

Verantwortung im Internet

Themenpapier im Projekt „Digitaler Kodex“¹

von Dr. Till Kreutzer, Partner iRights.Lab

¹ Das iRights.Lab führt im Auftrag des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI) das Projekt „Braucht Deutschland einen Digitalen Kodex?“ durch.

I. Vorbemerkung

Das Netz ist ein komplexes System, ein sozialer, Wirtschafts- und Kommunikationsraum, also ein Handlungsraum mit allen denkbaren Facetten. Dieser Lebens- und Handlungsraum ist in das sonstige Dasein eingebettet. Wie in jedem anderen Teilbereich des Lebens und Wirkens spielt Verantwortung im Netz eine große Rolle. Wenn niemand Verantwortung trägt oder sich jeder nur für seine eigenen Belange verantwortlich fühlt, herrscht Chaos. Auch im Internet muss es daher Verantwortung geben, muss Verantwortung übernommen werden und es müssen Konzepte für deren Verteilung und Zuordnung existieren.

II. Verantwortungsbegriff

Es gibt keine allgemeingültige Definition von Verantwortung². Vorliegend soll Verantwortung verstanden werden als die Pflicht einer Person, Institution, Korporation oder Gruppe (Verantwortungssubjekt), für bestimmte Umstände einzustehen. Verantwortung bezieht sich daher nicht auf die Handlung, sondern auf die Handlungsfolgen. Verantwortung kann unterschiedlich begründet sein, etwa durch Moral, Ethik, soziale Normen, Recht oder aus rein intrinsischen Motiven. In der Regel wird sie durch Normen zugeschrieben. Sie kann sich auf durch Handeln, Unterlassen oder auch ohne menschliches Zutun entstandene Umstände (z. B. die Folgenbeseitigung bei Naturkatastrophen) beziehen. Normenverstöße haben meist Folgen und ziehen in der Regel Sanktionen nach sich, v. a. soziale oder rechtliche.

Auch wenn Verantwortung in öffentlichen Debatten gerade im Zusammenhang mit dem Internet häufig vorwiegend in juristischer Hinsicht diskutiert wird, geht Verantwortung weit über den juristischen Begriff der Haftung hinaus. Haftung setzt eine durch Recht gesetzte Pflicht zur Verantwortung voraus, bei deren Verletzung das Verantwortungssubjekt in Regress genommen werden kann (Picht 1969/2004).

Verantwortung kann jedoch auch rein intrinsisch entstehen (jemand fühlt sich aus innerem Antrieb verantwortlich) oder mit anderen als rechtlichen Mitteln zugeordnet und gesteuert werden. Von Entstehung und Zuordnung von Verantwortung zu unterscheiden sind die Sanktionen, die drohen oder drohen können, wenn der Verantwortung nicht Genüge getan wird. Einer Verantwortung nicht zu genügen, wird für den Verantwortlichen meist Folgen haben, zwingend ist dies jedoch nicht. Erst recht müssen diese Folgen nicht juristischer Natur sein. Soziale Normen etwa sind weder juristisch verbindlich noch ziehen sie staatliche Sanktionen nach sich. Sie werden durch die Gesellschaft selbst überwacht und durchgesetzt. Die Folgen können u. U. gravierender sein als rechtliche Sanktionen, beispielsweise bei einem Ausschluss aus der Gemeinschaft wegen Fehlverhaltens.

III. Arten von Verantwortung

Um zu identifizieren, welche Akteure in einem Handlungsumfeld, z. B. dem Internet, Verantwortung tragen und worauf sie sich bezieht, ist es sinnvoll, zwischen zwei Formen von Verantwortung zu

² Siehe zu den unterschiedlichen Definitionen Wikipedia: Verantwortung, <http://de.wikipedia.org/wiki/Verantwortung>.

unterscheiden: Verantwortung *ex ante* und Verantwortung *ex post* (Lessig 1998). Erstere ist eine Handlungsverantwortung mit ordnungsgestaltendem Inhalt: Der Verantwortliche hat dafür zu sorgen, dass Rahmenbedingungen geschaffen werden, die erwünschte Handlungen und Handlungsfolgen fördern und unerwünschtes Verhalten vermeiden. Die *ex-ante*-Verantwortung ist also prospektiv orientiert (Bayertz 1995, 32). Ein Beispiel ist die Verantwortung des Staates zur Regelsetzung oder eine mögliche Pflicht der Anbieter sozialer Netzwerke, die anonyme Nutzung ihrer Dienste zu ermöglichen³.

Ex-post-Verantwortung würde in diesem Beispiel entstehen, wenn es eine Norm in Form einer Selbstverpflichtungs- oder Rechtsnorm gäbe, die Anonymität vorschreibt und der Anbieter sich nicht hieran hält. *Ex-post*-Verantwortung bedeutet, für Normverstöße oder allgemein für negative Umstände eintreten zu müssen und sich hierfür „zu verantworten“.

Verantwortung kann individuell oder kollektiv bestehen. Individuell kann sie einem Individuum, einer Institution oder einem Unternehmen zugeordnet werden. Kollektive Verantwortung tragen Gruppen (z. B. die Wirtschaft), soweit ihnen eine Rolle mit identifizierbarem Interesse zukommt. Zudem sind Eigenverantwortung (für selbst herbeigeführte Handlungsfolgen) und Mitverantwortung (für durch andere herbeigeführte Handlungsfolgen) zu unterscheiden.

