Was ist ein Digitaler Kodex?

Überlegungen zu möglichen Anwendungsbereichen, Adressaten
und zum Begriff „Digitaler Kodex“

Themenpapier im Projekt „Braucht Deutschland einen Digitalen Kodex?“[1]

von Dr. Till Kreutzer, Partner iRights.Lab

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

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?

Die Überlegungen 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[2]. Er erfasst eine Vielzahl sehr unterschiedlicher Dienste und Dienstarten, in denen unterschiedliche Akteure in sehr disparaten Strukturen agieren. Angesichts dieser

[2] Hier (Weitzmann (2013), S.2) heißt es: „Plattformen im Sinne dieses Textes sind alle mit dem Internet in Verbindung stehenden technischen Infrastrukturen, die grundsätzlich für eine Benutzung (z.B. 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 (z.B. 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“) aufgezogen sind. Bewusst ausgenommen sind die physische Kommunikations-Infrastruktur und ihre Betreiber (z.B. Internet-Service-Provider und TK-Unternehmen).“

Vielfalt erscheint es angebracht, die Frage, wie eine Regulierung[3] von Plattformen funktioniert oder funktionieren könnte, anhand von konkreter gefassten Beispielkonstellationen zu untersuchen.

1.1. 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.

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

1.1.1. 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 *distributed networks*, s. u.).

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 u. a. für mögliche Adressaten einer durch einen Kodex zu regelnden Verantwortungsverteilung.

1.1.2. 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.

1.1.3. 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 einge-

[3] 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 z. B. soziale Normen als eine – häufig unkodifizierte – Form der Selbstregulierung.

bunden sein können. Die Struktur von Kommunikationsnetzwerken kann in drei Gattungen unterteilt werden: Zentrale, dezentrale und verteilte Netzwerke (*distributed networks*). Die drei Formen unterscheiden sich v. a. 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[4]. Im Unterschied zum Client-Server-Modell spricht man hier vom Peer-to-Peer-Prinzip (P2P).

Die nachstehende Grafik verdeutlicht die unterschiedlichen Konzepte von Netzwerkarchitekturen (Quelle: Baran 1964, 4):

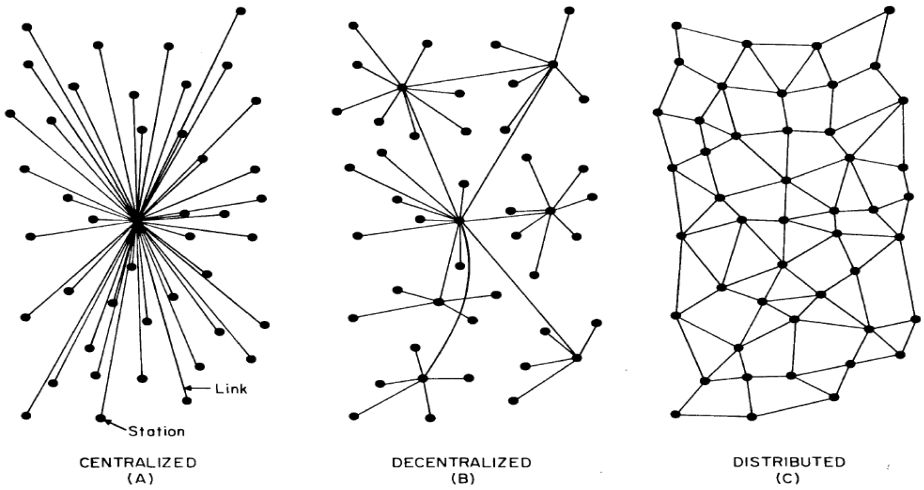

FIG. 1 — Centralized, Decentralized and Distributed Networks

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[5]. Diese unterschiedlichen Konzepte finden sich auch bei den durch Plattformen gebildeten Netzwerken.

1.1.3.1. Zentrale Plattformen

Viele Plattformen bilden ein zentrales, in sich geschlossenes Netzwerk. In sozialen Netzwerken, Video-, Verkaufs- oder Versteigerungsplattformen, Cloud-Diensten usw. verläuft in der Regel sämtlicher Datenverkehr über die Infrastruktur eines einzelnen Anbieters. Üblicher Weise sind zentrale Plattformen nicht Teil eines übergeordneten dezentralen Netzwerks. Der Grund hierfür sind fehlende Interkonnektivität und Datenportabilität. Gerade

[4] Siehe hierzu auch die Anmerkung in Fn. 5.
[5] 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 z. B. 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 Bereichen des Netzes (auf Plattformen) geht.

