ICANN - Bin ich schon drin?

Bei Schlemihl war die Sache ganz einfach. Er hatte einen Schatten, der entstand, wenn die Sonne auf ihn schien. Dieser Schatten war sehr schön und fiel klar umrissen von seinen Füßen bis zur nächsten Hauswand. Eines Tages kam dieser Fremde, ein teuflischer Geselle wie jeder weiß, und kaufte ihm seinen Schatten ab. Nun mußte Schlemihl ohne Schatten leben, denn es war der einzige, den er je besessen hatte. Doch leider sind die Dinge nur im Märchen so einfach und so klar. Wer heutzutage seinen Schatten verkaufen will, steht vor unzähligen Schwierigkeiten. Sie machen sich bereits bemerkbar, wenn ein einfaches Angebot zum Schattenkauf formuliert werden soll. Denn es müßte alle essentialia negotii des Vertages enthalten, so u.a. den Gegenstand des Kaufes. Das kann natürlich ganz einfach der Sonnenschatten sein. Aber daneben gibt es ja noch den Datenschatten, genaugenommen mehrere verschiede Datenschatten und hier wird es nun schon schwieriger. Es fragt sich, wieviele Datenschatten es sind, wer für sie verantwortlich ist, wo sie liegen, wer über sie verfügt, wie breit sie sind, wie wahrhaftig man jeweils abgebildet wird ... .

A. Wer für die Entstehung des Schattens verantwortlich ist

I. Staat

Es muß unterschieden werden, ob die Entstehung des Schattens auf staatlichem oder privatem Handeln beruht, da beides verschiedenen rechtlichen Anforderungen unterliegt. Der Staat erhebt schon seit grauen Vorzeiten Daten von seinen Untertanen oder heute Bürgern; nur hat er in der heutigen digitalisierten Welt umfangreichere Möglichkeiten dazu. Schurken können einfacher abgehört und überwacht werden, bei Bedarf hilft eine Gendatei sie zu überführen. Und falls ein ganz Cleverer auf Hawai zwischen Blumenmädchen Zuflucht sucht, wird sofort Europol eingeschaltet. Der brave Bürger kann sich dann über den Erfolg der Staatsorgane freuen. Oder aber er ist entsetzt, angesichts dieser umfangreichen Möglichkeiten Daten zu erheben und aufs schnellste weiterzuleiten. Im schlimmsten Falle empfindet er es als unerträgliche Bedrohung seiner Persönlichkeit, im juristischen Sinne als (Grundrechts-) Eingriff. Aber die rechtlichen Fragestellungen, die sich daraus ergeben, sind noch lange nicht so erstaunlich und neuartig, wie die sie hervorrufende moderne Technik mit ihren fast unbegrenzten Möglichkeiten. Denn es stehen sich ganz klassisch Staat und Bürger gegenüber. Zwischen ihnen gelten die althergebrachten Regeln *des Grundgesetzes*: daß sich der Bürger nicht gegen jede bloße hoheitliche Belästigung zur Wehr setzen kann (Eingriffserfordernis) und daß der Staat die Freiheit seiner Bürgern grundsätzlich nur in gesetzlich geregeltem und verhältnismäßigem Umfang beschränken darf. Auch die neuen Maßnahmen selbst können teilweise auf traditionelle staatliche Vorgehensweisen zurückgeführt werden. So ist die Videoüberwachung (ohne Aufzeichnung) eines Platzes im wesentlichen das Gleiche, wie ein Polizist der höchstpersönlich auf diesem Platz Streife geht. Natürlich kann man sich fragen, ob vorbeugende, nach möglichen Gefahren Ausschau haltende Streifengänge bereits einer Ermächtigung durch Gesetz bedürfen. Anders mag man das dann bei der grenzenlosen Videoüberwachung einer ganzen Stadt sehen, bei Video*aufzeichnungen* oder, sofern es einmal schnell genug zum praktischen Einsatz ist, bei dem laufenden Abgleich der Videobilder mit visuellen Verbrecherdateien. Die Antwort auf solche Fragen ergibt sich aus schon bestehenden Überlegungsmodellen. So muß immer wieder überprüft und hinterfragt werden, wann ein Grundrechtseingriff und wann eine bloße Belästigung vorliegt; inwiefern

bestehende Ermächtigungsgrundlagen ausreichen und was als verhältnismäßig anzusehen ist. Im Rahmen einer Verhältnismäßigkeitsprüfung muß abgewogen und bewertet werden, ob der Staat mit seiner Maßnahme nicht über das selbstgesetzte Ziel hinausgeschossen ist. Das Filmen einer gesamten Stadt wäre zum Beispiel sowohl zur Abwehr von Gefahren als auch zur Verfolgung von Straftätern unverhältnismäßig. Gleiches würde für eine dazu ermächtigende Norm gelten. Insgesamt dürfen die Grundrechte der betroffenen Bürger niemals aus den Augen verloren werden. Sie müssen mit ihrem Schutzbereich stets anhand des konkreten Falls (neu) bestimmt werden. Dabei kann das Grundrecht in seinem Geltungsgehalt und -umfang hinterfragt und dann eine (u.U. neue) Wertung getroffen werden. Eine Möglichkeit, die sich nicht nur beim Einsatz neuer technischer Methoden, sondern bei jeder hoheitlichen Maßnahme ergibt.
Angesichts dieser ganzen Bewertung und Abwägung, die den Juristen in der täglichen Arbeit allerdings nicht zum Gähnenm, sondern zur ständigen Kritikbereitschaft verleiten sollte, drängt sich als wesentliche Grundfrage auf, ob man nicht nach einem Grundrechtsverständnis und also einem Staat-Bürger-Verständnis mit etwas festeren Konturen trachten sollte.