IV. Grundzüge zur Zuschreibung von Verantwortung

Verantwortung setzt nach traditionellem Verständnis Handlungsfreiheit und -fähigkeit voraus. Wer nicht handeln kann, ist nicht verantwortlich, wer keine Wahl hat, wie er handelt, z. B. bei Reflexhandeln, ebenfalls nicht. Verantwortung steht damit in einem engen Zusammenhang mit Freiheit. Wer keine Möglichkeiten zum Handeln hat, ist zwar frei von Verantwortung, aber auch unfrei.

V. Eigenverantwortung versus Mitverantwortung

„Verantwortung ist im ersten Schritt ein Anspruch an sich selbst und für sich selbst.“ (Picht 1969/2004). Jeder Handelnde ist für eigenes Verhalten und dessen Folgen zunächst selbst verantwortlich. Der Handelnde kann sein Tun am besten steuern, sein Einfluss auf die Folgen des Handelns ist generell am unmittelbarsten. So ist es beispielsweise zunächst an den Nutzern von YouTube, keine geschützten Inhalte auf die Plattform zu laden, ohne hierfür die notwendigen Rechte zu haben. Nur wenn sie ihrer Eigenverantwortung faktisch nicht nachkommen und man sie durch Sanktionen nicht effizient daran hindern kann, kann man dem Dienstanbieter Mitverantwortung übertragen.

Im Übrigen vollzieht sich Handeln oft in komplexen Handlungsgeflechten. Handlungsfolgen basieren in der Regel auf vielschichtigen Kausalketten, daher können Handlungsfolgen nicht immer (nur) einer individuellen Handlung zugeordnet werden. Bei alleiniger Anwendung des Prinzips der Eigenverantwortung käme es hier im Zweifel zu einer Verantwortungsdiffusion, also dem Effekt, dass niemand Verantwortung übernimmt. Um zu vermeiden, dass in überkomplexen Handlungsgefügen verantwortungsfreie Bereiche entstehen oder zu kompensieren, dass der eigentlich Verantwortliche nicht verantwortlich gemacht werden kann, können *ex-ante*-Verantwortlichkeiten geschaffen werden.

³ Zum Thema: <https://www.datenschutzzentrum.de/presse/20130424-facebook-klarnamen-ovg.htm>.

Dieser Gedanke steht etwa hinter der Gefährdungshaftung oder dem Organisationsverschulden. In diese Richtung gehen viele Debatten über die Haftung im Internet, v. a., da hier der eigentlich verantwortliche Nutzer häufig nicht identifizierbar ist. Ein Beispielsfall liegt in der Auseinandersetzung, ob Sharehoster wie Rapidshare Filter einsetzen müssen, um ihre Nutzer daran zu hindern, geschütztes Material zu verbreiten. Eine solche Verantwortungsverteilung hieße, dem Anbieter eine Pflicht aufzuerlegen, seinen Dienst so zu organisieren, dass Rechtsverletzungen möglichst verhindert werden.

Hieran zeigt sich, dass es effizienter, gerechter oder aussichtsreicher sein kann, die Verantwortung vom Handelnden auf einen Dritten zu verlagern. Hierum geht es im Kern auch bei der Diskussion um Nutzerdaten in sozialen Netzwerken. Zunächst ist es an den Nutzern selbst, sorgsam mit persönlichen Inhalten und Daten umzugehen. Zeigt sich aber, dass in vielen Fällen unverantwortlich gehandelt wird, ist es denkbar, die Anbieter zu verpflichten, deutlich auf die Folgen hinzuweisen oder gar bestimmte Handlungen gar nicht erst zu ermöglichen. Hiermit wird die Verantwortung des Nutzers ganz oder teilweise auf den Anbieter verlagert, sowohl *ex ante* als auch *ex post*.

In diesem Beispiel würde die teilweise „Entmündigung“ des Nutzers mit der faktischen Unachtsamkeit der Nutzer in eigener Sache und evtl. damit begründet, dass sie ihrer Eigenverantwortung mangels Einsicht häufig gar nicht nachkommen können. Andere Gründe für die Zuordnung von (Mit-)Verantwortung an Dritte können darin liegen, dass der Handelnde seiner Eigenverantwortung aus faktischen Gründen nicht nachkommen kann, ihm die (alleinige) Verantwortung nicht zugemutet werden kann oder es effizienter wäre, sie einem anderen oder einem Kollektiv zuzuordnen.

VI. Verantwortung im und außerhalb des Internets

Dinge, die in der gegenständlichen Welt selbstverständlich sind, werden häufig hinterfragt, wenn es um das Internet als Handlungsraum geht. So auch der Begriff und das Konzept von Verantwortung.

Wie gesagt ist Verantwortung die Pflicht einer Person, Institution, Korporation oder Gruppe, für bestimmte Umstände einzustehen. Dadurch, dass Verantwortung durch Moral oder Normen individuell oder kollektiv zugeschrieben wird, entsteht ein wichtiges Ordnungsprinzip, das auf Regeln und Grundsätzen basiert. Kann man hierauf im Internet verzichten?

Viele der zu Beginn des Informationszeitalters geprägten und bis heute gebräuchlichen Begriffe für das Internet suggerieren, dass das Internet virtuell und damit nicht real sei. Begriffe wie *Cyberspace*, Datenraum, virtuelle Umgebung oder vermeintliche Antagonismen wie *Cyberspace vs. Realspace* legen den Schluss nahe, dass Handeln im Internet weniger oder keine tatsächlichen Konsequenzen hat. Dies hat einen Einfluss auf das Konzept von Verantwortung, auf das Verantwortungsbewusstsein der Akteure und auf die Regeln zur Zuordnung von Verantwortlichkeit. Denn wenn das Handeln keine reale Konsequenz hat, spielt Verantwortung auch keine entscheidende Rolle.

