

Erschienen in: D. Klumpp / H. Kubicek /A. Roßnagel (Hrsg.), Next Generation Information Society? Notwendigkeit einer Neuorientierung, Talheimer Verlag, Mössingen-Talheim 2003, 423 – 432.

## **Recht und Technik in der globalen Informationsgesellschaft**

*Alexander Roßnagel*

Die Vorstellungen einer Rechtsordnung für die Informationsgesellschaft waren lange Zeit von weiten Freiheitsräumen geprägt. Staat und Recht waren in diesen Vorstellungen an den Rand gedrängt. Neue technische Grundlagen sollten auch neue Formen des Zusammenlebens ermöglichen. Die rasanten Veränderungen in den Produktionsmitteln und Produktivkräften weckten Visionen über veränderte Produktionsverhältnisse und Kooperationsbeziehungen. Frühere Analysen und Entwürfe zur Regulierung der Informationsgesellschaft (I.) sollen im Folgenden einem Review unterworfen werden (II.), auf dem aufbauend künftige Handlungsmöglichkeiten erörtert werden sollen (III).

### **I. Das Internet: Raum der Freiheit, Grenze nationaler Staatsmacht**

Die Vorstellungen über die ordnungstiftende Aufgabe von Recht und Staat in der Informationsgesellschaft wurden seit der Verbreitung des Internet von der Diskussion geprägt, welche verbindlichen sozialen Regeln das Internet benötigt und wie diese Regeln entstehen können. Dabei bestimmten zwei spezifische Charakteristika des Internet die Debatte: die Globalität des Netzes und die Virtualität des von ihm konstituierten neuen Sozialraums. Im Internet bildete sich eine neue körperlose Welt, in die zunehmend fast alle Formen sozialer Kontakte übertragen wurden. Dieser körperlose Sozialraum kannte keine Grenzen. Vielmehr war in ihm nahezu gleichzeitig die gesamte Welt zu erreichen.

Hieraus wurde geschlossen, dass in der Welt der Netze Staat und Recht nicht mehr in der Lage sind, ihre Ordnungsvorstellungen durchzusetzen. Sie sind als Nationalstaat und Nationalrecht konzipiert, basieren auf national ausgerichteter Demokratie und üben ihre Macht letztlich durch ihr Monopol körperlicher Gewaltanwendung aus. Daher seien globale, grenzenlose und unkörperliche Sozialräume von ihnen nicht mehr zu kontrollieren. In ihnen könne sich jeder allgemein verbindlichen Vorgaben entziehen. In einem

weltweiten, dezentral organisierten, chaotisch wachsenden Netz wie dem Internet seien gezielt steuernde Eingriffe eines Nationalstaats ohne durchschlagenden Erfolg.<sup>1</sup>

Diese Analyse wurde einerseits positiv mit libertären Vorstellungen verbunden: Anfangs wurde das Internet vielfach als rechtsfreier Raum verstanden, der keine Verhaltensregeln erfordere. In ihm herrsche vor allem unbeschränkte Meinungs- und Informationsfreiheit. Mit ihm seien die Enge des Nationalstaats und dessen Kontrollinteressen überwunden. Soweit Verhaltensregelungen als notwendig erschienen, wurde Selbstregulierung als einzige dem globalen und virtuellen Charakter dieses Sozialraums mögliche und angemessene Form der Regelsetzung bezeichnet und für eine Regelfindung ohne Intervention eines Nationalstaats plädiert.<sup>2</sup> Als Beispiel für eine solche Regelsetzung werden vielfach die unterschiedlichen Verhaltensregeln, die von verschiedenen Gruppen als „Netiquette“ aufgestellt wurden,<sup>3</sup> angeführt. Regeln des verträglichen Zusammenlebens sollten von den „Netzbürgern“ selbst aufgestellt werden. Als Ausfluss dieser Entwicklungsvorstellungen blieb vor allem die „International Corporation for Assigned Names and Numbers (ICANN)“ übrig. In ihr findet in institutionalisierter Form zumindest eine Selbstregulierung hinsichtlich der Fragen der Domainverwaltung statt.<sup>4</sup>

