

INGO RUHMANN

# Politik im digitalen Zeitalter

## Ein Flickenteppich

Immer wieder führt der Einsatz von Computern zu Auseinandersetzungen darüber, ob dieser mit unserem Rechtssystem oder den Vorstellungen von Sitte und Moral vereinbar sei. Die breite Palette von Konfliktthemen reicht dabei von der Totalüberwachung der Arbeitsleistung durch den Einsatz von „Schnüffelsoftware“ über die Debatte zur Kontrolle der Telekommunikation durch Sicherheitsbehörden oder dem Ausspähen von Kunden elektronischer Kaufhäuser durch Anbieter bis zu der Frage, wie das Internet so eingegrenzt werden könne, dass dem Jugendschutz Geltung verschafft wird. Der breite Einsatz von Computern und Internet hat der Politik ein neues Arbeitsfeld geschaffen. Doch die Umsetzung ist nicht frei von Widersprüchen.

Seit fast 20 Jahren wird darüber gestritten, ob Software zur Verschlüsselung von elektronischer Kommunikation frei verfügbar sein darf oder besser einer strikten staatlichen Kontrolle unterliegen sollte. Gesetze wurden erlassen, geändert und wieder verändert, nachdem Wissenschaftler neue Verschlüsselungsverfahren gefunden und Programmierer diese als Software zur freien Benutzung angeboten hatten.

Noch komplizierter scheint die Lage bei der Regelung des Zugangs zu Inhalten im Internet, die entweder nach jeweils nationaler Rechtslage illegal oder nach allgemeinen Vorstellungen für Jugendliche nicht geeignet sind. Hier gibt es in einigen Staaten wie der Volksrepublik China oder dem Iran harte Zensurmaßnahmen, in anderen Staaten wie etwa in Deutschland Gesetze, die allenfalls eingeschränkt anwendbar und nur bedingt für die Strafverfolgung bedeutsam sind. In wieder anderen Staaten wie etwa den USA scheint es zwei getrennte Bereiche zu geben, bei denen im politischen Bereich fast alles erlaubt ist, in den Bereichen Jugendschutz oder Online-Glücksspiele dagegen strenge Regeln gelten, die zudem von US-Bundesstaat zu Bundesstaat anders sind und anders verfolgt werden.

### 1. Debatten mit der Dramaturgie einer Fernsehserie

Konfliktfeldern dieser Art liegen gegensätzliche Vorstellungen von Softwareentwicklern und Computerbenutzern auf der einen Seite und von Sicherheits-

behörden, Juristen und Hütern der Moral auf der anderen Seite zu Grunde. Die Politik ist das Spielfeld, auf dem unterschiedliche Ansichten miteinander mit dem Ziel wettstreiten, Änderungen der aktuellen Situation herbeizuführen. In einer Mediengesellschaft ist es politisch attraktiv, die durch Neuerungen hervorgerufenen Unsicherheiten bei Bürgerinnen und Bürgern durch politische Botschaften aufzugreifen, die zwar allgemeine politische Ziele formulieren, sich aber nicht in konkrete politische Aktionen übersetzen lassen.

Ernsthafte Politik beabsichtigt jedoch Änderungen und diese bestehen – zumindest in westlichen Demokratien – im Wesentlichen darin, Politikziele in Gesetze zu gießen und, wo nötig, die Einhaltung dieser Gesetze durch die Exekutive zu kontrollieren. Bei der Informationstechnologie (IT) bietet sich der Politik zusätzlich die Möglichkeit, Forschung und Entwicklung durch Fördergelder gezielt zu stimulieren und diesen damit eine Richtung zu geben.

Die Debatte in der IT-Politik ähnelt seit den 90er-Jahren einer unendlichen Fernsehserie. Statt zu einer Problemlösung zu kommen, werden die immer gleichen grundsätzlichen Argumente in beinahe regelmäßigen Abständen immer wieder in die Medien gespült, angereichert bestenfalls mit gerade aktuellen Facetten. Die Dramaturgie solcher Auseinandersetzungen verläuft nach mittlerweile bekanntem Muster. Beginnend mit der Klage über einen durch Computereinsatz verursachten Missstand wird eine technische Lösung verlangt, mit der die rechtlich oder moralisch begründeten Probleme beseitigt werden sollen. Wenn ein entsprechender technischer Vorschlag gemacht wird, folgt fast umgehend der Nachweis seiner technischen Untauglichkeit, weil die Lösung entweder die betroffenen Computersysteme lahm legen würde oder auf kinderleichte Art und Weise zu umgehen sei. In hartnäckigen Fällen wird dann auch eine fehlerhafte Lösung gefordert, weil diese wenigstens symbolische Besserung verspricht. Das klassische Beispiel ist die Sperrung von gefährdenden oder illegalen Inhalten, bei dem Gesetze angewandt werden sollen durch technische Maßnahmen, die in keiner Weise tauglich sind.

Die scheinbare Fruchtlosigkeit dieser immer wiederkehrenden Klagen, Vorschläge und Konflikte um den Computereinsatz haben das öffentliche Interesse an vielen Themen mit Computerbezug mittlerweile erlahmen lassen. Kaum mehr wahrgenommen wird dadurch aber, dass die sich dahinter verbergenden realen Konfliktlinien in durchaus einschneidender Weise die Bedingungen verändern, unter denen wir mailen und im Internet surfen, aber auch arbeiten und kommunizieren.

## 2. Widersprüchliches politisches Verständnis für IT

Die politische Gestaltung all dessen, was mit Informationstechnik zu tun hat, ist in Deutschland nur schwer auf einen Nenner zu bringen. Die Bundesrepublik Deutschland ist in allem schon früh aktiv geworden, was sich im weitesten Sinne als »Computerrecht« bezeichnen lässt. Mit der Datenschutzgesetz-

gebung der 70er-Jahre, den Hackerparagrafen der 80er-Jahre, den Gesetzen zum Internet, den Regelungen zum E-Commerce und der digitalen Signatur der 90er-Jahre ist eine im internationalen Vergleich hohe Regelungsdichte entstanden.

Zu Beginn des 21. Jahrhunderts gibt es nun auch in allen etablierten Parteien Standpunkte zum Politikfeld Informationstechnik oder Internet. Den Anfang machte 1995 die Bundestagsfraktion von Bündnis 90/Die Grünen mit einem Grundsatzantrag,<sup>1</sup> der die damalige Bundesregierung aufforderte, ein umfassendes Konzept zur Gestaltung der Informationsgesellschaft vorzulegen, und zusätzlich zahlreiche einzelne Forderungen stellte. Dem folgte die Bundestagsfraktion der SPD 1996 mit einem eigenen Antrag,<sup>2</sup> der neben den bereits von den Grünen benannten Punkten auch die Entwicklung von Fernsehen und Rundfunk ansprach und eine gemeinsame Weiterentwicklung beider Bereiche forderte. Aufgefrischt wurden diese Forderungen mit einem 20-Punktepapier der SPD im Juli 2001.<sup>3</sup> Die CDU beklagte im Jahr 2000: »Eine deutsche Internet-Politik gibt es bislang nicht«<sup>4</sup> und forderte die sofortige Bündelung von Zuständigkeiten. Von einer Kommission wurden in der Folge 47 akzentuierte Forderungen zu ähnlichen Themen ausgearbeitet, wie sie in den vorher entstandenen Papieren ebenfalls zu finden sind.<sup>5</sup>

Nach dem lange Zeit vorherrschenden Eindruck, dass es vor allem der Legislative, aber auch der Exekutive – also dem Parlament einerseits und der Bundesregierung samt ausführender Verwaltung andererseits – an einem realistischen Verständnis für die Möglichkeiten und Grenzen der Informationstechnik mangle, scheint sich mittlerweile eine Besserung eingestellt zu haben. Der bei allen Parteien in wesentlichen Punkten sehr ähnliche Kanon von Forderungen zur Entwicklung des Internets und der Informationstechnik lässt sogar die Vermutung aufkommen, es gebe bei allen Differenzen so etwas wie einen parteiübergreifenden Konsens in grundsätzlichen Fragen.