Dass dies ein Trugschluss ist, dürfte evident sein. Das Netz ist ein realer Handlungsraum, genau genommen besteht es aus einer Vielzahl zu unterscheidender Handlungsräume. Auch online ziehen Handlungen reale Auswirkungen nach sich (Goldsmith 1998, 1200). Sie können physischer oder immaterieller Natur sein, sind aber nicht weniger tatsächlich als im gegenständlichen Raum.

Im Internet finden sich alle Facetten gesellschaftlichen Lebens, denn das Netz ist Teil desselben. Es ist nicht nur ein Kommunikations- oder medialer, sondern ein sozialer Raum (Mansell 2002). Die hier

handelnden Akteursgruppen sind dieselben wie außerhalb des Internets, also Menschen, Unternehmen, Institutionen und Politik. Internet-spezifische Verantwortungssubjekte, d. h. Akteure, die eigene Entscheidungen auf Basis von Handlungsfreiheit und -fähigkeit treffen, gibt es bislang nicht. Denn noch sind Technologien, die auf Basis künstlicher Intelligenz autonom denken und entscheiden, Zukunftsmusik. Alles, was im Internet passiert, ist auf menschliches Handeln zurückzuführen. Auch im Internet darf Verantwortung als Ordnungsprinzip daher weder in Frage gestellt noch die Bedeutung von Verantwortung heruntergespielt werden.

Das bedeutet jedoch nicht, dass konkrete Konzepte zur Beurteilung, Zuschreibung und Durchsetzung von Verantwortung im Internet keiner weiteren Überlegung bedürfen oder herkömmliche Gedankenmodelle und Systeme einfach auf das Internet übertragen werden können. Tatsächlich weist das Internet gegenüber gegenständlichen Umgebungen Besonderheiten auf. Diese machen eine Neuurteilung von Verantwortung in bestimmten Bereichen ebenso erforderlich, wie eine Überprüfung der Mittel, mit denen Verantwortung zugewiesen werden kann. Gründe können darin liegen, dass es hier z. T. andere Akteure gibt, sie andere Rollen einnehmen, dass sich die Akteure aufgrund der äußeren Umstände anders verhalten oder sich der Effekt von Handlungen gegenüber der gegenständlichen Welt unterscheidet.

Für den Aspekt der Verantwortung sind u. a. die folgenden Besonderheiten des Internets relevant:

Anonymität und Unkörperlichkeit: Individuen sind im Internet per se anonym, wenn sie sich für Anonymität entscheiden. Dass sie, z. B. über die Zuordnung von IP-Adressen, gegebenenfalls mittelbar identifiziert werden können, ändert hieran nichts. Fehlt, wie im Netz, physischer Kontakt, geht ein wesentliches Element sozialer Kontrolle verloren. Anonymität und Unkörperlichkeit verleiten dazu, Verantwortung zu negieren und erleichtern es, sich Verantwortung zu entziehen oder Sanktionen für unverantwortliches Verhalten zu vermeiden. Mit anderen Worten: Die Durchsetzung sozialer Normen wird erschwert. Murray (2011) drückt diesen Effekt so aus: *„The act of entering Cyberspace seems to drive us to shed our social responsibilities and duties. There is extensive anecdotal evidence to support this proposition, including the very high levels of anti-social and illegal activities seen online such as file-sharing in breach of copyright, the consumption of indecent and obscene content and high levels of insensitive or harmful speech.“* Der fehlende physische Kontakt zwischen den Individuen erschwert überdies bereits die Entstehung sozialer Normen. Mit dem physischen Kontakt entfällt ein wichtiger Faktor, der die Menschen in der gegenständlichen Welt zusammenschweißt und dazu bringt, gemeinsame Interessen zu verfolgen. Man könnte sagen, es gibt im Internet keine Nachbarn, oder, um die Umstände mit Webster (2002, 208) zu beschreiben: *„the move from a Realspace community of neighbours to a Cyberspace community of strangers.“* Zwar mag dem entgegengehalten werden, dass Nachbarschaft im Internet nicht über physische räumliche Nähe, sondern über Themen entsteht. Dies widerlegt jedoch nicht, dass physischer Kontakt auf das Verantwortungsbewusstsein einen wesentlichen Einfluss hat.

Globalität und Ubiquität: Handlungen im Internet wirken sich generell – jedenfalls theoretisch – global aus. Gleichzeitig bietet Globalität dem Handelnden Schutz vor Sanktionen. Dies gilt v. a. für die transnationale Verfolgung mit Rechtsmitteln. Gerade das Recht wird als eines der möglichen Ordnungssysteme für die Verantwortungszuschreibung angesichts des grenzenlosen Raums vor neue Herausforderungen gestellt.

Globalität erschwert zudem die Definition und Entstehung allgemeingültiger Wertvorstellungen und damit korrespondierenden sozialen Normen oder Gesetzen. Das Internet ist kein einheitlicher Kulturraum. Einstellung und Haltung zu bestimmtem Verhalten kann und wird im Internet aufgrund divergierender Wertvorstellungen oft sehr unterschiedlich sein. So z. B. die Haltung gegenüber Gewalt oder Nacktheit im Vergleich zwischen Europa und den USA (Machill/Waltermann 2000, 15). Dadurch kommt es z. B. zu einer themenbezogenen oder regionalen Fragmentierung von sozialen Normen.