Die gleiche Analyse wurde aus ordnungspolitischer Sicht negativ besetzt: Wenn der demokratische Rechtsstaat viele Gesetze, die er aufstellt, im Internet nicht vollziehen kann, dann sei er auch nicht mehr in der Lage, Gemeinwohlbelange durchsetzen und seinen Bürgern Schutz zu gewähren: Eine nationale Rechtsordnung könne nur die Handlungen regeln, die in ihrem Geltungsbereich erfolgen. Weltweite Informationsangebote, -verarbeitungen und -ströme könne sie kaum beeinflussen, auch wenn sie auf ihren Geltungsbereich einwirken. Grenzkontrollen seien weder akzeptabel noch wirksam möglich. Die Körperlosigkeit der Informationen verhindere, ihrer habhaft zu werden. Einmal entstanden, könnten sie nicht mehr unterdrückt oder beseitigt werden.<sup>5</sup> Eine Rechtsordnung, die letztlich auf dem staatlichen Monopol legitimer körperlicher Gewaltausübung beruht, sei hilflos gegenüber unkörperlichen Informationen, die in einem weltweiten Netz zirkulieren. Der Staat könne nur da eingreifen, wo die immaterielle Welt des Netzes in die körperliche Welt übergeht: Er könne Täter festnehmen, Geräte

---

<sup>1</sup> S. hierzu z.B. *Roßnagel*, Globale Datennetze: Ohnmacht des Staates - Selbstschutz der Bürger, Zeitschrift für Rechtspolitik 1997, 26 ff.

<sup>2</sup> S. z.B. die Veröffentlichungen von *Johnson* und *Post* auf den Servern des Cyberlaw-Instituts, [www.cli.org](http://www.cli.org), und der Electronic Frontier Foundation, [www.eff.org](http://www.eff.org), sowie die Nachweise in *Mankowski*, Wider ein transnationales Cyberlaw, Archiv für Presserecht 1999, 138f.

<sup>3</sup> S. z.B. RFC 1855/FYI 28 vom Oktober 1995.

<sup>4</sup> S. [www.icann.org](http://www.icann.org); s. zu ICANN z.B. *Kleinwächter*, ICANN als United Nations der Informationsgesellschaft, MultiMedia und Recht 1999, 452; *Strömer*, Das ICANN-Schiedsverfahren – Königsweg bei Domainstreitigkeiten, Kommunikation & Recht 2000, 587; *Bettinger*, ICANN's Uniform Domain Name Dispute Resolution Policy, Computer und Recht 2000, 234.

<sup>5</sup> S. *Engel*, Inhaltskontrolle im Internet, Archiv für Presserecht 1996, 220; *Roßnagel* (Fn. 1), 26 ff.; *Köhntopp/Köhntopp/Seeger*, Sperrungen im Internet, Datenschutz und Datensicherung 1997, 626.

und Datenträger beschlagnahmen, wenn diese sich körperlich in seinem Herrschaftsreich befinden. Er könne die Befolgung seiner Gesetze erzwingen, wo er seine Zwangsgewalt körperlich ausüben kann. In der körperlosen Netzwelt aber sei er weitgehend machtlos. In ihr habe der Staat keine Zwangsmittel, kein Gewaltmonopol und keine Souveränität.

## II. Die Wirklichkeit nationalstaatlicher Regulierung

Welche dieser Einschätzungen und Prognosen wurde durch die Entwicklung bestätigt?

### *1. Zunahme der staatlichen Regulierung*

Zumindest die Anzahl der nationalstaatlichen Regelungen widerspricht ihnen. Nach anfänglichem Zögern haben die meisten Staaten der Informationsgesellschaft viele spezifische Regelungen für das Internet erlassen. Beispielsweise haben sowohl Europa als auch Deutschland die wichtigsten Fragen inzwischen geregelt – in der E-Commerce-, in der Signatur-, in der Fernabsatz- und den Datenschutz-Richtlinien einerseits und im Fernabsatzgesetz, im Gesetz für den elektronischen Geschäftsverkehr, im Signaturgesetz, im Gesetz zur Anpassung der privatrechtlichen Formvorschriften, im Dritten Verwaltungsverfahrenänderungsgesetz und im Mediendienste-Staatsvertrag der Länder andererseits.<sup>6</sup>

Allgemeine und verbindliche Regelungen werden auch im Internet benötigt. In ihm finden soziale Kontakte, wirtschaftlicher Austausch und rechtlicher Verkehr statt, in ihm werden Interessen verfolgt, Konflikte ausgetragen und Macht ausgeübt. In ihm begegnet man auch vielen bekannten Problemen des sozialen Zusammenlebens wie Diskriminierung, Ausbeutung, Perversion und Kriminalität. Die erforderliche Ordnung des sozialen Zusammenlebens kann aber nicht der spontanen Selbstorganisation und dem Wettbewerb des Markts überlassen werden. Diese gewährleisten nämlich keinen Schutz für Individualinteressen wie Sicherheit, Jugendschutz, Datenschutz, Verbraucherschutz, Urheberrecht oder Informationszugang und vermögen Allgemeininteressen wie Vielfaltsschutz, Wettbewerbssicherung, Völkerverständigung, Strafverfolgung, öffentliche und nationale Sicherheit oder Steuererhebung nicht durchzusetzen. Im Internet geht es nämlich nicht mehr nur um belanglose Kommunikation oder nur um individuelle Vertragsbeziehungen, sondern letztlich um alle Formen des privaten und öffentlichen Rechtsverkehrs.