II. Private

Beim Austausch von E-Mails, Verbreiten von Internetseiten und sonstigen Online-Diensten stehen sich Privatpersonen gegenüber, die jeweils das Entstehen und Verbreiten eines Datenschattens beeinflussen.[1] Die dazu vorhandenen Möglichkeiten reichen vom einfachen Abfragen persönlicher Daten über gefährliche Netz-Würmer bis hin zu unerkannten Cookies; Bezeichnungen wie Mail-bombing, trojanisches Pferd[2], Viren und DNS-Manipulation schreien geradezu danach, den digitalen Krieg ausrufen zu lassen. Unfaßbar denkt man und fragt sich, ob der friedliche Internet-Nutzer nicht vor solchen Angriffen geschützt werden muß. Das würde aber nichts anderes heißen, als daß ein Individuum vor dem anderen geschützt werden soll. *Inwieweit* sich der Staat (hier) in Privatangelegenheiten einmischen darf oder sich ihrer gar annehmen muß - darüber sind sich sowohl die Internet-Freaks als auch die Juristen nicht einig. Das Bundesverfassungsgericht aber weiß ganz sicher: der Staat hat dafür zu sorgen, daß die Grundrechte in gewisser Weise auch zwischen Privaten zur Geltung kommen.[3] Das ist den Hütern der Verfassung immer dann aufgefallen, wenn es um Leben und Gesundheit ging, zum Beispiel beim Bau von Atomkraftwerken. Daher soll sich aus den Grundrechten eine gewisse Schutzpflicht des Staates insbesondere vor technischen Risiken ergeben, wobei stets ein bestimmtes Restrisiko hinzunehmen sei[4]. Grundsätzlich kann der Staat also verpflichtet sein, die Einhaltung von Grundrechten auch durch Private zu gewährleisten.

1. Pflicht zum Grundrechtsschutz auch in der Netzwelt?

Aber gibt es eine solche Schutzpflicht auch im Rahmen der Netzwelt? Kann das Internet als risikoreiche Technik betrachtet werden? Es sind kaum Möglichkeiten denkbar, wie jemandem allein durch die Nutzung des Internet ein irreparabler Schaden an Leben oder Gesundheit entstehen soll. Denn hier geht es allein um den Transfer von verschiedensten Daten. Und es kann auch in unserer Informationsgesellschaft nicht behauptet werden, daß ein Datenschatten - seine Existenz oder seine Manipulation - in irgendeiner Weise unmittelbar mit dem physischen und psychischen Wohlergehen zusammenhängt.
Etwas anderes mag für den Fall gelten, daß zum Beispiel die Daten eines Krankenhauscomputers willkürlich vertauscht und die Patienten dadurch fehlerhaft versorgt werden. Diese Möglichkeit basiert zwar zur Zeit lediglich auf der nicht nachprüfbaren Behauptung einiger Hacker, ist aber nicht von vornherein auszuschließen. Sehr kritisch muß auch ein, durch das Internet ungemein erleichtertes, Delikt beobachtet werden, daß direkt die Existenz des Opfers gefährdet. Gemeint ist der allein in den USA aufgetretene (und mögliche) Diebstahl einer bestimmten fremden Identität, indem sich der Täter nahezu des gesamten Datenschattens seines Opfers bemächtigt.
Eher ist hier das ebenfalls aus dem Grundgesetz abgeleitete *Recht auf informationelle Selbstbestimmung* (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) berührt. Es umfaßt unter anderem das Recht des Einzelnen, über "unbegrenzte Erhebung, Speicherung, Verwendung und

---

[1] Die Möglichkeit, daß auch öffentliche Stellen über das Internet kommunizieren oder dort auftreten soll hier nicht weiter vertieft werden, da sie dann den gleichen Regeln, wie jeder private Nutzer unterliegen bzw. sich die Fragestellung größtenteils an II. annähert.
[2] Gut erklärt vom Caos Computer Club (https://www.ccc.de/faq_2.html#trojan).
[3] So seit BVerfGE 7, 198 (204f., 207) Lüth-Urteil; B. Pieroth/B. Schlink, Grundrechte, Staatsrecht II, 15. Aufl. 1999 Heidelberg, Rn. 81.
[4] BVerfGE 49, 89 (143); 53, 30 (58f.); 72, 300 (316); 65, 1 (42 ff.).

Weitergabe seiner persönlichen Daten"[5] selbst zu entscheiden. Unbestritten kann allein im Rahmen einer einzigen Internet-Sitzung an diesem Recht ein *irreparabler Schaden* für die betreffende Person entstehen, indem Informationen über das Nutzerverhalten oder gar persönliche Daten registriert werden.
Sehr beliebt ist zur Zeit das Hamstern von Informationen mittels Bannerwerbung: Dem Internet-Nutzer weht so eine Art Fahne in die obere Bildschirmhälfte, um für irgend etwas zu werben, ohne daß er sich dagegen ernsthaft wehren könnte. Dabei wird meist unbemerkt eine kleine Datei auf den Rechner installiert, sogenannte Cookies. Sie speichern die verschiedensten Nutzerdaten und können dann von ihrem Urheber (aus)gelesen werden. Ein werbender Banner ist noch eine Spur trickreicher und ermöglicht es, auch Informationen aus bereits vorhandenen, fremden Cookies abzuzweigen. Wer sich dann mit seinen persönlichen Daten beispielsweise bei einem Email-account anmeldet, hat bereits einen Datenschatten erzeugt. Dieser kann, je nach Vorhaben und Phantasie, mit anderen bereits vorhandenen Informationen über den Nutzer kombiniert werden. Verwendet man Angaben aus einer Internet-Bestellung von Kleidung, sind auch schon die intimsten Details wie Schuhgröße und Brustumfang einer konkreten, identifizierbaren Person bekannt. Hier kann von Selbstbestimmung über persönliche Daten nicht mehr die Rede sein. Und unzweifelhaft ist auch eine *Weiterentwicklung* in diese Richtung *nicht beherrschbar*.[6] Reicht das aus, um eine staatliche Pflicht zum Schutz des Rechts auf informationelle Selbstbestimmung, zum staatlich gewährleisteten Datenschutz anzunehmen? Jedenfalls nur, wenn und soweit ein solcher Schutz überhaupt realisierbar ist. Tatsächliche und rechtliche Grenzen ergeben sich hier aus der Eigenart der Netzwelt.

[5] BVerfGE 65, 1 (43).
[6] Zu diesen Kriterien siehe B. Pieroth/B. Schlink (Fn.3), Rn. 92.