Technizität: Wie man sich im Netz verhalten kann, wird stark durch die Verfügbarkeit und Beherrschbarkeit der Technik bestimmt. Handeln, das in der gegenständlichen Welt ohne Hilfsmittel möglich ist, setzt im Netz die Existenz und Benutzung technischer Mittel voraus, da es ein technisch basiertes Medium ist. Ohne Kommunikationsprotokolle, Server, Telekommunikationsnetze, Tools und Dienste ist Handeln im Internet nicht möglich. Während die physische Umgebung auf Gegebenheiten der Natur und deren Gesetzen basiert, ist die Netzarchitektur ein menschliches Produkt (Lessig 1998, 1999). Aufgrund dessen sind im Internet die Architekten und Anbieter als neue Verantwortungssubjekte zu berücksichtigen, die in der gegenständlichen Welt allenfalls ein übernatürliches Pendant haben (z. B. Gott).

Dezentralität: Im Internet wird kopiert. Dadurch verliert der Handelnde schnell die Kontrolle über die Handlungsfolgen, etwa wenn sich eine beleidigende Aussage viral im Netz verbreitet. An einer solchen Folge haben mehrere teil und sind u. U. damit gemeinsam verantwortlich.

Verkörperung und Unvergänglichkeit: Handlungen im Netz werden meist verkörpert, gespeichert, dauerhaft festgehalten. Während Aussagen im persönlichen Gespräch flüchtig sind, sind sie im Netz verkörpert. Das Netz kann zwar vergessen, die Verkörperung kann verschwinden oder entfernt werden. Hierauf hat der individuelle Akteur aber oft nur sehr eingeschränkten Einfluss und kann daher nur eingeschränkt Verantwortung tragen. Aus diesem Grund wird etwa die Frage gestellt, ob man den Nutzern nicht ein „Recht auf Vergessenwerden“ zuerkennen und die Verantwortung für dessen Realisierung Diensteanbietern zuschreiben sollte (Meyer-Schönberger 2010, EU-Kommission 2012).

VII. Wer trägt Verantwortung im Internet? Verantwortungssubjekte (Akteure) und deren Rollen

Im Prinzip sind die handelnden Akteure im Internet dieselben wie in gegenständlichen Lebensräumen, also Bürger, die Wirtschaft und ihre Interessenvertretungen, nichtstaatliche Institutionen (NGO), religiöse Organisationen, Medien und der Staat. Als weiterer wichtiger Akteur haben die Architekten, Entwickler und Beherrscher der technischen Infrastruktur und der Tools, die das Internet technisch ausmachen, großen Einfluss. Hierzu zählen neben Zertifizierungsstellen, Registraren und Standardisierungsgremien v. a. die Anbieter der Telekommunikationsnetze, die Zugangsprovider, Plattform- und Suchmaschinenanbieter und andere *gate keeper*. All diese Akteure sind Teil eines komplexen Beziehungsgeflechts mit sich überschneidenden Verantwortungsbereichen.

Die Beziehungsgeflechte im Internet unterscheiden sich zum Teil erheblich von der gegenständlichen Welt. Handeln im Internet hat häufig einen anderen, nicht selten weiterreichenden, Effekt auf Andere. Globalität und Ubiquität führen dazu, dass Handlungen sich generell über Grenzen und Kulturkreise hinaus auswirken oder auswirken können. Staatliches Handeln hat oft grenzüberschreitende Wirkung und betrifft Bürger, denen gegenüber der souveräne Staat keine demokratische Legitimation hat

(Barlow 1996). Dezentralität und dauerhafte Verkörperung können dazu führen, dass Handlungen für den Einzelnen unüberschaubare Auswirkungen haben, die wiederum nur von anderen begrenzt werden könnten. Diese und andere Umstände machen es im Zweifel erforderlich, dass Verantwortungsbereiche im Internet neu geordnet und Rollen neu beurteilt werden müssen.

Die Zuordnung von Verantwortung bei einer Vielzahl denkbarer Verantwortungssubjekte bewegt sich in einem Spannungsfeld von Gerechtigkeits- und Effizienzerwägungen. Um sich im Rahmen eines Digitalen Kodex der Frage zu nähern, wer welche Verantwortung im Internet tragen und wie sie zugewiesen werden sollte, erscheint es zunächst sinnvoll zu ergründen, wie sich Handeln im Internet in konkreten Konstellationen auf andere auswirkt. In der Auswirkung von Handlungen auf Dritte liegt ein wichtiger Indikator für die Verantwortungszuweisung. Wessen Handlungen großen Einfluss auf die Freiheiten anderer haben, trägt viel Verantwortung und muss sich entsprechend verhalten.

Neben dem Verursacherprinzip sind bei der Zuordnung von Verantwortung andere Faktoren zu berücksichtigen, um ungerechtfertigte Ergebnisse oder Dysfunktionalitäten zu vermeiden. Verantwortung muss Grenzen haben, die sich nicht nur an dem theoretisch Möglichen, sondern auch dem praktisch Machbaren und subjektiv Zumutbaren orientieren müssen. Insofern kann es sinnvoll sein, Verantwortung durch Adäquanzbeschränkungen zu reduzieren oder zu verlagern. Wer mit einfachen Mitteln unerwünschte Handlungsfolgen vermeiden kann, ist gegebenenfalls eher verantwortlich als der, dem dies nur unter großem Aufwand möglich ist, auch wenn er die Handlungsfolgen gar nicht selbst unmittelbar verursacht hat. Wer unmittelbare Handlungsmacht hat, ist vorrangig gegenüber dem verantwortlich, der nur mittelbaren Einfluss hat.