Auch haben sich Rechtsregelungen als Vorbedingung für elektronischen Rechts-Geschäfts- und Verkehrsverkehr erwiesen. Damit diese überhaupt in breitem Um-

---

<sup>6</sup> S. auch den Beitrag von Holznagel in diesem Band.

fang entstehen können, bedarf es Regelungen, die Vertrauen und Rechtssicherheit in einer Welt ermöglichen, in der sich alle nur virtuell begegnen.<sup>7</sup> Electronic Commerce und Electronic Government wird es nur geben, wenn allgemeinverbindliche Regelungen – positiv – Sicherheit und Vertrauenswürdigkeit gewährleisten und – negativ – rechtliche Hindernisse in der bestehenden Rechtsordnung für ein Handeln in der unkörperlichen Welt beseitigen.

Hierfür konnte in vielen Fällen nicht auf die bestehenden Regeln für die körperliche Welt zurückgegriffen werden. Vielmehr mussten die Eigenheiten des Internet als körperlosen Sozialraums berücksichtigt werden. Hier aber gelten weitgehend andere Bedingungen wie in der körperlichen Welt: Zum Beispiel begegnet man sich im Internet nur virtuell. Dies ermöglicht, andere Identitäten anzunehmen und neue Verhaltensweisen zu erproben, erschwert aber auch, Verantwortung sicherzustellen. Informationen sind nicht auf materiellen Trägern verkörpert. Sie haben damit keine Geschichte. Sie können jederzeit spurlos verändert werden. Die nicht verkörperte Information bietet nicht mehr den Unterschied zwischen Original und Kopie. Von allen Inhalten im Internet – auch von einmaligen geistigen und künstlerischen Schöpfungen – können beliebige Vervielfältigungen ohne Qualitätsverlust hergestellt und schnell und weit verbreitet werden. Im Internet spielen Zeit und Ort kaum eine Rolle. Jede Information kann jederzeit überallhin in Sekunden übermittelt werden. Unkörperlichkeit des Handels heißt nicht, dass es keine Spuren gibt. Im Gegenteil gibt es mehr Spuren als in der körperlichen Welt, weil jede Handlung die Verarbeitung von Daten voraussetzt, die auch gesammelt und einer Person zugeordnet werden können.<sup>8</sup>

Soweit diese Eigenheiten eine Rolle spielen, genügen die alten Rechtsregeln für die körperliche Welt nicht. Sie bieten weder effektiven Schutz noch ausreichende Rechtssicherheit, geben den neuen Entwicklungen keinen Rahmen und verhindern durch ihre Bindung an Ort, Zeit oder Körperlichkeit (z.B. Papier und Unterschrift) viele Internetanwendungen. Spezifische Regeln sind daher mindestens aus drei Gründen notwendig: Erstens müssen sie effektiven Schutz und ausreichende Rechtssicherheit bieten – etwa im Jugendschutz, Verbraucherschutz und Datenschutz sowie in Straf-, Beweis- und Verwaltungsverfahren. Zweitens müssen sie den neuen Infrastrukturen einen Rahmen vorgeben und drittens sind sie notwendig, um Internetanwendungen den Weg frei zu machen, etwa um Handlungen im Internet in das Recht der Willenserklärungen, der Verwaltungsverfahren und der Gerichtsordnungen einzupassen.

## 2. Staatliche Regulierung statt Selbstregulierung

Diese staatlichen Regelungen konnten und können nicht durch Selbstregulierung ersetzt werden. Die verschiedenen Netiquetten haben sich schnell als völlig unzureichend

---

<sup>7</sup> S. z.B. *Fuhrmann*, Vertrauen im Electronic Commerce, 2001.

