DIVSI
Deutsches Institut
für Vertrauen und
Sicherheit im Internet

www.divsi.de

Braucht Deutschland einen Digitalen Kodex?

Braucht Deutschland einen Digitalen Kodex?

VERANTWORTUNG, PLATTFORMEN UND SOZIALE NORMEN IM INTERNET

Eine Untersuchung des iRights.Lab im Auftrag des
Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI)

DIVSI
Deutsches Institut für Vertrauen und Sicherheit im Internet

iRIGHTS lab

Hamburg, Mai 2014

Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI)
Mittelweg 142, 20148 Hamburg
www.divsi.de
Matthias Kammer, Direktor
Joanna Schmölz, Wissenschaftliche Leitung
Michael Schneider, Leitung Kommunikation
Meike Demattio, Projekte
Dr. Dirk Graudenz, Projektleitung

iRights.Lab
Almstadtstraße 9/11, 10119 Berlin
www.irights-lab.de
Philipp Otto, Projektleitung
Dr. Till Kreutzer, Autor
Matthias Spielkamp, Autor
John Weitzmann, Autor
Unter Mitwirkung von: Valie Djordjevic, Jörg Garbers, Wiebke Glässer, Tom Hirche, Hanka Holzapfel, Susanne Lang, Jana Maire, Julia Schrader

INHALTSVERZEICHNIS

Braucht Deutschland einen Digitalen Kodex?

Wir leben in einer Phase des Umbruchs. Dieser Satz gilt auch und besonders im Hinblick auf das Internet und die Entwicklung unserer Gesellschaft in der digitalen Zeit. Äußere „Parameter" wie Plattformen, Kommunikationsmöglichkeiten und Endgeräte ändern sich in sehr kurzen Rhythmen. Anregend und mitreißend für viele, kompliziert und oftmals unverständlich für alle Nicht-Technikbegeisterten.

Egal, welche Sichtweise der Einzelne präferiert – kaum einer wird bestreiten, dass das gigantische Spektrum der digitalen Angebote des Internets unser Leben auf vielen Feldern erleichtert. Gleichwohl sollten wir dabei die Schattenseiten nicht übersehen. Denn das Internet ist voller Fallstricke. Manche Methoden und Geschäftsgebaren im Netz sind unseriös. Viele haben das als Opfer schon leidvoll erfahren müssen. Umso mehr benötigen wir verlässliche Vertrauensanker. Doch wo und wie diese finden?

Das Geschehen im Netz wird zunehmend komplexer und hat gleichzeitig für ein kaum erklärbares Phänomen gesorgt. Zwar nutzen immer mehr Menschen immer öfter Angebote der sich laufend vergrößernden Internet-Palette. Doch kaum einer hinterfragt, worauf er sich dabei einlässt.

Diese Nachlässigkeit (Gleichgültigkeit?) kann zum Tsunami für die Integrität der eigenen Daten werden. Es ist deshalb an der Zeit für allgemein gültige und anerkannte Antworten auf vor allem zwei Fragen:

Welche Regeln gelten überhaupt im Internet? Wer übernimmt die Verantwortung dafür, dass das Internet ein Raum wird, in dem jeder vertraulich und sicher kommunizieren kann?

Das DIVSI hat daher ein Projekt gestartet, das sich dieser Fragestellung annimmt. Wir wollen ausloten, ob ein Digitaler Kodex ein geeignetes Mittel zur Lösung des Problems ist. Der hier vorgelegte Bericht zeigt, dass ein solcher Ansatz sehr lohnend sein kann.

Überlegungen unseres Schirmherrn Prof. Dr. Roman Herzog haben bereits vor gut einem Jahr in die genannte Richtung gewiesen. Der Altbundespräsident war und ist überzeugt, dass „in unserem digitalen Zeitalter Fragen der Ethik einen zunehmend größer werdenden Raum einnehmen". Prof. Herzog sprach in diesem Zusammenhang von „Leitplanken, die uns auf dem richtigen Weg halten. Ein Digitaler Kodex, von allen Verantwortlichen getragen, könnte ein Weg dahin sein."

Ich stimme dem vorbehaltlos zu. Die permanenten Veränderungen im Internet haben längst Auswirkungen über das rein Technische hinaus. Sie bringen erhebliche Veränderungen für das Zusammenleben aller Menschen mit sich. Sowohl, was das persönliche Miteinander angeht, als auch, was die Beziehungen des Einzelnen zur Wirtschaft und zum Staat betrifft.

Unsere in den beiden vergangenen Jahren veröffentlichten Studien zu den DIVSI Internet-Milieus haben gezeigt, dass die Anforderungen der Nutzer sehr

Foto: Frederike Heim

Matthias Kammer,
Direktor
DIVSI – Deutsches Institut für Vertrauen und Sicherheit im Internet

unterschiedlich sind. Im Hinblick auf die Verantwortung im Internet gilt: Je nach Milieu wird sie beim Staat, bei den Anbietern oder beim Nutzer selbst gesehen.

Am deutlichsten wird der Wandel bei Kindern, Jugendlichen und jungen Erwachsenen, wie die im März 2014 publizierte „DIVSI U25-Studie" gezeigt hat. Die jungen Befragten „gehen nicht mehr online", sondern sind „always online". Das Internet ist für sie unverzichtbarer Teil des Lebens geworden, ein Leben „ohne" ist fast nicht mehr vorstellbar. Auch sorgt das Netz bei ihnen für ein geändertes Unrechtsempfinden im Vergleich zu älteren Generationen. „Erlaubt ist, was alle machen" gilt ihnen als Richtschnur – jedenfalls für das Herunterladen von Filmen, Musik oder Spielen.

Digitale Kommunikation hält sich nicht an geografische Grenzen, die bislang unsere rechtlichen Räume überschaubar und (zu)greifbar machten. Deshalb ist das aktuelle Problem so unendlich komplex. Und deshalb tun wir vielleicht gut daran, gemeinsam einen Digitalen Kodex zu entwickeln.

Sicherlich existieren bereits rechtliche Rahmenbedingungen. Doch weltweit agierende Internet-Unternehmen wissen, wo Schlupflöcher sind, und erschweren es, geltendes Recht überhaupt durchzusetzen. Auch deshalb ist eine neue, andere Form des Miteinanders im Internet erforderlich. In diesem Kommunikationsraum gibt es keine physische Präsenz. Menschliches Handeln ist hier nach neuen Maßstäben zu messen.

Es liegt an uns, diese Richtschnüre zu finden und durchzusetzen. Noch ist Zeit dafür. Denn auch wenn die Entwicklung der digitalen Welt hin zu einem globalen Kulturraum bereits weit fortgeschritten erscheint, befinden wir uns erst in der zweiten Dekade einer historischen Entwicklung.

Und so, wie diese fundamentale Umwälzung unaufhaltbar fortschreiten wird, werden sich die Formen des Miteinanders der Akteure im Netz weiter ausdifferenzieren. Es wäre fatal, tatenlos zuzusehen, in welche Richtung diese Entwicklung geht. Ein Schulterzucken nach dem Motto „Ich kann ohnehin nichts ändern" ist deswegen sicherlich der falsche Weg. Positive Aktivitäten sind das Gebot der Stunde. Dazu gehören auch kritische Ansätze. Beispielsweise so: Benötigen wir für das digitale Zeitalter im rousseauschen Sinne vielleicht einen neuen Gesellschaftsvertrag?

Unser Bericht zur Frage, ob Deutschland einen Digitalen Kodex braucht, steuert nicht nur zu diesem Gedanken Anregungen bei. Er bietet darüber hinaus generelle Anstöße, über die nachzudenken sicherlich lohnt. Ich freue mich auf Ihr Feedback zu einem Fragenkomplex, der kaum hoch genug angesiedelt sein kann.

Ein Digitaler Kodex kann eine Antwort sein

Der digitale Raum sieht sich massiven Vereinnahmungen ausgesetzt. Unternehmen definieren unseren digitalen Alltag. Bunte Verkaufsplattformen, Gadgets, Text- und Videoschnipsel täuschen darüber hinweg, dass ein großer Teil der Kommunikation im Netz inzwischen nur noch um den Preis unserer Daten möglich ist. Im Rahmen staatlicher Überwachung werden viele unserer Bewegungen im Internet mitgeschnitten, oftmals ohne konkreten Anlass einer Straftat oder sonst eines nicht staatskonformen Verhaltens. Es geht von mehreren Seiten um die maximale Kartografierung unserer Existenz im Internet. Gigantisch und eigentlich unvorstellbar.

Eine Auseinandersetzung mit diesen Veränderungen ist nicht nur geboten, sondern unerlässlich, denn zur flächendeckenden Vereinnahmung kommt die flächendeckende Sprachlosigkeit. Wie soll man reagieren? Ist es nicht höchste Zeit, ins Lenkrad zu fassen und abrupt die Richtung zu ändern, um zumindest grundsätzliche Rahmenbedingungen der Nutzung, des Austausches und der Kontrolle sicherzustellen oder zumindest die Hoheit über die Gestaltung des digitalen Lebensraumes wieder zu übernehmen? Wer sind unsere Statthalter, und wer kümmert sich darum?

Im April 2013 hat das Deutsche Institut für Vertrauen und Sicherheit im Internet das iRights.Lab mit dem Projekt „Braucht Deutschland einen Digitalen Kodex?" beauftragt. Ziel des Projekts war die Klärung, ob es neben dem Gesetzeskanon und industriellen Selbstverpflichtungen eines neuen Instrumentariums – eines Digitalen Kodex – bedarf, um Entwicklungen im Netz so zu steuern, dass die legitimen Interessen aller Akteure angemessen berücksichtigt werden. Es hat sich im Verlauf des Projekts sehr schnell gezeigt, dass die Frage, wem Verantwortung zugeschrieben wird und wer diese nach dem Status quo innehat, eine zentrale Rolle spielt. In einem zweiten Schritt ging es um den Umgang von Anbietern und Nutzern mit personenbezogenen Daten in sozialen Netzwerken.

Fehlen dem Internet an vielen Stellen rechtliche Regeln? Dem ist unserer Meinung nach nicht so, wir halten das Netz vielfach sogar für überregu-

Foto: Jürgen Keiper

Philipp Otto,
Leiter des Projekts „Braucht Deutschland einen Digitalen Kodex?" sowie Partner des Think Tanks iRights.Lab

liert. Eines der Ergebnisse des Projekts ist, dass insbesondere explizite und implizite Vereinbarungen in Form von allgemein anerkannten gesellschaftlichen Normen, die als nicht gesetzliche Spielregeln einen „Common Sense" bei den Nutzerinnen und Nutzern wie auch den Anbietern und Regulatoren von Dienstleistungen im Netz bilden, eine Lösung sein können. Solche Regeln haben sich auch aufgrund der jungen Geschichte des Internets noch nicht in verbindlicher Form herausbilden können – es herrscht vielfach keine Einigkeit darüber, was eigentlich richtig und was falsch ist oder wie man sich in bestimmten Situationen verhalten soll.

Ein Digitaler Kodex, für konkrete Anwendungsgebiete und Akteure, kann großen Nutzen stiften, entscheidend wird aber seine Ausgestaltung sein – auch im Hinblick auf internationale Aspekte. Im Projekt haben wir zwei gegensätzliche Modelle entwickelt: den „moderierten digitalen Straßenkampf" und das Modell einer institutionalisierten Aushandlung. Die beiden Modelle adressieren unterschiedliche Aspekte der Begründung, Aushandlung und Überführung in ein wirkmächtiges Instrument.

Im Laufe des Projektes wurden über 50 ausgewiesene Experten aus Wissenschaft, Politik, Wirtschaft sowie aus Initiativen und Verbänden konsultiert. Teils kontrovers, aber immer bedeutend klar in der Position, haben diese Gespräche die Vielfalt möglicher Positionen zu Handlungsansätzen konturiert. Einige ausgewählte Ergebnisse sind in Form von Interviews und pointierten Zitaten in diesen Projektbericht eingeflossen.

Im Projekt war eine spannende Annäherung an ein komplexes Thema möglich. Es geht bei dem Thema um nichts weniger als die Frage, wie wir unsere digitale Zukunft gestalten wollen. Wir freuen uns über Ihre Anregungen.

1. Einleitung

Das Internet ist ein Kommunikations- und Handlungsraum, der als Massenmedium erst zwei Jahrzehnte alt ist. Deshalb steht die Ausbildung eines allgemeingültigen Konsenses für akzeptiertes Verhalten aller Akteure in diesem Raum auch noch ganz am Anfang. Deutlich wird dies daran, dass es grundsätzliche Konflikte gibt, die regelmäßig aufscheinen und für deren Lösung noch keine allgemein anerkannten Vorgehensweisen existieren. Einer der Gründe dafür ist, dass Kommunikation im Internet in ihrer Form und Reichweite keine direkte Entsprechung in der physischen[1] Welt hat. Ein prominentes Beispiel für einen solchen Konflikt ist der Umgang mit persönlichen Daten auf und durch Internet-Plattformen.

Die Verhaltensregeln, die bestimmen, wie wir in unserer Gesellschaft miteinander umgehen, haben sich im Laufe von Jahrhunderten herausgebildet und ausdifferenziert. Bei vielen Menschen ist das Gefühl entstanden, dass diese Regeln aus der analogen in der digitalen Welt nicht gelten oder funktionieren. Überkommene Mechanismen zur Regelsetzung, zur Zuordnung von Verantwortung und zur Steuerung von Verhalten stoßen im Netz[2] häufig an ihre Grenzen. Das gilt gleichermaßen für Gesetze, Selbstregulierungsansätze und soziale Normen, die das Verhalten im Netz steuern sollen. Diesem Umstand abzuhelfen stellt alle Akteure, vom individuellen Internet-Nutzer über den Staat bis zur Wirtschaft, vor große Herausforderungen. Was ist akzeptables Verhalten, und wie entwickeln sich die Normen, die es verbindlich machen?

Sich dieser Fragestellungen anzunehmen, ist eine der wichtigsten Aufgaben im digitalen Zeitalter. Das Netz ist Realität, und es verändert die Lebenswelt von Milliarden von Menschen. Längst gehen die Menschen nicht mehr ins Netz – wie man früher sagte –, sondern sie sind im Netz, zu jeder Zeit und an jedem Ort. Hier finden sich alle Facetten gesellschaftlichen Lebens, denn das Netz ist Teil desselben. Es ist nicht nur ein Kommunikations- oder medialer, sondern insbesondere auch ein sozialer Raum. Die Erschließung dieses Raums geht mit vielen Veränderungen einher, die sich erheblich auf die Frage auswirken, wie und mit welchen Mitteln der Umgang miteinander zu regeln ist.

1.1 Kommunikation im Netz

Die genannten Veränderungen betreffen alle Lebensbereiche: die Arbeits-, Freizeit- und Wirtschaftswelt ebenso wie die Politik. Beeinflusst wird zum Beispiel die Kommunikation, die gerade bei jüngeren Bevölkerungsgruppen zunehmend über soziale Netzwerke, *Instant* oder *Social Messaging*[3] und andere Werkzeuge stattfindet. Technisch basierte Kommunikation steht in vielen Fällen schon heute im Vordergrund.

Wenn die Teilnehmer beim Kommunizieren nicht physisch zusammenkommen, ändert sich das Kommunikationsverhalten. Regeln, die im körperlichen Umgang selbstverständlich sind, scheinen bei der technisch gestützten Kommunikation oft nicht zu

1 In diesem Dokument werden die Adjektive „physisch", „körperlich", „analog" und „gegenständlich" als Gegenpole zu „digital" und „virtuell" verwendet. Die Auswahl des jeweiligen Wortes erfolgte nach intendierter Ausprägung der Bedeutung.

2 Die Begriffe „Internet" und „Netz" werden in diesem Dokument im Wesentlichen als Synonyme benutzt.

3 „Instant Messaging" bzw. „Social Messaging" sind spezifische Kommunikationsformen im Internet, die durch Echtzeitanforderungen bzw. -ablauf auf den entsprechenden Plattformen charakterisiert sind.

gelten. Die Gründe hierfür sind vielfältig, wesentlich ist der Umstand, dass digitale Kommunikation keine physische Präsenz am selben Ort erfordert. Hinzu kommt, dass – anders als bei der direkten, physischen Kommunikation – bei der digitalen Kommunikation oft ein dritter Akteur zwischengeschaltet ist. Hinter der Technologie, die diese moderne Art der Kommunikation ermöglicht, steht ein Anbieter, der eigene Regeln setzt und viel Wissen über die Kommunikationsvorgänge und -inhalte anhäufen kann, wenn er nur will. Technisch sind dem – das hat der 2013 aufgedeckte NSA- und GCHQ-Überwachungsskandal gezeigt – offenbar keinerlei Grenzen gesetzt. Digitale Kommunikation setzt damit großes Vertrauen voraus. Vertrauen darin, dass die mächtigen Konzerne, Regierungen und anderen Akteure eben nicht alles tun, was technisch möglich ist, sondern sich an Grenzen halten. Auch Regeln können solches Vertrauen schaffen, allerdings nur, wenn sie effektiv sind, das heißt, wenn alle Akteure sie beachten.

Der Überwachungsskandal hat, zumindest für einen Zeitraum von einigen Monaten und bei Menschen mit hoher Internet-Affinität, das Vertrauen in den digitalen Raum Internet in seinen Grundfesten erschüttert, da er gezeigt hat, dass sich gerade die Mächtigen an viele Regeln, wie Datenschutzrechte oder Persönlichkeitsschutz, nicht halten. Ob sich in Zukunft aufgrund dieser Entwicklungen die Verhaltensweisen der Internet-Nutzer tatsächlich verändern werden, kann natürlich niemand voraussagen. Ein anderes Beispiel aus der jüngeren Vergangenheit zeigt aber, dass Internet-Nutzer Vertrauen nicht bedenkenlos gegen Bequemlichkeit eintauschen: Nach dem Kauf von WhatsApp durch Facebook im Februar 2014 haben sich Nutzer von WhatsApp abgewandt und damit begonnen, Alternativen zu suchen. Die zukünftige Entwicklung wird auch stark davon abhängen, was Internet-Nutzer unter Privatheit verstehen. Die Bedeutung dieses Begriffs wandelt sich – Jugendliche und junge Erwachsene erwarten von einem Gegenüber auf sozialen Netzwerken die Preisgabe einiger persönlicher Informationen, um sie oder ihn überhaupt ernst zu nehmen. Gleichzeitig wird sehr genau differenziert, welche Formen von Information online und welche nur offline weitergegeben werden.[4]

1.2 Konsum im Netz

Auch beim zunehmend beliebten Konsum über das Netz, sowohl beim klassischen Einkauf auf Online-Plattformen als auch beim Bezug digitaler Inhalte, spielen die oben genannten Faktoren eine große Rolle. In globalen Märkten agieren globale Akteure, die bei steigender Marktkonzentration immer größer und mächtiger werden. Sie sind längst in der Lage, das Kaufverhalten und persönliche Vorlieben zu analysieren. Im Zuge der rasanten technischen Innovation verstärkt sich die so entstehende Konzentration der Informationsmacht. In aller Munde ist derzeit etwa das „Internet der Dinge", das vieles einfacher und angenehmer machen soll. In der Tat: Wie praktisch können intelligente Heizungen sein, die Daten mit den Rechnern des Anbieters austauschen, um so stets automatisch für das perfekte Raumklima zu sorgen, und wie sehr erleichtern Kühlschränke den Alltag, die per Datenübermittlung verhindern, dass jemals etwas fehlt. Hier geht es um *Convenience*[5] im privaten Alltag der gesamten Bevölkerung – allerdings durchaus zumindest potenziell zulasten der Privatsphäre: Denn wie der Online-Handel verfügen die Anbieter solcher Produkte und Systeme über viele sensible Informationen oder können zumindest über sie verfügen. Ob sie gesammelt und wie sie verwendet werden, muss Regeln unterliegen, die auch eingehalten werden. Ansonsten wird sich das Vertrauen, das erforderlich ist, um das positive Potenzial dieser Möglichkeiten zu erschließen, nicht entwickeln.

1.3 Informationsbeschaffung im Netz

Die gleiche Problematik gilt auf dem Gebiet der Informationsgewinnung und -vermittlung. Auch diese hat sich in der digitalen Welt grundlegend verändert. Für denjenigen, der Zugang zum Netz hat, liegt die Herausforderung nicht mehr darin, Informationen im Kopf

4 Siehe die DIVSI U25-Studie (DIVSI 2014).

5 „Convenience" bedeutet „Annehmlichkeit", „Bequemlichkeit". Die englische Schreibweise wird oft genutzt, wenn es um diese beiden Begriffe im Kontext von Konsum geht.

zu haben – zu wissen –, sondern vornehmlich darin, sie zu finden und zu selektieren. Auch in diesem Zusammenhang entstehen Informations- und damit Machtkonzentrationen. Denn bei der Informationsbeschaffung im Netz bedient man sich technischer Systeme, deren Betreiber zu mächtigen Akteuren, *Gatekeepern*[6], werden, die es vorher in dieser Form nicht gegeben hat. Die Abhängigkeit von Suchmaschinen, sozialen Netzwerken oder *Microblogging*[7]-Diensten, über die wir unsere Informationen beziehen, empfinden viele mittlerweile als unheimlich, wie auch den Umstand, dass die Gatekeeper über unvorstellbar viele Informationen über Menschen und ihre Interaktionen verfügen.

Diese Umstände münden in eine zentrale Erkenntnis: Die Entstehung neuer Machtgefüge erfordert neue verbindliche Regeln, denn große Macht geht mit großer Verantwortung einher. Verantwortung wird durch Regeln zugeordnet, seien es Gesetze, Konzepte der Selbstregulierung oder soziale Normen. Wenn diese Regeln versagen, ineffizient werden oder nicht durchgesetzt werden können, entstehen gravierende Probleme.

1.4 Warum ein Digitaler Kodex?

Der Begriff des Digitalen Kodex ist zunächst ein stellvertretender Terminus für eine alternative Form der Regulierung von Verhalten im Internet. Die Notwendigkeit, einen Digitalen Kodex aufzustellen, entsteht, wenn unerwünschtes Verhalten um sich greift, das man mit herkömmlichen Regelungsprinzipien nicht in den Griff bekommt. Eine solche Situation erwächst zum einen durch Regulierungslücken und fehlende soziale Normen, zum anderen infolge von Durchsetzungsdefiziten bzw. einer nicht ausreichenden Verbindlichkeit von impliziten und expliziten Vereinbarungen. Regulierungslücken können beispielsweise dadurch entstehen, dass es keine verpflichtenden Regelungen, vor allem keine Gesetze, gibt. Hierin liegt im digitalen Handlungsraum angesichts der national und teilweise auch international hohen gesetzlichen Regelungsdichte eher nicht das Problem. Problematisch ist vielmehr, dass bestehende Regelungen häufig nicht eingehalten werden, zum Beispiel, weil die Adressaten sie nicht akzeptieren und/oder sie nicht durchsetzbar sind, weil Sanktionsmechanismen versagen – in diesem Fall gibt es also einen Regulierer, aber seine Regeln werden nicht befolgt. Es reicht nicht aus, Regeln aufzuschreiben, wenn sie keine Wirkmacht entfalten, weil ein breiter Konsens fehlt, soziale Kontrolle oder staatliche Repression nicht greifen. Die Einführung von Regeln und ihre Umsetzung bedingen einander – gute Regeln halten fest, was Konsens ist, also für alle Akteure in akzeptabler Form umgesetzt werden kann, und nur solche Regeln sind gut, deren Umsetzung bei der Formulierung mitgedacht wird.

Das beschriebene Defizit zeigt sich im Netz in vielfältiger Form. Es ist zwar keineswegs ein rechtsfreier Raum, fühlt sich aber häufig so an. Wenn Geheimdienste oder Konzerne in zum Teil illegaler Weise ungestraft Daten von Millionen Menschen erheben und auswerten können, haben geltende Gesetze oder deren Umsetzung offensichtlich versagt. Wenn Anbieter sozialer Netzwerke sich durch ihre AGB das Recht verschaffen können, Nutzerdaten und Fotos zu Werbezwecken an Unternehmen zu verkaufen, jeden Tag aber trotzdem Tausende neuer Nutzer gewinnen, die zum Beispiel aufgrund der Komplexität der AGB hiervon gar keine Kenntnis nehmen, reicht ein schlichtes Transparenzgebot eindeutig nicht aus. Wenn Cybermobbing oder Persönlichkeitsrechtsverletzungen außer Kontrolle geraten, fehlt es an geeigneten Umgangsformen und Mechanismen, die für Verbindlichkeit sorgen.

All diese Phänomene sind weithin bekannt, Lösungen zumeist aber nicht in Sicht. Könnte dem mit alternativen Regelungsansätzen, zum Beispiel in Form eines Digitalen Kodex, begegnet werden? Um dies beurteilen zu können, muss zunächst nach den Ursachen gefragt werden: Warum funktionieren Regeln, die sich über lange Zeit entwickelt und bewährt haben, im Netz häufig gar nicht oder weniger gut?

6 „Gatekeeper" (engl. für Pförtner, Türhüter) im Internet sind Akteure, die den Zugang zu Informationen oder Interaktionen kontrollieren.

7 „Microblogging" ist eine Kommunikationsform im Internet, bei der Nutzer sehr kurze, oftmals situationsbezogene Nachrichten über eine Plattform veröffentlichen.

1.5 Verhaltensregulierung unter veränderten Rahmenbedingungen

Um sich der Antwort hierauf zu nähern, ist es zunächst erforderlich herauszufinden, wie sich das Netz als Handlungsraum von anderen Regelungsumfeldern unterscheidet, ob und inwieweit sich die Akteure hier anders verhalten, und wenn, aus welchen Gründen.

Tatsächlich weist das Netz gegenüber gegenständlichen Handlungsräumen eine Vielzahl von Besonderheiten auf, die sich auf das Verhalten der Akteure, deren Rollen, die Verteilung und Übernahme von Verantwortung erheblich auswirken. Hier treten neue Akteure auf, die Machtverhältnisse und Einflusssphären sind häufig anders gelagert. All dies hat Einfluss auf die Frage, wie Verantwortung verteilt werden muss und wie Regeln entstehen, wie sie ein- und umgesetzt werden müssen, um unerwünschtes Verhalten effizient verhindern zu können. Die in diesem Kontext relevanten Besonderheiten des Netzes sind vor allem Anonymität, Unkörperlichkeit, Globalität, Ubiquität, Technizität, Dezentralität und Unvergänglichkeit. Außerdem ist das Internet ein öffentlicher Raum in privater Hand.

Anonymität und Unkörperlichkeit

Individuen sind im Internet per se anonym, wenn sie sich für Anonymität entscheiden. Dass sie (zum Beispiel 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."* Mehr noch: Bereits die *Entstehung* sozialer Normen wird durch den fehlenden physischen Kontakt zwischen den Individuen erschwert. Er ist ein wichtiger Faktor, der die Menschen in der gegenständlichen Welt zusammenschweißt, soziale Kontrolle ermöglicht und sie dazu bringt, gemeinsame Interessen zu verfolgen. Im Internet, so könnte man sagen, gibt es 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 Verhalten im Allgemeinen und das Verantwortungsbewusstsein im Besonderen 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 vor allem für die transnationale Verfolgung mittels Sanktionssystemen. Dieser Umstand stellt das Recht als Regelungsinstrument vor neue Herausforderungen. Denn Recht basiert herkömmlich zumeist auf dem Souveränitäts- und Territorialitätsprinzip, es endet in der Regel an der Staatsgrenze. Wenn sanktionsbasierte Regelungssysteme versagen, stellt sich die Frage, ob die Setzung positiver Anreize eher verspricht, regelkonformes Verhalten zu fördern. Solche können darin liegen, dass die Regelungsadressaten selbst in die Entwicklung, Ein- und Umsetzung der Regeln einbezogen werden. Ein Digitaler Kodex, der über Debatten zwischen den betroffenen Akteuren entsteht, könnte solches unter Umständen leisten.

Globalität erschwert zudem die Definition und Entstehung allgemeingültiger Wertvorstellungen und der damit korrespondierenden sozialen Normen oder Gesetze. 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 zum Beispiel die Haltung gegenüber Gewalt oder Nacktheit im Vergleich zwischen Europa und den USA. Dadurch kommt es zu einer themenbezogenen oder

regionalen Fragmentierung von sozialen Normen, die im globalen Netz zu großen Schwierigkeiten führt, da von den Betreibern der Plattformen auf Themen, die für einen Kulturraum spezifisch sind, nur in wenigen Fällen eingegangen wird – es sei denn, das Geschäftsmodell ist bedroht.

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, Werkzeuge 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. Aufgrund dessen haben die Architekten und Anbieter im Netz viel Macht über das Verhalten der Menschen. Sie tragen daher auch große Verantwortung, die in der gegenständlichen Welt allenfalls einem übernatürlichen Pendant zukommt.

Das Netz: Öffentlicher Raum in privater Hand

Das Netz ist ein öffentlicher Raum in privater Hand. Die Existenzgrundlage des Netzes – Technik – ist privates Eigentum. Dies beeinflusst das Machtgefüge im Handlungsraum Internet in erheblichem Maß.

Das Netz ist nicht monolithisch, sondern besteht aus der Gesamtheit der über die Welt gespannten und miteinander verbundenen Rechner-Netze sowie der darauf betriebenen Dienste. Es wird nicht nur hinsichtlich seiner physischen Ebene großenteils von privaten Akteuren betrieben. Auch auf allen weiteren Ebenen spielen Unternehmen als Gatekeeper eine zentrale Rolle, seien es Zugangsprovider, Suchmaschinenanbieter, Plattformbetreiber oder IT-Unternehmen. Damit ist das Netz ein vorwiegend privater und kein öffentlicher Raum, der sich deutlich und mit spürbaren Konsequenzen von der physischen Welt unterscheidet.

Dies hat zunächst eine rein faktische Implikation: Im öffentlichen Raum macht der Staat die Regeln, der demokratisch legitimiert ist und vielen Bindungen unterliegt, zum Beispiel der Verfassung. Im privaten Raum gibt der Eigentümer vor, wie man sich verhalten darf, was man tun kann und tun darf.

Dieser Umstand hat rechtliche Konsequenzen. Im klassischen öffentlichen Raum, beispielsweise dem Straßen- und Verkehrsraum, leitet sich alles letztlich von staatlicher Gewährung ab. Wenn niemand sonst mehr zuständig ist, gibt es im öffentlichen Raum der gegenständlichen Welt eine Auffangzuständigkeit der öffentlichen Hand. Außerhalb privater Grundstücke gilt öffentliches Recht und nicht Privatrecht. Dagegen ist etwa ein Kaufhaus zwar auch ein öffentlich zugänglicher Raum, aber ein durchweg privater, denn ab der Türschwelle gilt das Hausrecht. Das Hausrecht der Betreiber privatwirtschaftlich betriebener Räume hat nur lockere Verfassungsbindung. Im Netz erlaubt es daher viel tiefere Eingriffe in die Handlungsfreiheit der Menschen, als es sich dieselben Menschen im klassischen öffentlichen Raum gefallen lassen müssen.

Obwohl im Zusammenhang mit dem Netz immer wieder Verkehrsvokabeln (wie *Traffic*[8], Datenautobahn usw.) verwendet werden, bewegen sich die Menschen hier – bildlich gesprochen – also durchweg im Kaufhaus und nicht auf der Straße, ist in der digitalen Welt vom Bürgersteig über die Transportmittel bis zu den (Daten-)Wolken fast alles privatwirtschaftlich organisiert. Abstrakt ausgedrückt: Mit Ausnahme der universitären Netz-Infrastrukturen und einiger staatlich betriebener Datendienste und öffentlich-rechtlicher *Content*[9]-Plattformen gibt es im Internet so gut wie keinen im rechtlichen Sinne genuin öffentlichen Raum, insbesondere nicht hinsichtlich derjenigen alltäglichen Dienste, die immer weiter in das Leben der Menschen hineinreichen. Elektronische Kommunikation, *Cloud-Speicher*[10],

8 „Traffic" steht für Internet-Verkehr im technischen Sinn.

9 „Content" ist ein Sammelbegriff für Inhalte, die kontextbezogen in erster Linie über das Internet abrufbar sind.

10 Die „Cloud" ist eine Organisationsform der Bereitstellung von Rechner- und Speicherleistungen. Kennzeichnend sind Zentralisierung und eine hohe Flexibilität der Verfügbarkeit der technischen Ressourcen.

mobiles Internet, soziale Medien, Nachrichtenaggregation, *Location-based Services*[11], Web-Suche und vieles mehr gibt es fast ausschließlich aus der Hand privater Plattformbetreiber.

Dezentralität

Im Netz wird kopiert und weiterverteilt. 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 unter Umständen gemeinsam dafür verantwortlich.

Unvergänglichkeit

Handlungen im Netz werden gespeichert und dauerhaft festgehalten, meist dezentral auf mehreren Quellen. Während Aussagen im persönlichen Gespräch flüchtig sind, werden sie im Netz dauerhaft gespeichert. Das Netz kann zwar vergessen, Inhalte können verschwinden oder entfernt werden. Hierauf hat der individuelle Akteur aber oft nur sehr eingeschränkten Einfluss und kann daher nur begrenzt 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 Dienstanbietern zuschreiben sollte.

All diese – und im Zweifel weitere – Aspekte tragen dazu bei, dass gesetzliche Regulierung im Netz oft versagt, hoheitliche Regelungen nicht durchsetzbar sind und sich soziale Verhaltensstandards verändern, nicht mehr akzeptiert oder zumindest nicht befolgt werden. Man könnte sagen, dass das Netz einen neuen Gesellschaftsvertrag benötigt. Dieser könnte möglicherweise in Form eines Digitalen Kodex etabliert werden.

11 „Location-based Services" sind Internet-Dienste, die auf dem geografischen Standort des Nutzers beruhen.

INTERVIEW MIT DR. VERENA METZE-MANGOLD

Wir brauchen eine neue Öffentlichkeit

? Wie sehen Sie das Verhältnis von Öffentlichem und Privatem in der digitalen Sphäre?

Verena Metze-Mangold: Aus meiner persönlichen Sicht hat sich das Verhältnis verändert. Ich teile die Sicht des ehemaligen Bundespräsidenten Richard von Weizsäcker, der das 1998 wunderbar in Gräfin Dönhoffs Montagsgesprächen zusammengefasst hat. Er sagte sinngemäß, die Globalisierung – und wir können da die Globalisierung durch das Netz mitdenken – gefährde das Öffentliche und erlaube dem Privaten, maßgebliche Teile des Öffentlichen an sich zu reißen. Fundamentalismus und globaler Kapitalismus verstärkten ihren Einfluss. Der „Heilige Krieg" brauche Gläubige und „McWorld"-Konsumenten, beide benötigten keine Staatsbürger. Was am langsamsten vorankomme, so Weizsäcker in seiner klugen Analyse, sei die Ethik rund um den Globus.

Federico Mayor, spanischer Wissenschaftler und zu der Zeit Generaldirektor der UN-Kultur- und Wissenschaftsorganisation UNESCO, kam zu demselben Schluss. Wenn das Recht auf Kommunikation ernst gemeint sei, müsse es um eine neue „Balance zwischen dem Öffentlichen und dem Privaten" gehen, zwischen dem Kommerziellen und Nichtkommerziellen, dem Geist des Marktes und dem der Teilhabe. Und so wie die Sache stehe, sei es unerlässlich, jenen Teil der Cyberwelt zu stärken, der für die Menschen öffentlich und Dienst an der Allgemeinheit sei. Ich folge diesem Schluss. Aber allgemein galt damals eher das Gegenteil.

Dr. Verena Metze-Mangold

ist Sozialwissenschaftlerin und Vizepräsidentin der Deutschen UNESCO-Kommission. Nach ihrem Studium der Politikwissenschaften, Soziologie und Geschichte leitete sie von 1976 bis 1987 die Evangelische Medienakademie (cpa) im Gemeinschaftswerk der Evangelischen Publizistik in Frankfurt. Sie wechselte als Kommunikationschefin zum Hessischen Rundfunk und baute dort die Medienforschung auf, die Abteilung für Neue Medien und das Marketing. Von 1987 bis 2011 arbeitete sie in der Intendanz des Hessischen Rundfunks in verschiedenen Funktionen, zuletzt als Geschäftsführerin der Filmförderung. Seit 1982 ist Verena Metze-Mangold Mitglied der

Foto: DUK

? Was ist denn die verbreitete Denkweise in Bezug auf die digitalen Technologien?

VMM: Vorherrschend war in den letzten zwei Jahrzehnten die Ideologie, dass der Staat sich heraushalten soll, damit der Markt und die neuen Technologien sich im globalen Maßstab entfalten können. Das Credo von Liberalisierung und Deregulierung kam vor allem aus den USA und verband sich mit amerikanischen Freiheitsmythen, half aber in Wahrheit wohl eher jenen, die Kapitalmacht und damit Regelungsmacht besaßen.

Wir entdecken hier in Europa in den letzten Jahren gerade wieder, dass der öffentliche Raum kostbar ist und neu verteidigt werden muss. Das ist etwas typisch Europäisches. Das amerikanische Gesellschaftsmodell teilt die gesellschaftliche Sphäre in einen möglichst großen Markt und einen möglichst kleinen Staat. In Europa gibt es traditionell ein Drittes, und das ist der öffentliche Raum.

Ein einfaches Beispiel dafür ist die gesellschaftliche Übereinkunft, dass Schulen grundsätzlich in die öffentliche Hand gehören. Es gibt zwar Privatschulen, aber das ist nicht die Regel. Dadurch sollen alle Zugang zu Bildung haben – und nicht nur jene, die es bezahlen können. Intelligenz ist zum Glück nicht an Schichten gebunden. Die Gesellschaft insgesamt profitiert davon, wenn alle eine gute Bildung haben – daran zweifelt hier niemand.

? In welche Richtung entwickelt sich das Internet gegenwärtig Ihrer Meinung nach?

VMM: Das Internet ist das vermutlich bedeutsamste Artefakt der Menschheit. Von Haus aus ist die technische und gesellschaftliche Struktur des Netzes so angelegt, dass sie frei ist – das heißt, dass die Informationen frei fließen können, unabhängig davon, wer sie sendet. Das hat sich aber in den letzten Jahren geändert. Wann sie umgebaut worden ist, von wem und nach welchen Regeln, müssen wir genauer untersuchen.

Das Internet ist eine Kommunikationsstruktur, die den Alltag sehr vieler Menschen, Organisationen und Firmen durch die Digitalisierung aller Lebensbereiche erfasst. Jede technische Neuerung

Deutschen UNESCO-Kommission (DUK), seit 1996 Vorstandsmitglied, seit 1997 Vizepräsidentin der DUK. 1996 bis 1998 war sie Vorsitzende des Fachausschusses Kommunikation, Information und Informatik. 2001 bis 2009 vertrat sie Deutschland im Zwischenstaatlichen Rat „Information for All Programme“ (IFAP).

Dr. Metze-Mangold lehrte unter anderem an den Universitäten von Frankfurt a. M., Marburg, Hannover, Leipzig, Berlin (FU), Potsdam, Utrecht und Maastricht. Schwerpunkt ihrer Veröffentlichungen sind Themen der Presse- und Informationsfreiheit, des Medienmarkts und der Medienentwicklung, der internationalen Regulierung, des Völkerrechts und der interkulturellen Kommunikation.

WIR BRAUCHEN EINE NEUE ÖFFENTLICHKEIT

ist auch Teil einer sozialen Organisation, mitunter sprengt sie auch die bisherigen Normen. Das ist beim Netz nicht anders. Ursprünglich hat sich das World Wide Web durch Normen entwickelt, die von Wissenschaft und Unternehmen geteilt, offengelegt und beherzigt wurden. Die Gremien, die heute bestimmen, wie die Internet-Protokolle definiert sind, auf denen der ganze Netz-Traffic beruht, bewegen sich außerhalb der normalen sozialen und politischen Entscheidungsprozesse. Die technische Expertise und die politische Expertise sind entkoppelt.

? Infrastruktur ist in vielerlei Hinsicht zentral, denn sie bestimmt, was Nutzer überhaupt machen dürfen. Brauchen wir dafür neue Regeln? Nehmen wir Facebook als Beispiel: Was müsste Facebook offenlegen, da es diese wichtige Rolle im Leben seiner Nutzer spielt?

VMM: Bevor ich antworte, muss ich einschränkend sagen, dass ich soziale Netzwerke selbst nicht nutze. Ich beschäftige mich theoretisch damit. Ich kann deshalb nicht aus eigener Erfahrung sprechen, sondern nur aus der Literatur und aus den Analysen. Ich kann mir vorstellen, dass es viele jüngere Menschen gibt, die mit dem Netz aufgewachsen sind, die sagen, mir fehlt nichts, ich kommuniziere mit der ganzen Welt und bin zufrieden und glücklich. Sie kennen es gar nicht anders. Ich persönlich aber glaube, dass wir bislang im Internet keinen öffentlichen Raum in dem gewohnten Sinne finden, sondern eine zerstreute Öffentlichkeit.

Ich vergleiche das gerne mit den verstreuten bäuerlichen Ansiedlungen in Irland. Da musste man lange laufen, bis man beim nächsten Hof war. Es gab keine Dörfer, in denen Leute aller Schichten zusammenkamen, sondern man erzählte sich am Kamin der Nachbarn Geschichten. Das war der Austausch. So was Ähnliches findet im Netz unentwegt statt. Theoretisch gibt es enorme Informationsvielfalt, es gibt ja alles, aber in der Praxis kennt man nur die Informationen seiner Nachbarn und Freunde.

Das ist aus meiner Sicht ein Schritt zurück in der Geschichte der bürgerlichen Öffentlichkeit. Diese Art von Öffentlichkeit ist vielleicht eine idealisierte Vorstellung, hat aber sehr dazu beigetragen, dass der Mensch sich emanzipieren kann. Ich weiß nicht, wie es sein wird, wenn wir eine solche Öffentlichkeit vielleicht nicht mehr haben. Tim Berners-Lee, der Erfinder des World Wide Web, hat das auf den Begriff gebracht: Nicht die Revolution frisst ihre Kinder – die erfolgreichsten Kinder fressen die Revolution.

? In welche Richtung soll die Entwicklung des Netzes denn gehen? Was wünschen Sie sich?

VMM: Für viele Leute ist das Netz eine Infrastruktur. Eine Infrastruktur folgt normalerweise den Regeln der Gesellschaft. Und da wir in einer kapitalistischen Gesellschaft leben, finden viele Menschen es völlig in Ordnung, dass die großen Unternehmen die Entscheidungen treffen. Ich persönlich würde das infrage stellen. Es ist das erste Mal in der Menschheitsgeschichte, dass gesellschaftliche Fragen von privater Seite entschieden werden. Der Einfluss digitaler Großmächte auf das Alltagsleben und politische Entscheidungen wächst exponentiell.

Wir haben politisch leider keine Instanz, mit der wir global agierende Unternehmen in irgendeiner

> **Der Einfluss digitaler Großmächte auf das Alltagsleben und politische Entscheidungen wächst exponentiell.** Dr. Verena Metze-Mangold

Weise beeindrucken können. Wir können ihnen nur bedingt Schranken setzen oder sie sanktionieren, wenn etwas gegen das gesellschaftliche Interesse geht. Herausforderungen muss man mit neuen Institutionen – also internationalem Recht – oder neuen Verfahren begegnen, sagte Niklas Luhmann. Wir haben die Konvention für kulturelle Vielfalt, die einschlägige Normen bis hin zur Netzneutralität und Public Domain setzt, und Verfahren der Selbstregulierung in Stakeholder-Prozessen, die noch in den Anfängen steckt. Es wäre aber wichtig, auch den Netz-Bereich demokratisch zu regeln und diese Regeln mindestens regional, also etwa in Europa, und daneben interregional im Sinne einer Clustertheorie zu entwickeln.

Zum Zweiten müssen wir uns über die Grundlagen einigen, zum Beispiel, indem wir noch mal überlegen, was genau beim Netz anders ist als bei bisherigen Infrastrukturen. Das muss man erst mal sehr genau erfassen, damit man überhaupt eine gemeinsame Basis hat. Wir leben in Zeiten des Umbruchs und müssen überlegen, was wir unbedingt aus der alten Welt in die neue mitnehmen möchten. Welche Normen sollen bleiben, welche Grundprinzipien sind uns wichtig? Am Punkt des Umbruchs also nicht besinnungslos nach vorne stürmen, vielmehr zurückschwingen und uns verständigen. Auch darüber, mit welchen Begriffen wir arbeiten und wie diese Begriffe belegt sind. Haben wir dasselbe Verständnis? Sonst redet man notorisch aneinander vorbei.

? Gibt es denn international ein bestehendes Gremium, das diese Aufgabe und diese Verantwortung übernehmen könnte? Oder müssten wir etwas ganz Neues aufbauen?

VMM: Ich könnte mir vorstellen, dass man das nicht von oben aufsetzen kann – das würde niemand akzeptieren. Zum gesellschaftlichen Konsens heute gehört, dass wir uns darüber auseinandersetzen müssen, wie Entscheidungen zustande kommen. Es gibt inzwischen neben dem Regime des Welthandels auch das des neuen internationalen Kulturrechts. Es erlaubt Staaten, politische Entscheidungen zugunsten des öffentlichen Raumes zu fällen, ohne von der WTO deshalb verklagt zu werden. Europäische und internationale Gerichtshöfe bilden neue Rechtsstrukturen aus. Es gibt Entwürfe, die uns die Selbstverständigung in der internationalen Zivilgesellschaft erlauben – zum Beispiel Konzepte einer humanen Wissensgesellschaft (beispielsweise von Robin Mansell, Professorin an der London School of Economics[12]), einer digitalen Ökologie[13] oder das Konzept der „Internet Universality" der UNESCO[14]. Daneben gibt es Deklarationen – sogenanntes *Soft Law* – zu den Prinzipien der Informationsethik.

12 Siehe dazu die Homepage von Robin Mansell an der London School of Economics (www.lse.ac.uk/researchAndExpertise/Experts/profile.aspx?KeyValue=r.e.mansell%40lse.ac.uk).

13 William H. Dutton, Anna Dopatka, Michael Hills, Ginette Law, and Victoria Nash: „Freedom of Connection/Freedom of Expression: The changing legal and regulatory ecology shaping the internet", Oxford Internet Institute, University of Oxford: www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/full-list/freedom-of-connection-freedom-of-expression-the-changing-legal-and-regulatory-ecology-shaping-the-internet/

14 „Auf welchen Normen basiert das Internet? Offene Konsultationen zum neuen UNESCO-Konzept der ‚Internet-Universalität'", September 2013, www.unesco.de/8159.html

WIR BRAUCHEN EINE NEUE ÖFFENTLICHKEIT

> **Es gibt immer mehr den Willen, einen neuen öffentlichen Raum zu schaffen oder den alten zu bewahren.** Dr. Verena Metze-Mangold

Wir haben zwischenstaatliche Strukturen, die auch funktionieren – siehe den Vorstoß von Brasilien und Deutschland nach der NSA-Affäre bei den Vereinten Nationen. Ob sie aber reichen? Da habe ich Zweifel. Angesichts der Beschleunigung und der Auswüchse der Prozesse scheint es eher einen Rückfall in nationalstaatliche Kontrollfantasien zu geben – ein klares Zeichen, dass die Auswüchse ihr Gegenteil induzieren.

Gleichzeitig gibt es aber in den letzten fünfzehn Jahren immer wieder Signale einer Verständigung, wie zum Beispiel bei der *Millennium Declaration*[15], der immerhin 190 Staats- und Regierungschefs zugestimmt haben. Sie wurde von den Vereinten Nationen im Herbst 2000 verabschiedet. Dort gibt es ein ganz wunderbares Zitat gleich im ersten Absatz, das sinngemäß sagt, die zusammengerückte Welt des 21. Jahrhundert nötigt uns ab, uns nicht nur um unsere eigene Nation, unseren eigenen Staat und unsere eigene Gesellschaft zu kümmern, sondern miteinander zu kooperieren, also Verantwortung für eine Weltgemeinschaft zu übernehmen. Die Staaten allein werden das nicht schaffen, es muss das Einverständnis der Menschen finden. Das bedeutet, Wirtschaft und Zivilgesellschaft müssen einbezogen werden.

? Wer sind in Deutschland die wesentlichen Akteure? Wenn wir ein Regulierungsgremium besetzen würden, wer müsste teilnehmen?

VMM: Es gibt da viele, und ich habe den Eindruck, dass gerade ein neues Selbstbewusstsein entsteht. Es gibt immer mehr den Willen, einen neuen öffentlichen Raum zu schaffen oder den alten zu bewahren. Beispiele sind Legion – von Stiftungen über die Landesmedienanstalten, die ihre Rolle ändern und gesellschaftspolitische Angebote machen, bis zu neuen Kooperationen zwischen Staat, Civil Society und Wirtschaft etwa bei der Konferenz *EuroDig*, die 2014 in Berlin unter dem gemeinsam erarbeiteten Titel „Digital Society@stake" stattfindet. Es geht um Gesellschaftspolitik in der digitalen Ära.

Ich könnte mir vorstellen, dass man einen Staatssekretär im Bundeskanzleramt sitzen hat, der auf der einen Seite solche Prozesse interdisziplinär verbindet, aber auf der anderen Seite auch neue Prozesse entwickelt. Ein anderes Werkzeug könnte die Wiederaufnahme des Medienberichts der Bundesregierung sein, den es früher alle drei Jahre gab. Ich glaube, der letzte wurde 2008 veröffentlicht. Das wäre zum Beispiel ein guter Reflexionsrahmen, um uns klarzuwerden: Wo stehen wir eigentlich? Wo infiltriert diese Infrastruktur auf neue Weise unsere Gesellschaft?

15 www.un.org/millennium/declaration/ares552e.htm

1.6 Das Projekt „Braucht Deutschland einen Digitalen Kodex?“

Das Deutsche Institut für Vertrauen und Sicherheit im Internet (DIVSI) hat das iRights.Lab, einen Berliner Think Tank zu Strategien in der digitalen Welt, mit dem Projekt „Braucht Deutschland einen Digitalen Kodex?“ beauftragt. Das Projekt erstreckte sich von April 2013 bis Mai 2014. Es hat ausgelotet, ob ein Digitaler Kodex die Lücke zwischen den etablierten Regeln der analogen Welt und den noch unklaren Verantwortlichkeiten im Internet schließen kann. Neben einer inhaltlichen Klärung der Fragestellung, für die eine Reihe von namhaften Experten einbezogen worden ist und deren Ergebnisse in Themenpapieren vorliegen, wurde die interessierte Öffentlichkeit in Form von Diskussionsveranstaltungen beteiligt.

DAS PROJEKT IM ZEITLICHEN ÜBERBLICK

April 2013

Projektbeginn

Juni 2013

Auftaktworkshop der Expertengruppe in Hamburg

Veröffentlichung der Themenpapiere „Verantwortung im Internet“ und „Plattformen und die Rolle ihrer Betreiber in Bezug auf Verantwortung im Internet“

Juli 2013

Öffentliche Diskussionsveranstaltung in München:
„Jeder macht im Netz, was er will – Verantwortung in der digitalen Welt“

September 2013

2. Expertenworkshop in Berlin

Veröffentlichung des Themenpapiers
„Was ist ein Digitaler Kodex?“

November 2013

Öffentliche Diskussionsveranstaltung in Hamburg:
„Facebook, WhatsApp, Google+:
Wer macht die Regeln?“

Januar 2014

3. Expertenworkshop in Berlin

Februar 2014

Veröffentlichung des Themenpapiers
„Konzept für die Entstehung, Struktur und Umsetzung/Durchsetzung eines Digitalen Kodex“

Mai 2014

Veröffentlichung des Projektberichts

Öffentliche Diskussionsveranstaltung in Berlin:
„Digitaler Straßenkampf oder Selbstverpflichtung – Wie entstehen Regeln im Netz?“

DIE EXPERTENGRUPPE

Das Projekt hat wesentliche Anregungen von einer hochrangigen, interdisziplinär besetzten Expertengruppe erhalten, die das Projektteam als Impulsgeber und Sounding Board begleitet hat. Neben dieser Gruppe, die in mehreren Workshops den Diskussionsprozess vorangetrieben hat, wurden weitere Experten aus Politik, Wirtschaft, Interessenverbänden und Initiativen in Form von Interviews und Konsultationen beteiligt, um spezifische Aspekte des komplexen Themas zu erschließen. Die Stimmen der Experten haben über die eingefügten Interviews und Zitate Einzug in diesen Bericht gehalten.

Foto: privat

Dr. Eva Flecken

Stabsstelle Digitale Projekte, Netz- und Medienpolitik, Medienanstalt Berlin-Brandenburg (mabb)

„Die Unterscheidung ‚online oder offline' ist für viele Menschen heute schon nicht mehr wirklich sinnvoll, schließlich sind wir dank der smarten Alleskönner immer und überall online. Doch dürfen wir nicht vergessen, dass die digitale Vernetzung viele Menschen vor Herausforderungen stellt, manche sogar abhängt. Umso dringlicher müssen wir eine gesellschaftliche Vorstellung davon entwickeln, wer im digitalen Weltgeschehen wofür Verantwortung übernimmt. Wie kann ein Digitaler Kodex ausgestaltet sein, der uns als Navigator im Internet berät und auch mal in die Schranken weist? Diese Frage geht uns alle an, da sich unsere individuelle Lebenswirklichkeit fortwährend digitalisiert – ob wir wollen oder nicht, es geschieht."

Foto: privat

Prof. Dr. Rüdiger Grimm

Professor für IT-Riskmanagement im Fachbereich Informatik an der Universität in Koblenz

„Eigentlich sind Datenschutz und Urheberrecht klar geregelt, für das Internet sind sogar aktuelle Novellierungen in Kraft getreten. De facto aber werden beide Rechte im Internet notorisch ignoriert, oder jedenfalls anders behandelt, als vom Recht vorgesehen. Es ist die Frage, ob die traditionelle Form der Rechtsetzung für die modernen Kommunikationsformen im Internet und mit mobilen Anwendungen noch ausreichend oder überhaupt angemessen ist. Welche anderen Formen verbindlicher Festlegung von Verhalten sind dann aber denkbar? Hier betreten wir Neuland. Das Zusammenspiel von ethischen Normen, guten Sitten, klaren Rechtsansprüchen und innovativen Grenzüberschreitungen ist eine der spannendsten Herausforderungen der modernen Gesellschaft. Hierzu ist interdisziplinäre Zusammenarbeit in der Kommunikation zwischen Praktikern und Theoretikern der Medien, Politik, Wirtschaft und Forschung erforderlich."

Dr. Hans Hege

Direktor der Medienanstalt Berlin-Brandenburg (mabb)

„Wir brauchen eine breite und fundierte Diskussion zu der Frage, wer im Netz welche Verantwortung wofür trägt. Die digitale Lebenswirklichkeit ist überaus chancenreich, sie fordert uns aber auch einiges ab. Politik und Gesellschaft müssen gemeinsam einen Rahmen für zeitgemäße Zuständigkeiten, moderne Sicherheitsstrukturen sowie innovative Förderung im Netz erarbeiten. Auch die Medienregulierung muss sich dahingehend neu entwerfen. Als Regulierer liegt mir besonders daran, dass der Zugang zu Infrastrukturen und Inhalten allen gleichermaßen offensteht."

Foto: mabb, Nikolaus Brade

Dr. Michael Littger

Geschäftsführer von Deutschland sicher im Netz (DsiN e.V.)

„Der Umgang mit digitalen Veränderungen gehört zu den zentralen Herausforderungen unserer Zeit. Er erfordert eine Debatte über kluge Regulierungsstrategien – und damit auch über die geeigneten Regelungsinstrumente. Ein Kodex hat das Potenzial, relevante Fragen der Digitalisierung rasch aufzugreifen und daraus intelligente Lösungen zu entwickeln. Zudem können sich eine hohe Dynamik bei der Regelfindung sowie eine stärkere Akzeptanz bei den Adressaten ergeben. Die Anforderungen an die Kodex-Architektur und ihre Umsetzung müssen dafür jedoch genau geprüft werden. Das Projekt von DIVSI und iRights.Lab schafft sehr gute Voraussetzungen, diese Zukunftsdebatte – aus unterschiedlichen Blickwinkeln – konstruktiv zu bestreiten."

Foto: privat

Nico Lumma

Freier Autor und Berater

„Die Digitalisierung der Gesellschaft sorgt für eine Neubestimmung unserer Positionen und unserer Werte als westliche Gesellschaft. Daher ist die Diskussion um einen Digitalen Kodex längst überfällig."

Foto: privat

DIE EXPERTENGRUPPE

Foto: privat

Dr. Alexandra Manske

Freiberufliche Soziologin in Berlin, ehemals Humboldt-Universität zu Berlin

„Als Mitglied der Experten-Kommission ‚Digitaler Kodex' treiben mich aus soziologischer Perspektive folgende Fragen um: Wer hat welche Interessen im Netz? Wie könnten soziale Verkehrsregeln im digitalen Leben aussehen? Wie vermitteln sich Interessen mit Verantwortung, und was heißt das: Verantwortung übernehmen im digitalen, sozialen Regelgeflecht?"