Dennoch agiert der Gesetzgeber – heute wie früher – immer noch auf abgegrenzten, politisch aktuellen Spielfeldern wie der Kontrolle des Internets, anstatt Informationstechnik und die Auswirkungen ihres Einsatzes in systematischer Weise politisch anzugehen. Allenfalls in wenigen Einzelbereichen – zu nennen sind hier Pilotprojekte zur digitalen Verwaltung, in Teilen auch die Reaktion auf die Fachkräfteknappheit im IT-Sektor – gehen die Aktionen über Einzelmaßnahmen hinaus und verknüpfen mehrere Schritte auf unterschiedlichen Gebieten zur Umsetzung eines größeren Ziels.

Die heutigen Regierungsparteien haben früher ein abgestimmtes Konzept einer IT-Politik gefordert, ohne dies bislang selbst umgesetzt zu haben. Die CDU wiederum beklagt heute zwar die mangelnde Koordinierung, hat dies zu ihrer Regierungszeit selbst aber nicht betrieben und reduziert Informationstechnik genauso auf das Internet wie der ehemalige SPD-Generalsekretär und jetzige Vorsitzende der SPD-Bundestagsfraktion Müntefering,<sup>6</sup> für den das Internet »Auslöser, Gegenstand und Medium« für einen neuen »Gestaltungsauftrag« an die Politik ist.<sup>7</sup> Alle politischen Richtungen fordern also

gleichermaßen eine koordinierte IT-Politik. An der Umsetzung jedoch hapert es bislang. Die Folgen sind widersprüchlich: Während Nutzungsbehinderungen fallen sollen, werden gleichzeitig neue errichtet. Was fehlt, ist die viel beschworene Verlässlichkeit.

### 3. IT-Politik – mehr als die Summe ihrer Einzelteile

Computer sind zu einer uns umgebenden Infrastruktur geworden, die genauso sinnvoll geformt werden kann wie die Bedingungen der Verkehrspolitik, der Ökologie oder des Gesundheitswesens und anderer technisch-wissenschaftlicher Bereiche von großer politischer und gesellschaftlicher Bedeutung. Die Entwicklung zur mobilen Gesellschaft wurde begleitet von der Einsicht, dass Verkehrspolitik mehr ist als der Bau von Autos, entsprechender Fahrwege und die Stimulation der Wirtschaft durch möglichst hohe Produktionszahlen. Statt den Straßenbau zu privatisieren, TÜV und Straßenverkehrsordnung abzuschaffen und die Automobilbranche dem freien Spiel der Marktkräfte zu überlassen, wurde nach Wegen gesucht, Mobilität zumindest nach den mittelfristigen Bedürfnissen einer gesamten Gesellschaft zu ermöglichen und zugleich wirtschaftlichen Wohlstand zu erzielen.

Wären die Reden über Chancen und Herausforderungen der Informationsgesellschaft wirklich ernst gemeint, müsste es heute eine IT-Politik in einem umfassenderen Sinn ebenso geben wie eine Verkehrs-, Umwelt- oder Bildungspolitik. IT-Politik könnte sich weder auf die politisch üblichen Forderungen beschränken, das Marktgeschehen dynamischer zu gestalten, noch darauf, alle an der Informationsgesellschaft teilhaben zu lassen, sondern würde den Einsatz der Informationstechnik unter den Vorgaben unserer Verfassung und unseres demokratischen politischen Systems und dann zusätzlich auch unter ökonomischen und sozialen Aspekten betrachten.

Die gegenwärtige Lage gibt jedoch nur wenige Anhaltspunkte dafür, dass die enge Verzahnung von kaum veränderbaren technischen Eigenarten, formbaren Standards, Entwicklungen und dem Marktgeschehen sowie deren sozialen, ökonomischen und vor allem politischen Folgen auch als eigenständige und umfassende politische Aufgabe wahrgenommen wird. Anhand von Beispielen soll verdeutlicht werden, um welche Sichtweisen es geht.

#### 3.1 Telekommunikation

Das Internet wird heute als Teil der Telekommunikation begriffen, die alles umfasst, was elektronisch zwischen zwei Kommunikationspartnern übermittelt wird. Die Art und Weise, in der herkömmliche Telekommunikation und das Internet geformt und verwaltet werden, könnte jedoch unterschiedlicher kaum sein. Die Telekommunikation war in den 70er- und 80er-Jahren ein Thema, das in Deutschland heftige politische Konflikte ausgelöst hat. Ein

kleiner Ausschnitt dieser Konflikte soll hier genügen, um diese unterschiedlichen Denkweisen zu erläutern.

Schwer vorstellbar sind heute die hohen Wellen, die vor knapp 20 Jahren die Einführung des ISDN-Telefons schlug. Ein Teil der Auseinandersetzung galt der Frage, warum nicht jeder Haushalt mit einem Glasfaseranschluss ausgestattet werde, um Datenübertragung in hoher Geschwindigkeit zu erlauben. Ein wesentlicher Teil der Aufregung entstand aus der mit ISDN verbundenen Möglichkeit, alle für den Aufbau und die Abwicklung eines Telefonats anfallenden Daten zu speichern und teilweise auch weiterzugeben. Es ging also – in der heutigen Denkweise – um die Netzinfrastruktur, ihre technischen Möglichkeiten, aber auch um ihre Überwachung.

Wir sollten uns daran erinnern, dass vor der Einführung eines digitalen Telefonnetzes die Daten darüber, wer wann wie lange mit wem telefoniert hatte, aus technischen Gründen gar nicht erst entstehen konnten. Ohne besonderen Aufwand blieb unbekannt, welche Nummern von einem Anschluss aus angerufen wurden. Auch jeder Anrufer blieb für den Angerufenen anonym. Sollte ein Anrufer – etwa für eine Ermittlung in Strafsachen – zurückverfolgt werden, musste dafür ein hoher technischer und personeller Aufwand getrieben werden. Heute wird bereits gespeichert, wer mit wem telefonieren will, bevor der Angerufene überhaupt zum Hörer greift. Der Angerufene sieht die Nummer des Anrufers auf dem Display und kann sich entscheiden, ob er das Gespräch annehmen will oder nicht.

Solche Eigenschaften gehören heute zu den normalen Dienstmerkmalen der Telekommunikation. Sie haben aber weitergehende Folgen. Nacht für Nacht werden in Deutschland die Daten aller Telefonverbindungen von den Vermittlungscomputern an die Abrechnungsrechenzentren der Anbieter übermittelt. Auf diese Weise entsteht ein vollständiges Profil über den gesamten Telekommunikationsverkehr des Landes einschließlich der Datenkommunikation. Solche Datensammlungen werden Kommunikationsprofile genannt. Für einige sind sie ein sinnvoller Dienst, für andere eine interessante Datenquelle.

Jeder Telefonkunde – also beispielsweise das Call-Center eines Unternehmens – kann mit Hilfe entsprechender Technik jederzeit nicht nur Ziel und Dauer abgehender Gespräche speichern, sondern auch die Daten aller eingehenden Verbindungen oder Verbindungsversuche. Die Daten der zu den Telefonnummern gehörenden Personen vervollständigen ein komplettes Bild aller Kommunikationskontakte eines Unternehmens mit der Außenwelt oder gar eines ganzen Landes.