Angesichts dieser Faktoren zeigt sich eine wichtige Aufgabe für das Projekt „Digitaler Kodex“: Um ein Verantwortungskonzept für das Internet zu entwickeln, wäre es wichtig, den Akteuren Rollen zuzuordnen und sie nach Verantwortungsarten und -bereichen zu ordnen, also die Frage zu beantworten, wem angesichts seines Wissens und seiner Handlungsmacht welche Verantwortung zuzuschreiben ist.

VIII. Wie kann Verantwortung im Netz zugewiesen und gesteuert werden?

Die herrschenden sozio-ökonomischen Regulierungstheorien gehen davon aus, dass das Internet nicht ohne Steuerung auskommt. Dies gilt auch und besonders für die Verteilung von Verantwortung. Dass sich Verantwortung sinnvoll, gerecht und effizient „von selbst“ und ohne Steuerung verteilt, ist in komplexen Handlungsräumen wie dem Internet nicht zu erwarten. Das komplexe System von Verantwortlichkeiten in der Gesellschaft wird sich nicht vollständig selbst regulieren, weder im noch außerhalb des Internets.

Wer diese Aufgabe übernehmen sollte und welche Mittel hierbei eingesetzt werden können, wird unterschiedlich beurteilt. Die Cyberliberalistische Schule (*Cyberlibertarian School*, vgl. Murray, 2011, 269), eine frühe Strömung im Diskurs über die Steuerung des Netzes ging davon aus, dass sich das Internet jedenfalls nicht mit staatlichen Mitteln steuern und regulieren lasse (vgl. Barlow und Johnson/Post, beide 1996). Zum einen seien die Regierungen souveräner Nationalstaaten nicht legitimiert, das Netz zu regieren. Da sich jede Regulierung unweigerlich grenzüberschreitend auf alle Nutzer auswirke, fehle es dem Nationalstaat an Legitimation. Zum anderen könnten Nationalstaaten das Verhalten im Netz ohnehin nicht wirksam kontrollieren. Hieraus wird die Forderung abgeleitet, das

Netz vollständig der Selbstregulierung zu überlassen (dagegen Murray 2011, 271, Goldsmith 1998, 1200). Damit trüge das Individuum sämtliche Verantwortung zur Ordnung von Verantwortlichkeiten und soziale Normen wären das einzige Ordnungsmittel.

Die herrschenden Regulierungstheorien sehen eine reine Selbstregulierung des Netzes durch seine Nutzer jedoch als utopisch an und bezweifeln die von den Cyberliberalisten vorgebrachten Argumente. Nach den *Cyberpaternalisten* (siehe z. B. Reidenberg 1998, Lessig 1999) ist die Verantwortung des Einzelnen im Gegenteil eher gering. Die Handlungsmöglichkeiten des Individuums seien gerade im Netz aufgrund von vier externen Faktoren ganz erheblich eingeschränkt. Recht, (soziale) Architektur⁴, soziale Normen und der Markt hätten auf die Handlungsoptionen des Individuums so großen Einfluss, dass der einzelne Nutzer einem von außen gesteuerten *pathetic dot* gleiche (daher wird die Lehre auch als *Pathetic Dot Theory* bezeichnet, vgl. Lessig 1998, 1999). Wäre dem zu folgen, trüge das Individuum kaum Verantwortung. Mehr oder weniger jede Verantwortung würde von der Gesellschaft, der Politik, der Wirtschaft und den Architekten/Gatekeepern getragen.

Die *Network Communitarian School* (Murray 2011, 276) schlägt eine Brücke zwischen Cyberliberalisten und -paternalisten. Die Netz-Kommunitaristen stimmen letzteren darin zu, dass die Faktoren Recht, Markt, soziale Normen und Technik handlungsbeschränkende und damit steuernde Wirkung haben. Allerdings steht das Individuum hiernach nicht isoliert da, sondern ist Mitglied einer starken Gemeinschaft. Die Gemeinschaft wiederum hat auf die steuernden Faktoren erheblichen Einfluss. Das Recht werde durch die von ihr gewählten Volksvertreter gemacht. Die Gemeinschaft beeinflusse den Markt, der nur ein Reflex ihrer (monetären) Wertvorstellungen und Nachfrage sei. Soziale Normen seien ohnehin nur eine Kodifizierung gesellschaftlicher Werte. Auch auf den Code übe die Gesellschaft mittelbar, also über die von ihr mitgestalteten Steuerungsfaktoren Recht, soziale Normen und Markt, Einfluss aus. Dies zeige sich z. B. daran, dass DRM-Systeme auf dem Musikmarkt erst entschärft wurden und dann verschwunden sind (Murray 2011, 277).

Wie in der Cyberliberalistischen Lehre haben die Bürger bzw. die Zivilgesellschaft hiernach die (*ex ante*) Verantwortung, die Rahmenbedingungen zu schaffen, damit Verantwortung effizient und gerecht zugeschrieben wird. Sie haben es selbst in der Hand, für gute Gesetze zu sorgen, indem sie die richtigen Politiker wählen, sie können Transparenz erzwingen, indem intransparente Dienste nicht genutzt werden und sie können den Markt steuern, indem sie sich gegen unfaires Marktverhalten mit Kaufverweigerung oder gar Shit-Storms wehren. Um ihre Macht als Gruppe, als Community, ausüben zu können, müssen die Individuen in einen Dialog treten, sich abstimmen und konsolidieren. Ihre Macht üben sie – anders als in der Vorstellung der Liberalisten – zu großen Teilen über Repräsentanten (wie der Politik) aus.