Foto: privat

Peter Schaar

Vorstand der Europäischen Akademie für Informationsfreiheit und Datenschutz

„Gesellschaftliche Wertvorstellungen brauchen Zeit, um sich herauszubilden. Die rasante technologische Entwicklung stellt Entscheider und Betroffene ständig vor neue Fragen, die sich vielfach nicht innerhalb eines gewachsenen Normensystems beantworten lassen. Der insbesondere in Deutschland unternommene Versuch, alle Eventualitäten im Detail zu regeln, ist zum Scheitern verurteilt. Deshalb brauchen wir einen Top-down-Ansatz, der ausgehend von grundlegenden Wertentscheidungen rechtliche Vorgaben und Ziele definiert, die unter Mitwirkung aller Betroffenen konkretisiert werden. Die dabei entwickelten Vorgaben sollten für alle Beteiligten verbindlich sein. Voraussetzung dafür ist ein stabiler gesetzlicher Rahmen, der auch Verfahrensregelungen und Durchsetzungsmechanismen festlegt. Ein ‚Digitaler Kodex', der entwicklungsoffen den jeweiligen Stand beschreibt und Verhaltensrichtlinien gibt, kann hierfür hilfreich sein."

Foto: privat

Thorsten Schilling

Leiter des Fachbereichs Multimedia der Bundeszentrale für politische Bildung in Bonn und Berlin (bpb)

„Ich finde die Themen, die bei der Diskussion um einen möglichen Digitalen Kodex diskutiert werden, wichtig und wert, sie in den verschiedensten Bereichen und Perspektiven zu betrachten. Spannend finde ich auch, ob meine doch ausgeprägte Skepsis, was die Möglichkeit der Erstellung eines solchen Kodex in den eher idyllischen Rahmenbedingungen einer Expertenrunde angeht, im Laufe der Diskussion widerlegt werden kann. Wirksame Kodizes entstehen doch eher im Zuge von Streit, glaube ich."

Dr. Sönke E. Schulz

Wissenschaftlicher Assistent und Geschäftsführer des Lorenz-von-Stein-Instituts für Verwaltungswissenschaften

„Angesichts der oft fehlenden Steuerungswirkungen des Rechts in der digitalen Welt – die einem als Juristen durch neueste Entwicklungen beständig vor Augen geführt werden – erscheint eine intensivere Befassung mit außerrechtlichen Wirkungsmechanismen aus interdisziplinärer Perspektive zielführend. Damit setzt das Projekt Digitaler Kodex zur richtigen Zeit an der richtigen Stelle an – und kann auch für Rechtspolitik, Rechtswissenschaft und Rechtspraxis wertvolle Hinweise liefern."

Foto: privat

Prof. Dr. Wolfgang Schulz

Direktor des Hans-Bredow-Instituts für Medienforschung und des Alexander von Humboldt Instituts für Internet und Gesellschaft

„Gerade im Netz strukturiert nicht allein formales Recht das Verhalten, auch soziale Normen und der ‚Code', die Softwarearchitektur, sind bedeutsam. Wenn wir uns fragen, wie eine angemessene Regelungsstruktur für die digitale Gesellschaft aussieht, müssen wir das Zusammenspiel dieser Faktoren verstehen. Ausgangspunkt sollte dabei immer ein konkretes Problem sein, Regulierung ist kein Selbstzweck. Die Reaktion auf ein solches Problem kann möglicherweise eine neue Kodifizierung – ein ‚Digitaler Kodex' – sein, vielleicht muss die Regelungsstruktur aber auch auf andere Weise optimiert werden."

Foto: Hans-Bredow-Institut

Patrick von Braunmühl

Geschäftsführer des Vereins Selbstregulierung Informationswirtschaft (SRIW)

„Was die digitale Revolution für unseren Gesellschaftsvertrag bedeutet und ob soziale Normen teilweise neu definiert werden müssen, ist eine der spannendsten Fragen unserer Zeit. Ich bin gespannt, welche Antworten das Projekt Digitaler Kodex auf diese Fragen findet."

Foto: privat

1.7 Konkretisierung eines Bezugspunktes für einen Digitalen Kodex

Worauf könnte sich ein Digitaler Kodex beziehen? Schon am Anfang des Projekts stand die Erkenntnis, dass die generelle Frage „Braucht Deutschland einen Digitalen Kodex?" zu abstrakt ist, um in voller Allgemeinheit beantwortet werden zu können. Sie bedurfte weiterer Präzisierung und Vorarbeiten, um sinnvoll bearbeitet werden zu können. Wesentlich war zunächst, sich über die grundsätzlichen Rahmenbedingungen Klarheit zu verschaffen, auf denen die Entstehung, Einsetzung und Umsetzung von Regeln im Netz basiert. Wie bereits deutlich gemacht wurde, ist dabei der Aspekt der Verantwortung zentral. Zu wissen, wie Verantwortung entsteht, wie sie in verschiedenen Handlungsräumen bestimmten Akteuren zugeschrieben wird und welche Akteure speziell im Internet Verantwortung tragen, ist erforderlich, um zu verstehen, welches Ziel mit einem Digitalen Kodex zu verfolgen wäre. Um diese Aspekte wiederum beurteilen zu können, ist es notwendig zu analysieren, wie das Machtgefüge im Netz beschaffen ist, da die Zuweisung von Verantwortung hierauf basiert. Wer viel Gestaltungs- und Handlungsmacht hat, hat viel Einfluss auf das Verhalten Dritter und trägt damit viel Verantwortung bzw. sollte viel Verantwortung tragen. Daher wurde zunächst der Aspekt der Verantwortung eingehend untersucht. Die Ergebnisse finden sich im Themenpapier „Verantwortung in Internet", das sich im Volltext im Annex findet.

Weiterhin im Vordergrund stand von vornherein die Aufgabe, die abstrakte Frage, ob Deutschland einen Digitalen Kodex braucht, weiter zu konkretisieren. Es ist evident, dass sie nicht beantwortet werden kann, wenn sie sich allgemein auf jegliches Verhalten aller Akteure im Netz bezieht. Daher wurde schon früh im Projektverlauf eine Fokussierung auf Verhaltensregeln für Online-Plattformen vorgenommen. Angesichts der Erkenntnis, dass auch die Frage, ob Deutschland einen Digitalen Kodex für Online-Plattformen braucht, noch zu allgemein ist, wurden im Laufe des Projekts weitere Präzisierungen des Untersuchungsthemas vorgenommen.

Dieser notwendige Zwischenschritt wurde durch ein Themenpapier „Was ist ein Digitaler Kodex?" vorbereitet, das sich ebenfalls im Volltext im Annex findet. Es geht zunächst der Frage nach, auf welche Bereiche des Netzes bzw. welche Arten von Plattformen sich ein Digitaler Kodex beziehen könnte. Im Vordergrund stand hierbei die Erkenntnis, dass es „das Netz" ebenso wenig gibt wie „die Online-Plattform". Vielmehr gibt es eine Vielzahl unterschiedlicher Formen von Online-Diensten, die diesem Begriff entsprechen würden. Dieser Umstand wurde durch eine eingehende Untersuchung mit dem Titel „Plattformen und die Rolle ihrer Betreiber in Bezug auf Verantwortung im Internet" deutlich. Auch diese Untersuchung ist in den Annex aufgenommen.

Angesichts des Umstands, dass sich das Machtgefüge, die Akteursstruktur und die Verhaltensweisen bei einem Vergleich von beispielsweise sozialen Netzwerken und Videoplattformen als erheblich unterschiedlich erweisen, ist es kaum möglich zu beurteilen, ob sich ein Digitaler Kodex allgemein als Instrument zur Regelsetzung *auf Plattformen* eignet und wie ein solcher Kodex aussehen müsste. Es bedarf also auch diesbezüglich einer weiteren Konkretisierung der Ausgangsfrage.

Hinzu kommt, dass die Frage nach den im Projekt gewonnenen Erkenntnissen themenspezifisch gestellt werden muss. Die Grundfaktoren eines Kodex variieren erheblich, je nachdem, ob sich der Kodex an Anbieter, Nutzer oder gar den Staat richten und ob er den Umgang mit personenbezogenen Informationen durch Anbieter sozialer Netzwerke, Regeln gegen Cybermobbing oder weiter gehende Transparenzgebote betreffen soll. Kurzum: Die Frage, ob Deutschland einen Digitalen Kodex braucht, wie ein solcher entstehen, ein- und umgesetzt werden könnte, hängt davon ab, worauf er sich beziehen soll. Die Themenwahl ist in einem Projekt, das mit einer sehr allgemeinen Frage gestartet ist, eine Gratwanderung. Je konkreter die diesbezügliche Themenstellung formuliert ist, desto erkenntnisreicher wird die Antwort für das jeweilige Thema ausfallen. Je enger jedoch der Betrachtungsgegenstand, desto geringer der Erkenntnisgewinn für die allgemeine Frage, ob sich das Konzept Digitaler Kodex an sich für eine alternative Form der Regelsetzung im Netz eignet.

Gemeinsam mit der Expertengruppe hat das Projektteam eine Reihe möglicher Anwendungsfelder für einen Digitalen Kodex identifiziert. Die Bandbreite der

Themen ist groß. Sie zeigt einerseits, wie viele prekäre Regelungsfelder sich noch immer im Netz finden, und andererseits, wie unterschiedlich und vielfältig die Themen sind, die durch einen Digitalen Kodex oder eine Vielzahl von Kodizes adressiert werden könnten. Sie reichen vom Umgang mit personenbezogenen Informationen in sozialen Netzwerken (durch Nutzer und/oder Anbieter) über Cybermobbing, Urheberrechtsverletzungen, Anonymität im Netz, Transparenz, Daten als Währung, *Privacy-by-design*[16], Sicherheit, Zensur durch Hausrecht bis zum Umgang der Nutzer miteinander.

Ebenso wichtig, wie einen möglichen Anwendungsbereich für einen Digitalen Kodex zu identifizieren, ist naturgemäß die Frage, was einen solchen ausmacht, was ein Kodex in diesem Sinne ist oder sein könnte. Ohne eine Antwort auf diese Frage kann man weder die Ausgangsfrage, ob man einen Digitalen Kodex braucht, beantworten, noch diese Option in einem Modellversuch praktisch oder theoretisch durchspielen.

Zu diesem Zweck wurde zunächst eine abstrakte Begriffsbestimmung des Terminus Kodex vorgenommen.

Auf der Basis der Begriffsbestimmung wurde im Projekt die Frage debattiert, wie, von wem und mit welchen Mitteln ein Digitaler Kodex – also ein Kodex zur Regelung bestimmter Verhaltensweisen und Sachverhalte im Netz – entstehen sowie ein- und umgesetzt werden müsste, um Wirkmacht zu entfalten und

WAS IST EIN DIGITALER KODEX?

Alltagssprachlich verstehen wir unter einem Kodex eine Sammlung von Verhaltensregeln, die für eine gesellschaftliche Gruppe oder die ganze Gesellschaft Geltung besitzt. Allerdings ist ein solcher Begriff recht unscharf, sodass sämtliche geschriebenen oder ungeschriebenen Verhaltenskataloge Kodizes genannt werden könnten. Wenn man sich jedoch Kodizes ansieht, die heutzutage unter diesem Namen in Kraft sind, dann fällt auf, dass sie sich fast immer auf eine Berufsgruppe beziehen. Als Beispiele können hier der Pressekodex, der für Ärzte bedeutende Eid des Hippokrates und der Kodex zur „Sicherung guter wissenschaftlicher Praxis“ der Deutschen Forschungsgemeinschaft genannt werden.[17]

Kodizes sind demnach Verhaltenskataloge der besonderen Art. Sie spitzen zentrale moralische Prinzipien und soziale Normen mithilfe von Praxisregeln auf ein Berufsfeld zu, sie formulieren Grundsätze des handwerklichen Könnens, und sie geben in der Regel auch an, warum diese Verhaltensregeln für diese Gruppe überhaupt aufgestellt werden: wegen der gesellschaftlich bedeutsamen Funktion eines Berufsstandes. Hinzu kommen drei Besonderheiten: (a) Kodizes bringen in der Regel eine „externe“ Beobachtungsinstanz mit, die eine Kontrollfunktion übernimmt, beim Pressekodex zum Beispiel den Presserat. Dies dürfte auch daran liegen, dass (b) Kodizes nicht selten von Repräsentanten des jeweiligen Berufsstandes selbst ins Leben gerufen werden, die die Umsetzung ihres eigenen Kodex im Zweifel weniger streng kontrollieren als ein Gremium, dessen Mitglieder dem Berufsstand nicht angehören. (c) Kodizes haben mehrere Funktionen: Sie sollen eine weiter gehende Professionalisierung vorantreiben, Orientierung ermöglichen, Reflexion anstoßen, öffentlich wahrnehmbare Korrekturen anmahnen und ein Selbstbild der Profession etablieren.

16 „Privacy by design“ steht für einen Ansatz, bei dem Privatheit auf allen Ebenen, von der Technik bis zu den Prozessen, in den Designprozess eines Systems einbezogen worden ist.

17 Ausnahmen bilden Kodizes für spezielle kulturelle Gruppen. Solche Verhaltenskataloge (etwa ein Samurai-Kodex) richten bzw. richteten sich allerdings an Mitglieder einer Gruppe, die ihnen eine Primäridentität verleiht, an die sich ein Lebensstil knüpft. Weil sich Identitäten in modernen Gesellschaften kaum noch in dieser Weise ausbilden, sind sie im Rahmen dieser Überlegungen wenig relevant.

Regelungsdefizite zu beheben. Vorläufiges Ergebnis dieser Überlegungen war, dass ein solcher Kodex auf alternativen Regelungskonzepten basieren muss, die sich von herkömmlichen staatlichen und Selbstregulierungsformen unterscheiden. Die Historie zeigt, dass auf Aushandlungsprozessen basierende Kodizes mitunter große Wirkmacht entfaltet haben, zum Teil auch für lange Zeit. Als Beispiele könnte man die Magna Carta Libertatum, den Codex Hammurabi, den Dekalog und die Haager Landkriegsordnung nennen. Die Zahl der Fälle, in denen Kodizes angestoßen wurden, letztlich jedoch gescheitert sind, entweder weil sie gar nicht erst zustande kamen oder nach Verabschiedung nicht eingehalten wurden, dürfte jedoch erheblich größer sein. Gerade Internet-bezogene Selbstregulierungsansätze sind in der Vergangenheit selten erfolgreich gewesen, wie beispielsweise der 2013 endgültig gescheiterte Versuch des deutschen Innenministeriums, einen Verhaltenskodex der Anbieter sozialer Netzwerke zum Datenschutz herbeizuführen.

Ob Kodizes scheitern oder erfolgreich sind, hängt von einer Vielzahl unterschiedlicher Faktoren ab. Offensichtlich erscheint etwa, dass manche Regelungssachverhalte sich besser hierfür eignen als andere. Beispielsweise funktioniert die regulierte Selbstregulierung (wenn man diese als eine Art Kodex verstehen will) im deutschen Jugendschutzrecht bei traditionellen Medien recht gut. Im Internet stößt sie indes an ihre Grenzen, und ein entsprechend anerkanntes Pendant auf dem Gebiet des Online-Datenschutzes

WAS IST EIN DIGITALER KODEX?

Diese Auffassung des Kodex-Begriffs passt sehr gut zur Gegenwartsgesellschaft. Sie zeichnet sich unter anderem dadurch aus, dass das meiste in ihr sich durch organisatorisches Handeln vollzieht. Die in Organisationen handelnden Menschen sind an professionelle Rollen gebunden. Personen in diesen Rollen sind dadurch in der Regel auf eine rollenspezifische Aufgabenverantwortung ausgerichtet, die ihnen durch die Organisation übertragen wird. Dies verhindert freilich nicht, dass sie als Personen moralisch verantwortlich sein können (und vielleicht auch wollen) und Aufgabenverantwortung und moralische Verantwortung konfligieren können.

Ein Kodex, der sich auf professionelles Rollenhandeln bezieht, ist insofern ein interessantes Korrektiv zu den von Organisationen formulierten Aufgabenverantwortungen, die primär über Geschäftsinteressen definiert sind. Er appelliert an professionelle Akteure, in ihrem Handeln weitere Gesichtspunkte zu berücksichtigen, die gesellschaftlich oder moralisch als relevant erachtet werden, weil diese professionellen Akteure – Ärzte, Journalisten oder Wissenschaftler – großen Einfluss auf diese gesellschaftlichen Aspekte oder moralischen Güter haben.

Um welche Aspekte oder Güter es sich bei Plattformanbietern handelt, wäre zu untersuchen. Ebenso, ob aus den genannten, sich an individuelle Akteure richtenden Verhaltenskodizes Erkenntnisse abgeleitet werden können, die sich auf Kodizes für Organisationen bzw. die in Organisationen – Plattformen – handelnden Verantwortlichen übertragen lassen.

Der vorgeschlagene „Kodex"-Begriff ist durchaus kompatibel mit dem zentralen Moralbegriff moderner Gesellschaften: Verantwortung. Dieses Zuschreibungskonzept für Handlungsfolgen (oder Aufgaben) hat sich gegenüber anderen Begriffen, wie zum Beispiel der Pflicht, durchgesetzt, weil es das Wissen um die Relevanz von Handlungsmacht bereits impliziert. Je größer die Handlungsmacht und je weitreichender die Einflussmöglichkeiten von jemandem sind, desto mehr Verantwortung trägt er für sein Handeln oder das Unterlassen von Handlungen.

ist erst recht nicht in Sicht. Der Umstand, dass das gleiche Modell in Bezug auf den einen Regelungssachverhalt und das eine Medium funktioniert, bei einem anderen Thema und in einer anderen Umgebung jedoch versagt, wird viele Gründe haben. Ein Faktor wird darin liegen, dass Jugendschutz noch immer einen anderen moralischen Stellenwert hat als Datenschutz. Eine andere Erklärung wird lauten, dass Daten im Netz heute zumeist die wichtigste Währung und damit wesentliche Grundlage von Online-Geschäftsmodellen sind. Ein hohes Datenschutzniveau kann die Erwerbsmöglichkeiten der Unternehmen in ihren Grundfesten erschüttern, wobei Jugendschutz im Regelfall weniger geschäftskritisch sein wird.

Ein weiterer neuralgischer Punkt, dies wurde in den Untersuchungen und Diskussionen immer wieder deutlich, liegt darin, wie ein Kodex entsteht, wer an dessen Erstellung beteiligt ist und wie er eingesetzt wird. Dem Erfolg abträglich wird es in der Regel sein, wenn die betroffenen Akteure nicht am Aushandlungsprozess beteiligt oder unterrepräsentiert sind. Da Kodizes gerade im Netz angesichts der dort herrschenden Durchsetzungsdefizite nicht primär auf Sanktionen angewiesen sein können, liegt die wesentliche Herausforderung darin, Modelle für Aushandlungsprozesse zu finden, an denen alle vom jeweiligen Kodex betroffenen Akteure – wie die Bürger, Unternehmen oder auch der Staat – angemessen beteiligt sind.

Ob ein Digitaler Kodex als alternative Regelungsform für netzbezogene Verhaltensregeln geeignet ist, ob Deutschland einen solchen braucht, hängt damit maßgeblich davon ab, wie er entsteht und wie der Prozess zu dessen Entstehung konzipiert und umgesetzt wird. In welcher Form sich das Ergebnis von Debatte und Aushandlung manifestiert, ist dagegen – vermutlich – von eher untergeordneter Bedeutung. Ein Kodex-Prozess kann in einen konkreten Regelkatalog münden, etwa in Form von „zehn Geboten zum Umgang mit personenbezogenen Daten" oder „zwanzig Regeln für die Interoperabilität zwischen Plattformen". Das Ergebnis des Aushandlungsprozesses kann sich jedoch auch in ungeschriebenen Normen oder rein faktisch entstehenden Verhaltensregeln manifestieren, etwa in der Form, dass sich die Anbieter von Plattformen nach Abschluss einer öffentlichen Debatte aufgrund des hierdurch entstandenen Handlungsdrucks selbst dafür entscheiden, für Interoperabilität zu sorgen.

Für die Konzeption solcher Aushandlungsprozesse sind mehrere Varianten denkbar. Im Projekt wurden zwei mögliche Ansätze entwickelt, die sich stark voneinander unterscheiden. Die erste Variante zeigt ein Modell auf, in dem Elemente klassischer institutioneller Regulierung mit netzspezifischen Konzepten der Bürgerbeteiligung kombiniert werden. Der Aushandlungsprozess wird in diesem Fall institutionell eingebettet, was vorbestimmte, klar geregelte Abläufe impliziert.

Das zweite Modell, das den Arbeitstitel „Moderierter digitaler Straßenkampf" trägt, setzt dagegen mehr auf den Einfluss einer – naturgemäß nur eingeschränkt steuerbaren – massenhaften Meinungsäußerung. Hier steht die Konfrontation mächtiger Akteure wie dem Staat oder den Internet-Unternehmen mit gesellschaftlichen Forderungen durch die Nutzer im Vordergrund. Das Modell basiert auf dem Prinzip „Hilfe zur Selbsthilfe". Es basiert auf der Annahme, dass es möglich ist, die Bürger und/oder die Zivilgesellschaft dabei zu unterstützen, Diskussionen anzustoßen und ihre Forderungen gegenüber den mächtigen Akteuren zu formulieren und durchzusetzen. Derzeit verlaufen Massenbewegungen im Netz zumeist mehr oder weniger unkoordiniert und ohne konkrete Konzepte. Das Modell wäre wirksam, wenn es gelänge, Prozesse zu entwickeln und zur allgemeinen Verfügung zu stellen, die es ermöglichen, solche Bewegungen besser vorbereiten und steuern zu können und damit deren Erfolgsaussichten zu erhöhen. Die Umsetzung solcher Prozesse – und hierin läge eine Kombination beider Modelle – könnte wiederum institutionell unterstützt werden.

Allgemeines Fazit des Projekts ist, dass die Ausgangsfrage: „Braucht Deutschland einen Digitalen Kodex" – wenn sie so abstrakt gestellt wird – zu bejahen ist. Offensichtlich reichen die geltenden Regelungen und Regelungskonzepte nicht aus, um das Verhalten in vielen Bereichen des Netzes effizient zu steuern sowie Verantwortung angemessen zu verteilen. Insofern sollte der Frage, wie alternative Regelungsansätze konzipiert und Verhaltensregeln für konkrete Problemfelder entwickelt, ein- und umgesetzt werden, weiter nachgegangen werden. Die Fokussierung auf Deutschland in der Fragestellung hat

zwei Gründe: Zum einen sind – grundsätzlich – soziale Normen sehr stark vom Kulturraum abhängig, in dem sie wirken, zum anderen ist es – aus praktischen Gesichtspunkten – durchaus denkbar und möglich, auch für Plattformen, deren Betreiber ihren Konzernsitz im außereuropäischen Ausland haben, lokale Regelungen einzufordern und einzuführen, da es häufig Niederlassungen in Deutschland oder Europa gibt. Nicht alles wird sich aber in einem nationalen Rahmen lösen lassen.

Für die Einführung eines Digitalen Kodex sind verschiedene Wege denkbar. Sinnvoll erscheint es, zunächst eine begrenzte Zahl konkreter Themen für den Anwendungsbereich eines Digitalen Kodex auszuwählen und hieran die Funktionsfähigkeit des einen oder anderen Modells theoretisch oder in Form eines Modellversuchs durchzuspielen. Im Zweifel wird es nur im Praxisversuch gelingen, die Stärken und Schwächen der konzeptionellen Ansätze aufzudecken und sie zu optimieren. In der Auswahl des Regelungsgegenstandes liegt dabei – neben der konzeptionellen Ausgestaltung des Prozesses – ein neuralgischer Punkt. Die Relevanz des gewählten Themas ist für die Akteure, die an der Entstehung des Kodex teilhaben und ihn letztlich befolgen sollen, ein zentraler Faktor, um zu handeln.

1.8 Aufbau des Dokuments

Im vorliegenden Dokument werden im zweiten Kapitel zunächst die Grundlagen in Form einer Auseinandersetzung mit der elementaren Frage gelegt, wie Verantwortung im Netz zuzuordnen ist, welche besonderen Rahmenbedingungen des Netzes hierbei zu beachten und welche Akteure generell zu berücksichtigen sind bzw. welche Rollen sie im Machtgefüge einnehmen. Im dritten Kapitel wird der Frage nachgegangen, worauf sich ein Digitaler Kodex beziehen könnte. Im vierten Kapitel werden schließlich die beiden im Projekt erarbeiteten Modelle für Aushandlungsprozesse zu einem Digitalen Kodex dargestellt. In die genannten Kapitel sind Experteninterviews und Berichte zu den öffentlichen Veranstaltungen in München und Hamburg integriert. Das Dokument schließt mit einem Epilog. Die Themenpapiere, aus denen im Text referiert wird, werden im Annex in vollständiger Fassung wiedergegeben, zusammen mit ausführlichen Berichten über die öffentlichen Veranstaltungen in München und Hamburg.

2. Verantwortung in der digitalen Welt

Verantwortung setzt Interessen und Ideen voraus. Aber wer verfolgt im Netz welche Interessen? Wie erkenne ich im Internet, dass jemand verantwortungsbewusst handelt, und wie kann man Verantwortung effektiv steuern?

Durch die Digitalisierung entstehen in atemberaubender Geschwindigkeit neue Handlungsoptionen, ohne dass sich zugleich schnell genug Strukturen dafür herausbilden, um zu bestimmen, wie Verantwortung für diese Handlungen zugewiesen werden kann. Dies führt dazu, dass Akteure zunächst alle sich bietenden Möglichkeiten nutzen wollen – auch um Vorteile für sich zu erlangen –, ohne aber gleichzeitig immer die Verantwortung dafür zu übernehmen. Die Gründe dafür können unterschiedlich sein: Überforderung, kalkulierte Risikoweggabe, Nicht-kümmern-Wollen oder schlicht Unkenntnis über die Tragweite der eigenen Handlungen. Die im Widerspruch stehenden Vorstellungen der gesellschaftlichen Gruppen, etwa wenn es darum geht, Verantwortung für Sicherheit im Internet zu übernehmen, wurden im Rahmen der DIVSI Milieu-Studie und der DIVSI Entscheider-Studie zu Vertrauen und Sicherheit im Internet herausgearbeitet. Eines der Ergebnisse dieser Studien ist, dass Menschen Verantwortung für Sicherheit jeweils bei anderen betroffenen Akteuren sehen. Dies zeigt bereits, wie komplex und zentral es ist, die Frage zu beantworten, wie Verantwortung zugewiesen werden kann.

> **„Anonymität und Pseudonymität führen dazu, dass man sich anders verhält. Das muss nichts Schlechtes sein, aber echtes Verantwortungsgefühl erzeugt man erst, wenn man das Gefühl bekommt, echten Menschen gegenüberzustehen."**
>
> **Stefan Plöchinger,** Chefredakteur Süddeutsche.de und Geschäftsführender Redakteur Online der Süddeutschen Zeitung, Diskussion, Öffentliche Veranstaltung München, 04.07.2013

Das Netz ist ein komplexes System und ein 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 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.

Eine allgemeingültige Definition von Verantwortung gibt es jedoch nicht.[18] Hier 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 (zum Beispiel die Folgenbeseitigung bei Naturkatastrophen) beziehen. Normenverstöße haben meist Folgen und ziehen in der Regel Sanktionen nach sich, vor allem 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 (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 unter Umständen gravierender sein als rechtliche Sanktionen, beispielsweise bei einem Ausschluss aus der Gemeinschaft wegen Fehlverhaltens.

2.1 Arten von Verantwortung

Um zu identifizieren, welche Akteure in einem Handlungsumfeld (zum Beispiel dem Internet) Verantwortung tragen und worauf sie sich bezieht, ist es sinnvoll, zwischen zwei Formen von Verantwortung zu 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 ermöglichen.[19]

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 einstehen zu müssen und sich hierfür „zu verantworten".

> **„Verantwortung als solche ist ständig in Bewegung. Wir weisen sie zu, wir teilen sie, wir weisen sie von uns, wir reißen sie an uns – es ist ein sehr mobiles Konzept."**
>
> **Dr. Jeanette Hofmann,** Gründungsdirektorin am Alexander von Humboldt Institut für Internet und Gesellschaft und wissenschaftliche Mitarbeiterin/Projektleiterin am Wissenschaftszentrum Berlin für Sozialforschung, Öffentliche Veranstaltung München, 04.07.2013

Verantwortung kann individuell oder kollektiv bestehen. Individuell kann sie einem Individuum, einer Institution oder einem Unternehmen zugeordnet werden. Kollektive Verantwortung tragen Gruppen (zum Beispiel die Wirtschaft), soweit ihnen eine Rolle mit

18 Siehe zu den unterschiedlichen Definitionen Wikipedia: Verantwortung, de.wikipedia.org/wiki/Verantwortung.

19 Zum Thema: www.datenschutzzentrum.de/presse/20130424-facebook-klarnamen-ovg.htm.

identifizierbarem Interesse zukommt. Zudem sind Eigenverantwortung (für selbst herbeigeführte Handlungsfolgen) und Mitverantwortung (für durch andere herbeigeführte Handlungsfolgen) zu unterscheiden.

Verantwortung setzt nach traditionellem Verständnis Handlungsfreiheit und -fähigkeit voraus. Wer nicht handeln kann, ist nicht verantwortlich, wer keine Wahl hat, wie er handelt (zum Beispiel 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.

2.2 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. Dieser Gedanke steht etwa hinter der Gefährdungshaftung oder dem Organisationsverschulden. In diese Richtung gehen viele Debatten über die Haftung im Internet, vor allem, da hier der eigentlich verantwortliche Nutzer häufig nicht identifizierbar ist. Ein Beispielfall 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.

> **„Der Nutzer als ‚Datensouverän' wäre ein Wunschgedanke und stünde im Gegensatz zum Schutzgedanken, den der Datenschutz ganz klassisch beinhaltet. Der Nutzer sollte in der Lage sein, Entscheidungen bezüglich seiner Daten im Netz eigenständig zu treffen. Dafür braucht es Transparenz und Tools, die den Nutzer in diese Position versetzen. Der Schutzgedanke sollte aber nicht vollständig aufgehoben werden. Der Anbieter hat Verpflichtungen beispielsweise zur Transparenz, die durch Regulierung erwirkt werden. Dadurch kann der Nutzer ein ‚Datensouverän' werden. Es muss also eine Mischung aus Regulierung, Verpflichtung der Anbieter und Nutzersouveränität sein."**
>
> **Stephan Noller,**
> nugg.ad CEO, Konsultation

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.

2.3 Verantwortung im und außerhalb des Internets

Wie neu ist „neu", und ist „neu" ein Wert an sich? Ist die digitale Welt nur ein Spiegelbild der realen Welt?

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.

Verantwortung ist 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*[20], 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.

> **„Ich denke, dass den meisten Nutzern erst mal klar werden muss, dass das Internet keine irreale Welt ist. Es ist real, und daher besteht auch die Notwendigkeit, dass sich auch für das Netz allgemein geltende Regeln und Werte entwickeln."**
>
> **Tatjana Halm,** Referatsleiterin Markt und Recht bei der Verbraucherzentrale Bayern, Diskussion, Öffentliche Veranstaltung München, 04.07.2013

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 (Menschen, Unternehmen, Institutionen, Politik). Internet-spezifische Verantwortungssubjekte (also Akteure, die eigene Entscheidungen auf Basis von Handlungsfreiheit und -fähigkeit treffen) gibt es bislang nicht, denn noch gibt es keine Technologien, die auf Basis künstlicher Intelligenz autonom denken und entscheiden. Alles, was im Internet passiert, ist auf menschliches Handeln zurückzuführen. Auch im Internet darf Verantwortung als Ordnungsprinzip daher weder infrage gestellt noch die Bedeutung von Verantwortung heruntergespielt werden.

20 Der Begriff „Cyberspace" wurde zu Beginn der 1980er-Jahre eingeführt und wird im Allgemeinen als Synonym für einen virtuellen Interaktionsraum (im Gegensatz zum „Realspace") verwendet.

> **„Wie spielen eigentlich im Internet die unterschiedlichen Faktoren wie soziale Normen, Code/Softwarearchitektur und formales Recht zusammen, und welche Akteure haben welche Rolle?“**
>
> **Prof. Dr. Wolfgang Schulz,** Direktor des Hans-Bredow-Instituts für Medienforschung und des Alexander von Humboldt Instituts für Internet und Gesellschaft, Auftaktworkshop, 03.06.2013

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, siehe die Diskussion in der Einleitung. Diese machen eine Neubeurteilung 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 zum Teil 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.

Öffentliche Veranstaltung in München

JEDER MACHT IM NETZ, WAS ER WILL – VERANTWORTUNG IN DER DIGITALEN WELT

Michael Siemens,
Mitglied des Landesschülerrats
Bayern (bis 2013)

Die Öffentlichkeit als Spiegel der ersten Projektschritte

Matthias Kammer, Direktor des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI)

Ein wesentliches Element des Projekts war die Einbindung interessierter Kreise der Bevölkerung über öffentliche Veranstaltungen. Den Auftakt bildete am 4. Juli 2013 eine öffentliche Diskussionsveranstaltung in München. Zwei Keynotes verdeutlichten unterschiedliche Facetten der Frage der Verantwortung in der digitalen Welt. Während Dr. Jeanette Hofmann, Gründungsdirektorin am Alexander von Humboldt Institut für Internet und Gesellschaft und wissenschaftliche Mitarbeiterin/Projektleiterin am Wissenschaftszentrum Berlin für Sozialforschung, den Verantwortungsbegriff aus sozialwissenschaftlicher Perspektive erläuterte, berichtete Michael Siemens, Mitglied des Landesschülerrats Bayern (bis 2013), aus seinem digitalen Leben.

Prof. Dr. Johannes Buchmann, Vizedirektor des Center for Advanced Security Research Darmstadt und Professor für Informatik und Mathematik an der Technischen Universität Darmstadt

Fotos: Christian Back

Auf Basis dieser beiden Gegenpole – Wissenschaftlerin vs. Digital Native – diskutierte im Anschluss ein divers besetztes Podium: Prof. Dr. Johannes Buchmann, Vizedirektor des Center for Advanced Security Research Darmstadt und Professor für Informatik und Mathematik an der Technischen Universität Darmstadt, Dr. Christoph Habammer, bis Ende 2013 Leiter der Stabsstelle des IT-Beauftragten der Bayerischen Staatsregierung, Tatjana Halm, Referatsleiterin Markt und Recht bei der Verbraucherzentrale Bayern, und Stefan Plöchinger, Chefredakteur Süddeutsche.de und Geschäftsführender Redakteur Online der Süddeutschen Zeitung. Aspekte der Diskussion waren neben der Notwendigkeit einer verstärkten Förderung der Medienkompetenz die Herausforderungen durch die Dauerhaftigkeit von Informationen im Netz und die Schattenseiten von Anonymität insbesondere im Hinblick auf soziales Verhalten.

Nicht zuletzt in der Diskussion mit dem Publikum zeigten sich

Dr. Jeanette Hofmann, Gründungsdirektorin am Alexander von Humboldt Institut für Internet und Gesellschaft und wissenschaftliche Mitarbeiterin/Projektleiterin am Wissenschaftszentrum Berlin für Sozialforschung (oben), Teilnehmerin der Publikumsdiskussion (unten)

unterschiedliche Haltungen zur Frage, welche Verantwortung die Akteure im digitalen Raum tragen und welche Möglichkeiten angesichts der globalen Ausrichtung des Netzes bestehen, diese zu regulieren. Dass dennoch eine öffentliche Debatte über diese Themen notwendig ist, kristallisierte sich gleichzeitig als Konsens heraus und bestätigte den Bedarf an einem öffentlichen Diskurs. ⊡

2.4 Wer trägt Verantwortung im Internet?

Im Prinzip sind die handelnden Akteure im Internet dieselben wie in gegenständlichen Lebensräumen, also Bürger, die Wirtschaft und ihre Interessenvertretungen, nicht staatliche Institutionen (NGOs[21]), religiöse Organisationen, Medien und der Staat. Als weiterer wichtiger Akteur haben die Architekten, Entwickler und Beherrscher der technischen Infrastruktur und der Werkzeuge, die das Internet technisch ausmachen, großen Einfluss. Hierzu zählen neben Zertifizierungsstellen, Registraren und Standardisierungsgremien vor allem die Anbieter der Telekommunikationsnetze, die Zugangsprovider, Plattform- und Suchmaschinenanbieter und andere Gatekeeper. All diese Akteure sind Teil eines komplexen Beziehungsgeflechts mit sich überschneidenden Verantwortungsbereichen.

> **„Ein dritter Akteur neben den Nutzern und Anbietern im Netz sind die Entwickler. Die technische Ausgestaltung beeinflusst maßgeblich das Handeln im Netz. Insofern könnten bei einem Digitalen Kodex auch die Entwickler eine mögliche Adressatengruppe sein."**
>
> **Prof. Dr. Rüdiger Grimm,** Professor für IT-Riskmanagement im Fachbereich Informatik an der Universität in Koblenz, 2. Expertenworkshop, 10.09.2013

Die Beziehungsgeflechte im Internet unterscheiden sich zum Teil erheblich von der gegenständlichen Welt. Handeln im Internet hat häufig einen anderen, nicht selten weiter reichenden, 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 damit 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 Nutzer sind nicht nur in Deutschland, sondern auf der ganzen Welt. Die Anbieter sind ebenfalls nicht nur in einem Land aktiv. Bei sozialen Normen geht es ja häufig nicht nur um Durchsetzungsdefizite, sondern es geht ja auch darum, dass viele Probleme im Netz in der physischen Welt nicht vorkommen. Da geht es nicht unbedingt um Verhaltensweisen, die verboten sind, und wenn das so ist, dann reicht der Ansatz, in Deutschland gilt deutsches Recht, nicht aus. Es geht um Verhalten, das nicht direkt reglementiert werden kann."**
>
> **Dr. Till Kreutzer,** Partner beim iRights.Lab und der Rechtsanwaltskanzlei iRights.Law, Redaktionsleiter von iRights.info, 2. Expertenworkshop, 10.09.2013

Die Zuordnung von Verantwortung bei Existenz einer Vielzahl denkbarer Verantwortungssubjekte bewegt sich in einem Spannungsfeld zwischen 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. Jemand, dessen 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. Insofern kann es sinnvoll sein, Verantwortung

21 „Non-governmental organisations"

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.

> **„Es gibt in vielen Bereichen des Netzes dringenden Handlungsbedarf für den Staat, allerdings kann nicht alles über Gesetze geregelt werden. Der Staat, öffentliche Verwaltungen, Gewerkschaften und Parteien müssen sich aber ganz allgemein viel mehr diesen Themen widmen und sie öffentlich problematisieren. Vor allem die Kultur des Freigebens von Daten und dass das Netz nicht vergisst, sind Probleme, die verstärkt in der Gesellschaft diskutiert werden sollten. Zu den staatlichen Aufgaben zählt, für Arbeitgeber gesetzlich zu definieren, dass sie von Bewerbern und Beschäftigten im Netz veröffentlichte Aussagen, die nicht im Kontext mit der eigenen Firma stehen, nicht auswerten und für Entscheidungen heranziehen dürfen."**
>
> **Carlos Sievers,** Abteilungsleiter öffentliche Dienste, DGB Nord, Konsultation

> **„Der Staat kann und darf in Bezug auf die Themen der digitalen Welt nicht neutral sein. Dies resultiert zunächst vor allem daraus, dass er seiner Schutzfunktion gegenüber dem Bürger gerecht werden muss."**
>
> **Halina Wawzyniak MdB,** Netzpolitische Sprecherin der Fraktion Die Linke im Bundestag, Konsultation

Angesichts dieser Faktoren zeigte sich eine wichtige Aufgabe für das Projekt „Braucht Deutschland einen Digitalen Kodex?": Um ein Verantwortungskonzept für das Internet zu entwickeln, ist 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.

> **„Für einen Digitalen Kodex müssen die unterschiedlichen Interessen, Akteurskonstellationen und Machtverhältnisse im Netz identifiziert werden. Die sozialen Regeln sehe ich eher im Sinne einer Dynamik, die diese Beziehungen strukturiert."**
>
> **Dr. Alexandra Manske,** freiberufliche Soziologin in Berlin, ehemals Humboldt-Universität zu Berlin, Auftaktworkshop, 03.06.2013

2.5 Wie kann Verantwortung im Netz zugewiesen und gesteuert werden?

Die herrschenden sozioökonomischen 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 Internet noch außerhalb desselben.

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.

> **„Es gibt nicht den einen Nutzer oder die Nutzerin, gerade das Nutzungsverhalten im Internet ist sehr individuell. Viele sind sich nicht im Klaren darüber, wo sie mit ihrem Handeln im Netz eine Verpflichtung eingehen und welche Folgen das haben kann. Ein Klick ist schneller gesetzt als ein Vertrag unterschrieben, und der Finger ist dabei oft schneller als der Kopf."**
>
> **Jutta Croll,** Geschäftsführendes Mitglied des Vorstands der Stiftung Digitale Chancen, Diskussion, Öffentliche Veranstaltung Hamburg, 07.11.2013

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 zum Beispiel 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) Architektur[22], soziale Normen und der Markt hätten auf die Handlungsoptionen des Individuums so großen Einfluss, dass der einzelne Nutzer einem von außen gesteuerten *pathetic dot*[23] 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 zum Beispiel daran, dass *DRM-Systeme*[24] auf dem Musikmarkt erst entschärft wurden und dann verschwunden sind (Murray 2011, 277).

> **„Beim Agieren im Netz ist zumeist ein Vertrauensvorschuss nötig, weil man nicht alles überblicken kann, vor allem die Technik nicht."**
>
> **Dr. Ralf Kleindiek,** Staatssekretär im Bundesministerium für Familie, Senioren, Frauen und Jugend (bis Januar 2014 Staatsrat der Behörde für Justiz und Gleichstellung der Freien und Hansestadt Hamburg), Begrüßung, Öffentliche Veranstaltung Hamburg, 07.11.2013

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 Shitstorms wehren. Um ihre Macht als Gruppe, als Community, ausüben zu können, müssen die Individuen in einen Dialog treten, sich abstimmen und

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

23 Wörtlich übersetzt: „armseliger Punkt", d.h. ein Akteur, der als relevante Größe zu vernachlässigen ist.

24 „DRM" steht für „Digital Rights Management", also digitale Rechteverwaltung.

konsolidieren. Ihre Macht üben sie – anders als in der Vorstellung der Liberalisten – zu großen Teilen über Repräsentanten (wie in der Politik) aus.

> **„Seit vielen Jahren wird immer deutlicher, dass die zentralen Weichenstellungen im Internet durch Monopol- oder Oligopolanbieter rein unter kommerziellen Gesichtspunkten vorgenommen werden. Die Nutzer werden als Kunden und nicht als Bürger wahrgenommen und haben nur sehr beschränkte Möglichkeiten, an der Gestaltung des Netzes mitzuwirken. Oft ist die einzige Möglichkeit der Partizipation, einen bestimmten Dienst nicht mehr in Anspruch zu nehmen. Andernfalls können die Nutzer eigentlich nur den bestehenden Handlungsrahmen akzeptieren. Das ist für mich ein sehr unbefriedigender Zustand. Der gesellschaftliche Gestaltungsanspruch muss gestärkt werden – gegebenenfalls auch mithilfe gesetzlicher Regelungen."**
>
> **Peter Schaar,** Vorstand der Europäischen Akademie für Informationsfreiheit und Datenschutz (bis Dezember 2013 Bundesbeauftragter für den Datenschutz und die Informationsfreiheit), 2. Expertenworkshop, 10.09.2013

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.

INTERVIEW MIT DR. JEANETTE HOFMANN

Selbstregulierung funktioniert beim Datenschutz nicht

? Wir haben im Prinzip im Netz drei große Player: die Unternehmen, die Nutzer und den Staat. Wie ist das Verhältnis zwischen diesen drei Gruppen?

Jeanette Hofmann: Zunächst einmal: Dieser Dreiklang aus Wirtschaft, Nutzern und Staat ist umstritten. Viele Leute – vor allem in den internationalen Gremien, in denen ich mich bewege – finden, dass zum Beispiel die technische Community, die das Netz entwickelt, einen eigenen Status hat, also weder zum einen noch zum anderen Feld gehört. Sie gehört nicht zu den Nutzern und der Zivilgesellschaft, aber auch nicht zur Wirtschaft. Aber um die Frage zu beantworten: Zurzeit bestimmt eindeutig die Wirtschaft am stärksten, wie das Internet genutzt wird und wie es sich entwickelt.

? Wie würden Sie die Rolle der Wissenschaft beschreiben? Ist die Wissenschaft auch ein Mitspieler in diesem Bereich, oder könnte sie auch als Schiedsrichter dienen?

JH: Im Bereich der Ingenieurwissenschaften ist die Wissenschaft eindeutig konstituierend. Dort werden beispielsweise die Algorithmen entwickelt, die so etwas wie Suchmaschinen hervorbringen oder das Börsengeschehen beeinflussen. Die ganze Weiterentwicklung der Netz-Architektur ist zum

Dr. Jeanette Hofmann

Die Politikwissenschaftlerin ist Gründungsdirektorin am Alexander von Humboldt Institut für Internet und Gesellschaft und wissenschaftliche Mitarbeiterin/Projektleiterin am Wissenschaftszentrum Berlin für Sozialforschung. Sie forscht am Wissenschaftszentrum Berlin zu den Themen Global Governance, Regulierung des Internets, Informationsgesellschaft und Wandel des Urheberrechts. 2010 ist sie als Sachverständige in die Enquetekommission Internet und digitale Gesellschaft berufen worden. Sie hat aktiv am UN-Weltgipfel zur Informationsgesellschaft mitgewirkt und engagiert sich seit 2006 im Folgeprozess als Mitglied der Multi-Stakeholder Advisory Group in der Organisation des Internet Governance Forum.

Foto: Humboldt Institut für Internet und Gesellschaft

großen Teil durch Forschung bestimmt. Ein Teil dieser Forschung ist an Universitäten beheimatet und wird aus öffentlichen Mitteln kofinanziert. Gleichzeitig fließen aber auch viele private Mittel. Außerdem unterhalten große Unternehmen wie Facebook und Google ihre eigenen Forschungsabteilungen.

? Der Slogan „Code is Law" besagt, dass in der Software schon Nutzungsformen festgeschrieben sind. Wie sehr beeinflusst Technik, wie das Netz genutzt wird?

JH: Das lässt sich so einfach nicht beantworten. Technische Konfigurationen sind oft offen für Neuinterpretationen. Techniken sind nie hundertprozentig von den Produzenten vorgegeben. Von Seiten der Nutzer findet immer auch ein Aneignungsprozess statt, der unter Umständen dazu führt, dass der eigentlich vorgesehene Zweck einer Technik geändert wird. Eines der bekanntesten Beispiele ist die SMS, eine ehemalige Steuerungsnachricht, die nicht mal Geld gekostet hat. Sie wurde zu einer maßgeblichen Einkommensquelle von Mobilfunkanbietern, als die Nutzer sich diese Technik angeeignet und ihr eine neue Bedeutung gegeben haben. Diese Art des Einflusses von Nutzern kann man überall und immer beobachten.

? Sollte Technik nicht immer flexibel und reinterpretierbar sein?

JH: Ich bin mir da nicht sicher. Es gibt viele Beispiele, wo man sich das nicht wünscht. Wir möchten zum Beispiel nicht, dass man Autos jederzeit in Rennautos verwandeln kann. Es kommt darauf an, wie risikoreich eine Technologie ist und ob eine Reinterpretation gesellschaftlich wünschenswert ist. Im Augenblick kommt diese Diskussion bei 3-D-Druckern auf: Müssen wir künftig damit rechnen, dass Leute sich ihre eigenen Waffen ausdrucken?

Solche Fragen lassen sich sehr schlecht verallgemeinern. Aber es gibt tatsächlich eine große Diskussion darüber, ob Organisationen, die technische Standards setzen, stärker das gesellschaftliche Wohl und die Folgen ihrer eigenen Standards in den Blick nehmen sollten. Die Snowden-Debatte hat zum Beispiel dazu geführt, dass Service-Provider darüber reden, wie Datenschutz-Gesichtspunkte stärker berücksichtigt werden können.

? In Ihrer Forschung über das Urheberrecht haben Sie die Frage untersucht, ob es neben dem Recht weitere Aspekte gibt, die man stärker im Rahmen einer Regulierung einbeziehen sollte. Könnten Sie kurz erläutern, was Sie damit meinen?

JH: Das Recht, so wie es geschrieben steht, passt nicht immer auf alle gesellschaftlichen Situationen, in denen es angewandt wird. Beim Urheberrecht ist das, was geschützt wird, nicht immer das, was das Produkt ausmacht. Das Urheberrecht schützt nicht die Idee, sondern nur die konkrete Form, den Ausdruck eines Werkes. Wenn aber die Idee das zentrale Element eines Produkts ist, gibt es eine Regulierungslücke. Ein Beispiel dafür – und das haben wir auch untersucht – sind TV-Formate. Hier ist die zentrale Idee bedeutsam, aber sie ist nicht urheberrechtlich geschützt.

Wir haben aber festgestellt, dass die Produzenten solcher Güter sich mit anderen Mitteln be-

SELBSTREGULIERUNG FUNKTIONIERT BEIM DATENSCHUTZ NICHT

helfen. Diese Mittel könnte man als soziale Normen bezeichnen. Das geschieht so, dass alle Beteiligten so tun, als wären Formate geschützt. Das bedeutet beispielsweise, dass man ein TV-Format als Lizenz weitergibt, obwohl das unnötig ist: Andere könnten die Idee für das Format übernehmen und für sich adaptieren, ohne Lizenzgebühren zu zahlen. Aber alle Beteiligten profitieren davon und halten sich daran. Es haben sich soziale Konventionen ausgebildet, die diesen Markt ordnen.

Soziale Normen scheinen vor allem dann zu wirken, wenn die Zahl der Teilnehmer überschaubar ist und die Beteiligten sich untereinander kennen. Dadurch können Sanktionen durchgesetzt werden, wenn Leute zu weit ausscheren. Es ist auffällig, dass es um TV-Formate relativ selten zu Gerichtsprozessen kommt. Rechtliche Auseinandersetzungen werden meistens durch außergerichtliche Vergleiche geklärt. Es gibt also Verfahren, wie man mit diesen Problemen umgeht, nur sind sie rechtlich nicht kodifiziert. Aber sie funktionieren: Auffällig wenig Produzenten rufen nach strengeren Urheberrechten oder nach einem expliziten Formatschutz.

? Würde es auch im Bereich des Datenschutzes funktionieren, dass man mit sozialen Konventionen statt mit rechtlichen Normen arbeitet?

JH: Da bin ich skeptisch. Generell hat man bei rechtlichen Regeln ja immer das Problem mit der Durchsetzung: Wie stellt man sicher, dass die Gesetze eingehalten werden? Das Problem gibt es beim Datenschutz sowohl bei geschriebenem als auch ungeschriebenem Recht.

? Heißt das, beim Datenschutz muss das Primat des Gesetzes aufrechterhalten werden?

JH: Wir haben es im Internet mit einem globalen Raum zu tun. Damit stößt das Recht beständig an seine Grenzen. Das stellt vor allen Dingen dann ein Problem dar, wenn wir viele Güter aus einem Land beziehen, das ganz andere Datenschutztraditionen hat als Europa und Deutschland. Das Recht funktioniert international nur sehr begrenzt.

Gleichzeitig produzieren so viele Menschen datenschutzrelevante Inhalte, dass Selbstregulierung an ihre Grenzen stößt. Bei den Produzenten von TV-Formaten ist die Anzahl der Player überschaubar, und alle sind aufeinander angewiesen. Diese wechselseitige Abhängigkeit sorgt dafür, dass schwarze Schafe aus den Netzwerken ausgestoßen werden. Das ist im Datenschutz ganz anders – man kann nicht eben mal auf Facebook verzichten. Deshalb wage ich zu bezweifeln, dass wir mit Selbstregulierung weiterkommen: Der ökonomische Anreiz, Datenschutzprinzipien zu ignorieren, ist erheblich höher, als sie anzuwenden und einzuhalten.

? Könnten Sie sich denn Anreize – egal welcher Art – vorstellen, die groß genug wären, dass eine Firma wie Facebook Zugeständnisse macht?

JH: Ehrlich gesagt, nein. Ich sehe eher die gegenteilige Entwicklung. Für Start-ups, die im Bereich Big Data arbeiten, besteht der Anreiz der neuen Märkte darin, so viele Daten wie möglich zu sammeln. Diese dienen dazu, um Muster oder Wahrscheinlichkeiten zu erkennen und neue Produkte zu entwickeln. Sogar die öffentliche Hand arbeitet mit solchen Unter-

> **Enthüllungen wie die von Snowden müssen sich in Wahlergebnissen niederschlagen – dann wird sich etwas ändern.** Dr. Jeanette Hofmann

nehmen zusammen und verletzt selbst Datenschutzprinzipien, weil sie meint, davon zu profitieren. Man kann nicht vom Urheberrecht auf den Datenschutz schließen.

? Wir haben im Augenblick Diskussionen um nationale Netze. Können Sie sich Geschäftsmodelle vorstellen, die auf Datensparsamkeit beruhen und trotzdem ökonomisch erfolgreich sind?

JH: In bestimmten Bereichen kann ich mir das durchaus vorstellen, beispielsweise bei Herstellern von Routern, die stärker geografische Präferenzen ihrer Kunden reflektieren, oder bei Cloud-Anbietern, die in Europa eine Marktnische für sich aufbauen, indem sie zusichern, dass die Daten in Europa oder einzelnen Ländern bleiben. Ich kann mir vorstellen, dass europäische Anbieter künftig einen Vorteil gegenüber amerikanischen haben, weil hier der US-amerikanische Staat nicht ohne Weiteres Zugriff auf Daten hat. Das gilt aber nur für Unternehmen, die Dienstleistungen anbieten, die nicht auf der Auswertung von Daten beruhen. Sobald Daten und ihre Auswertung selbst der Geschäftszweck sind, sehe ich überhaupt keine ökonomischen Anreize.

? Wenn wir uns den NSA-Überwachungsskandal anschauen: Brauchen wir neue Kontrollinstanzen gegenüber dem Staat? Oder gewöhnen wir uns einfach daran, dass wir überwacht werden?

JH: Verschlüsselung ist zurzeit die beste Selbstverteidigung. Generell müssen die Geheimdienste aber stärkeren parlamentarischen Kontrollen unterzogen werden, auch wenn das gegenwärtig nicht sehr vielversprechend aussieht. Es gibt im Augenblick keinen ausreichenden politischen Willen, Spionage auf nationaler und internationaler Ebene zu regulieren.

? Was müsste passieren, damit dieser Wille entsteht?

JH: Die Bürger müssen sich stärker wehren. Enthüllungen wie die von Snowden müssen sich in Wahlergebnissen niederschlagen – dann wird sich etwas ändern. Das ist aber im Moment nicht absehbar.

? Woran liegt das? Sind die Leute überfordert? Sind sie zu technikfeindlich?

JH: Die Auswirkungen der totalen Überwachung sind noch nicht im Erfahrungshorizont der Bürger angekommen. Erst wenn der Nachbar den Hypothekenkredit nicht bekommt, das Kind keinen Ausbildungsplatz erhält oder nicht in den Staatsdienst übernommen wird, wird etwas passieren. Das wird aber noch eine ganze Weile dauern.

Vielleicht macht das folgende Analogie deutlich: Man ist erst willens, in ein besseres Schloss zu investieren und die eigene Wohnung stärker gegen Einbrecher zu schützen, wenn im eigenen Haus mehrfach eingebrochen worden ist. Solange das abstrakt irgendwo in der Welt passiert, macht man das nicht.

Wir haben die konkreten Auswirkungen dieser Art der Überwachung in unserem persönlichen Erfahrungsraum und dem unserer Bekannten und Freunde noch nicht zu spüren bekommen. Es muss häufiger vorkommen, dass Leute wie du und ich daran gehindert werden, ein Flugzeug zu besteigen. Dann wird klar, das sind keine Einzelfälle, sondern strukturrelevante Ergebnisse von Überwachungstechniken.

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.

> **„Wir hatten in den vergangenen 15 Jahren nie eine richtige, kenntnisreiche, gesamtgesellschaftliche Debatte darüber, was im Netz passiert. Eine Diskussion, die den Namen verdient, könnte auch klügere rechtliche Regelungen anregen. Denn ja: Es braucht klare Regeln statt gefühlter, irgendwie tolerierter ‚Hinterzimmervereinbarungen', bei denen dann Unternehmen im Nachteil sind, die sich zum Beispiel beim Thema Transparenz oder Datenschutz wegweisend und verantwortungsbewusst verhalten."**
>
> **Stefan Plöchinger,** Chefredakteur Süddeutsche.de und Geschäftsführender Redakteur Online der Süddeutschen Zeitung, Diskussion, Öffentliche Veranstaltung München, 04.07.2013

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 behaupten.[25] Als grenzenloser Handlungsraum für die ganze Gesellschaft übertrifft das Internet in seiner Komplexität jedoch bisherige transnationale Regelungsmaterien (wie zum Beispiel internationales Seerecht) erheblich.