Es gibt aber auch andere Motive, um zu erfahren, wer mit wem kommuniziert hat. Vom Telefonanschluss einer Redaktion führt die Spur zum anonymen Informanten, von dem des Rechtsanwalts zum Gesuchten und von dem eines Arztes schließlich zum Patienten. Die Beziehungen von Journalisten, Anwälten und Ärzten zu ihren Klienten oder Patienten geht Dritte eigentlich nichts an. Die Kommunikationsprofile geben dennoch darüber Aufschluss.

All dies haben die Computer in den Vermittlungsknoten heute möglich gemacht. Das Auswerten ist nur nicht jedem jederzeit gestattet. Denn: Um die Möglichkeiten der Technik zu einer Kommunikationsüberwachung zu begrenzen, mussten neue Gesetze regeln, was mit den Daten geschehen darf und was verboten ist. Die Möglichkeiten von Sicherheitsbehörden hat der Gesetzgeber dabei in den vergangenen Jahren kontinuierlich ausgeweitet. Mit Daten-Suchläufen über die Verbindungsdaten ist heute das weitgehend wahr geworden, was in den 80er-Jahren noch für Aufregung sorgte: Telekommunikation ist schon lange nicht mehr anonym.

Zusätzliche Eigenschaften bietet die GSM-Mobiltelefonie. Auf dem Markt sind heute technische Dienste, durch die ein eingeschaltetes Handy zum Peilsender mit 50 Meter Genauigkeit wird.<sup>8</sup> Wieder ist die Technik schneller als der Gesetzgeber: Zahlende Kunden können diese »Location Based Services« in Anspruch nehmen. Für Ermittlungen in Strafsachen ist diese Eigenschaft von Handys gegenwärtig unregelt. Peilsender sind bislang nur in eng begrenzten Fällen und mit richterlicher Genehmigung erlaubt, um die Observation einer Person zu unterstützen. Forderungen nach Änderungen der Strafprozessordnung, um diese technischen Dienste auch für Ermittlungen zu nutzen, sind damit nur folgerichtig.

Solche Auswertungsmöglichkeiten wurden von einer kleinen Zahl von Telekommunikationsfirmen gezielt entwickelt und in den internationalen Gremien zur Entwicklung der Telekommunikation weltweit koordiniert, damit ein Telefonat von Europa in die USA oder nach Asien am Zielort auch verarbeitet werden kann. Die Möglichkeiten der neuen Technik sind für Sicherheitsbehörden sehr attraktiv. Es entstanden Gremien, die international technische Schnittstellen für den Zugriff auf interessante Daten definierten. Damit bestand kein Grund, eine Technik wie ISDN oder die GSM-Mobiltelefone auf eine Weise zu entwickeln, bei der erheblich weniger Daten benötigt und erzeugt werden.

In Deutschland waren diese Entwicklungen schon früh ein politisches Thema. Als Folge wurden einige Funktionen mit Kontrollcharakter für die Allgemeinheit eingeschränkt. Seit Mitte der 90er-Jahre geht es jedoch regelmäßig darum, Sicherheitsbehörden einen größeren Zugriff auf Daten zu geben, die bei der Telekommunikation erzeugt werden. Dabei wurde vielfach das legalisiert, was vorher in technischen Gremien definiert wurde.<sup>9</sup>

Bei der Telekommunikation wurden also technische Entwicklungsprozesse und politische Ausgestaltung relativ zeitnah miteinander verbunden und politisch diskutiert. Möglich war diese Debatte aber nur, solange das Postwesen als staatliche Aufgabe und damit als Politikfeld begriffen wurde. Der Ausbau der Telekommunikation wurde durch Fachgremien und Kommissionen vorbereitet und durch alternative Studien kritisch hinterfragt.<sup>10</sup> Zum wichtigen Thema entwickelte sich dabei die Kontrolle der Telekommunikation. Hierbei wurde im Wesentlichen das technisch Machbare nur gesetzlich begrenzt.

Das Internet ist wesentlich offener und flexibler als die ISDN-Technik. In den USA saßen zwar Ende der 80er-Jahre ebenfalls Vertreter aus Wirtschaft und Politik zusammen und entwarfen allgemeine Visionen für die Verbreitung des Internets.<sup>11</sup> Dass sich aber aus der Internet-Euphorie der ersten Hälfte der 90er-Jahre ein so umfassender Siegeszug entwickeln würde, übertraf die kühnsten Erwartungen. In nur zehn Jahren hatte sich das Internet so weit ausgebreitet, dass heute etwa die Hälfte der Bevölkerung der westlichen Industriestaaten entweder an ihren Arbeitsplätzen oder zu Hause Zugang hat.

Im Internet werden widerstreitende Ansichten zur Datenerhebung und Datenvermeidung nicht allein in verbaler Form ausgetragen, sondern durchaus auch in Software formuliert und in der Praxis erprobt. Hier versucht eine vergleichsweise große Zahl von Computerexperten, mit Technik auch ihre Sicht von Politik umzusetzen.

Eine völlige Neuerfindung des Internets in einer sicheren und datenschutzgerechten Form ist damit zwar nicht möglich, aber immerhin lassen sich alle Arten von Diensten in sehr unterschiedlicher Weise zur Verfügung stellen, bei denen entsprechende Software entweder verteilt bei jedem Endnutzer läuft oder bei einer kleinen Zahl von Computern im Internet. Mit ein wenig Aufwand lassen sich so Computer konfigurieren, die ein anonymes Surfen oder Mailen im Internet erlauben.<sup>12</sup> Es ist genau diese Offenheit gegenüber Ideen und Bedürfnissen der Benutzer, die das Internet einerseits so erfolgreich gemacht hat, andererseits politischen Eingriffen bislang nur begrenzte Erfolgsaussichten gibt.

Ein einziger Internetnutzer kann eine neue Idee programmieren und die Lösung an Millionen Internetnutzer verteilen. Grenzen dieser Möglichkeiten zeigt allerdings die chinesische Lösung: Wer in der Volksrepublik Software zur Verschlüsselung von E-Mails einsetzt, macht sich strafbar. Weil im Internet jedes Datenpaket immer mit der IP-Adresse des Absenders und des Adressaten versehen ist, weisen verschlüsselte Datenpakete in dem durch staatliche Stellen streng überwachten chinesischen Teil des Netzes sofort den Weg zu solchen Gesetzesbrechern, die verbotene Software einsetzen.

Die Hoffnung auf eine unkontrollierte Internetentwicklung beruht also auf der Gewissheit, dass im Internet jeder Kontrollmechanismus auf Dauer unterlaufen werden könnte und Kontrollmaßnahmen in einen technischen Wettlauf zwischen Überwachern und Überwachten münden. Das Ende dieses Wettlaufs wäre dann erreicht, wenn die Verbreitung von Programmiersprachen eingeschränkt wird und im Internet nur vorgegebene Software erlaubt ist. Der Unterschied zwischen Internet und Telefonnetzen besteht also darin, dass das Internet die Möglichkeit eröffnet, Kommunikationsnetze in Eigenregie zu formen, aber auch durch Eigenentwicklungen zu stören. Die Frage, wohin die Entwicklung geht, ist keine Planungsaufgabe für staatliche Stellen, sondern hängt von der Motivation aller Beteiligten und einem nicht steuerbaren Wettlauf zwischen Kontrolle und Unabhängigkeit ab, dessen Ergebnis durch Zufälle bedingt ist.

