nicht, wie

13 Als verschlossen gilt ein Schriftstück, wenn es mit einer »Vorkehrung versehen ist, welche dem Vordringen zum gedanklichen Inhalt ein Hindernis bereitet.« Vgl. Günther M. Sander: *Münchener Kommentar zum Strafgesetzbuch*, Bd. 4, *§§ 185–262 StGB*, München 2012, zum § 202 StGB, Rdn. 14. Ein bloßes Zusammenfalten reicht hingegen nicht aus. Vgl. ebd., Rdn. 15. Aus dieser Unterscheidung wird bereits deutlich, dass der Gesetzgeber und die Rechtsprechung mehr als eine triviale Sicherung im Sinn gehabt haben und hierbei offenbar von der Vorstellung eines körperlichen Schriftstücks mit Schriftzeichen, also beispielsweise in Briefform, ausgingen. Vgl. ebd., Rdn. 9.

14 Analogieschlüsse im Strafrecht sind insbesondere deshalb heikel und daher zu vermeiden, da sie die Tatbestände der bestehenden Normen ausweiten und so den Grundsatz *nulla poena sine lege* verletzen.

15 Die besondere Sicherung wird dabei ähnlich wie schon im Fall des § 202 durch ein Hindernis erreicht, wird also nicht durch Überwachungsmechanismen oder dergleichen realisiert. Die Unüberwindlichkeit der Sicherung ist nicht erforderlich. Vgl. ebd., zum § 202a, Rdn. 35. Die vom Gesetzgeber gesehene Analogie zum § 202 führt im Fall des § 202a jedoch aufgrund der Vielzahl möglicher Sicherungsmaßnahmen zu einer eher unüberschaubaren Lage, die von baulichen Maßnahmen über Passwortsicherungen bis hin zur Verschlüsselung und der Wahl geeigneter Verstecke [!] reicht. Vgl. ebd., Rdn 35–47.

beispielsweise von den Grünen gefordert,[16] durch technische Sicherungsmaßnahmen und die Haftbarmachung der Hersteller und Betreiber von Computersystemen, war jedoch eine Pfadentscheidung. Sie wirkt bis heute in der Debatte zur Computerkriminalität nach – und auch in unserer Wahrnehmung digitaler Technologien.[17] Die Frage aber ist keineswegs trivial: Welche Sicherungsmaßnahmen wären den Herstellern von Computersystemen grundsätzlich möglich und wirtschaftlich zumutbar (gewesen)? Das Problem, wer für Manipulation oder Manipulierbarkeit einzustehen hat, berührt die Frage nach den Disponiblen und den Opportunitätskosten einer Sicherungsproblematik, die bis heute technisch beforscht wird. Während noch immer offen ist, inwieweit es mit vertretbarem Aufwand möglich ist, beweisbar sichere Systeme zu konstruieren, war zu Beginn der 1980er Jahre bereits klar, dass Computersysteme und ihre Sicherungsmechanismen ausgiebiger Tests bedürfen. Entwicklungskosten und Zeit bis zur Markteinführung wären erheblich gestiegen.[18] Der Gesetzgeber hat also 1986 eine deutliche Entscheidung im Interesse der Computerindustrie getroffen, als er auf Abschreckung durch Strafgesetze setzte.[19]

Es wäre gleichwohl vorschnell, hinter dem ›Hackerparagraphen‹ lediglich wirtschaftspolitische Motive zu vermuten. Die Parlamentarier waren seinerzeit auf ›Experten‹ angewiesen, die ihrerseits nicht müde wurden, die fehlende Umsetzbarkeit gewisser Sicherheitsvorstellungen zu betonen.[20]

Darüber hinaus war da jene Figur, die Computersysteme nicht bloß als Mittel, sondern sogar noch als Medium für die eigene Lebensgestaltung identifiziert hatte:

16 Vgl. Deutscher Bundestag (Hg.): *Protokolle des Rechtsausschusses* 10/63, a.a.O., S. 33: Abgeordneter Norbert Mann (Grüne) fragt, »ob man auf den sich rasant vollziehenden technischen Wandel nicht besser präventiv mit technischen Mitteln reagieren solle als mit den Mitteln des Strafrechts. Diejenigen, um deren wirtschaftliches Interesse es hier gehe, sollten sich technische Vorkehrungen einfallen lassen, die neue Strafvorschriften überflüssig machen würden.« Andere Mitglieder des Rechtsausschusses stimmten hier grundsätzlich zu: Die Kreditwirtschaft sei durchaus in der Pflicht, eine besondere Sicherung vorzunehmen.

17 Mit der Entscheidung, eine strafrechtliche Lösung des Sicherheitsproblems zu implementieren, entschied sich der Gesetzgeber damals für die Übernahme einer Abschreckungslogik, deren Scheitern eigentlich absehbar war: Gerade bei über Datennetze ausgeübten Handlungen ist das Problem, Handlungen zuverlässig zu attribuieren, kaum zu lösen. IT-Sicherheitsforschung betrachtet heute strafrechtliche Regelungen allenfalls als Beiwerk einer deutlich umfassenderen Strategie. Damals wie heute schreckt der Gesetzgeber zudem davor zurück, allzu konkrete Sicherungsvorschriften ins Gesetz aufzunehmen – nicht nur wegen der unternehmerischen Freiheit, sondern gerade auch wegen einer als unvorhersehbar vermuteten technologischen Entwicklung. Vgl. dazu den BMJ-Referentenentwurf des 2. WiKG vom 19.12.1978.

18 Mit dem Verweis auf Tests ist ein apparatives und instrumentelles Technikverständnis verbunden. Die aktuelle Forschung geht aber immer stärker darauf aus, die Medialität der Computertechnik in den Blick zu nehmen und beispielsweise nach Programmiersprachen zu suchen, in denen sich bestimmte, unsichere Programmkonstruktionen gar nicht mehr ausdrücken oder sie sich mit formalen oder wenigstens mit heuristischen Methoden systematisch auf ihre Sicherheit hin untersuchen lassen.

19 Dass Unternehmen mitunter einfachste Grundregeln beim Betrieb von Datenverarbeitungsanlagen missachteten, wurde auf der Expertenanhörung deutlich. Vgl. Deutscher Bundestag (Hg.): *Protokolle des Rechtsausschusses* 10/26, a.a.O., S. 170ff.

20 Vgl. Deutscher Bundestag (Hg.): »Kurzfassung der Stellungnahme der Nixdorff Computer AG, Anlage zum Protokoll«, in: *Protokolle des Rechtsausschusses* 10/26, a.a.O., S. 41.

der schon erwähnte ›Computer-Hacker‹.[21] In seiner Rede zur Plenardebatte hob der Abgeordnete Eicke Götz von der CDU/CSU-Fraktion darauf ab, man habe ganz bewusst und entgegen der Forderung der CDU-geführten Bundesregierung darauf verzichtet, ein bloßes Gefährdungsdelikt einzuführen, um damit auch ein solches Verhalten (von ›Freaks‹) zu kriminalisieren, bei dem es bloß darum gehe, sich (Stichwort ›Hobby‹) Zugang zu fremden Computersystemen zu verschaffen, ohne dabei Daten auszuspähen oder andere Rechtsgüter zu verletzen. Wie ist diese überraschende Einschränkung zu verstehen?