2. Recht auf informationelle Selbstbestimmung versus Informationsfreiheit

So ist es kaum möglich, Regelungen zum Schutz persönlicher Daten durchzusetzen, ohne in den Fluß der Daten einzugreifen, ihn zumindest zu behindern. Das widerspricht nicht nur der oberste Prämisse des Internet - *"Informations wants to be free."* Man befindet sich dadurch auch im Einflußbereich der grundgesetzlichen Informationsfreiheit (Art. 5 Abs. 1 S. 1 GG), die hier dem Datenschutz und damit dem Recht auf informationelle Selbstbestimmung gegenübersteht. Zwischen diesen beiden Fronten kann die Pflicht des Staates angesiedelt werden, ein geregeltes Wirtschaftsleben zu ermöglichen. Auf das Internet bezogen, bedeutet das, Grundlagen für den Handel und die Geschäftsabwicklung im Netz zu schaffen. Dazu bedarf es einerseits eines gut funktionierenden, also relativ freien Datenflusses und andererseits des Datenschutzes. So bleibt es bei der Frage, ob und wieweit das Recht auf informationelle Selbstbestimmung zu Lasten der Informationsfreiheit geschützt werden darf. Dem Datenschutz als Ausprägung des Rechts auf *informationelle Selbstbestimmung* wird, nicht nur vom Bundesverfassungsgericht, ein sehr hoher Rang eingeräumt.[7] Und zur Zeit wird ihm vor allem für den privaten Internet-Nutzer Bedeutung in "besonders hohem Maße" beigemessen.[8] Um die *Informationsfreiheit* ist man dagegen nicht so besorgt. Dabei ist sie doch nach dem Grundgesetz von gleichem Rang und auch im täglichen Leben von gleicher Wichtigkeit. Denn die Information und der freie Zugang zu ihr gewinnt mehr und mehr an Bedeutung. Immerhin nennen wir unsere Epoche Informationszeitalter. Ein Ansteigen der Informationsmenge insgesamt hat nun einmal zwangsläufig auch ein Ansteigen der verfügbaren Informationen über einzelne Individuen zur Folge. So wurde auch schon erkannt, daß mit Zunahme der verschiedensten Medienarten und der wachsenden Masse verfügbarer Daten ein Recht auf gleichen (u.U. geförderten) Informations*zugang* bestehen muß. Daher relativiert sich das Recht auf informationelle Selbstbestimmung in dem Maße, indem der Informationsgrad über alles und jeden steigt. Das sollte man vor allem bei der Abwägung und Gegenüberstellung der beiden Grundrechte nicht vergessen, die das Bundesverfassungsgericht letztendlich auch neben der Sonderrechtslehre verlangt. Daher muß über ein *verändertes Verständnis der (Informations-) Grundrechte* und der Rechtsbegriffe nachgedacht werden, aus der Sicht einer digitalen vernetzten Gesellschaft. Denn wir haben die Entwicklung des Internet gerade dem freien Fluß sämtlicher Informationen zu verdanken und auch weitere technische Entwicklungen werden darauf angewiesen sein. Aus dieser Sicht relativiert sich die Pflicht zum Schutz der informationellen Selbstbestimmung. Vielleicht kann ja der mangelnde Datenschutz im Internet als so etwas wie ein Restrisiko hingenommen werden - als Preis für die verschiedenen Vorteile und Annehmlichkeiten. Ein *umfassende* Pflicht des Staates, *vollständigen* Datenschutz im Internet zu gewährleisten, kann jedenfalls nicht festgestellt werden.

---

[7] BVerfGE 65, 1 (42).

[8] H. Möller, Gesetzliche Vorgaben für anonyme E-Mail, DuD 2000, S. 6; vgl. auch P. Schaar, Cookies: Unterrichtung und Einwilligung des Nutzers über die Verwendung, DuD 2000, S. 275 (276).

3. Tatsächliche Grenzen

Trotzdem existieren bereits umfangreiche gesetzliche Regelungen zum Schutz der informationellen Selbstbestimmung, die in der Netzwelt zur Geltung kommen sollen.[9] Allerdings stoßen solche rechtlichen Maßnahmen an technische Grenzen. Nicht alles was verboten wird, läßt sich auch durchsetzen. Für verschiedene gesetzgeberische Ziele fehlen noch die technischen Möglichkeiten. Zudem sind der staatlichen Gewalt (sowohl rechtlich als auch tatsächlich) dort Grenzen gesetzt, wo es um Aktivitäten ausländischer Netzteilnehmer geht. Aus den gleichen Gründen ist es auch problematisch, eine Pflicht des Staates anzunehmen, datenschützende Technik zu entwickeln. Dadurch würde nicht nur der Spielraum des Staates eingeschränkt, zu entscheiden, *wie* er seiner Schutzpflicht nachkommen will. Sondern man würde dabei wohl ebenfalls an technische Grenzen stoßen, zumindest aber beim Einsatz an die nationalen Grenzen. Also sind der staatlichen Schutzpflicht Schranken gesetzt, da der Staat zu zu nichts verpflichtet sein kann, wozu er technisch nicht in der Lage ist.

4. Zu wenig Grundrechtsschutz im Internet?

Ist der internetnutzende Bürger dann aber noch ausreichend in seinen Grundrechten geschützt oder ist dieser Schutz gefährdet? Wo keine Schutzpflicht besteht, kann der Staat auch nicht zu wenig Schutz bieten. Ein Mindestmaß an Grundrechtsgewähleistung ist durch die bereits vorhandenen gesetzlichen Regelungen bereits gewahrt. Daher liegt auch keine Aushöhlung der Grundrechte vor, wenn ein Bürger durch einen anderen außerhalb der unmittelbaren Grundrechtsgeltung in seinem (Persönlichkeits-) Recht beeinträchtigt wird. Natürlich kann sich der Staat trotzdem entschließen, die Bürger positiv zu schützen, insbesondere durch den Erlaß entsprechend weitgehender Gesetze. Allerdings sollte der Datenschutz im Internet behutsam und restriktiv gehandhabt werden. Das heißt, er darf nicht zur Inhaltskontrolle mißbraucht und damit einseitig zu Lasten der Informationsfreiheit betrieben werden. Zumal eine Regelungsflut, die an der Lebenswirklichkeit vorbeigeht, in keinem Bereich ein Gewinn ist. Am besten wäre es, wenn der Schutz der informationellen Selbstbestimmung durch die Netzwelt selbst gewährleistet würde. Denn nicht nur der Einflußbereich des Grundgesetzes, sondern auch die Regelungen der anderen Staaten sind national begrenzt. Daher können die Gesetze eines einzelnen Staates allein keinen Datenschutz im Internet gewährleisten; sie wären ein Tropfen auf den heißen Stein. Die Staaten könnten sich natürlich zusammenschließen, um einheitlich den Schutz der informationellen Selbstbestimmung durchzusetzen. Daß ein entsprechender Konsens entsteht, ist aber, wenn schon auf europäischer Ebene problematisch, nicht sehr wahrscheinlich. Daher sollten die Fähigkeiten des Internet zur Gewährleistung von Datenschutz genauer betrachtet werden. nichts verpflichtet sein kann, wozu er technisch nicht in der Lage ist.