Anders als die ISDN-Einführung wurde die Internettechnologie ohne Einflussnahme deutscher Regierungsstellen entwickelt,<sup>13</sup> ihre breite zivile Einführung vor allem von der US-Regierung Anfang der 90er-Jahre stark befördert. Zugleich war die Liberalisierung der Telekommunikation schon so weit gediehen, dass Infrastrukturfragen keine staatliche Aufgabe mehr darstellten. Dementsprechend gering waren die Steuerungsmöglichkeiten auf deutscher Seite.<sup>14</sup>

Auch wenn es beim ISDN vordergründig »nur« um eine neue Form des Telefons ging, so lautet die Schlussfolgerung Nummer Eins: Ein korrekter Blick in die gesellschaftliche Zukunft eines Technikeinsatzes ist durchaus möglich und kann in einer politischen Debatte zur Ausgestaltung und teilweisen Eingrenzung von Technik führen. Im Gegensatz dazu bietet das Internet den Vorteil, seinen Benutzern eine offene technische Umgebung zur Verfügung zu stellen, die einen Wettbewerb zwischen regulierenden Auflagen und technischen Ausweichversuchen möglich macht. Dabei ist die Grenze undefiniert zwischen demokratisch legitimierten Anforderungen an die Technik und Technikentwicklungen Einzelner, die sich guerillaartig ausbreiten. Im Ergebnis gibt es aber bei beiden Technologien – bei der einen geplant, bei der anderen nachträglich realisiert – staatliche Rahmenvorgaben, die eine unabhängige Entwicklung begrenzen.

### 3.2 Digitale Dienstleistungen

Die Vorteile des schnellen Datenaustausches lassen sich noch ausbauen, wenn damit komplexere Transaktionsprozesse verbunden werden. Geld gegen Ware oder gar ein Wegfall lästiger Besuche auf Ämtern und anderen Verwaltungsstufen sind die Ziele der zahlreichen neuen Dienstleistungsformen, die alle mit dem Kürzel »E-« beginnen: E-Commerce und E-Government, also das Einkaufen oder Verwalten per Internet. Weil die Kunden Teile der Verwaltungsarbeit selbst erledigen, sollten diese Angebote auch kostengünstiger werden.

Von dieser Theorie ist die Praxis aber immer noch weit entfernt. Einerseits ist es etwas kompliziert, Arbeitsabläufe auf das Internet umzustellen. Ganz wesentlich ist aber das Handicap, dass die Internetkommunikation in einer Weise abläuft, die nur sehr schwer mit den Anforderungen an die Eindeutigkeit und Nachprüfbarkeit der Abläufe vereinbar ist, die man erwartet, wenn es um Geld oder um staatliche Verwaltungsakte geht. Das grundsätzliche Problem besteht darin, dass es im Internet mit wenigen Ausnahmen keinen Tausch von Geld gegen Ware gibt, sondern dort nur bestellt wird – geliefert und bezahlt werden muss auf anderen Wegen.

Im Internet kann man sich mit nur mäßigem Aufwand als beliebige Person, aber auch als beliebiger Anbieter ausgeben. Wer mit wem Geschäfte macht, ist dadurch sehr viel schwieriger zu klären als bei anderen Geschäftsformen. Aus Anbietersicht sollte die Lösung darin liegen, mehr Daten über Kunden zu sam-

meln. Die Kunden üben dabei Zurückhaltung, weil sie nicht mit Werbemüll überschwemmt werden wollen. Aus Kundensicht sollten solche Geschäfte nur einfach und zuverlässig funktionieren. Tests von Verbraucherschutzverbänden und anderen zeigen dagegen, dass immer noch bei vielen Internetangeboten Waren- oder Preisangaben fehlen und ein unangemessen großer Prozentsatz von Bestellungen per Internet zu spät oder gar nicht ausgeführt wird.<sup>15</sup> Immer wieder aufgedeckte Probleme mit der Sicherung der Kreditkartennummern von Kunden vor Unbefugten bei E-Commerce-Anbietern verunsichern obendrein. Seit die EU-Kommission das Rechtssystem der Anbieterseite für den Handel als bindend erklärt hat, kann die undurchsichtige Herkunft eines Internetangebots für Kunden auch noch unangenehme juristische Konsequenzen haben: Wer nicht zahlt, setzt sich erst einmal einem Betrugsverdacht aus. Wer sein Recht als Kunde bekommen will, muss im Ausland klagen.

Das E-Government kommt über ein Anfordern von Formularen oder allgemeine Informationen nicht hinaus, weil eine sichere Identifikation im Internet den breiten Einsatz von amtlich geprüften digitalen Unterschriften oder anderen Verfahren erfordert. Hier konkurrieren gegenwärtig noch mehrere technische Systeme gegeneinander. Die Unternehmensseite sieht den Staat gefordert, die digitale Signatur per Chipkarte zu verbreiten: »Mit einem Chip-Personalausweis geht das am besten«, so Stefan Grosse vom Branchenverband Bitkom.<sup>16</sup> Aber selbst dort, wo es Ausweise und Signaturen auf einer Plastikarte gibt, ist die digitale Signatur teuer und wenig brauchbar: »Es fehlen einfach noch die nützlichen Anwendungen«, so Ritva Viljanen aus Finnland, wo digitale Ausweise schon gelten.<sup>17</sup> Auch dort kommt E-Government nicht recht von der Stelle.

Alle »E-Dienstleistungen« gründen auf Anforderungen an die Internet-technologie, die von dieser zumindest auf absehbare Zeit nicht erfüllt werden können. Warum sollten Kunden umfassende Daten über sich preisgeben, bloß um am elektronischen Handel teilzunehmen? Sie können nicht einmal sicher gehen, ob sie es mit einem seriösen Anbieter oder einem fliegenden digitalen Händler zu tun haben. Die Kosten, um den Informationskanal Internet so sicher und vertrauenswürdig zu machen wie den kleinen Laden um die Ecke, drohen den erwarteten Gewinn aufzuwiegen.

Das politische Verständnis einer Begleitung von E-Dienstleistungen ging zuerst von der vernünftigen Haltung aus, dass sich erst einmal E-Business entwickeln müsse, bevor der Staat regulierend eingreifen solle. Als das Unbehagen der Kundschaft wie der Anbieter als Hindernis spürbar wurde, entstanden zuerst auf nationaler, dann auf europäischer Ebene Gesetze zur digitalen Signatur als technischem Zusatzdienst, um die elektronischen Identitätsprobleme zu lösen. Das Verfahren ist aber komplizierter als das herkömmliche Internet-Shopping und kostet Gebühren. Auch wichtige Sicherheitsfragen sind ungeklärt – Informatiker haben gezeigt, wie nichts ahnenden Benutzern beliebige falsche Schriftstücke zur digitalen Unterschrift untergeschoben werden können.<sup>18</sup>

Das neue deutsche Signaturgesetz ermöglicht gemäß der EU-Richtlinie ausdrücklich neben der so genannten »fortgeschrittenen« Signatur auch die »einfache« Signatur. Dabei wird die digitale Signatur in vielen Bereichen der eigenhändigen Unterschrift gleich gestellt. Die einfache Signatur beruht auf den allgemeinen Haftungsregeln. Hier muss der Kunde den Schaden selbst nachweisen. Dem Anbieter bleibt es überlassen, welche Sicherheiten er gewährt. Einfacher wäre dagegen eine Haftungsregelung für Schäden, die entstehen, wenn Unternehmen eine billige und manipulationsanfällige Lösung einer sicheren vorziehen. Weil der E-Commerce-Anbieter das Signatursystem wählt und damit seinen Kunden vorschreibt, müsste er auch das Risiko tragen.