<sup>8</sup> S. hierzu *Roßnagel*, Weltweites Internet – globale Rechtsordnung?, *MultiMedia und Recht* 2002, 67 ff. m.w.N.

erwiesen. Diese Form der Selbstregulation funktioniert allenfalls, solange sich die „Netizens“ im „Netzparadies“ der Gleichgesinnten befinden. Ist die Unschuld aber durch die Einmischung mächtiger und divergierender Interessen verloren, bedarf es der regulierenden Funktion demokratischer Gesetzgebung. Der Staat bleibt aufgefordert, auch im körperlosen Sozialraum des Internet für Sicherheit, Daten-, Verbraucher-, Jugend- und Urheberschutz zu sorgen.

Aber auch die mächtigen wirtschaftlichen Interessen propagieren Selbstregulierung und Selbstkontrolle. Beispielsweise mit der Initiative des Global Business Dialogue<sup>9</sup> haben sie auch einen ersten Ansatz geschaffen, einzelne Fragen des Internethandels weltweit selbst zu regulieren. Sie versprechen mit dieser Form der Regulierung, problemadäquate und akzeptierte Regelungen schnell, flexibel und weltweit zu schaffen.<sup>10</sup> Ihnen ist eine Chance einzuräumen, soweit sie diese Versprechen tatsächlich erfüllen können. Dies wird in geschlossenen Gruppen eher möglich sein als für das offene Netz und für einige der genannten Regelungsprobleme eher realisierbar sein als für andere. Bisher waren die Leistungen der Selbstregulierung allerdings noch nirgendwo besonders überzeugend. Hinsichtlich der praktischen Erfolge ist selbst in Einzelfällen Skepsis angesagt.

Davon unabhängig taugen Selbstregulierung und Selbstkontrolle nicht als durchgängiges Prinzip der Regulierung im Internet. In der Selbstregulierung setzen sich meist die wirtschaftlich stärksten Interessen durch, zu Lasten von Konkurrenten, Verbrauchern, Zulieferern, unbeteiligter Dritter oder künftiger Generationen. Individual- und Minderheiteninteressen werden systematisch benachteiligt. Den durch Selbstregulierung entstandenen Regelungen fehlt nicht nur die demokratische Legitimation, sie ermangeln meist auch der Interessenrepräsentativität. Sie gelten nie allgemein, sondern nur gegenüber denjenigen, die sich ihnen freiwillig unterworfen haben. Dies ist in der Regel die Minderheit der notwendigen Adressaten. Für die Mehrheit greifen sie nicht. Für viele Fragen wird aber eine alle Teilnehmer und alle Fälle erfassende Rechtsordnung benötigt. Auch geht es im Internet nicht nur um den Handel, sondern auch um die Wahrnehmung öffentlicher Aufgaben und die Durchführung staatlicher Verfahren. Die selbstgesetzten Regeln können gegen Abweichende<sup>11</sup> nicht durchgesetzt werden, da die Regulierungsgremien über keine wirksamen Kontroll- und Zwangsmechanismen verfügen.<sup>12</sup> Im

---

<sup>9</sup> S. [www.gbd.org](http://www.gbd.org). Für den Datenschutz s. auch die Online Privacy Alliance – s. [www.privacyalliance.org](http://www.privacyalliance.org).

<sup>10</sup> S. zu diesen Vorteilen *Roßnagel*, Konzepte der Selbstregulierung, in: ders. (Hrsg.), Handbuch Datenschutzrecht, Kap. 3.6, Rn. 53 ff.; *Ukrow*, Die Selbstkontrolle im Medienbereich in Europa, 2000, 12 ff.; *Mankowski* (Fn. 2), 139f.

<sup>11</sup> Zum Befolgungsgrad s. den enttäuschenden Bericht der *Federal Trade Commission*, Fair Information Practices in the Electronic Marketplace, 2000, [www.ftc.gov/reports/privacy2000](http://www.ftc.gov/reports/privacy2000).

<sup>12</sup> Allein der Ausschluss aus den Selbstregulierungsverband als schärfste Sanktion ist i.d.R. kein ausreichendes Zwangsmittel. Etwas anderes gälte nur dann, wenn etwa der Verlust einer hinterlegten Kaution drohen würde – s. z.B. *Spindler*, Sicherheit im E-Commerce = Rechtssicherheit, in: Müller/Reichenbach (Hrsg.), Sicherheitskonzepte für das Internet, 2001, 167.