[9] Beispielsweise das Telekommunikationsgesetz, das Teledienstegesetz, der Staatsvertrag über die Mediendienste der Länder.

B. Kann ein effektiver Schutz der informationellen Selbstbestimmung eigenständig durch die Netzwelt gewährleistet werden?

- Eine Vision ? -

Doch was ist das Netz, das Internet eigentlich? Natürlich weiß jeder, daß man darunter das gesamte, weltweit durch Datenautobahnen verbundene Informationssystem versteht, mit all seinen einzelnen verschiedenen Kommunikationsebenen. Seine rechtliche Qualität zu umreißen, ist schon komplizierter. Das Internet ist unabhängig von einer nationalen Hoheit entstanden, funktioniert unabhängig von ihr und wird grundsätzlich auch weiterhin unabhängig von nationalen Einflüssen bestehen. Aufgrund dieser Autonomie gegenüber staatlicher Autorität und der völkerrechtlichen Verständigung zwischen den verschiedenen Staats-Hoheiten scheint es nicht ausgeschlossen, dem Internet gewissermaßen eigene Souveränität zuzusprechen. Recht naheliegend erscheint bei einem weltübergreifenden Netz auch der Gedanke an Supranationalität (im juristischen wie im unjuristischen Sinn). Dem steht jedoch ebenfalls die Unabhängigkeit des Internet von nationaler Hoheit entgegen. Zudem kann es in keiner Weise *über* den Staaten angesiedelt werden, wie das Wort "supranational" nahelegt. Das wird insbesondere an der Funktionsweise und Technik des Internet deutlich. Dieser liegt *kein global einheitliches System* zugrunde, sondern eine Ansammlung verschiedener technischer Voraussetzungen, die den noch so uneinheitlichen Computern und Netzwerken der Welt Datenaustausch und damit Kommunikation ermöglicht.[10] Das Organisieren dieser technischen Grundlagen des Datenaustauschs hat sich nun in der Form des Internet institutionalisiert. So existiert zwar eine staatenübergreifende Kommunikation, aber kein staatenübergreifendes System. Folglich kann man kaum von Supranationalität sprechen. Treffender scheint dann schon der Gedanke einer eigenen Staatlichkeit des Internet. Mit etwas Phantasie lassen sich auch Ansätze für die drei wesentlichen Elemente des Staates finden: Staatsvolk, Staatsgebiet und Staatshoheit.[11]

I. Die Netzbürger als Staatsvolk

Als Staatsvolk kommen die Internet-Nutzer in Betracht, die in Insiderkreisen bereits sehr bezeichnend *Netizen* - Netzbürger genannt werden.[12] Diese *internet community* bildet natürlich keine homogene Masse. Sondern sie verfolgen die verschiedensten Interessen, schließen sich in entsprechenden Gruppen[13] zusammen und nutzen verschiedene Kommunikationsebenen (Newsgroups, Diskussionsforen, Email, Mailinglisten, Chat Foren,

---

[10] P. G. Mayer, Das Internet im öffentlichen Recht, 1999 Berlin, S. 31 (I. Technik des Internets).

[11] vgl. auch "L'état est un droit gouvernement de plusieurs mesnages et de ce que leur est commun avec puissance souveraine" (Unter dem Staat versteht man die am Recht orientierte, souveräne Regierungsgewalt über eine Vielzahl von Haushaltungen und das, was ihnen gemeinsam ist.), J. Bodin, Sechs Bücher über den Staat, Übersetzt und mit Anmerkungen, 1981 München, Buch I, 1. Kapitel, S. 98.

[12] Dies sind nach Angaben des Computer Industry Almanac bereits mehr als 259 Millionen weltweit (http://www.c-i-a.com/199903pcuse.htm).

[13] Wie z.B. im Chaos Computer Club e.V. "Der Chaos Computer Club ist eine galaktische Gemeinschaft von Lebewesen, unabhaengig von Alter, Geschlecht und Rasse sowie gesellschaftlicher Stellung, die sich grenzueberschreitend fuer Informationsfreiheit einsetzt und mit den Auswirkungen von Technologie auf die Gesellschaft sowie das einzelne Lebewesen beschaeftigt und das Wissen um diese Entwicklung foerdert. Der CCC setzt sich fuer ein Menschenrecht auf zumindest weltweite, ungehinderte Kommunikation ein. Dies schliesst natuerlich technische Forschung, Entwicklung von entsprechenden technischen Hilfsmitteln und die Diskussion entsprechender technischer Sachgebiete sowie oeffentliche Demonstrationen mit ein." (https://www.ccc.de/index.html).

etc.) mit jeweils eigenen Kulturen. Damit unterscheiden sich die *Netzbewohner*[14] kaum von anderen Staatsbürgern. Auch der Einwand, daß ein Staatsvolk einigermaßen bestimmbar sein muß, läßt sich ausräumen, indem man auf die Registrierung von Domain-Namen oder IP-Adressen abstellt. Die Netizen müßten sich dauerhaft einer gemeinsamen Ordnung unterworfen haben. Als solche kann die Strukturierung des Netzes betrachtet werden und die Regeln, die erfüllt werden müssen, um das Funktionieren und die Stabilität des Netzes zu gewährleisten.