Bei der fortgeschrittenen Signatur hingegen haften Anbieter für die Richtigkeit und Vollständigkeit der Angaben im Zertifikat zum Ausstellungszeitpunkt. Der deutsche Gesetzgeber konnte jedoch nicht völlig den Forderungen aus Brüssel nachgeben. Deshalb führte er zusätzlich eine so genannte »qualifizierte Signatur« ein, was von der europäischen Richtlinie nicht gefordert war. Diese Signatur wird nur von den Trust-Centern erzeugt, die sich zuvor freiwillig von der Regulierungsbehörde akkreditieren lassen. Dafür erhalten sie ein offizielles Gütesiegel. Auf Grund der Haftungsfrage sprechen sich die Verbraucherschützer in Deutschland für die qualifizierte Signatur aus. Doch der Preis für eine qualifizierte Signatur ist so hoch, dass diese für die Anbieter derzeit nicht rentabel ist: Schätzungsweise 1300 Euro Vollkosten entfallen auf eine einzige zertifizierte Signaturkarte, die dann für etwa 50 Euro angeboten wird. Eine Softwarelösung ist dagegen schon für jeweils 10 Euro zu haben.<sup>19</sup>

Der Gesetzgeber zog bei der digitalen Signatur vor, bekannte Probleme zu ignorieren und Risiken auf die Kunden abzuwälzen. Ein gerechter Ausgleich zwischen den Interessen von Anbietern und Kunden beim E-Commerce ist nicht gefunden. Der Staat hat seine unabhängige Position nicht genutzt, sondern beschränkt sich darauf, den Rahmen für technisch noch nicht ausgereifte Lösungen zu setzen.

Die Schlussfolgerung Nummer Zwei lautet daher: Bevor viel Arbeit und Kapital darin investiert werden, Alltagsvorgänge in die Welt des Internets zu übertragen, sollte gründlich überlegt werden, warum diese Alltagsvorgänge so und nicht anders ablaufen und was die Informationstechnik dafür an gleichwertigen Eigenschaften bieten kann und was nicht.

### 3.3 Sicherheit im Internet

Wenn die Internet-Technologie schon über keine ausreichenden Mechanismen für den Beweis der Identität einer Person verfügt, so werden diese Probleme noch verschärft durch Manipulationen und das mutwillige Herbeiführen von Schäden. Mittlerweile ist auch der Öffentlichkeit offenbar, wie leicht die an das Internet angeschlossenen Computer angegriffen werden können.

Eher ärgerlich sind E-Mails, deren Größe die eigene Mailbox zusammenbrechen lässt. Für Anbieter geschäftsbedrohlich ist es, wenn sich ihre Internetangebote nicht mehr erreichen lassen, nachdem ein gezieltes Datenpaket ihren Zentralrechner zum Absturz gebracht hat oder er durch ein Dauerfeuer aus Tausenden kleinster Anfragen in die Knie gezwungen wurde. Computerviren und Würmer verbreiten sich rasend schnell per elektronischer Post. Wer sich Software auf die Festplatte lädt, riskiert damit zugleich, so genannte Trojaner zu installieren. Das ist eine verborgene Software, die den eigenen Rechner von außen fernsteuerbar macht oder vielleicht sogar zu einem Instrument in einem verteilten Angriff tausender Computer auf die Rechner Dritter.

Privatanwender sind nur mühsam zum Einsatz von Virenscannern und vielleicht etwas mehr Vorsicht beim Herumklicken in E-Mails oder dem Herunterladen von Software zweifelhafter Herkunft zu bewegen. Kaum beachtet wird der Rat der Datenschützer, sich stärker selbst zu schützen.

Nach den Terroranschlägen im September 2001 stand auf staatlicher Seite die internationale Abstimmung von Gesetzen gegen Computermanipulationen, das so genannte Cyberkriminalitäts-Abkommen, im Mittelpunkt des öffentlichen Interesses. Auf deutscher Seite wurde angestrebt, den seit 1987 in Deutschland geltenden Strafgesetzen gegen Computerkriminalität auch außerhalb der Landesgrenzen mehr Geltung zu verschaffen. Gleichzeitig wurden aber im deutschen Recht bewusst ausgeklammerte Regelungen getroffen, nach denen es nun strafbar sein kann, die Unsicherheit von Computersystemen zu testen. Mit der Konvention wurde obendrein der Weg geebnet für weitere Gesetze, die das Umgehen von Sicherungsmechanismen wie den Kopierschutz von CDs oder Software unterbinden sollen. In einen Topf geworfen wurden dabei so unterschiedliche Bereiche wie das Urheberrecht, das Hacken oder der so genannte »Cyberterrorismus«.

Auf die gesetzliche Ebene kann auch auf diesem Gebiet nicht verzichtet werden – nur wehe dem, der in diesem Land auch nur versucht hat, erkannte Angreifer auf seine Computersysteme zur Anzeige zu bringen. Die derartigen Sachverhalten fachlich gewachsenen Stellen bei Bundes- und Landeskriminalämtern, Staatsanwaltschaften und Polizeidienststellen sind schnell aufgezählt. Obwohl die einschlägigen Paragraphen seit fast 15 Jahren eingeführt sind, gibt es nur wenige Ermittlungen und kaum Verurteilungen.<sup>20</sup>

Begründet wird dies damit, dass es an Experten fehle, die derartige Taten fachkundig bewerten könnten. Deswegen wurden zentrale Stellen zur Reaktion auf Sicherheitsvorfälle verstärkt. »Computer Emergency Response Teams« (CERTs) sind immer stärker gefordert. Die Mitarbeiter sind jedoch vollauf damit beschäftigt, das »Bestiarium« der Computerschädlinge im Zaum und außerdem die Sicherheitslücken einer immer größeren Zahl von Softwareprodukten im Auge zu behalten. Einer Studie der »Initiative D21« zufolge bieten von den gerade einmal zehn CERTs in Deutschland nur zwei ihre Dienste für kleine und mittlere Unternehmen, kein einziges jedoch der allgemeinen Öffentlichkeit an.<sup>21</sup>

Nirgendwo werden gegenwärtig umfassende Strategien entwickelt, wie die Sicherheit bei Computern und Internet verbessert werden könnte. Allenfalls einzelne Vorschläge wie die Aufteilung des Internets in einen öffentlichen und einen sicheren, abgeschotteten Teil werden laut, die jedoch das Gesamtproblem nicht mindern. Diese Vorschläge erkennen lediglich an, dass viele Angriffe im Internet auf der Schäden verursachenden Zweckentfremdung vorhandener Mechanismen beruhen, ohne die aber der Datenverkehr unmöglich wäre.

Völlig untauglich sind Ideen, die Veröffentlichung von Sicherheitslöchern zu unterbinden: Die Angreifer sind es, die Informationslücken ihrer Opfer in puncto Sicherheit ausbeuten. Ohne eine breite Information über Probleme erfahren die allermeisten der potenziellen Opfer nichts von der Gefahr, in der sie schweben, während die Angreifer zusätzliche Zeit und Gelegenheiten erhalten, ihr Werk in die Tat umzusetzen. Genau aus diesem Grunde fordert die Wirtschaftsinitiative D21, die Nutzerinnen und Nutzer zu sensibilisieren und zu informieren.

Genauso wenig, wie ein Rennwagen allein mit einer Handbremse im Straßenverkehr kontrollierbar ist, so sollte deutlich sein, dass es mit der bestehenden Informationstechnik keine größere Sicherheit in Sachen Computer geben wird. Schon die grundlegendsten Kenntnisse der Informationstechnik führen jedem vor Augen, dass Sicherheit auch nicht per Gesetz herstellbar ist.