> **„Facebook ist ein supranationaler Akteur, der sich mit seiner Plattform über alle Nationalstaaten legt. Der Wert dieses Konzepts liegt darin, dass über Landesgrenzen hinweg problemlos und einfach kommuniziert werden kann. Aus ökonomischer und kommunikativer Perspektive ist auch sinnvoll, dass alles von einem Service ausgeht und es keine nationalstaatlichen Regelungen gibt, aber dies führt zu einem Spannungsfeld mit den nationalen Rechtsordnungen."**
>
> **Prof. Dr. Wolfgang Schulz,** Direktor des Hans-Bredow-Instituts für Medienforschung und des Alexander von Humboldt Instituts für Internet und Gesellschaft, Keynote, Öffentliche Veranstaltung Hamburg, 07.11.2013

> **„Dem Staat fehlt die Power, das zu regeln – wir haben keine technologische Souveränität in Bezug auf die digitalen Infrastrukturen."**
>
> **Dr. Ralf Kleindiek,** Staatssekretär im Bundesministerium für Familie, Senioren, Frauen und Jugend (bis Januar 2014 Staatsrat der Behörde für Justiz und Gleichstellung der Freien und Hansestadt Hamburg), Begrüßung, Öffentliche Veranstaltung Hamburg, 07.11.2013

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 Maße 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 Nor-

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

men können hier Vorteile haben und Gesetze unter Umständen als Steuerungsform ersetzen oder ergänzen. Da sie von der Gemeinschaft selbst kontrolliert werden, sind staatlich-formalisierte Durchsetzungsmechanismen nicht erforderlich.

> **„Ich bin grundsätzlich der Auffassung, der Staat sollte nicht in alle Lebensbereiche hineinregulieren. Nun ist aber die Frage, was passieren muss, wenn – wie jetzt mit der Digitalisierung – revolutionsartige gesellschaftliche Umbrüche stattfinden. Ich glaube, dass man hier im digitalen Bereich, bei dem man oft von einer digitalen Revolution spricht, um Regulierung durch Gesetzgebung überhaupt nicht herumkommt. Das Verhalten von bestimmten Plattformen in Bezug auf das Sammeln von Daten lässt mich stark daran zweifeln, ob diese Unternehmen überhaupt einen Hauch von Interesse an der Wahrung der Grund- und Menschenrechte haben. Die pauschalen Forderungen nach Selbstverpflichtungen greifen deshalb zu kurz, und gesetzliche Normierungen sind daher zwingend erforderlich."**
>
> **Dr. Konstantin von Notz MdB,** Stellvertretender Fraktionsvorsitzender Bündnis 90/Die Grünen, Konsultation

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

Soziale Normen

Soziale Normen sind gesellschaftliche Verhaltensregeln. 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 zum Beispiel ein Verhaltenskodex für die Nutzer von Internet-Foren.

> **„Auch im Netz gibt es soziale Normen bzw. haben die Regeln der analogen Welt weiter Bestand. Auf einer tieferen Ebene bilden sich aber auch spezifische Adäquanz-Normen und Prozedural-Normen aus, wie man beispielsweise eine Plattform angemessen bedient, um zu zeigen, dass man dazugehört. Ein gutes Beispiel dafür ist Twitter. Es hat sich die Erwartung oder die Regel herausgebildet, dass man Twitter für eine bestimmte Form der Kommunikation nutzen kann. Man schreibt zum Beispiel kein Kondolenzschreiben an die Oma, selbst wenn diese auf Twitter aktiv ist. Es haben sich also bestimmte Regeln und Normen entwickelt, wie man Twitter richtig anwendet. Diese Regeln sind aber allgemeineren Normen wie der Authentizität oder Privatsphäre untergeordnet."**
>
> **Dr. Jan-Hinrik Schmidt,** wissenschaftlicher Referent für digitale interaktive Medien und politische Kommunikation am Hans-Bredow-Institut für Medienforschung, Interview

Soziale Normen können in Bezug auf ihre Legitimität und Effizienz gegenüber anderen Mitteln zur Zuweisung von Verantwortung, insbesondere 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 Internet-Nutzer* wird es nicht geben, da die viel beschworene „Netz-Gemeinde" (Internet-Community) nicht existiert. Sie ist so vielfältig und amorph wie die Gesellschaft an sich. Soziologen (zum Beispiel 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 hoch spezialisierte Mikrogesellschaften 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.

Sind Werte und soziale Normen 1:1 in die digitale Welt transferierbar?

Collaborative Governance und „regulierte Selbstregulierung"

Ebenso wie Verantwortung in der Gesellschaft häufig über soziale Normen zugewiesen werden kann, können Wirtschaftsgruppen durch *Codes of Conduct*[26] 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, zum Beispiel 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).[27] 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, zum Beispiel um staatliche Regulierung zu vermeiden.

> **„Selbstregulierung ist immer da erfolgreich, wo wir ein regulatorisches Bedürfnis auf der einen Seite haben und auf der anderen Seite ein hohes Maß an Fachwissen brauchen."**
>
> **Oliver Süme,** Rechtsanwalt und Stellvertretender Vorstandsvorsitzender des Verbands der deutschen Internetwirtschaft e.V. eco, Konsultation

Das Konzept der Co-Regulierung oder regulierten Selbstregulierung versucht dieses Manko zu verhin-

26 Ein „Code of Conduct" ist ein Regelsatz, in dem Verhaltensregeln niedergelegt sind, die von einer Institution oder einem spezifischen Personenkreis befolgt werden sollen.

27 Dies hat sich in der Vergangenheit schon verschiedentlich gezeigt, unter anderem 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.). Auch der in Deutschland gestartete Versuch, einen Kodex zur Selbstregulierung für soziale Netzwerke auf den Weg zu bringen, ist gescheitert (siehe www.telemedicus.info/article/2569-Kodex-zur-Selbstregulierung-fuer-soziale-Netzwerke-gescheitert.html).

dern, indem externe Druckmittel implementiert werden, wie zum Beispiel 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).

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.

> **„Der Code beinhaltet handlungsleitende Aspekte der Kommunikation, die durch Hardware und Software entstehen. Es ist der Handlungsrahmen, der Ihnen entgegentritt, wenn Sie beispielsweise eine Plattform nutzen."**
>
> **Prof. Dr. Wolfgang Schulz,** Direktor des Hans-Bredow-Instituts für Medienforschung und des Alexander von Humboldt Instituts für Internet und Gesellschaft, Keynote, Öffentliche Veranstaltung Hamburg, 07.11.2013

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, Netz-Betreibern, Zugangsprovidern, Plattform- und Suchmaschinenanbietern und anderen Gatekeepern, kommt daher große Verantwortung zu. Zum einen tragen sie Verantwortung dafür, Handlungsoptionen zu eröffnen oder zu verhindern, was auf eine Mitverantwortung für die Internet-Nutzer hinausläuft. Hiermit verbunden ist die Verantwortung für die Nutzungsfreiheit. Würde zum Beispiel die Angabe personenbezogener Information bei sozialen Netzwerken technisch unterbunden, würde den Nutzern viel Eigenverantwortung abgenommen. Allerdings würde so auch die Nutzungsfreiheit massiv eingeschränkt.

> **„Datenschutzerklärungen müssen eine Balance herstellen zwischen Ausführlichkeit und Detailtiefe auf der einen und Verständlichkeit und Zugänglichkeit für den Nutzer auf der anderen Seite. Wir sind davon überzeugt, dass uns das bei Einführung unserer aktuellen Datenschutzerklärung gelungen ist."**
>
> **Sabine Frank,** Leiterin Regulierung, Jugendschutz und Medienkompetenz Google Deutschland, Diskussion, Öffentliche Veranstaltung Hamburg, 07.11.2013

An diesem Beispiel zeigt sich ein weiteres Spannungsfeld. Wirtschaftliche Akteure tragen auch wirtschaftliche Verantwortung, zum Beispiel 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.

> **„Von Hause aus ist die Netz-Architektur frei. Ab wann war sie das nicht mehr? Wann ist sie umgebaut worden und von wem? Nach welchen Regeln ist das passiert? Wir haben hier ein Verständigungsproblem: Die ‚Techniker' fragen die Sozialwissenschaftler, wie die Infrastruktur weiterentwickelt werden soll, aber die Sozialwissenschaftler verstehen die technischen Fragestellungen nicht."**
>
> **Dr. Verena Metze-Mangold,** Sozialwissenschaftlerin und Vizepräsidentin der Deutschen UNESCO-Kommission, Interview

Angesichts der Macht des Codes wird es meist geboten erscheinen, auf die Architekten des jeweiligen Angebots regulierend einzuwirken. Die Cyberpaternalisten weisen die Verantwortung hierfür dem de-

mokratisch 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 könnte.[28]

2.6 Zwischenfazit: Andere Rahmenbedingungen im Netz als in der gegenständlichen Welt

Die Entstehung, Verteilung und Zuweisung von Verantwortung im Internet unterliegt in vielerlei Hinsicht anderen Umständen und Rahmenbedingungen als in der gegenständlichen Welt. Daher ist es wichtig, eine Systematik für diesen Themenkreis zu entwickeln und die Frage zu beantworten, ob und wie sie in einem Digitalen Kodex umgesetzt werden kann.

Der Verantwortungsbegriff ist in seiner Globalität schwer zu handhaben. Die Fragen, *wer* Verantwortung *wofür* und *auf welche Weise* übernehmen sollte, müssen eingegrenzt werden, um eine Vorstellung dafür zu entwickeln, ob ein Digitaler Kodex eine Möglichkeit sein kann, bestehende Konflikte zu lösen.

28 Siehe „Raus aus der digitalen Unmündigkeit", www.golem.de/news/code-raus-aus-der-digitalen-unmuendigkeit-1305-99125.html.

3. Ein Kodex im Kontext von Plattformen

Das Netz hat viele Facetten. Es besteht aus zahllosen, sehr unterschiedlich organisierten Diensten mit variierenden Akteursgruppen und Machtstrukturen. Plattformen bilden eine wichtige Gattung in diesem komplexen System. Je nachdem, wie man den Begriff der Plattformen definiert, ist auch diese Gattung äußerst divers. Es ist hilfreich, zunächst von einem weiten Plattform-Begriff auszugehen, um die Untersuchung nicht unnötig einzuschränken.

Als Plattformen werden alle mit dem Internet in Verbindung stehenden technischen Infrastrukturen verstanden, die grundsätzlich für eine Benutzung (zum Beispiel Zugriff, Einsichtnahme und Interaktion) auch durch andere als den Betreiber geeignet oder sogar vorgesehen sind. Soziale Medien und kollaborative Projekte werden damit genauso als Plattformen verstanden wie sonstige serverbasierte Infrastrukturen jeder Art (zum Beispiel *Streaming-Plattformen*[29], *Blog-Dienste*[30], Foto-Communitys und sonstige Angebote rund um *„User Generated Content"*[31]), Cloud-Dienste sowie vergleichbare Angebote – unabhängig davon, ob es sich um Strukturen handelt, die rundfunkähnlich *(„one to many")* oder interaktiv *(„many to many")* aufgezogen sind.[32]

Die große Bandbreite denkbarer Konstellationen führt zu dem Schluss, dass es *das* Konzept zur Zuordnung von Verantwortung im Netz ebenso wenig geben kann wie *das* Zuordnungskonzept für Plattformen. Gleichermaßen ist *der* Digitale Kodex als alternatives Regelungsmodell für *das* Netz oder *die* Plattform nicht denkbar.

Fragen wie: „Braucht Deutschland einen Digitalen Kodex (für Plattformen)?", oder: „Ist ein Digitaler Kodex als alternatives Regelungskonzept geeignet, um Verhalten im Netz (auf Plattformen) zu steuern und Verantwortung effizient zuzuordnen?", provozieren daher zwangsläufig drei grundlegende Gegenfragen:

- Auf welche Bereiche des Netzes, welche Art von Plattformen, soll sich der Digitale Kodex beziehen (sachlicher Anwendungsbereich)?
- Auf welche Problematik, auf welches Verhalten soll sich der Digitale Kodex beziehen (inhaltlicher Anwendungsbereich)?
- Was wird unter einem Digitalen Kodex verstanden, an wen kann er sich richten, und wie kommt er zustande (Konzeption)?

Auf diese drei Gegenfragen wird im Folgenden näher eingegangen. Um sich der Frage zu nähern, auf welche Arten von Plattformen sich ein Digitaler Kodex beziehen könnte, werden zunächst Ordnungsprinzipien beleuchtet, nach denen diese variantenreiche Gattung von Online-Systemen typologisiert werden kann. Im Ergebnis wird sich zeigen, dass sich – abstrakt betrachtet – auf Aushandlungsprozessen basierende alternative Regelungskonzepte für manche Arten von Plattformen im Zweifel besser eignen werden als für andere. Gleiches gilt für die hierin zu behandelnden Regelungssachverhalte und -adressaten. Ob ein alternatives Regelungsmodell funktionieren kann und wie es konzipiert sein müsste, um Relevanz und Wirkmacht zu entfalten, hängt da-

29 „Streaming" steht für ein Datenübertragungsverfahren, bei dem die Daten bereits während der Übertragung angesehen oder angehört werden können und nicht erst nach der vollständigen Übertragung. Des Weiteren werden die Daten nicht auf dem jeweils genutzten Endgerät gespeichert.

30 „Blog" ist die Abkürzung von „Weblog", einem öffentlichen digitalen Tagebuch.

31 „User Generated Content" steht für Inhalte, die von Nutzern erstellt werden (im Gegensatz zu Inhalten von Plattform-Betreibern).

32 Siehe zum Begriff und zu dessen weiterer Erläuterung das im Projekt erstellte Themenpapier (Weitzmann 2013).

von ab, auf welches Verhalten sich die Regeln beziehen und an wen sie sich richten.

Die Antwort auf die letztlich für Erfolg oder Misserfolg entscheidende Frage, wie ein Digitaler Kodex konzipiert sein müsste, hängt davon ab, für welche Dienstart, Themen und Adressaten er gelten würde. Dies ergibt eine Vielzahl konstellationsbezogen unterschiedlicher Konzepte, die man unter den Begriff „Digitaler Kodex" subsumieren könnte. Die Herausforderung liegt schließlich darin, eines oder mehrere Konzepte zu entwerfen und deren Funktionsfähigkeit in einem Modellversuch anhand einer oder mehrerer ausgewählter Beispielkonstellationen zu untersuchen.

3.1 Sachlicher Anwendungsbereich: Auf welche Bereiche des Netzes könnte sich ein Digitaler Kodex beziehen?

Typologie der Plattformen im Internet

Plattformen können offene oder geschlossene Netze sein. Sie können zentral (durch einen Anbieter) oder dezentral organisiert sein. Je nachdem, um welche Art Plattform es sich handelt, sind im Zweifel unterschiedliche Ansätze zur Steuerung von Verhalten und Zuordnung von Verantwortung zu verfolgen.

Wer ist das Netz? Die dominierenden Plattformen? Wer sind die Plattformen?

Vor diesem Hintergrund stellt sich die Frage, ob und nach welchen Kriterien Plattformen typologisiert werden können, damit die für Regulierungsfragen[33] relevanten Unterschiede deutlich werden.

Unterscheidung nach Anbieter und Zielgruppe

Plattformen können zunächst nach Anbietern und Zielgruppen unterschieden werden. Plattformen können von Unternehmen angeboten und an Privatpersonen gerichtet sein (B2C). Manche Dienste werden von Unternehmen anderen Unternehmen angeboten (B2B). Schließlich existieren auch Plattformen, die von Privatpersonen für die Nutzung durch andere Privatpersonen bereitgestellt werden (wie verteilte Netzwerke, siehe unten).

Wer eine Plattform anbietet und wer sie nutzen kann, ist für Regulierungsfragen von erheblicher Bedeutung. Dieses Kriterium ist entscheidend für die Frage nach den agierenden Akteuren, deren Interessen und Rollen und damit unter anderem für mögliche Adressaten einer durch einen Kodex zu regelnden Verantwortungsverteilung.

Unterscheidung nach Interaktionsmöglichkeiten

Ob eine Plattform Interaktion ermöglicht oder nicht, ist wiederum bedeutsam für das Verhalten der Nutzer. Rein statische Webauftritte, bei denen beispielsweise Unternehmen oder Personen präsentiert werden, werden nicht im Fokus eines Digitalen Kodex stehen, da sich die komplexen Probleme, die ein solcher Kodex adressieren soll, hier zumeist nicht stellen. Im Übrigen sind sie in Zeiten des „Web 2.0" von zunehmend geringer Relevanz.

Unterscheidung nach Netzwerkstruktur: zentrale, dezentrale und verteilte Netzwerke

Plattformen sind im Prinzip Netze im Netz. Mit anderen Worten bilden sie offene oder in sich geschlossene Kommunikationsnetzwerke, die wiederum in größere Netzwerke eingebunden sein können. Die Struktur von Kommunikationsnetzwerken kann in drei Gattungen unterteilt werden: zentrale, dezentrale und verteilte Netzwerke *(distributed networks)*. Die drei Formen unterscheiden sich vor allem dadurch, ob sie von einem oder mehreren Anbietern zentral gesteuert werden, über deren Server der Datenverkehr abgewickelt wird (zentrale und dezentrale Netzwerke). Sie basieren auf dem Client-Server-Prinzip. In verteilten Netzwerken vernetzen sich die Nutzer – ohne Zwischenschaltung eines Anbieters – direkt miteinander. Im Unterschied zum Cli-

33 Der Begriff der Regulierung wird hier im denkbar weitesten Sinn verstanden. Gemeint sind nicht nur staatliche Interventionen in Form von Gesetzen oder anderen Normsystemen. Gemeint sind ebenfalls – als ein Beispiel – soziale Normen als eine – häufig unkodifizierte – Form der Selbstregulierung.

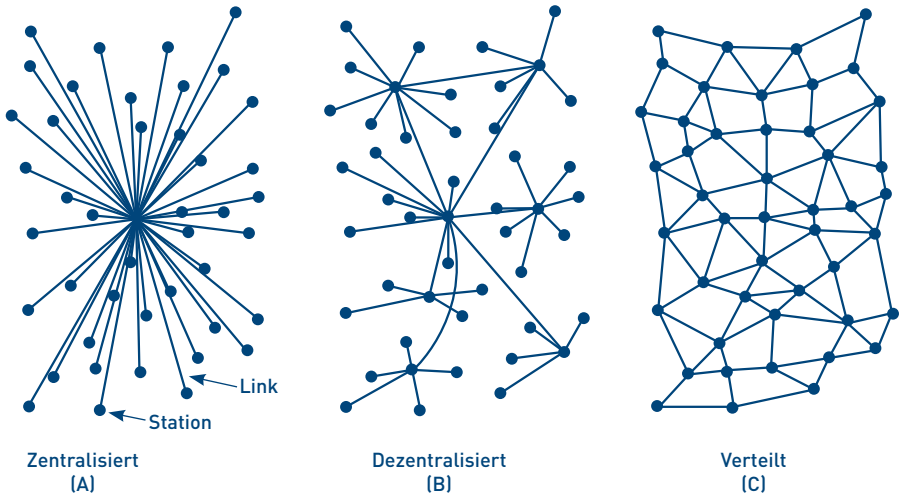
ent-Server-Modell spricht man hier vom Peer-to-Peer-Prinzip (P2P).

Die nachstehende Grafik verdeutlicht die unterschiedlichen Konzepte von Netzwerk-Architekturen: In zentralisierten Kommunikationsnetzwerken erfolgt jegliche Datenübertragung über einen zentralen Anbieter. Bei dezentralisierten Netzwerken sind mehrere Anbieter beteiligt. In verteilten Netzwerken vernetzen sich die Nutzercomputer dagegen direkt miteinander, ohne dass es eines oder mehrerer zentraler Anbieter und deren Infrastruktur bedürfte.[34] Diese unterschiedlichen Konzepte finden sich auch bei den durch Plattformen gebildeten Netzwerken.

Zentrale Plattformen

Viele Plattformen bilden ein zentrales, in sich geschlossenes Netzwerk. In sozialen Netzwerken, auf Video-, Verkaufs- oder Versteigerungsplattformen, bei Cloud-Diensten und so weiter verläuft in der Regel sämtlicher Datenverkehr über die Infrastruktur eines einzelnen Anbieters. Üblicherweise sind zentrale Plattformen nicht Teil eines übergeordneten dezentralen Netzwerks. Der Grund hierfür sind fehlende Interkonnektivität und Datenportabilität. Gerade soziale Netzwerke wie Facebook, Google+ oder LinkedIn bieten keine Möglichkeit, direkt mit den Nutzern anderer Netzwerke zu kommunizieren oder die in einem Netzwerk generierten Daten, Inhalte und Kontakte in ein anderes Netzwerk zu exportieren.

Zentrale Plattformen gewinnen im Internet immer mehr an Bedeutung. Medienökonomische Hintergründe – wie Netzwerk- und Skaleneffekte – führen zunehmend zu einer Zentralisierung des Netzes und fördern die Entstehung von in sich geschlossenen Netzen im Netz (Deterding 2010, 24 ff.). Dieser Trend zeigt sich besonders deutlich an der Strategie von Apple. Das Unternehmen bietet vom Endgerät über die Applikationen bis zur Infrastruktur – wie Cloud-Speicherdienste – alles aus einer Hand an. Angesichts der Gefahren von Rezentralisierungstendenzen befürworten Wissenschaftler und Internet-Aktivisten die Bildung offener Netzwerke als Alternative zu den bestehenden, anbietergeführten Systemen. Beispielsweise sollen *distribu-*



Konzepte von Netzwerk-Architekturen (Quelle: Baran 1964, 4)

34 Diese Aussage bezieht sich auf die Organisation der Plattform, nicht des Mediums (Internet), auf dem die Plattform läuft, oder auf die physische Netz-Infrastruktur. Es liegt auf der Hand, dass die physische Netz-Infrastruktur bei jedem Datenverkehr im Internet in Anspruch genommen wird und damit stets auch privatwirtschaftliche Anbieter involviert sind. Bezieht man diesen Faktor mit ein (wie bei Deterding 2010, 12 ff.), ist das „freie Internet" eine Illusion. Im hier betrachteten Zusammenhang ist diese Überlegung jedoch nicht von Belang, da es hier um das Verhalten aktiv Handelnder und um bestimmte Bereiche des Netzes (Plattformen) geht.

ted social networks bzw. *federated social networks* wie Diaspora gefördert werden, in denen die Nutzer mehr Macht über ihre Internet-Aktivitäten haben als in „proprietären" Systemen (Esguerra 2011).

> **„Der Nutzer sollte in die Lage versetzt werden, informierte Entscheidungen hinsichtlich der Freigabe von personenbezogenen Daten und deren Verwendung zu treffen. Die Informiertheit ist Grundlage für die Idee der informationellen Selbstbestimmung. Auf proprietären Plattformen, auf denen die Datennutzung konzeptionelle und monetäre Voraussetzung ist, wären direkt sichtbare und verständliche Tutorials sinnvoll, in denen erklärt wird, was wann und wie passiert. Grundsätzlich braucht ein modernes Datenschutzrecht aber auch andere Möglichkeiten, einen technischen Datenschutz zu realisieren, als nur die Einwilligung durch den Nutzer. So ist das Modell der Pseudonymisierung in Deutschland erfolgreich etabliert und in der Lage, Daten ohne einen unmittelbaren Personenbezug zu nutzen."**
>
> **Thomas Schauf,** Head of European & International Affairs, Bundesverband Digitale Wirtschaft (BVDW) e.V., Konsultation

> **„Google schafft das Superprofil. Alles wird verknüpft: E-Mail, YouTube, Kalender und so weiter. Am Ende hat Google alle Daten und kann mit ihnen arbeiten."**
>
> **Ole Reißmann,** Redakteur bei Spiegel Online im Ressort Netzwelt, Diskussion, Öffentliche Veranstaltung Hamburg, 07.11.2013

Dezentrale Netzwerke

Andere Plattformen sind offen und damit Teil von dezentralen Netzwerken. Solche finden sich zum Beispiel bei E-Mail oder IRC (Internet Relay Chat). Sie zeichnen sich dadurch aus, dass eine Mehrzahl von Anbietern in einen einzigen Kommunikationsvorgang involviert sein kann – und regelmäßig sein wird. Dies wird durch Interkonnektivität ermöglicht. Wie im Telefonnetz können Nutzer unterschiedlicher Anbieter und Serverbetreiber per IRC oder per E-Mail miteinander kommunizieren.

Verteilte Netzwerke

Verteilte Netzwerke – auch *distributed networks* genannt – kommen gänzlich ohne zentrale Anbieter oder Infrastrukturen aus. Die Datenkommunikation erfolgt ohne Zwischenschaltung von zentralen Servern. Ein Beispiel für solche Netzwerke sind vor allem dezentrale (Peer-to-Peer-)Filesharing-Systeme.

Aus Sicht der Ausfallsicherheit, Redundanz oder auch des Schutzes von Freiheitsrechten haben verteilte Netzwerke große Vorteile. Sie werden nicht von dominanten Akteuren, die vornehmlich eigene – vor allem wirtschaftliche – Interessen verfolgen, gesteuert. Der Ausfall eines Teilnehmers beeinträchtigt nicht ihre Funktionsfähigkeit. Daten werden in einer Vielzahl von unabhängigen Instanzen gespeichert und vorgehalten.

> **„Dezentrale Plattformen sind sehr interessant, weil die Nutzer dort ein ganz anderes Verhalten an den Tag legen und viel mehr in Grauzonen unterwegs sind. Hier findet Kommunikation eben ohne die zentrale Regelung durch einen Anbieter statt, der unter Umständen Material entfernt und das Verhalten durch den Code steuert. Gerade diese Problematik hat man bei den dezentralen Plattformen nicht."**
>
> **Nico Lumma,** freier Autor und Berater, 2. Expertenworkshop, 10.09.2013

Die Kehrseite dieser Eigenschaften ist, dass verteilte Netzwerke besonders schwer zu regulieren

35 Zu den Theorien, die sich mit Regulierung durch die Gestaltung des Codes beschäftigen, siehe Kreutzer 2013.

sind. Da ein Betreiber als zentraler Akteur als Regelungsadressat fehlt, ist es gerade bei massenhaftem Fehlverhalten kaum möglich, Normen effizient durchzusetzen. Auf solche Netzwerke haben – neben den Nutzern – lediglich die Entwickler der Protokolle, Standards oder Anwendungen Einfluss, die bei der jeweiligen Kommunikation verwendet werden. Sie können zwar das Verhalten der Nutzer nicht unmittelbar beeinflussen, über die Ausgestaltung der Technologie (des *Codes*) jedoch mehr oder weniger genau definieren, welches Verhalten überhaupt möglich ist und welches nicht.[35] Dies zeigt sich zum Beispiel, wenn man die Maßnahmen gegen Urheberrechtsverletzungen auf zentralen Plattformen mit denen in dezentralen Filesharing-Netzen vergleicht. Will ein Rechteinhaber diesem Massenphänomen mit rechtlichen Mitteln begegnen, bleibt bei einem P2P-Netzwerk wie Bittorrent nichts anderes übrig, als die Filesharer mit Massenabmahnungen zu überziehen. Bei Rechtsverletzungen auf Musikplattformen dagegen richten die Rechteinhaber rechtliche Maßnahmen nicht gegen die Nutzer, sondern den Anbieter. Eine schwierige, aber zumindest zu bewältigende Aufgabe, wie sich an den Vereinbarungen zwischen Google/YouTube und Tausenden von Musiklabels und Verwertungsgesellschaften auf der ganzen Welt zeigt.

> **„Das übergeordnete Ziel des Urheberrechts ist die Würdigung des Urhebers in sozialer und in ökonomischer Hinsicht."**
>
> **Prof. Dr. Rüdiger Grimm,** Professor für IT-Riskmanagement im Fachbereich Informatik an der Universität in Koblenz, 2. Expertenworkshop, 10.09.2013

> **„Die technische Ausgestaltung und das Geschäftsmodell der Plattformen (zum Beispiel, dass möglichst viele Inhalte veröffentlicht werden sollen) lädt allerdings dazu ein, Inhalte einzustellen mit der Folge, dass hierdurch auch Rechtsverletzungen seitens der Nutzer erfolgen können."**
>
> **Lina Ehrig,** Leiterin des Teams Digitales und Medien, Verbraucherzentrale Bundesverband, Konsultation

Die Differenzierung in zentrale, dezentrale und verteilte Dienstarten erleichtert es, verschiedene Kernaspekte der Frage, ob ein Digitaler Kodex sinnvoll und zielführend wäre, gezielter zu untersuchen. Dies gilt vor allem für die Identifizierung der Akteure und deren Handlungsmacht, Konzepte zur Zuschreibung von Verantwortung und ebenso für die Frage, welche Regulierungsformen im jeweiligen Bereich effizienter oder weniger effizient sind. Aus Sicht der Regulierung ist die zunehmende Zentralisierung des Netzes zum Beispiel durch private Firmen wie Facebook, Apple oder Google Fluch und Segen zugleich. Einerseits fördert sie regulatorisch unerwünschte Effekte, wie Monopolisierung, Zensur und übermäßigen Einfluss einzelner Akteure auf das Sozialverhalten der Nutzer. Andererseits erleichtert sie wiederum die Regulierung, da es zentrale Akteure gibt, an die Regulierungsmaßnahmen beziehungsweise Regulierungsanforderungen gerichtet werden können.

Unterscheidung nach der Primärfunktion der Plattform

Plattformen sind in ihrer Art, Ausrichtung und Ausgestaltung so unterschiedlich, dass es sinnvoll erscheint, sie inhaltsbezogenen Kategorien zuzuteilen. Fraglich ist hierbei, welche Kriterien sich zur Differenzierung im Hinblick auf eine aussagekräftige Strukturierung eignen.

> **„Ganze Generationen sind derzeit ‚always online'. Plattformen spielen dabei eine zentrale Rolle. Sie bieten Platz für vieles: Kommunikation, öffentliche Debatten, gesellschaftliche Bewegungen ebenso wie für jegliche Trivialität des Alltags."**
>
> **Matthias Kammer,** Direktor des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI), Begrüßung, Öffentliche Veranstaltung Hamburg, 07.11.2013

Orientiert man sich beispielsweise an den technischen Funktionen der jeweiligen Dienste als Unterscheidungskriterium, stößt man sehr schnell an Grenzen. Auf modernen Plattformen werden zumeist unterschiedlichste Funktionen kombiniert. Amazon

ist beispielsweise vorrangig eine Verkaufsplattform. Mit ihrem Bewertungs- und Kommentierungssystem bietet sie jedoch auch die Möglichkeit, sich auszutauschen und zu diskutieren. Allein anhand der technischen Funktionen lässt sich daher keine zuverlässige Kategorisierung vornehmen.

Naheliegender erscheint es daher, danach zu unterscheiden, wozu eine Plattform vorrangig dient, also nach der Primärfunktion. Eine Klassifizierung nach diesem Kriterium könnte zum Beispiel so aussehen:

A) Plattformen, die vor allem dem sozialen Austausch in der Öffentlichkeit oder in Teilöffentlichkeiten dienen (Kommunikationsplattformen). Beispiele: „Marktplätze der Meinungen" wie Social-Media-Plattformen, Meinungs-Foren oder IRC-Plattformen.

B) Plattformen, die der nicht öffentlichen Individual- oder (Klein-)Gruppenkommunikation dienen. Beispiele: IP-Telefonie-Dienste wie Skype, Messaging-Dienste, E-Mail-Dienste, Conferencing-Systeme.

C) Plattformen, die dem Handel und Verkauf von Sachen oder der kommerziellen Zugänglichmachung immaterieller Inhalte dienen. Beispiele: Auktions-Plattformen, Online-Shops, App-Stores, Download- oder Streaming-Dienste.

D) Plattformen zum Austausch und zur Speicherung von Daten. Beispiele: Infrastructure-as-a-Service-Dienste wie Cloud-Speicher-Services, Filesharing-Netze, Sharehoster.

E) Plattformen für Online-Computing. Beispiele: Cloud-Application- bzw. Software-as-a-Service-Dienste wie Google Docs, Microsoft Azure.

F) Plattformen zur Nachrichten- und Informationsvermittlung. Beispiele: Blogs, Verlagswebseiten, Wikipedia.

G) Informationsmehrwertdienste. Beispiele: Suchmaschinen, Nachrichten- und sonstige Informationsaggregatoren.

H) User-Generated-Content-Plattformen, die vorrangig zur Veröffentlichung von kreativen Inhalten durch die Nutzer dienen. Beispiele: Video- und Fotoplattformen wie YouTube, Instagram oder Flickr.

I) Games-Plattformen. Beispiel: Steam.

> **„Die Kommunikationsordnung geht immer vor private Interessen. Die freie öffentliche Kommunikation ist Grundlage einer demokratischen Meinungsbildung. Ich warne davor zu sagen, das Internet sei ein privater Bereich und sei deshalb auch so wie andere private Bereiche zu behandeln: Es ist eben kein privater Bereich, sondern hier findet Öffentlichkeit statt."**
>
> **Dr. Hans Hege,** Direktor der Medienanstalt Berlin-Brandenburg (mabb), Auftaktworkshop, 03.06.2013

Natürlich kann man in Bezug auf die Kategorienbildung und umso mehr zur Zuordnung konkreter Plattformen in die einzelnen Kategorien geteilter Meinung sein. Hierauf soll es im Detail an dieser Stelle jedoch nicht ankommen. Die Kategorisierung soll vielmehr die große Vielfalt von Internet-Plattformen aufzeigen und eine Orientierung ermöglichen. Zudem soll sie es – in Ergänzung zu den weiteren, oben beschriebenen, Typologisierungsmerkmalen – erleichtern, unter den mannigfaltigen Optionen eine Auswahl hinsichtlich eines beispielhaften Anwendungsbereichs für einen Digitalen Kodex zu treffen.

> **„In der analogen Welt gibt es öffentliche und private Räume, im Internet sind grundsätzlich alle Räume privat. Welche Konsequenzen kann man daraus ableiten?"**
>
> **Dr. Sönke E. Schulz,** wissenschaftlicher Assistent und Geschäftsführer des Lorenz-von-Stein-Instituts für Verwaltungswissenschaften, Auftaktworkshop, 03.06.2013

> **„Vernetzung und Kommunikation, Unterhaltung, Information und Werbung – das sind für mich die wichtigsten Funktionen von Plattformen."**
>
> **Moritz Nickel,** Student an der Bucerius Law School, Keynote, Öffentliche Veranstaltung Hamburg, 07.11.2013

3.2 Welche Plattform kann von einem Digitalen Kodex profitieren?

Die vorstehenden Überlegungen haben aufgezeigt, dass man Online-Plattformen nach zumindest vier Kriterien unterscheiden kann: Zielgruppe, Interaktivität, Netzwerkstruktur und Primärfunktion. Fraglich ist nun, auf welche Art Plattform man sich unter Anwendung dieser Kriterien für die Formulierung eines Digitalen Kodex fokussieren sollte.

Es stellt sich die Frage, ob ein Digitaler Kodex geeignet erscheint, das Sozialverhalten der Nutzer und das Anbieterverhalten zu steuern. Vor diesem Hintergrund liegt es nahe, bei der Wahl eines beispielhaften Anwendungsbereichs zunächst solche Dienste und Plattformen auszuschließen, die zum einen keine sozialen Funktionen bieten oder nicht interaktiv sind und die sich zum anderen nur an Unternehmen richten.

Unter den verbleibenden Optionen bietet es sich an, angesichts der stetig steigenden Bedeutung und damit Repräsentativität der hier auftretenden Problemlagen, sich auf zentrale Plattformen zu fokussieren. Gleichzeitig zentrale Netzwerke und verteilte Netzwerke auf die Frage nach dem Sinn und Zweck sowie der Umsetzung eines Digitalen Kodex hin zu untersuchen, würde mehrere Untersuchungsstränge erfordern. Dies gilt auch und vor allem deshalb, da die Akteursstruktur jeweils sehr unterschiedlich ist, was etwa eine einheitliche Beurteilung unmöglich macht, wer Adressat eines solchen Kodex sein könnte.

Das gleiche Problem entsteht, wenn man versucht, gleichzeitig zentrale und dezentrale Netzwerkstrukturen in den Blick zu nehmen. Auch hier unterscheidet sich die Akteursstruktur wesentlich, sodass kaum einheitlich beurteilt werden kann, wo eine etwaige Regulierung ansetzen müsste, wer Verantwortung tragen soll, wie Regeln implementiert oder durchgesetzt werden können. All diese Fragen hängen elementar davon ab, wer Handlungsmacht hat und wie sie ausgeprägt ist.

Zudem erscheint es sinnvoll, sich bei der weiteren Vorgehensweise zunächst auf eine bestimmte Plattform-Kategorie zu beschränken. Schon auf den ersten Blick dürfte deutlich werden, dass manche – für Regulierungsfragen relevante – Umstände schon innerhalb der Gruppen sehr unterschiedlich sein können. So treten die Nutzer bei Social-Media-Plattformen in der Regel nicht anonym auf. Anonymität behindert einen bei solchen Diensten wichtigen Effekt: das digitale Aufrechterhalten physisch begründeter Beziehungen. Dieser Faktor spielt – anders als bei sozialen Netzwerken – bei Diskussions-Foren eine erhebliche Rolle. Hier treten die Nutzer in aller Regel nicht unter ihrem Realnamen auf, sondern unter einem Pseudonym.

> **„Ein Kritikpunkt an sozialen Netzwerken ist die Anonymität und fehlende physische Präsenz. Das führt dazu, dass die Leute irgendeinen Mist raushauen. Sozialkompetent ist das oft nicht."**
>
> **Moritz Nickel,** Student an der Bucerius Law School, Keynote, Öffentliche Veranstaltung Hamburg, 07.11.2013

Zwischen den Kategorien werden diese Unterschiede erheblich größer. Die Fragen, die sich bei Software-as-a-Service-Plattformen im Hinblick auf eine Regulierung des Nutzer- oder Anbieterverhaltens stellen, sind mit denen bei Telefondiensten oder gar Social-Media-Plattformen nicht vergleichbar. Dies gilt schon aufgrund des Umstands, dass die Handlungsmöglichkeiten der Nutzer auf diesen Plattformen völlig unterschiedlich sind.

Es liegt nahe, sich weiter auf Plattformen zum sozialen Austausch (Gruppe A) zu fokussieren. Hierfür spricht zunächst, dass sich gerade bei solchen Diensten viele der derzeit als besonders gravierend angesehenen Problemfelder kumulieren, wie zum Beispiel Datenschutz, Persönlichkeitsschutz, illegale Inhalte, Cybermobbing und so weiter. Zudem sind die Akteursstrukturen in diesem Sektor relativ einheitlich und nicht übermäßig komplex. Wie gesagt, liegt die Besonderheit solcher Systeme darin, dass jegliche Kommunikation und jeglicher Datenaustausch über die Systeme eines einzigen Anbieters erfolgen. In derart geschlossenen Netzen hat der Anbieter maximale Steuerungsmöglichkeit. Er entscheidet darüber, was die Nutzer auf seiner Plattform tun können – oder eben auch nicht. Die Steuerung des Nutzerverhaltens erfolgt einerseits über die Programmierung des – proprietären – Systems und andererseits über die Nutzungsbedingungen, also privatrechtliche Verträge (Weitzmann 2013).

> **„Plattformen verstehen sich als regelsetzende Institutionen, durch was auch immer. Die Macht ist faktisch – durch die Macht der Schnelligkeit."**
>
> **Dr. Verena Metze-Mangold,** Sozialwissenschaftlerin und Vizepräsidentin der Deutschen UNESCO-Kommission, Interview

Die hieraus sich ergebende Handlungsmacht zeigt sich an einer Analogie: Wäre im öffentlichen Raum ein derartiges Zusammenspiel von rechtlicher und technischer Regulierung möglich, wäre die Steuerungsmöglichkeit des Staates annähernd unbegrenzt. Er könnte beispielsweise Geschwindigkeitsbegrenzungen im Straßenverkehr – also die rechtliche Norm – durch Einsatz technischer Systeme durchsetzen, die jedes Fahrzeug ständig automatisch auf die jeweils zulässige Geschwindigkeit drosseln.

> **„Ist es eigentlich richtig, dass das Internet eine Veranstaltung der Privatwirtschaft ist?"**
>
> **Thorsten Schilling,** Leiter des Fachbereichs Multimedia der Bundeszentrale für politische Bildung in Bonn und Berlin (bpb), 2. Expertenworkshop, 10.09.2013

Die technischen und rechtlichen Steuerungsmöglichkeiten der Anbieter haben kaum Einschränkungen. Technisch ist fast alles möglich. Wie die Nutzungsbedingungen gestaltet werden, ist – da es sich um privatrechtliche Verträge handelt – nur sehr eingeschränkt geregelt. Das zeigt sich an einem Beispiel: Der Umstand, dass in sozialen Netzwerken massenweise Daten gesammelt und zu unterschiedlichsten Zwecken genutzt werden, ist nach geltendem Recht so lange nicht zu beanstanden, wie die Nutzer dem durch privatrechtliche Willenserklärungen zustimmen. Willigt ein – vollständig geschäftsfähiger – Nutzer ein, dass seine Daten zu Werbezwecken an andere Unternehmen weitergegeben werden, dass seine Inhalte vom Anbieter genutzt und „verkauft" werden können oder dass ausführliche Bewegungsprofile angelegt werden, handelt es sich um eine wirksame und rechtlich bindende Erklärung, auf die sich der Anbieter berufen kann.

> **„Plattformen wie Facebook – aber auch andere Anbieter – lassen sich über die AGB weitreichende Rechte einräumen und regeln umfassende Pflichten der Nutzer. So wälzen sie die Verantwortung für Rechtsverletzungen in der Regel auf den Nutzer ab."**
>
> **Lina Ehrig,** Leiterin des Teams Digitales und Medien, Verbraucherzentrale Bundesverband, Konsultation

In die hierdurch begründeten vertraglichen Anbieter-Nutzer-Verhältnisse kann das Gesetz aufgrund des Grundsatzes der Vertragsfreiheit nur sehr eingeschränkt eingreifen. Der Staat kann lediglich allgemeine Regeln aufstellen und Transparenz vorschreiben oder beschränkt geschäftsfähige oder ansonsten schutzbedürftige Nutzergruppen, wie zum Beispiel Minderjährige oder die durchaus noch große Gruppe der Nutzer, die sich im Internet nicht versiert bewegen, „vor sich selbst" schützen.

> **„Die persönlichen Daten der Nutzer werden von den Anbietern als Währung gehandelt. Die Anbieter sammeln alle Daten, um sie potenziell mit anderen Funktionen zu verknüpfen und Geld damit zu verdienen. Bei jeglicher Nutzung von anderen Diensten der analogen Welt muss die Nutzung bezahlt werden (Beispiel: Kino). Die Nutzung sozialer Netzwerke ist allerdings zunächst kostenlos. Der Nutzer zahlt allerdings mit seinen Daten – und das für immer, weil seine Daten gespeichert werden. Auf Seiten der Nutzer hat sich in Bezug auf diesen Datenraub eine Kultur des Hinnehmens eingestellt. Es ist nötig, ein Problembewusstsein bei den Nutzern zu schaffen."**
>
> **Thomas Krüger,** Präsident der Bundeszentrale für politische Bildung (bpb), Konsultation

Hinzu kommt, dass die Anbieter zentraler Plattformen – als privatwirtschaftliche Unternehmen –

nicht, oder nur sehr eingeschränkt, durch die Grundrechte gebunden sind. Anders als der Staat als „Anbieter" öffentlicher Räume sind sie rechtlich nicht verpflichtet, grundrechtlich verbriefte Freiheitsrechte zu gewährleisten. Ob sie sich darüber hinaus aus ethischen, moralischen oder kulturellen Gründen eine Art Selbstbindung auferlegen, wird in aller Regel in ihrer eigenen Entscheidung liegen. Aus solchen Faktoren jedoch eigene Prinzipien aufzustellen und umzusetzen, ist ein hochkomplexes Problem. Rosen (2013) beschreibt sehr aufschlussreich, dass die Anbieter durchaus in einem schwierigen Spannungsfeld von Gesetzen, Moralprinzipien und Traditionen operieren und sich auch bemühen, diesen Schwierigkeiten gerecht zu werden. Er macht aber auch deutlich, wie schwierig es gerade für international operierende Anbieter ist, praktikable Lösungen zu finden, etwa wenn es um den Umgang mit *hate speech* auf Social-Media-Plattformen geht.

> **„Die Haftungsregeln von Plattform-Anbietern können mit Grundrechten im Konflikt stehen. Plattform-Anbieter beschränken beispielsweise in ihren AGB das Grundrecht der Meinungsfreiheit, damit sie nicht in die Haftung genommen werden können."**
>
> **Dr. Jeanette Hofmann,** Gründungsdirektorin am Alexander von Humboldt Institut für Internet und Gesellschaft und wissenschaftliche Mitarbeiterin/Projektleiterin am Wissenschaftszentrum Berlin für Sozialforschung, Keynote, Öffentliche Veranstaltung München, 04.07.2013

Dennoch: Die besondere – und angesichts der Entwicklung des Netzes repräsentative – Akteurskonstellation bei zentralen Kommunikationsplattformen prädestiniert diese Form des Netzwerks als Testumgebung für Überlegungen zu einem Digitalen Kodex.

> **„Die Diskussion um einen Digitalen Kodex sollte meines Erachtens nicht zu abstrakt und allgemein geführt werden. Vorab ist zu klären, welche Player Zugänge kontrollieren. Dabei müssen sowohl Zugänge zu Inhalten als auch zu Infrastrukturen in den Blick genommen werden."**
>
> **Dr. Eva Flecken,** Stabsstelle Digitale Projekte, Netz- und Medienpolitik bei der Medienanstalt Berlin-Brandenburg (mabb), 2. Expertenworkshop, 10.09.2013

Zentrale Kommunikationsplattformen als Fallbeispiel zu wählen, bietet sich auch aus einem weiteren Grund an. In Bezug auf die Nutzer und die auftretenden Probleme stellen solche Netzwerke ein Abbild der großen Vielfalt und Komplexität des Internets selbst dar. Sie wenden sich an jeden Nutzer, unabhängig von Alter, Geschlecht, gesellschaftlichem Status oder kultureller Herkunft. Sie werden zumeist international angeboten und daher in verschiedensten Rechts- und Kulturräumen genutzt. Sie prägen das Kommunikations- und Sozialverhalten gerade jüngerer Generationen in besonderem Maße. Man könnte sagen: Zentrale soziale Plattformen sind als soziales Betrachtungsfeld ein Abbild des Internets an sich, allerdings realisiert in einer überschaubaren Organisationsstruktur. Diesbezüglich gewonnene Erkenntnisse werden daher in vielerlei Hinsicht auf andere Bereiche und Fragestellungen übertragbar sein.

INTERVIEW MIT DR. JAN-HINRIK SCHMIDT

Soziale Medien sind eine Art öffentlicher Raum

? Social Media bestimmt einen großen Teil der Aktivitäten im Internet. Aus Sicht der Anbieter gesehen: Wer ist der ideale Nutzer?

Jan-Hinrik Schmidt: Die Antwort müsste sich jeder Anbieter selbst geben – das hat etwas mit dem Geschäftsmodell und den Nutzungsversprechen zu tun. Wenn man sich die dominierenden Geschäftsmodelle in den sozialen Medien anguckt, hat der ideale Nutzer oder die ideale Nutzerin aktiv zu sein – möglichst oft und möglichst viel. Die Geschäftsmodelle beruhen in der Regel darauf, dass man eine aktive Nutzerschaft mit vielen kommunikativen Aktivitäten vorweisen kann. Als Nebenprodukt fallen viele Daten an. Die Nutzeraktivität kann man analysieren und dann sagen: Wir haben bestimmte Zielgruppen und Nutzersegmente, für die wir sehr zielgenau Werbung anbieten können.

? Gibt es denn auch Nutzer, die zu viel mitmachen und dadurch den Ablauf stören?

JHS: Es gibt sicherlich unterschiedliche Störungen für Social-Media-Anbieter. Auf der einen Seite diejenigen, die sich registrieren, aber dann nicht mehr wiederkommen oder das Angebot nur sporadisch nutzen: Da wird aus Sicht der Anbieter das Potenzial nicht ausgeschöpft. Auf der anderen Seite Nutzer, die zu viel mitmachen und mitbestimmen wollen. Die sich zum Beispiel dagegen wehren, dass Privatsphäre-Einstellungen geändert werden. Sie stören, weil sie Forderungen stellen, die die Anbieter letztlich nicht erfüllen wollen.

Dr. Jan-Hinrik Schmidt

ist wissenschaftlicher Referent für digitale interaktive Medien und politische Kommunikation am Hans-Bredow-Institut für Medienforschung in Hamburg. Nach seinem Studium der Soziologie an der Otto-Friedrich-Universität Bamberg und der West Virginia University (USA) promovierte er 2004 mit einer Arbeit über lokalbezogene Internet-Angebote. Von 2005 bis 2007 war er stellvertretender Leiter der Forschungsstelle „Neue Kommunikationsmedien" an der Universität Bamberg. Seine Forschungsinteressen liegen im Bereich der Online-Medien, und hier insbesondere in den Veränderungen, die soziale Medien wie Facebook, Twitter oder YouTube für Beziehungen, Informationsverhalten, politische Teilhabe und gesellschaftliche Öffentlich-

Foto: Hans-Bredow-Institut

Was können denn Nutzer im Gegenzug von einer Social-Media-Plattform erwarten?

JHS: Die meisten Nutzer, gerade bei den großen Plattformen, erwarten, dass sie ein Werkzeug bekommen, das stabil ist, funktioniert und ihre kommunikativen Zwecke erfüllt. Zum Beispiel: Ich will alte Freunde wiederfinden, ich will mich austauschen. Das bezieht sich auch auf das Technische, also die Usability. Zusätzlich ist eine Plattform aber auch ein kommunikativer und sozialer Raum, der bestimmte Strukturen vorgibt, in dem ich mich aufhalte und eine Identität entwickle. Ich verstehe mich als Nutzer von Facebook, von Twitter oder von Tumblr. Es bilden sich auf den Plattformen eigene Normen und soziale Strukturen heraus.

Es gibt Nutzer, die weiter gehende Erwartungen haben, wie Datensicherheit, Mitwirkungsmöglichkeiten im Sinne von Adaptionsmöglichkeiten, Privatsphäre-Einstellungen und so weiter – das ist aber eine Minderheit. Sie tritt vor allem dann auf, wenn die Anbieter grundlegende Änderungen vornehmen, zum Beispiel an den Privatsphäre-Einstellungen oder am Design. Das ist aber von Plattform zu Plattform und von Nutzergruppe zu Nutzergruppe unterschiedlich.

Wenn sich nur eine kleine Gruppe bewusst einmischt, ist es dann überhaupt angemessen, dass man von den Anbietern verlangt, dass sie die Wünsche der Nutzer mit einbeziehen?

JHS: Soziale Netzwerke sind in den letzten Jahren zu einer ganz zentralen Infrastruktur für Öffentlichkeit geworden, die in großem Maße die Privatsphäre und die persönlichen Bereiche der Nutzer berührt. Sie sollten nicht rein nach marktlichen Gesetzmäßigkeiten strukturiert werden. Deshalb muss man die Nutzer als Bürger verstehen und begreifen, dass sie ein Mitbestimmungsrecht haben sollten, weil es zentrale Bereiche ihres Lebens angeht.

Im Moment kollidieren zwei unterschiedliche Rollen: die Kundenrolle und die Bürgerrolle. Der Fokus liegt gegenwärtig ganz klar auf der Kundenrolle. Das Argument der Plattform-Betreiber ist: Ihr müsst diese Plattform ja nicht nutzen, ihr könnt sie jederzeit verlassen. Das übersieht, dass die Plattformen so zentral für den Alltag vieler Nutzer sind, dass es oft nicht möglich ist zu sagen: Ich nutze es nicht mehr, ich ziehe mich raus. In bestimmten Altersgruppen oder Szenen isoliert man sich, wenn man auf der Plattform nicht ist.

Wo sind die Grenzen der Öffentlichkeit? An welchem Punkt können die Anbieter von ihrem „Hausrecht" Gebrauch machen? Ist ein soziales Netzwerk eher wie eine Fußgängerzone oder wie eine Kneipe?

keit bringen. Ergebnisse seiner Forschungsarbeit sind in zahlreichen wissenschaftlichen Publikationen veröffentlicht; sein jüngstes Buch „Social Media" richtet sich aber ausdrücklich an nichtwissenschaftliche Zielgruppen, die die Entwicklungen des Internets in den letzten Jahren verstehen und eingeordnet sehen wollen. Aktuelle Informationen sind auch in seinem Blog unter www.schmidtmitdete.de zu finden.

SOZIALE MEDIEN SIND EINE ART ÖFFENTLICHER RAUM

JHS: Die Betreiber von sozialen Medien müssen genauso wie der Wirt der Kneipe abwägen, will ich hier mein Hausrecht durchsetzen und es so machen, wie ich es will, oder höre ich auf meine Kundschaft. Andererseits gibt es auch im privatwirtschaftlichen Raum einer Kneipe gesetzliche Regeln, wie zum Beispiel, ob dort geraucht werden darf oder nicht. Hier greift der Staat aus übergeordneten Überlegungen in das Hausrecht des Wirts ein. In dem Fall: Wir wollen die Besucher schützen. Das allgemeine Interesse steht über dem Individualinteresse des Wirts als Geschäftsmann.

Ich sehe Facebook ebenfalls nicht als reines Privatangebot. Neben der Funktion als quasi öffentlicher Nutzerraum stellen auch Organisationen und Institutionen relevante Informationen bereit. Das bedeutet, dass klassisch publizistische Funktionen in die sozialen Medien wandern und sie zu einem ganz wesentlichen Bestandteil von Öffentlichkeit machen. Das sind alles Gründe, weshalb reine privat- und marktwirtschaftliche Gesichtspunkte nicht ausreichen.

? Zusammengefasst: An welchen Punkten sehen Sie konkret Bedarf für Mitbestimmung?

JHS: Ich sehe drei wichtige Punkte: erstens die Voreinstellungen, also was per default öffentlich und was privat gemacht wird – was können alle sehen, was nur bestimmte Leute. Zweitens die Frage der Algorithmen, die mir bestimmte Informationen anzeigen und andere ausblenden, zum Beispiel bei Facebooks Newsfeed. Und drittens geht es um die Transparenz bei der Verwendung von privaten Daten. Was passiert damit? Das muss für mich als Nutzer transparent sein. Die Anbieter müssen mich konkret informieren, was sie mit den Daten in den unterschiedlichen Situationen anstellen.

? Muss man den Firmen nicht ein Stück Unabhängigkeit zugestehen? Wir verlangen ja auch nicht von Coca-Cola, das Geheimrezept herauszugeben.

JHS: Transparenz muss nicht heißen, dass man komplett alles offenlegt, also den Programmcode, die Algorithmen und so weiter. Man kann den Nutzerinnen und Nutzern vermitteln, wie bestimmte Dinge grundsätzlich funktionieren: was zum Beispiel mit den Daten passiert, welche Informationen angezeigt werden. Für die allermeisten Nutzerinnen und Nutzer wäre das schon ein Transparenzgewinn. Dafür muss man dann nicht das geheime Rezept offenlegen.

Außerdem gibt bei Web-Plattformen die technische Struktur nur den Rahmen vor. Der Erfolg von Facebook besteht mindestens zu 50 Prozent in den Inhalten der Nutzer. Das Besondere ist nicht zwingend, dass die Oberfläche von Facebook besonders gut programmiert ist, sondern dass meine Freunde dort sind, aber auch Informationsanbieter wie „Zeit Online", die SPD und iRights.info und so weiter. Das heißt, selbst wenn Facebook zum Beispiel den Algorithmus für den Newsfeed offenlegen würde und andere Anbieter ihn nachbauen könnten, würden sie Facebook nicht kopieren können. Sie hätten nämlich nicht ausreichend Nutzer, und die bekommt man nicht so ohne Weiteres.

? Digitale Räume werden über Algorithmen, über Strukturen, über das, was vorgegeben wird, gestaltet – Stichwort „Code is law" oder „Privacy by design". Auf der anderen Seite gibt es das kodifizierte Recht. Was ist heute wirksamer? Die Vorgaben von Facebook oder das Recht?

JHS: Das kommt darauf an. Recht kann grundsätzlich wirksamer sein, wenn es umgesetzt und sanktioniert wird. Wir haben aber das Problem, dass wir es mit nationalen und EU-weiten rechtlichen Rahmenbedingungen zu tun haben, die aber gegenüber glo-

> **Recht kann möglicherweise nicht mit den einzelnen Änderungen Schritt halten, aber es ist dafür zuständig, bei den großen Fragen hereinzugrätschen.** Dr. Jan-Hinrik Schmidt

bal agierenden Akteuren im Netz schwer durchzusetzen sind. Recht ist zwar in der Theorie stärker, faktisch aber wird es überstimmt. Da kommen die Geschäftsbedingungen von Facebook, die dieses privatwirtschaftliche Kundenverhältnis regulieren, ins Spiel.

Wir haben dieses Viereck: Law, Contract, Code und Social Norms (Gesetze, Verträge, Code und soziale Normen, Anm. d. Red.). Contract und Code liegen im Wesentlichen in der Gestaltungsmacht des Anbieters, während Recht und soziale Normen außerhalb des Einflusses von Facebook liegen. Im Moment übertrumpft Code das Recht, weil wir es mit einer Situation zu tun haben, in der sich das Recht nicht durchsetzen kann.

? Fällt das Recht damit komplett aus?

JHS: Recht kann möglicherweise nicht mit den einzelnen Änderungen Schritt halten, aber es ist dafür zuständig, bei den großen Fragen hereinzugrätschen, wenn es sein muss. Die Folgerung wäre sonst, dass man gleich alles dem Markt überlassen kann – und den Entwicklern und den Juristen von Facebook, die die Verträge und Geschäftsbedingungen aufsetzen. Das Recht gibt einen übergeordneten Rahmen vor, gewisse Grundstrukturen, die das Bewusstsein der Nutzer schärfen. Dadurch, dass es generell eine Datenschutzgesetzgebung gibt, wird klargemacht, dass informationelle Selbstbestimmung wichtig ist. Das prägt das Bewusstsein der Nutzer und sorgt vielleicht dafür, dass einige irgendwann sagen: Moment mal, Facebook, wir hätten gerne mehr Möglichkeiten, unsere Privatsphäre zu schützen.