II. Der Cyberspace als Staatsgebiet

Um ein Staatsgebiet für die *Netizen* zu finden, hilft ein Blick in die Geschichte der Staatslehre weiter: So definierte sich der Staat in der Antike als eine Bürgergemeinde, deren Identität nicht notwendig an den Wohnsitz gekoppelt ist.[15] Auch im Mittelalter gab es noch den Personalverbandsstaats mit persönlichem Gefolgschaftsverhältnis.[16] Das Staatsgebiet wurde erst Voraussetzung eines Staates, als die Gebiete einigermaßen abgesteckt waren und zu jeder Gefolgsmannschaft eine bestimmte Fläche zu gehören pflegte - als der Begriff Vaterland geprägt wurde. Warum soll also nicht wieder auf das Erfordernis eines geographisch umgrenzten (territorialen) Staatsgebiets verzichtet werden können? Auch die heutige Bezeichnung des *Wesens* eines Staatsgebiets scheint ihrem *Wortlaut* nach nicht dagegen zu sprechen. Danach ist das Staatsgebiet der *räumliche* Geltungbereich, in dem sich die Hoheitsgewalt eines Staates verwirklichen kann. (Oder andersherum betrachtet, die Gebietshoheit ist Staatsgewalt unter dem Gesichtspunkt räumlicher Ausdehnung.[17]) Die nationalen Regelungen aber, die stets auch Ausdruck der jeweiligen nationalen Staatshoheit sind, entfalten in der Netzwelt oft keine oder nicht ihre volle Wirkung. Die Geltung der nationalen Gewalt stößt also auf gewisse Grenzen. Ein Grund dafür ist unter anderem die Losgelöstheit des Internet von traditionellen, rechtlichen Schlüsselbegriffen wie Person, Ort und Zeit.[18] Daher sollten diese Begriffe hinterfragt und eigene für die Netzwelt gültigen Lösungen gefunden werden. Dann erscheint es nicht mehr fernliegend, andere traditionelle rechtliche Bezeichnungen ebenfalls zu überdenken und den räumlichen Geltungsbereich einer Hoheitsmacht nicht mehr allein geographisch zu verstehen, sondern auch digital virtuell - als Cyber*space*. Will man sich dagegen an das herkömmliche Verständnis von einem Staatsgebiet halten, sieht es nicht gut aus für die Netzbewohner. Dann ist es auch bedeutungslos, ob das Fürstentum Sealand sein Territorium dem Internet zur Verfügung stellt, da ihm ebenfalls ein herkömmliches Staatsgebiet abgesprochen wird.[19]

---

[14] A. Müller-Maguhn in C. Ahlert, Andy Müller-Maguhn - Ein Hacker will Direktor werden, SPIE-GEL ONLINE vom 24.08.2000 (http://www.spiegel.de/netzwelt/politik/0,1518,90471,00.html).
[15] G. Jellinek, Allgemeine Staatslehre, 2. Aufl. 1905 Berlin, S. 359.
[16] K. Stern, Das Staatsrecht der Bundesrepublik Deutschland, Bd. I, 2. Aufl. 1984 München, § 7 I2.
[17] K. Stern (Fn. 16), § 7 I3.
[18] vgl. dazu T. Hoeren, Internet und Jurisprudenz - zwei Welten begegnen sich, NJW 2000, S. 188.
[19] vgl. M. Sontheimer, Prinzen und Cyperpunks, DER SPIEGEL, 25/2000 i.V.m. VG Köln, DVBl. 1978, S. 510.

III. Eine Staatsgewalt in der Netzwelt?

Als letztes muß untersucht werden, ob es in der Welt der Datenautobahnen so etwas ähnliches wie eine Staatsgewalt gibt, die absolut unabhängig ist und frei in ihren Entscheidungen.[20] Sie umfaßt die gesetzgebende sowie in deren Folge die vollziehende und rechtsprechende Gewalt.

1. Regelgebung / Gesetzgebung

Fest steht zunächst, daß im Internet bereits konkret definierte Regeln existieren, die von allen Beteiligten befolgt werden müssen. Sonst könnte ein globales Netz nicht funktionieren. Der Schwerpunkt liegt hier unbestritten bei den *technischen Standards*, die die Modalitäten des Datenaustauschs festlegen. Für deren Entstehung hat sich ein strukturiertes und transparentes[21] Normierungsverfahren herausgebildet.[22] Die verschiedenen Zuständigkeiten und Rechte, insbesondere die Entscheidungskompetenzen der einzelnen Gremien werden in diesem Verfahren streng getrennt. So obliegt die Entwicklung neuer technischer Regelungen einem anderen Gremium[23] als die abschließende Beschlußfassung[24] darüber, ob ein Entwurf letztendlich Gültigkeit erlangen soll. Während dieses Prozesses müssen sich die zukünftigen Regelungen auf verschiedenen Stufen praktisch bewähren. Dabei werden sie ständig diskutiert und hinterfragt. Weil es keinen *legitimierten* Gesetzgeber gibt, wie man ihn aus der realen Welt kennt, da die Zusammensetzung der Gremien auf ihrer Entstehungsgeschichte und fast ausschließlich auf Sachverstand beruht, ist es sehr wichtig, einen breiten Konsens für die künftigen Standards zu finden. Denn die technischen Normen werden nur dann *verbindlich*, wenn sie funktionieren und sich ihr deshalb ein Großteil der Netizen freiwillig unterwirft. Erst dann (und nur solange) ist sie gültig. Legitimation durch *rough consensus and running code!?* Von den relativ verbindlichen technischen Normen der Datenübertragung sind solche Regeln zu unterscheiden, die den *Inhalt* der Übertragung betreffen. Dafür hat sich noch kein gleichermaßen formalisiertes Normgebungsverfahren im Internet entwickelt.[25] Deshalb existieren auch keine Regelungen mit einem den technischen Standards vergleichbaren Gültigkeitsanspruch.[26] Zudem hängt die Verbindlichkeit sozialer und moralischer Umgangsformen in wesentlich größerem Maße als bei technischen Regeln von der netzweiten Akzeptanz ab. Und da das gleichzeitig weltweite Akzeptanz bedeutet, ist es ungleich schwieriger als im technischen Bereich den kleinsten gemeinsamen Nenner für *notwendige* soziale Spielregeln zu finden. Ein gutes Beispiel hierfür war die Verbannung "rechter" Propaganda-Seiten von deutschen Servern, die einen Aufschrei der freiheitsliebenden Amerikaner nach sich zog. Sie fanden es völlig unverständlich, daß das Recht auf freie Meinungsäußerung in Deutschland auf solch drastische Weise eingeschränkt ist. Dennoch ist sich eine Vielzahl von Internet-Nutzern über wesentliche Punkte einig. Diese Grundregeln werden *Netiquette* genannt. Sie umfassen Fragen der allgemein- bzw. netzverträglichen

---

[20] vgl. J. Bodin (Fn. 11), Buch I, 8. Kapitel, S. 205 ff.
[21] Zu dieser Ansicht gelangt P. G. Mayer (Fn. 10), S. 75, die gewiß nur für Netizen gelten kann.
[22] Hier wird das Verfahren der ISOC zugrundegelegt. Es soll aber nicht unterschlagen werden, daß das Standardisierungsverfahren i.R.d. W3C bei vorliegender Betrachtung weniger ergiebig wäre.
[23] Internet Engineering Task Force (IETF).
[24] Internet Engineering Steering Group (IESG).
[25] Vgl. dazu und zu näheren Bemühungen in diese Richtung M. Recke, FS II 97-104, Identität zu verkaufen, Probleme und Entwicklunsoptionen des Internet Domain Name Service (DNS); Kapitel: Wo policy durch die Hintertür hereinschleicht ... (http//:duplox.wz-berlin.de/texte/dns/node6. html).
[26] P. G. Mayer (Fn. 10), stellt fest, daß es bereits "wenige geschriebene Regeln" über die Inhalte von Internet-Kommunikation gibt (S. 60) und "nur teilweise" - aber bereits vorhandene Kodifikationen sozialer Verhaltensnormen. Leider wird dazu keine Quellenangabe bzw. kein sonstiger genauerer Anhaltspunkt gegeben.