Der einzige Ausweg ist die klare Definition von Regeln, welche Sicherheitseigenschaften auch ein Computer – etwa auf der Intensivstation im Krankenhaus – zu erfüllen hat und die Verbreitung neuer und sicherer Systeme. In vielen Bereichen werden Gesetze zur Ausschaltung von Risiken erlassen, die unwahrscheinlicher sind als ein Lottogewinn. Gleichzeitig hält es der Gesetzgeber für vertretbar, den Einsatz von Computersystemen hinzunehmen, deren Sicherheitslöcher – oder schlimmer noch: deren reguläre Funktionen – zu gewaltigen Schadenssummen führen. Computer, die sicherer sind als der Durchschnitt, sind längst verfügbar. Sicherheit spielt aber bei der Auswahl von Systemen nur eine vernachlässigte Rolle. Das rächt sich schon im täglichen Einsatz und wird noch unangenehmer, wenn Hacker nachhelfen.

Die Schäden werden zumeist hinter vorgehaltener Hand beziffert. Dem »I love you«-Virus wurden weltweit Schäden durch gelöschte Daten und der Arbeit zur Wieder-Inbetriebnahme von Computern in Höhe von über 1 Mrd. Dollar angelastet, den drei am stärksten verbreiteten Viren der letzten 18 Monate 11 Mrd. Dollar.<sup>22</sup> Hacker und Viren verursachen aber nur den geringsten Teil aller Schadensfälle bei Computern, weit über 40 Prozent entstehen durch Programmfehler oder Fehler in Verbindung mit unsachgemäßer Bedienung.<sup>23</sup> Allen verfügbaren Statistiken zufolge »schwankt der auf Computerkriminalität zurückzuführende Anteil von IT-Sicherheitsproblemen seit den 80er-Jahren um etwa 15 Prozent«, stellte der Deutsche Bundestag 1998 in seinem Bericht »Sicherheit und Schutz im Netz« fest.<sup>24</sup> Computersoftware, die ganz ohne Hacker Fehlfunktionen hat, ist so häufig, dass vielfach kaum er-

kennbar ist, ob die Software Fehler verursacht oder Hacker ein System manipulieren. Solange sich aber ein bisweilen unerklärliches, aber ungefährliches Verhalten von Computern nicht eindeutig vom Eindringen von Hackern und Viren unterscheiden lässt, wird sichtbar, wie grundlegend die Defizite bei der IT-Sicherheit sind.

Die dritte Schlussfolgerung lautet daher, dass es nicht nur an Basiswissen zu Erfordernissen für und Möglichkeiten von Sicherheit beim Einsatz von Computern fehlt, sondern offensichtlich grundsätzlich an dem Problembewusstsein, dass es kein Naturgesetz ist, dass heute Computersysteme unzählige Fehlfunktionen aufweisen. Das Unverständnis gegenüber den alltäglichen Auswüchsen dieser fehlenden Sicherheit ist davon eine Folge.

### 3.4 Folgen der neuen Zukunft von Eigentum an Software

Noch stärker auseinander laufen die Interessen der Allgemeinheit und zukünftige gesetzliche Vorschriften bei den Folgen, die Tendenzen bei der Sicherung des geistigen Eigentums erkennen lassen. Dabei geht es nicht um Bilder oder Texte, sondern um die zukünftig geltenden Einsatzbedingungen von Software.

Software scheint anderen Bedingungen unterworfen zu sein als andere Produkte. Heute hat jeder Benutzer eines Softwaresystems bei der Installation einer Endbenutzer-Lizenzvereinbarung zuzustimmen, die den Softwarehersteller – anders als die Hersteller beliebiger anderer Produkte – von den meisten Schadensersatzansprüchen durch Fehler im Produkt freistellt.

Auch die Kunden scheinen Software als etwas Eigenes zu sehen. Kaum in Frage gestellt wird, dass das Raubkopieren von Software vergleichsweise weit verbreitet ist. Dagegen schützen sich Softwarehersteller mit technischen Sicherungen, die aber – wie fast alle Sicherheitsfeatures bei Software – umgangen werden können. Das Internet hat dazu geführt, die Installation von Software an den Hersteller online zu melden, um dem illegalen Treiben besser auf die Spur zu kommen. Seit Microsoft bei der Installation des Betriebssystems Windows 95 versuchte, Daten über den Kunden an einen zentralen Rechner zu übermitteln, sind immer mehr dieser Techniken ans Licht gekommen. Das neue Betriebssystem Windows XP kontaktiert den Microsoft-Zentralrechner nicht nur bei der Installation, sondern regelmäßig und unkontrolliert, wenn der Benutzer ins Internet geht.

Übermittelt werden dabei heute Daten. Das mag sich in Zukunft verschärfen. In den USA ist mit dem »Uniform Computer Information Transaction Act« (UCITA)<sup>25</sup> gegenwärtig ein Gesetz für den Handel mit Software in den parlamentarischen Beratungen und in einigen US-Bundesstaaten auch schon verabschiedet, nach dem ein Softwareanbieter den Käufern seiner Produkte die völlig legal gekaufte Software per Internet unbrauchbar machen darf. Zulässig wäre dies, wenn zum Beispiel der Kunde beklagt, dass das Softwarepro-

dukt fehlerhaft ist. Der Anbieter dagegen soll das Recht erhalten, dem Kunden bekannte Fehler des Softwareprodukts zu verschweigen.

Was heute noch ein Trojanerprogramm im Computer ist, das den Computer lahm legt, kann also morgen schon eine gesetzlich zulässige Reaktion auf Reklamationen von Kunden sein. Eingesetzt werden könnte dies, um zuerst den illegalen Softwareeinsatz aufzuspüren, dann – wie früher bei Großcomputern – vom Kauf zur Miete von Software überzugehen, bei der für jeden Aufruf eines Programms zu bezahlen ist, um schließlich zu bestimmen, welche Software anderer Hersteller auf dem eigenen Computer installiert werden darf und welche nicht. Für alle diese Varianten gab es bereits Beispiele, die für die Zukunft weiterentwickelt werden. Neu wäre allein, das Lahmlegen eines Computersystems – nach deutschem Recht eine Straftat – als Form der Konfliktlösung zwischen Softwarehersteller und -käufer zu erlauben.<sup>26</sup> Jeder Staat, der sich dazu entschließt, gibt den Anspruch auf, Konflikte durch Recht und Gesetz zu regeln und erklärt den Cyberspace zur weitgehend rechtsfreien Zone.

Schlussfolgerung Nummer vier lautet daher: Wenn die Einzelinteressen auf so kleinen Politikfeldern wie dem Urheberrecht so völlig ohne Zusammenhang selbst zum Strafrecht gesehen werden, dass damit Strafverfolgung bei IT-Sicherheitsdelikten ad absurdum geführt werden kann, hat der Staat zugleich seine Arbeit und Aufgabe unterminiert sowie das Vertrauen in die Informationstechnik nachhaltig zerstört.

#### 4. Fazit

Die Politik im digitalen Zeitalter sieht sich neuen Problemen gegenüber. Antworten findet sie bislang vor allem darin, alte Regeln auf die neue Technik zu übertragen und bestenfalls kleinere Neuerungen zu wagen. Das Ergebnis dieser Politik ist weit davon entfernt, sachgerecht zu sein.