⁴ Mit sozialer Architektur meint Lessig (1998, 1999) alle Eigenschaften der Welt, die das Handeln beeinflussen, seien sie vorgefunden oder erschaffen. Beispiel sind Naturgesetze, geographische Umstände usw. Die maßgebliche soziale Architektur im Netz ist der Code, also die Technologie, auf der das Netz basiert.

IX. Mechanismen zur Zuweisung der Verantwortung im Internet

Zur Zuweisung und Verteilung von Verantwortung im Internet stehen vielfältige Mechanismen zur Verfügung. Diese können isoliert angewendet werden, werden sich aber in der Regel ergänzen.

1. Gesetze

Traditionell wird Verantwortung hauptsächlich durch Gesetze zugeordnet. Gesetze steuern Verantwortlichkeit durch Androhung von staatlich verordneten Sanktionen (Lessig, 1998). Sie werden zwar von Politikern gemacht, diese werden jedoch, jedenfalls in Demokratien, von den Bürgern gewählt. Auch die Bürger tragen also für die Gesetze eine gewisse mittelbare Verantwortung.

Gesetze stoßen im Hinblick auf ihre Effizienz und andere Faktoren im Internet zunehmend auf Grenzen. Recht ist traditionell eine territoriale Materie. Das Mandat des souveränen Nationalstaats, Recht zu setzen, beschränkt sich grundsätzlich auf das eigene Territorium. Transnationale Rechtssetzung ist zwar weder eine Neuigkeit noch ist sie unmöglich, wie es die Cyberliberalisten behaupten⁵. Als grenzenloser Handlungsraum für die ganze Gesellschaft übertrifft das Internet in seiner Komplexität jedoch bisherige transnationale Regelungsmaterien (wie internationales Seerecht o. ä.) erheblich.

Ob durch Gesetze oder andere Normen: International einheitliche Verhaltensnormen für das Internet zu schaffen, ist äußerst schwierig, da sich der Handlungsraum Internet über jede kulturelle Grenze hinweg erstreckt. Erschwerend hinzu kommt bei Gesetzen, dass ihre regelnde Wirkung in besonderem Maß auf ein funktionierendes Sanktions- und Durchsetzungssystem angewiesen ist. Die Rechtsverfolgung funktioniert jedoch bislang im transnationalen Raum nur eingeschränkt. Zwischenstaatliche Rechtshilfemodelle beispielsweise sind längst noch nicht so weit ausgeprägt, dass man von einer effizienten internationalen Durchsetzung von rechtlichen Verantwortungs- und Verhaltensnormen sprechen könnte. Soziale Normen können hier Vorteile haben und Gesetze u. U. als Steuerungsform ersetzen oder ergänzen. Da sie von der Gemeinschaft selbst kontrolliert werden, sind staatlich-formalisierte Durchsetzungsmechanismen nicht erforderlich.

Die Effizienz von Gesetzen als Ordnungsmechanismus für das Internet wird zudem häufig angesichts der langwierigen Prozesse angezweifelt, die für ihre Entwicklung, Umsetzung und Anpassung erforderlich sind. Rechtssetzungsmechanismen (v. a. supranationale) könnten mit der Dynamik im Internet häufig nicht Schritt halten (Hirsch 2010). Auch der Umstand, dass Regelungsgegenstände im Internet häufig sehr technisch, komplex, neu und ohne Vorbild sind, wirkt sich auf die Effizienz von Gesetzen als Steuerungsmechanismus aus. All diese Faktoren können dazu führen, dass Gesetze an den eigentlichen Notwendigkeiten vorbei regulieren. Fraglich ist jedoch, ob diese Befürchtungen das Recht als Ordnungsmechanismus an sich betreffen, oder nur in bestimmten Konstellationen greifen. So wäre zu überlegen, ob der negative Einfluss der genannten Faktoren davon abhängt, ob es sich

⁵ Cyberliberalisten wie Barlow (1996) oder Johnson/Post (1996) sahen die Schwierigkeit transnationaler Regelungen als so gravierend, dass sie den souverän-territorialen Nationalstaaten jegliche Legitimation zur Regulierung von Internet-Sachverhalten absprechen wollen (dagegen Murray 2011, 269/270, Goldsmith, 1998).

um Regelungen mit konkretem Bezug oder um solche handelt, in denen die „großen Linien“, Rahmenregelungen oder Grundprinzipien (etwa Staatsverfassungen) definiert werden.

2. Soziale Normen

Soziale Normen sind gesellschaftliche Verhaltensvorschriften. Sie können, müssen aber nicht in einer bestimmten Form kodifiziert sein. Sie werden durch die Gesellschaft gesetzt und auch kontrolliert, Verstöße werden von der Gesellschaft selbst sanktioniert. Da sie dem sozialen Wandel unterliegen und gesellschaftlich und kulturell bedingt sind, sind soziale Normen von Gesellschaft zu Gesellschaft verschieden. Zudem werden sie häufig bereichsspezifisch sein, wie z. B. ein Verhaltenskodex für die Nutzer von Internet-Foren.