Nutzung des Internet bis hin zu sozialen und moralischen Anforderungen an die Nutzung, wie zum Beispiel die Unverletzlichkeit der Privatsphäre bzw. den Schutz privater Daten. Ihr Vorteil gegenüber unseren staatlichen Normen ist, daß sie immer wieder diskutiert und hinterfragt werden und somit stets auf einem aktuellen Konsens beruhen. Ihr Nachteil ist die fehlende Verbindlichkeit. Setzt aber das Bestehen eines Staates überhaupt soziale Normen voraus, die so verbindlich wie unsere heutigen Gesetze sind und nicht lediglich auf gegenseitiger Anerkennung beruhen? Diese Frage soll hier nicht weiter erörtert werden und mag den Philosophen überlassen bleiben. Gleiches gilt für die Überlegung, daß das Funktionieren der digitalen Kommunikation zu allererst von der Einhaltung der technischen Regeln abhängt, so wie die sozialen Regeln der realen Welt das Funktionieren der gesellschaftlichen Kommunikation ermöglichen.[27] Dies legt den Schluß nahe, daß soziale Regeln in der realen Welt eine ganz andere Funktion und Bedeutung haben als im Internet. Man könnte die grundsätzlich verbindlichen technischen Regeln der Netzwelt den sozialen der Realwelt gegenüberstellen. Und man müßte man sich nicht daran aufhalten, daß es im Internet keine Regelung hinsichtlich übertragener Inhalte gibt. Hier baut sich aber ein weiteres Problem - ein weiterer Unterschied auf: Die verbindlichen Regeln sind in der realen Welt nur die Voraussetzung für das reibungslose *Funktionieren* der Kommunikation in der Gesellschaft, während die verbindlichen Regeln des Internet (die Technik) gleichzeitig die Voraussetzung für die *Existenz* dieser Kommunikation, also der Netz-Gesellschaft selbst sind. Festzuhalten bleibt, daß das Internet über eigene feste Regeln verfügt - mögen sie auch nur technischer Natur sein - die durch keine übergeordnete Stelle bestätigt werden müssen.[28] Sie ergehen in einem formalisierten Verfahren, daß funktionierende Strukturen einer Regelsetzungenthält, die sich der staatlichen Gesetzgebung annähern. Zudem werden auch grundrechtsähnliche Rechte anerkannt, insbesondere das in diesem Bereich wesentliche Recht auf den Schutz persönlicher Daten.

[27] Dabei darf natürlich nicht vergessen werden, daß auch "unsoziale" Verhaltensweisen (Mißbrauchsformen) die Kommunikation im Netz erheblich behindern können.
[28] vgl. J. Bodin (Fn. 11), Buch I, 8. Kapitel, S. 207.

2) Exekutive

Weiterhin müßte es eine Ausführende Gewalt im Internet geben. Was aber deren Bestandteile und Voraussetzungen sind, ist keiner Definition zu entnehmen.[29] Verwaltung im weiteren Sinne läßt sich je nach Staatsform und ihrer Funktion innerhalb der jeweiligen Gesellschaft anders fassen.[30] Daher soll hier nur auf die heute wesentlichen Elemente eingegangen werden.

a) Gesetzesvollzug
Zunächst verbindet man mit Exekutive als der vollziehenden Gewalt den *Gesetzesvollzug.* Nach obigen Ausführungen kommt im Internet vor allem die Durchsetzung technischer Standards in Betracht. Als Beispiel dafür kann die technische Umstellung[31] von 1983 im APRANET, dem wesentlich überschaubaren Vorgänger des Internet, angeführt werden. Sämtlichen Nutzern wurde bereits einige Monate vorher durch zeitweilige "Abschaltung" der alten Regeln drastisch vor Augen geführt, daß sie von der Kommunikation ausgeschlossen sein werden, falls sie sich nicht den neuen Regeln unterwerfen.[32] Äußerst fraglich ist jedoch, ob eine solche Methode auch noch im viel weitläufigeren Internet möglich wäre. Denn das ist nicht nur von vornherein auf Dezentralität und Delegation von Verantwortung ausgelegt. Sondern es hat zudem, wie jede andere riesige Verbindung auch, mit seiner unglaublichen Größe an Flexibilität eingebüßt. Der Vollzug der Netiquette scheitert bereits daran, daß er durch entsprechende Technik unterstützt werden müßte. Diese ist jedoch erst in eingeschränktem Maße vorhanden - soweit es überhaupt möglich ist, sie zu entwickeln. Mangelnde Durchsetzungsmöglichkeit der Netiquette und ihre Unverbindlichkeit stehen hier in gewisser Wechselwirkung. Persönlichkeits-, insbesondere Datenschutz kann somit auf dem derzeitigen Stand und ohne entsprechende Weiterentwicklung nicht durch die Netzwelt selbst mit der Wirkungskraft gewährleistet werden, die staatliche Regelungen in der realen Welt entfalten. Dabei darf man aber nicht vergessen, daß auch eine nationalstaatliche Regelung das technische Problem der Durchsetzung nicht behebt und stets hinter der Wirkung des Grundrechtsschutzes in anderen Lebensbereichen zurückbleiben muß.

b) Verwaltung im engeren Sinne
Verwaltung im engeren Sinne läßt sich ebenfalls nicht definieren.[33] In Bezug auf die *Tätigkeit* bezeichnet das Wort *Verwalten* das Organisieren von fremdem oder privatem Vermögen. Daraus wird abgeleitet, daß sich öffentliches Verwalten auf öffentliches Vermögen bezieht.[34] Das Internet als solches ist zwar für jeden offen. Denn eine Datenverbindung, die tatsächlich zum Internet gehört (und nicht nur wie ein Extra- oder Intranet einen beschränkten Zugang zu ihm hat), kann nicht für einzelne Teilnehmer auf bestimmten Strecken gesperrt werden. Aber die eigentlichen Datenautobahnen und Speicherplätze sind grundsätzlich Privateigentum und daher ist auch ihre Nutzung in keiner Weise öffentliches Vermögen. Das Augenmerk muß auf einen anderen Vermögenswert gerichtet werden, der einen immensen Machtfaktor darstellt: der *Domain Names Service (DNS)*. Die *Domains* bzw. die Internet-Adressen sind in ihrer konkreten Fassung stets nur einmal vorhanden und die besonders begehrten Namen sind begrenzt. Aber ist der Namensraum ein zu verwaltendes *öffentliches Gut?* Nach dem traditionellen Verständnis der Internet-Ordnung wurde er als eine *öffentliche Ressource*