Lassen wir die Computer-Hacker in Gestalt ihres noch heute größten Vereins in Deutschland zu Wort kommen, der zu Beginn der 1980er Jahre gerade seine Gründungsphase erlebte: der Chaos Computer Club (CCC). In dessen eigener Zeitschrift namens *Datenschleuder*, deren hier zitierte Erstausgabe in kaum mehr als einem eilig zusammenkopierten Faltblatt bestand, heißt es sofort grundsätzlich:

> »Wir verwirklichen soweit wie möglich das ›neue‹ Menschenrecht auf zumindest weltweiten freien, unbehinderten und nicht kontrollierbaren Informationsaustausch (Freiheit für die Daten) unter ausnahmslos allen Menschen und anderen intelligenten Lebewesen.«[22]

Der CCC positionierte sich dabei entschieden anti-etatistisch: »Der Chaos Computer Club ist eine galaktische Vereinigung ohne feste Strukturen« mit einer auf die Zukunft gerichteten Rolle: »Nach uns die Zukunft: vielfältig und abwechslungsreich durch Ausbildung und Praxis im richtigen Umgang mit Computern wird oft auch als ›hacking‹ bezeichnet).[sic!]« Die praktische Ausbildung schien den Verfassern des Textes eine absolute Notwendigkeit, da es um nicht weniger als ihre (neue) Lebenswelt insgesamt ging: »Computer sind dabei eine nicht wieder abschaffbare Voraussetzung. Computer ist Spiel-, Werk- und Denk-Zeug; vor allem aber: das wichtigste neue Medium.«

Die Hacker, die sich im CCC zusammenfanden, sahen sich bald in der Tradition der ›Ur-Hacker‹ des MIT der 1960er Jahre, wie Steven Levy sie Anfang der 1980er Jahre beschrieben hatte.[23] Ebenso wie ihre Vorbilder misstrauten sie Autoritäten und richteten sich gegen große, anonyme und zentralistische Systeme.

21 Über die Hacker wurde viel Gutes und viel Schlechtes geschrieben. Ich verzichte auf eine Rekonstruktion dieser Diskussion und beschränke mich hier auf die für den interessierenden Zeitraum relevanten Selbst- und Fremddarstellungen.

22 Chaos Computer Club (Hg.): »Der Chaos Computer Club stellt sich vor«, in: *Datenschleuder* (1984), Heft 1.

23 Steven Levy formulierte die ›Hacker Ethic‹, auf die sich der CCC bis heute bezieht. Levy schrieb dabei den Hackern am MIT die Maxime ›Mistrust Authority – Promote Decentralization« ebenso zu wie »All information should be free«. Vgl. Steven Levy: *Hackers. Heroes of the Computer Revolution*, New York, London 2002 [1984], S. 28–29. Erst der CCC fügte als neuen Punkt der übersetzten »Hacker-Ethik« den Satz »Öffentliche Daten nützen, private Daten schützen« hinzu, der seine Position zum Datenschutz unterstrich. Vgl. http://www.ccc.de/de/hackerethik (aufgerufen 23.4.2014).