? Wie kann man denn die Anbieter dazu bringen, dass sie sich beim Datenschutz und bei der Transparenz öffnen? Welche Anreize gibt es?

JHS: Grundsätzlich könnte man sagen, dass die Kunden stärkeres Vertrauen fassen und länger auf der Plattform bleiben, wenn die Anbieter zum Beispiel Datenschutz fördern oder ihre Nutzungen transparent halten – also das Argument Kundenbindung. Es gibt dafür aber keine empirischen Beweise.

? Facebook könnte dann sagen: Das ist uns total egal, weil die sowieso alle bei uns sind.

JHS: Darauf kann man antworten, dann müsst ihr damit rechnen, dass ihr Probleme mit dem deutschen und europäischen Datenschutz bekommt. Es muss ganz klar sein: Wenn eine Firma in Europa aktiv sein will, muss sie sich an die Vorgaben halten. Letztlich müsste man mit Sanktionen drohen. Es ist natürlich möglich, dass eine Firma sagt, wir vergessen Deutschland und konzentrieren uns auf andere Länder, wo wir nicht solche Probleme haben. Auf der anderen Seite ist Deutschland – und Europa – ein wichtiger Markt. Letzten Endes kann sich eine Firma nicht sicher sein, was in zwei oder drei Jahren passiert. Eventuell gibt es dann andere Anbieter, die attraktiver sind, sodass ein Anbieter immer darauf achten muss, Schwachpunkte zu verbessern. ⊡

3.3 Auf welche Problematik könnte sich ein Digitaler Kodex beziehen?

Regulierung – ob per Gesetz oder durch einen Kodex – bezieht sich stets auf bestimmte Regelungssachverhalte. In der Regel steht der Regelungssachverhalt im Mittelpunkt jeder Überlegung über Regulierungsmaßnahmen. „Das Verhalten von Anbietern und Nutzern auf zentralen Kommunikationsplattformen" ist kein Sachverhalt, der konkreten oder auch nur konzeptionellen Überlegungen zu Regulierungsmöglichkeiten zugänglich wäre. Diese Themendefinition beschreibt kein Verhalten und keinen Interessenkonflikt und daher keinen Regelungssachverhalt, an dem man die Effizienz von Regulierungsansätzen beispielhaft untersuchen könnte. Es ist zudem nicht möglich zu untersuchen, warum sich Nutzer und Anbieter verhalten, und entsprechend, wie man gewissen Handlungen vorbeugen kann, ohne eine oder mehrere bestimmte Verhaltensweisen in den Blick zu nehmen. Schließlich umfasst ein derart abstrakt definierter Betrachtungsgegenstand eine solche Vielfalt von Problematiken, dass die Komplexität der Aufgabe eine zielführende Lösung kaum erwarten ließe. Aus diesem Grund wurde bereits oben angemerkt, dass die Frage „Braucht Deutschland einen Digitalen Kodex?" nicht beantwortet werden kann, ohne gleichzeitig anzugeben, worauf (sachlich, persönlich, inhaltlich) sich ein solcher Kodex beziehen soll.

Insofern erscheint es naheliegend, sich bei der Untersuchung nicht nur auf eine sektorspezifische Betrachtung zu konzentrieren, sondern zudem auf bestimmte – besonders gravierende und repräsentative – konkrete Fragestellungen.

Mögliche Themenschwerpunkte für eine weitere Untersuchung sind beispielsweise:

A) Cybermobbing,
B) Umgang mit persönlichen Informationen und Daten durch Nutzer und Anbieter,
C) Verstoß gegen fremde Urheberrechte.

Alle drei Themen werden derzeit als besonders gravierend wahrgenommen. Sie stehen gewissermaßen stellvertretend für den Eindruck, dass sowohl das Sozialverhalten der Menschen als auch der Anbieter im Netz anders ist als in der gegenständlichen Welt. Es geht um bedeutende Internet-spezifische Phänomene, wie die veränderte Wahrnehmung von Privatheit, die vermeintliche Unkontrollierbarkeit des Verhaltens, eine zumindest gefühlte „Verrohung der Sitten", die Grundeinstellung zum Umgang mit Rechten Dritter und vieles mehr. [36]

> **„Wir sollten einen breiten gesellschaftlichen Diskurs führen. Und dazu brauchen wir einen langen Atem. Die Debatte, die es derzeit gibt, wird heftig geführt, und sie wird uns noch lange erhalten bleiben. Ob sie aber schon das Interesse der breiten Bevölkerung gefunden hat, bezweifle ich. Dies können wir nur anhand von konkreten Beispielen erreichen, für die sich die Menschen interessieren. Insofern ist die Frage völlig berechtigt, welches konkrete Problem wir denn jetzt als Nächstes anpacken."**
>
> **Matthias Kammer,** Direktor des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI), 2. Expertenworkshop, 10.09.2013

Die genannten Themen betreffen Nutzer und Anbieter gleichermaßen. Den Nutzern wird vorgeworfen, sorglos zu handeln, sich unsozial zu verhalten und fremde Rechte nicht zu achten. Anbieter haben stetig mit Vorwürfen zu kämpfen, nicht genug Schutz vor derart unerwünschten – und zum Teil illegalen – Handlungen zu bieten, nicht genug Einfluss zu nehmen, übermäßig Daten zu sammeln, ihre Hände in Unschuld zu waschen, kurzum: sich unverantwortlich zu verhalten. Gleichzeitig wird von ihnen verlangt – und dies liegt häufig auch in ihrem eigenen Interesse –, nur sehr behutsam oder gar nicht in die Marktplätze der Meinungen einzugreifen, die sie ihren Nutzern bereitstellen. Dieses Spannungsfeld und die genannten Problemlagen finden sich – in gleicher oder ähnlicher Form – auch in anderen Bereichen des Netzes.

36 Weitere Ausführungen zu den Beispielthemen finden sich in der vollständigen Fassung des Themenpapiers „Was ist ein Digitaler Kodex?" im Annex.

Findet man für diese Themen im genannten Sektor Antworten auf die Frage, ob ein Digitaler Kodex zur Problemlösung beitragen und wie er konzipiert sein müsste, um Wirkmacht zu entfalten, ließen sich viele Erkenntnisse auf andere Bereiche und Problemfelder übertragen.

> **„Es gibt ein Dilemma: Auf der einen Seite kennen wir die positiven Aspekte von Anonymität im Netz, auf der anderen Seite wissen wir aber auch, dass Anonymität dazu führen kann, dass die Hemmschwelle absinkt und es beispielsweise zu Cybermobbing kommt. All die Straftaten im Netz können nicht verfolgt werden. Es ist die Frage, ob wir das überhaupt wollen? Wie kriegen wir die Leute dazu, im Internet anständig und fair miteinander umzugehen? Ich plädiere überhaupt nicht dafür, Anonymität aufzugeben, aber es ist auch ein Fehler, die Opfer allein zu lassen. Wie können wir mit dieser Problematik sinnvoll umgehen?“**
>
> **Prof. Dr. Dirk Heckmann,** Professor für Öffentliches Recht, Sicherheitsrecht und Internetrecht an der Universität Passau, Diskussion, Öffentliche Veranstaltung München, 04.07.2013

INTERVIEW MIT DOROTHEE BÄR

Wir brauchen kein eigenes Strafgesetzbuch fürs Internet

? Man kann im Netz drei Gruppen identifizieren: Unternehmen, Nutzer und den Staat. Gibt es ein Ungleichgewicht zwischen diesen Gruppen?

Dorothee Bär: Ich weiß nicht, ob man wirklich schon sagen kann, dass es ein eklatantes Ungleichgewicht gibt. Ich denke aber, man muss aufpassen, dass es nicht dazu kommt.

? Gibt es denn Bereiche, wo Sie meinen, dass der Staat mehr tun müsste, um im Netz für Fairness zu sorgen?

DB: Meines Erachtens müsste der Staat mehr im Bereich der schulischen Bildung tun. Ich habe jahrelang in der CSU dafür gekämpft, dass Medienkunde in Bayern als eigenes Schulfach eingeführt wird. Beim letzten Parteitag wurde dieser wichtige Schritt nun von den Delegierten beschlossen. Mir ist ein solcher Ansatz wesentlich lieber als gesetzliche Regulierungsversuche.

? Wird das denn konkrete Auswirkungen haben?

DB: Es ist ein wichtiger Anfang, und hier geht es zunächst um Landesgesetzgebung. Aber steter

Dorothee Bär

ist seit Dezember 2013 Staatssekretärin beim Bundesminister für Verkehr und digitale Infrastruktur. Bär ist seit 2001 Mitglied im CSU-Parteivorstand und wurde bei der Bundestagswahl 2002 über die Landesliste in den Bundestag gewählt. 2009 kandidierte Bär erstmals direkt und gewann mit einer Mehrheit im Wahlkreis Haßberge, Rhön-Grabfeld und Bad Kissingen. Von 2009 bis 2013 war sie für die CSU stellvertretende Generalsekretärin und für die gesamte CDU/CSU-Bundestagsfraktion Sprecherin für die Bereiche Familie, Senioren, Frauen und Jugend.

Foto: ToKo

Tropfen höhlt den Stein, und wir bleiben an dem Thema dran.

? Müsste der Gesetzgeber mehr tun, um die Privatsphäre im Netz stärker zu schützen?

DB: Die Schwierigkeit liegt in der Durchsetzbarkeit. Natürlich stellt sich die Frage, ob alles, was technisch möglich ist, auch erlaubt sein darf – gerade beim Datenschutz. Um ein Beispiel zu nennen: Nur weil Systemadministratoren von Unternehmen theoretisch Zugriff auf jeden Rechner dort haben, dürfen sie dann jede E-Mail lesen? Nein, dürfen sie nicht. Die Frage ist aber: Wie kann man durchsetzen und sichergehen, dass sie es nicht tun? Ein Unbehagen ist jedenfalls da.

? Muss man Unternehmen nicht zwingen, die Privatsphäre ihrer Nutzer besser zu schützen beziehungsweise sie erst einmal zu beachten? Welche Maßnahmen wären Ihrer Meinung nach wichtig?

DB: Für mich ist die Frage nach Opt-in und Opt-out das Entscheidende. Nutzer hätten wesentlich mehr Vertrauen, wenn sie die Weitergabe von Daten erst freischalten müssten – also Opt-in – und nicht umgekehrt, dass jegliche Datenweitergabe von Anfang an freigegeben ist und man erst einmal die nötigen Einschränkungen vornehmen muss.

? Selbst wenn sie vierzig Mal einen Haken setzen müssten?

DB: Prinzipiell ja. Es muss vielleicht auch nicht alles auf einmal abgefragt werden. Nutzerinnen und Nutzer könnten zum Beispiel am Anfang einen beschränkten Zugang erhalten, und dann erklärt man ihnen, was mit ihren Daten passiert und wo genau sie welche Funktion freischalten können.

Das Phänomen, dass man mit seinen Daten sparsam umgehen sollte, gilt aber nicht nur für das Internet. Ich schaffe es zum Beispiel oftmals nicht, den Leuten klarzumachen, dass Unternehmen bei einem Preisausschreiben nicht aus reiner Freundlichkeit Autos verschenken oder dass eine Payback-Karte nicht dazu da ist, Geld zu sparen, sondern eben um Daten zu sammeln. Hier fehlt es an der nötigen Sensibilität.

Viele sehen da eher eine abstrakte Gefahr. Zwar verändern manche Menschen zum Beispiel durch die NSA-Affäre ihr Online-Verhalten teilweise, aber die meisten tun das eben nicht. Bisweilen ist die vorherrschende Meinung eher die, zu sagen, man habe ohnehin nichts zu verbergen. Das ist das Vogel-Strauß-Prinzip.

? Wenn die Nutzer selbst dieses Bewusstsein nicht entwickeln, sollte dann nicht der Gesetzgeber einschreiten? Man könnte zum Beispiel versuchen, die deutschen Internet-Provider dazu zu bewegen, E-Mail standardmäßig mit PGP-Verschlüsselung anzubieten, sodass niemand mitlesen kann, auch nicht der Provider. Das wäre ein starker Eingriff in den Markt zum Schutz der Nutzer. Wie sehen Sie das?

WIR BRAUCHEN KEIN EIGENES STRAFGESETZBUCH FÜRS INTERNET

DB: Ich weiß nicht, wie sich das mit den Mitwettbewerbern aus dem Ausland verträgt. Grundsätzlich ist das eine interessante Idee, aber wir müssen aufpassen, dass wir den Standort Deutschland nicht durch eine Überregulierung schwächen und wir dadurch nicht mehr konkurrenzfähig sind.

Das Problem bei Verschlüsselung ist außerdem, dass man als Nutzer immer das Gefühl hat, wenn man so einen Dienst nutzen möchte, muss man unheimlich viel wissen. Man fragt sich dann: Was bedeutet das überhaupt, verschlüsselte E-Mails zu verschicken? Muss man etwas Besonderes beachten, lernen, anklicken? Ein solcher Vorgang müsste also wirklich voll automatisiert funktionieren, damit die breite Masse der E-Mail-Nutzer davon profitieren kann. Wenn man sich zu viele Gedanken machen muss, nutzt man ein Angebot nicht.

? Für viele Firmen sind Datenschutzregeln erst mal ein Hindernis. Vor allem Start-ups nehmen sie so wahr. Können Sie sich Geschäftsmodelle vorstellen, für die Datenschutz vorteilhaft ist?

DB: Eine Vielzahl neuer Anwendungen funktioniert nur durch die Analyse von Daten. Denken Sie zum Beispiel an ein Smartcar: Da haben Sie ein Auto, das von selbst beschleunigt und abbremst, sodass Sie möglichst sparsam und mit möglichst geringem CO_2-Ausstoß fahren. Das funktioniert nur, weil es über einige Informationen von Ihnen verfügt. Sie müssen also damit leben, dass Sie entsprechend ausgelesen werden. Oder im medizinischen Bereich: Smart-Apps könnten regelmäßig den Blutdruck messen und die sportlichen Aktivitäten aufzeichnen. Es gibt bereits Überlegungen, die Nutzung solcher Anwendungen in die Krankenkassentarife einfließen zu lassen. Solche Anwendungen würden nur akzeptiert werden, wenn die Menschen wüssten, dass mit ihren Daten kein Missbrauch geschieht. Dies zu garantieren, sehe ich sehr kritisch.

? Welche Rolle spielt der Breitbandausbau? In den Großstädten haben die Menschen ganz einfach Zugang zu schnellem Internet – das sieht auf dem Land teilweise ganz anders aus. Was würde sich ändern, wenn ganz neue Bevölkerungsschichten ins Netz kämen, weil sie plötzlich Breitband hätten?

DB: Zugang ist ein ganz wichtiges Thema. Laut Branchenverband Bitkom verfügen zwar über 99 Prozent der Menschen in Deutschland über einen Breitbandzugang, allerdings gilt dabei bereits ein 1-MBit-Zugang als breitbandig. Das geht natürlich gar nicht. Wir haben im Koalitionsvertrag vereinbart, dass Deutschland bis 2018 flächendeckend ein 50-MBit-Netz aufbauen soll. Flächendeckend bedeutet nicht 95 Prozent der Orte, sondern 100 Prozent, sodass man von der Hallig über den kleinsten Weiler bis auf die Almhütte ins schnelle Netz kommt. Zugang ist das alles Entscheidende.

Wir haben bei der Landtagswahl in Bayern die Bevölkerung

> **Es wird in Zukunft nicht nur um barrierefreies Bauen gehen, sondern auch um einen barrierefreien Zugang zum Netz.**
>
> Dorothee Bär

über die Gleichwertigkeit der Lebensverhältnisse abstimmen lassen, und sie ist jetzt Teil der bayerischen Verfassung geworden. Wenn unsere Vorfahren der Meinung gewesen wären, es lohne sich nicht, wirklich alle Bürgerinnen und Bürger mit Briefen, Telefonleitungen oder mit einem Wasser- und Abwassersystem zu versorgen, würden wir heute in einem anderen Land leben. Zugang entscheidet über Bildung, wirtschaftlichen Erfolg, Wertschöpfung und über medizinische Versorgung. Dazu gehört auch das selbstbestimmte Leben im Alter. Es wird in Zukunft nicht nur um barrierefreies Bauen gehen, sondern auch um einen barrierefreien Zugang zum Netz. Das ist ein Megathema in allen Lebensbereichen, denn alles steht und fällt mit der Digitalisierung.

? Ein Thema, das insbesondere in den Städten wichtig ist, ist flächendeckendes WLAN. Dabei gibt es aber immer noch ein Haftungsproblem, denn gegenwärtig hängt die Haftung am einzelnen Betreiber. Müssten wir das stärker fördern?

DB: Auf jeden Fall. Ich finde, WLAN ist wichtig. Wir müssen die Störerhaftung in den Griff bekommen – auch dies steht im Koalitionsvertrag. Anbieter, die ein solches Funknetz aufbauen, müssen die Möglichkeit haben, das zu tun, ohne dass sie später dafür haften müssen.

? Es gibt neben gesetzlichen noch soziale Normen in einer Gesellschaft – auch im Netz. Glauben Sie, dass dieser Bereich stärker betont werden sollte? Müssen wir neue soziale Normen im Netz entwickeln?

DB: Zuallererst muss man einen Unterschied machen zwischen Erwachsenen über 18 Jahren und Jugendlichen und Kindern unter 18. Von einem mündigen Bürger, der wählen gehen darf und der die vollen Rechte und Pflichten eines Erwachsenen besitzt, erwarte ich mehr als von einem Menschen, der noch nicht volljährig ist. Und gerade im Jugendschutz geht mir die Selbstverpflichtung oftmals nicht weit genug.

? Wer macht die Regeln? Ist das der Staat, oder können das auch andere sein? Das Modell eines Digitalen Kodex zum Beispiel könnte ein Mischmodell sein zwischen Selbstverpflichtung und staatlicher Aufsicht.

DB: Wir haben schon sehr viele Gesetze, die sowohl online als auch offline greifen, zum Beispiel bei den Themen Betrug, Stalking oder Ähnlichem. Der Staat kann sich nicht ganz aus der Verantwortung ziehen, denn viele Gesetze müssen an neue Gegebenheiten angepasst werden, aber ich glaube nicht, dass wir ein eigenes Strafgesetzbuch nur fürs Internet brauchen.

Was einen Kodex betrifft, kann man meiner Meinung nach einen gewissen Bewusstseinswandel feststellen. Immer mehr Menschen kritisieren den schlechten

WIR BRAUCHEN KEIN EIGENES STRAFGESETZBUCH FÜRS INTERNET

> **Verhaltensregeln aufzustellen ist ein Prozess, der nie abgeschlossen sein wird. Aber es ist wichtig und richtig, solche Regeln zu entwickeln.** Dorothee Bär

Ton im Netz, Themen wie Cybermobbing stehen weiter oben auf der Agenda als früher. Man hört immer öfter, dieses und jenes gehöre sich nicht. Ein solcher Kodex wird dabei nie ein abgeschlossenes Regelwerk sein, denn dazu ist unsere Gesellschaft viel zu differenziert und globalisiert. Ist es zum Beispiel heute noch unhöflich, wenn man während einer Präsentation oder in einem Gespräch immer wieder auf sein Handy schaut? Früher war das wesentlich verpönter als heute. Gesellschaftliche Kodizes sind auch nicht auf der ganzen Welt gleich: In manchen Ländern gilt es beispielsweise als unhöflich, etwas auf dem Teller übrig zu lassen, in anderen wiederum wird es nicht gern gesehen, wenn man alles aufisst.

Es wird immer Fragen geben, über die man sich streiten wird. Das Recht auf Anonymität im Netz ist zum Beispiel ein solches Reizthema. Ich bin eine Verfechterin dieses Rechts, aber viele sehen es geradezu als Grund allen Übels. Sie glauben, dass Anonymität beleidigende Aussagen im Internet fördert. Ich antworte dann immer gerne, dass ich die meisten Beschimpfungen und Beleidigungen von Personen bekomme, die mit ihrem Klarnamen auftreten, nicht von anonymen Nutzern.

Verhaltensregeln aufzustellen ist ein Prozess, der nie abgeschlossen sein wird. Aber es ist wichtig und richtig, solche Regeln zu entwickeln. Vermutlich werden die nachfolgenden Generationen über unsere heutigen Diskussionen über den vernünftigen Umgang mit den „neuen" Kommunikationsmitteln nur noch schmunzeln können. Eine Gesellschaft entwickelt sich. Auch eine digitale.

3.4 An wen könnte sich ein Digitaler Kodex richten?

Welche Akteure und welches Verhalten sind für einen Digitalen Kodex relevant?

In den vorangegangenen Abschnitten wurde eine Kategorisierung von Plattformen im Internet vorgenommen, um die Vielfalt von existierenden Plattform-Typen vor Augen zu führen. Sie verdeutlicht, dass es kaum zum Ziel führen kann, im Hinblick auf die Erfolgschancen eines Digitalen Kodex ganz allgemein von Plattformen und Akteurskonstellationen zu sprechen: Jeder Plattform-Typus bringt eine für ihn spezifische Akteurskonstellation mit sich. Auf Basis der Kategorisierung können bestimmte Fallbeispiele gebildet werden, auf die sich weitere Schritte fokussieren.

Die folgenden Überlegungen basieren auf der Entscheidung, *eine* Kategorie von Plattform auszuwählen, um die für sie typische Akteurskonstellation zu betrachten. Zu diesem Zweck wird die Kategorie *zentrale Kommunikationsplattform* weiter detailliert, also allem voran soziale Netzwerke wie Facebook oder Google+. Auf ihnen kommen einige der meistdiskutierten Fälle von unerwünschtem Verhalten massenhaft vor. Das Ziel des folgenden Abschnitts ist es, an der Akteurskonstellation solcher Plattformen zu illustrieren, welche netzspezifischen Faktoren das Verhalten der Akteure beeinflussen, das heißt aufzuzeigen, welche Besonderheiten der Handlungsraum „zentrale Kommunikationsplattform" für die Nutzer, die Anbieter und den Staat aufweist.

Um diesbezüglich eine rein abstrakte Erörterung zu vermeiden, werden diese Besonderheiten des Handlungsraums anhand eines der drei Themen dargestellt, die vorstehend als beispielhafte Regelungssachverhalte für die weitere Erörterung der Frage nach einem Digitalen Kodex vorgeschlagen wurden: der Umgang mit persönlichen Informationen und Daten. An diesem Beispiel zeigen sich typische Akteurskonstellationen und Problemlagen sowie deren Ursachen, die auf vielen Konfliktfeldern im Netz in ähnlicher Form vorzufinden sind.

Beobachtung des Akteursverhaltens auf zentralen Kommunikationsplattformen am Beispiel „Umgang mit persönlichen Informationen und Daten"

Die Hauptakteure auf zentralen Kommunikationsplattformen sind die Nutzer und die Dienste-Anbieter. Dem Staat kommt eine Rolle als Regulierungsinstanz zu. Bei der Charakterisierung der Akteure wird deutlich, dass im Falle von Anbietern und Staat Organisationsinteressen, Machtfragen und die Frage der Verantwortlichkeit im Mittelpunkt stehen, während im Falle der Nutzer sozialpsychologische Aspekte zentral sind. Daran lässt sich erahnen, dass der Status von Nutzern sich von den anderen beiden Akteuren klar unterscheidet. Im Folgenden sollen die Rollen der verschiedenen Akteure am oben genannten Beispielthema aufgezeigt werden. Hierdurch soll verdeutlicht werden, welche netzspezifischen Verhaltensfaktoren ein Fehlverhalten beim Umgang mit persönlichen Informationen und Daten begünstigen beziehungsweise dazu führen, dass ein solches Fehlverhalten derzeit nicht effektiv verhindert wird.

> **„Es gibt eine gesellschaftliche Wandlung in der Wahrnehmung von öffentlichen Räumen. Viele Menschen würden das, was sie auf Plattformen posten, als öffentlich bezeichnen, während sie beispielsweise ein Gespräch in der U-Bahn als privat empfinden."**
>
> **Dorothee Bär MdB,** Staatssekretärin beim Bundesminister für Verkehr und digitale Infrastruktur, Interview

Öffentliche Veranstaltung in Hamburg

FACEBOOK, WHATSAPP, GOOGLE+: WER MACHT DIE REGELN?

Fotos: Sarah Porsack

Weiterführen des öffentlichen Diskurses

Bei der zweiten Veranstaltung am 7. November 2013 in Hamburg bot sich die Gelegenheit, mit neuen Ergebnissen des Projekts den Diskurs mit der interessierten Öffentlichkeit weiterzuführen. Nachdem in der ersten Veranstaltung Fragestellungen der Verantwortung im Vordergrund standen, lag nun der Fokus auf der Thematik der Plattformen. Mit Prof. Dr. Wolfgang Schulz, Direktor des Hans-Bredow-Instituts für Medienforschung und des Alexander von Humboldt Instituts für Internet und Gesellschaft, und Moritz Nickel, Student an der Bucerius Law School, standen sich in den einleitenden Keynotes wiederum Wissenschaftler und Digital Native gegenüber. Während Wolfgang Schulz eine Analyse der Struktur von Plattformen lieferte, stellte Moritz Nickel die Vor- und Nachteile sozialer Netzwerke aus seiner persönlichen Perspektive gegenüber.

Die Bedeutung der Förderung der Medienkompetenz fand als einendes Element – analog zur Veranstaltung in München – auch in die sich hier anschließende Debatte Einzug. Auf dem Podium diskutierten Jutta Croll, Geschäftsführendes Mitglied des Vorstands der Stiftung Digitale Chancen, Sabine Frank, Leiterin Regulierung, Jugendschutz und Medienkompetenz Google Deutschland, Dr. Ralf Kleindiek, Staatssekretär im Bundesministerium für Familie, Senioren, Frauen und Jugend (bis Januar 2014 Staatsrat der Behörde für Justiz und Gleichstellung der Freien und Hansestadt Hamburg), Ole Reißmann, Redakteur bei Spiegel Online im Ressort Netzwelt, sowie Moritz Nickel ihre Positionen.

Die Betonung der Eigenverantwortung der Nutzer traf auf einen kritischen Blick auf monopolistisch agierende Plattform-Betreiber. Der Hinweis auf den zunehmenden Zugriff auf die Nutzerdaten stand neben dem Verweis auf die darauf aufbauenden nützlichen Funktionen. Nicht zuletzt fand sich auch in der Frage der Rolle des Staates weder unter den Diskutanten auf dem Podium noch in der sich anschließenden Publikumsdiskussion eine einheitliche Linie. Die kontroverse Diskussion machte deutlich, wie wichtig ein gesellschaftlicher Diskurs in diesem Themenfeld ist. ⊡

Keynote und Diskussion.
Prof. Dr. Wolfgang Schulz, Direktor des Hans-Bredow-Instituts für Medienforschung und des Alexander von Humboldt Instituts für Internet und Gesellschaft (oben links),
Jutta Croll, Geschäftsführendes Mitglied des Vorstands der Stiftung Digitale Chancen, Ole Reißmann, Redakteur bei Spiegel Online im Ressort Netzwelt, Sabine Frank, Leiterin Regulierung, Jugendschutz und Medienkompetenz Google Deutschland, Moritz Nickel, Student an der Bucerius Law School (oben rechts, v.l.n.r.),
Dr. Ralf Kleindiek, Staatssekretär im Bundesministerium für Familie, Senioren, Frauen und Jugend (bis Januar 2014 Staatsrat der Behörde für Justiz und Gleichstellung der Freien und Hansestadt Hamburg) (unten)

Datenschutzprobleme auf Kommunikationsplattformen entstehen im Umgang mit personenbezogenen Daten sowohl auf Nutzer- als auch auf Anbieterseite.

Einerseits sind es die Nutzer selbst, die massenhaft eigene oder fremde personenbezogene Daten, persönliche Informationen, Bilder und so weiter auf Online-Plattformen verbreiten, ohne sich über die Folgen ihres Handelns Gedanken zu machen. Einige Facebook-Nutzer etwa geben bei ihrer Kommunikation zahlreiche private Informationen in der Annahme preis, ihre Kontakte nur über eine rege Publikationstätigkeit zum Kommunizieren bewegen zu können.[37] Viele Nutzer achten dabei nicht auf einen möglichst „sparsamen" Umgang mit ihren Daten und persönlichen oder gar intimen Informationen.

Die Anbieter haben an diesem unbekümmerten Umgang mit persönlichen Daten ein Interesse. Ihre Geschäftsmodelle basieren zumindest teilweise auf einer ökonomischen Verwertung personenbezogener Daten, unter anderem auf deren Weitergabe an Dritte und auf ihrer mannigfaltigen Auswertung. Dabei sind die Modelle und Methoden häufig nicht transparent. Aufgrund ihrer Gestaltungsmacht sehen sich die Anbieter andererseits erheblichen Forderungen von Politik und Gesellschaft ausgesetzt, Daten und persönliche Informationen ihrer Nutzer zu schützen und Maßnahmen für den Schutz der Nutzer vor sich selbst zu treffen.

> **„Wenn ich mir anschaue, was die ein oder andern Leute bei Facebook veröffentlichen, zum einen über sich selbst, zum anderen über andere, und über Dinge, die sie eigentlich nicht wirklich betreffen, finde ich das schon gefährlich. Und deswegen finde ich es sehr gut, dass es jetzt hier dieses Projekt gibt."**
>
> **Michael Siemens,** Mitglied des Landesschülerrats Bayern (bis 2013), Keynote, Öffentliche Veranstaltung München, 04.07.2013

Fehlverhalten von Nutzern beim Umgang mit persönlichen Informationen und Daten

Nutzer, die die Angebote zentraler Kommunikationsplattformen in Anspruch nehmen, tun dies aus unterschiedlichsten Bedürfnissen. Eine Besonderheit bei diesen Plattformen ist, dass sie gratis zugänglich sind. Als Gegenleistung „zahlen" Nutzer dieser Dienste mit ihren preisgegebenen Daten und persönlichen Informationen.

> **„Ein Verfallsdatum für Daten wäre der Idealfall, die zweitbeste Lösung wären konkretere und verbindlichere Löschfristen als heute üblich."**
>
> **Lothar Schröder,** Mitglied des ver.di-Bundesvorstands, Konsultation

Im Übrigen erscheint es plausibel, dass die Nutzer sozialer Netzwerke private Informationen bewusst in extensivem Maße preisgeben, um ihre Kommunikationschancen zu erhöhen – und dies gerade in Bezug auf vergleichsweise „lose" Kontakte mit schwachen Bindungen. Der amerikanische Soziologe Mark Granovetter stellte in den 1970er-Jahren seine Theorie von der *Stärke schwacher Bindungen* (Granovetter 1973) zur Diskussion. Weil starke Bindungen, etwa bei Freundschaften, Familienangehörigen oder Arbeitskollegen, in der Regel dazu führen, dass die beteiligten Personen ein sehr ähnliches Beziehungsgeflecht aufweisen, wird zwischen ihnen nur vergleichsweise wenig neue Information ausgetauscht. Dagegen haben schwache Bindungen – zum Beispiel solche, die auf flüchtigen physischen oder unkörperlichen Begegnungen basieren, wie sie in sozialen Netzwerken oft vorkommen – weitaus mehr Potenzial, um an Neuigkeiten und innovative Ideen zu gelangen. Um als Kommunikationspartner in schwachen Bindungen auch für andere attraktiv zu sein und zu bleiben, sind Nutzer bereit, weitaus mehr Informationen in sozialen Netzwerken preiszugeben, als es bei Kontakten mit starken Bindungen notwendig wäre.

37 So hat fast jeder zweite im Rahmen der DIVSI U25-Studie befragte 14- bis 24-Jährige angegeben, dass man in einer „Online-Community nichts verloren habe", wenn man nichts über sich preisgebe (DIVSI 2014).

> **„Bei allen Diskussionen sollte man immer berücksichtigen, dass das Internet durch seine Kommunikationsmöglichkeiten zur Demokratisierung viel mehr beigetragen hat als zur Einschränkung derselben. Das ist eine wichtige Aussage, wenn man die Probleme im Netz diskutiert."**
>
> **Prof. Dr. Johannes Buchmann,** Vizedirektor des Center for Advanced Security Research Darmstadt und Professor für Informatik und Mathematik an der Technischen Universität Darmstadt, Diskussion, Öffentliche Veranstaltung München, 04.07.2013

Die Bindung an zentrale Kommunikationsplattformen gewinnt ihre Kraft nicht allein aus den bestehenden und vertrauten Kontakten, sondern auch aus den Möglichkeiten der vergleichsweise losen Kontakte. Laut der BITKOM-Studie 2011 suchten 37 Prozent der Nutzer jenseits ihrer bestehenden Kontakte nach neuen Kontakten. In der Regel wird es sich hierbei um die Suche nach Kontakten mit schwacher Bindung handeln. Entsprechend spricht einiges für die Annahme, dass diese zu besonderer Offenheit anreizenden Kontaktformen in sozialen Netzwerken eine besondere Rolle spielen.

> **„Ein negativer Aspekt von Plattformen ist, dass viele Informationen und Posts belanglos sind, dabei geht es nicht mehr um Information oder Kommunikation."**
>
> **Moritz Nickel,** Student an der Bucerius Law School, Keynote, Öffentliche Veranstaltung Hamburg, 07.11.2013

Daneben liegt eine wichtige Motivation zur Nutzung sozialer Netzwerke natürlich auch in der privaten Kontaktpflege mit Freunden und Bekannten (BITKOM 2011). In diesen Kontakten mit starker Bindung spielen weitere Bedürfnisse eine relevante Rolle, zum Beispiel die Diskussion wichtiger persönlicher Angelegenheiten oder (politischer) Ereignisse. Neben diesen engen Kontakten besteht aber auch das Bedürfnis, sich über Veranstaltungen und Unternehmungen zu informieren sowie „auf dem Laufenden" zu bleiben.

> **„Auch die Nutzer tragen eine Verantwortung im Netz, die sie nicht einfach nur auf den Staat und die Wirtschaft abschieben können. Ich bin verantwortlich für die Daten, die ich hergebe, und muss überlegen, bevor ich auf OK klicke. Als Nutzer muss ich also die Konsequenzen meines Handelns selbst tragen. Dafür muss ich allerdings bestimmte Regeln kennen, denn völlige Naivität führt zu negativen Ergebnissen. Die Verantwortung des Nutzers liegt somit auch darin, sich zu informieren."**
>
> **Thomas Götzfried,** Beirat DIVSI und Unternehmer, Konsultation

Umgang der Anbieter mit personenbezogenen Daten und persönlichen Informationen

Auf Seiten der Anbieter sind bezüglich Datenschutz zumindest zwei Aspekte von Belang: zum einen der Umgang der Anbieter mit den Daten und personenbezogenen Informationen, die die Nutzer hinterlassen, zum anderen die Frage danach, welchen Einfluss die Anbieter auf das Verhalten der Nutzer hinsichtlich des Umgangs mit ihren eigenen Daten haben.

> **„Die allermeisten Nutzer erwarten, dass eine Plattform ihnen einfach ein technisch verlässliches Umfeld bietet, in dem sie schnell und unkompliziert kommunizieren und sich austauschen können."**
>
> **Dr. Jan-Hinrik Schmidt,** wissenschaftlicher Referent für digitale interaktive Medien und politische Kommunikation am Hans-Bredow-Institut für Medienforschung, Interview

Anbieter zentraler Kommunikationsplattformen sind privatwirtschaftliche Unternehmen. Ein wesentlicher Punkt, der das Verhalten der Anbieter erklärt, sind die besonderen wirtschaftlichen Gegebenheiten, denen zentrale Online-Angebote unterliegen. Die meisten der großen Kommunikationsplattformen sind kostenlos nutzbar, ihr Angebot aber ist mit hohen Kosten verbunden. Um Refinanzierungsmöglichkei-

ten zu eröffnen, müssen die Dienste so gestaltet sein, dass mittelbar Einnahmen erzielt werden können.

Hierfür gibt es verschiedene Ansätze. Beispielsweise werden gezielt Daten gesammelt, um eine möglichst zuverlässige Wissensbasis für die individualisierte Zielgruppenansprache, vor allem durch individualisierte Werbung, zu schaffen. Gerade soziale Netzwerke scheinen hierauf zu setzen. Ein weiterer Baustein der Geschäftsmodelle, besonders ausgeprägt wiederum bei sozialen Netzwerken, liegt darin, dass Interkonnektivität und Datenportabilität unterbunden werden. Facebook, Google+, LinkedIn und XING bieten keine Möglichkeit, direkt mit den Nutzern jeweils anderer Netzwerke zu kommunizieren oder die in einem Netzwerk generierten Daten, Inhalte und Kontakte in ein anderes Netzwerk zu exportieren. Auf diese Weise gewinnt der Anbieter maximale Hoheit über die Datenkommunikation. Ohne Interkonnektivität und Datenportabilität werden Netzwerk- und Lock-In-Effekte, also die Bindung an einen Anbieter, erheblich gesteigert. Dies wiederum fördert Monopolbildung und zentralisierte Märkte (Zittrain 2008, 177) und wirkt sich erheblich auf die Handlungsmacht und den Einfluss der Anbieter gegenüber ihren Nutzern aus. Können Nutzer den Anbieter beziehungsweise die Plattform aufgrund solcher Umstände nicht wechseln, wird die Entstehung von Wettbewerb erschwert. Es können sich faktische Monopole bilden, was sich wiederum auf die Regulierung auswirken muss. So ist zum Beispiel Transparenz in monopolisierten Märkten – insbesondere wenn das Produkt oder der Dienst für die Zielgruppe von großer Bedeutung ist – ein wenig wirksames Mittel. Um solche Effekte zu verringern, enthält der Entwurf für eine EU-Datenschutzverordnung ein „Recht auf Datenübertragbarkeit".[38]

Solche Geschäftsmodelle führen schnell zu Konflikten mit rechtlichen und sozialen Normen. Auch stoßen sie häufig auf Unverständnis und führen zu weitgehenden Forderungen an die Anbieter, etwa in der Form, sich neben ihrer profitorientierten Tätigkeit als Hüter von Nutzer-Grundrechten oder Paternalisten zu verstehen.

> **„Inakzeptable Geschäftspraktiken: Löschen muss auch Löschen bedeuten."**
>
> **Dr. Alexander Dix,** Berliner Beauftragter für Datenschutz und Informationsfreiheit, Konsultation

Dabei wandeln sich Geschäftsmodelle im Netz sehr stark und sind in ständigem Fluss. Plattform-Anbieter scheinen oftmals erst einmal Daten zu sammeln, ohne zu wissen, ob sie mit dem Gesammelten (zum Beispiel personenbezogenen Informationen) etwas anfangen, ob sie sie kommerzialisieren können. Anbieter haben bei Daten- und Persönlichkeitsschutzfragen einander entgegengesetzte Motivationen zu balancieren; das Streben nach wirtschaftlichem Erfolg auch unter Einsatz ihres gesammelten Datenmaterials steht in Konflikt mit den Datenschutz- und Privatsphärenschutzansprüchen, die Politik und Gesellschaft an sie herantragen.

> **„Dienste wie soziale Netzwerke handeln mit Daten und eignen sich die Daten der Nutzer an, ohne dieses Vorgehen hinreichend kenntlich zu machen. Über Skaleneffekte und Monopolpositionen machen sie enorme Gewinne."**
>
> **Lothar Schröder,** Mitglied des ver.di-Bundesvorstands, Konsultation

Zu fragen wäre hier, ob es Möglichkeiten gibt, die Anbieter dazu zu bringen, freiwillig Datenschutz- und anderen Bestimmungen über den Schutz der Privatsphäre nachzukommen. Was könnte ihnen als Ausgleich für unter Umständen verloren gegangene Gewinnerwartungen als Anreiz geboten werden? Wie bringt man diese Unternehmen dazu, mehr oder weniger freiwillig die staatliche Aufgabe, für Bürger im Bereich Schutz der Privatsphäre Fürsorge zu tragen, zumindest in Teilen zu übernehmen?

38 Siehe Art. 18 des Entwurfs unter: eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:DE:PDF. Siehe hierzu auch das Interview mit dem Bundesdatenschutzbeauftragten Peter Schaar unter www.collaboratory.de/w/Interviewzusammenfassung_Peter_Schaar#Datenportabilit.C3.A4t.

INTERVIEW MIT PROF. DR. JOHANNES CASPAR

Die Autonomie des Nutzers darf nicht wegbrechen

? Welchen Regelungsbedarf gibt es beim Datenschutz im Internet?

Johannes Caspar: Ein besonders hohes Regulierungsbedürfnis besteht bei sozialen Netzwerken. Wir haben es hier mit unterschiedlichen Playern zu tun, die sich zum Teil nicht an nationale Regelungen halten, weil sie der Auffassung sind, dass für sie andere Regulierungsinstanzen zuständig sind bzw. nicht die deutschen Rechtsvorschriften gelten.

Ein Beispiel ist die Auseinandersetzung über die automatische Gesichtserkennung bei Facebook in den vergangenen zwei Jahren. Dabei ging es um die Frage, ob biometrische Merkmale verarbeitet werden dürfen, ohne dass die Betroffenen vorher zustimmen. Zunächst scheint es ja so, als böte eine Hilfe zur Markierung von Freunden auf Fotos wenig Grund für datenschutzrechtliche Sorgen. Wenn man aber weiß, dass für dieses Feature im Hintergrund die Gesichter von Millionen von Facebook-Nutzern biometrisch vermessen und diese Daten in einer Datenbank hinterlegt werden, ist dies – nicht zuletzt vor einer massenhaften und maßlosen Ausspähung durch insbesondere US-Geheimdienste – ein Datenschutzthema ersten Ranges. Die Missbrauchspotenziale einer biometrischen Gesichtsdatenbank sind immens. Man könnte sie etwa

Prof. Dr. Johannes Caspar

ist seit Mai 2009 Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit. Caspar promovierte 1992 an der Fakultät für Rechtswissenschaften an der Universität Göttingen. 1999 habilitierte er sich für Staats- und Verwaltungsrecht sowie für Rechtsphilosophie. Danach war Caspar als Wissenschaftler in Frankfurt und als Rechtsanwalt in Hamburg und Berlin tätig. Von 2002 bis 2009 leitete er den Wissenschaftlichen Dienst im Landtag von Schleswig-Holstein stellvertretend.

Foto: Thomas Krenz

DIE AUTONOMIE DES NUTZERS DARF NICHT WEGBRECHEN

dazu nutzen, um Gesichter wiederzuerkennen, die mithilfe von Videoüberwachungskameras aufgezeichnet wurden. Das wäre das Ende der Anonymität des Einzelnen in der Öffentlichkeit und ein machtvolles Instrument in der Hand gerade von undemokratischen Regimen zur Einschüchterung und Ermittlung politisch Andersdenkender, etwa anlässlich von Demonstrationen.

Das Bundesdatenschutzgesetz fordert für die Erhebung und Verarbeitung personenbezogener Daten eine Einwilligung der Nutzer. Im Einklang mit der EU-Datenschutzrichtlinie ist hierfür ein Opt-in der Betroffenen im Sinne einer vorab erfolgten expliziten Einwilligung nötig. Facebook beantwortet diese Frage allerdings anders: Es sei ausreichend, dass die Nutzer der Verarbeitung ihrer biometrischen Gesichtsmerkmale nicht widersprechen. Die Widerspruchsoption wurde in einer kaum auffindbaren Weise im Dschungel der Profileinstellungen versteckt. Die Rechtsauffassung begründete Facebook mit Berufung auf die für den europäischen Hauptsitz des Unternehmens in Dublin zuständige irische Datenschutzbehörde und dem allein einschlägigen irischen Datenschutzrecht.

Der Fall zeigt deutlich: Wir haben eine europäische Datenschutzrichtlinie, die überall unterschiedlich umgesetzt wird. Künftig brauchen wir gerade für global agierende Unternehmen einen europaweiten einheitlichen Datenschutzraum. Derartige Fälle müssen nicht nur klar geregelt sein, sondern auch in einheitlicher Weise von den Aufsichtsbehörden vollzogen werden.

? Bei der Gesichtserkennung konnte der Datenschutz am Ende dennoch erfolgreich umgesetzt werden – die Funktion ist für die Nutzer in Europa deaktiviert. Da hat die Gesetzeslage offenbar ausgereicht.

JC: Am Ende hat Facebook dem Druck zwar nachgegeben, die automatische Gesichtserkennung abgeschaltet und die Profile gelöscht: ein Etappensieg in einer sehr wichtigen Angelegenheit. Das Grundproblem, dass ein einheitlicher hoher Datenschutzstandard in Europa fehlt, bleibt bestehen. Bei den letzten Überarbeitungen der Datenschutzbestimmungen hat Facebook die automatische Gesichtserkennung mit erweiterter Funktion erneut aufgenommen. Die Funktion wird im Augenblick in Europa zwar nicht genutzt, die Möglichkeit, sie kurzfristig wieder einzuführen, hat sich Facebook aber nach wie vor offengehalten.

? Was sollten oder könnten Internet-Unternehmen tun, um dem Datenschutz Genüge zu tun oder um sich in diesem Bereich weniger angreifbar zu machen?

JC: Da ist zunächst einmal die Transparenz gegenüber den Nutzern, also klare Informationen über die Daten, die gespeichert werden. Das gilt auch und gerade für die Nutzungsdaten. Was wird mit den Daten gemacht? Wie werden pseudonyme Nutzungsdaten verwendet? Werden sie mit den Trägern des Pseudonyms zusammengeführt? Das sind Fragen, die nicht nur durch die Datenschutzbeauftragten gestellt werden, sondern auch für die Nutzer von Bedeutung sind. Diese Fragen müssen offen beantwortet werden. Gleichzeitig sollten die Unternehmen auch die Möglichkeit schaffen, dass die Beauftragten zumindest in besonderen Fällen Einblick in die Quellcodes erhalten, um bestehende Argumentationen über den Einsatzzweck, etwa für Cookies, zu überprüfen.

Für datenschutzfreundliche soziale Netzwerke müssen ferner die Nutzerführung verbessert und die Standard-Profileinstellungen so gestaltet werden, dass jedes neue Mitglied nach der Registrierung einen optimalen Datenschutz genießt. Nutzer müssen zudem in der Lage sein, Profileinstellungen selbstverantwortlich zu ändern. Gerade bei sozialen Netzwerken gilt, dass die Daten von Nutzern,

Der Nutzer sollte eigenverantwortlich sein Datenmanagement betreiben.

Prof. Dr. Johannes Caspar

die häufig noch jung und unerfahren sind, erst einmal zurückgehalten werden. Jeder soll später dann selbst entscheiden können, diese Voreinstellungen zu erweitern.

Müssen auch die Default-Einstellungen geändert werden? Sind Sie für ein generelles Opt-in?

JC: Ich bin generell für optimale Nutzer-Transparenz. Wir gehen insoweit konform mit den geplanten EU-Regelungen, die unter den Stichworten „Privacy by Default" oder „Privacy by Design" eben das verlangen. Allerdings sind die bisherigen Punkte viel zu allgemein geregelt. Da müssen konkretere Formulierungen her, die möglicherweise auch bedeuten, dass Opt-in-Verfahren wesentlich häufiger nötig werden, als bisher tatsächlich abgefragt.

Wie steht es denn mit der Eigenverantwortung des Nutzers?

JC: Der Nutzer sollte eigenverantwortlich sein Datenmanagement betreiben. Das heißt, er muss autonom bestimmen können, in welcher Weise er seine Daten im Netzwerk preisgeben will. Darüber hinaus muss er aber auch respektvoll mit den Daten Dritter umgehen. Das ist in den Netzwerken ein ganz wesentlicher Punkt. Letztlich geht es dabei um den Bereich des Selbstdatenschutzes. Datenschutzkompetenzförderung tut also not. Hier haben wir ganz wesentliche Defizite. Kinder und Jugendliche müssen nicht nur die technischen Anforderungen, wie sie am besten an die Daten herankommen, beherrschen, sondern darüber hinaus auch über die Bedeutung und Risiken ihrer Daten als Zahlungsmittel in der digitalen Welt aufgeklärt sein. Dies gilt es gerade in der schulischen Ausbildung zu vermitteln.

Was heißt überhaupt Privacy? Da gibt es ja international durchaus kulturell unterschiedliche Ansichten. In den USA finden die Nutzer andere Einstellungen akzeptabel als in Deutschland.

JC: Privatsphäre ist die Fähigkeit, selbstverantwortlich darüber zu entscheiden, mit wem ich meine Daten teile oder nicht teile. Diese Autonomie bricht immer mehr weg. Es ist auch für den amerikanischen Nutzer interessant, was mit seinen Daten passiert. Insofern sollte der kulturelle Unterschied eigentlich keine Rolle spielen. Diesseits und jenseits des Atlantiks gilt: Daten sind nicht nur ökonomische Optionen für private Akteure, sie vermitteln auch Macht über andere, sodass eine transparente demokratische Kontrolle gerade bei der Frage nach dem staatlichen Umgang mit Daten eine zentrale Rolle spielt.

Was ist für Nutzer gefährlicher: die private oder staatliche Überwachung von Daten? Seit Edward Snowden im vergangenen Jahr die NSA-Aktivitäten und diejenigen anderer Geheimdienste aufdeckte, können wir gar nicht mehr anders, als diese Ebene mitzudenken.

JC: Das kann man nicht mehr trennen. Die 1980er-Jahre waren von Ängsten gegenüber einem Überwachungsstaat geprägt. Als Antwort darauf haben wir das Recht auf informationelle Selbstbestimmung bekommen. Gesetzliche Garantien und Implementierungsprozesse im Bereich der Verwaltung haben den Umgang

DIE AUTONOMIE DES NUTZERS DARF NICHT WEGBRECHEN

> **Eine Bürgerbewegung für einen modernen Datenschutz ist sehr wichtig.** Prof. Dr. Johannes Caspar

des Staats mit unseren Daten seither rechtsstaatlich umrahmt. Dann – Anfang der 2000er-Jahre – hat sich die Situation verändert: Das Geschäft des Datenverarbeitens hat sich verlagert auf private Akteure. An die Stelle des Überwachungsstaats ist die Überwachungsgesellschaft getreten. Daten haben als ökonomische Ressource für Unternehmen ganz entscheidende Bedeutung erlangt – der rasante technologische Wandel hat die Ökonomisierung der persönlichen Daten noch beschleunigt.

Mit den Erkenntnissen von Edward Snowden, mit der Dokumentation des massenhaften Ausspähens der digitalen Kommunikation durch Nachrichtendienste, haben wir wieder eine ganz andere Ebene erreicht. Wir wissen heute, es gibt ein System der internationalen, staatlichen Überwachung, die demokratisch weitgehend unkontrolliert stattfindet und sich aller gangbaren Mittel und Wege bedient. Hier werden staatliche Stellen aktiv, die dann wieder untereinander Daten austauschen und die sich bei global agierenden Internet-Dienstleistern bedienen können.

Es gibt Stellen, die wissen, was in Echtzeit passiert, welche Kommunikation über die Internet-Knotenpunkte läuft; sie haben darüber hinaus Zugriff auch auf weit in die Vergangenheit zurückreichende Informationen bei den privaten Anbietern. Insofern haben wir es mit einer absoluten, entgrenzten Überwachung zu tun. Hier wird alles gemacht, was technisch machbar ist.

? Brauchen wir angesichts dieser Entwicklungen eine digitale Bürgerrechtsbewegung – so wie in den 1980er-Jahren die Umweltbewegung?

JC: Eine Bürgerbewegung für einen modernen Datenschutz ist sehr wichtig. Es hat sich in den letzten Jahren ganz deutlich gezeigt, dass die Politik aus eigener Kraft heraus bislang nicht willens oder zumindest nicht fähig war, klare Regeln für einen zeitgemäßen Schutz der Daten zu formulieren. Wir sind seit Jahren in bestimmten Bereichen auf Regelungen aus dem analogen Zeitalter beschränkt. Da muss sich etwas bewegen. Der Fortgang politischer Prozesse kann gerade durch ein verstärktes Engagement von Bürgerinnen und Bürgern wesentlich befeuert werden.

? Sehen Sie dies denn kommen? Die Empörung der Bevölkerung ist gering.

JC: Der derzeitige Protest ist natürlich keine Massenbewegung – nicht etwa so wie damals gegen die Volkszählung. Es scheint, als würde das Thema in der öffentlichen Wahrnehmung mit jeder Berichterstattung weiter an Gewicht verlieren, als würden wir uns schrittweise daran gewöhnen, dass unsere digitalen Grundrechte, die Basis für eine freie und offene Welt der Kommunikation, immer stärker von der sozialen Realität einer massenhaften, entgrenzten Kontrolle entwertet werden. Das ist ein schleichender Prozess, der am Ende an die Wurzeln des demokratischen Rechtsstaats geht. Diese Entwicklung erfüllt mich mit Sorge. Denn wenn wir weiter in diese Richtung gehen, werden wir immer mehr Freiheit und Selbstbestimmung über die eigenen Daten und damit auch über unser eigenes Leben verlieren. Es wird Zeit für Konsequenzen. Ansätze hierfür gibt es genug.

Ein anders gelagerter Aspekt in diesem Zusammenhang ist die Frage, inwieweit die Anbieter das Nutzerverhalten im Umgang mit eigenen personenbezogenen Informationen steuern können. Beispielsweise nehmen die Anbieter durch die Standardeinstellungen für die Privatsphäre der Nutzerkonten Einfluss auf das Nutzerverhalten, etwa wenn es darum geht, wer die Nutzerprofile einsehen kann. Große Teile der Nutzer nehmen die Möglichkeit, ihre Einstellungen an die persönlichen Belange anzupassen, nicht wahr. Was der Anbieter als Standard voreinstellt, bleibt also sehr häufig in Kraft. Hieran zeigt sich deutlich, wie Anbieter unreflektiertes Nutzerverhalten lenken können.

Gerade bei Anbietern mit einer nahezu monopolartigen Marktstellung ist zu bezweifeln, dass kritische Debatten in der medialen Öffentlichkeit sie in diese oder jene Richtung beeinflussen können. Warum sollen sie etwa selber auf Gefahren hinweisen, die im Zusammenhang mit einem allzu sorglosen Umgang mit persönlichen Informationen entstehen können? Warum sollten sie sich zu mehr Transparenz verpflichten, wenn Intransparenz und Komplexität für ihre eigenen Belange von Vorteil ist? Zwar ist durchaus anzunehmen, dass den Anbietern zentraler Kommunikationsplattformen daran gelegen ist, zumindest ein basales Vertrauensverhältnis mit den Nutzern aufrechtzuerhalten. Immerhin sind die Nutzer und ihre Inhalte ihr hauptsächliches – vielleicht sogar einziges – Kapital. Solange sich aber zum Beispiel ein etwaiger Vertrauensrückgang bei jugendlichen Nutzern – einen solchen diagnostiziert zum Beispiel die JIM-Studie 2012 (Jugend, Information Multimedia) des medienpädagogischen Forschungsverbundes Südwest[39] – nicht nennenswert negativ auf die Nutzerzahlen auswirkt oder diese aus anderen Gründen sogar steigen, stellt sich die Frage, warum die Anbieter mit selbstbeschränkenden Maßnahmen reagieren sollten.[40]

„Plattformen könnten mehr Aufklärung betreiben und beispielsweise umfassend über die Verwendung der persönlichen Daten informieren. Damit würden Sie gegebenenfalls aber ihr eigenes Interesse konterkarieren, da die Nutzer möglicherweise darauf reagieren würden und beispielsweise auf andere Dienste ausweichen würden."

Lina Ehrig, Leiterin des Teams Digitales und Medien, Verbraucherzentrale Bundesverband, Konsultation

Das Verhalten des Staates im Umgang mit persönlichen Informationen und Daten

Wie im Strafrecht ist die staatliche Gestaltungsmacht gegenüber zentralen Kommunikationsplattformen auch in Bezug auf den Datenschutz beschränkt. Dies zeigt sich zum Beispiel daran, dass die Versuche des Gesetzgebers, bei Datenschutzerklärungen der Anbieter mehr Transparenz zu erreichen, bislang kaum erfolgreich waren.[41] Dass die meisten Anbieter dieses Plattform-Typs außerhalb des Staatsgebiets angesiedelt sind, verringert den Einfluss eines einzelnen Staates erheblich.

Das zeigt sich an einem Beispiel: Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) hatte versucht, Facebook dazu zu zwingen, sich von der Klarnamenpflicht – jedenfalls für deutsche Nutzer – abzuwenden. Der Grund: Deutsches Datenschutzrecht schreibt vor, dass Online-Dienste generell so ausgestaltet werden müssen, dass sie auch anonym genutzt werden können. Erfolg hatte das ULD am Ende nicht. Das Oberverwaltungsgericht Schleswig lehnte das Anliegen in einer rechtskräftigen Entscheidung mit der Begründung ab, dass der Dienst nicht deutschem, sondern irischem Datenschutzrecht unterliege.[42]

39 www.mpfs.de/index.php?id=527.

40 Auch die DIVSI U25-Studie zeigt, dass bei Jugendlichen und jungen Erwachsenen Facebook mit 64 % eine der am meisten genutzten Plattformen im Internet ist. Das in Facebook gesetzte Vertrauen ist dabei eher gering bis durchschnittlich (der Wert ist 5,4 auf einer Skala von 1 bis 10) – siehe (DIVSI 2014, S. 156/157).