Soziale Normen können in Bezug auf ihre Legitimität und Effizienz gegenüber anderen Mitteln zur Zuweisung von Verantwortung, wie v. a. Gesetzen, Vorteile haben. Sie werden von den Betroffenen selbst gesetzt und basieren auf tatsächlichen gemeinsamen Wertvorstellungen. In Gesetzen werden Wertvorstellungen dagegen über einen „politischen Filter“ umgesetzt, der vielen Einflussfaktoren unterliegt. Hierdurch kann es zu Verfälschungen kommen. Ein weiterer Vorteil kann darin liegen, dass soziale Normen gemeinsam mit den Wertvorstellungen selbst entstehen und auch wieder entfallen. Dadurch ist die Gefahr, dass Regel und Realität zunehmend voneinander abweichen, hier potenziell geringer als bei Gesetzen. Letztere zu ändern oder abzuschaffen bedarf eines formalen Akts, der generell viel Zeit in Anspruch nimmt und oft gar nicht erfolgt.

Bedient man sich sozialer Normen als Mittel zur Zuschreibung von Verantwortung, so ist zu bedenken, dass das Internet ein kultur- und gesellschaftsübergreifender Handlungsraum ist. So etwas wie allgemeingültige, umfassende Verhaltensnormen für *die Internetnutzer* wird es nicht geben, da die viel beschworene „Netzgemeinde“ (Internet-Community) nicht existiert. Sie ist so vielfältig und amorph wie die Gesellschaft an sich. Soziologen (z. B. Sunstein 2001, Castells 2001, Webster 2002) sehen sogar einen Trend zu einer „Balkanisierung des Internets“ (Sunstein 2001, 61). Es stehe zu befürchten, dass im Netz zunehmend hochspezialisierte Mikro-Gesellschaften entstehen, die keine gemeinsamen Werte haben oder verfolgen, sondern sich nur noch um ihre speziellen Individualinteressen sorgen. Ein umfassendes System sozialer Normen zu etablieren und zu kodifizieren würde hierdurch zusätzlich erschwert.

3. Collaborative Governance und Regulierte Selbstregulierung

Ebenso wie Verantwortung in der Gesellschaft häufig über soziale Normen zugewiesen werden kann, können Wirtschaftsgruppen durch *Codes of Conduct* oder ähnliche Regelwerke Verantwortung übernehmen. Eine solche Selbstregulierung hat gegenüber gesetzlicher Regelung die auch schon bei sozialen Normen genannten praktischen Vorteile. Sie ist im Zweifel weniger statisch. Sie gilt häufig nicht territorial, sondern sektorspezifisch. Auch könnte man annehmen, dass gegen selbst gesetzte Regeln, z. B. aus moralischen Gründen, weniger leichtfertig verstoßen wird als gegen oktroyierte Gesetze.

Reine Selbstregulierung wird in der Regel allerdings nur funktionieren, wenn starke intrinsische Motive vorhanden sind. Je höher die Ambivalenz und der Anteil extrinsischer Faktoren, desto geringer sind

die Erfolgsaussichten, da es an effizienten Druckmitteln fehlt (Hirsch 2010)⁶. Insofern ist wohl davon auszugehen, dass soziale Normen, die vorwiegend intrinsisch motiviert sind, als Selbstregulierungsinstrument der Gesellschaft effizienter sind als Verhaltenskodizes von Wirtschaftsgruppen. Letztere sind meist auch erheblich extrinsisch motiviert, z. B. um staatliche Regulierung zu vermeiden.

Das Konzept der Co-Regulierung oder regulierten Selbstregulierung versucht dieses Manko zu verhindern, indem externe Druckmittel implementiert werden, wie z. B. staatliche Überwachung durch Regulierungsbehörden. Hängt mit dem Gegenstand der Selbstregulierung große Verantwortung, etwa für Grund- oder Freiheitsrechte Dritter zusammen, wird eine staatliche Steuerung in der Regel obligatorisch sein (siehe Brown, 2010).

4. Architektur/Code

Da das Internet auf Code basiert, kann Verhalten über dessen Gestaltung sehr effizient gesteuert werden. Die Steuerung wirkt – anders als Gesetze oder soziale Normen – unmittelbar handlungsleitend. Über die Ausgestaltung der Technik können Handlungen, und damit Verantwortung gänzlich unterbunden, Akteure ausgeschlossen oder benachteiligt werden.

Als Basisschicht des Internets ist die Technik ein mächtiges Instrument, um Verantwortung entstehen zu lassen, zu vermeiden, zuzuordnen oder durchzusetzen (McIntyre/Scott 2008). Die Steuerung über Code steht jedoch in einem Spannungsfeld zur Freiheit. Je mehr Einschränkungen die Technik aufweist, desto weniger frei ist die Nutzung des Internets.

Den Herrschern über die Technik, wie Zertifizierungsstellen, Registraren und Standardisierungsgremien, Netzbetreibern, Zugangsprovidern, Plattform- und Suchmaschinenanbietern und anderen *gate keepers* kommt daher große Verantwortung zu. Zum einen tragen sie Verantwortung dafür, Handlungsoptionen zu eröffnen oder zu verhindern, was auf eine Mitverantwortung für die Internetnutzer hinausläuft. Hiermit verbunden ist die Verantwortung für die Nutzungsfreiheit. Würde z. B. die Angabe personenbezogener Information bei sozialen Netzwerken technisch unterbunden, würde den Nutzern viel Eigenverantwortung abgenommen. Allerdings würde so auch die Nutzungsfreiheit massiv eingeschränkt.