Wenige Beispiele machen die Widersprüche klar: Die immer wieder diskutierten Verbote von Verschlüsselungssoftware stehen im Widerspruch zu Datenschutzvorschriften. Die Nutzung des Internets wird in außerordentlicher Weise gefördert, zugleich wird versucht, den Zugang zu Inhalten, die in anderen Rechtssystemen zur Verfügung gestellt werden, zu unterbinden. Im E-Commerce wurden die Gewichte zwischen Kunden und Anbietern zu Lasten der Kunden verschoben, womit sich die technisch und rechtlich versiertere Seite durchgesetzt hat. Gesetze zur digitalen Signatur wiederum wollen Sicherheit schaffen auf Computersystemen, deren Manipulierbarkeit bekannt ist und hingenommen wird. Hacken ist ungesetzlich, wird aber trotz schärferer Gesetze seit fast 15 Jahren faktisch kaum verfolgt, weil es an Strafverfolgern und IT-Experten mit ausreichendem Fachwissen fehlt. Die Folge ist eine wachsende Bereitschaft zur Selbstverteidigung. Schutz gewährt der

Staat damit nicht, sondern macht – als absurde Folge dieser und insbesondere neuer Gesetze zum Schutz geistigen Eigentums – das Aufdecken von Sicherheitslöchern in IT-Systemen strafbar. Software verhält sich immer undurchschaubarer, für Softwareanbieter drohen Gesetze zu entstehen, mit denen diese ihren Kunden im Zweifelsfall das ordentlich bezahlte IT-System mit verborgenen Funktionen aus der Ferne zerstören können. Solche Gesetze hebeln rechtsstaatliches Handeln aus und setzen das Recht des Stärkeren an dessen Stelle.

Auf diese Weise ist der Versuch einer IT-Politik entstanden, bei der Regelungen nur kleinteilig realisiert werden. Dabei wird kaum darauf geachtet, ob sie überhaupt umsetzbar sind oder auch, ob sie sich zu einem Gesamtbild zusammenfügen lassen. Ergebnis ist ein Flickenteppich von Vorschriften, angebotlicher und realer Regelungslücken, ohne die Lage für alle Beteiligten zu verbessern oder zu vereinfachen.

Als Problem erkannt wird dies kaum. Herbert Kubicek, der die Entwicklung seit den 70er-Jahren als Experte begleitet, weist darauf hin, dass Deutschland gegenwärtig den dritten Anlauf auf dem Weg in die Informationsgesellschaft nimmt. Bislang werde aber weder aus den bisherigen Schritten gelernt, noch würden neue Konzepte entwickelt.<sup>27</sup> Seit der Ausgliederung der Telekommunikation aus dem Kanon der Politikfelder ist im Gegenteil eine immer geringere Neigung zu erkennen, die mit der Verbreitung von Computer und Internet einhergehenden komplexen Probleme überhaupt politisch anzugehen. Dabei ist es offensichtlich durchaus machbar, wesentliche Entwicklungen der IT-Politik im Zeitraum von mehreren Jahren im Voraus zu identifizieren und Handlungsvorschläge zu entwickeln.<sup>28</sup>

IT-Politik geht sehr deutlich über Fragen der informationellen Selbstbestimmung, der unbeobachteten Kommunikation oder der Meinungsfreiheit hinaus. Es geht heute um die Sicherung von Grundfragen unseres Rechtssystems in der Informationsgesellschaft. Der IT-Einsatz hat bereits das ansonsten streng gehütete staatliche Gewaltmonopol ausgehöhlt. In wenigen Jahren steht – geht es nach einigen wenigen IT-Anbietern – eine Neubestimmung dessen an, was die Gesetzbücher heute noch als Eigentum definieren. Für eine IT-Politik geht es also um eine umfassende Sicherung unserer Grundrechte auch in einer digitalen Welt. Die Notwendigkeit dessen lässt sich kaum eindringlicher belegen.

Die Zurückhaltung auf politischer Seite und die Reduktion der Vorschläge auf wenige Bereiche wird gern mit der hohen Dynamik der Informationstechnik begründet, die politisches Handeln zum Bremsklotz mache. Dagegen ist diese Technik für Experten aus Wirtschaft und Wissenschaft weder zu dynamisch, noch zu unübersichtlich, um darin für sich zu einem sehr frühen Zeitpunkt Entscheidungen zu treffen. Das bedeutet aber, dass auch eine IT-Politik bei ausreichender Fachkenntnis machbar wäre.

IT-Politik ist aber nicht nur notwendig und machbar. Als kohärente Politik wäre sie obendrein den heute oft mehr oder weniger willkürlichen politischen

Bemühungen vorzuziehen, kleine Ausschnitte des Problems mit nicht selten widersprüchlichen Ergebnissen anzugehen. Die Ausgestaltung der Informationsgesellschaft stellt also neue Anforderungen an unser politisches System. In wenigen Jahren wird sich zeigen, ob es den Herausforderungen gewachsen war.

## Anmerkungen

- 1 Ein ökologischer, sozialer und demokratischer Weg in die Informationsgesellschaft II, Bundestags-Drucksache 13/3010, 10. 11. 1995.
- 2 Deutschlands demokratischer Weg in die Informationsgesellschaft, Bundestags-Drucksache 13/5197, 27. 6. 1996.
- 3 20 Thesen zu Politik und Internet, <http://www.spd.de/events/internet-kongress/20thesen.html>
- 4 Beschluss des Bundesvorstands der CDU Deutschlands am 8. 5. 2000, Punkt 5, [http://www.cdu.de/politik-a-z/beschluesse/internet\\_080500.htm](http://www.cdu.de/politik-a-z/beschluesse/internet_080500.htm)
- 5 <http://www.cdu.de/chancen-deutschland/massnahmen.pdf>
- 6 Franz Müntefering, Mut zur Politik im digitalen Zeitalter, [http://www.spd.de/partei/organisation/generalsekretaer/mut\\_zur\\_politik.html](http://www.spd.de/partei/organisation/generalsekretaer/mut_zur_politik.html)
- 7 Ebd.
- 8 Ekkehard Müller-Jentsch, Allgemeiner Lauschangriff, in: *Süddeutsche Zeitung*, 29. 11. 01, S. 45.
- 9 Vgl. die Übersicht zur Entwicklung in Deutschland in: Ingo Ruhmann/Christiane Schulzki-Haddouti, Abhör-Dschungel, in: *c't*, Heft 5, 1998, S. 82–93. Die Geschichte der internationalen Abstimmung von Überwachungstechnik beschreibt Erich Moechel in den ETSI-Dossiers, Teil vier erschien als »Lauscher am Netz« in *c't*, Heft 4, 2002, S. 80–82.
- 10 Den Anfang machte die Kommission für den Ausbau des Telekommunikationssystems (KtK) 1974–1976. Die Ziele in den 80er-Jahren wurden formuliert von der Regierungskommission Fernmeldewesen, die 1987 Ergebnisse vorlegte. Als politische Alternative dazu finanzierten die Arbeits- und Wirtschaftsministerien des Landes Nordrhein-Westfalen die Studie »Optionen der Telekommunikation«, die ebenfalls 1987 Ergebnisse vorlegte. In diesen Papieren finden sich schon so gut wie alle Themen wieder, die auch heute noch eine Rolle spielen – Zugang für alle, breitbandige Netze zu bezahlbaren Kosten und vieles mehr.
- 11 1989 publizierte das »Computer Science Policy Project«, ein Konsortium von 13 Unternehmern der Computerindustrie, die Studie »Perspectives on the National Infrastructure«. Darin wurde eine Vision für unternehmerische und politische Aktivitäten zum Ausbau des Internets entwickelt. Aufgegriffen wurde dies vom späteren US-Vizepräsidenten Al Gore. Das Papier war Anstoß für Fördergesetze und die Politik der späteren Clinton-Administration.
- 12 Vgl. den Beitrag von Marit Hansen und Christian Krause in diesem Band.
- 13 Die Erfordernisse der Forschungseinrichtung des US-Verteidigungsministeriums, der Defense Advanced Projects Agency (DARPA), nach sicherer Kommunikation finden sich dagegen deutlicher im ursprünglichen Internet-Protokoll (RFC 791). Dort wurde der Aufbau der Datenpakete so definiert, dass in jedes Datenpaket sowohl Angaben über Sicherheitsstufen (bis zu Top Secret) wie Übermittlungswege oder die Selektion nach Dringlichkeit eingebaut werden können. Diese Daten werden im zivilen Teil des Internets heute nicht ausgewertet, sondern ignoriert.