Konfliktfall vermögen sie keinen effektiven Schutz der schutzbedürftigen Interessen zu bieten. Schließlich können unterschiedliche Selbstregulierungsregimes auch zu einer weiteren Rechtszersplitterung statt einer Rechtsvereinheitlichung führen.<sup>13</sup>

Im Ergebnis ist eine rechtliche Regulierung unvermeidbar. Nur sie kann die notwendige allgemeinverbindliche Ordnung und den erforderlichen rechtlichen Schutz gewährleisten. Dabei sollten aber die Vorteile der Selbstregulierung dort genutzt werden, wo dies inhaltlich vertretbar und tatsächlich effektiv ist. Dies wird in der Regel nur in der Form möglich sein, dass Recht der Selbstregulierung Ziele setzt und ihr es überlässt, diese zu konkretisieren. Auch muss das Recht der Selbstregulierung einen Rahmen vorgeben, der ein faires Verfahren für das Aufstellen der Verhaltensregeln gewährleistet und die Durchsetzung der Verhaltensregeln unterstützt. Hierfür sind Mechanismen erforderlich, die für eine rechtssichere und möglichst weitgehende Geltung und Anwendung der Verhaltensregeln sorgen.<sup>14</sup>

### 3. Grenzen nationalstaatlicher Regulierung

Auch wenn die Nationalstaaten viele Regelungen für das Internet getroffen haben, an ihrer Durchsetzung hapert es. Sie gelten immer nur für nationale Rechtsordnungen und sind nur vollziehbar, soweit die körperliche Zwangsgewalt eines Staats reicht. Insofern hat sich die frühere Analyse bestätigt. Virtualität und Globalität setzen der Durchsetzung staatlicher oder suprastaatlicher Rechtsregeln Grenzen. Zugleich zeigt sich immer deutlicher, dass in der Informationsgesellschaft auch die Technik rechtlicher Regulierung Grenzen setzt. Alle diese Grenzen verursachen Schutzdefizite für schützenswerte Rechte und Interessen.

## III. Entwicklungspotenziale

Wie könnten diese Defizite reduziert und die notwendigen Regelungen weltweit im Internet zur Geltung gebracht werden? Hierfür gibt es zwei Ansätze – zum einen die Umsetzung rechtlicher Regeln in technische Systeme und zum anderen die Globalisierung des Rechts.

### 1. Recht durch Technik

Die Weltveränderungskapazität der Informations- und Kommunikationstechnik verändert nicht nur die Gesellschaft, sondern damit zugleich auch die Verwirklichungsbedingungen von Recht. Die zahlreichen Neben- und Folgewirkungen des Technikeinsatzes verbessern oder verschlechtern die Möglichkeiten, die Ziele rechtlicher Normen zu ver-

---

<sup>13</sup> S. zu ausländischen Beispielen *Roßnagel* (Fn. 10), Rn. 71 ff.

<sup>14</sup> S. als Beispiel *Roßnagel/Pitzmann/Garstka*, Modernisierung des Datenschutzrechts, Gutachten für das Bundesinnenministerium, 2001, 154 ff.

folgen, verursachen neue Gefährdungen oder schaffen neue Entfaltungschancen.<sup>15</sup> Über den Anpassungsdruck, den technische Wirklichkeitsgestaltung auf Rechtsregeln ausübt, kann Technik sogar Recht selbst verändern.<sup>16</sup>

Je stärker Technik die gesellschaftliche Ordnung und Entwicklung prägt, umso schwieriger wird es, rechtliche Ziele durchzusetzen. Ohne technische Unterstützung droht Recht in einer technikgeprägten Welt folgenlos zu bleiben. Recht ist auf rechtsgemäße Technik angewiesen. Wenn Technik zum einflussreichsten Ersatzgesetzgeber wird, muss Recht – schon allein um den demokratischen Steuerungsanspruch zu bewahren – Technik beeinflussen.<sup>17</sup>

Technik kann helfen, rechtliche Ziele zu erreichen und Schutzaufträge zu erfüllen. Technischer Schutz ist auch viel effektiver als rein rechtlicher Schutz. Wo etwa Technik Datenmissbrauch verhindert oder Kinder vor gefährdenden Informationen schützt, ist eine Durchsetzung von Recht durch Polizei oder Gerichte nicht mehr erforderlich. Was technisch verhindert wird oder einfach technisch nicht möglich ist, muss nicht mehr verboten und überwacht werden. Gegen Verhaltensregeln kann verstoßen werden, gegen technische Begrenzungen eines Techniksystems nicht. Rechtsgemäße Technikgestaltung kann Kontroll- und Überwachungsaufwand, Bußgeld- und Strafverfahren überflüssig machen.