---

[29] So für die Verwaltung im weiteren Sinn E. Forsthoff, Lehrbuch des Verwaltungsrechts, I. Band, Allgemeiner Teil, 7. Aufl. 1958 München Berlin, S. 1.
[30] Vgl. E. Forsthoff (Fn. 29), S. 2ff.
[31] Am 1. Januar 1983 wurde das APRANET-System der NCP-Protokolle auf TCP/IP umgestellt.
[32] V. Cerf, How the Internet Came to Be, 1997 (http://www.bell-labs.com/user/Zhwang/vcerf. html).
[33] H. Maurer, Allgemeines Verwaltungsrecht, 12. Aufl. 1999 München, § 1 Rn. 5-8.
[34] E. Forsthoff (Fn. 29), S. 2; H. Maurer (Fn. 33), § 1 Rn. 1.

betrachtet, die zur Aufrechterhaltung der Netzordnung verwaltet werden muß.[35] Allerdings entwickelte sich die *Network Solution Inc. (NSI)*, die Hauptkoordinatorin der amerikanischen Domains, von einem gemeinnützigen Verwalter zu einem wirtschaflichen Monopolisten, als sie Gebühren für die Registrierung und Verwaltung der Domain Names erhob.[36] Vor allem aber wurde ein Wandel der Domains vom öffentlichen Gut zu einer privatrechtlichen Position durch ihre Gleichsetzung mit (geschützten) Markennamen begünstigt. Dazu waren die Domains ursprünglich nicht gedacht gewesen, sondern eher als eine Art leicht zu merkender Anschlußnummern ohne jede handelsrechtliche Bedeutung. Nun aber macht sich wesentlich stärker bemerkbar, daß es im Internet einen bestimmten Namen nur einmal geben kann. Natürlich erstreckt sich Verwaltung gerade auf die koordinierte Verteilung einer *begrenzten öffentlichen Ressource*. Seitdem sich jedoch durch nationale Gerichte geurteilt wurde, daß sich markenrechtlicher Schutz auch auf das Internet erstreckt, ist es möglich Anspruch auf eine *bestimmte* Domain zu erheben. Das hat nicht nur zur Folge, daß das Recht der realen Welt einen wesentlichen Bereich der Netzwelt überlagert, ihn für sich reklamiert: Das ursprünliche Prinzip der Domain-Vergabe *"First come, first served"* gilt nicht mehr uneingeschränkt; Domain Names müssen als Markennamen geschützt werden. Sondern es scheint dadurch nicht mehr angebracht vom Namensraum als einer öffentlichen Ressource zu sprechen. In diese Richtung weisen auch die Bestrebungen, der NSI die Monopolstellung zu nehmen sowie die Registrierung der Domains zu kommerzialisieren und dem Wettbewerb zugänglich zu machen.[37] Demnach gäbe es nichts zu verwalten, also auch keine Verwaltung im engeren Sinn.

---

[35] M. Recke, FS II 97-104, Identität zu verkaufen, Probleme und Entwicklunsoptionen des Internet Domain Name Service (DNS); Kapitel: Aktuelle Probleme des DNS, Rechtsfragen des DNS, (http//:duplox.wz-berlin.de/texte/dns/node4.html).

[36] W. Kleinwächter, ICANN als United Nations der Informationsgesellschaft? Der lange Weg zu Selbstregulierung des Internet, MMR 1999, S. 452 (454).

[37] vgl. Domain Name Agreements between the U.S. Department of Commerce, Network Solutions, Inc. and the Internet Corporation for Assigned Names and Numbers (http://www.ntia.doc.gov/ntiahome/domainname/agreements).

c) Regierung
Aber was bedeutet es, wenn man zur Zeit ständig von ICANN[38], der Internet-Regierung, liest?[39] Zu deren demokratischer Wahl aufgerufen ist? Schließlich stellt man sich unter Regierung eine Verwaltung auf höherer Ebene vor. Gibt es also doch eine Internet-Verwaltung? *Aufbau, Funktion von ICANN* ICANN wurde als nicht gewinnorientierte Gesellschaft gegründet. Ihr obliegt es unter anderem, die Verwaltung der Internet-Adressen und des Domain Name System zu überwachen sowie das Netz funktionsfähig zu halten. Sie ist "global, netzwerkartig und nahezu basisdemokratisch organisiert".[40] So vertritt sie nicht nur kommerzielle Interessen, sondern soll auch weltweit die nichtkommerziellen Internet-Nutzer repräsentieren - mit durch demokratische Wahlen legitimierten Vertretern. Desweiteren sind Maßnahmen getroffen, ICANN vor einer Einflußnahme nationaler Regierungen (theoretisch auch der amerikanischen) zu schützen.[41] *Einwirkungsmöglichkeiten von ICANN* Die Organisation selbst beteuert, daß sie nur für technische Fragen zuständig sei, keine Regierungsmacht habe und daher auch keine demokratische Institution sei. Allerdings erinnert ihre Aufgabe, die Stabilität des Internet und des Domain Name System zu gewährleisten, stark an die Aussage, daß Verwaltung Tätigkeit des Staates zur Erfüllung seiner Zwecke ist[42] - zur Aufrechterhaltung der verschiedenen Funktionen, des Systems. Und es erscheint auch sehr verwunderlich, daß es demokratische Wahlen für eine nicht-demokratische Organisation geben soll. Auf keinen Fall aber kann die tatsächliche Macht geleugnet werden, die in der Entscheidungskompetenz über die Existenz des Einzelnen im Netz liegt. Auch politische und rechtliche Fragen, zum Beispiel inwieweit und wodurch die Privatsphäre der Netizens geschützt wird, können nicht *gegen* ICANN durchgesetzt werden. Denn die entsprechenden Lösungen müßten im Internet technisch realisiert werden (s.o.). Damit zeigt sich auch, daß ein einzelner Staat im Alleingang seinen Vorstellungen von Persönlichkeitsrecht und von Schutz der Privatsphäre im Internet nicht im Alleingang vollständig zur Geltung verhelfen kann. Insofern liegt in ICANN wirklich das Potential für eine weltweite Regierung des Cyberspace und vielleicht auch der Schlüssel zur Frage nach seiner Souveränität. Ob diese Anlagen genutzt und ausgebaut oder (wieder) an nationalen Regierungen abgegeben werden, liegt in der Zukunft.