›System‹ meinte nicht nur technische Anlagen, sondern auch die großen wirtschaftlichen und gesellschaftlichen Institutionen – allen voran natürlich der vorgeblich zentralisierte Staat und auch seine als bürokratisch empfundenen Behörden im Einzelnen. Es war schließlich die Bundespost, die das durch das Fernmeldeanlagengesetz begründete Telekommunikationsmonopol ausübte, und damit den technischen Zugang zu den Datennetzen kontrollierte – und so zur Lebenswelt der Hacker. Aus deren Sicht erwies sich die Post als verantwortungslose Bremserin, die einerseits die Markteinführung beispielsweise schneller Modems behinderte, andererseits selbst unzuverlässige und unsichere Produkte auf den Markt brachte.[24] Folglich war dem CCC jede Gelegenheit willkommen, ›den Gilb‹ und seine oft schwerfällige Kommunikationsstrategie öffentlich vorzuführen. Das technisch noch weitgehend unausgereifte Bildschirmtextsystem – damals *das* Prestigeprojekt der Post – bot hierfür viele Gelegenheiten. Öffentlich demonstrierte Fehler und Sicherheitslücken brachten aus Sicht von Hackern (und Presse) die Post in Erklärungsnot. Ende 1984 trug sich ein Ereignis nach diesem Muster zu. Zwei Hacker des CCC waren an die Btx-Zugangsdaten der Hamburger Sparkasse gelangt und übertrugen mit einem kleinen Programm innerhalb einer Nacht beinahe 135.000 DM vom Btx-Konto der Sparkasse auf das ihres Clubs – wohlgemerkt: Es handelte sich lediglich um das Btx-Konto, das als einfaches Bezahlsystem über die Telefonrechnung der Bank abgerechnet worden wäre. Die Hacker meldeten die damals allenfalls als Ordnungswidrigkeit einzustufende Tat umgehend dem zuständigen Datenschutzbeauftragen, gelobten öffentlich, das Geld zurückzugeben und wiesen zugleich auf die Sicherheitslücken im Btx-System hin. Dass die Aussage der Hacker, sie hätten die Zugangsdaten über eben eine solche Sicherheitslücke erhalten, möglicherweise gar nicht stimmte, tröstete die Bundespost wohl kaum über die Blamage hinweg. So liest sich die Stellungnahme im Bundestagsausschuss für Post und Telekommunikation einige Wochen später zerknirscht, in welchem die Grünen umgehend die einstweilige Abschaltung von Btx beantragten.[25] Zum Kommunikationsdebakel trug auch der hanseatische Kommentar des Direktors der Hamburger Sparkasse bei: Er dankte den Hackern im heute journal dafür, auf die eklatanten Sicherheitslücken im Btx aufmerksam gemacht zu haben.[26]

Man wird sagen müssen, dass die ›Hacker-Ethik‹ Levys eher die Deskription eines Arbeitsethos war. Der normative Charakter, der die Hacker-Ethik heute in der Selbstdarstellung der Hacker oft begleitet, scheint so eine überaus deutsche Erfindung zu sein.

24 Vgl. Chaos Computer Club (Hg.): »Kabel frei für Telefonamateure!«, in: *Datenschleuder* (1985), Heft 11/12.

25 Vgl. Protokoll des Ausschusses für Post- und Fernmeldewesen, 10. WP, 17. Sitzung vom 16. Januar 1985, S. 12–13 unter ›Verschiedenes‹. Ebenda heißt es in der Diskussion zur ›Systemsicherheit‹ von Btx, dass Zweifel an dieser zwar nicht völlig ausgeräumt seien, dies aber darauf zurückzuführen sei, dass die DBP nicht schnell genug auf die falsche Berichterstattung reagiert habe. Es bestand im Ausschuss offenbar Konsens darüber, dass tatsächlich kein Systemfehler vorlag, sondern es sich um ein Kommunikationsproblem der Post mit den Medien gehandelt habe. Das habe Btx geschadet, heißt es im Protokoll. Auf dieser Sitzung wurde auch der genannte Antrag der Grünen gestellt und mit den Stimmen der CDU/CSU und der SPD abgelehnt.

26 Vgl. http://youtu.be/Urx4gA15brw (aufgerufen 24.4.2014).

Die öffentliche Diskussion ließ die mit dem 2. WiKG befassten Parlamentarier nicht unbeeindruckt. Es schien ihnen ungerechtfertigt, diejenigen zu kriminalisieren, die gewissermaßen als *Avantgarde des Informationszeitalters* nur auf den ersten Blick juvenile Streiche spielten, sich aber tatsächlich für Daten- und Verbraucherschutz engagierten. Trotz der deutlichen Warnung des Bundesjustizministeriums, keine Ausnahme für Hacker ins Gesetz aufzunehmen,[27] hielt der Ausschuss im Konsens zwischen den großen Fraktionen an seiner Position fest. Man milderte den Entwurf des § 202a entsprechend ab. Handlungen, die zum Aufdecken von Sicherheitslücken dienten, sollten straffrei bleiben. Um die Kodifizierung von Motiven zu vermeiden, entschied man sich erneut für eine folgenreiche Lösung: § 202a wurde auf das ›Ausspähen‹ von Daten beschränkt, während das bloße ›Eindringen‹ in Systeme straflos bleiben sollte.[28] Dem hierfür plädierenden Abgeordneten Götz (CSU) schloss sich auch Manfred Schmidt (SPD) an, wie das Protokoll vermerkt:

> »Auch seine Fraktion wolle nicht, daß jemand mit dem Strafgesetzbuch in Konflikt komme, nur weil er beispielsweise den Nachweis führe, daß die Sicherung gegen unbefugtes Abfragen von Daten nicht ausreichend seien.«[29]

3. ›Big Brother total zerhackt‹

Es wäre vorschnell, die Ausnahme fürs ›Eindringen‹ als frühen Fall des Schutzes von *Whistleblowing* zu sehen. Die Dankbarkeit und Anerkennung, die den Hackern seitens der Politik und der Presse entgegen gebracht wurde, bezog sich auch nicht einfach auf vermutete Missstände bei der Bundespost. Sie folgte vielmehr einem Narrativ, das die Hacker 1984 in der bereits zitierten *Datenschleuder* sich selbst nur zu gerne zu eigen gemacht hatten. Auf einer mit *Unsere Aufgaben für 1984 und die nähere Zukunft* überschriebenen Liste kündigten sie nämlich »[p]raktische gegenseitige Unterstützung

27 Vgl. Deutscher Bundestag (Hg.): *Protokolle des Rechtsausschusses* 10/63, a.a.O., S. 43ff. und Deutscher Bundestag (Hg.): *Protokolle des Rechtsausschusses* 10/69 (15.1.1986), S. 6ff. und S. 13. Die Frage, inwiefern nicht auch die Integrität von ganzen Datenverarbeitungsanlagen ein zu schützendes Rechtsgut sei, diskutierte der Ausschuss nur am Rande. Das Bundesjustizministerium übte genau hieran immer wieder scharfe Kritik und verwies auf einen Bruch mit der bisherigen Rechtspraxis; insbesondere würden sich rechtspraktisch Beweisschwierigkeiten ergeben, da nur teilweise erfolgreiche Täter sich auf das Straffreiheitsprivileg berufen könnten. Im Einzelfall von Strafe abzusehen sei bereits über die Strafprozessordnung möglich. Vgl. Deutscher Bundestag (Hg.): *Protokolle des Rechtsausschusses* 10/63, a.a.O., S. 47. Das Ministerium setzte sich jedoch nicht durch. Vgl. Schreiben des Bundesjustizministeriums an den Vorsitzenden des Rechtsausschusses vom 26.11.1985, S. 4ff. der Anlage.

28 Vgl. Deutscher Bundestag (Hg.): *Protokolle des Rechtsausschusses* 10/71 (22.1.1986), S. 5ff. Es wurde damals seitens der Grünen zu Recht bezweifelt, dass die Entschärfung des § 202a den gewünschten Effekt haben werde. So bemerkte 20 Jahre später Stefan Ernst anlässlich einer Novelle des § 202a StGB im Jahr 2007, dass nun zwar ›Hacking‹ explizit unter Strafe stünde, der Tatbestand des alten § 202a aber schon durch das bloße Abrufen der Verzeichnisstruktur erfüllt gewesen sei, so dass die Klarstellung keine praktische Veränderung mit sich bringe. Die Beseitigung der untauglichen Abgrenzung von 1986 sei gleichwohl zu begrüßen. Vgl. Stefan Ernst: »Das neue Computerstrafrecht«, in: *Neue Juristische Wochenschrift* (2007), S. 2661–2662.