Notwendig ist also ein Systemschutz, bei dem die technischen Systeme so gestaltet sind, dass rechtliche Anforderungen von selbst, eben durch die normale Nutzung der Technik durchgesetzt werden.<sup>18</sup> Dies wird bei multifunktionaler Technik oft nicht möglich sein. Aber es wäre schon viel gewonnen, wenn zum Beispiel die Defaulteinstellungen immer so wären, dass sie den rechtlichen Anforderungen oder Zielsetzungen entsprechen.

Schutz durch Technik ist oft die einzig mögliche Antwort auf Probleme der Globalisierung. Je mehr die Durchsetzung der Schutzziele dem Einflussbereich des nationalen Gesetzgebers entwindet, desto mehr muss der Schutz weltweit wirksam werden. Dies ist mangels einer wirksamen Weltrechtsordnung nur dann möglich, wenn er in die Technik eingelassen ist. Dieser Weg bietet zwei Vorteile: Schutztechniken sind – im Gegensatz zu nationalem Recht – weltweit wirksam und Technikunternehmen sind – im Gegensatz zu Gesetzgebern – sehr schnell lernende Systeme. Beide Vorteile lassen sich nutzen, wenn es gelingt, für Schutztechniken einen Markt zu entwickeln. Wenn diese

---

<sup>15</sup> S. hierzu näher *Roßnagel/Wedde/Hammer/Pordesch*, Digitalisierung der Grundrechte, Zur Verfassungsverträglichkeit der Informations- und Kommunikationstechnik, 1990.

<sup>16</sup> S. hierzu ausführlich *Roßnagel*, Rechtswissenschaftliche Technikfolgenforschung, 1993, 14 ff.

<sup>17</sup> S. hierzu *Roßnagel*, Allianz von Medienrecht und Informationstechnik – Hoffnungen und Herausforderungen, in: ders. (Hrsg.), Allianz von Medienrecht und Informationstechnik? 2001, 23 ff.

<sup>18</sup> *Dix*, Konzepte des Systemschutzes, in: *Roßnagel* (Hrsg.), Handbuch Datenschutzrecht, Kap. 3.5. m.w.N.; s. hierzu auch *Büllesbach* in diesem Band.

sich verkaufen, werden sie sich ebenso dynamisch entwickeln wie neue technische Herausforderungen für die jeweiligen Schutzgüter.

Die Durchsetzung von Interessen durch Technik ist allerdings ambivalent. Sie ist zu begrüßen, wenn dabei legitimierte Rechtsziele offen verfolgt werden. So ist es sehr hilfreich, wenn technische Codes weltweit anerkannte Mindestregelungen unterstützen, wie etwa der Datenschutzstandard P3P des W3C die datenschutzrechtliche Mindestregel des „Notice and Choice“. Verhindert werden müssen jedoch Techniklösungen, durch die Partikularinteressen unerkannt und unlegitimiert in Technikstrukturen eingebaut werden, wie etwa das unbemerkte Speichern von Identifikatoren in Microsoft-Programmen. Daher müssen Rechtsregeln der technischen Gestaltung demokratisch legitimierte Ziele vorgeben, weil nur dann legitime und illegitime Technikausprägungen festgestellt werden können.<sup>19</sup>

Viele rechtliche Ziele werden im globalen Kontext aber nur noch durchsetzbar sein, wenn der Betroffene zumindest einen Teil seines Schutzes selbst übernimmt. Staat und Recht sind bei einer globalen und unkörperlichen Bedrohung von Schutzgütern mit einer „Rundumversorgung“ und einem „Vollschutz“ überfordert. Sie müssen von einer zu weitgehenden Erfüllungsverantwortung für diese Schutzaufgabe befreit werden. An deren Stelle muss eine Gewährleistungsverantwortung<sup>20</sup> oder für die Informationstechnik spezifischer eine Strukturverantwortung treten.<sup>21</sup> Diese ist zu koppeln mit dem Konzept des Selbstschutzes. Wenn Staat und Recht den Bürger nicht mehr vollständig vor Rechtsverletzungen schützen können, müssen sie ihn in die Lage versetzen, sich – defensiv – selbst zu schützen. Ihre Interessen selbst zu schützen, können die Staaten ihren Bürger nicht abnehmen. In ihre Aufgabe der Infrastrukturvorsorge fällt aber, über diese Möglichkeiten aufzuklären, das Angebot rechtsgemäßer technischer Instrumente des Selbstschutzes zu fördern und den notwendigen rechtlichen, technischen und organisatorischen Rahmen für die jeweils erforderliche Infrastruktur mit Zulassungs- und Prüfverfahren, Auszeichnungen und sonstigen Dienstleistungen zu bieten.<sup>22</sup>

## 2. Globalisierung des Rechts

Rechtsdurchsetzung durch Umsetzung von Verhaltensregeln und Selbstschutzmechanismen in Technik wird nur für manche Probleme eine Lösung bringen. Für die verbleibenden Probleme stellt sich die Frage, wie die notwendige Rechtsordnung weltweit hergestellt werden kann. Wenn das globale Internet für den elektronischen Wirtschafts- und Rechtsverkehr einen einheitlichen „Cyberspace“ erzeugt, dann müssen für diesen mög-

---

<sup>19</sup> S. z.B. *Roßnagel* (Fn. 17), 17 ff.