- 14 US-Regierungsstellen behalten sich auch heute die Kontrolle über die Schaltstellen des Internets vor. Die Verwaltung der Internetadressen wird durch eine private Einrichtung, aber im Auftrag des US-Wirtschaftsministeriums abgewickelt. Bei der Ausgestaltung dieser Aufgabe werden die Grenzen von der US-Regierung gezogen. Vgl. dazu etwa Ute Bernhardt, Von Namen und Nummern. Der demokratische Aspekt bei der ersten Wahl der Internetverwaltung Ican, in: Telepolis. 2000, <http://www.heise.de/tp/deutsch/inhalt/te/8673/1.html>
- 15 Bei Testkäufen von Verbraucherverbänden hat sich die Lage nur bedingt gebessert. 1999 waren bei Tests der Stiftung Warentest nur erstaunlich niedrige 40 Prozent der E-Commerce-Anbieter in der Lage, die gewünschte Ware in der angebotenen Form zu liefern, 60 Prozent lieferten dagegen falsch oder gar nicht (Karl Kollmann, Internet-Shopping im Test aus Verbrauchersicht: [www.heise.de/tp/deutsch/inhalte/te/5248/1.html](http://www.heise.de/tp/deutsch/inhalte/te/5248/1.html)). Mitte 2000 wurden in den USA E-Commerce-Anbieter wegen verspäteter Lieferungen zur Zahlung von insgesamt 1,5 Mio. US-Dollar verurteilt (US-Online-Shops wegen verspäteter Lieferungen verurteilt; [www.heise.de/newsticker/data/axv-27.07.00-001/](http://www.heise.de/newsticker/data/axv-27.07.00-001/)). Auch 2001 wurde bei Testkäufen von Hardware in Online-Shops immer wieder über Probleme berichtet, so zum Beispiel Georg Schnurer, VERAMScht. c't-Kaufstest, in: c't, Heft 16, 2001, S. 94 ff.
- 16 Staat und Wirtschaft bluffen im Poker um die Smartcard, in: Computer-Zeitung Nr. 4, 2002.
- 17 Vater Staat soll für Signatur den Geburtshelfer spielen, in: Computer-Zeitung, Nr. 5, 2002.
- 18 Armin B. Cremers/Adrian Spalka/Hanno Langweg, Vermeidung und Abwehr von Angriffen Trojanischer Pferde auf Digitale Signaturen, in: Bundesamt für Sicherheit in der Informationstechnik (Hg.), 2001 – Odyssee im Cyberspace? Sicherheit im Internet!, Ingelheim 2001, S. 113–125.
- 19 Schlaue Karten helfen Firmen bei Kundenbindung und IT-Sicherheit, in: Computer-Zeitung Nr. 5, 2002.
- 20 Als Computerdelikt gelten nach § 263 StGB auch Manipulationen an und mit Kredit- oder Scheckkarten, bei denen schon seit den 90er-Jahren die Deliktrate deutlich anstieg. Laut IuK-Meldedienst des Bundeskriminalamtes wurden im Jahr 2000 101 Fälle des »Ausspähens von Daten«, 39 Fälle »Datenveränderung« und 52 Fälle »Computersabotage« registriert, darunter 14 Fälle von Denial-of-Service-Angriffen.
- 21 D21 – AG5, CERT Infrastruktur Deutschland, Bericht, Berlin, 29. 1. 2002, S. 7.
- 22 Bei derartigen Berechnungen ist zwar große Vorsicht geboten, zur Schadensbewertung gibt es jedoch kaum brauchbare Alternativen: <http://www.computereconomics.com/cei/press/pr92101.html>
- 23 Einer IBM-Studie von 1986 zufolge entfielen nur 3,6 Prozent der Schadensursachen auf externe Ursachen. Vgl. ÖVD-Online, Nr. 10, 1986, S. 36.
- 24 Enquête-Kommission des Deutschen Bundestages »Zukunft der Medien in Wirtschaft und Gesellschaft. Deutschlands Weg in die Informationsgesellschaft« (Hrsg.), Sicherheit und Schutz im Netz, Schriftenreihe Band 7, Duisburg 1998, S. 50.
- 25 Das Gesetz wurde in Maryland und Virginia beraten und erlassen, in acht weiteren US-Bundesstaaten ist es in der Gesetzesberatung. Der Text ist verfügbar unter: <http://www.law.upenn.edu/bll/ulc/ucita/ucita200.htm>, eine aktuelle Übersicht zum Stand der Beratungen gibt: <http://www.ucitaonline.com/whathap.html>; Kritik des größten Informatiker-Verbandes unter: <http://www.acm.org/usacm/copyright/>
- 26 DirecTV, ein US-Betreiber von Satellitenfernsehen, brachte im Januar 2001 Hunderttausende Fernsehgeräte in Kanada zum Absturz. Die Zuschauer besaßen eine gehackte TV-Karte, mit der sie umsonst die kostenpflichtigen TV-Programme sehen konnten. So urteilten in Kanada Gerichte, dass an der Nutzung der Piratenkarten

nichts zu beanstanden sei. Denn DirecTV sende außerhalb des kanadischen Territoriums. Über 200 000 Kanadier sollen sich die Piratenkarte besorgt haben. Rein juristisch war DirecTV machtlos. Deshalb griff die Firma zur »elektronischen Gegenmaßnahme«, wie die Attacke im US-Militärjargon bezeichnet wird. Die Aktion führte eine DirecTV-Abteilung namens »Signals Integrity« durch, in der nach Informationen der kanadischen Tageszeitung »Montreal Gazette« ehemalige FBI-Agenten arbeiteten. Über mehrere Monate hinweg verschickte das Team kleine Segmente des Computer-Virus per Rückkanal. Der Code wurde auf den Piratenkarten gespeichert. Am 21. Januar, dem Sonntag vor dem Super-Bowl, dem Mega-Fernseh ereignis in Nordamerika, verschickte DirecTV die letzte Nachricht, die den Virus aktivierte. Rund 98 Prozent der Piratenkarten wurden so ausgeschaltet. Doch nur drei Wochen später, am 6. Februar 2001, stellten Hacker eine »Reparatursoftware« ins Netz. Vgl. Christiane Schulzki-Haddouti, Virenattacken – Lehrstücke und Abwehrwaffen aus Firmensicht, in: VDI-Nachrichten, 12. 10. 2001, S. 13.

- 27 Herbert Kubicek, Von der Angebots- zur Nachfrageförderung, in: Blätter für deutsche und internationale Politik, Nr. 9, 1998, S. 1093–1104.
- 28 Ute Bernhardt/Ingo Ruhmann, Informations- und Kommunikationstechnologie-Politik 1995–1998, Studie, Bonn 1995; Dies., Zukunft der IT-Politik, in: telepolis, 15. 10. 1998, <http://www.heise.de/tp/deutsch/inhalt/te/1593/1.html>