29 Vgl. Deutscher Bundestag (Hg.): *Protokolle des Rechtsausschusses* 10/71, a.a.O., S. 6.

beim Umgang mit der schönen neuen Welt im Jahr der großen Brüderlichkeit« an und verorteten sich damit unverhohlen aufseiten des Widerstands gegen etwas, was sie, halb ironisch, halb ernst gemeint, als informationstechnische Materialisierung des Orwellschen Überwachungssystems darstellten. Wie wirkmächtig dieser Bezug war, zeigt der Beitrag des Wissenschaftsjournalisten Thomas von Randow in der *ZEIT* vom 30. November 1984. Unter der Überschrift »Ein Schlag gegen das System. Ein Computerclub deckt Sicherheitslücken im Btx-Programm der Post auf« heißt es da:

> »Ein solcher Schlag gegen ein Computersystem vermittelt einen köstlichen Triumph, der den finanziellen Vorteil, der manchmal damit verbunden ist, weit überwiegt, ein Befreiungsschlag ist es, der uns für ein paar Augenblicke der Apparateherrschaft entwindet.«[30]

Von Randows Redeweise macht klar, dass es bei der Sicherheitslücke des Btx-Systems keineswegs um einen Mangel an einem einzelnen technischen ›System‹ ging, sondern – und damit war er keineswegs allein – sofort um das ganze System, in dem eine sich ständig ausbreitende Herrschaft der Apparate Handlungsoptionen immer weiter beschränkte. Von Randow folgte damit der kulturpessimistischen Technikkritik, die diagnostizierte, dass wir in eine Abhängigkeit von technischen Mitteln geraten, indem technische Kategorien in einer Logik des *Sachzwangs* dominant werden.[31] Diese Richtung der Technikkritik verweist im Weiteren auf den Verlust von Widerständigkeiten, die qua Handlungserfolg und -misserfolg Feedback über das Handlungsmedium geben sollten, aber durch die technischen Fortschritte verschwinden und schließlich zu einem Verlust an Spuren führen.[32] Man muss dieser Deutung der modernen Technik als einer Technik ohne Spuren nicht zustimmen (und mag sie für das noch sehr unausgereifte Btx-System der frühen 1980er Jahre übertrieben finden), um dennoch ihren Niederschlag in den einschlägigen Zeitungsartikeln zu entdecken. Hierzu trug insbesondere noch Wau Holland – Gründer des CCC in Hamburg und einer der für den »Btx-Bankraub« Verantwortlichen – bei, der immer wieder auf die Gefahren der ›Verdatung‹ hinwies:

> »Kündige Deine Abbuchungsaufträge. Bedenke, was ein einzelner Programmierer bei den Elektrizitätswerken anrichten kann mit ein paar Millionen automatischen

30 *DIE ZEIT* 49 (30.11.1984), zit. nach: Chaos Computer Club Hamburg (Hg.): *Die Hackerbibel* Teil 1, Löhrbach 1985[?], S. 38.

31 Vgl. Christoph Hubig: *Die Kunst des Möglichen I. Technikphilosophie als Reflexion der Medialität*, Bielefeld 2006, S. 136.

32 Vgl. Christoph Hubig: »Wirkliche Virtualität – Medialitätsveränderung der Technik und der Verlust der Spuren«, in: Gerhard Gamm und Andreas Hetzel (Hg.): *Unbestimmtheitssignaturen der Technik – Eine neue Deutung der technisierten Welt*, Bielefeld 2005, S. 39–62.

Einziehungsaufträgen. – Laß Dich nicht verkabeln. Halte Deine Daten selbst in Ordnung und überlasse es nicht anderen, auch wenn es bequemer ist.«[33]

Entsprechend der Klage über den mutmaßlichen Verlust an Spuren lassen sich Sicherheitslücken und Programmierfehler als gerade die Überraschungen und Widerständigkeiten des technischen Handlungsmediums auffassen, in dem sie aufblitzen und gegenüber der ›Apparateherrschaft‹ die Möglichkeit des Widerstands versprechen.[34] Dass der Hacker hier eher als Freiheitskämpfer denn als Bedrohung erscheint, entsprach also durchaus dem Zeitgeist. Ungleich genüsslicher als die bürgerliche *ZEIT* listete die *taz* die Mängel des Btx-Systems auf, das ›eine gigantische Verbraucherverarschung‹ sei.[35] Überhaupt hatte die *taz* schon Anfang desselben Jahres kein Blatt vor den Mund genommen. Berichte über Schwierigkeiten mit den Computersystemen großer Firmen kommentierend erklärte sie ›Big Brother‹ kurzerhand für ›brutal zerhackt‹: »Das aufgeblähte Phantom ›big brother‹ wurde pünktlich zum Orwelljahr durch einen gezielten Großeinsatz von Hackern an Computerterminals in aller Welt hart getroffen«, und aktualisierte einen berühmten Brecht-Ausspruch für das Informationszeitalter: »Was ist das Bombardieren von Computersystemen gegen logische Bomben im Rechner?«[36]