41 Vgl. Weitzmann 2013.

42 Vgl. die Pressemitteilung des ULD vom 24. April 2013, www.datenschutzzentrum.de/presse/20130424-facebook-klarnamen-ovg.htm.

Um einem solchen „Forum-Shopping" innerhalb von Europa vorzubeugen, versucht die EU schon seit einiger Zeit, Einigung über eine EU-Datenschutzverordnung zu erzielen. Eine solche würde zu einer echten Harmonisierung des Datenschutzrechts – jedenfalls in Bezug auf die hierin geregelten Themen – führen, da sie in den Mitgliedstaaten unmittelbar anwendbar wäre. Ob sich der Ansatz durchsetzt und den Einfluss der Mitgliedstaaten bei der Durchsetzung hoher Datenschutzstandards in der gesamten EU gegenüber US-amerikanischen Anbietern von Kommunikationsplattformen erhöht, ist derzeit aber eher zweifelhaft. Zum einen liegt das Vorhaben offenbar bis auf Weiteres auf Eis.[43] Zum anderen wäre es den Anbietern auch in diesem Fall unter Umständen noch möglich, dem höheren Schutzniveau zu entgehen, etwa indem sie ihre Datenverarbeitung vollständig in den USA durchführen und in Europa gar keine Niederlassungen mehr betreiben, in denen Daten verarbeitet werden.

> **„Die EU-Datenschutzgrundverordnung sieht eine ausdrückliche Verankerung des Marktortprinzips vor. Das ist zu begrüßen. Bei der Verarbeitung von personenbezogenen Daten gilt dann auch für Unternehmen, die nicht in der Union niedergelassen sind, unstreitig das europäische Datenschutzrecht. Entscheidend ist, dass die Unternehmen sich mit ihren Dienstleistungen an Personen richten, die in der EU niedergelassen sind. Das bringt zunächst einmal Rechtsklarheit und schützt die Nutzer auf der dann einheitlichen Grundlage des EU-Rechts. Allein die Anwendbarkeit der Datenschutzgrundverordnung reicht jedoch nicht aus: Darüber hinaus muss auch sichergestellt sein, dass das europäische Recht durch die Datenschutzaufsichtsbehörden einheitlich vollzogen wird. Wie dies künftig sichergestellt werden soll, ist der wohl umstrittenste Aspekt in der derzeitigen Reformdiskussion. Der durch die Kommission vorgeschlagene ‚One-Stop-Shop' darf nicht dazu führen, dass Unternehmen durch die Bestimmung einer Hauptniederlassung innerhalb der EU sich die allein zuständige Aufsichtsbehörde selbst aussuchen können. Es gilt daher, ein Verfahren zu entwickeln, bei dem Datenschutzanforderungen auch bei Untätigkeit der Behörde am Ort der Hauptniederlassung eines Unternehmens durchgesetzt werden können. Das ließe sich etwa durch ein Selbsteintrittsrecht von nationalen Aufsichtsbehörden sicherstellen. Wenn es künftig nicht gelingt, hier ein wirksames Verfahren einzuführen, das einen einheitlichen Vollzug auf hohem Datenschutzniveau sichert, erwartet uns ein ‚race to the bottom', bei dem die schwächste Behörde künftig für den Einzugsbereich von einer halben Milliarde Nutzern die Schutzstandards für den Vollzug des Datenschutzrechts vorgibt."**
>
> **Prof. Dr. Johannes Caspar,** Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit, Interview

Diese Beispiele zeigen, dass die Handlungsoptionen des Staates im Bereich der gesetzlichen Regulierung und Sanktion eingeschränkt sind. Indem er sich allerdings rein auf Beratungs- und Aufklärungsangebote beschränkt, um die Bürger von einem allzu sorglosen Umgang mit ihren Daten und persönlichen Informationen abzuhalten, wird der Staat seinem Schutzauftrag für die Bürger kaum vollständig Genüge tun können.

> **„Der Staat sollte fördernd und fordernd auftreten. Er muss klare rechtliche Vorgaben setzen und die Einhaltung angemessen kontrollieren. Der Einsatz zertifizierter**

43 Siehe www.telemedicus.info/article/2584-EU-Datenschutzverordnung-vorerst-auf-Eis-gelegt.html.

> **Produkte könnte hierfür eine wichtige Basis sein, um ein gefordertes Sicherheitsniveau zu gewährleisten."**
>
> **Prof. Dr. Claudia Eckert,** Professorin für IT-Sicherheit an der Technischen Universität München und Leiterin des Fraunhofer-Instituts für Angewandte und Integrierte Sicherheit (AISEC), Konsultation

Es wäre daher zu untersuchen, ob der Staat bei alternativen Regulierungsformen wie einem „Digitalen Kodex" mitwirken und welche Rolle er hierbei spielen könnte. Bisherige Versuche in dieser Richtung waren nicht von Erfolg gekrönt. So ist beispielsweise ein von der deutschen Politik mit erheblichem Aufwand unterstützter Versuch, einen Verhaltenskodex für die Anbieter sozialer Netzwerke zu etablieren, gescheitert.[44] Solche Fälle werfen wichtige Fragen über mögliche Erfolgs- und Misserfolgsfaktoren bei der Konzeption und Implementierung von Kodizes auf: Wäre es beispielsweise möglich, bestimmte Anreizsysteme in einem Digitalen Kodex zu verankern, die geeignet wären, das Verhalten von Plattform-Betreibern positiv zu beeinflussen? Wie können Anreize aussehen, die die Anbieter dazu bringen, ihr Verhalten – unter Umständen entgegen den eigenen Interessen – zu verändern? Sind Kodizes für ein einziges Land – also etwa ein Digitaler Kodex für Deutschland – für die Anbieter interessant genug bzw. überhaupt handhabbar?

Zusammenfassung: Die Akteure auf zentralen Kommunikationsplattformen, deren Verhalten und Beweggründe

Die Betrachtung der Akteurskonstellation auf zentralen Kommunikationsplattformen an einem Beispiel für eine regulativ derzeit ungelöste Problemlage sollte auf zweierlei hinweisen. Zum einen auf ein mögliches Themenfeld für einen Digitalen Kodex. Zum anderen sollte verdeutlicht werden, inwieweit der Handlungsraum Internet Besonderheiten für die Akteure und ihr Verhalten aufweist, die ein Digitaler Kodex in Rechnung stellen müsste.

> **„Eine ideale Plattform würde den Nutzer nicht überfordern, wäre leicht handhabbar und gleichzeitig transparent in Bezug auf das, was beispielsweise mit den Daten passiert. Wenn man sich den Erfolg der Mitgliederzahlen von Facebook ansieht, wird aber deutlich, dass die Nutzer diese Idealform scheinbar nicht brauchen und auf Usability und Transparenz verzichten können. Diese Diskrepanz ist problematisch, da sie zu einer Realitätsverzerrung führt. Was der Gesetzgeber, das Unternehmen, aber auch der Nutzer selbst tun kann oder sollte, ist demnach ungeklärt. Die Diskussion, ob der Nutzer überfordert ist und einen regulierten Rahmen braucht oder ob man ihn damit entmündigt, ist dabei zentral."**
>
> **Martin Falenski,** Justiziar bei der Initiative D21, Konsultation

> **„Ich bin kein Freund von zu viel Paternalismus. Dieses absolute Pochen auf ganz viel Datenschutz kann ich nur bedingt verstehen, da man ja auch irgendwie selbstständig Entscheidungen trifft. Jeder Nutzer muss aufpassen, wie er sich im Netz verhält."**
>
> **Moritz Nickel,** Student an der Bucerius Law School, Keynote, Öffentliche Veranstaltung Hamburg, 07.11.2013

Für Nutzer bestehen die Besonderheiten zentraler Kommunikationsplattformen im Internet vor allem darin, dass sie *unkörperliches* und *anonymes* Handeln ermöglichen, welches unerwünschtes Verhalten provozieren kann. Des Weiteren zeigt sich, dass Nutzer auf diesen Plattformen tendenziell zu einem gesteigerten Publikationsverhalten neigen, um ihre Attraktivität für andere Nutzer – vor allem im Rahmen „loser" Bindungen – zu steigern. Dieses Verhalten scheint die Reflexionsbereitschaft im Hinblick auf Probleme des Datenschutzes abzuschwächen. Zwar ist hier auch von Wissens- und Sensibilisierungsde-

44 Siehe www.telemedicus.info/article/2569-Kodex-zur-Selbstregulierung-fuer-soziale-Netzwerke-gescheitert.html.

fiziten auszugehen, doch ein gewichtiger Teil der Probleme, die bei Nutzern auftreten, müssen dem Anbieter mit angelastet werden.

> **„Wenn die Einsichtsfähigkeit der Nutzer hoch ist, ist davon auszugehen, dass die Nutzer wissen, was sie tun. In diesem Fall kann man ein Unternehmen nicht dafür haftbar machen, was die Nutzer tun und eben auch freiwillig aufgeben, indem sie beispielsweise private Dinge auf Plattformen offenlegen. Die Autonomie von Plattform-Anbietern muss erhalten bleiben. Sie sind private Unternehmen, deren Zweck nicht die öffentliche Daseinsvorsorge, sondern das Geldverdienen ist. Ihnen vorzuschreiben, beispielsweise welche Posts sie wiederherstellen müssen, stellt insofern einen erheblichen Eingriff in die Unternehmensautonomie dar."**
>
> **Martin Falenski,** Justiziar bei der Initiative D21, Konsultation

Die Anbieter haben große Gestaltungsmacht, weshalb es zunächst naheliegend erscheint, ihnen erhebliche Verantwortung, auch für das Verhalten der Nutzer, zuzuschreiben. Daraus ergibt sich für sie als Akteure eine zwiegespaltene Rolle, weil sie in erster Linie privatwirtschaftliche Interessen über netzspezifische Geschäftsmodelle verfolgen, aber zugleich von ihnen verlangt wird, ihre Nutzer zu schützen. Die Situation wird zusätzlich durch interne Interessenkonflikte verkompliziert: Ein effizienter Nutzerschutz kann zum Beispiel langfristigen Geschäftsinteressen dienen, obwohl er kurzfristig wirtschaftliche Einbußen bedeutet. So mag es die Attraktivität eines sozialen Netzwerks steigern und Vorbehalte verringern, wenn weniger Daten gesammelt oder die gesammelten Daten sensibler und weniger extensiv zu kommerziellen Zwecken genutzt werden. Allerdings würde der Anbieter hiermit möglicherweise seinem wirtschaftlichen Erfolg schaden. Der Anbieter befindet sich daher in einem internen Interessenkonflikt, dessen Abwägung aufgrund einer Vielzahl unkalkulierbarer Faktoren kaum präzise möglich ist. Wie viele neue Nutzer der Anbieter durch einen sparsameren Umgang mit persönlichen Daten und Informationen anziehen würde, ist zum Beispiel kaum zu ermitteln.

Infrage steht, inwieweit es Anbietern zugemutet werden kann und bei genereller Betrachtung wünschenswert ist, für die Realisierung von Gemeinwohlinteressen und die Sicherung von Grundrechten in die Pflicht genommen zu werden, also für Aufgaben, die genuine Staatsaufgaben sind. Man könnte die Frage auch anders stellen: Inwieweit kann es geboten und gerechtfertigt sein, in die Geschäftsmodelle und Funktionsfähigkeit der Plattformen einzugreifen, um etwaigen schädlichen Auswirkungen von Kommunikationsplattformen auf Grund- und Freiheitsrechte zu begegnen?

> **„In welchem Verhältnis stehen eigentlich Cybermobbing, Shitstorm und bürgerliche Grundrechte? Inwieweit hat der Anbieter Sorge dafür zu tragen, dass die Netzwerkteilnehmer vom Anbieter nicht nur als kommerzielle Konsumenten konstruiert werden, sondern auch gewissermaßen als Konsumenten von Bürgerrechten?"**
>
> **Dr. Alexandra Manske,** freiberufliche Soziologin in Berlin, ehemals Humboldt-Universität zu Berlin, 2. Expertenworkshop, 10.09.2013

Schon auf den ersten Blick zeigt sich eine erhebliche Ambivalenz bei der Regulierung von zentralen Kommunikationsplattformen. Regulierungsmaßnahmen müssen sich zunächst stets an der Tatsache orientieren, dass solche Netzwerke als zentrale Marktplätze der Meinungen erhebliche Bedeutung für die Ausübung der Kommunikationsgrundrechte der Nutzer haben. Massive oder gar existenzbedrohende staatliche Eingriffe gegenüber den Anbietern verbieten sich also schon hinsichtlich des Schutzes der Nutzerinteressen. Daneben ist zu berücksichtigen, dass die Geschäftsinteressen der Anbieter ebenfalls Grundrechtsschutz genießen. Auch dies ist zu bedenken, wenn erwogen wird, ihnen Schutzfunktionen gegenüber den Nutzern aufzuerlegen, die ihren eigenen Interessen widersprechen. Die Anbieterinteressen werden sich in vielen Fällen mit

solchen Aufgabenverpflichtungen nicht in Einklang bringen lassen. Es ist fraglich, welcher Spielraum für Regulierung angesichts dieser Gemengelage verbleibt.

> **„Insofern liegt der Regelungsbedarf eigentlich eher darin: Wie findet man auf internationaler Ebene einen Common Sense, der die Interessen in Ausgleich bringen kann? Und der eben auch die Interessen der Plattform-Anbieter berücksichtigen kann?“**
>
> **Dominik Höch,** Fachanwalt für Urheber- und Medienrecht bei Höch Kadelbach Rechtsanwälte, Konsultation

> **„Der Anreiz für Plattformen, beispielsweise mehr über die Verwendung der Nutzerdaten aufzuklären, liegt darin, dass die Kunden bzw. Nutzer stärkeres Vertrauen fassen und so länger auf der Plattform aktiv bleiben. Zumindest sollten Plattform-Anbieter dieses Argument im Hinblick auf ihre potenziellen Konkurrenten, die mit Sicherheit in einigen Jahren da sein werden, berücksichtigen. Auch Facebook ist irgendwann nicht mehr in und muss sich neu erfinden. Wenn sie diese Flanke schließen könnten, dann müsste das aus meiner Ansicht ein Anreiz sein.“**
>
> **Dr. Jan-Hinrik Schmidt,** wissenschaftlicher Referent für digitale interaktive Medien und politische Kommunikation am Hans-Bredow-Institut für Medienforschung, Interview

Natürlich könnten die Anbieter ein Interesse daran entwickeln, ihre Geschäftsmodelle im Hinblick auf die Nutzer-Datenverwertung – als vertrauensbildende Maßnahme – freiwillig anzupassen. Zumindest könnten sie diesbezüglich mehr Transparenz herstellen, etwa indem den Nutzern klar verständlich dargelegt wird – sofern das angesichts der Komplexität solcher Materien überhaupt möglich ist –, was mit ihren Datenspuren geschieht und wie sie gegebenenfalls kommerzialisiert werden. Solange die Nutzerzahlen sozialer Netzwerke allerdings steigen und das Nutzervertrauen nicht über alle Maßen abnimmt, werden die Anbieter ihre jetzige Haltung kaum ändern.

> **„Die Nutzer verstehen den Datenschutz und die Konsequenzen ihres Handelns im Netz nicht weitreichend genug und können deshalb wenig Verantwortung für ihr Handeln tragen. Dieser Problematik kann in erster Linie mit der Förderung der Medienkompetenz entgegengewirkt werden. Aktuell ist es so, dass die Lehrer oder Eltern es den Kindern nicht vermitteln können, weil sie es selbst nicht verstehen. Hier ist auch der Staat in der Pflicht, da Bildungspolitik zunächst Aufgabe des Staates bzw. der Länder ist. Die Umsetzung kann allerdings nur in Bündnissen erfolgen, da der Staat hier wenig Know-how hat. Der Staat sollte in diesem Bereich mit anderen Akteuren wie der Wissenschaft, der Wirtschaft oder den Anbietern zusammenarbeiten bzw. deren Expertise nutzen.“**
>
> **Oliver Süme,** Rechtsanwalt und Stellvertretender Vorstandsvorsitzender des Verbands der deutschen Internetwirtschaft e.V. eco, Konsultation

Der Staat handelt mit seinen herkömmlichen Regulierungsformen im Falle transnational operierender Plattform-Anbieter unter erschwerten Bedingungen, seine Bemühungen um Einflussnahme sind bislang eher ineffizient. Hinzu treten die oben genannte Ambivalenz und Abwägungsschwierigkeiten in Bezug auf die staatliche Einflussnahme in solche kommunikativen Räume. Im Rahmen seiner Fürsorgepflicht tritt er angesichts solcher und im Zweifel weiterer Probleme weniger als Schutzherr über Bürgerrechte, sondern eher als Initiator und Förderer von Aufklärungs- und Beratungsprogrammen auf. Dieses Engagement des Staates ist allerdings in vielerlei Hinsicht noch defizitär. Obwohl zum Beispiel das Thema „soziale Netzwerke“ Schulen bereits erreicht hat, fehlt es dort häufig an qualifiziertem Lehrpersonal. Ganz generell werden Themen zur Medienpraxis und Medienkritik nicht in einem eigenen Fach behandelt, sondern tau-

chen eher bruchstückhaft im Deutsch- oder Informatikunterricht auf.[45]

Hiervon abgesehen stellt sich die Frage, ob der Staat seiner Akteursrolle angesichts der evidenten Regulierungs- und Durchsetzungsdefizite mit Bildungs- und alternativen Regulierungsansätzen ausreichend gerecht werden kann. Könnte er darüber hinaus bei der Aufsetzung und Implementierung eines Digitalen Kodex eine weitere Rolle einnehmen? Wie könnte sie aussehen?

45 Vergleiche DIVSI 2014, S. 160.

4. Der Digitale Kodex: zwei Modelle

Ein „Digitaler Kodex" ist zunächst nur ein möglicher Begriff für ein alternatives Konzept für die Regelung von netzspezifischen Konfliktfeldern. Dahinter steht die Frage, wie das Verhalten im Netz effizienter und wirkmächtiger geregelt werden kann, als es herkömmliche Regulierungsformen offensichtlich leisten können.

> **„Die Idee eines Digitalen Kodex halte ich für sehr sinnvoll. Auch im Bereich der digitalen Arbeitswelt wäre so etwas wünschenswert. Dies betrifft beispielsweise die ständige Erreichbarkeit für Arbeitnehmer und mobile Arbeitsweisen, wie sie durch die Digitalisierung der Arbeit möglich geworden sind."**
>
> **Michael Schwemmle,** Geschäftsführer von Input Consulting GmbH, Konsultation

Wie ein Digitaler Kodex aussehen müsste, um bestimmten unerwünschten Verhaltensweisen im Netz begegnen zu können, hängt dabei entscheidend davon ab, wie er konzipiert ist und wie er umgesetzt wird. Um sich über das „Ob" (Deutschland einen Digitalen Kodex braucht) klar zu werden, muss zumindest eine ungefähre Vorstellung vom „Wie" (ein solcher Kodex aussehen könnte) bestehen.

Die denkbaren Möglichkeiten sind vielfältig. Ein Digitaler Kodex könnte etwa durch Mechanismen der Selbstregulierung der Wirtschaft oder der regulierten Selbstregulierung entstehen, oder rein durch die ungesteuerte Durchsetzung von sozialen Normen, die sich die Nutzer selbst setzen und die aus intrinsischen Motiven eingehalten werden. Denkbar sind auch Zwischenmodelle, die Aspekte dieser Konzepte kombinieren.

> **„Das Internet wird von verschiedenen Akteuren gestaltet und gepflegt: Technologieanbietern, Nutzern und Regierungen. Um einheitliche Standards im Netz zu schaffen, muss man auch auf diesen verschiedenen Ebenen aktiv arbeiten."**
>
> **Michelle Thorne,** Global Strategist bei der Mozilla Foundation, Konsultation

Im Anschluss werden daher konzeptionelle Überlegungen vorgestellt, wie ein Digitaler Kodex auf- und umgesetzt werden könnte. Hierbei handelt es sich um die modellhafte Skizzierung zweier denkbarer, sehr unterschiedlicher Optionen, die als Arbeitshypothese und damit als Diskussionsgrundlage dienen können.

4.1 Modell A: „Institutionalisierte Aushandlung zwischen allen Beteiligten"

Kurzbeschreibung

Es wird eine institutionalisierte Struktur mit hoher Glaubwürdigkeit geschaffen. Die Glaubwürdigkeit entsteht durch die in der Struktur vertretenen Akteursgruppen bzw. deren Vertreter und demokratische Entscheidungsprozesse. Die in der Struktur vertretenen Akteursgruppen identifizieren und evaluieren Regulierungsfelder, gegebenenfalls mithilfe direkter Bürgerbeteiligung. Sie ermitteln also den konkreten Regelungsbedarf und plausibilisieren, ob eine Problematik im Rahmen eines Digitalen Kodex behandelt werden kann und sollte. Sofern diese Fragen in Bezug auf ein konkretes Thema bejaht werden, wird ein Digitaler Kodex im Rahmen der Struktur entwickelt und imple-

mentiert. Durch bestimmte Anreizmechanismen für regelkonformes Verhalten wird dem Kodex zur Wirkmacht verholfen.

Wer entwickelt nach Modell A den Kodex, macht ihn bekannt und setzt ihn durch?

- Es wird eine unabhängige und institutionalisierte Struktur konzipiert, die den Prozess der inhaltlichen Ausarbeitung von Kodizes organisiert und umsetzt.

> **„Es gibt ein hohes Misserfolgsrisiko in Bezug auf das Konzept der institutionalisierten Aushandlung. Zentral für den Erfolg ist die Präsenz einer handlungsfähigen Institution, die ernst genommen wird."**
>
> **Dr. Sönke E. Schulz,** wissenschaftlicher Assistent und Geschäftsführer des Lorenz-von-Stein-Instituts für Verwaltungswissenschaften, 3. Expertenworkshop, 27.01.2014

- Die Finanzierungsstruktur der institutionellen Struktur muss so gestaltet sein, dass sie gegen Einflussnahme von Partikularinteressen geschützt ist und nachhaltig operieren kann. So könnten die Mittel aus unterschiedlichen Quellen stammen, zum Beispiel von der öffentlichen Hand, der Privatwirtschaft oder aus Spenden.
- In der Struktur sind alle betroffenen Akteursgruppen vertreten. Dies sind zumindest Bürger, Nichtregierungsorganisationen, Unternehmen, öffentliche Hand, Wissenschaft.
- Die Vertreter der Akteursgruppen bilden einen Rat als oberstes Entscheidungsgremium, ähnlich einem Parlament. In dem Rat sind alle Akteursgruppen angemessen vertreten.
- Es wird festgelegt, wie Vertreter der einzelnen Akteursgruppen in den Rat aufgenommen werden. Zum Beispiel: Die Bürgervertreter werden durch eine Online-Wahl bestimmt, für die sie als Individuen kandidieren – mit oder ohne Unterstützung einer NGO. Wirtschaftsvertreter werden durch Branchenverbände entsandt.
- Der Rat setzt Expertengruppen ein, die ihn bei seinen Entscheidungen zum Beispiel in technischer oder rechtlicher Hinsicht unterstützen, und bestimmt deren Besetzung.
- Der Rat kann in Einzelfällen Anhörungen durchführen, um weiteren von einem Kodex betroffenen Parteien die Möglichkeit der Stellungnahme zu geben.

> **„Es gilt zunächst einmal, die Interessenlagen auszumachen. Hier ist eine Bottom-up-Strategie sinnvoll. In jedem Fall sollte der Prozess aber einen Multi-Stakeholder-Ansatz verfolgen und alle beteiligten Akteure involviert sein."**
>
> **Peter Schaar,** Vorstand der Europäischen Akademie für Informationsfreiheit und Datenschutz (bis Dezember 2013 Bundesbeauftragter für den Datenschutz und die Informationsfreiheit), 3. Expertenworkshop, 27.01.2014

> **„Beim Konzept der institutionalisierten Aushandlung muss die Metaebene immer berücksichtigt werden. Wer könnte einen solchen Rat aufsetzen? Welche Legitimation besitzt er? Werden politische Instanzen – etwa die Bundesregierung – dabei mit einbezogen?"**
>
> **Patrick von Braunmühl,** Geschäftsführer des Vereins Selbstregulierung Informationswirtschaft (SRIW), 3. Expertenworkshop, 27.01.2014

Wie entsteht ein Digitaler Kodex nach Modell A?

Die Struktur implementiert Prozesse, über die konkreter Regelungsbedarf zu bestimmten Themen ermittelt wird. Wird ein Regelungsbedarf identifiziert, wird festgelegt, wofür Regelungen getroffen oder inwieweit bestehende Regelungen angepasst werden sollten. Dies kann auf zwei Wegen geschehen und soll anschließend am Beispiel „Umgang mit persönlichen Informationen und Daten in sozialen Netzwerken" erläutert werden.

Die durch Repräsentanten im Rat vertretenen Nutzer schlagen vor, einen Digitalen Kodex zum Thema „Umgang mit persönlichen Informationen und Daten in sozialen Netzwerken" zu entwickeln und umzusetzen. Der Rat stimmt über den Antrag ab und entscheidet darüber, ob dieses Thema evaluiert werden soll. Er entscheidet sich dafür und lässt, zum Beispiel durch ein Meinungsforschungsinstitut, ermitteln, ob nach Auffassung der betroffenen Akteure (hier: Nutzer, NGOs, Anbieter) tatsächlich Regelungsbedarf besteht, und wenn dies der Fall ist, in Bezug auf welche Problemfelder. Ergibt die Evaluierung, dass und inwiefern ein Regelungsbedarf besteht, wird der Entwicklungsprozess für einen Kodex zu diesem Thema („Teilkodex") eingeleitet.

Alternative: Bürger haben über ein hierfür bereitgestelltes Bürgerbeteiligungssystem vorgeschlagen, einen Digitalen Kodex zum Thema „Umgang mit persönlichen Informationen und Daten in sozialen Netzwerken" zu entwickeln und umzusetzen. Das Verfahren orientiert sich am Modell der Online-Petition. Für den Antrag hat sich eine durch die Statuten der Struktur vorgegebene Anzahl an Unterstützern ausgesprochen. Der Rat muss nun evaluieren, welche Themen im Digitalen (Teil-)Kodex zur Frage „Umgang mit persönlichen Informationen und Daten in sozialen Netzwerken" adressiert werden sollen. Die Evaluierung erfolgt mit den oben beschriebenen Methoden.

Der Rat lässt einen Entwurf für den Digitalen Kodex („Teilkodex") zum Thema „Umgang mit persönlichen Informationen und Daten in sozialen Netzwerken" von einer der Expertengruppen entwickeln. Die Expertengruppe ist mit Datenschutzexperten, aber auch mit Sozialpsychologen und anderen mit der Thematik vertrauten Fachleuten besetzt. Im Anschluss wird der Expertenentwurf im Rat beraten, gegebenenfalls angepasst und überarbeitet und schließlich verabschiedet.

Alternative: Der vom Rat beschlossene Entwurf tritt erst in Kraft, nachdem er von den betroffenen Akteursgruppen auf dem Wege partizipativer Online-Demokratie kommentiert werden konnte. Entsprechende Werkzeuge werden für diesen Zweck, wenn nötig, angepasst und entsprechend eingesetzt. Der Rat verabschiedet die endgültige Fassung unter Berücksichtigung der Kommentare. Die Alternative bietet sich insbesondere für einen Kodex zum „Umgang mit persönlichen Informationen und Daten in sozialen Netzwerken" an, da sich dieser neben den Anbietern an die Nutzer richten soll.

Die Entscheidung des Rates über den Teilkodex zum „Umgang mit persönlichen Informationen und Daten in sozialen Netzwerken" ist für einen zu definierenden Mindestzeitraum für die Anbieter bindend. Eine Wiederbefassung des Rates mit der gleichen Frage kann erst nach Ablauf einer bestimmten Frist erfolgen. Ergibt sich auf den oben beschriebenen Wegen erneuter Regelungsbedarf oder der Bedarf nach einer Reform oder Ergänzung des Kodex, wird erneut ein Verfahren eingeleitet.

> **„Im Allgemeinen darf die Debatte nicht zu technisch sein, wenn die breite Masse angesprochen werden soll. Es dürfen also nicht die technischen Dinge im Vordergrund stehen, sondern vielmehr die praktischen Fragen, die die Leute bewegen."**
>
> **Peter Schaar,** Vorstand der Europäischen Akademie für Informationsfreiheit und Datenschutz (bis Dezember 2013 Bundesbeauftragter für den Datenschutz und die Informationsfreiheit), 3. Expertenworkshop, 27.01.2014

Wie sieht der Digitale Kodex nach Modell A aus?

Der in diesem Zuge entstandene Digitale Kodex zum „Umgang mit persönlichen Informationen und Daten in sozialen Netzwerken" ist ein Modul des Gesamtkodex. Der Gesamtkodex ist eine Regelungsstruktur mit themenspezifischen Bereichen („Teilkodizes"). Durch seinen modularen Aufbau und den oben beschriebenen Entstehungsprozess ist die dynamische Weiterentwicklung des „Digitalen Gesamtkodex" gewährleistet.

Wie wird ein Kodex nach Modell A wirkmächtig?

Die Wirkmacht des Kodex basiert vor allem auf der Legitimation der Struktur. Sie überprüft die Einhaltung des Kodex durch die Adressaten.

Um die Einhaltung des Kodex zu fördern und dem Kodex zusätzliche Wirkmacht zu verleihen, werden themen- und akteursspezifische Anreize geschaffen. Diese können unterschiedlicher Natur sein, zum Beispiel in Zertifizierungen oder Auszeichnungen oder auch in staatlich-regulativen Privilegien bestehen. Welche Anreizsysteme jeweils erforderlich und Erfolg versprechend sind, hängt vom jeweiligen Regelungsthema ab. Manche Systeme werden themenübergreifend einsetzbar sein, andere sich sehr speziell auf den zu regelnden Bereich beziehen.

Für den Kodex zum „Umgang mit persönlichen Informationen und Daten in sozialen Netzwerken" könnte ein Anreizsystem in Form eines Zertifikates oder eines Siegels geschaffen werden. Dieses erhält, wer die Regeln des Kodex einhält, es kann bei Regelverstößen wieder entzogen werden. Das Anreizsystem ist über diesen Fall hinaus geeignet, für andere Anbieterkodizes in anderen Regelungsfeldern und Branchen eingesetzt zu werden. Auf diese Weise kann auf Dauer eine Bewertungsinstanz mit hoher Glaubwürdigkeit entstehen.

Der Rat überwacht die Einhaltung des Kodex durch die Anbieter. Stellt er wiederholte Verstöße fest oder zeigt sich, dass sich das Regelungsthema als nicht für die Regulierung durch einen Digitalen Kodex geeignet erweist, kann er dem Gesetzgeber gesetzlich-regulatorische Maßnahmen empfehlen.

Wenn im Wege der Evaluierung und durch die Empfehlung des Rates festgestellt wird, dass geltende Regelungen einer Problemlösung oder Erstellung eines Teilkodex im Wege stehen, so empfiehlt der Rat dem Gesetzgeber, diese Regelungen zu ändern oder aufzuheben.

4.2 Modell B: „Moderierter digitaler Straßenkampf"

Kurzbeschreibung

Das Modell dient dazu, einen Digitalen Kodex oder mehrere Digitale Kodizes auf dem Weg über Massenbewegungen auf den Weg zu bringen. Solche Bewegungen gehen, wenn überhaupt, derzeit von den Nutzern direkt aus und/oder werden durch einzelne Akteure der Zivilgesellschaft (NGOs) unterstützt. Das Internet bietet im Prinzip die Möglichkeit, massenhafte Bewegungen entstehen zu lassen. In sozialen Netzwerken beispielsweise können Forderungen der Nutzer dadurch wirkmächtig werden, dass sie von vielen Nutzern geteilt werden.

> **„Soziale Netzwerke können auch als Organisation der Nutzer benutzt werden. Ein Beispiel dafür sind die Austritte und Proteste, als Facebook das geistige Eigentum über die Nutzerinhalte reklamieren wollte. Über Facebook kann man sich organisieren und andere Unternehmen an den Pranger stellen. Sie sind ein Beitrag zur Relativierung der Machtasymmetrie zwischen Unternehmen und Verbrauchern, da Letztere eine Möglichkeit haben, sich selbst zu organisieren: das soziale Netz als nutzerorganisierende Plattform."**
>
> **Patrick von Braunmühl,** Geschäftsführer des Vereins Selbstregulierung Informationswirtschaft (SRIW), Auftaktworkshop, 03.06.2013

Bislang sind solche Bewegungen jedoch nur vereinzelt aufgetreten. Es ist zu vermuten, dass viele Bewegungen angestoßen werden, aber zu keinem Erfolg führen. Dies kann unterschiedlichste Gründe haben, etwa, dass das Thema nicht wichtig genug ist, dass die falschen Mittel oder die falsche Ansprache gewählt wurden usw. Auffällig ist zudem auch, dass Massenbewegungen im Netz eher darauf abzielen, etwas zu verhindern – wie beispielsweise die ACTA-Proteste oder diejenigen gegen die Vorratsdatenspeicherung –, als dass eigene Forderungen aufgestellt würden, deren Umsetzung verlangt wird. Ein Digitaler Kodex oder etwas, dass eine solche Bezeichnung verdienen würde, ist bis heute ersichtlich weder gefordert noch durchgesetzt worden.

Das Modell dient dazu, die Betroffenen dabei zu unterstützen, sich selbst zu helfen. Zu diesem Zweck sollen sie dabei unterstützt werden, gesellschaftlich relevante Themen zu ermitteln, konkrete Forderungen an die Adressaten zu formulieren und mit Nachdruck vorzubringen.

> **„Wir brauchen einen ADAC für das Internet. Dieser fehlt bisher, und das spürt man an vielen Punkten. Wir brauchen eine Bürgerbewegung, die dazu führt, dass sich Interessenorganisationen der Bürger entwickeln, die das Ungleichgewicht zwischen Wirtschaft, Politik und den Nutzern in der digitalen Welt ausgleichen."**
>
> **Dirk von Gehlen,** Leiter Social Media bei der Süddeutschen Zeitung, Konsultation

Das Modell basiert dabei auf der Annahme, dass es möglich ist, die Bürger und/oder Zivilgesellschaft dabei zu unterstützen, ihre Forderungen gegenüber mächtigen Akteuren, wie dem Staat oder den Internet-Unternehmen, zu formulieren und durchzusetzen. Die Mittel, um dies zu erreichen, liegen in diesem Modell darin, dass Regelungsbedarfe ermittelt und dann unter Einbeziehung von Akteuren aus der Zivilgesellschaft konkrete Forderungen an den jeweiligen Adressaten erarbeitet werden. Die gefundenen Formulierungen wären auf ihre Konsensfähigkeit und Realitätsnähe hin zu untersuchen und würden dann gezielt in technische Systeme eingespeist, über die sie aufgenommen und massenhaft weiterverbreitet werden können.

> **„Der Prozess an sich ist ein wichtiger Bestandteil für einen Kodex. Es geht nicht so sehr darum, Regeln aufzustellen, die dann ad hoc zu befolgen sind, sondern die Aushandlungsprozesse für Verhaltensregeln müssen auch im Alltag stattfinden."**
>
> **Dr. Malte Ziewitz,** Soziologe an der New York University, Interview

Im Unterschied zum erstgenannten, institutionalisierten Modell ist bei einer solchen Vorgehensweise offen, ob ein Kodex entsteht, wie er aussieht oder ob er letztlich angenommen und umgesetzt wird.

> **„Wie geht man am besten vor? Herkömmlich strukturierte Ansätze sind ausreichend vorhanden. Mir scheint ein moderierter ‚digitaler Straßenkampf' eine reizvolle Variante zu sein, um neue Wege zu beschreiten."**
>
> **Matthias Kammer,** Direktor des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI), 3. Expertenworkshop, 27.01.2014

> **„Beim Modell des digitalen Straßenkampfes sehe ich die Schwierigkeit, wesentliche Probleme zu identifizieren. Denn nicht selten finden – insbesondere – die Themen ihren Weg in die breite Öffentlichkeit, die sensationell und nicht zwangsläufig auch relevant sind."**
>
> **Dr. Eva Flecken,** Stabsstelle Digitale Projekte, Netz- und Medienpolitik bei der Medienanstalt Berlin-Brandenburg (mabb), 3. Expertenworkshop, 27.01.2014

Wer entwickelt in Modell B den Kodex, macht ihn bekannt und setzt ihn durch?

Die Initialzündung für einen Digitalen Kodex kann von Nutzervereinigungen oder anderen Einrichtungen – zum Beispiel einem Forschungsinstitut, einer NGO oder einem Unternehmen – ausgehen (nachstehend „Initiator" genannt). Das Konzept erfordert nicht, eine spezielle Struktur neu zu erschaffen. Es ist auch nicht auf eine bestimmte Institution ausgerichtet, sondern beschreibt lediglich einen Prozess, der von unterschiedlichen Akteuren angestoßen und durchgeführt werden kann. Wesentliche Voraussetzung ist, dass der Akteur die notwendigen Mittel in finanzieller und personeller Hinsicht aufbringen kann, um den Prozess entsprechend durchführen zu können.

Der Grundgedanke liegt darin, im Rahmen eines zentral oder innerhalb eines Netzwerks initiierten und koordinierten Prozesses Regelungsbedarfe aufzudecken, in Zusammenarbeit mit relevanten Akteursgruppen Forderungen zu formulieren und dabei Unterstützung zu leisten, ihnen möglichst großen Nachdruck zu verleihen. Dieser Prozess kann schließlich in einem Digitalen Kodex münden oder in einer anderen Form von (Selbst-)-Regulierung.

Die Bekanntmachung und Durchsetzung der Forderungen obliegt den Bürgern/Nutzern selbst. Ihnen

werden – eingehend evaluierte und sorgfältig formulierte – Forderungen zur Verfügung gestellt, die sie dann selbst zum Ausdruck bringen können. Wird den Forderungen durch die Masse an Unterstützern genügend Nachdruck verliehen, kann und wird dies vermutlich die Adressaten zu einem bestimmten Verhalten bewegen. Der Prozess basiert daher auf dem Grundprinzip der „Hilfe zur Selbsthilfe".

Wie entsteht ein Digitaler Kodex in Modell B?

Der Initiator ermittelt eine Problemlage mit gesellschaftlicher Relevanz, zum Beispiel ungeregelte oder unbefriedigend regulierte Bereiche mit Gesellschaftsbezug. Diese mögen angesichts der öffentlichen und/oder politischen Diskussion offensichtlich sein. Sie können sich aus Hinweisen der Betroffenen, der Medien oder auch aus speziellen Kenntnissen des Initiators ergeben, zum Beispiel Branchenkenntnis, Wissen über soziale Umstände oder rechtliche Verhältnisse. Auf welchem Weg der Initiator ein Thema identifiziert, ist nicht entscheidend.

> **„Die Themen müssen die Gefühle der breiten Masse ansprechen und dabei sehr konkret formuliert sein. Ein Beispiel für ein solches Thema wäre: ‚Meine Daten sind Geld' oder ‚Daten als Währung'. Die Zielrichtung sollte dabei nicht unbedingt Empörung sein, sondern auch Begeisterung, sich für das Thema einzusetzen bzw. ein Problembewusstsein zu entwickeln. Positive Emotionalisierung wäre hier das Stichwort."**
>
> **Prof. Dr. Rüdiger Grimm,** Professor für IT-Riskmanagement im Fachbereich Informatik an der Universität in Koblenz, 3. Expertenworkshop, 27.01.2014

Entscheidend ist, dass der Initiator das – unter Umständen vermeintliche – gesellschaftliche Problem auf seine reale Relevanz untersucht, bevor weitere Maßnahmen ergriffen werden. Bevor der Initiator sich dafür entscheidet, bei der Entstehung eines Digitalen Kodex unterstützend tätig zu werden, muss er durch Meinungsumfragen oder andere wissenschaftliche Methoden verifizieren, dass es sich hierbei um ein reales Problem handelt, für dessen Behebung sich die betroffene Akteursgruppe auch aktiv einsetzen würde. Wie weitgehend der Initiator diese Evaluierung betreibt und mit welchen Methoden, hängt im Wesentlichen von seiner eigenen Risikoabschätzung dahingehend ab, ob sich sein Engagement lohnt. Handelt es sich letztlich nur um ein Scheinproblem, wird seine Initiative scheitern, zum Beispiel, weil der gesellschaftliche Leidensdruck nicht hoch genug ist, um ausreichend Unterstützer zu finden.

Das Maß der hierfür erforderlichen Untersuchungen wird auch vom Thema abhängen. Dass sich beispielsweise viele Nutzer jedenfalls im Grundsatz für einen Digitalen Kodex von Facebook hinsichtlich des Umgangs mit ihren persönlichen Informationen und Daten aussprechen und im Zweifel auch einsetzen würden, mag einigermaßen vorhersehbar sein. Ob sich dagegen für eine Forderung nach der Umsetzung bestimmter Standards bei der Datenmigration von einem Anbieter zu einem anderen ebenfalls eine kritische Masse an Nutzern einsetzen würde, ist fraglich.

Hat der Initiator über die vorgenannten oder andere Methoden belastbare Informationen über die Relevanz des Problems, dessen konkreten Inhalt und die Bereitschaft zur aktiven Unterstützung erlangt, gilt es, entsprechende Forderungen zu formulieren. Hierin liegt eine besondere Herausforderung. Da das Ziel darin besteht, eine Massenbewegung von Individuen in Gang zu setzen, ist die Zielgruppe sehr inhomogen. Gerade in Bezug auf komplexe Fragen liegt die Schwierigkeit darin, „massenkompatible" und verständliche Formulierungen zu finden, die möglichst viele Unterstützer finden und die trotzdem sinnvoll und für die Adressaten in ihrem Gehalt umsetzbar sind. Bei der Erarbeitung und Abstimmung der Formulierungen empfiehlt es sich, potenzielle institutionelle Unterstützer – insbesondere NGOs aus dem Bereich der digitalen Zivilgesellschaft oder Verbraucherorganisationen – einzubeziehen. Deren Unterstützung wird letztlich gebraucht werden, um die kritische Masse zu erreichen und den notwendigen Druck aufzubauen.

Hat der Initiator – gegebenenfalls gemeinsam mit einflussreichen potenziellen institutionellen Unterstützern – Formulierungen gefunden, kann er deren

Validität durch weitere Meinungsumfragen oder ähnliche Methoden erneut überprüfen und entsprechend anpassen.

Schließlich muss der Initiator, unter Umständen mit seinen institutionellen Unterstützern, die Verbreitung der gefundenen Forderungen anstoßen und – soweit möglich – unterstützen. Um hier möglichst effizient vorzugehen, ist im Rahmen des Prozesses zu untersuchen, welche Mittel im jeweiligen Fall besonders geeignet erscheinen, um möglichst viele Unterstützer zu finden und um möglichst großen Druck auf den jeweiligen Adressaten zu erzeugen. Hier ergeben sich vielfältige Varianten, die vom Thema, den Adressaten und anderen Umständen abhängen.

Beispielsweise mögen Forderungen, die sich auf einen einzigen Anbieter richten, besonders effektiv sein, wenn sie sich auf dessen eigenen Systemen verbreiten. Im Beispiel eines Kodex für den Umgang mit persönlichen Informationen und Daten, der sich vor allem an Facebook richtet, wäre es etwa im Zweifel ratsam, eine entsprechende Landing-Page auf dem Netzwerk zu gründen und von dort gezielte Aktivitäten zu entfalten. Diese Aufgabe könnte der Initiator selbst oder ein kooperierender institutioneller Unterstützer übernehmen. Sollen sich die Forderungen dagegen an den Bund oder eine bestimmte Bundesbehörde richten, wären andere Mittel vorrangig, beispielsweise Systeme zur automatisierten Verschickung von Abgeordnetenanfragen oder Ähnliches.

Ob, in welcher Weise und mit welchem Inhalt die Forderungen letztlich als Digitaler Kodex der Adressaten umgesetzt werden, liegt in diesem Modell nicht beim Initiator oder seinen Verbündeten. Ebenso wenig kann er Einfluss darauf ausüben, ob der Kodex eingehalten wird, oder gegen Verstöße vorgehen.

Wie sieht der Digitale Kodex in Modell B aus?

Angesichts der Eigenheiten des Modells sind viele Varianten denkbar, in denen sich das Engagement des Initiators und die Forderungen der Betroffenen letztlich realisieren. Die eigentliche Umsetzung liegt im Ermessen des oder der jeweiligen Adressaten.

Schon die Forderungen, die im Rahmen des Prozesses entstehen, können sehr unterschiedlich sein. Sie können darauf abzielen, dass ein Anbieter seine Geschäftsbedingungen ändert, eine Gruppe von Anbietern sich auf einen Verhaltenskodex einigt oder der Gesetzgeber neue Regelungen einführt. Auch sind Mischformen denkbar, etwa dahingehend, dass vom Staat gefordert wird, bestimmten Anbietern im Ausgleich für eine – eigentlich ihren Interessen widersprechende – Änderung ihrer Geschäftsbedingungen steuerliche oder regulative Vorteile anzubieten. Entsprechend vielfältig sind die Umsetzungsmöglichkeiten.

Wie wird ein Kodex in Modell B wirkmächtig?

Ebenso vielfältig wie die Umsetzungsmöglichkeiten eines in diesem Prozess entstehenden Kodex sind die Mechanismen, die ihm zur Wirkmacht verhelfen können.

Das Modell setzt darauf, die Adressaten der jeweiligen Forderungen zu einem Verhalten zu bewegen. Häufig wird es sich um ein Verhalten handeln, das den eigenen Interessen des Adressaten zuwiderläuft – ansonsten hätte er sich im Zweifel schon selbst hierfür entschieden.

Das entscheidende Mittel zur Herstellung von Wirkmacht ist in diesem Modell die Macht der massenhaften Meinungsäußerung. Die Herausforderung liegt darin, durch einen koordinierten Prozess möglichst viele Anreize zum Mitmachen zu schaffen, damit sich die Betroffenen letztlich selbst helfen können.

> **„Werte sind im digitalen Raum prekär geworden (Mobbing, Geschäftsgeheimnisse etc.). Welches sind also die geltenden Werte im Netz? Was ist die Ökologie der Daten? Was heißt Datensouveränität von Gruppen und Einzelnen? Was muss ich von Unternehmen verlangen können? Hier ist viel Spielraum für die aktuelle Situation zwischen dem, was passiert, und dem, was man machen könnte. Hier müssen konkrete Forderungen formuliert werden, die in einem zweiten Schritt institutionell abgesichert werden müssten."**
>
> **Thorsten Schilling,** Leiter des Fachbereichs Multimedia der Bundeszentrale für politische Bildung in Bonn und Berlin (bpb), 3. Expertenworkshop, 27.01.2014

INTERVIEW MIT DR. MALTE ZIEWITZ

Regeln werden immer irgendwie ausgehandelt

? Sie haben als Wissenschaftler sehr viel zum Thema Bewertungssysteme gemacht. Was ist das eigentlich genau?

Malte Ziewitz: Heutzutage gibt es so gut wie nichts, was man nicht bewerten kann im Internet. Hotels, Bücher, Waschmaschinen, Ärzte, Rechtsanwälte, Exfreunde, Restaurants, Frisuren, Lehrer – immer öfter werden Nutzer nach einem Werturteil gefragt, das dann auf einer Webseite veröffentlicht wird. Wie war der Mathe-Professor? War das Buch anständig verpackt? Würden Sie diese Pizzeria weiterempfehlen? Das geschieht meistens im Namen von hehren Zielen. So sollen Nutzerbewertungen zum Beispiel Transparenz schaffen, die Verantwortlichen zur Rechenschaft ziehen oder den Ungehörten Gehör verschaffen. In der Praxis sieht das häufig etwas anders

Dr. Malte Ziewitz

ist Postdoctoral Research Fellow am Department of Media, Culture, and Communication und dem Information Law Institute der New York University. Sein Interesse gilt vor allem alltäglichen und nicht offensichtlichen Formen von Regulierung und Governance in digital vernetzten Umgebungen. In seiner Dissertation beschäftigte er sich mit der Rolle von Bewertungsplattformen im Gesundheitswesen und dem Suchmaschinenmarketing, die er in einer Reihe von Fallstudien ethnografisch untersuchte. Dazu kommen Arbeiten zur Vermachtung und Politisierung von Algorithmen, der Geschichte und Performativität von Internet-Governance-Diskursen, dem Potenzial von „crowd wisdom“ in der Regulierung, den Herausforderungen von „differential privacy“ in der Analyse sozialwissenschaftli-

Foto: Sarvenaz Bakhtiar

aus. Und genau das ist es, was mich interessiert: Was passiert, wenn Dienstleistungen, Produkte und Menschen auf einmal öffentlich bewertet werden? Wie bringt man so ein System zum Laufen? Und wie verlagern sich Machtverhältnisse, Probleme und Verantwortlichkeiten in der alltäglichen Nutzung?

cher Datensätze und das ESRC-geförderte „How's My Feedback?"-Projekt. Malte Ziewitz hat in Hamburg (1. Juristisches Staatsexamen), Harvard (M.P.A.) und Oxford (D. Phil.) studiert. Im Juli 2014 beginnt er als Assistant Professor am Department of Science & Technology Studies der Cornell University.

? Haben Sie möglicherweise ein paar allgemeine Erkenntnisse, welche Voraussetzungen vorliegen müssen, damit sich Leute an solchen Bewertungssystemen beteiligen? Ist das nur persönliche Betroffenheit, oder geht es auch um Usability?

MZ: Die Beteiligung ist in der Tat ein großes Problem für viele Betreiber. Das hat sich auch in meinen ethnografischen Studien gezeigt. Ein Schwerpunkt meiner Arbeit war Patient Opinion, ein unabhängiges Social Enterprise, das 2005 in Großbritannien gegründet wurde (www.patientopinion.org.uk). Patient Opinion hat sich zum Ziel gesetzt, das britische Gesundheitswesen und damit vor allem den National Health Service (NHS) zu verbessern. Das soll dadurch geschehen, dass Patienten, Angehörige und Mitarbeiter die Möglichkeit haben, auf der Patient-Opinion-Webseite ihre Erfahrungen mit Krankenhäusern und bestimmten anderen Gesundheitsdiensten zu veröffentlichen.

Nun ist es aber nicht selbstverständlich, dass sich Leute, in diesem Fall Patienten, zu einer Webseite begeben und dort aufschreiben, was gut und was schlecht gelaufen ist. Das ist harte Arbeit. Sie müssen sich hinsetzen und eine kleine Geschichte schreiben. Sie müssen sich damit wohlfühlen, diese Geschichte unter einem Pseudonym zu veröffentlichen und womöglich doch erkannt zu werden.

Ich hatte am Anfang meiner empirischen Feldarbeit die Vorstellung, dass das Management solcher Plattformen vor allem eine technische Herausforderung ist. Dem war aber nicht so. Was das Team von circa acht bis zehn Leuten da wirklich macht, hat weniger mit Internet und Web zu tun als mit Marketing und einer gehörigen Portion Idealismus. Ein Großteil der Arbeit bestand darin, durch das Land zu reisen, mit Patientengruppen zu reden, bei Funktionären und Politikern vorzusprechen, Workshops in Krankenhäusern zu veranstalten. Das Patient-Opini-

REGELN WERDEN IMMER IRGENDWIE AUSGEHANDELT

on-Team nutzte dafür alle möglichen Kanäle. Das waren neben den Reisen vor allem eine aktive Twitter-Präsenz, gelegentliche Gastbeiträge in großen Zeitungen, Vorträge auf Konferenzen, Flyer in Wartezimmern und so weiter. Das ist ein Riesenaufwand.

? Wie sehen Sie das Verhältnis zwischen Recht und Technik? Ist das Recht der bestimmende Faktor oder die Technik? Durch technische Voreinstellungen kann man sehr viel beeinflussen. Hat das Recht da überhaupt eine Chance?

MZ: Meine Erfahrung ist, dass man Recht und Technik zwar analytisch ganz gut auseinanderhalten kann. In der Praxis ist das aber schwer bis unmöglich. Was wir in der Regulierungstheorie als rechtliche und technische Aspekte verstehen, ist praktisch oft miteinander verschränkt. Voreinstellungen oder technisches Design spielen natürlich eine Rolle. Sie entstehen aber nicht im luftleeren Raum.

Nehmen Sie das Beispiel Patient Opinion. Jede Bewertung wird vor ihrer Veröffentlichung vom Team moderiert. Das heißt, je nach Bedarf wird der Text des Postings vom Team so redigiert, dass er bestimmte Anforderungen erfüllt. Dabei spielt natürlich das englische Haftungsrecht eine große Rolle, ist aber keinesfalls allein entscheidend. Es geht vielmehr darum, den bestmöglichen Kompromiss zwischen den vielen relevanten Lesarten und Nutzergruppen zu finden: Die Autoren sollen nicht zensiert werden, die Mitarbeiter im Krankenhaus nicht beleidigt sein, ein Besucher der Webseite sollte gleich verstehen, um was es geht, ein klagefreudiger Anwalt sollte keinen Grund haben, aktiv zu werden, und in die Datenbankarchitektur muss es auch noch passen mit den richtigen Tags und Stichwörtern.

Sowohl Technik als auch Recht sind also nur ein Gedanke unter vielen, und sie treten in dieser reinen Form nur äußerst selten in Erscheinung. Natürlich gibt es für die Moderation interne Richtlinien, eine sogenannte „editorial policy". Diese Regeln wirken aber weniger als konkrete Handlungsanweisung, sondern vielmehr als rhetorische Legitimation. Wenn zum Beispiel jemand mit einem moderierten Posting nicht einverstanden ist, ist es ganz praktisch, sagen zu können: „Sorry, aber unsere Editorial Policy verlangt das."

? Glauben Sie, dass wir in Deutschland zusätzliche gesetzliche Regelungen brauchen?

MZ: Meine empirische Forschung hat sehr viele meiner Annahmen über Regulierung auf den Kopf gestellt. Der Regulierungsdiskurs basiert auf dem Gedanken, dass man Probleme allgemein definieren und angehen kann. In der Praxis ist es so, dass es zwar viele Probleme gibt, dass diese aber oft nur schwer zu verallgemeinern sind. Um beim Beispiel von Patient Opinion zu bleiben: Natürlich beschweren sich die Mitarbeiter manchmal, dass das Libel Law (Ehrschutz) in England sehr strikt ist und man das eigentlich lockern könnte. Auf der anderen Seite ist aber die außergewöhnliche Sorgfalt und Fairness, mit der sich das Team um einzelne Bewertungen

> **Sowohl Technik als auch Recht sind also nur ein Gedanke unter vielen.** Dr. Malte Ziewitz

kümmert, auch sein Markenzeichen.

Das Problem „Gesetzliche Regelungen – ja oder nein" basiert letztlich auf einer Beschreibung, die nicht aus den spezifischen Zusammenhängen der Praxis kommt, sondern aus einem Regulierungsdiskurs, der sich in weiten Teilen selbst trägt. Viele der Regeln funktionieren wunderbar in Policy-Meetings, Positionspapieren und Debatten. Nur erfüllen sie dort häufig ganz andere Zwecke, als wir uns das in der Praxis vorstellen.

? Im Netz haben sich Verhaltensweisen herausgebildet, die nicht rechtlich festgeschrieben sind. Ist das die adäquate Art und Weise, wie Regeln gefunden und festgelegt werden sollen? Ist das ein festes Regelwerk, oder verändert sich das?

MZ: Wie bei jedem Werkzeug kommt es darauf an, wie man es benutzt. Allein unsere Vorstellungen von einer „Regel" sind ja schon sehr vielschichtig. Eine sehr populäre Sichtweise ist zum Beispiel, sich Regeln als eine Art moralischen Wegweiser vorzustellen, den Leute verinnerlichen, um dann in konkreten Situationen danach zu handeln. Eine andere Möglichkeit ist, Regeln vor allem als Beschreibung zu sehen, die regelmäßiges oder typisches Verhalten wiedergibt. Außerdem werden Regeln häufig als praktisches Werkzeug benutzt, mit dem wir bestimmtes Verhalten relativ einfach als gut oder schlecht beschreiben können. Das ist ein bisschen so wie in den Wirtschaftswissenschaften, wo es nicht so sehr darum geht, ob die ökonomischen Modelle nun mit irgendeiner Wirklichkeit übereinstimmen, sondern vielmehr dem Betrachter ein probates Mittel an die Hand geben, um zu sagen, was effizient ist und was nicht.

Die Medienwissenschaftlerin Danah Boyd hat gerade ein Buch veröffentlicht („It's Complicated: The Social Lives of Networked Teens"), das sich mit Teenagern in sozialen Netzwerken auseinandersetzt. Was sie dabei herausbekommen hat, ist faszinierend – vor allem, weil sie einige weitverbreitete Annahmen über die Gefährdung von Jugendlichen kritisch hinterfragt. Boyd zeigt zum Beispiel, dass ihre Gesprächspartner in Sachen Datenschutz und Privacy auf Social-Networking-Seiten eine Vielfalt an eigenen Strategien entwickelt haben. Diese drehen sich aber nicht so sehr um grobe Kategorien wie „öffentlich" oder „privat", sondern um die Möglichkeit, bestimmten Äußerungen und Interaktionen einen eigenen Sinn zu geben. Das findet nicht auf der Ebene von universellen Regeln, staatlicher Kontrolle oder einem Kodex statt. Der würde vielleicht sogar wohlwollend ignoriert werden. Stattdessen haben sie ihre kleinen Tricks im Alltag, die wir besser verstehen müssen. Was steckt dahinter, wenn ein Jugendlicher regelmäßig die Postings des Vortages löscht? Warum deaktivieren manche Nutzer ihren Account nach jeder Session, anstatt sich auszuloggen? Solche Praktiken sind schwer mit einem Kodex zu fassen.