An diesem Beispiel zeigt sich ein weiteres Spannungsfeld. Wirtschaftliche Akteure tragen auch wirtschaftliche Verantwortung, z. B. gegenüber ihren Shareholdern oder Arbeitnehmern. Ein soziales Netzwerk, in dem personenbezogene Informationen nicht verwendet werden können, kann im Zweifel nicht funktionieren. Die wirtschaftliche Verantwortung als Unternehmen wird häufig mit anderen Verantwortungsrollen kollidieren.

⁶ Dies hat sich in der Vergangenheit schon verschiedentlich gezeigt, u. a. im Hinblick auf das Datenschutzrecht im Internet. Bislang hat es keine Selbstregulierungsinitiative geschafft, sich auf einen allgemeingültigen Ansatz zu einigen und diesen auch konsequent durchzuhalten. Ambitionierte Initiativen sind im Gegenteil meist gescheitert. Beispiele sind etwa die Online Privacy Alliance oder die Network Advertising Initiative (siehe zu den Gründen und weiteren Beispielen Hirsch 2010, 34 ff.). Wie gerade publik wurde, ist auch der in Deutschland gestartete Versuch gescheitert, einen Kodex zur Selbstregulierung für soziale Netzwerke auf den Weg zu bringen (siehe <http://www.telemedicus.info/article/2569-Kodex-zur-Selbstregulierung-fuer-soziale-Netzwerke-gescheitert.html>).

Angesichts der Macht des Codes wird es meist geboten erscheinen, auf die Architekten regulierend einzuwirken. Die Cyberpaternalisten weisen die Verantwortung hierfür dem demokratisch legitimierten Gesetzgeber zu. Andere, wie Viktor Mayer-Schönberger oder Evgeny Morozov, fordern Maßnahmen regulierter Selbstregulierung, etwa die Einführung einer Algorithmus-Ethik, die von einer Art TÜV überwacht werden könnte⁷.

X. Fazit

Die Entstehung, Verteilung und Zuweisung von Verantwortung im Internet unterliegt in vielerlei Hinsicht anderen Umständen und Rahmenbedingungen als in der gegenständlichen Welt. Insofern müssen neue Konzepte beleuchtet und bestehende Konzepte hinterfragt werden. Rollen müssen neu definiert und Zuweisungskonzepte im Zweifel anders bewertet werden. Eine Hauptaufgabe im Projekt „Digitaler Kodex“ wird darin liegen, eine Systematik hierfür zu entwickeln und die Frage zu beantworten, ob und wie sie in einem Digitalen Kodex umgesetzt werden kann.

⁷ Siehe <http://www.golem.de/news/code-raus-aus-der-digitalen-unmuendigkeit-1305-99125.html>.

Literatur

Barlow, John Perry (1996): A Declaration of the Independence of Cyberspace, <https://projects.eff.org/~barlow/Declaration-Final.html>

Bayertz, Kurt (1995): Politik und Ethik

Brown, Ian (2010): Internet Self-Regulation and Fundamental Rights in „Index on Censorship, Vol. 1, March 2010“, <http://ssrn.com/abstract=1539942>

Castells, Manuel (2001): The Internet Galaxy: Reflections on the Internet, Business, and Society, Oxford University Press

Ellickson, Robert (1991): Order without Law: How Neighbors Settle Disputes, Harvard University Press

Europäische Kommission: Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), Brüssel, den 25.1.2012, KOM(2012) 11 endgültig

Goldsmith, Jack L. (1998): Against Cyberanarchy, 65 University of Chicago Law Review S. 1199 ff. (<http://cyber.law.harvard.edu/property00/jurisdiction/cyberanarchyedit.html>)

Hirsch, Dennis D. (2010): The Law and Policy of Online Privacy: Regulation, Self-Regulation or Co-Regulation?, http://works.bepress.com/dennis_hirsch/1

Johnson, David R./David G. Post (1996): Law And Borders: The Rise of Law in Cyberspace, Stanford Law Review 48, 1367

McIntyre, TJ/Scott, Colin (2008): Internet Filtering: Rhetoric, Legitimacy, Accountability and Responsibility, in Brownsword, R./Yeung, K. (Hrsg.): Regulating Technologies, Oxford Hart Publishing, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1103030

Lessig, Lawrence (1998): „The New Chicago School“. The Journal of Legal Studies 27 (S2): 661–691

Lessig, Lawrence (1999): „The Law of the Horse: What Cyberlaw Might Teach“, 113 Harvard Law Review, S. 501

Lessig, Lawrence (1999, 2006): Code and other Laws of Cyberspace, zweite Auflage

Luhmann, Niklas (2004): Law as a Social System, Oxford Unternehmenspartner

Machill, Marcell/Waltermann, Jens: Verantwortung im Internet, 2000

Mansell, Robin (ed.) (2002): Inside the Communication Revolution: Evolving Patterns of Social and Technical Interaction, Oxford University Press

Mayer-Schönberger, Viktor (2010): Delete. Die Tugend des Vergessens in digitalen Zeiten, Berlin University Press

Murray, Andrew D. (2011): „Internet Regulation“, Handbook on Regulation. Ed. David Levi-Faur, http://works.bepress.com/andrew_murray/4



Picht, Georg (1969, 2004): Der Begriff der Verantwortung. In: ders.: Wahrheit, Vernunft, Verantwortung. Philosophische Studien, 318-342

Reidenberg, Joel (1998): „Lex Informatica: The Formulation of Information Policy Rules Through Technology“, 76 Texas Law Review 553

Sunstein, Cass (2001): Republic.com, Princeton University Press

Webster, Frank (2002): Theories of the Information Society (2ed)