<sup>20</sup> S. z.B. *Hoffmann-Riem* Innovationen durch Recht und im Recht, in: Schulte (Hrsg.), Technische Innovation und Recht – Antrieb oder Hemmnis?, 1996, 21f.

<sup>21</sup> *Roßnagel* (Fn. 1), 30.

<sup>22</sup> S. *Roßnagel*, Konzepte des Selbstschutzes, in: ders. (Hrsg.), Handbuch Datenschutzrecht, Kap. 3.4.



lichst einheitliche Regelungen festgelegt und durchgesetzt werden. Im E-Commerce ist es weder für einen Anbieter noch für einen Nachfragenden zumutbar, eventuell über hundert Rechtsordnungen beachten zu müssen.<sup>23</sup>

Für globale Regelungen besteht daher ein großer Bedarf. Was aber könnte der Legitimationsgrund für die Geltung dieser globalen Regelungen sein? Ein globaler Gesetzgeber ist nirgendwo in Sicht. Er müsste auf einer globalen Demokratie beruhen. Diese setzt aber mehr voraus als einen weltweit einheitlichen Wahlmodus für das Gesetzgebungsorgan – wobei dieser bereits ein schier unüberwindliches Problem darstellt. Eine globale Demokratie müsste materiell wenigstens auf einigen gleichen Werten und Entwicklungszielen ruhen. Sie müsste sich inhaltlich aus einem globalen politischen Diskurs speisen, der weltweite Parteien und Verbände hervorbringt, aus denen heraus sich Kandidaten zur Wahl stellen. Diese Grundlagen für eine materielle und personelle demokratische Legitimation eines globalen Gesetzgebers aber fehlen. Globale Rechtsregeln können daher nur von den nationalen Demokratien her legitimiert werden, die – im Rahmen internationaler Organisationen – möglichst gut zu einer einheitlichen weltweiten Rechtsordnung zusammen arbeiten. Diese Angleichung der Rechtsordnungen kann nur evolutionär erfolgen.

Dies wiederum setzt einen globalen Konsens über Regelungsbedürftigkeit und Regelungsinhalte voraus. Diesen Konsens haben wir aber noch nicht erreicht. Noch fehlt auch für diesen Weg die inhaltliche Grundlage für eine einheitliche Rechtsordnung, soll nicht einfach das US-amerikanische Recht weltweit zur Anwendung kommen.

Globale Regelungen stehen nicht am Anfang, sondern eher am Ende der Rechtsentwicklung. Bis dahin ist die Internetgesetzgebung Sache der Staaten, die in einen Wettbewerb der Regelungssysteme und der kulturellen Vielfalt stehen.<sup>24</sup> Einzelne Staaten – etwa wie Deutschland im Datenschutz- oder Signaturrecht – müssen mit eigenen Regelungen vorgehen können. Andere werden diesem Beispiel folgen oder es ablehnen. Diese Entwicklung und Einschränkung von Optionen fördert die globale Willensbildung über geeignete Problemlösungen. Solange jedoch wesentliche kulturelle und rechtliche Unterschiede bestehen, ist eine Vereinheitlichung, die diese nicht berücksichtigt, nicht wünschenswert.

Dies schließt es nicht aus, dass eine gegenseitige Rechtsanpassung erfolgt. Vielmehr ist dies für einen weltweiten elektronischen Rechtsverkehr sogar eine notwendige Voraussetzung. Eine globale Annäherung der Rechtsvorstellungen können internationale Orga-

---

<sup>23</sup> Das Risiko der Rechtsanwendung und der Rechtsdurchsetzung erzeugt Unsicherheit und unverträglich hohe Transaktionskosten - s. *Spindler* (Fn. 12), 175f. Doch genügt es nicht, schlicht das Herkunftslandprinzip zu Anwendung zu bringen – s. kritisch z.B. *Hoeren*, Vorschlag für eine EU-Richtlinie über E-Commerce, MultiMedia und Recht 1999, 194f.; *Mankowski*, Herkunftslandprinzip und Günstigkeitsvergleich in § 4 TDG-E, Computer und Recht 2001, 630.