? Würde es helfen, wenn ein Kodex zwischen mehreren Parteien ausgehandelt wird?

REGELN WERDEN IMMER IRGENDWIE AUSGEHANDELT

> **Es geht nicht darum, einmal Regeln zu schaffen, die dann für die Ewigkeit angewendet werden.** Dr. Malte Ziewitz

MZ: Das würde im Prinzip nichts ändern. Regeln werden ja immer irgendwie ausgehandelt – sogar und vor allem dann, wenn sie einmal festgeschrieben waren. Das ist ein häufiges Missverständnis, dass Regeln deterministisch funktionieren. Wenn ich dies und das tue, dann passiert dies und das. Dieses Wenn-Dann suggeriert, dass da irgendwie ein Automatismus am Werk ist. In der Praxis funktioniert das aber nicht so. Was zum Beispiel sind „persönliche" Daten? Wo fängt Cyberbullying an, wo hört die Meinungsfreiheit auf? Keine Regel ohne Aushandlungsprozess.

Das verweist übrigens auf eine weitere sehr produktive Funktion von Kodizes: Es geht nicht darum, einmal Regeln zu schaffen, die dann für die Ewigkeit angewendet werden. Vielmehr ist das Arbeiten an Regeln selbst ein Instrument, um sich mit schwierigen Fragen auseinanderzusetzen. Schon in der Diskussion über einen Kodex können viele Sachen zur Sprache gebracht werden, die sonst wahrscheinlich nur schwer zu thematisieren wären.

? Das sind alles eher weiche Funktionen eines Kodex. Könnte denn ein Digitaler Kodex Recht tatsächlich ersetzen, wenn es um richtig harte Sachen geht, zum Beispiel um Datenschutz? Wenn wir nicht nur über Beteiligung sprechen, sondern über den Schutz elementarer persönlicher Daten? Oder braucht man da auf jeden Fall das Recht?

MZ: Das kommt darauf an. Wenn man von Recht spricht, verbirgt sich dahinter ja ein komplexes Gefüge von Institutionen, Rollen, Gewohnheiten, Praktiken und Menschen, die oft über Jahre trainiert wurden, „rechtlich" zu denken. Recht ist also nicht nur das, was im Gesetz steht, sondern vor allem auch eine handfeste Infrastruktur. Ein Text allein, ein Dokument, ein Digitaler Kodex kann da natürlich nicht ohne Weiteres mithalten. Auf der anderen Seite gibt es aber auch Institutionen, die vielleicht mit einem Kodex mehr anfangen können. Familien, Freunde, Lehrer, Kollegen sind da häufig viel näher dran.

5. Epilog

Die Ergebnisse zeigen, dass die Frage nach der Zuweisung von Verantwortung im Internet und entsprechenden Instrumenten zur Kodifizierung und Durchsetzung von Regeln eine hohe Komplexität besitzt. Es gibt keine universell anwendbaren Blaupausen, sondern es ist bei der Formulierung eines Digitalen Kodex insbesondere eine Differenzierung nach Art der Plattform und inhaltlichem Anwendungsbereich notwendig. Dann ist die Frage seiner Durchsetzung wesentlich – wie kann erreicht werden, dass ein Kodex wirkmächtig wird? Und schließlich ist zu klären, wie ein Kodex entsteht und welche Akteure sich beteiligen bzw. beteiligt werden.

Die Entwicklung eines Digitalen Kodex für den Umgang mit persönlichen Daten auf Kommunikationsplattformen könnte ein sehr lohnendes Unterfangen sein, weil dadurch zentrale und aktuelle Fragestellungen exemplarisch adressiert werden. Die aktuellen Diskussionen um Geschäftsmodelle und Marktmacht großer sozialer Netzwerke zeigen, wie virulent das Thema ist. Gleichzeitig werden dabei Regulierungsbereiche berührt, die auch mit anderen Domänen, das heißt Ausprägungen von Plattformen, Akteursgruppen und Inhalten, eine relevante Schnittmenge besitzen.

Auch wenn das Internet aus Sicht einer breiten Anwendung erst 20 Jahre alt ist, hat es doch schon wesentliche Veränderungen in allen Lebensbereichen bewirkt, bei der privaten Kommunikation, bei Geschäftsprozessen der Wirtschaft und teilweise auch bei der politischen Partizipation. Ein Prozess der Aushandlung von Digitalen Kodizes kann in diesen konkreten Bereichen zu klaren Verantwortlichkeiten führen. Darüber hinaus würde aber auch ein Reflexionsraum über allgemeine Prinzipien eröffnet, wie die neuen digitalen Medien wirken, welche Risiken bestehen und welche Chancen sich eröffnen.

Annex

In diesem Annex befinden sich die drei zentralen Themenpapiere des Projekts im Volltext. Der Leser kann so bei Interesse noch einmal tiefer beziehungsweise kompakter in einzelne Themenbereiche einsteigen und die Texte zusammenhängend lesen. Ebenso finden sich hier die Zusammenfassungen der öffentlichen Veranstaltungen im Juli 2013 in München und im November 2013 in Hamburg mit den wesentlichen Inhalten der Keynotes und Diskussionen.

THEMENPAPIER: PLATTFORMEN UND DIE ROLLE IHRER BETREIBER IN BEZUG AUF VERANTWORTUNG IM INTERNET

Vorbemerkungen

Anlass dafür, Internet-Plattformen und ihre Betreiber als eigenen Schwerpunkt für die Frage nach der Sinnhaftigkeit eines „Digitalen Kodex" herauszugreifen, ist der Umstand, dass im Internet vor allem Plattformen diejenigen Orte sind, an denen sich Nutzer und andere Beteiligte in irgendeiner Weise aufhalten und verhalten. Vor allem dort können deshalb soziale Normen entstehen, wirksam werden und sich verändern.

Plattformen im Sinne dieses Textes sind alle mit dem Internet in Verbindung stehenden technischen Infrastrukturen, die grundsätzlich für eine Benutzung (zum Beispiel Zugriff, Einsichtnahme und Interaktion) auch durch andere als den Betreiber geeignet oder sogar vorgesehen sind. Soziale Medien und kollaborative Projekte werden damit genauso als Plattformen verstanden wie sonstige serverbasierte Infrastrukturen jeder Art (zum Beispiel Streaming-Plattformen, Blog-Dienste, Foto-Communitys und sonstige Angebote rund um „User Generated Content"), Cloud-Dienste sowie vergleichbare Angebote – unabhängig davon, ob es sich um Strukturen handelt, die rundfunkähnlich („one to many") oder interaktiv („many to many") organisiert sind. Bewusst ausgenommen sind die physische Kommunikations-Infrastruktur und ihre Betreiber (zum Beispiel Internet-Service-Provider und TK-Unternehmen).

A. Übergeordnete Fragen

In Bezug auf das Für und Wider eines „Digitalen Kodex" zum Umgang mit Internet-Plattformen und zur Rolle ihrer Betreiber stellen sich in erster Linie die folgenden übergeordneten Fragen:

- Welche sozialen Normen gibt es, wo fehlen (geeignete) Regeln, inwieweit birgt dieses Fehlen nennenswerte Risiken für die Beteiligten, und worin bestehen diese?
- Reicht ein Verhaltenskodex aus, um unerwünschte Entwicklungen zu vermeiden, und in welchen Bereichen kann sich ein solcher Kodex realistischerweise durchsetzen?
- Falls ein „Digitaler Kodex" konzipiert wird, wie kann er so ausgestaltet werden, dass er auch bei stetigem gesellschaftlichen und technischen Wandel Gültigkeit behält?

B. Subjekte und Spektrum der Betrachtung

Eine zentrale Rolle haben die Betreiber von Internet-Plattformen inne. Bei ihnen handelt es sich vor

allem um privatwirtschaftliche Unternehmen. Dieser Eigenschaft kommt in der Diskussion vielfach eine entscheidende Bedeutung zu. Einige der Ausführungen gelten jedoch genauso auch für die übrigen Plattformbetreiber, die keine Unternehmen sind.

Eine weitere wichtige Gruppe in der anzustoßenden Diskussion sind die Nutzer der Plattformen, und zwar je nach Kontext in verschiedenen Eigenschaften als Verbraucher/Konsument, Arbeitnehmer in einer durch das Internet geprägten Alltagswelt oder als Staatsbürger. Obwohl auch Institutionen Nutzer von Plattformen sein können, sind im Text überwiegend individuelle Nutzer gemeint.

Als dritter Akteur rückt der Staat in den Blick bzw. staatliche Stellen allgemein. Dem Staat kommt üblicherweise dann eine besondere Bedeutung zu, wenn es um die Kodifizierung und Durchsetzung von Regeln geht. Nicht selten hat er jedoch auch Eigeninteressen, die relevant sein können. Auch er steht in Beziehung sowohl zu den Internet-Plattformen und ihren Betreibern als auch den Nutzern.

C. Natur des Internets als wichtiger Teil der Ausgangslage

Die Befassung mit Internet-Plattformen findet in der Natur des Internets, in seiner Grundstruktur und Organisation, eine bestimmte Ausgangslage vor. Neben technischen Faktoren, wie der dezentralen Rechnerstruktur und der Verarbeitung aller im Internet verschickten Datenpakete, scheint für den anstehenden Kodex-Prozess insbesondere relevant zu sein, von wem das Internet betrieben wird. Dieses Netz ist keineswegs monolithisch, sondern wird gebildet aus der Gesamtheit der über die Welt gespannten und miteinander verbundenen Rechner-Netze sowie der darauf betriebenen Dienste. Es wird nicht nur hinsichtlich seiner physischen Ebene großenteils von privaten Akteuren betrieben. Auch auf allen weiteren Ebenen[1] spielen Unternehmen als Provider und Plattformbetreiber eine zentrale Rolle. Dadurch unterscheidet sich das Internet deutlich und mit spürbaren Konsequenzen von der physisch-analogen Welt. Im klassischen öffentlichen Raum, dem Straßen- und Verkehrsraum, leitet sich alles letztlich von staatlicher Gewährung ab. Wenn niemand sonst mehr zuständig ist, gibt es im öffentlichen Raum der analogen Welt eine Auffangzuständigkeit der öffentlichen Hand. Außerhalb privater Grundstücke gilt öffentliches Recht und nicht Privatrecht. Dagegen ist etwa ein Kaufhaus zwar auch ein öffentlich zugänglicher Raum, aber ein durchweg privater, denn ab der Türschwelle gilt das Hausrecht. Das Hausrecht der Betreiber privatwirtschaftlich betriebener Internet-Plattformen hat – genau wie das der Kaufhausbetreiber – nur lockere Verfassungsbindung. Es erlaubt daher viel tiefere Eingriffe in die Handlungsfreiheit der Menschen im Netz, als es dieselben Menschen sich im klassischen öffentlichen Raum gefallen lassen müssen.

Der Hausrechtsinhaber kann Dinge untersagen und erlauben, die im öffentlichen Raum nie in gleicher Weise untersagt/erlaubt werden könnten. Er kann Teilhabe untersagen und mittels zivilrechtlicher AGB nach Gutdünken Verhaltensregeln aufstellen. Anders als in genuin öffentlichen Räumen kann dem kein Recht auf Teilhabe entgegengehalten werden und kann sich niemand auf den Grundsatz der Gleichbehandlung berufen. Es sind die Plattformbetreiber, die mit ihren Angeboten diese virtuelle und doch sehr wirkliche Welt erzeugen. Sie sind die Architekten des digitalen Zeitalters. Soweit die Gleichsetzungen „architecture is law" und „code is law"[2] zutreffen, sind die Plattformbetreiber damit zugleich Gesetzgeber der digitalen Welt, wenn auch nicht die einzigen.

Obwohl im Zusammenhang mit dem Internet immer wieder Verkehrsvokabeln (wie Traffic, Datenautobahn usw.) verwendet werden, bewegen sich die Menschen im Internet – bildlich gesprochen – also durchweg im Kaufhaus und nicht auf der Straße, ist in der digitalen Welt vom Bürgersteig über die Transportmittel bis zu den (Daten-)Wolken fast alles privatwirtschaftlich organisiert. Abstrakt ausgedrückt: Mit Ausnahme der universitären Netz-Infrastrukturen und einiger staatlich betriebener Datendienste und öffentlich-rechtlicher Content-Plattformen gibt es im Internet so gut wie keinen im rechtlichen Sinne genuin öffentlichen[3] Raum, insbesondere nicht hinsichtlich

1 Siehe als eine Darstellungsweise unter mehreren die Schichten nach dem OSI-Modell: de.wikipedia.org/wiki/OSI-Modell.

2 L. Lessig: „Code is Law – On Liberty in Cyberspace", Harvard Magazine, Feb. 2000, siehe auch harvardmagazine.com/2000/01/code-is-law-html.

3 Obwohl es auch eine umgangssprachliche Konnotation hat, ist das Wort „öffentlich" hier im formaljuristischen Sinne gemeint.

derjenigen alltäglichen Dienste, die immer weiter in das Leben der Menschen hineinreichen. Elektronische Kommunikation, Cloud-Speicher, mobiles Internet, soziale Medien, Nachrichtenaggregation, Location-based Services, Web-Suche und vieles mehr gibt es fast ausschließlich aus der Hand privater Plattformbetreiber. Ähnlich wie der Sektor der Printpublikationen ist auch das Internet staatsfern organisiert und ebenso darauf ausgelegt, dass Pluralität und ein Gleichgewicht der Kräfte durch einen funktionierenden Wettbewerb gewahrt bleiben.

Darum ist es auch nicht überraschend, dass es in der Online-Welt keine echte staatliche Daseinsvorsorge gibt. Die meisten Segnungen des Netzes stehen unter dem Vorbehalt, dass Wohlwollen und Geschäftsmodelle privatwirtschaftlicher Unternehmen, der sogenannten „Gatekeeper", sie dauerhaft (mit-)tragen. Nur was diesen privatwirtschaftlichen Strukturen dient oder ihnen zumindest nicht schadet und daher ohne großen Ressourceneinsatz mitbetrieben werden kann, kann sich im Netz ungehindert entfalten. Solange die Online-Welt auf diese Weise nachhaltig betrieben wird, besteht für den Staat auch keinerlei Veranlassung, zum Erhalt des Internets mehr als indirekt regulativ in die Netz-Infrastrukturen und den Wettbewerb der Anbieter einzugreifen. Selbst für eigene Zwecke bedient sich der Staat oft der privat betriebenen Netz-Infrastrukturen, statt mit großem Aufwand eigene zu schaffen.

D. Diskussionsstränge für einen Kodex-Prozess im Einzelnen

Die folgende Diskussion bewegt sich entlang der Verantwortungs- und Verantwortlichkeitsverhältnisse, die es zwischen den oben unter B. benannten Beteiligten gibt.

1. Verantwortungsverhältnis zwischen Plattformbetreibern und Gesellschaft insgesamt

a) Besonderes Gewicht der Plattformbetreiber

Das Internet kommt nicht aus einer Hand, sondern aus den Händen vieler Anbieter, die in der Regel Plattformbetreiber sind (siehe dazu auch oben unter C.). Für die allermeisten Menschen gilt daher: Kein Netzzugang ohne Internet-Service-Provider, kein E-Mail-Postfach ohne Mail-Provider, kein privater Blog ohne Blog-Hoster, keine Cloud-Nutzung ohne Cloud-Dienste-Anbieter, keine Kommunikation über soziale Netzwerke ohne das Zutun ihrer Betreiber – im Falle browserbasierter Betriebssysteme nicht einmal irgendeine Reaktion des eigenen Rechners ohne Zutun eines ganz bestimmten Diensteanbieters. Die Wenigsten sind in der Lage, auch nur die einfachsten Internet-Dienste in Eigenregie auf eigener Hardware zu betreiben.

Das Angewiesensein auf Plattformen betrifft neben den Bürgern auch alle weiteren Internet-Nutzer in unterschiedlichem Umfang. Spätestens seit dem Cloud-Computing-Boom sind Plattformbetreiber in so gut wie allen Bereichen des digitalen Lebens und Wirtschaftens Teil des Geschehens.

Die zentrale Rolle der Plattformbetreiber macht sich dabei auf dreifache Art bemerkbar:

- Erstens hat durch die Umstellung zahlreicher Prozesse hin zu plattformbasierter Arbeit bereits die bloße Existenz bzw. der Fortbestand der jeweiligen Plattformbetreiber unmittelbare Auswirkungen auf alle Plattformnutzer.
- Zweitens besitzen die Plattformbetreiber aufgrund der meist nicht offengelegten Architekturen ihrer Plattformen eine überaus große technische und prozessuale Gestaltungsmacht.
- Drittens können Plattformbetreiber über die Ausgestaltung ihrer Nutzungsbedingungen eine nur teilweise gesetzlich beschränkte rechtliche Gestaltungsmacht ausüben.

Ob die Plattformbetreiber jeweils diese Rolle anstreben, sie als Belastung ansehen oder ihr gegenüber indifferent sind, kann an dieser Stelle dahingestellt sein. Denn allein aus den drei genannten Umständen ist bereits abzulesen, dass der große Einfluss der Plattformbetreiber, von denen so vieles abhängt, auch eine große Verantwortung mit sich bringt.

Dabei darf nicht außer Acht gelassen werden, dass der wirtschaftliche Erfolg eines privatwirtschaftlich handelnden Plattformbetreibers ein ebenso legitimes Unternehmensziel ist, wie es der Marktanteil eines Unternehmens in jeder Branche ist.

Auch die Nutzer- bzw. Kundenbindung ist für Plattformbetreiber nicht weniger zentral als für andere Unternehmen, und die Strategien, um diese Bindung zu erreichen, werden keineswegs verwerflich, nur weil es sich bei dem jeweils handelnden Unternehmen um einen Plattformbetreiber der digitalen Lebenswelt handelt. Dennoch hat Unternehmenshandeln im Internet oft ein wesentlich höheres Gewicht als in der analogen Welt, auch und gerade in Bezug auf die Bildung und Ausgestaltung sozialer Normen, da bereits der Rahmen möglichen Verhaltens vorgegeben wird: In der analogen Welt endet die unmittelbare Kontrolle eines Unternehmens über ein Produkt, das es verkauft, meist mit dem Verkauf und der Übergabe an den Kunden. Im Internet aber bleiben die Plattformen als Produkte in der Hand des Unternehmens, und die Kunden begeben sich als Nutzer in diese Produkte hinein. Der Umgang mit dem Produkt findet dauerhaft im geschützten Raum des Unternehmens statt, was den Unternehmen große Gestaltungsmacht verleiht.

Eine Person kann ein gekauftes Produkt zweckentfremden oder verschenken, kein Hersteller kann das unterbinden oder auch nur untersagen. Sie kann auch, um einen weiteren Verkehrsvergleich (wie oben unter C.) zu ziehen, durchaus bei Rot über eine Ampel gehen, auch wenn das ordnungswidrig sein mag. Dadurch jedoch, dass der digitale Raum großenteils erst durch die von Plattformbetreibern beherrschte Technik (Hard- und Software) geschaffen wird, können die Betreiber dafür sorgen, dass es nicht nur verboten ist, bei Rot zu gehen, sondern technisch gar nicht möglich. Allgemein geben die Funktionen, die eine Plattform anbietet, bereits teilweise vor, wie sich die Nutzer auf ihr verhalten können.

b) Plattformen als Katalysatoren einer Veränderung der Arbeitswelt

Die „Rationalisierung und Kommodifizierung des Selbstseins“[4] durch die Betreiber von Online-Plattformen – nicht zuletzt durch soziale Netzwerke – nimmt Dimensionen an, die noch vor wenigen Jahren kaum jemand vorhergesehen hat. Die durch diese Plattformen beförderte und zugleich auf sie angewiesene „soziale Wertschöpfung“[5] hat einen großen Raum im Erwerbsleben immer größerer Teile der Bevölkerung. Dies löst Verschiebungen aus, welche die Gesellschaft insgesamt erfassen, von der politischen Landschaft und den Gewichten in der Sozialpartnerschaft bis hin zu den Geldströmen.

Während die unmittelbare monetäre Wertschöpfung, die daraus folgt, in der Regel weitgehend bei den Betreibern der sozialen Netzwerke erfolgt und als Vermögenswert dort auch verbleibt, gibt es kaum übergeordnete Regelungsinstanzen und partizipieren die auf die Plattformen angewiesenen „Selbst-Unternehmer“ geringfügiger in direkter Form. Sie haben dafür aber in vielen Fällen unzweifelhaft einen zunächst nicht monetären, aber gegebenenfalls monetarisierbaren Sekundärnutzen, beispielsweise durch die Kontakte, die sie über die Netzwerke gewinnen, oder durch die Aufmerksamkeit, die ihnen zuteilwird. Zudem haben sie mit den neuen Netzwerken und Technologien Möglichkeiten zur Selbstentfaltung, über die früher – wenn überhaupt – nur ein Bruchteil der Bevölkerung verfügte.

Vieles an dieser Entwicklung ist ambivalent. Im Fall von Crowdsourcing-Geschäftsmodellen, die sich in den vergangenen Jahren ausdifferenziert haben, ist ein breites Spektrum von eher geringfügig entlohnten Modellen der Form „Humans as a service“ (HaaS) bis hin zu Marktplätzen für hoch spezialisierte Wissensarbeiter zu beobachten. Bei vielen Geschäftsmodellen sind dabei Konzentrationsprozesse zu beobachten (im Sinne von „Winner takes all“-Märkten) – Nutzer legen aus Effizienzgründen Profile bei möglichst wenigen Plattformen an, Plattformbetreiber versuchen, für möglichst jede Form von Nutzerwünschen eigene Dienste anzubieten, und Netzwerkeffekte führen zu einer stärkeren Bindung der Plattformnutzer. Im Gegenzug haben die Plattformbetreiber allerdings bei den vielen Gratisdiensten auch die Kosten allein zu tragen.

4 Eva Illouz „Metamorphosen des Kapitalismus - und seiner Kritik“, S. 235; gemeint ist das durch Internet-Mechanismen möglich gewordene Eingesogenwerden aller Aspekte der Persönlichkeit – auch und gerade der früher nur der Freizeit vorbehaltenen Anteile – in das Arbeitsleben als notwendige Anreicherung des eigenen wirtschaftlichen Marktwertes.

5 Tiziana Terranova meint damit jederzeitige professionelle Verfügbarkeit, die nur durch ein „Always On“ und entsprechende Kommunikationsplattformen möglich wird.

Es ergibt sich ein ambivalentes Bild auch hinsichtlich der Verantwortungsverteilung: Einerseits kann von Plattformbetreibern schwerlich verlangt werden, sie sollten auf Gestaltungsmacht durch Netzwerkeffekte und auf andere Vorteile freiwillig verzichten und damit der Konkurrenz das Feld überlassen. Andererseits ist es gängige Praxis, Anbieter von Produkten für die Folgen der von diesen Produkten ausgehenden Gefahren einstehen zu lassen. Wo also endet die Verantwortlichkeit (gerade der großen) Plattformbetreiber in Bezug auf das, was sie mit ihren Plattformen tun und was sie im Gegensatz dazu auf ihren Plattformen gar nicht erst zulassen? Wo beginnt die Verantwortlichkeit der Nutzer und der Gesellschaft insgesamt? Was ist bewusst und durch wen gestaltbar, und was ist schlicht irreversibler technischer bzw. wirtschaftlicher Fortschritt?

c) Zunehmende Aneignungstendenzen

Gerade in Bezug auf soziale Netzwerke ist zu beobachten, dass sich Plattformbetreiber neben den Daten, Kontakten und der Aufmerksamkeit ihrer Nutzer zunehmend auch die durch die Nutzer[6] erzeugten Inhalte direkt anzueignen versuchen oder bestrebt sind, sich zumindest eine monetarisierbare Teilhabe daran zu sichern.

Gemeint ist hier nicht in erster Linie der Wert personenbezogener Daten, auf die unter 2.a) noch eingegangen wird. Das, was den hier gemeinten Aneignungstendenzen unterliegt, geht auch noch deutlich über das hinaus, was gemeinhin als „User Generated Content" bezeichnet wird. Begehrt sind vielmehr sämtliche immateriellen Werte, die die Nutzer auf den Plattformen erzeugen – neben Werken im urheberrechtlichen Sinne („Intellectual Property") und Verhaltensprofilen sind dies beispielsweise auch die Anerkennung, die Nutzer sich erarbeiten, die Communitys, die sie bilden, die Playlists, die sie generieren, die Ideen, die sie preisgeben.

Erneut hat man es mit keiner eindeutigen Konstellation zu tun.[7] Einerseits kann es Unternehmen kaum verwehrt werden, die Gewinne zu realisieren, die ihre Plattformen hergeben. Schließlich stellt es in der Regel gerade die unternehmerische Leistung dar, dass die Plattformen überhaupt existieren und genutzt werden. Andererseits stellt die Aussicht auf Gewinn keinen Freibrief dar, und es wird allgemein akzeptiert, dass Vorteile nur insoweit gezogen werden, wie keine höherrangigen gesellschaftlichen Werte vorgehen. Hierzu zählen selbstverständlich auch die sozialen Normen einer Gesellschaft, die das wirtschaftliche Leben gleichermaßen betreffen wie alle übrigen Gesellschaftsbereiche.

Das führt zu weiteren konkreten Fragen, die im Verlauf des Prozesses zum „Digitalen Kodex" gegebenenfalls vertieft werden sollten: Was besagen diese sozialen Normen, und wann gehen sie als höherrangig im Zweifel vor? Wem „gehört" der *Clickstream*[8], der bei der Benutzung von Online-Plattformen entsteht, und wem sollte er gehören?

d) Technisch basierte Lenkungsmacht der Plattformbetreiber

Der Vormarsch der Online-Plattformen, die immer mehr den Alltag der oft beschworenen Wissensgesellschaft durchdringen, wurde in den Abschnitten C. und D.1.a) bereits teilweise dargestellt. Aus der daraus – so zumindest eine mögliche These – erwachsenden Verantwortung der Betreiber der Plattformen und den zugleich ebenso wirksamen wirtschaftlichen Gesetzen der Marktwirtschaft ergibt sich ein Spannungsfeld, in welchem sich die meisten Plattformbetreiber immer wieder neu positionieren müssen.

Während es auf der einen Seite legitime Machtinteressen zur Steuerung der eigenen Plattform, zur Kundenbindung und für den Schutz der eigenen Systeme vor Angriffen und Missbrauch gibt, können technische wie rechtliche Stellschrauben, die

6 Georg Franck, „Ökonomie der Aufmerksamkeit" (1998); gemeint ist eine Wirtschaftsordnung, in der nicht mehr Geld, sondern die Aufmerksamkeit der Menschen zum knappen und damit limitierenden Faktor für Entwicklung geworden ist.

7 Besonders interessant könnte es sein, zu diskutieren, ob bzw. inwieweit es sich bei der hier wieder aufscheinenden Uneindeutigkeit um einen möglicherweise durch die Plattformbetreiber kalkulierten Zustand handelt.

8 Der Clickstream ist die Sequenz der Links, die ein Nutzer auf einer Plattform oder beim Übergang zwischen Plattformen auf dem Internet anwählt. Da aus der Abfolge ein inhaltlicher Zusammenhang konstruiert werden kann, ist der Clickstream werthaltig.

den Plattformbetreibern zur Verfügung stehen, umgekehrt ihrerseits missbräuchlich etwa zur Ausforschung der Nutzer oder für eine sehr wirksame Zensur eingesetzt werden. Das gilt umso mehr, je weniger echte Alternativen die Nutzer jeweils haben, je stärker also die sogenannten „Netzwerkeffekte" sind. Je nach betrachtetem Sektor reicht die Spanne von starkem Wettbewerb zwischen Plattformanbietern bis zu Quasi-Monopolen, an denen Nutzer nicht vorbeikommen, wenn sie am digitalen Austausch teilhaben wollen.

Daneben sind zahllose Algorithmen am Werk, die auch inhaltlich massiven Einfluss darauf haben, womit sich die Menschen beschäftigen, welche Informationen ihnen von der Plattform geliefert werden[9], wovon sie überhaupt erfahren und wie sie darauf innerhalb der jeweiligen Plattformmechanik reagieren können. Hier erweitert sich auch die Betrachtung des Verhältnisses zwischen Plattformbetreibern und Gesellschaft auf das Verhältnis zwischen Staat, Plattformbetreibern und Bürgern, auf das unten noch eingegangen wird. Plattformbetreiber erhalten Eingriffsmöglichkeiten, die in ihrer Reichweite denen klassischer staatlicher Befugnisse kaum nachstehen, ohne dass die Plattformbetreiber dadurch zu quasistaatlichen Akteuren würden.

Es stellen sich insofern mehrere sehr grundsätzliche Fragen hinsichtlich der Positionierung der Plattformbetreiber: Gibt es überhaupt universelle, weltweit gültige soziale Normen, oder können diese zwangsläufig immer nur lokal Gültigkeit haben, zum Beispiel orientiert an Kultur- und Sprachräumen? Sind Phänomene wie „Filter Bubbles" real, und wenn ja, richten sie sich per se gegen bestimmte Interessen der Nutzer? Auch diese Fragen können im Verlauf des Prozesses zum „Digitalen Kodex" gegebenenfalls vertieft werden.

2. Verantwortungsverhältnis zwischen Plattformbetreibern und Nutzern

a) Datenschutz in sozialen Netzen

Personenbezogene Daten sind in manchen Bereichen des Netzes zunehmend Ware und Währung („Wer nichts bezahlt, bezahlt mit seinen Daten"), siehe dazu auch oben 1.c). Über diese Entwicklung wird viel geschrieben und polemisiert – allein eine offene Aushandlung dazu zwischen den Nutzern als „Datengebern" und den Plattformbetreibern als „Datennehmern" findet kaum statt. Stattdessen entstehen seitenlange AGB-Texte und versuchen Gesetzgeber, über genaue Anforderungen an Datenschutzerklärungen mehr Transparenz zu erreichen.

Doch auf diese Weise erfahren Nutzer allenfalls in kryptischen Worten, was mit ihren Daten in welchen Fällen passieren darf, sofern sie einwilligen. Um die Tragweite dieser Einwilligung aber wirklich erfassen zu können, müssten die Nutzer auch in die Lage versetzt werden, zu überblicken, warum mit ihren Daten in der geforderten Weise umgegangen werden soll. Es nützt einem Nutzer wenig zu erfahren, dass seine Daten „in Länder außerhalb des Europäischen Wirtschaftsraumes transferiert werden können", wie es in den Nutzungsbedingungen vieler Cloud-Dienste-Anbieter heißt. Soweit nicht bereits die legalistische Sprache solcher Regelwerke die rechtlichen Laien vom Weiterlesen abschreckt, wird dadurch jedenfalls nicht erklärt, welche Folgen gerade eine Verlagerung der Daten nach außerhalb des EWR bedeuten kann und warum das überhaupt mitgeteilt wird. Genaue Einblicke ins Räderwerk der Datenweiterverarbeitung werden in der Regel nicht gewährt, was unter dem Gesichtspunkt schützenswerter Betriebsgeheimnisse auch durchaus gerechtfertigt sein kann.

Dieses Beispiel zeigt, wie gut gemeinte Regulierung versagen oder sogar das falsche Mittel sein kann. Umso interessanter ist es, über die Potenziale eines Kodex zu diskutieren, der auch solche Datenschutzthemen erfasst. Zu fragen wäre etwa: Inwieweit sollten Unternehmen ihren Nutzern mit einfachen Worten beschreiben, was sie mit Nutzerdaten in wel-

9 Nach dem erstmals durch Eli Pariser vorgebrachten, allerdings nicht unumstrittenen Konzept der „Filter Bubbles".

chem Umfang vorhaben? Inwieweit rechtfertigen marginale Geschäftsmodelle[10] allgemein (bei ansonsten für den Nutzer kostenfreien Angeboten) die „Datensammelwut" der Anbieter? Wie ist der Widerstreit zwischen legitimen Datensammelinteressen und einem „Recht auf Vergessen" aufzulösen, und gibt es ein solches Recht überhaupt? Und ist es vielleicht einfacher, ein solches Recht nicht regulativ, sondern als vom Plattformbetreiber beachtete soziale Norm zu etablieren?

b) Geschäftsmodelle und ihre Offenlegung

Die Frage, ob und inwieweit eine echte Aushandlung des Quidproquo beim Geschäft mit Nutzerdaten zu fordern wäre, verweist noch weiter auf die Geschäftsmodelle der Plattformbetreiber insgesamt. Trotz zahlloser Gratisangebote wird den Nutzern gegenüber nur in seltenen Fällen klar kommuniziert, worauf das Geschäftsmodell der jeweiligen Plattform basiert. Unmittelbar hat dies vor allem zwei Auswirkungen:

- Unbedarfte Personen geben tendenziell persönliche Daten in einem Maße an, das sie später als zu umfangreich empfinden, aber nicht mehr zurücknehmen können (dies wird vielfach unter anderem durch Behörden, Verbraucherschützer, Jugendschutz-Initiativen und Medien angeprangert, gelegentlich bis hin zum Alarmismus).
- Besser informierte Personen entwickeln Strategien, um sich vor übermäßiger Ausspähung durch Plattformbetreiber zu schützen (zum Beispiel durch Angabe falscher Geburtsdaten, Nutzung von *Fake Accounts*[11] bzw. verkürzten Namen für soziale Netzwerke und bewusst gestreute Nutzung der Angebote verschiedener Betreiber).

Die weiter gehende Folge beider oben genannter Auswirkungen ist ein fortschreitender Verlust des Grundvertrauens in die Lauterkeit von Online-Angeboten – und nicht nur derjenigen, die gratis gemacht werden. Nach einer endlos erscheinenden Kette von Datenskandalen müssen Internet-Nutzer heutzutage nachgerade den Eindruck haben, bei den Angeboten von Plattformbetreibern werde dem Nutzer standardmäßig vorenthalten, worauf das Geschäftsmodell basiert, wo also umgangssprachlich „der Haken" ist. Das gilt vermutlich in vergleichbarem Maße selbst für diejenigen Angebote, die offensichtlich (auch) auf Werbung als Finanzierung setzen, denn auch dort kann es ja weitere verdeckte Finanzierungsquellen zusätzlich zur leicht erkennbaren Werbung geben.

Vom Blickwinkel der über 50-Jährigen aus, insbesondere sofern sie in ihrem Alltag nur wenig oder gar nicht direkt mit dem Internet und seinen Diensten konfrontiert sind[12], vermischt sich diese Unklarheit der Geschäftsmodelle gedanklich mitunter mit der Berichterstattung über „echte" Cyberkriminalität zu einer Gesamtsicht, nach der das Internet generell etwas Halbseidenes oder Böses sei.

Je nach betrachteter Gruppe innerhalb der Internet-Nutzer ist zudem eine Art „Zockermentalität" zu beobachten. Ihr liegen Gedankengänge wie „Wenn Anbieter im Internet durch Verschweigen ihrer Geschäftsmodelle versuchen, mich als Nutzer zu ködern und zu übervorteilen, dann habe ich jedes Recht, auch meinerseits konsequent meinen Vorteil zu suchen und – im Zweifel auch auf Kosten anderer – alles mitzunehmen, was ich bekommen kann" zugrunde. Man könnte dies als die aggressive Seite der viel beklagten „Gratis-Mentalität" bezeichnen. Es bedarf keiner wissenschaftlichen Analyse, um zu erkennen, dass diese Entwicklungen zu einer Verrohung des Umgangs miteinander beitragen können, und zwar aufgrund der weiter fortschreitenden Durchdringung des Alltags durch Online-Dienste in der gesamten Breite der Gesellschaft.

Es wurde bereits vieles versucht, um insbesondere auf Seiten der Anbieter von Internet-Diensten (als der besser regulierbaren Gruppe) mehr Transparenz gegenüber den Nutzern zu erzwingen. Darauf zielen-

10 Dies sind Geschäftsmodelle, bei denen an der einzelnen Transaktion nur extrem wenig verdient werden kann (Beispiel: einzelne Anfrage an eine Suchmaschine), sodass erst eine sehr große Anzahl von Transaktionen das Modell tragfähig macht, was in einigen Bereichen die starke Tendenz zu Konzentration und Wachstum erklärt.

11 Fake Accounts sind Nutzerprofile, bei deren Registrierung bewusst falsche Daten angegeben werden und die meist auch ohne größere Nachteile für die darunter registrierte Person gelöscht werden können.

12 So beispielsweise ablesbar für die Milieus „Ordnungsfordernde Internet-Laien" (Durchschnittsalter 51 Jahre) und „Internetferne Verunsicherte" (Durchschnittsalter 62 Jahre) nach der DIVSI-Milieustudie 2012, S. 37, 129, 132/133, 143, 145.

de Regelungen finden sich in Deutschland nicht nur im Telemediengesetz, sondern auch im Gesetz gegen den unlauteren Wettbewerb, im Rundfunkstaatsvertrag und nicht zuletzt in den Datenschutzgesetzen. Wie geeignet diese Regelungsansätze sind und ob bzw. inwieweit ein allgemeiner Kodex geeigneter sein könnte, sollte im Rahmen des Kodex-Prozesses diskutiert werden.

3. Verantwortungsverhältnis zwischen dem Staat und den übrigen Beteiligten

Das Internet als mehrschichtiges und komplexes Konstrukt wird von der Infrastruktur- bis zur Anwendungsschicht zu großen Teilen durch Private betrieben und gestaltet (siehe dazu oben Abschnitt C.). Entsprechend wird das allermeiste, was im Internet regelungsbedürftig erscheint, zivilrechtlich durch Verträge geregelt.

Zumindest in dem Maße, in welchem Gestaltungsmacht und Gestaltungswille[13] der Plattformbetreiber zunehmen, geht die staatliche Gestaltungsmacht zurück. Verstärkt wird dies dadurch, dass das Internet weitgehend unabhängig von Staatsgrenzen funktioniert. Die beiden regulatorischen Anker für jedes staatliche Handeln, das Staatsgebiet (hinsichtlich Gütern und des Umgangs mit ihnen) und die Staatsangehörigkeit (hinsichtlich Personen und ihrer Handlungen) bieten im Zusammenhang mit dem Internet weit weniger Halt als in der Offline-Welt.

Das bedeutet zwar keineswegs, dass Staaten nicht versuchen würden, ihre Hoheit auch auf das Internet auszudehnen. Dies ist jedoch bisher keinem Staat und keinem Staatenverbund wirklich gelungen, sondern es bestehen stattdessen mehrere teils konkurrierende Governance-Strukturen nebeneinander. Vielfach entscheidet faktisch schon die Technik darüber, wer etwas wie weitgehend regulieren kann (siehe dazu auch oben 1.d). Sofern man auch staatliche Stellen als „Unterzeichner" eines Digitalen Kodex in Betracht zieht, ergeben sich insoweit mögliche Verantwortlichkeiten des Staates in zwei Richtungen: Zum einen gegenüber seinen Bürgern, zum anderen gegenüber den Plattformbetreibern. Gegenüber Letzteren sieht sich der Staat in einem Wettbewerb um die Gestaltungsmacht, der in seiner Reichweite und in seinem Entwicklungstempo vermutlich bisher einmalig ist in der Geschichte der Neuzeit. Gegenüber seinen Bürgern hat der Staat mehrere und teils widerstreitende Aufgaben: Auf der einen Seite ist er zur Fürsorge verpflichtet und Schutzgarant auch jedes Einzelnen, auf der anderen Seite ist er Hüter der öffentlichen Ordnung. Beide Blickrichtungen des Staates sind differenziert zu betrachten.

a) Durch Plattformen geförderte Asymmetrie bei staatlichen Eingriffen

Diejenigen staatlichen Einrichtungen, die für Schutz und Fürsorge zuständig sind, haben auch und gerade angesichts der rasanten und oft allein von Privaten bestimmten Entwicklungen der Online-Welt weiterhin den Anspruch, diese Online-Welt für die Nutzer (hier Nutzer im Sinne von Bürgern) besser beherrschbar zu machen. Die Schwierigkeiten, dies auch umzusetzen, müssen nachgerade zu Frustration der Entscheidungsträger und dem – aus Staatssicht eher ungewohnten – Gefühl der Ohnmacht führen. Immer wieder werden Anläufe unternommen, den Online-Angeboten privater Unternehmen öffentlich getragene Alternativen zur Seite zu stellen, und immer wieder scheitern solche Alternativen im weltweiten Wettbewerb.

Die für öffentliche Ordnung und Strafverfolgung zuständigen staatlichen Organe hingegen haben nicht nur mit neuen Formen von Regelverstößen zu kämpfen, sondern können sich der privat gestalteten Infrastrukturen des Netzes teilweise auch für die eigenen Aufgaben bedienen. Tun sie dies, ergeben sich aus der privatwirtschaftlichen Prägung der Online-Welt weitreichende Folgen: Repressives bzw. präventives Handeln des Staates kann sich dann gleichsam hinter den unmittelbar gegenüber den Nutzern allein auftretenden Plattformbetreibern verstecken. Grundfreiheiten und Abwehrrechte greifen dann im Netz längst nicht so umfassend, wie es gegenüber direkten staatlichen Eingriffen der Fall wäre (siehe dazu auch oben Abschnitt C.). Hier kommt es also zu einer Asymmetrie, die in der Offline-Welt so nicht besteht: Während den Nutzern gegenüber Plattformbetreibern viele Abwehrmöglichkeiten fehlen, die ihnen als Bür-

13 Dieser Gestaltungswille und die Konkurrenz zum staatlichen Gestaltungsanspruch gehen beispielsweise aus der DIVSI-Meinungsführerstudie 2012 hervor (S. 27, 28).

ger gegenüber direkten staatlichen Eingriffen in Freiheitsrechte selbstverständlich gegeben wären, sind die Eingriffsmöglichkeiten des Staates nicht unbedingt in gleicher Weise beschränkt. Im Gegenteil, dadurch, dass das Geschehen im Internet immer stärker auf immer weniger Plattformen konzentriert abläuft, deren Betreiber nicht so unmittelbar den strengen verfassungsrechtlichen Ansprüchen der freiheitlich demokratischen Grundordnung genügen müssen, ergeben sich ganz neue Eingriffsmöglichkeiten, die der Staat mit eigenen Mitteln schwerlich realisieren könnte. Die Konzentration der Nutzerkommunikation auf wenige Plattformen erübrigt das Sammeln von Daten im Wege unzähliger Einzelmaßnahmen, da aus technischer Sicht automatisierte Massenabfragen möglich werden.

Große Teile des Alltags der Bürger werden weitgehend automatisch so genau dokumentiert, wie es früher nur Inlandsgeheimdienste mit großem Aufwand und vereinzelt vermochten. Aus Bewegungsprofilen, mitgeloggter Kommunikation, persönlichen Vorlieben, der Struktur des „Social Graph" und vielen weiteren Daten bis hin zur Suchhistorie eines Bürgers lassen sich Erkenntnisse gewinnen, die durch herkömmliche Ermittlungsmethoden oft schon deshalb nicht zu erlangen wären, weil für die entsprechenden Maßnahmen keine richterliche Genehmigung erteilt würde.

Diese Zugriffsmöglichkeiten gehen mitunter sogar weit über die Staatsgrenzen hinaus. So können Sicherheitsbehörden der Vereinigten Staaten, gestützt auf den Patriot Act und andere Regelungen, in den USA ansässige Unternehmen zur Herausgabe von Nutzerdaten zwingen und so auf umfangreiche Daten von Millionen Menschen weltweit zugreifen, ohne dass für die Betroffenen ein durchsetzbares Abwehrrecht greifen würde.[14]

Die Betroffenen erfahren in der Regel nicht einmal etwas von den erfolgenden Eingriffen und können dies auch nicht, da ihnen gegenüber stets nur die Plattformbetreiber mit ihren zivilrechtlichen Nutzungsregeln als handelnde Akteure auftreten. Wer vor Eingriffen sicher sein will, ist auf Selbsthilfe angewiesen, etwa durch eigenständige Verschlüsselung des eigenen Kommunikationsverkehrs, muss von vornherein auf Teile der Kommunikation verzichten – oder muss eben auf das Gute im Staate vertrauen bzw. auf das Gute in Staaten weltweit, wobei den meisten Betroffenen gar nicht klar sein dürfte, wie oft und auf welchen Wegen sich ihre Daten online in einem internationalen Raum um die Erde bewegen.

b) Fürsorgefunktion des Staates unter veränderten Rahmenbedingungen

Demgegenüber sind dem Staat als Fürsorger oft genug die Hände gebunden, wenn er auch im Netz seine Bürger – etwa vor bestimmten Geschäftspraktiken von Plattformbetreibern – schützen will. Dann wird der Staat mit seinen Angeboten durch die Dominanz der Unternehmen von der Aufmerksamkeit seiner Bürger abgeschirmt, und seine Schutzinstrumente (Datenschutzregeln, fiskalische Steuerung) stellen sich nicht selten als wenig wirksam heraus. Zugleich wächst die Bedeutung des Netzes für den Einzelnen nach wie vor stetig weiter, was eine gesellschaftliche Diskussion darüber, welchen Umfang staatliche Fürsorge in Zeiten des Internets haben kann und sollte, erforderlich erscheinen lässt.

Insofern hat es in doppelter Weise Sinn, auch den Staat als möglichen Adressaten eines Vertrauen stiftenden Kodex anzusehen. Die dazu zu stellenden Fragen könnten lauten: Müssen Plattformbetreiber grundsätzlich Rücksicht auf Staaten nehmen und ihnen im Sinne der Bürger freiwillig Gestaltungsspielräume belassen? Inwieweit haben staatliche Stellen die Verantwortung, ihre Bürger gegenüber Plattformbetreibern zu ebenso umfassenden Abwehrmöglichkeiten zu verhelfen, wie sie die Bürger gegenüber dem Staat direkt haben? Ergeben sich durch die faktische Gestaltungsmacht der Plattformbetreiber nachhaltige Verschiebungen im Staatsverständnis, und kann ein Kodex diese sinnvoll aufnehmen?

4. Verantwortungsverhältnis der Nutzer untereinander

Diese Konstellation sollte in erster Linie Gegenstand der übergeordneten Diskussion über Verantwortung

14 Siehe unter anderem den Wortlaut des Paragrafen (Sec.) 212 des sogenannten „Patriot Act", dort a. E., der eine entsprechende Änderung von Titel 18, Sec. 2703 des United States Code bewirkt hat.

und Verantwortlichkeit im Internet sein; für dieses Thema wird auf den Themenaufriss „Verantwortung im Internet" verwiesen. Da jedoch fast an jeder denkbaren Interaktion von Bürgern untereinander, die über das Internet stattfindet, auch Plattformbetreiber (wenigstens passiv) beteiligt sind, muss die Rolle und Verantwortlichkeit der Plattformbetreiber auch bezogen auf das Verhältnis der Nutzer untereinander angesprochen werden. Grundsätzlich ist das Verhalten der Nutzer (in diesem Kontext als Internet-Nutzer und Staatsbürger) nur sehr schwer überhaupt beeinflussbar. Zudem stellt sich die Frage, wie neue Regelungen für den Umgang der Menschen untereinander im Internet beschaffen sein müssen, da zumindest ein Teil altbekannter sozialer Normen auch ins Internet getragen wird und sich dort folglich keine gänzlich neuen von Grund auf herausbilden können und müssen.

Die Frage nach dem Bedarf neuer sozialer Normen stellt sich (abgesehen von der schieren Zahl von interagierenden Individuen und der gut begründeten Ablehnung totalitärer Herrschaftsstrukturen, die Vorsicht gebieten) aber auch deshalb, weil mit dem Staat als Konstrukt ja bereits ein Beteiligter besteht, der – obschon er nicht identisch mit der Gesamtheit seiner Staatsbürger ist – zumindest auch die Rolle einer Repräsentanz aller seiner Bürger innehat. Es bleibt allerdings zu beachten, dass der Staat als Beteiligter immer auch Eigeninteressen hat und diese auch verfolgt und dadurch zwangsläufig in einem Interessenkonflikt steht (siehe dazu auch oben 3.a). Der Staat ist de facto eben nie nur Stellvertreter der Interessen aller Bürger – ein Zustand, der ihn möglicherweise nicht dafür qualifiziert, die vollständige Prokura für seine Bürger zu übernehmen, wenn es um verantwortungsvolles Verhalten und Vertrauen im Internet geht.

Umso mehr rücken wieder die Plattformbetreiber ins Blickfeld, allerdings ebenfalls nicht als Handlungsbevollmächtigte der ihre Plattformen nutzenden Personen und auch nicht als Regulierte oder Regulierende, sondern eher als Vermittler zwischen den Nutzern. Kaum bestreitbar stellt das Annehmen und Ausfüllen dieser vermittelnden Rolle für die Plattformbetreiber in der Regel jedoch eine zusätzliche Belastung dar und unterbleibt oft ganz oder teilweise. Hinzu kommt, dass das „Wie" des Ausfüllens dieser Rolle ein einigermaßen gefestigtes Wertesystem voraussetzt. Über Kontinente und Kulturen hinweg gibt es gemeinsame Grundwerte jedoch nur in begrenztem Umfang, was es insbesondere für weltweit tätige Unternehmen schwierig bis unmöglich macht, sich an jedem Ort der Welt adäquat zum gültigen Wertesystem der vor Ort lebenden Menschen zu verhalten.

Zugleich ist es Unternehmen aber ebenso wenig möglich, sich „nicht zu verhalten". Zumindest, wenn es um Content und den Zugang dazu geht, transportiert jede Plattform zwangsläufig irgendein Wertesystem dorthin, wo sie verfügbar gemacht wird. Beispielsweise ist im ökonomischen Modell internationaler Bücherverkaufsplattformen keine grundsätzliche Buchpreisbindung vorgesehen. Seit sie in Deutschland verfügbar wurden, kollidieren sie insoweit mit dem hiesigen Wertesystem[15], welches aus kulturpolitischen Gründen eine Buchpreisbindung vorsieht.

Im Rahmen des Kodex-Prozesses wäre demnach auch folgende Frage zu diskutieren: Kann ein Kodex den Transport von Werten, der durch Plattformen und ihre Betreiber ohnehin stattfindet, in einer Weise ausgestalten, dass dieser Transport eine vermittelnde Wirkung zugunsten aller entfaltet? Und (wie) kann dies geschehen, ohne die Plattformbetreiber unangemessen stark zu belasten?

E. Fazit

Plattformen im Internet sind der gemeinsame Bezugspunkt einer Dreier-Konstellation von Akteuren, die aus den Betreibern der Plattformen, ihren Nutzern und staatlichen Stellen gebildet wird. Jede dieser Gruppen steht mit allen übrigen in Beziehung, in jeder dieser Beziehungen gelten soziale Normen, und die Verantwortlichkeit für das Geschehen verteilt sich oft nicht in ganz eindeutiger Art und Weise. Einer wachsenden Gestaltungsmacht der Plattformbetreiber stehen sowohl ein in der Zeit vor dem Internet verankerter Begriff der staatlichen Daseinsvorsor-

15 In der Ausgestaltung, die dieses im Rechtssystem gefunden hat.

ge als auch neue Möglichkeiten staatlicher Eingriffe gegenüber.

Die Nutzer sind, je nach Kontext, in verschiedenen Rollen als Verbraucher, Arbeitnehmer, Selbst-Unternehmer oder Staatsbürger mit sich ständig wandelnden Gegebenheiten konfrontiert. Während der Staat sie weder voll repräsentieren noch wie in analogen Zeiten schützen kann, können bzw. wollen die Plattformbetreiber dies nicht vollständig kompensieren. Sie sind als mächtige Architekten des Netzes zugleich wirtschaftlichen Gesetzen unterworfen und auch den Interessen der Nutzer verpflichtet, die wiederum neben Nutznießern von Online-Diensten zugleich in Teilen das Vermarktungsobjekt der jeweiligen Betreiber sind.

Im Hinblick auf die Sinnhaftigkeit eines Kodex stellen sich zahlreiche Fragen, für Plattformbetreiber unter anderem nach Rücksichtnahme auf lokale soziale Normen sowie danach, ob sie eine Brückenfunktion für Nutzer untereinander sowie zwischen den Nutzern und dem Staat erfüllen sollten und wie sie Forderungen nach Transparenz hinsichtlich Geschäftsmodellen und Einhegungstendenzen erfüllen können. Die Nutzer müssen sich fragen lassen, wie weit sie für eigene Interessen einzutreten in der Lage und bereit sind und welche Unterstützung sie jeweils bei Staat und Plattformbetreibern einfordern.

Der Staat wiederum muss vor allem dazu Stellung beziehen, welche Gestaltungsmacht wirklich nur durch ihn wahrgenommen werden kann, wann gesamtstaatliche Interessen an Sicherheit und Ordnung hinter Individualinteressen der Bürger zurücktreten müssen und wie der Staat seine Rolle in den Gestaltungsabläufen des Internets zu finden gedenkt.

THEMENPAPIER: VERANTWORTUNG IM INTERNET

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 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 Verantwortung.[16] 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 (zum Beispiel die Folgenbeseitigung bei Naturkatastrophen) beziehen. Normenverstöße haben meist Folgen und ziehen in der Regel Sanktionen nach sich, vor allem 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 ver-

16 Siehe zu den unterschiedlichen Definitionen Wikipedia: Verantwortung, de.wikipedia.org/wiki/Verantwortung.

antwortlich) 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 unter Umständen 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, zum Beispiel dem Internet, Verantwortung tragen und worauf sie sich bezieht, ist es sinnvoll, zwischen zwei Formen von Verantwortung zu 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 ermöglichen.[17]

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 einstehen 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 (zum Beispiel 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, zum Beispiel 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 überkomple-

17 Zum Thema: www.datenschutzzentrum.de/presse/20130424-facebook-klarnamen-ovg.htm.

xen Handlungsgefügen verantwortungsfreie Bereiche entstehen, oder zu kompensieren, dass der eigentlich Verantwortliche nicht verantwortlich gemacht werden kann, können **Ex-ante**-Verantwortlichkeiten geschaffen werden. Dieser Gedanke steht etwa hinter der Gefährdungshaftung oder dem Organisationsverschulden. In diese Richtung gehen viele Debatten über die Haftung im Internet, vor allem, 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, das heißt 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 infrage 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 Neubeurteilung 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 zum Teil 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 unter anderem die folgenden Besonderheiten des Internets relevant:

Anonymität und Unkörperlichkeit: Individuen sind im Internet per se anonym, wenn sie sich für Anonymität entscheiden. Dass sie, zum Beispiel 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 vor allem 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 können und werden im Internet aufgrund divergierender Wertvorstellungen oft sehr unterschiedlich sein. So zum Beispiel die Haltung gegenüber Gewalt oder Nacktheit im Vergleich zwischen Europa und den USA (Machill/Waltermann 2000, 15). Dadurch kommt es zum Beispiel 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, Werkzeuge 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 (zum Beispiel 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 unter Umständen gemeinsam dafür 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 begrenzt 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 Dienstanbietern 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, nicht staatliche Institutionen (NGO), religiöse Organisationen, Medien und der Staat. Als weiterer wichtiger Akteur haben die Architekten, Entwickler und Beherrscher der technischen Infrastruktur und der Werkzeuge, die das Internet technisch ausmachen, großen Einfluss. Hierzu zählen neben Zertifizierungsstellen, Registraren und Standardisierungsgremien vor allem die Anbieter der Telekommunikationsnetze, die Zugangsprovider, Plattform- und Suchmaschinenanbieter und andere Gatekeeper. 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 weiter reichenden, 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 damit 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. 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 demjenigen verantwortlich, der nur mittelbaren Einfluss hat.

Angesichts dieser Faktoren zeigt sich eine wichtige Aufgabe für das Projekt „Braucht Deutschland einen Digitalen Kodex?": Um ein Verantwortungskonzept für das Internet zu entwickeln, wäre es wichtig, den Akteuren Rollen zuzuweisen 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 sozioökonomischen 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 zum Beispiel 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) Architektur[18], 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 zum Beispiel 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

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

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 Shitstorms 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 in der Politik) aus.

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 behaupten.[19] 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 unter Umständen 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 (vor allem 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 vorbeiregulieren. 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 um Regelungen mit konkretem Bezug oder um solche handelt, in denen die „großen Linien", Rahmenregelungen oder Grundprinzipien (etwa Staatsverfassungen) definiert werden.

19 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 wollten (dagegen Murray 2011, 269/270, Goldsmith, 1998).

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 zum Beispiel 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, insbesondere 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 Internet-Nutzer 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 (zum Beispiel 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 hoch spezialisierte 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, zum Beispiel 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).[20] 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, zum Beispiel, um staatliche Regulierung zu vermeiden.

Das Konzept der Co-Regulierung oder regulierten Selbstregulierung versucht, dieses Manko zu verhindern, indem externe Druckmittel implementiert werden, wie zum Beispiel staatliche Überwachung durch Regulierungsbehörden. Hängt mit dem Gegenstand der Selbstregulierung große Verantwortung, etwa für Grund- oder Freiheitsrechte Dritter, zusammen, wird

20 Dies hat sich in der Vergangenheit schon verschiedentlich gezeigt, unter anderem 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.). Auch der in Deutschland gestartete Versuch ist gescheitert, einen Kodex zur Selbstregulierung für soziale Netzwerke auf den Weg zu bringen (siehe www.telemedicus.info/article/2569-Kodex-zur-Selbstregulierung-fuer-soziale-Netzwerke-gescheitert.html).