3. Rechtschutz / rechtsprechende Gewalt

Ansätze für eine rechtsprechenden Gewalt kann man darin sehen, daß ICANN die *Uniform Domain Name Dispute Resolution Policy (UDRP)* errichtet hat, eine Schlichtungsstelle für Streitigkeiten über Domain Names mit festgelegtem Verfahren. Allerdings werden die Parteien von hier größtenteils an die nationalen Gerichte verwiesen, so daß in der Netzwelt selbst kein (ausreichendem) Rechtschutz besteht.[43] Natürlich ist es auch hier noch eine entsprechende Entwicklung der Netzgesellschaft möglich. Insgesamt betrachtet, lassen sich also alle drei klassischen Elemente des Staates zumindest ansatzweise in der Organisation der Internet-Gesellschaft finden. Allein die Rechtsprechung weist *zur Zeit noch* größere Defizite auf. Natürlich steht damit nicht fest, daß es sich hier um ein staatenähnliches Gebilde handelt, das Autonomie gegenüber anderen Staaten beanspruchen kann. Wesentlich ist aber, die Eigenständigkeit, Eigenwilligkeit und Einzigartigkeit dieses Gebildes zu erkennen und sich

---

[38] Internet Corporation for Assigned Names and Numbers.
[39] z.B. SPIEGEL ONLINE, http://www.spiegel.de (Stand: 20.09.2000); H. Schumann, Wettlauf der Wähler, DER SPIEGEL, 31/2000, S. 198.
[40] W. Kleinwächter (Fn. 36), S. 452.
[41] Näheres dazu bei W. Kleinwächter (Fn. 36), S. 452 (459).
[42] E. Forsthoff (Fn. 29), S. 2, 7.
[43] vgl. M. Ermert, Namenspatron, Die neue Internet-Domain-Verwaltung ist endgültig geklärt, c't 24/99, S. 48.

davon inspirieren zu lassen. Auch wenn also das Recht auf informationelle Selbstbestimmung und der Datenschutz zur Zeit nicht durch die Netzwelt selbst gewährleistet werden kann, sollte ein Ausbau der Staatsansätze nicht ausgeschlossen werden. Eine Entwicklung in diese Richtung zeichnet sich vielleicht schon mit der Etablierung von ICANN ab und mit den Anstrengungen, technische Möglichkeiten zur Verwirklichung sozialer Regeln zu finden.

C. Schlußfolgerungen

Was folgt nun für den Staat, der das Grundrecht auf informationelle Selbstbestimmung auch im Internet verwirklicht sehen will, aus diesen Überlegungen? Er sollte dieses Bestreben für den nationalen Bereich angehen, aber *(erstens)* insbesondere bei der Gesetzgebung wohlüberlegt verfahren und nur regeln, was auch wirklich technisch möglich und zudem mit der Struktur des Internet grundsätzlich vereinbar ist. Denn der Schutz des Persönlichkeitsrechts und der Privatsphäre muß auf jeden Fall auch in der Netzwelt gewährleistet sein. Doch es muß *(zweitens)* gefragt werden, wie weit dieser Schutz, der letztlich Datenschutz bedeutet, in einer Gesellschaft reichen kann, die in hohem Maße auf den freien Fluß von Daten angewiesen ist. Vielleicht ergibt sich aus der Sicht eines "globalen" Netizen ein ganz anderes Verständnis von Persönlichkeitsrecht und Privatsphäre. Und weil ein umfassender globaler Schutz letztendlich doch nur mit der Technik des Internet gewährleistet werden kann, sollte sich der Staat bemühen, *(drittens)* durch seine Regelungen die technische Entwicklung der Netzwelt nicht zu hemmen und sie *(viertens)* durch Engagement auf internationaler Ebene voranzutreiben. Vielleicht bringt dieses Vorgehen dem Staat noch weitere Vorteile und erleichtert ihm, einer anderen Aufgabe gerecht zu werden, die er zur Zeit sträflich vernachlässigt. Denn wenn die technische Entwicklung einmal Datenschutz unmittelbar durch die Netzwelt erlaubt, wäre dies der einzige und perfekte Schutz gegen staatliche Abhörmaßnahmen. Mancher Internet-Nutzer empfindet das militärisch angehauchte Echelon,[44] ein weltweites elektronisches Überwachungssystem oder Carnivor, das heimlich eingesetzte Email-Überwachungsprogramm des FBI, wesentlich bedrohlicher, als private und kommerzielle Bespitzelung. Hiergegen wird staatlicherseits nur schleppend vorgegangen und eine Grundrechtsbeeinträchtigung als ausgeschlossen betrachtet. Doch das Problem könnte sich eventuell gerade durch weniger Datenschutzregelungen für das Internet von selbst lösen ... So macht es aus nationalstaatlicher Sicht durchaus Sinn, die Staatsansätze im Internet zu fördern und darauf zu drängen, daß die Staatlichkeit des Internet erwachsen wird. *Letztendlich sollte man es wie Schlemihl halten. Man sollte über seinen eigenen Schatten springen und seinen (Daten-)Schatten für ein Paar Stiefel opfern, mit denen man sieben Meilen weit ausschreiten, die Welt umrunden und fortschrittlich Neues entdecken kann. Auch Schlemihl mußte dafür altes, gewohntes aufgeben. Er ging freiwillig das Risiko ein, daß er, je schneller er vorankam, immer weniger von sich selbst an einem Ort hinterließ, für den unbeteiligten Zuschauer immer konturenloser wurde. Und können wir heute nicht auch frei entscheiden, ob wir unseren (Daten-)Schatten fest an uns binden wollen oder ob wir voller Neugier das Internet mit seinen stündlichen Neuheiten erkunden wollen, dessen Geschwindigkeit und Weltumspanntheit (mit der daraus resultierenden Datenmenge) einfach jeden (Daten-)Schatten verändert, konturenlos werden läßt, relativiert?*

[44] Zum Kenntnisstand der Bundesregierung sehr anschaulich C. Schultzki-Haddouti, Bundesregierung bestätigt Existenz von Echelon (http://www.heise.de/tp/deutsch/special/ech/6748/1.html).