<sup>24</sup> S. hierzu auch *Grewlich*, Konstitutionalisierung des „Cyberspace“, 2001, 42 ff.

nisationen wie UNCTAD, UNCITRAL, OECD oder WTO einerseits und private internationale Vereinigungen wie der Global Business Dialog andererseits unterstützen, indem sie beispielsweise Musterregelungen entwerfen. Allerdings ist nicht in jedem Regelungsbereich eine weltweite Koordination gleichermaßen dringlich. Ein hohes Maß an Vereinheitlichung ist beispielsweise hinsichtlich der Rechtssicherheit von rechtsverbindlichen Handlungen im Internet geboten. Ob eine Willenserklärung im Internet zulässig, formgerecht und beweisgeeignet ist, sollte möglichst gleichförmig geregelt werden, da bei unterschiedlichen Regelungen ein globaler E-Commerce ausgeschlossen oder stark behindert ist. Keine Vereinheitlichung, aber ein hohes Maß an Kooperation zwischen den Staaten ist für die Rechtsdurchsetzung geboten. Hinsichtlich der materiellen Schutzstandards erscheint eine vollständige Anpassung der Rechtsordnungen dagegen nicht unbedingt erforderlich. Für die Bereiche des Verbraucher- und Datenschutzes könnte eine Form der Koordinierung gewählt werden, wie sie auch für die einschlägigen europäischen Richtlinien gewählt worden ist. Hier könnte es ausreichen, sich auf ein einheitliches Mindestniveau zu verständigen, das in einzelnen Rechtsordnungen aber gesteigert werden kann. Diese Regelungsform kann zum Experimentieren mit Regelungskonzepten und -formen sowie zum Wettbewerb von Regelungsalternativen und -niveaus genutzt werden. Sie ermöglicht eine Fortentwicklung des Internetrechts und hält dieses lernfähig.

#### **IV. Ausblick: Allianz von Recht und Technik**

Informationsgesellschaft war nie eine Kategorie des Rechts, aus der bestimmte Rechtsfolgen abgeleitet worden wären. Sie war auch keine brauchbare Beschreibung zur Systematisierung eines eigenen Rechtsgebiets. Zu Beginn der Debatte über die Informationsgesellschaft waren Juristen sogar überwiegend der Auffassung, dass mit dem Begriff der Informationsgesellschaft keine spezifischen rechtlichen Probleme verbunden seien. Nach und nach hat es sich dann aber auch bei Juristen herumgesprochen, dass sich mit der gesellschaftlichen Nutzung der Informations- und Kommunikationstechniken spezifisch neue Rechtsprobleme ergeben haben. Die Unkörperlichkeit, Zeitlosigkeit, Gleichzeitigkeit, Ortlosigkeit, Ubiquität, Flüchtigkeit, Unzuordenbarkeit, Manipulierbarkeit, Vervielfältigbarkeit der Information und weitere spezifische Charakteristika veränderten auch die Voraussetzungen und Folgen des Umgangs mit Informationen. Für die Aufgaben des Rechts, Freiheit und Ordnung zu gewährleisten, veränderten sich damit wichtige Bedingungen, sie zu erfüllen. Der Begriff der Informationsgesellschaft erwies sich als eine brauchbare Sammelbeschreibung, um diese spezifisch neuen Bedingungen zu benennen.

Die Informationsgesellschaft wird dann lebenswert sein, wenn sie die Freiheitsräume und Zielsetzungen einer freien Gesellschaft realisiert. Auch in der Informationsgesellschaft wird Gerechtigkeit hergestellt werden müssen, indem die individuellen Interessen und Rechte der Schwächeren geschützt werden. Diese Schutzaufgaben sind in ihrer grundsätzlichen Aktualität relativ stabil, erfordern jedoch eine ständige Anpassung ihrer Durchsetzungsmechanismen. Diese werden durch Globalität und Virtualität des Han-

delns vor neue Herausforderungen gestellt. Um diese zu bewältigen, bieten sich zwei Wege an, die sich ergänzen müssen. Zum einen ist eine Allianz von Recht und Technik notwendig. Wo möglich müssen rechtliche Ziele in der Entwicklung und Gestaltung von Technik berücksichtigt werden. Zum anderen muss versucht werden, divergierende rechtliche Ziele – wo notwendig und möglich – evolutionär einander anzugleichen und anzupassen.