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 Gatekeepern, kommt daher große Verantwortung zu. Zum einen tragen sie Verantwortung dafür, Handlungsoptionen zu eröffnen oder zu verhindern, was auf eine Mitverantwortung für die Internet-Nutzer hinausläuft. Hiermit verbunden ist die Verantwortung für die Nutzungsfreiheit. Würde zum Beispiel 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, zum Beispiel 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.

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 könnte.[21]

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 der Hauptaufgaben im Projekt „Braucht Deutschland einen Digitalen 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.

21 Siehe www.golem.de/news/code-raus-aus-der-digitalen-unmuendigkeit-1305-99125.html.

THEMENPAPIER: WAS IST EIN DIGITALER KODEX?

Vorbemerkung

Im vorliegenden Themenpapier wird untersucht, was man sich unter einem Digitalen Kodex vorstellen könnte. Die Überlegungen schließen folgende Punkte ein:

1. **Sachlicher Anwendungsbereich:** Auf welche Bereiche des Netzes kann sich ein Digitaler Kodex beziehen?
2. **Inhaltlicher Anwendungsbereich:** Auf welche Problematik, auf welches Verhalten kann sich ein Digitaler Kodex beziehen?
3. **Begriffsbestimmung und personeller Anwendungsbereich/Adressat:** Was kann man unter einem Digitalen Kodex verstehen, und an wen kann er sich richten?

Diese Fragen dienen dazu, die Überlegungen weiter zu präzisieren, die in den Themenaufrissen zu **Verantwortung im Internet** und **Plattformen** sowie im ersten Expertenworkshop angestellt wurden, sowie Orientierungspunkte für die weitere Diskussion zu liefern. Zu diesem Zweck werden Vorschläge für mögliche Anwendungsbereiche und konzeptionelle Ansätze eines Digitalen Kodex unterbreitet. Nachdem das Thema Regulierung und Verantwortung im Netz bzw. auf Plattformen zunächst sehr grundlegend diskutiert wurde, ist es nun notwendig, den Untersuchungsgegenstand weiter zu präzisieren.

Die abstrakte Frage, ob mit einem Digitalen Kodex gewissen unerwünschten Verhaltensweisen im Internet begegnet werden könnte, wird man so nicht beantworten können. Die Antwort wird lauten: Es kommt darauf an, um welche Phänomene und Verhaltensweisen es geht, in welchen Bereichen des Netzes sie auftreten, welche Akteure sich dort finden und an welche Akteure sich ein solcher Kodex richten könnte. Diese Aspekte sollen nachstehend näher beleuchtet werden.

1. Sachlicher Anwendungsbereich: Auf welche Bereiche des Netzes könnte sich ein Digitaler Kodex beziehen?

Der Fokus der Untersuchung wurde zunächst auf die Themen „Verantwortung" und „Plattformen" gelegt. Die insofern präzisierte Ausgangsfrage würde lauten: „Braucht Deutschland einen Digitalen Kodex für Plattformen?"

Auch diese Frage ist jedoch im Zweifel zu abstrakt, um sie beantworten zu können. Dies zeigt sich schon an der – im Themenaufriss Plattformen herausgearbeiteten – Tatsache, dass der Begriff der Plattform sehr weit verstanden wird oder zumindest verstanden werden kann.[22] Er erfasst eine Vielzahl sehr unterschiedlicher Dienste und Dienstarten, in denen unterschiedliche Akteure in sehr disparaten Strukturen agieren. Angesichts dieser Vielfalt erscheint es angebracht, die Frage, wie eine Regulierung[23] von Plattformen funktioniert oder funktionieren könnte, anhand von konkreter gefassten Beispielkonstellationen zu untersuchen.

Disparität von Plattformen und deren Systematisierung

Ebenso wenig, wie es „das Internet" gibt, gibt es „die Plattform". Plattformen können offene oder geschlossene Netze sein. Sie können zentral (durch einen Anbieter) oder dezentral organisiert sein. Je nachdem, um welche Art Plattform es sich handelt, sind im Zweifel unterschiedliche Ansätze zur Steuerung von Verhalten und Zuordnung von Verantwortung zu verfolgen.

22 Hier (Weitzmann 2013) heißt es: „Plattformen im Sinne dieses Textes sind alle mit dem Internet in Verbindung stehenden technischen Infrastrukturen, die grundsätzlich für eine Benutzung (zum Beispiel Zugriff, Einsichtnahme und Interaktion) auch durch andere als den Betreiber geeignet oder sogar vorgesehen sind. Soziale Medien und kollaborative Projekte werden damit genauso als Plattformen verstanden wie sonstige serverbasierte Infrastrukturen jeder Art (zum Beispiel Streaming-Plattformen, Blog-Dienste, Foto-Communities und sonstige Angebote rund um „User Generated Content"), Cloud-Dienste sowie vergleichbare Angebote – unabhängig davon, ob es sich um Strukturen handelt, die rundfunkähnlich („one to many") oder interaktiv („many to many") organisiert sind. Bewusst ausgenommen sind die physische Kommunikations-Infrastruktur und ihre Betreiber (zum Beispiel Internet-Service-Provider und TK-Unternehmen)."

23 Der Begriff der Regulierung wird hier im denkbar weitesten Sinn verstanden. Gemeint sind nicht nur staatliche Interventionen in Form von Gesetzen oder anderen Normsystemen. Gemeint sind auch zum Beispiel soziale Normen als eine – häufig unkodifizierte – Form der Selbstregulierung.

Vor diesem Hintergrund stellt sich die Frage, ob und nach welchen Kriterien Plattformen typologisiert werden können, damit die für Regulierungsfragen relevanten Unterschiede deutlich werden.

Erstes Typologisierungsmerkmal: Anbieter und Zielgruppe

Plattformen können zunächst nach Anbietern und Zielgruppen unterschieden werden. Plattformen können von Unternehmen angeboten und an Privatpersonen gerichtet sein (B2C). Manche Dienste werden von Unternehmen anderen Unternehmen angeboten (B2B). Schließlich existieren auch Plattformen, die von Privatpersonen für die Nutzung durch andere Privatpersonen bereitgestellt werden (wie verteilte Netzwerke, siehe unten).

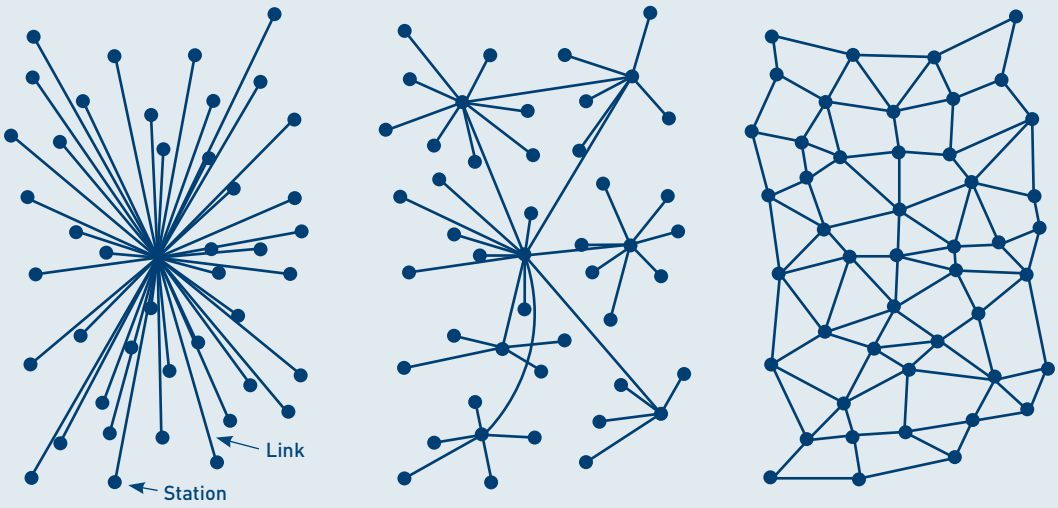
Wer eine Plattform anbietet und wer sie nutzen kann, ist für Regulierungsfragen von erheblicher Bedeutung. Dieses Kriterium ist entscheidend für die Frage nach den agierenden Akteuren, deren Interessen und Rollen und damit unter anderem für mögliche Adressaten einer durch einen Kodex zu regelnden Verantwortungsverteilung.

Zweites Typologisierungsmerkmal: Interaktionsmöglichkeit

Ob eine Plattform Interaktion ermöglicht oder nicht, ist wiederum bedeutsam für das Verhalten der Nutzer. Rein statische Webauftritte, bei denen beispielsweise Unternehmen oder Personen präsentiert werden, werden nicht im Fokus eines Digitalen Kodex stehen, da sich die komplexen Probleme – die ein solcher Kodex adressieren soll – hier zumeist nicht stellen. Im Übrigen sind sie in Zeiten des „Web 2.0" von zunehmend geringer Relevanz.

Drittes Typologisierungsmerkmal: Netzwerkstruktur – Zentrale, dezentrale und verteilte Netzwerke

Plattformen sind im Prinzip Netze im Netz. Mit anderen Worten bilden sie offene oder in sich geschlossene Kommunikationsnetzwerke, die wiederum in größere Netzwerke eingebunden sein können. Die Struktur von Kommunikationsnetzwerken kann in drei Gattungen unterteilt werden: zentrale, dezentrale und verteilte Netzwerke (distributed networks). Die drei Formen unterscheiden sich vor allem dadurch, ob sie



Zentralisierte, dezentralisierte und verteilte Netzwerke

von einem oder mehreren Anbietern zentral gesteuert werden, über deren Server der Datenverkehr abgewickelt wird (zentrale und dezentrale Netzwerke). Sie basieren auf dem Client-Server-Prinzip. In verteilten Netzwerken vernetzen sich die Nutzer – ohne Zwischenschaltung eines Anbieters – direkt miteinander.[24] Im Unterschied zum Client-Server-Modell spricht man hier vom Peer-to-Peer-Prinzip (P2P).

Die Grafik links verdeutlicht die unterschiedlichen Konzepte von Netzwerkarchitekturen (Quelle: Baran 1964, 4). In zentralisierten Kommunikationsnetzwerken erfolgt jegliche Datenübertragung über einen zentralen Anbieter. Bei dezentralisierten Netzwerken sind mehrere Anbieter beteiligt. In verteilten Netzwerken vernetzen sich die Nutzercomputer dagegen direkt miteinander, ohne dass es eines oder mehrerer zentraler Anbieter und deren Infrastruktur bedürfte.[25] Diese unterschiedlichen Konzepte finden sich auch bei den durch Plattformen gebildeten Netzwerken.

(a) Zentrale Plattformen

Viele Plattformen bilden ein zentrales, in sich geschlossenes Netzwerk. In sozialen Netzwerken, auf Video-, Verkaufs- oder Versteigerungsplattformen, bei Cloud-Diensten usw. verläuft in der Regel sämtlicher Datenverkehr über die Infrastruktur eines einzelnen Anbieters. Üblicherweise sind zentrale Plattformen nicht Teil eines übergeordneten dezentralen Netzwerks. Der Grund hierfür sind fehlende Interkonnektivität und Datenportabilität. Gerade soziale Netzwerke wie Facebook, Google+ oder LinkedIn bieten keine Möglichkeit, direkt mit den Nutzern jeweils anderer Netzwerke zu kommunizieren oder die in einem Netzwerk generierten Daten, Inhalte und Kontakte in ein anderes Netzwerk zu exportieren.

Zentrale Plattformen gewinnen im Internet immer mehr an Bedeutung. Medienökonomische Hintergründe – wie Netzwerk- und Skaleneffekte – führen zunehmend zu einer Zentralisierung des Netzes und fördern die Entstehung von in sich geschlossenen Netzen im Netz (Deterding 2010, 24 ff.). Dieser Trend zeigt sich besonders deutlich an der Strategie von Apple. Das Unternehmen bietet vom Endgerät über die Applikationen bis zur Infrastruktur – wie Cloud-Speicherdienste – alles „aus einer Hand" an.[26]

(b) Dezentrale Netzwerke

Andere Plattformen sind offen und damit Teil von dezentralen Netzwerken. Solche finden sich zum Beispiel bei E-Mail oder *IRC*[27] (Internet Relay Chat). Sie zeichnen sich dadurch aus, dass eine Mehrzahl von Anbietern in einen einzigen Kommunikationsvorgang involviert sein kann – und regelmäßig sein wird. Dies wird durch Interkonnektivität ermöglicht. Wie im Telefonnetz können Nutzer unterschiedlicher Anbieter/Serverbetreiber per IRC oder per E-Mail miteinander kommunizieren.

(c) Verteilte Netzwerke

Verteilte Netzwerke kommen gänzlich ohne zentrale Anbieter oder Infrastrukturen aus. Die Datenkommunikation erfolgt ohne Zwischenschaltung von zentralen Servern. Ein Beispiel für solche Netzwerke sind vor allem dezentrale (Peer-to-Peer) Filesharing-Systeme.

Aus Sicht der Ausfallsicherheit, Redundanz oder auch des Schutzes von Freiheitsrechten haben verteilte Netzwerke große Vorteile. Sie werden nicht von dominanten Akteuren, die vornehmlich eigene – vor allem wirtschaftliche – Interessen verfolgen, gesteuert. Der Ausfall eines, ganz gleich welchen, Teilnehmers beeinträchtigt nicht ihre Funktionsfähigkeit. Daten werden in einer Vielzahl von unabhängigen Instanzen gespeichert und vorgehalten.

---

24 Siehe hierzu auch die Anmerkung in der folgenden Fußnote.

25 Diese Aussage bezieht sich auf die Organisation der Plattform, nicht des Mediums (Internet), auf dem die Plattform läuft, oder die physische Netzinfrastruktur. Es liegt auf der Hand, dass die physische Netzinfrastruktur bei jedem Datenverkehr im Internet in Anspruch genommen wird und damit stets auch privatwirtschaftliche Anbieter involviert sind. Bezieht man diesen Faktor mit ein (wie zum Beispiel bei Deterding 2010, 12 ff.), ist das „freie Internet" eine Illusion. Vorliegend ist dies jedoch unbeachtlich, da es hier um das Verhalten aktiver Akteure und bestimmte Bereiche des Netzes (Plattformen) geht.

26 Angesichts der Gefahren von Rezentralisierungstendenzen befürworten Wissenschaftler und Internet-Aktivisten die Bildung offener Netzwerke als Alternative zu den bestehenden, anbietergeführten Systemen. Beispielsweise sollen distributed social networks bzw. federated social networks wie Diaspora gefördert werden, in denen die Nutzer mehr Macht über ihre Internet-Aktivitäten haben als in „proprietären" Systemen (Esguerra 2011).

27 Siehe zur Definition: de.wikipedia.org/wiki/IRC-Netzwerk und de.wikipedia.org/wiki/Internet_Relay_Chat.

Die Kehrseite dieser Eigenschaften ist, dass verteilte Netzwerke besonders schwer zu regulieren sind. Da ein Betreiber als zentraler Akteur als Regelungsadressat fehlt, ist es gerade bei massenhaftem Fehlverhalten kaum möglich, Normen effizient durchzusetzen.[28] Dies zeigt sich zum Beispiel, wenn man die Maßnahmen gegen Urheberrechtsverletzungen auf zentralen Plattformen mit denen in dezentralen Filesharing-Netzen vergleicht. Will ein Rechteinhaber diesem Massenphänomen mit rechtlichen Mitteln begegnen, bleibt bei einem P2P-Netzwerk wie Bittorrent nichts anderes übrig, als die Filesharer mit Massenabmahnungen zu überziehen. Bei Rechtsverletzungen auf Musikplattformen dagegen richten die Rechteinhaber rechtliche Maßnahmen nicht gegen die Nutzer, sondern den Anbieter. Eine schwierige, aber zumindest zu bewältigende Aufgabe, wie sich an den Vereinbarungen zwischen Google/YouTube und Tausenden von Musiklabels und Verwertungsgesellschaften auf der ganzen Welt zeigt.

Bedeutung der Netzwerkstruktur für einen Digitalen Kodex

Die Differenzierung in zentrale, dezentrale und verteilte Dienstarten erleichtert es, verschiedene Kernaspekte der Frage, ob ein Digitaler Kodex sinnvoll und zielführend wäre, gezielter zu untersuchen. Dies gilt vor allem für die Identifizierung der Akteure und deren Handlungsmacht, Konzepte zur Zuschreibung von Verantwortung und ebenso für die Frage, welche Regulierungsformen im jeweiligen Bereich effizienter oder weniger effizient sind. Aus Sicht der Regulierung ist die (Re-)Zentralität[29] des Netzes Fluch und Segen zugleich. Einerseits fördert sie regulatorisch unerwünschte Effekte, wie Monopolisierung, Zensur und übermäßigen Einfluss einzelner Akteure unter anderem auf das Sozialverhalten der Nutzer. Andererseits erleichtert sie die Regulierung wiederum, da es hier zentrale Akteure gibt, an die Regulierungsmaßnahmen bzw. Regulierungsanforderungen gerichtet werden können.

Viertes Typologisierungsmerkmal: Primärfunktion der Plattform

Plattformen sind in ihrer Art, Ausrichtung und Ausgestaltung so unterschiedlich, dass es sinnvoll erscheint, sie inhaltsbezogenen Kategorien zuzuteilen. Fraglich ist hierbei, welche Kriterien sich zur Differenzierung im Hinblick auf eine aussagekräftige Strukturierung eignen.

Orientiert man sich beispielsweise an den technischen Funktionen der jeweiligen Dienste als Unterscheidungskriterium, stößt man sehr schnell an Grenzen. Auf modernen Plattformen werden zumeist unterschiedlichste Funktionen kombiniert. Amazon ist beispielsweise vorrangig eine Verkaufsplattform. Mit ihrem Bewertungs- und Kommentierungssystem bietet sie jedoch auch die Möglichkeit, sich auszutauschen und zu diskutieren. Allein anhand der technischen Funktionen lässt sich daher keine zuverlässige Kategorisierung vornehmen.

Naheliegender erscheint es daher, danach zu unterscheiden, wozu eine Plattform vorrangig dient, also nach der Primärfunktion. Eine Klassifizierung nach diesem Kriterium könnte zum Beispiel derart aussehen:

A) Plattformen, die vor allem dem sozialen Austausch in der Öffentlichkeit oder in Teilöffentlichkeiten dienen. Beispiele: „Marktplätze der Meinungen" wie Social-Media-Plattformen, Meinungs-Foren oder IRC-Plattformen.

B) Plattformen, die der nichtöffentlichen Individual- oder (Klein-)Gruppenkommunikation dienen. Beispiele: IP-Telefonie-Dienste wie Skype, Messaging-Dienste, E-Mail-Dienste, Conferencing-Systeme.

C) Plattformen, die dem Handel und Verkauf von Sachen oder der kommerziellen Zugänglichma-

28 Auf solche Netzwerke haben – neben den Nutzern – lediglich die Entwickler von Protokollen, Standards oder Anwendungen Einfluss, die bei der jeweiligen Kommunikation verwendet werden. Sie können zwar das Verhalten der Nutzer nicht unmittelbar beeinflussen, über die Ausgestaltung der Technologie (des Codes) jedoch mehr oder weniger genau definieren, welches Verhalten überhaupt möglich ist und welches nicht. Siehe zu den Theorien, die sich mit Regulierung durch die Gestaltung des Codes beschäftigen, Kreutzer (2013).

29 Mit Rezentralisierung des Internets ist gemeint, dass es zwar als verteiltes Netzwerk konzipiert wurde (diesbezüglich sehr lehrreich ist das BBC-Interview mit Vint Cerf, einem der „Väter des Internets": BBC 2009, The Virtual Revolution – Rushes Sequences, www.bbc.co.uk/blogs/digitalrevolution/2009/11/rushes-sequences-vint-cerf-int.shtml). Durch die Dominanz von Plattformen und andere Rezentralisierungs-Trends wird die konzeptionelle Dezentralität des Netzes zunehmend aufgeweicht, wodurch bedeutende Bereiche des Netzes angreifbar werden (Deterding 2010).

chung immaterieller Inhalte dienen. Beispiele: Auktions-Plattformen, Online-Shops, App-Stores, Download- oder Streaming-Dienste.

D) Plattformen zum Austausch und zur Speicherung von Daten. Beispiele: Infrastructure-as-a-Service-Dienste wie Cloud-Speicher-Services, Filesharing-Netze, Sharehoster.

E) Plattformen für Online-Computing. Beispiele: Cloud-Application- bzw. Software-as-a-Service-Dienste wie Google Docs, Microsoft Azure.

F) Plattformen zur Nachrichten- und Informationsvermittlung. Beispiele: Blogs, Verlagswebseiten, Wikipedia.

G) Informationsmehrwertdienste. Beispiele: Suchmaschinen, Nachrichten- und sonstige Informationsaggregatoren.

H) User-Generated-Content-Plattformen, die vorrangig zur Veröffentlichung von kreativen Inhalten durch die Nutzer dienen. Beispiele: Video- und Fotoplattformen wie YouTube, Instagram oder Flickr.

I) Games-Plattformen. Beispiel: Steam.

Natürlich kann man in Bezug auf die Kategorienbildung und umso mehr zur Zuordnung konkreter Plattformen in die einzelnen Kategorien geteilter Meinung sein. Hierauf soll es im Detail an dieser Stelle jedoch nicht ankommen. Die Kategorisierung soll vielmehr die große Vielfalt von Internet-Plattformen aufzeigen und eine Orientierung ermöglichen. Zudem soll sie es – in Ergänzung zu den weiteren, oben beschriebenen Typologisierungsmerkmalen – erleichtern, unter den mannigfaltigen Optionen eine Auswahl hinsichtlich eines beispielhaften Anwendungsbereichs für einen Digitalen Kodex zu treffen.

Vorschlag für die Wahl des sachlichen Anwendungsbereichs zur Untersuchung der Frage „Braucht Deutschland einen Digitalen Kodex?“

Die vorstehenden Überlegungen haben aufgezeigt, dass man Online-Plattformen nach zumindest vier Kriterien unterscheiden und kategorisieren kann: Zielgruppe, Interaktivität, Netzwerkstruktur und Primärfunktion. Fraglich ist nun, auf welche Art Plattform man sich unter Anwendung dieser Kriterien fokussieren könnte.

Das generelle Ziel der Untersuchung liegt darin, zu analysieren, ob ein Digitaler Kodex geeignet erscheint, das Sozialverhalten der Nutzer und/oder das Anbieterverhalten zu steuern. Vor diesem Hintergrund liegt es nahe, bei der Wahl eines beispielhaften Anwendungsbereichs zunächst solche Dienste und Plattformen auszuschließen, die zum einen keine sozialen Funktionen bieten oder nicht interaktiv sind und die sich zum anderen nur an Unternehmen richten.

Unter den verbleibenden Optionen bietet es sich an, angesichts der stetig steigenden Bedeutung und damit Repräsentativität der hier auftretenden Problemlagen, sich auf zentrale Plattformen zu fokussieren. Gleichzeitig zentrale Netzwerke und verteilte Netzwerke auf die Frage nach dem Sinn und Zweck sowie der Umsetzung eines Digitalen Kodex hin zu untersuchen, würde mehrere Untersuchungsstränge erfordern. Dies gilt auch und vor allem deshalb, da die Akteursstruktur jeweils sehr unterschiedlich ist, was etwa eine einheitliche Beurteilung unmöglich macht, wer Adressat eines solchen Kodex sein könnte.

Das gleiche Problem entsteht, wenn man versucht, gleichzeitig zentrale und dezentrale Netzwerkstrukturen in den Blick zu nehmen. Auch hier unterscheidet sich die Akteursstruktur wesentlich, sodass kaum einheitlich beurteilt werden kann, wo eine etwaige Regulierung ansetzen müsste, wer Verantwortung tragen soll, wie Regeln implementiert oder durchgesetzt werden können. All diese Fragen hängen elementar davon ab, wer Handlungsmacht hat und wie sie ausgeprägt ist.

Zudem wäre es sinnvoll, sich bei der Untersuchung zunächst auf eine bestimmte Plattformkategorie zu beschränken. Schon auf den ersten Blick dürfte deutlich werden, dass manche – für Regulierungsfragen relevante – Umstände schon innerhalb der Gruppen sehr unterschiedlich sein können. So treten die Nutzer bei Social-Media-Plattformen in der Regel nicht anonym auf – wenn es auch vorkommt. Anonymität behindert einen bei solchen Diensten wichtigen Effekt: die digitale Perpetuierung oder Wiederaufnahme physisch begründeter Beziehungen. Bei Diskussions-Foren ist dies genau umgekehrt. Hier treten die Nutzer in aller Regel nicht unter ihrem Realnamen auf, sondern unter Pseudonym.

Interkategorial werden diese Unterschiede erheblich größer. Die Fragen, die sich bei Soft-

ware-as-a-Service-Plattformen im Hinblick auf eine Regulierung des Nutzer- und/oder Anbieterverhaltens stellen, sind mit denen bei Telefondiensten oder gar Social-Media-Plattformen nicht vergleichbar. Dies gilt schon aufgrund des Umstands, dass die Handlungsmöglichkeiten der Nutzer auf diesen Plattformen völlig unterschiedlich sind.

Angesichts der Ausrichtung der Untersuchung soll hier der Vorschlag unterbreitet werden, sich auf zentrale Kommunikationsplattformen (Gruppe A) zu fokussieren. Hierfür spricht zunächst, dass sich gerade bei solchen Diensten viele der derzeit als besonders gravierend angesehenen Problemfelder kumulieren, wie zum Beispiel Datenschutz, Persönlichkeitsschutz, illegale Inhalte, Cybermobbing usw. Zudem sind die Akteursstrukturen in diesem Sektor relativ einheitlich und nicht übermäßig komplex. Wie gesagt, liegt die Besonderheit solcher Systeme darin, dass jegliche Kommunikation und jeglicher Datenaustausch über die Systeme eines einzigen Anbieters erfolgen. In derart geschlossenen Netzen hat der Anbieter maximale Steuerungsmöglichkeit. Er entscheidet darüber, was die Nutzer auf seiner Plattform tun können – oder eben auch nicht. Die Steuerung des Nutzerverhaltens erfolgt einerseits über die Programmierung des – proprietären, nicht offenen – Systems und andererseits über die Nutzungsbedingungen, also privatrechtliche Verträge.[30]

Die hieraus sich ergebende Handlungsmacht zeigt sich an einer Analogie: Wäre im öffentlichen Raum ein derartiges Zusammenspiel von rechtlicher und technischer Regulierung möglich, wäre die Steuerungsmöglichkeit des Staates annähernd unbegrenzt. Er könnte beispielsweise Geschwindigkeitsbegrenzungen im Straßenverkehr – also die rechtliche Norm – durch Einsatz technischer Systeme durchsetzen, die jedes Fahrzeug ständig automatisch auf die jeweils zulässige Geschwindigkeit drosseln.

Die technischen und rechtlichen Steuerungsmöglichkeiten der Anbieter haben kaum Einschränkungen. Technisch ist fast alles möglich. Die Ausgestaltungsmöglichkeiten der Nutzungsbedingungen sind – da es sich um privatrechtliche Verträge handelt – auch nur sehr eingeschränkt begrenzt. Das zeigt sich wiederum an einem Beispiel: Der Umstand, dass in sozialen Netzwerken massenweise Daten gesammelt und zu unterschiedlichsten Zwecken genutzt werden, ist rechtlich so lange nicht zu beanstanden, wie die Nutzer dem durch privatrechtliche Willenserklärungen zustimmen. Willigt ein – vollständig geschäftsfähiger – Nutzer ein, dass seine Daten zu Werbezwecken an andere Unternehmen weitergegeben werden, dass seine Inhalte vom Anbieter genutzt und „verkauft" werden können oder dass ausführliche Bewegungsprofile angelegt werden, handelt es sich um eine wirksame und rechtlich bindende Erklärung, auf die sich der Anbieter berufen kann. In die hierdurch begründeten vertraglichen Anbieter-Nutzer-Verhältnisse kann das Gesetz aufgrund des Grundsatzes der Vertragsfreiheit nur sehr eingeschränkt eingreifen. Der Staat kann lediglich allgemeine Regeln aufstellen und Transparenz vorschreiben oder beschränkt geschäftsfähige oder ansonsten schutzbedürftige Nutzergruppen, wie zum Beispiel Minderjährige oder Verbraucher, „vor sich selbst" schützen.

Hinzu kommt, dass die Anbieter zentraler Plattformen – als privatwirtschaftliche Unternehmen – nicht oder nur sehr eingeschränkt durch die Grundrechte gebunden sind. Anders als der Staat als „Anbieter" öffentlicher Räume sind sie damit rechtlich nicht verpflichtet, grundrechtliche Freiheitsrechte zu gewährleisten. Ob sie sich darüber hinaus aus ethischen, moralischen oder kulturellen Gründen eine Art Selbstbindung auferlegen, wird in aller Regel in ihrer eigenen Entscheidung liegen. Aus solchen Faktoren jedoch eigene Prinzipien aufzustellen und umzusetzen, ist ein hochkomplexes Problem (Rosen, 2013[31]).

Dennoch: Die besondere – und angesichts der Entwicklung des Netzes repräsentative – Akteurskonstellation bei zentralen Kommunikationsplattformen prädestiniert diese Form des Netzwerks als Testumgebung für Überlegungen zu einem Digitalen Kodex.

Zentrale Kommunikationsplattformen als Fallbeispiel zu wählen, bietet sich auch aus einem weiteren

30 Siehe hierzu auch schon Weitzmann (2013).

31 Rosen beschreibt sehr aufschlussreich, dass die Anbieter durchaus in einem schwierigen Spannungsfeld von Gesetzen, Moralprinzipien und Traditionen operieren und sich auch bemühen, diesen Schwierigkeiten gerecht zu werden. Er macht aber auch deutlich, wie schwierig es gerade für international operierende Anbieter ist, praktikable Lösungen zu finden, etwa wenn es um den Umgang mit „hate speech" auf Social-Media-Plattformen geht.

Grund an. In Bezug auf die Nutzer und die auftretenden Probleme stellen solche Netzwerke ein Abbild der großen Vielfalt und Komplexität des Internets selbst dar. Sie wenden sich an jeden Nutzer, unabhängig von Alter, Geschlecht, gesellschaftlichem Status oder kultureller Herkunft. Sie werden zumeist international angeboten und daher in verschiedensten Rechts- und Kulturräumen genutzt. Sie prägen das Kommunikations- und Sozialverhalten gerade jüngerer Generationen in besonderem Maße. Man könnte sagen: Zentrale soziale Plattformen sind als soziales Betrachtungsfeld ein Abbild des Internets an sich, allerdings realisiert in einer überschaubaren Organisationsstruktur. Diesbezüglich gewonnene Erkenntnisse werden daher in vielerlei Hinsicht auf andere Bereiche und Fragestellungen übertragbar sein.

2. Inhaltlicher Anwendungsbereich: Auf welche Problematik könnte sich ein Digitaler Kodex beziehen?

Regulierung – ob per Gesetz oder durch einen Kodex – bezieht sich stets auf bestimmte Regelungssachverhalte. In der Regel steht der Regelungssachverhalt im Mittelpunkt jeder Überlegung über Regulierungsmaßnahmen. „Das Verhalten von Anbietern und Nutzern auf zentralen Kommunikationsplattformen" ist kein Sachverhalt, der konkreten oder auch nur konzeptionellen Überlegungen zu Regulierungsmöglichkeiten zugänglich wäre. Diese Themendefinition beschreibt kein Verhalten und keinen Interessenkonflikt und daher keinen Regelungssachverhalt, an dem man die Effizienz von Regulierungsansätzen beispielhaft untersuchen könnte. Es ist zudem nicht möglich, zu untersuchen, warum sich Nutzer und Anbieter verhalten – und entsprechend, wie man gewissen Handlungen vorbeugen kann –, ohne eine oder mehrere bestimmte Verhaltensweisen in den Blick zu nehmen. Schließlich umfasst ein derart abstrakt definierter Betrachtungsgegenstand eine solche Vielfalt von Problematiken, dass die Komplexität der Aufgabe eine zielführende Lösung kaum erwarten ließe. Aus diesem Grund wurde bereits in der Einleitung angemerkt, dass die Frage „Braucht Deutschland einen Digitalen Kodex" nicht beantwortet werden kann, ohne gleichzeitig anzugeben, worauf (sachlich, persönlich, inhaltlich) sich ein solcher Kodex beziehen soll.

Insofern erscheint es naheliegend, sich bei der Untersuchung nicht nur auf eine sektorspezifische Betrachtung zu konzentrieren, sondern zudem auf bestimmte – besonders gravierende und/oder repräsentative – konkrete Fragestellungen.

Inhaltlich könnte sich die weitere Untersuchung beispielsweise auf folgende Themenschwerpunkte fokussieren:

A) Cybermobbing;
B) Umgang mit persönlichen Informationen und Daten durch Nutzer und Anbieter;
C) Verstoß gegen fremde Urheberrechte.

Alle drei Themen werden derzeit als besonders gravierend wahrgenommen. Sie stehen gewissermaßen stellvertretend für den Eindruck, dass sowohl das Sozialverhalten der Menschen als auch der Anbieter im Netz anders ist als in der gegenständlichen Welt. Es geht um bedeutende Internet-spezifische Phänomene, wie die veränderte Wahrnehmung von Privatheit, die (vermeintliche) Unkontrollierbarkeit des Verhaltens, eine (zumindest gefühlte) „Verrohung der Sitten", die Grundeinstellung zum Umgang mit Rechten Dritter u.v.m.

Die genannten Themen betreffen Nutzer und Anbieter gleichermaßen. Den Nutzern wird vorgeworfen, sorglos zu handeln, sich unsozial zu verhalten und fremde Rechte nicht zu achten. Anbieter haben stetig mit Vorwürfen zu kämpfen, nicht genug Schutz vor derart unerwünschten – und zum Teil illegalen – Handlungen zu bieten, nicht genug Einfluss zu nehmen, übermäßig Daten zu sammeln, ihre Hände in Unschuld zu waschen, kurzum: sich unverantwortlich zu verhalten. Gleichzeitig wird von ihnen verlangt – und dies liegt häufig auch in ihrem eigenen Interesse –, nur sehr behutsam oder gar nicht in die Marktplätze der Meinungen einzugreifen, die sie ihren Nutzern bereitstellen. Dieses Spannungsfeld und die genannten Problemlagen finden sich – in gleicher oder ähnlicher Form – auch in anderen Bereichen des Netzes. Findet man für diese Themen im genannten Sektor Antworten auf die Frage, ob ein Digitaler Kodex zur Problemlösung beitragen und wie er konzipiert sein müsste, um Wirkmacht zu entfalten, ließen sich viele Erkenntnisse auf andere Bereiche und Problemfelder übertragen.

3. Persönlicher Anwendungsbereich: An wen könnte sich ein Digitaler Kodex richten?

Die Frage der Adressaten: Welche Akteure und welches Verhalten sind für einen Digitalen Kodex relevant?

In den vorangegangenen Abschnitten wurde eine Kategorisierung von Plattformen im Internet vorgenommen, um die Vielfalt von existierenden Plattform-Typen vor Augen zu führen. Sie verdeutlicht, dass es kaum zum Ziel führen kann, im Hinblick auf die Erfolgschancen eines Digitalen Kodex ganz allgemein von Plattformen und Akteurskonstellationen zu sprechen: Jeder Plattform-Typus bringt eine für ihn spezifische Akteurskonstellation mit sich. Auf Basis der Kategorisierung können bestimmte Fallbeispiele gebildet werden, auf die sich die Untersuchung fokussiert.

Die nun folgenden Überlegungen basieren auf der Entscheidung, eine Kategorie von Plattform auszuwählen, um die für sie typische Akteurskonstellation zu betrachten. Zu diesem Zweck wurde vorgeschlagen, die Kategorie „zentrale Kommunikationsplattform" auszuwählen, also allem voran soziale Netzwerke wie Facebook oder Google+. Auf ihnen kommen einige der meistdiskutierten Fälle von unerwünschtem Verhalten massenhaft vor. Das Ziel des folgenden Abschnitts ist es, an der Akteurskonstellation solcher Plattformen zu illustrieren, welche netzspezifischen Faktoren das Verhalten der Akteure beeinflussen, das heißt aufzuzeigen, welche Besonderheiten der Handlungsraum „zentrale Kommunikationsplattform" für die Nutzer, die Anbieter und den Staat aufweist.

Um auch diesbezüglich eine rein abstrakte Erörterung zu vermeiden, werden diese Besonderheiten des Handlungsraums anhand der drei Themen dargestellt, die oben als beispielhafte Regelungssachverhalte für die weitere Erörterung der Frage nach einem Digitalen Kodex vorgeschlagen wurden: Cybermobbing, Fehlverhalten beim Datenschutz und Urheberrechtsverletzungen. Damit werden neben drei möglichen Adressaten (das heißt den Akteuren) zugleich drei inhaltliche Themenbereiche angesprochen, auf die sich ein Digitaler Kodex mit Bezug auf zentrale Kommunikationsplattformen beziehen könnte.

Beobachtung des Akteursverhaltens auf zentralen Kommunikationsplattformen an drei Beispielen unerwünschter Phänomene

Die Hauptakteure auf zentralen Kommunikationsplattformen sind die Nutzer und die Dienste-Anbieter. Dem Staat kommt eine Rolle als Regulierungsinstanz zu.[32] In Bezug auf drei Beispielfälle von unerwünschtem Verhalten wird ihre Rolle im Folgenden in aller Kürze charakterisiert. Dabei soll verdeutlicht werden, welche netzspezifischen Verhaltensfaktoren **Cybermobbing, Fehlverhalten beim Umgang mit personenbezogenen Daten und persönlichen Informationen und Urheberrechtsverstöße** begünstigen bzw. dazu führen, dass diese Arten des unerwünschten Verhaltens derzeit nicht effektiv verhindert werden.

Erstes Phänomen: Cybermobbing – das hässliche Gesicht der sozialen Netzwerke

Cyber-Mobbing nennt man das Beleidigen, Bedrohen, Bloßstellen oder Ausgrenzen anderer mithilfe digitaler Kommunikationsmittel. Der zentrale Tatort für Cybermobbing sind soziale Netzwerke. Die am häufigsten betroffene Gruppe sind Jugendliche, die von Gleichaltrigen gemobbt werden. Die Opfer müssen Beleidigungen und Beschimpfungen ertragen, leiden unter der Verbreitung von Lügen oder Gerüchten über sie, werden bedroht oder in Online-Communitys ausgegrenzt. Eine empirische Studie, die im Frühjahr 2013 vorgestellt wurde, ergab, dass etwa 17 % aller Schüler schon Opfer von Cybermobbing geworden sind. 80 % dieser Fälle finden auf sozialen Netzwerken

32 Bei der Charakterisierung der Akteure wird deutlich werden, dass im Falle von Anbietern und Staat Organisationsinteressen, Machtfragen und die Frage der Verantwortlichkeit im Mittelpunkt stehen, während im Falle der Nutzer sozialpsychologische Aspekte zentral sind. Daran lässt sich bereits erahnen, dass der Status von Nutzern sich von den anderen beiden Akteuren klar unterscheidet. Dieser Aspekt wird später relevant werden, wenn die Frage behandelt wird, inwiefern Nutzer Adressaten eines Digitalen Kodex sein können.

statt. Die Studie ergab außerdem, dass nur jeder fünfte Schüler die Vorfälle den Betreibern der betroffenen Plattformen gemeldet hat.[33]

(a) Mögliche Gründe für Cyber-Mobbing und handlungsleitende Faktoren auf Online-Plattformen: Anonymität, Unkörperlichkeit

Bei dem Versuch, dieses Phänomen zu erklären, rücken die Handlungsbedingungen auf zentralen Kommunikationsplattformen in den Vordergrund: In der analogen Lebenswelt werden Umgangsformen durch die physische Präsenz einer gegebenenfalls sanktionsbereiten Öffentlichkeit stabilisiert. Umgekehrt hat die Möglichkeit, auf Kommunikationsplattformen **unkörperlich** aufzutreten, anscheinend einen enthemmenden Effekt und scheint unsoziales Verhalten wahrscheinlicher zu machen.[34] Hinzu kommen andere Faktoren, wie durch Vernetzungseffekte verstärkte Gruppendynamik und unter Umständen Anonymität.

Dass Letztere keine Grundvoraussetzung – sondern lediglich ein verstärkender Faktor – für Cybermobbing und ähnliches unsoziales Gruppenverhalten ist, zeigt sich daran, dass solche Phänomene gerade in sozialen Netzwerken besonders häufig vorkommen (siehe oben). Solche Netzwerke dienen aber grundsätzlich nicht dazu, anonym zu kommunizieren. Anbieter wie Facebook schreiben in ihren Nutzungsbedingungen sogar die Angabe zutreffender persönlicher Daten vor. Zwar können, da diese Angaben nicht systematisch auf ihre Richtigkeit überprüft werden, Nutzer ohne Weiteres auch falsche Angaben machen und sogenannte Fake-Profile anlegen, die ihnen anonyme Nutzungsmöglichkeiten gestatten. Zudem können – mangels Verifizierung der Angaben – auch Profile unter fremden Namen angelegt werden.[35]

Dennoch: Anonymität ist in vielen Fällen keine Grundvoraussetzung für die Beteiligung an Cybermobbing-Aktionen. Teils scheint es schon zu genügen, in der Masse aufzugehen, wie sich an der massenhaften Beteiligung personenbezogener Shitstorms zeigt.[36] Je nachdem, welche Züge solche Aktionen annehmen, kann man auch hier von einer Form des Cybermobbings sprechen. Sind Prominente Opfer solcher Attacken, werden sie meist sicht- und nachvollziehbar, weil diese Vorkommen zu Medienereignissen werden. Diese Angriffe belegen die Wirkungsmacht eines Handlungsraums, in dem allein das Ausbleiben von körperlicher Anwesenheit der Kommunikationsteilnehmer zu enthemmenden Effekten führt. Ob dies anonym geschieht oder nicht, scheint häufig zweitrangig zu sein.

(b) Cybermobbing und das Verhalten der Anbieter

Das Problem, wie Anbieter von Kommunikationsnetzwerken mit Cybermobbing umgehen können oder sollten, ist repräsentativ für ein generelles Problem. Je mehr der Anbieter der Plattform in die Kommunikation der Nutzer – und deren Auseinandersetzungen – eingreift, desto kostenintensiver und komplizierter wird der Betrieb des Dienstes. Die Anbieter würden sich zudem in eine staatsähnliche Rolle hineinmanövrieren, die in aller Regel mehr Schwierigkeiten aufwirft, als sie ihren eigenen Interessen nützt.

Hieran zeigt sich ein gewisses Grunddilemma bei zentralen Kommunikationsplattformen: Einerseits haben die Anbieter sehr großen Einfluss darauf, was auf ihren Diensten möglich ist und was nicht. Sie sind daher ein entscheidender Akteur, dem aufgrund seiner Handlungsmacht im Prinzip viel Verantwortung zuge-

33 Vgl. die Studie „Cyberlife – Spannungsfeld zwischen Faszination und Gefahr. Cybermobbing bei Schülerinnen und Schülern" des Bündnisses gegen Cybermobbing aus dem Mai 2013: www.buendnis-gegen-cybermobbing.de/Studie/cybermobbingstudie.pdf.

34 Der Sozialpsychologe John Suler (2004) spricht davon, dass durch mangelnde physische Präsenz (umschrieben mit invisibility – Unsichtbarkeit) Enthemmungs-Effekte (disinhibition effects) erzeugt werden. In unkörperlichen Räumen verhalten sich Menschen enthemmter, was positive wie negative Effekte nach sich zieht. Einerseits wird ein offener, persönlicher und intimer Umgang auch zwischen Menschen gefördert, die keine engen Beziehungen haben. Andererseits fördert der Abbau von Hemmungen auch unsoziale Verhaltensweisen. Murray (2011) drückt letzteren 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."

35 Findige Mobber machen hiervon mitunter Gebrauch, um ein zweites Profil ihres Opfers anzulegen. Hieraus ergeben sich perfide Möglichkeiten, es bloßzustellen. Die technisch erzeugten Handlungsräume digitaler Kommunikationsplattformen können – wie sich hieran zeigt – entgegen den Intentionen der Anbieter „umgenutzt" werden. Von diesen Möglichkeiten wird so lange Gebrauch gemacht werden, wie sie nicht systematisch vom Anbieter unterbunden werden.

36 Im vergangenen Jahr sind unter anderem der Schauspieler Jan Josef Liefers, der Sportler Mario Götze und die Politiker Horst Seehofer und Claudia Roth massiven Angriffen auf Facebook ausgesetzt gewesen.

schrieben werden kann. Fraglich ist jedoch, ob und in welchem Maß dies effizient und vor allem zumutbar wäre. Als privatwirtschaftliche Unternehmungen sind die Plattform-Anbieter keine gemeinnützigen Organisationen und können auch nur in Grenzen gezwungen werden, Gemeinwohlinteressen zu fördern oder moralische Kommunikationsstandards festzulegen und durchzusetzen.

Einheitliche Maßstäbe für alle Nutzer aufzustellen, wirft für den Anbieter zudem große Schwierigkeiten auf. Zentrale Kommunikationsplattformen sind globale Handlungsräume, in denen Nutzer aus unterschiedlichen Kulturen sich möglichst frei bewegen können sollen. Globale Erreichbarkeit führt oft zu Spannungen, interkulturellen Konflikten zwischen dem Anbieter und verschiedenen Nutzergruppen, mitunter sogar Regierungen oder religiösen Gruppen.[37]

Die US-amerikanischen Anbieter – und das sind zurzeit die entscheidenden – haben im Laufe der vergangenen Jahre eine zunehmend klare Position zu diesen Problemen entwickelt: Sie verstehen sich in erster Linie als Verteidiger der Meinungsfreiheit, weniger als Gralshüter von Zivilisationsstandards (Rosen, 2013). Sie stehen auf dem Standpunkt, dass die Durchsetzung solcher Zivilisationsstandards allgemeinverbindliche, klare und kulturübergreifende Standards erfordern würde, von denen man bezweifeln kann, dass es sie gibt. Sobald ganz unterschiedliche lokale kulturelle Ansprüche berücksichtigt würden, müssten für bestimmte Inhalte regional Publikationsverbote in Kraft treten, die letztlich zu einer „Balkanisierung des Internets" führen, die viele positive Effekte der globalen Kommunikation und Informationsvermittlung behindern würde. Letztlich bergen solche Eingriffe auch die sehr reale Gefahr in sich, ein System von Zensurmaßnahmen nach sich zu ziehen bzw. die Funktionsfähigkeit bestehender Zensur-Systeme auf das Internet zu übertragen (Rosen, 2013).

Des Weiteren spielen hier ökonomische Interessen der Anbieter eine bedeutende Rolle, die ihr Verhalten in starkem Maße beeinflussen: Sie wollen ihren Nutzern bei deren Wunsch nach größtmöglichen Handlungsmöglichkeiten entgegenkommen – eine Beschneidung dieser Möglichkeiten würde die Attraktivität ihres Plattform-Angebots potenziell schmälern.

(c) Cybermobbing und das Verhalten des Staates

Cybermobbing zu unterbinden, wäre, sofern hierbei rechtswidrige, vor allem strafbare Handlungen vorgenommen werden, auch die Aufgabe des Staates. Finden sie jedoch auf Online-Kommunikationsplattformen statt, stoßen die Regulierung durch Gesetz und Sanktionen über das Gewaltmonopol des Staates auf viele praktische Schwierigkeiten. Zwar sind viele im Rahmen des Mobbings begangene Handlungen in großen Teilen der Welt rechtswidrig oder sogar strafbar – man denke etwa an Beleidigungen oder Bedrohungen. Hiergegen kann daher – theoretisch – mit zivil- oder strafrechtlichen Maßnahmen vorgegangen werden.[38] Auch sind Maßnahmen gegen den Anbieter, wie Löschungspflichten etc., denkbar. Der Effizienz und Durchsetzbarkeit solcher Maßnahmen sind jedoch enge Grenzen gesetzt, die sich aus den besonderen Umständen bei Online-Kommunikationsplattformen ergeben.

Soweit sich Sanktionen gegen den Anbieter richten, stellt sich häufig das Problem, dass dieser nicht innerhalb der eigenen Jurisdiktion angesiedelt ist. Zwangsmaßnahmen werden hierdurch – zumindest auf der Durchsetzungsebene – erschwert. Richten sich etwaige Sanktionen an die Täter von Cybermobbing, ist zunächst erforderlich, dass diese bekannt sind. Selbst wenn sie bekannt sind, ist eine effiziente Rechtsdurchsetzung im Prinzip nur im Inland möglich. Extraterritorial ergeben sich nicht nur Schwierigkeiten bei der Durchsetzung von rechtlichen Maßnahmen gegen Verstöße, sondern auch im Hinblick auf die national unterschiedliche Rechtslage. Eine Tat, die in Deutschland strafbar ist, muss kei-

37 Ein Beispiel hierfür sind die Mohammed-Karikaturen, die 2010 erstmals in der dänischen Zeitung *Jyllands Posten* erschienen waren. Trotz Aufforderungen verschiedener religiöser Gruppen weigerte sich Facebook mit Verweis auf den eigenen, selbst gesetzten Kodex über den Umgang mit Hate Speech, sie in seinem System zu löschen (siehe im Einzelnen Rosen, 2013). Ein anderes Beispiel ist das Abschalten der Videoplattform YouTube in der Türkei, weil dort eine karikaturistische Darstellung Atatürks zu sehen war.

38 Vgl. hierzu Weitzmann, „Cyber-Mobbing, Cyberbullying und was man dagegen tun kann", irights.info/cyber-mobbing-cyberbullying-und-was-man-dagegen-tun-kann-2.

neswegs auch in Italien oder Russland strafbar sein. Selbst wenn es gelingt, den oder die Nutzer als Täter zur Rechenschaft zu ziehen, ist wegen der Persistenz und Dezentralität der Datenspeicherung nicht immer gewährleistet, dass die Tatfolgen – also insbesondere die zwecks Mobbing ins Netz gestellten Inhalte – effizient entfernt werden können.

Die Möglichkeiten des Staates sind damit häufig begrenzt. Es entsteht der Eindruck, dass er im Hinblick auf negative Phänomene wie Cybermobbing seine Verantwortung auf die Anbieter und Nutzer abschiebt. Er selbst scheint sich eher darauf zu verlegen, sich im Rahmen seiner Fürsorgepflicht gegenüber den Bürgern in schulischen Aufklärungsprogrammen zu betätigen und auf Beratungsangebote für Betroffene zu verweisen.[39]

Zweites Phänomen: Umgang mit personenbezogenen Daten und persönlichen Informationen durch Nutzer und Anbieter

Datenschutzprobleme auf Kommunikationsplattformen entstehen im Umgang mit personenbezogenen Daten sowohl auf Nutzer- als auch auf Anbieterseite.

Einerseits sind es die Nutzer selbst, die massenhaft eigene oder fremde personenbezogene Daten, persönliche Informationen, Bilder usw. auf Online-Plattformen verbreiten, ohne sich über die Folgen ihres Handelns Gedanken zu machen. Facebook-Nutzer etwa geben bei der Gestaltung ihres Profils und bei ihrer Kommunikation zahlreiche private Informationen in der Annahme preis, nur über eine rege Publikationstätigkeit ihre Kontakte in vollem Umfang mit Leben füllen zu können. Viele Nutzer achten dabei nicht auf einen möglichst „sparsamen" Umgang mit ihren Daten, persönlichen oder gar intimen Informationen.

Die Anbieter haben an diesem unbekümmerten Umgang der Nutzer mit ihren persönlichen Daten in gewisser Hinsicht ein Interesse. Ihre Geschäftsmodelle basieren offensichtlich zumindest teilweise auf einer ökonomischen Verwertung personenbezogener Daten, unter anderem auf deren Weitergabe an Dritte und mannigfaltiger Auswertung. Dabei sind die Modelle und Methoden häufig nicht transparent. Aufgrund ihrer Gestaltungsmacht sehen sich die Anbieter andererseits erheblichen Forderungen von Politik und Gesellschaft ausgesetzt, Daten und persönliche Informationen ihrer Nutzer zu schützen und Maßnahmen für den Schutz der Nutzer vor sich selbst zu treffen.

(a) Fehlverhalten beim Umgang mit personenbezogenen Daten und persönlichen Informationen von Seiten der Nutzer

Nutzer, die die Angebote zentraler Kommunikationsplattformen in Anspruch nehmen, tun dies aus unterschiedlichsten Bedürfnissen. Eine Besonderheit bei diesen Plattformen ist, dass sie gratis zugänglich sind. Als Gegenleistung „zahlen" Nutzer dieser Dienste mit ihren preisgegebenen Daten und persönlichen Informationen.[40]

Im Übrigen erscheint es plausibel, dass die Nutzer sozialer Netzwerke private Informationen bewusst in extensivem Maß preisgeben, um ihre Kommunikationschancen zu erhöhen – und dies gerade in Bezug auf vergleichsweise „lose" Kontakte mit schwachen Bindungen. Der amerikanische Soziologe Mark Granovetter stellte in den 1970er-Jahren seine Theorie von der **Stärke schwacher Bindungen** (Granovetter 1973) zur Diskussion.[41] Weil starke Bindungen, etwa bei Freundschaften, Familienangehörigen oder Arbeitskollegen, in der Regel dazu führen, dass die beteiligten Personen ein sehr ähnliches Beziehungsgeflecht aufweisen, wird zwischen ihnen nur vergleichsweise wenig neue Information ausgetauscht. Dagegen haben schwache Bindungen – zum Beispiel solche, die auf flüchtigen physischen oder unkörperlichen Begegnungen basieren, wie sie in sozialen Netzwerken oft vorkommen – weitaus mehr Potenzial, um an Neuigkeiten und innovative Ideen zu gelangen. Um als Kommunikationspartner in schwachen Bindungen auch für andere attraktiv zu sein und zu bleiben, sind Nutzer bereit, weitaus mehr Informationen in sozialen Netzwerken preiszugeben, als es bei Kontakten mit starken Bindungen notwendig wäre.

39 www.bmfsfj.de/cybermobbing.

40 Vgl. nächster Abschnitt.

41 Einführend zu Granovetter der Eintrag in Wikipedia: de.wikipedia.org/wiki/Mark_Granovetter.

Die Bindung an zentrale Kommunikationsplattformen gewinnt ihre Kraft nicht allein aus den bestehenden und vertrauten Kontakten, sondern auch aus den Möglichkeiten der vergleichsweise losen Kontakte. Jenseits ihrer bestehenden Kontakte suchten laut der BITKOM-Studie 2011 37 % der Nutzer auch nach neuen Kontakten. In der Regel wird es sich hierbei um die Suche nach Kontakten mit schwacher Bindung handeln. Entsprechend spricht einiges für die Annahme, dass diese – zu besonderer Offenheit anreizenden Kontaktformen – in sozialen Netzwerken eine besondere Rolle spielen.

Daneben liegt eine wichtige Motivation zur Nutzung sozialer Netzwerke natürlich auch in der privaten Kontaktpflege mit Freunden und Bekannten (BITKOM 2011, 4). In diesen Kontakten mit starker Bindung spielen weitere Bedürfnisse eine relevante Rolle, zum Beispiel die Diskussion wichtiger persönlicher Angelegenheiten oder (politischer) Ereignisse. Neben diesen engen Kontakten besteht aber auch das Bedürfnis, sich über Veranstaltungen und Unternehmungen zu informieren sowie „auf dem Laufenden" zu bleiben.

(b) Umgang mit personenbezogenen Daten und persönlichen Informationen auf Seiten der Anbieter

Auf Seiten der Anbieter sind in puncto Datenschutz zumindest zwei Aspekte von Belang: (i) zum einen der Umgang der Anbieter mit den Daten und personenbezogenen Informationen, die die Nutzer hinterlassen, (ii) zum anderen die Frage danach, welchen Einfluss die Anbieter auf das Verhalten der Nutzer hinsichtlich ihres Umgangs mit ihren eigenen Daten haben.

(i) Anbieter zentraler Kommunikationsplattformen sind privatwirtschaftliche Unternehmen. Ein wesentlicher Punkt, der das Verhalten der Anbieter erklärt, sind die besonderen wirtschaftlichen Gegebenheiten, denen zentrale Online-Angebote unterliegen. Die meisten der großen Kommunikationsplattformen sind kostenlos nutzbar, deren Angebot aber ist mit hohen Produktionskosten verbunden. Um Refinanzierungsmöglichkeiten zu eröffnen, müssen die Dienste so gestaltet sein, dass mittelbar Einnahmen erzielt werden können.

Hierfür gibt es verschiedene Ansätze. Beispielsweise werden gezielt Daten gesammelt, um eine möglichst zuverlässige Wissensbasis für die individualisierte Zielgruppenansprache, vor allem durch individualisierte Werbung, zu schaffen. Gerade soziale Netzwerke scheinen hierauf zu setzen. Ein weiterer Baustein der Geschäftsmodelle, besonders ausgeprägt bei sozialen Netzwerken, liegt darin, dass Interkonnektivität und Datenportabilität unterbunden werden. Facebook, Google+, LinkedIn und XING bieten keine Möglichkeit, direkt mit den Nutzern jeweils anderer Netzwerke zu kommunizieren oder die in einem Netzwerk generierten Daten, Inhalte und Kontakte in ein anderes Netzwerk zu exportieren. Auf diese Weise gewinnt der Anbieter maximale Hoheit über die Datenkommunikation. Ohne Interkonnektivität und Datenportabilität werden Netzwerk- und Lock-In-Effekte, also die Bindung an einen Anbieter, erheblich gesteigert. Dies wiederum fördert Monopolbildung und zentralisierte Märkte (Zittrain 2008, 177) und wirkt sich erheblich auf die Handlungsmacht und den Einfluss der Anbieter gegenüber ihren Nutzern aus.[42] Um solche Effekte zu verringern, enthält der Entwurf für eine EU-Datenschutzverordnung ein „Recht auf Datenübertragbarkeit".[43]

Solche Geschäftsmodelle führen schnell zu Konflikten mit rechtlichen und sozialen Normen. Auch stoßen sie häufig auf Unverständnis und führen zu weitgehenden Forderungen an die Anbieter, etwa in der Form, sich neben ihrer profitorientierten Tätigkeit als Hüter von Nutzer-Grundrechten oder Paternalisten zu verstehen.