Wenn auch nicht stets maschinenstürmerisch, so doch überaus skeptisch standen Presse und Politik den neuen, großen, schwer durchschaubaren und zentralistischen Systemen gegenüber, in welchen einzelne Sicherheitslücken nur eine beständige und systematische Bedrohung aktualisierten, die auch existentielle Ausmaße für die Gesellschaft annehmen könnte, wie der CCC bemerkte.[37] Hätte es die Figur des Hackers nicht gegeben, wären diese Narrative bei einer bloß negativen Kritik stehengeblieben. Dass es die ›Hacker‹, als neue Widerstandskämpfer in Gestalt von Verbraucher- und Datenschützern gab, trug nicht nur bei zu einer bis heute nachwirkenden Romantisierung von Informationstechnik, sondern begründete auch die Basis für all die semi-politischen Narrative von den großen, undurchdringbaren und zentralistischen

33 Wau Holland: »Praktischer Hinweis«, in: Chaos Computer Club Hamburg (Hg.): *Die Hackerbibel* Teil 1, a.a.O., S. 45. Aus Sicht der kulturpessimistischen Technikkritik muss die Antwort in einer ›konservativen Revolution‹ oder im ›Ideal einer Askese‹ bestehen, die natürlich auf die entsprechende Gratifikation verzichtet. Dies fordert auch Wau Holland, wenn er auffordert, überaus kritisch bei der Herausgabe der eigenen Daten zu sein und auf die Gratifikation der neuen Informationstechnik zu verzichten.

34 Vgl. Hubig: *Die Kunst des Möglichen I*, a.a.O., S. 138.

35 *taz* (22.12.1984), zit. nach: Chaos Computer Club Hamburg (Hg.): *Die Hackerbibel* Teil 1, a.a.O., S. 41.

36 *taz* (2.1.1984), S. 5.

37 Wer hier eine einfache Form eines Versicherheitlichungssprechaktes vermutet, liegt richtig: Der CCC bediente sich dieser bereits in den frühen 1980er Jahren: »Je einfacher eine Maschine konstruiert ist und je weniger Teile sie hat, desto weniger störanfällig ist sie auch. Eine vergleichsweise einfache Maschinerie ist also flexibler und kann leichter an wechselnde Bedürfnisse angepaßt werden. Im Gegensatz dazu hat unsere technologische Gesellschaft ihre Funktionen so spezialisiert, daß das ganze System zusammenzubrechen droht, wenn auch nur ein Teil der Maschinerie versagt.« (»Fortschritt ins Chaos«, in: Chaos Computer Club Hamburg (Hg.): *Hackerbibel*, a.a.O., S. 45.)

Systemen, die heute nicht mehr durch eine deutsche Behörde, sondern durch amerikanische Firmen betrieben werden. Dass ein ›virtueller‹ Bankraub noch die ansonsten eher konservative Rechtspolitik vor den Hackern den Hut ziehen ließ, war gegenüber dem, was danach kam, nur ein kleines Vorgeplänkel. Die Doppeldeutigkeit zwischen den jugendlichen Computer-Freaks und ihrem Hobby einerseits und ihrem Image als neue Widerstandskämpfer gegen das »System« andererseits blieb jedenfalls bis heute erhalten und kennzeichnet noch immer zahlreiche Konflikte netzpolitischer Debatten.