Dabei wandeln sich Geschäftsmodelle im Netz sehr stark und sind in ständigem Fluss. Plattform-Anbieter scheinen oftmals erst einmal Daten zu sammeln, ohne zu wissen, ob sie mit dem Gesammelten (zum Beispiel personenbezogenen In-

42 Können Nutzer den Anbieter bzw. die Plattform aufgrund solcher Umstände nicht wechseln, wird die Entstehung von Wettbewerb erschwert. Es können sich faktische Monopole bilden, was sich wiederum auf die Regulierung auswirken muss. So ist zum Beispiel Transparenz in monopolisierten Märkten – insbesondere, wenn das Produkt oder der Dienst für die Zielgruppe von großer Bedeutung ist – ein wenig wirksames Mittel.

43 Siehe Art. 18 des Entwurfs unter: www.eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:DE:PDF.
Siehe hierzu auch das Interview mit dem Bundesdatenschutzbeauftragten Peter Schaar unter www.collaboratory.de/w/Interviewzusammenfassung_Peter_Schaar#Datenportabilit.C3.A4t.

formationen) etwas anfangen, zum Beispiel die Daten kommerzialisieren können. Anbieter haben bei Daten- und Persönlichkeitsschutzfragen einander entgegengesetzte Motivationen zu balancieren; das Streben nach wirtschaftlichem Erfolg auch unter Einsatz ihres gesammelten Datenmaterials steht in Konflikt mit den Datenschutz- und Privatsphärenschutz-Ansprüchen, die Politik und Gesellschaft an sie herantragen.

Zu fragen wäre hier, ob es Möglichkeiten gibt, die Anbieter dazu zu bringen, freiwillig Datenschutz- und anderen Bestimmungen über den Schutz der Privatsphäre nachzukommen. Was könnte ihnen als Ausgleich für unter Umständen verloren gegangene Gewinnerwartungen als Anreiz geboten werden? Wie bringt man diese Unternehmen dazu, mehr oder weniger freiwillig die staatliche Aufgabe, für Bürger im Bereich Schutz der Privatsphäre Fürsorge zu tragen, zumindest in Teilen zu übernehmen?

(ii) Ein anders gelagerter Aspekt in diesem Zusammenhang ist die Frage, inwieweit die Anbieter das Nutzerverhalten im Umgang mit eigenen personenbezogenen Informationen steuern können. Beispielsweise nehmen die Anbieter durch die Standardeinstellungen für die Privatsphäre der Nutzerkonten Einfluss auf das Nutzerverhalten, etwa wenn es darum geht, wer die Nutzerprofile einsehen kann. Große Teile der Nutzer nehmen die Möglichkeit, ihre Einstellungen an die persönlichen Belange anzupassen, nicht wahr. Was der Anbieter als Standard voreinstellt, bleibt also sehr häufig in Kraft. Hieran zeigt sich deutlich, wie Anbieter unreflektiertes Nutzerverhalten lenken können.

Gerade bei Anbietern mit einer nahezu monopolartigen Marktstellung ist zu bezweifeln, dass kritische Debatten in der medialen Öffentlichkeit sie in diese oder jene Richtung beeinflussen können. Warum sollen sie etwa selber auf Gefahren hinweisen, die im Zusammenhang mit einem allzu sorglosen Umgang mit persönlichen Informationen entstehen können? Warum sollten sie sich zu mehr Transparenz verpflichten, wenn Intransparenz und Komplexität für ihre eigenen Belange von Vorteil ist? Zwar ist durchaus anzunehmen, dass den Anbietern zentraler Kommunikationsplattformen daran gelegen ist, zumindest ein basales Vertrauensverhältnis mit den Nutzern aufrechtzuerhalten. Immerhin sind die Nutzer und ihre Inhalte ihr hauptsächliches – vielleicht sogar einziges – Kapital. Solange sich aber zum Beispiel ein etwaiger Vertrauensrückgang bei jugendlichen Nutzern[44] nicht nennenswert negativ auf die Nutzerzahlen auswirkt – oder diese aus anderen Gründen sogar steigen –, stellt sich die Frage, warum die Anbieter mit selbstbeschränkenden Maßnahmen reagieren sollten.

(c) Umgang mit personenbezogenen Daten und persönlichen Informationen und das Verhalten des Staates

Wie im Strafrecht ist die staatliche Gestaltungsmacht gegenüber zentralen Kommunikationsplattformen auch in Bezug auf den Datenschutz beschränkt. Dies zeigt sich zum Beispiel daran, dass die Versuche des Gesetzgebers, bei Datenschutzerklärungen der Anbieter mehr Transparenz zu erreichen, bislang kaum erfolgreich waren.[45] Dass die meisten Anbieter dieses Plattformtyps außerhalb des Staatsgebiets angesiedelt sind, verringert den Einfluss eines einzelnen Staates erheblich.

Das zeigt sich an einem Beispiel: Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) hatte versucht, Facebook dazu zu zwingen, sich von der Klarnamenpflicht – jedenfalls für deutsche Nutzer – abzuwenden. Der Grund: Deutsches Datenschutzrecht schreibt vor, dass Online-Dienste generell so ausgestaltet werden müssen, dass sie auch anonym genutzt werden können. Erfolg hatte das ULD am Ende nicht. Das Oberverwaltungsgericht Schleswig lehnte das Anliegen in einer rechtskräftigen Entscheidung mit der Begründung ab, dass der Dienst nicht deutschem, sondern irischem Datenschutzrecht unterliege.[46]

Um einem solchen „Forum-Shopping" innerhalb von Europa vorzubeugen, versucht die EU schon seit

44 Einen solchen diagnostiziert zum Beispiel die Jim-Studie 2012 (Jugend, Information Multimedia) des medienpädagogischen Forschungsverbundes Südwest, www.mpfs.de/index.php?id=527.

45 Vgl. Weitzmann (2013).

46 Vgl. die Pressemitteilung des ULD vom 24. April 2013, www.datenschutzzentrum.de/presse/20130424-facebook-klarnamen-ovg.htm.

einiger Zeit, Einigung über eine EU-Datenschutzverordnung zu erzielen. Eine solche würde zu einer echten Harmonisierung des Datenschutzrechts – jedenfalls in Bezug auf die hierin geregelten Themen – führen, da sie in den Mitgliedstaaten unmittelbar anwendbar wäre. Ob sich der Ansatz durchsetzt und den Einfluss der Mitgliedstaaten bei der Durchsetzung hoher Datenschutzstandards in der gesamten EU gegenüber US-amerikanischen Anbietern von Kommunikationsplattformen erhöht, ist derzeit aber eher zweifelhaft. Zum einen liegt das Vorhaben offenbar bis auf Weiteres auf Eis.[47] Zum anderen wäre es den Anbietern auch in diesem Fall unter Umständen noch möglich, dem höheren Schutzniveau zu entgehen, etwa indem sie ihre Datenverarbeitung vollständig in den USA durchführen und in Europa gar keine Niederlassungen mehr betreiben, in denen Daten verarbeitet werden.

Diese Beispiele zeigen, dass die Handlungsoptionen des Staates im Bereich der gesetzlichen Regulierung und Sanktion eingeschränkt sind. Indem er sich allerdings rein auf Beratungs- und Aufklärungsangebote beschränkt, um die Bürger von einem allzu sorglosen Umgang mit ihren Daten und persönlichen Informationen abzuhalten, wird der Staat seinem Schutzauftrag für die Bürger kaum vollständig Genüge tun können.

Es wäre daher zu untersuchen, ob der Staat bei alternativen Regulierungsformen wie einem Digitalen Kodex mitwirken und welche Rolle er hierbei spielen könnte. Bisherige Versuche in diese Richtung waren nicht von Erfolg gekrönt. So ist beispielsweise ein von der deutschen Politik mit erheblichem Aufwand unterstützter Versuch, einen Verhaltens-Kodex für die Anbieter sozialer Netzwerke zu etablieren, gescheitert.[48] Solche Fälle werfen wichtige Fragen über mögliche Erfolgs- und Misserfolgsfaktoren bei der Konzeption und Implementierung von Kodizes auf: Wäre es beispielsweise möglich, bestimmte Anreizsysteme in einem Digitalen Kodex zu verankern, die geeignet wären, das Verhalten von Plattform-Betreibern positiv zu beeinflussen? Wie können Anreize aussehen, die die Anbieter dazu bringen, ihr Verhalten – unter Umständen entgegen den eigenen Interessen – zu verändern? Sind Kodizes für ein einziges Land – also etwa ein Digitaler Kodex für Deutschland – für die Anbieter interessant genug bzw. überhaupt handhabbar?

Drittes Phänomen: Urheberrechtsverletzungen auf Kommunikationsplattformen

Das rechtswidrige Einstellen urheberrechtlich geschützter Inhalte ist ein häufiges Problem auf zentralen Kommunikationsplattformen. Den Nutzern drohen Abmahnungen, die Anbieter müssen diese Inhalte gegebenenfalls löschen, die Rechteinhaber können sich nicht effizient gegen schädliche und unerlaubte Nutzungen – sofern sie in solchen Konstellationen vorkommen – wehren.

Eine Lösung der Problematik in Form gesetzlicher Regulierung ist nicht abzusehen. Das Urheberrecht ist eine nationale Materie. Seine transnationale Durchsetzung ist (wie auch bei anderen Rechtsgebieten, siehe oben zum Cybermobbing) großen Schwierigkeiten unterworfen. Der Gesetzgeber könnte sich zwar entschließen, solche Nutzungen generell zu erlauben, und hierfür gegebenenfalls pauschale Vergütungszahlungen vorsehen. Solche Maßnahmen würden zu einer generellen Lösung für Nutzer, Rechteinhaber und Anbieter jedoch nur beitragen, wenn sie zumindest europaweit und besser international verankert wären. Dies ist jedoch weder kurz- noch mittelfristig zu erwarten.

(a) Urheberrechtsverletzungen und das Verhalten der Nutzer

Im Rahmen ihrer umfassenden, oft kreativen Publikationstätigkeiten bringen sich die Nutzer von Facebook oder YouTube häufig in Schwierigkeiten, indem sie zum Beispiel fremde Fotos oder selbst gedrehte Videos veröffentlichen, auf bzw. in denen urheberrechtlich geschütztes Material zu sehen ist: „Zeigen die Filmaufnahmen zum Beispiel die eigene Coverband, können die Komponisten, Interpreten und Plattenfirmen für das Nachspielen der Songs Lizenzgebühren verlangen. Auch das Einbinden von YouTube-Videos kann Ärger nach sich ziehen, denn der Nutzer haftet

47 Siehe www.telemedicus.info/article/2584-EU-Datenschutzverordnung-vorerst-auf-Eis-gelegt.html.

48 Siehe www.telemedicus.info/article/2569-Kodex-zur-Selbstregulierung-fuer-soziale-Netzwerke-gescheitert.html.

für die Inhalte des Filmschnipsels. Verletzt es bestehende Rechte, kann der Profilinhaber Post von Anwälten bekommen."[49]

Zu vermuten ist, dass viele dieser Urheberrechtsverletzungen aus Unwissenheit der Nutzer passieren. Doch auch gut informierten Nutzern können im Rahmen ihrer publizistischen Tätigkeiten auf den Plattformen Fehler unterlaufen. Dies zeigt sich unter anderem an Beispielen, in denen Unternehmen oder auch Politiker – im Zweifel unbewusst – gegen Urheberrechte verstoßen haben. Beispielsweise wurde im Jahr 2011 dem damaligen Vorsitzenden des Bundestags-Rechtsausschusses Siegfried Kauder vorgeworfen, auf seiner Webseite unautorisiert Fotos zu verwenden.[50]

Das Urheberrecht ist ein äußerst komplexes Rechtsgebiet, das ursprünglich ausschließlich für professionelle Adressaten (professionelle Künstler, Plattenfirmen, Verlage usw.) konzipiert wurde (Kreutzer 2012). Es korrekt anzuwenden und sich stets regelkonform zu verhalten, ist angesichts einer Vielzahl komplexer und ungeklärter Rechtsfragen heutzutage niemandem, schon gar nicht Privatpersonen, möglich.

(b) Urheberrechtsverletzungen und das Verhalten der Anbieter

Die Anbieter zentraler Kommunikationsplattformen beachten bestehende Urheberrechtsgesetze, indem sie auf ihnen angezeigte Urheberrechtsverstöße mit der Löschung der entsprechenden Inhalte auf ihren Seiten reagieren (sog. Notice-and-take-down-Verfahren).

Ein originäres Interesse am Schutz der Urheberrechte anderer haben Anbieter von zentralen Kommunikationsplattformen nicht. Ihr Angebot profitiert zunächst davon, dass alle möglichen Inhalte möglichst frei kursieren können. Ob sie vom Rechteinhaber selbst oder einem Dritten eingestellt werden, ob der Dritte hierfür eine Genehmigung hatte, macht für den Anbieter so lange keinen Unterschied, wie er nicht in die Rechtsbeziehungen zwischen den Nutzern und Dritten (hier: den Rechteinhabern) hineingezogen wird. Erst massenhafte Löschungsanfragen oder gar rechtliche Maßnahmen gegen den Anbieter selbst führen zu einer Beeinträchtigung der eigenen Interessen.

Angesichts dessen ist erklärlich, dass Anbieter sich aus diesen Auseinandersetzungen so weit wie möglich heraushalten wollen. Abgesehen von Vorrichtungen und Systemen, die Notice-and-take-down-Maßnahmen ermöglichen, wird in der Regel in erster Linie auf das Verhalten der Nutzer verwiesen. Durch vertragliche Nutzungsbedingungen werden sie angehalten, keine Urheber- oder sonstige Rechte Dritter zu verletzen, zumeist unter Androhung von Sanktionen. Wer bei Facebook beispielsweise unter Verstoß gegen die „Erklärung der Rechte und Pflichten" Rechtsverletzungen begeht, kann im Wiederholungsfall auch vom Dienst ausgeschlossen werden.

(c) Urheberrechtsverletzungen und das Verhalten des Staates

Ähnlich wie beim Datenschutz entziehen sich zentrale Kommunikationsplattformen weitgehend den traditionellen Werkzeugen staatlicher Lenkung, vor allem, weil sie über nationale Grenzen hinweg agieren. Zwar ist die Durchsetzung des Urheberrechts – anders als des Datenschutzrechts – als privatrechtliche Materie grundsätzlich nicht Sache des Staates. Dennoch wird von den politischen Akteuren oft gefordert, sich mehr für eine bessere Durchsetzbarkeit von Urheberrechten und diesbezügliche Systeme einzusetzen bzw. gesetzliche Vorgaben hierfür zu entwickeln. Ein Beispiel hierfür ist die Debatte um Warnhinweise bei urheberrechtsverletzenden Webseiten.[51]

Gesetzliche oder andere staatliche Maßnahmen gegen Urheberrechtsverletzungen auf zentralen Kommunikationsplattformen wie sozialen Netzwerken zu treffen, stößt auf eine Vielzahl erheblicher Schwierigkeiten. Diese decken sich teilweise mit denen beim Datenschutzrecht, ergeben sich also zum Beispiel daraus, dass die Dienstanbieter häufig im Ausland sitzen und daher schwer in die Verantwortung genommen werden können.

49 Siehe www.stern.de/digital/online/urheberrechtsverletzungen-bei-facebook-eine-pinnwand-fuer-15000-euro-1715257.html.

50 Siehe www.spiegel.de/netzwelt/netzpolitik/angebliche-foto-vergehen-copyright-kaempfer-kauder-hat-urheberrechte-verletzt-a-789073.html.

51 Siehe zum Beispiel www.netzpiloten.de/bundeswirtschaftsministerium-verhandelt-warnhinweismodell-unter-ausschluss-der-offentlichkeit/

Selbst wenn dies möglich wäre, stellt sich durchaus die Frage, ob, in welchem Umfang und mit welcher Begründung sie hierfür gesetzlich in die Verantwortung genommen werden können. Im Rahmen der allgemeinen Verantwortlichkeitsregeln für Internet-Dienste hat man sich schon bei Verabschiedung der E-Commerce-Richtlinie aus dem Jahr 2000 dafür entschieden, dass Internet-Service-Provider (wie die Anbieter sozialer Netzwerke) nur eingeschränkt für Rechtsverletzungen der Nutzer haften müssen. Sie können zwar zur Löschung entsprechender Inhalte verpflichtet, nicht aber für zum Beispiel Schadensersatz- oder andere Kompensationsansprüche in Anspruch genommen werden.[52] Diese Verantwortlichkeit auszuweiten, wird derzeit ersichtlich nicht ernsthaft erwogen. Dies wäre eine kritische Maßnahme, die dazu führen könnte, dass die Dienstanbieter in unzumutbarer Weise in die Rechtsverhältnisse zwischen ihren Nutzern und Dritten hineingezogen und so zu einer Art privatrechtlicher Hilfssheriffs gemacht würden.

Vor diesem Hintergrund stellt sich die Frage, welchen Einfluss der Staat ausüben könnte, um das Nutzerverhalten möglicherweise durch einen von den Anbietern zu implementierenden (siehe hierzu sogleich) Digitalen Kodex positiv beeinflussen zu können, und mit welchen Mitteln dies erreicht werden könnte.

Zusammenfassung: Die Akteure auf zentralen Kommunikationsplattformen, deren Verhalten und Beweggründe

Die Betrachtung der Akteurskonstellation auf zentralen Kommunikationsplattformen vor dem Hintergrund dreier Beispiele für unerwünschtes Verhalten sollte zweierlei aufzeigen: zum einen beispielhaft inhaltliche Bereiche, auf die sich ein Digitaler Kodex beziehen könnte. Zum anderen sollte verdeutlicht werden, inwieweit der Handlungsraum Internet Besonderheiten für die Akteure und ihr Verhalten aufweist, die ein Digitaler Kodex in Rechnung stellen müsste.

Für Nutzer bestehen die Besonderheiten zentraler Kommunikationsplattformen im Internet vor allem darin, dass sie unkörperliches und anonymes Handeln ermöglichen, welches unerwünschtes Verhalten provozieren kann. Des Weiteren zeigt sich, dass Nutzer auf diesen Plattformen tendenziell zu einem gesteigerten Publikationsverhalten neigen, um ihre Attraktivität für andere Nutzer – vor allem im Rahmen „loser" Bindungen – zu steigern. Dieses Verhalten scheint die Reflexionsbereitschaft im Hinblick auf Probleme des Datenschutzes und des Urheberrechts abzuschwächen. In allen drei Bereichen unerwünschten Verhaltens ist von Wissens- und Sensibilisierungsdefiziten auszugehen, doch ein gewichtiger Teil der Probleme, die bei Nutzern auftreten (insbesondere beim Datenschutz), müssen dem Anbieter mit angelastet werden.

Die Anbieter haben große Gestaltungsmacht, weshalb es zunächst naheliegend erscheint, ihnen erhebliche Verantwortung, auch für das Verhalten der Nutzer, zuzuschreiben. Daraus ergibt sich für sie als Akteure eine zwiegespaltene Rolle, weil sie in erster Linie privatwirtschaftliche Interessen über netzspezifische Geschäftsmodelle verfolgen, aber zugleich von ihnen verlangt wird, ihre Nutzer zu schützen. Die Situation wird zusätzlich durch interne Interessenkonflikte verkompliziert: Ein effizienter Nutzerschutz kann zum Beispiel langfristigen Geschäftsinteressen dienen, obwohl er kurzfristig wirtschaftliche Einbußen bedeutet.[53]

Infrage steht, inwieweit es Anbietern zugemutet werden kann, und bei genereller Betrachtung wünschenswert ist, für die Realisierung von Gemeinwohlinteressen und die Sicherung von Grundrechten in die Pflicht genommen zu werden, also für Aufgaben, die genuine Staatsaufgaben sind. Man könnte die Frage auch anders stellen: Inwieweit kann es geboten und gerechtfertigt sein, in die Geschäftsmodelle und Funktionsfähigkeit der Plattformen einzugreifen, um etwaigen schädlichen Auswirkungen von Kommunikationsplattformen auf Grund- und Freiheitsrechte zu begegnen?

52 Wie weit die Verantwortlichkeit eines Dienstanbieters im Einzelfall geht, ist eine komplexe und umstrittene Frage, die hier nicht im Detail erörtert werden kann. Es soll daher nur auf das Grundprinzip hingewiesen werden.

53 So mag es die Attraktivität eines sozialen Netzwerks steigern und Vorbehalte verringern, wenn Persönlichkeitsrechtsverletzungen und Cybermobbing effizient unterbunden werden. Allerdings müsste der Anbieter hierfür verstärkt in die Kommunikation zwischen den Nutzern eingreifen und hierfür aufwendige und kostspielige Systeme implementieren. Der Anbieter befindet sich daher in einem internen Interessenkonflikt, dessen Abwägung aufgrund einer Vielzahl unkalkulierbarer Faktoren kaum präzise möglich ist. Wie viele neue Nutzer ein effizientes Vorgehen gegen Cybermobbing anziehen würde, ist zum Beispiel kaum zu ermitteln.

Diese Fragen haben viele Facetten, auf die hier nicht im Einzelnen eingegangen werden kann. Schon auf den ersten Blick zeigt sich eine erhebliche Ambivalenz bei der Regulierung von zentralen Kommunikationsplattformen. Regulierungsmaßnahmen müssen sich zunächst stets an der Tatsache orientieren, dass solche Netzwerke als zentrale Marktplätze der Meinungen erhebliche Bedeutung für die Ausübung der Kommunikationsgrundrechte der Nutzer haben. Massive oder gar existenzbedrohende staatliche Eingriffe gegenüber den Anbietern verbieten sich also schon hinsichtlich des Schutzes der Nutzerinteressen. Daneben ist zu berücksichtigen, dass die Geschäftsinteressen der Anbieter ebenfalls Grundrechtsschutz genießen. Auch dies ist zu bedenken, wenn erwogen wird, ihnen Schutzfunktionen gegenüber den Nutzern aufzuerlegen, die ihren eigenen Interessen widersprechen. Die Anbieterinteressen werden sich in vielen Fällen mit solchen Aufgabenverpflichtungen nicht in Einklang bringen lassen. Es ist fraglich, welcher Spielraum für Regulierung angesichts dieser Gemengelage verbleibt.

Natürlich könnten die Anbieter ein Interesse daran entwickeln, ihre Geschäftsmodelle im Hinblick auf die Nutzer-Datenverwertung – als vertrauensbildende Maßnahme – freiwillig anzupassen. Zumindest könnten sie diesbezüglich mehr Transparenz herstellen, etwa indem den Nutzern klar verständlich dargelegt wird – sofern das angesichts der Komplexität solcher Materien überhaupt möglich ist –, was mit ihren Datenspuren geschieht und wie sie gegebenenfalls kommerzialisiert werden. Solange die Nutzerzahlen sozialer Netzwerke allerdings steigen und das Nutzervertrauen nicht über alle Maßen abnimmt, werden die Anbieter ihre jetzige Haltung kaum ändern.

Der Staat handelt mit seinen herkömmlichen Regulierungsformen im Falle transnational operierender Plattform-Anbieter unter erschwerten Bedingungen, seine Bemühungen um Einflussnahme sind bislang eher ineffizient. Hinzu treten die oben genannte Ambivalenz und Abwägungsschwierigkeiten in Bezug auf die staatliche Einflussnahme in solche kommunikativen Räume. Im Rahmen seiner Fürsorgepflicht tritt er angesichts solcher und im Zweifel weiterer Probleme weniger als Schutzherr über Bürgerrechte, sondern eher als Initiator und Förderer von Aufklärungs- und Beratungsprogrammen auf. Dieses Engagement des Staates ist allerdings in vielerlei Hinsicht noch defizitär. Obwohl zum Beispiel das Thema soziale Netzwerke Schulen bereits erreicht hat, fehlt es dort häufig an qualifiziertem Lehrpersonal. Ganz generell werden Themen zur Medienpraxis und Medienkritik nicht in einem eigenen Fach behandelt, sondern tauchen eher bruchstückhaft im Deutsch- oder Informatikunterricht auf.

Hiervon abgesehen stellt sich die Frage, ob der Staat seiner Akteursrolle angesichts der evidenten Regulierungs- und Durchsetzungsdefizite mit Bildungs- und alternativen Regulierungsansätzen ausreichend gerecht werden kann. Könnte er darüber hinaus bei der Aufsetzung und Implementierung eines Digitalen Kodex eine weitere Rolle einnehmen? Wie könnte sie aussehen?

„Kodex" – ein Begriffsvorschlag

Die hierzu angestellten Beobachtungen münden in einen ersten Vorschlag, wie der Terminus „Kodex" begrifflich angelegt sein könnte. Dieser Vorschlag soll unter anderem plausibilisieren, dass in erster Linie die Plattform-Anbieter als direkte Adressaten eines Digitalen Kodex infrage kommen und weniger die Nutzer oder der Staat. Eine Untersuchung, die die Etablierung eines Digitalen Kodex anstrebt, kommt nicht um die Aufgabe herum, den Grundbegriff „Kodex" näher zu bestimmen. Klar ist, dass es sinnlos ist, sich über die „wahre" Bedeutung von Wörtern zu streiten. Worauf es ankommt, ist, unterschiedliche Bedeutungen eines Wortes zu unterscheiden und sich darüber im Klaren zu sein, in welcher Bedeutung man es verwenden will.

An dieser Stelle kann keine vollständige Begriffsanalyse erfolgen, erst recht keine etymologische Untersuchung. Stattdessen soll eine bestimmte Verwendung des Begriffes plausibilisiert und zur Diskussion gestellt werden.

Alltagssprachlich verstehen wir unter einem Kodex eine Sammlung von Verhaltensregeln, die für eine gesellschaftliche Gruppe oder die ganze Gesellschaft Geltung besitzt. Allerdings ist ein solcher Begriff recht unscharf, sodass sämtliche geschriebenen oder ungeschriebenen Verhaltenskataloge Kodizes genannt werden könnten. Wenn man sich jedoch Kodizes ansieht, die heutzutage unter diesem Namen in Kraft sind,

dann fällt auf, dass sie sich fast immer auf eine Berufsgruppe beziehen. Als Beispiele können hier der Pressekodex, der Eid des Hippokrates und der Kodex zur „Sicherung guter wissenschaftlicher Praxis" der Deutschen Forschungsgemeinschaft genannt werden.[54]

Kodizes sind demnach Verhaltenskataloge der besonderen Art. Sie spitzen zentrale moralische Prinzipien und soziale Normen mithilfe von Praxisregeln auf ein Berufsfeld zu, sie formulieren Grundsätze des handwerklichen Könnens, und sie geben in der Regel auch an, warum diese Verhaltensregeln für diese Gruppe überhaupt aufgestellt werden: wegen der gesellschaftlich bedeutsamen Funktion eines Berufsstandes. Hinzu kommen drei Besonderheiten: (a) Kodizes scheinen immer eine „externe" Beobachtungsinstanz mit sich zu bringen, die eine Kontrollfunktion übernimmt, beim Pressekodex zum Beispiel den Presserat. Dies dürfte auch daran liegen, dass (b) Kodizes nicht selten von Repräsentanten des jeweiligen Berufsstandes selbst ins Leben gerufen werden, die die Umsetzung ihres eigenen Kodex im Zweifel weniger streng kontrollieren als ein Gremium, dessen Mitglieder dem Berufsstand nicht angehören. (c) Kodizes haben mehrere Funktionen: Sie sollen eine weiter gehende Professionalisierung vorantreiben, Orientierung ermöglichen, Reflexion anstoßen, öffentlich wahrnehmbare Korrekturen anmahnen und ein Selbstbild der Profession etablieren.

Diese Auffassung des Kodex-Begriffs passt sehr gut zur Gegenwartsgesellschaft. Sie zeichnet sich unter anderem dadurch aus, dass das meiste in ihr sich durch organisatorisches Handeln vollzieht. Die in Organisationen handelnden Menschen sind gebunden an professionelle Rollen. Personen in diesen Rollen sind dadurch in der Regel auf eine rollenspezifische Aufgabenverantwortung ausgerichtet, die ihnen durch die Organisation übertragen wird. Dies verhindert freilich nicht, dass sie als Personen moralisch verantwortlich sein können (und vielleicht auch wollen) und dass Aufgabenverantwortung und moralische Verantwortung konfligieren können.

Ein Kodex, der sich auf professionelles Rollenhandeln bezieht, ist insofern ein interessantes Korrektiv zu den von Organisationen formulierten Aufgabenverantwortungen, die primär über Geschäftsinteressen definiert sind. Er appelliert an professionelle Akteure, in ihrem Handeln weitere Gesichtspunkte zu berücksichtigen, die gesellschaftlich oder moralisch als relevant erachtet werden, weil diese professionellen Akteure – Ärzte, Journalisten, Wissenschaftler oder Plattformanbieter – großen Einfluss auf diese gesellschaftlichen Aspekte oder moralischen Güter haben. Um welche Aspekte oder Güter es sich bei Plattformanbietern handelt, wäre zu untersuchen. Ebenso, ob aus den genannten, sich an individuelle Akteure richtenden Verhaltenskodizes Erkenntnisse abgeleitet werden können, die sich auf Kodizes für Organisationen bzw. die in Organisationen – bei Plattformanbietern – handelnden Verantwortlichen übertragen lassen.

Der vorgeschlagene „Kodex"-Begriff ist durchaus kompatibel mit dem zentralen Moralbegriff moderner Gesellschaften: Verantwortung. Dieses Zuschreibungskonzept für Handlungsfolgen (oder Aufgaben) hat sich gegenüber anderen Begriffen, wie zum Beispiel der Pflicht, durchgesetzt, weil es das Wissen um die Relevanz von Handlungsmacht bereits impliziert. Je größer die Handlungsmacht und je weitreichender die Einflussmöglichkeiten von jemandem sind, desto mehr Verantwortung trägt er für sein Handeln oder das Unterlassen von Handlungen.

Auf welche Akteure könnte sich ein Digitaler Kodex beziehen?

Wenn man die vorgeschlagene Verwendung des Begriffs Kodex vorläufig akzeptiert, folgt daraus, dass sich ein Digitaler Kodex in direkter Weise auf Organisationen bzw. auf die sie repräsentierenden Akteure bezieht. Adressaten sind also theoretisch zunächst einmal Träger professioneller Rollen. Sofern er sich auf den Akteur „zentrale Kommunikationsplattform" beziehen soll, müsste er sich auf die relevanten, also die gestaltungsmächtigsten Rollenträger dieser Organisationen als Regelungsadressaten beziehen. Das bedeutet keineswegs, dass die anderen Akteure bei der Erarbeitung, Implementierung und Umsetzung eines Kodex keine Bedeutung, keine Rolle haben. Sie

54 Ausnahmen bilden Kodizes für spezielle kulturelle Gruppen. Solche Verhaltenskataloge (etwa ein Samurai-Kodex) richten bzw. richteten sich allerdings an Mitglieder einer Gruppe, die ihnen eine Primäridentität verleiht, an die sich ein Lebensstil knüpft. Weil sich Identitäten in modernen Gesellschaften kaum noch in dieser Weise ausbilden, sind sie im Rahmen dieser Überlegungen wenig relevant.

werden sich jedoch als Regelungsadressaten aus Effizienzgesichtsgründen kaum eignen.

An dieser Stelle wird deutlich, dass der Adressat eines Digitalen Kodex – wenn wir den hier eingebrachten Begriffsvorschlag probehalber akzeptieren – kein politischer Akteur sein kann. Wollte man den Kodex so ausrichten, so müsste er beispielsweise ein Kodex für medienpolitische Akteure sein. Damit wäre das anvisierte Regulierungsfeld verfehlt. Gleichwohl aber kann es wünschenswert sein, dass die Idee eines Digitalen Kodex aus dem politischen Feld Unterstützung erhält.

Eine weitere ganz entscheidende Frage betrifft die Nutzer von Online-Plattformen: Können sie Adressaten eines Digitalen Kodex sein? Die Antwort lautet im Zweifel: Nein. Ein Digitaler Kodex könnte Nutzer nicht direkt adressieren, sondern nur indirekt über den Weg eines Anbieter-Kodex. Um dies zu begründen, ist es vonnöten, sich auf der Begriffsebene kurz genauer anzusehen, worauf der eigentümliche Plural „die Nutzer" referiert.

„Die Nutzer" sind kein stabiles soziales Gebilde

Eine Charakterisierung von Nutzern steht generell vor der Schwierigkeit, dass Nutzer kein dauerhaftes, stabiles soziales Gebilde zu sein scheinen. Der Begriff „Nutzer" ist ein hypothetisches Konstrukt, das aus wissenschaftlichen Analysen von Daten über Individuen hervorgeht. Tatsächlich formieren sich „die Nutzer" von Fall zu Fall in der aktiven Hinwendung zu und Partizipation an medialen Angeboten, auch an Plattformangeboten.

Wenn man Nutzer von zentralen Plattformen charakterisieren möchte, dann scheint die aussichtsreichste Möglichkeit darin zu bestehen, zu beobachten, aus welchen Motiven sich Individuen diesem Angebotstyp zuwenden. Und es ist wichtig, sich dabei klarzumachen, dass man die Motive von Individuen beobachtet, aus denen erst zum Beispiel durch Clusteranalysen statistische Gruppen konstruiert werden. Dass auf Plattformen wie Facebook durchaus soziale Gruppen als Interessengemeinschaften entstehen können, liegt auf der Hand. Das ändert aber nichts daran, dass es eine homogene Gruppe der Kommunikationsplattform-Nutzer als existierendes soziales Gebilde nicht gibt. Ebenso wenig wie „die Gesellschaft" an sich eine kohärente Gruppe ist, existiert so etwas wie eine Netzgemeinde oder -Community als stabiles soziales Gebilde.

Dieser Punkt ist für die generelle Frage, inwieweit Nutzer (oder gar die Netzgemeinde) als Adressaten eines Digitalen Kodex fungieren können, von entscheidender Bedeutung. Im Unterschied zu Nutzern sind die Anbieter von zentralen Kommunikationsplattformen als stabile soziale Gebilde auszumachen: Zentrale Plattformen sind im Regelfall privatwirtschaftliche Unternehmen, also Organisationen, deren individuelle Akteure über ihre professionellen Rollen identifizierbar sind. Einige dieser Rollenträger haben die Aufgabe, das Plattform-Angebot zu gestalten, andere repräsentieren die Organisation: Sie sind die entscheidenden Stellen, an denen Verantwortungszuschreibungen festgemacht werden können.

Wenn sich dieses Argument als tragfähig erweisen sollte, dann ist klar, dass ein Digitaler Kodex die Nutzer von Online-Angeboten nicht direkt adressieren kann, wenn er Erfolg haben will. Die Absicht, dass Nutzer bestimmte soziale Normen berücksichtigen, lässt sich kaum über generelle Appelle erreichen. Es ist nicht verwunderlich, dass die meisten Beeinflussungsversuche von staatlicher oder zivilgesellschaftlicher Seite auf medienpädagogische Maßnahmen in Schulen, Familien und Universitäten und auf allgemeine Beratungsangebote zielen – mit dem zentralen Ziel, die neuen Generationen von vornherein für die Probleme einer digitalen Lebenswelt zu sensibilisieren.

Das muss für einen Digitalen Kodex aber keineswegs bedeuten, dass er Nutzer nicht als Zielgruppe aufnehmen kann. Der Weg eines Kodex jedoch, der für Nutzer etwas erreichen oder Nutzer beeinflussen will, müsste über die Anbieter führen. Wie die Ausgestaltung eines Digitalen Kodex, der sich primär auf Anbieter bezöge, aussehen könnte und wie nutzerbezogene Regeln oder Schutzrechte darin ausgestaltet werden könnten, wäre Gegenstand weiterer Diskussionen – ebenso wie die Fragen, wer einen Digitalen Kodex installieren könnte und ob für seine Anwendung praktikable Sanktionsmechanismen oder Anreizsysteme gefunden werden könnten.

ZUSAMMENFASSUNG DER ÖFFENTLICHEN DISKUSSIONS-VERANSTALTUNG IN MÜNCHEN: „JEDER MACHT IM NETZ, WAS ER WILL – VERANTWORTUNG IN DER DIGITALEN WELT“

Am 4. Juli 2013 fand im Münchener Oberangertheater die erste öffentliche Veranstaltung des Projekts „Braucht Deutschland einen Digitalen Kodex?“ statt. Im Rahmen von zwei Keynotes und einer Podiumsdiskussion näherten sich Vertreterinnen und Vertreter aus Politik, Wissenschaft und Verbraucherschutz sowie der Presse der Frage, ob Deutschland einen Digitalen Kodex braucht. Ein besonderer Schwerpunkt der Diskussion lag dabei auf der Verantwortung in der digitalen Welt und der Zuweisung von Verantwortlichkeiten im Netz.

Jeanette Hofmann (Gründungsdirektorin am Alexander von Humboldt Institut für Internet und Gesellschaft und wissenschaftliche Mitarbeiterin/Projektleiterin am Wissenschaftszentrum Berlin für Sozialforschung) erläuterte in der ersten Keynote den Verantwortungsbegriff aus sozialwissenschaftlicher Perspektive. Dabei hob sie besonders hervor, dass das Konzept der Verantwortung vor allem durch Veränderung geprägt sei: „Verantwortung ist als solche ständig in Bewegung: Wir weisen sie zu, wir teilen sie, wir weisen sie von uns, wir reißen sie an uns.“ Durch diese Dynamik und damit verbundene Verlagerungsprozesse von Verantwortung würden intendierte und nicht intendierte Policy-Effekte ausgelöst. Beispielhaft nannte Hofmann die Haftungsregeln von Plattform-Anbietern, die mit Grundrechten wie der Meinungsfreiheit im Konflikt stehen können. Unter den verschiedenen Typen von Verantwortung sei besonders das ethische Handeln für einen Digitalen Kodex relevant.

In der zweiten Keynote berichtete Michael Siemens (Landesschülerrat Bayern in 2013) aus seinem digitalen Leben. Anschaulich erläuterte Siemens, welch hohen Stellenwert das Internet im Alltag von jungen Erwachsenen einnimmt: „Früher hat man gesagt, der erste Eindruck zählt. Heute ist es so, dass man den ersten Eindruck braucht, um herauszufinden, wie der andere bei Facebook heißt, um sich mit ihm oder ihr zu vernetzen. Und dann zählt wiederum der Eindruck, den Facebook hinterlässt.“ Siemens betonte die Notwendigkeit eines Digitalen Kodex und bezog sich dabei vor allem auf die Veröffentlichung von sensiblen Daten auf Plattformen, die er als äußerst leichtsinnig und gefährlich einstufte.

In der Podiumsdiskussion, die auf die Keynotes folgte, zeigten sich die Positionen der einzelnen Teilnehmer zur digitalen Welt und zu einem möglichen Digitalen Kodex. Tatjana Halm (Referatsleiterin Markt und Recht bei der Verbraucherzentrale Bayern) wies darauf hin, dass ein Großteil der Verbraucher die Gefahren bestimmter Handlungen im Internet nicht kenne. Sie forderte deshalb einen besseren Informationsfluss durch die Anbieter und die Förderung der Medienkompetenz im Allgemeinen. Prof. Dr. Johannes Buchmann (Vizedirektor des Center for Advanced Security Research Darmstadt und Professor für Informatik und Mathematik an der Technischen Universität Darmstadt) stimmte dem zu, indem er den Digitalen Kodex als ein „Bildungsthema“ titulierte. Gleichzeitig sprach er sich dafür aus, die Chancen und Vorteile des Internets anzuerkennen, und warnte vor wenig definierten Befürchtungen vor dem Internet. Allerdings sei eine Reaktion darauf notwendig, dass Informationen im Netz persistent seien und zudem in anderen, vom Nutzer nicht erwarteten, Kontexten auftreten, so Prof. Buchmann. Stefan Plöchinger (Chefredakteur Süddeutsche.de und Geschäftsführender Redakteur Online der Süddeutschen Zeitung) kritisierte vor allem die Anonymität im Internet: „Verantwortung wird erst wahrgenommen, wenn man nicht das Gefühl hat, in einem irgendwie gearteten Raum zu sein, sondern Menschen sich gegenüberstehen.“ Es fehle an Transparenz und Informationen, die Vertrauen und Verantwortung schaffen könnten. Für einen Digitalen Kodex sei die Definition der wichtigsten Themen nötig, über die dann eine offen geführte Debatte stattfinden müsste, so der Journalist. Auch Dr. Christoph Habammer (bis Ende 2013 Leiter der

Stabsstelle des IT-Beauftragten der Bayerischen Staatsregierung) sprach sich für einen Kodex aus, der durch „einen Diskurs zwischen Verwaltung, Bürger und Politik" entstehen müsse.

Allgemein zeigten sich bei der Diskussion der Podiumsteilnehmer, aber auch in den Beiträgen aus dem Publikum, einige Divergenzen. Insbesondere herrschte keine Einigkeit über die Verantwortung der einzelnen Akteure im Netz. Hier wurde beispielsweise auf die internationale Dimension hingewiesen, die es schwierig mache, Verantwortlichkeiten zu regeln. Einig waren sich die Diskussionsteilnehmer allerdings darüber, dass es notwendig sei, die Medienkompetenz bei allen am Netz beteiligten Akteuren zu erhöhen.

Die Diskussion zeigte aber gleichzeitig, dass diese Forderung im Widerspruch zu der Komplexität des Internets steht, die es nicht zulässt, dass die Nutzer die technischen Zusammenhänge umfassend durchdringen können. Allgemeiner Konsens bestand darüber, dass wir, wie von Matthias Kammer (Direktor des Deutschen Instituts für Vertrauen und Sicherheit im Internet) betont, „am Beginn eines größeren Umbruchs stehen" und eine Debatte über mögliche Reaktionen darauf und aktives Handeln notwendig sind.

ZUSAMMENFASSUNG DER ÖFFENTLICHEN DISKUSSIONSVERANSTALTUNG IN HAMBURG: „FACEBOOK, WHATSAPP, GOOGLE+: WER MACHT DIE REGELN?"

Wer bestimmt die Regeln in sozialen Netzwerken? Diesen und vielen anderen Fragen stellten sich Vertreterinnen und Vertreter aus Politik, Wissenschaft, Verbraucherschutz, Presse und Wirtschaft am 7. November 2013 in der Hamburger Bucerius Law School. Nach einem erfolgreichen Auftakt in München im Juli dieses Jahres war es die zweite öffentliche Diskussionsveranstaltung im Rahmen des Projekts „Braucht Deutschland einen Digitalen Kodex?".

Prof. Dr. Wolfgang Schulz, Direktor des Hans-Bredow-Instituts für Medienforschung und des Alexander von Humboldt Instituts für Internet und Gesellschaft, erläuterte in seiner Keynote die Struktur von Plattformen. Wie Nutzer Social Networks wie Facebook, WhatsApp und Google+ verwenden, werde zum einen durch das Gesetz und informelle soziale Normen bestimmt. Darüber hinaus spielten aber auch Softwarearchitektur und Vertragsgestaltung eine zentrale Rolle, so Schulz. Heißt: Über bestimmte Formulierungen in den Nutzungsbedingungen, die die Nutzer anerkennen müssen, und technische Vorkehrungen bestimmen die privaten Betreiber, was Nutzer machen können und dürfen. Daraus folge, dass die Spielregeln auf Plattformen vornehmlich vom Anbieter dominiert würden. Um diese Probleme zu lösen, betonte Schulz, müssten alle vier Dimensionen der Netzstruktur in den Blick genommen werden. Eine Diskussion um einen Digitalen Kodex setze demnach ein Verständnis von Code, Technik, sozialen Normen und staatlichen Regeln voraus.

In der zweiten Keynote berichtete Moritz Nickel, Student an der Bucerius Law School, aus seinem digitalen Leben und diskutierte die Vor- und Nachteile sozialer Netzwerke. Besonders die Kommunikations-, Organisations- und Informationsfunktion von Plattformen hätten einen großen Nutzen, so der Student. Demgegenüber stünden Belanglosigkeit und Redundanz von Informationen, die in Social Networks entstehen.

In der anschließenden Podiumsdiskussion vertrat Jutta Croll, Geschäftsführendes Mitglied des Vorstands der Stiftung Digitale Chancen, die Ansicht, dass die Nutzer durchaus in der Lage seien, die Regeln in sozialen Netzwerken mitzugestalten – etwa indem sie sich bestimmten Funktionen entzögen oder beispielsweise Profile deaktivierten. Dies könne durch

die Förderung der Medienkompetenz verstärkt werden. In diesem Punkt stimmte ihr Sabine Frank, Leiterin Regulierung, Jugendschutz und Medienkompetenz Google Deutschland, zu und verwies darauf, dass Nutzer nicht nur verschiedene Möglichkeiten haben, Plattformen zu nutzen, sondern auch frei seien, zu entscheiden, was sie überhaupt nutzen. Auch Nickel schloss sich dieser Meinung an und hob die Eigenverantwortung der Nutzer hervor: „Jeder Nutzer muss aufpassen, wie er sich im Netz verhält." Deutlich kritischer stufte Ole Reißmann, Redakteur bei Spiegel Online im Ressort Netzwelt, die Nutzung von Plattformen ein und konstatierte: „Der Nutzer ist absolut ausgeliefert", Plattformen hätten zunehmend leichten Zugriff auf die Daten der Nutzer. Durch die monopolistische Position von Anbietern wie Facebook seien die Austrittshürden enorm hoch, was ihre Macht verstärke. Während Reißmann den Zugriff auf die Daten als Problem sieht, betonte Frank, dass dadurch nützliche Funktionen entstehen. Auch Nickel hob hervor, dass ihm persönliche Datensicherheit weniger wichtig sei als die Kommunikations- und Organisationsfunktionen von Plattformen.

In der Debatte zur Rolle des Staates in diesem Prozess kristallisierten sich ebenfalls divergierende Meinungen heraus. Reißmann sprach sich ganz klar für eine Regulierung durch den Staat aus, wies aber gleichzeitig darauf hin, dass die Zuständigkeiten bei den nationalen, aber auch internationalen Behörden nicht geklärt seien. Nickel hingegen plädierte für eine „sanfte Hand" des Staates. Dr. Ralf Kleindiek, Staatssekretär im Bundesministerium für Familie, Senioren, Frauen und Jugend (bis Januar 2014 Staatsrat der Behörde für Justiz und Gleichstellung der Freien und Hansestadt Hamburg), wies in diesem Zusammenhang auf fehlende Expertise hin: „Dem Staat fehlt die Power, das zu regeln. Wir haben keine technologische Souveränität in Bezug auf die digitalen Infrastrukturen." Die Vertreterin der Anbieter, Sabine Frank, sprach sich für das Modell der regulierten Selbstregulierung aus – jedoch fehle es an gesetzlichen Rahmenbedingungen für die Selbstregulierung.

Wer die Regeln in sozialen Netzwerken bestimmt, ist eine sehr komplexe Frage – das hat die Podiumsdiskussion mehr als deutlich gemacht. Ein Kodex, so Kleindiek, der durch einen Aushandlungsprozess entsteht, an dem viele Betroffene beteiligt sind, könnte den Herausforderungen effektiver begegnen als das zusammenhanglose Handeln einzelner Akteure.

Quellen- und Literaturhinweise

Baran, Paul (1964): „On distributed communications networks", RAND Publications, www.rand.org/pubs/research_memoranda/RM3420.html

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

Bayertz, Kurt (1995): „Politik und Ethik", Reclam

BITKOM (2011): „Soziale Netzwerke – Eine repräsentative Untersuchung zur Nutzung sozialer Netzwerke im Internet", 2. Auflage 2011, www.bitkom.org/files/documents/SozialeNetzwerke.pdf

Brown, Ian (2010): „Internet Self-Regulation and Fundamental Rights", Index on Censorship, Vol. 1, March 2010, siehe auch ssrn.com/abstract=1539942

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

Deterding, Sebastian (2010): „Das Internet ist dezentral", Präsentation Berlin 2010, codingconduct.cc/Das-Internet-ist-dezentral

DIVSI (2014): DIVSI U25-Studie, Deutsches Institut für Vertrauen und Sicherheit im Internet, März 2014

Esguerra, Richard (2011): „An Introduction to the Federated Social Network", www.eff.org/deeplinks/2011/03/introduction-distributed-social-network

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., siehe auch cyber.law.harvard.edu/property00/jurisdiction/cyberanarchyedit.html

Granovetter, Mark S. (1973): „The Strength of Weak Ties", The American Journal of Sociology 78 (6), S. 1360–1380, siehe auch www.stanford.edu/dept/soc/people/mgranovetter/documents/granstrengthweakties.pdf oder www.jstor.org/stable/2776392

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

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

Kreutzer, Till (2012): „Auf dem Weg zu einem Urheberrecht für das 21. Jahrhundert", Wirtschaftsdienst Berlin 2012, Heft 10, S. 699-705, siehe auch www.wirtschaftsdienst.eu/archiv/jahr/2012/10/2863/

Kreutzer, Till (2013): „Verantwortung im Internet", Themenaufriss im Projekt „Braucht Deutschland einen Digitalen Kodex?", abgedruckt im Annex dieses Dokuments

Lessig, Lawrence (1998): „The New Chicago School", The Journal of Legal Studies 27 (S2), S. 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", 2. Auflage, Basic Books

Machill, Marcell/Waltermann, Jens (2000): „Verantwortung im Internet", Verlag Bertelsmann Stiftung

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

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

Murray, Andrew D. (2011): „Internet Regulation", Handbook on Regulation, Ed. David Levi-Faur, Edward Elgar, siehe auch works.bepress.com/andrew_murray/4

Picht, Georg (1969, 2004): „Der Begriff der Verantwortung", in ders.: „Wahrheit, Vernunft, Verantwortung. Philosophische Studien", Klett-Cotta, S. 318-342

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

Rosen, Jeffrey (2013): „The Delete Squad. Google, Twitter, Facebook and the new global battle over the future of free speech", www.newrepublic.com/node/113045

Suler, J. R. (2004): „The Psychology of Cyberspace", Chapter 3.3: „The psychology of text relationships", siehe auch truecenterpublishing.com/psycyber/psytextrel.html

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

Webster, Frank (2002): „Theories of the Information Society" (2nd edition), Routledge

Weitzmann, John H. (2013): „Plattformen und die Rolle ihrer Betreiber in Bezug auf Verantwortung im Internet", Themenaufriss im Projekt „Braucht Deutschland einen Digitalen Kodex?", abgedruckt im Annex dieses Dokuments

Zittrain, Jonathan L. (2008): „The Future of the Internet – And How to Stop It", Yale University Press & Penguin UK, siehe auch dash.harvard.edu/handle/1/4455262

ÜBER DIVSI UND DAS IRIGHTS.LAB

Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI)

Das Deutsche Institut für Vertrauen und Sicherheit im Internet (DIVSI) hat das Ziel, einen offenen und transparenten Dialog über Vertrauen und Sicherheit im Netz zu organisieren. DIVSI sucht hierzu die gezielte Unterstützung von Wissenschaft und Forschung und arbeitet mit renommierten Instituten zusammen.

Das Internet hat zentrale Bedeutung für Gesellschaft, Wirtschaft und Kultur. Es revolutioniert unsere Arbeit und die Freizeit, unser Denken und die Kommunikation. Technologische Weiterentwicklungen und Netzwerke schaffen Raum für Ideen und offerieren vielfältige Möglichkeiten: von der Selbstentfaltung des Einzelnen über neuartige Lösungen und Geschäftsmodelle bis hin zur radikalen Veränderung etablierter Industrien und gewohnter Verhaltensweisen.

DIVSI möchte einen Beitrag zum Verständnis dieser hohen Bedeutung leisten, aber auch potenzielle Risiken im Umgang mit dem Internet untersuchen und analysieren. Aufklärungsarbeit soll für eine Sensibilisierung und für eine Steigerung von Vertrauen und Sicherheit im Internet sorgen. DIVSI setzt für einen interdisziplinären Meinungsaustausch zwischen Wissenschaft, Wirtschaft und Gesellschaft Impulse. Es bietet ein Forum für den Austausch ökonomischer, regulatorischer, rechtlicher, sozialer, kultureller und medienpolitischer Perspektiven. Untermauert wird dieses durch themenspezifische Tagungen und Veranstaltungen sowie strategische Projekte. Im Rahmen der Unterstützung von Wissenschaft und Forschung hat DIVSI der Technischen Universität München zu Jahresbeginn 2012 eine Professur für „Cyber Trust" gestiftet.

Schirmherr von DIVSI ist Bundespräsident a. D. Prof. Dr. Roman Herzog. Als Vorsitzende des Beirats fungiert Prof. Dr. Claudia Eckert (Inhaberin des Lehrstuhls für IT-Sicherheit, TU München). Direktor des Deutschen Instituts für Vertrauen und Sicherheit im Internet mit Sitz in Hamburg ist Matthias Kammer. DIVSI, eine Initiative der Deutsche Post AG, arbeitet unabhängig und gemeinnützig.

iRights.Lab

Das iRights.Lab ist zu Beginn des Jahres 2012 als unabhängiger Think Tank zur Entwicklung von Strategien im Umgang mit den Veränderungen in der digitalen Welt gegründet worden. Damit erweitert das iRights.Lab das thematische Feld von iRights.info auf neue Bereiche. Dazu gehören angewandte Forschung, die Entwicklung von Strategien für Unternehmen, Politik und die öffentliche Hand, die praktische Gestaltung von Veränderungsprozessen und die Bereitstellung eines geschützten Raumes zum interdisziplinären fachlichen Austausch zwischen Experten.

Leitbild des iRights.Lab ist, die Möglichkeiten der Digitalisierung und des Netzes zum Vorteil der Öffentlichkeit und der Gesellschaft zu nutzen. Das iRights.Lab ist weder parteipolitisch noch an Unternehmen gebunden. Vielmehr werden Fragestellungen entwickelt und die möglichen Antworten erforscht – interdisziplinär, unabhängig, verständlich, ergebnisoffen. Welche rechtlichen Rahmenbedingungen gibt es, wie sehen die technischen Möglichkeiten aus, wie entwickeln sich politische Prozesse, wie verhält man sich auf neuen Märkten, wie kommuniziert man über soziale Netzwerke? In thematischen Labs bearbeitet das iRights.Lab Themen wie kreative Arbeit und Kreativwirtschaft, Innovation, Journalismus, kulturelles Erbe oder Open Content – sowohl inhaltlich als auch strategisch.

DIVSI Studien

DIVSI U25-Studie (2014)

Die DIVSI U25-Studie liefert erstmals fundierte Antworten auf Fragen, die das Verhalten der nachwachsenden Generation im Hinblick auf das Netz betreffen. Über die Nutzungsformen hinaus werden auch die Denk- und Handlungslogiken sowie der lebensweltliche Hintergrund untersucht.

DIVSI Studie zu Bereichen und Formen der Beteiligung im Internet (2014)

Die DIVSI Studie bietet einen Überblick über den aktuellen Stand der Forschung, wie sich Beteiligung im Internet darstellt. Sie zeigt auf, was im Internet unter dem Begriff „Beteiligung" geschieht, und nimmt dabei die Bereiche Politik, Wirtschaft, Kultur, Gesundheit und Bildung in den Fokus.

DIVSI Studie zu Freiheit versus Regulierung im Internet (2013)

Wie sicher fühlen sich die Deutschen im Internet? Wie viel Freiheit und Selbstbestimmung wollen sie? Nach wie viel Regulierung wird verlangt? Die Studie zeigt ein detailliertes Bild des Nutzungsverhaltens der Deutschen im Internet und ihrer Wahrnehmung von Chancen und Risiken.

DIVSI Entscheider-Studie zu Vertrauen und Sicherheit im Internet (2013)

Wie denken Entscheider über das Internet? Welchen Akteuren schreiben sie welche Verantwortung und welche Einflussmöglichkeiten zu? Was sagen sie zu Sicherheits- und Freiheitsbedürfnissen? Die Studie verdeutlicht erstmals, wie diejenigen über das Internet denken, die wesentlich die Spielregeln gestalten und Meinungsbilder prägen.

DIVSI Meinungsführer-Studie „Wer gestaltet das Internet?" (2012)

Wie gut kennen sich Meinungsführer im Netz aus? Wie schätzen sie ihre Einflussmöglichkeiten ein? Welche Chancen, Konfliktfelder und Risiken erwachsen daraus? In persönlichen Gesprächen wurden führende Repräsentanten aus Politik, Wirtschaft, Verwaltung, Wissenschaft und Verbänden interviewt.

DIVSI Milieu-Studie zu Vertrauen und Sicherheit im Internet (2012) + Aktualisierung (2013)

Die Milieu-Studie differenziert erstmals unterschiedliche Zugangsweisen zum Thema Sicherheit und Datenschutz im Internet in Deutschland, basierend auf einer bevölkerungsrepräsentativen Typologie.

www.divsi.de