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[6].

1.1.3.2. Dezentrale Netzwerke

Andere Plattformen sind offen und damit Teil von dezentralen Netzwerken. Solche finden sich z. B. 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/Serverbetreiber per IRC[7] oder per E-Mail miteinander kommunizieren.

1.1.3.3. Distributed Networks

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

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

Die Kehrseite dieser Eigenschaften ist, dass *distributed networks* 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[8]. Dies zeigt sich z. B., 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 ei-

---

[6] Angesichts der Gefahren von Re-Zentralisierungstendenzen 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).

[7] Siehe zur Definition: https://de.wikipedia.org/wiki/IRC-Netzwerk und https://de.wikipedia.org/wiki/Internet_Relay_Chat.

[8] 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), S. 7 ff . (https://www.divsi.de/sites/default/files/Themenpapier_Verantwortung%20im%20Internet_final_2013_06_18.pdf).

nem 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.

1.1.3.4. 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 v. a. 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[9] des Netzes Fluch und Segen zugleich. Einerseits fördert sie regulatorisch unerwünschte Effekte, wie Monopolisierung, Zensur und übermäßigen Einfluss einzelner Akteure u. a. 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.

1.1.4. 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 z. B. derart aussehen:

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

[9] 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, http://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).

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.

Natürlich kann man in Bezug auf die Kategorienbildung und umso mehr eine 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.

1.2. 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 *distributed networks* 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 v. a. 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, so dass es 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 Software-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 z. B. 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[10].

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 solange 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 z. B. 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 hoch komplexes Problem (Rosen, 2013[11]).

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.

[10] Siehe hierzu auch schon Weitzmann (2013), S. 5.
[11] 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.

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.

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 internetspezifische 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 z. T. 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?

3.1. 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, d.h. 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 in Abschnitt II als beispielhafte Regelungssachverhalte für die weitere Erörterung der Frage nach einem Digitalen Kodex vorgeschlagen wurden: Cyber-Mobbing, Fehlverhalten beim Datenschutz und Urheberrechtsverletzungen. Damit werden neben drei möglichen Adressaten (d. h. den Akteuren) zugleich drei inhaltliche Themenbereiche angesprochen, auf die sich ein Digitaler Kodex mit Bezug auf zentrale Kommunikationsplattformen beziehen könnte.

3.2. 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[12]. In Bezug auf drei Beispielfälle von unerwünschtem Verhalten wird ihre Rolle im Folgenden in aller Kürze charakterisiert. Dabei soll verdeutlicht werden, welche netzspezifischen Verhaltensfaktoren *Cyber-Mobbing, 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.

3.2.1. 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-Communities 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 statt. Die Studie ergab dabei, dass die meisten Fälle nicht an den Anbieter gemeldet werden. Nur jeder fünfte Schüler hat die Vorfälle hiernach den Betreibern der betroffenen Plattformen gemeldet[13].

3.2.1.1. 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 stabilisiert durch die physische Präsenz einer gegebenenfalls

[12] 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 in Abschnitt 4 relevant werden, in dem die Frage behandelt wird, inwiefern Nutzer Adressaten eines Digitalen Kodex sein können.

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

sanktionsbereiten Öffentlichkeit. Umgekehrt hat die Möglichkeit, auf Kommunikationsplattformen *unkörperlich* aufzutreten, anscheinend einen enthemmenden Effekt und scheint unsoziales Verhalten wahrscheinlicher zu machen[14]. Hinzu kommen andere Faktoren, wie durch Vernetzungseffekte verstärkte Gruppendynamik und unter Umständen Anonymität.

Das gerade letztere keine Grundvoraussetzung – sondern lediglich ein verstärkender Faktor – für Cyber-Mobbing und ähnliches unsoziales Gruppenverhalten ist, zeigt sich daran, dass solche Phänomene gerade in sozialen Netzwerken besonders häufig vorkommen (s. o.). Solche Netzwerke dienen aber grundsätzlich gerade nicht dazu, anonym zu kommunizieren. Anbieter wie Facebook schreiben in ihren Nutzungsbedingungen sogar die Angabe zutreffender persönlicher Daten vor. Zwar können, da die Angaben nicht systematisch auf ihre Richtigkeit überprüfen, Nutzer ohne Weiteres auch falsche Angaben machen und sogenannte Fake-Profile anlegen, die ihnen anonyme Nutzungsmöglichkeiten ermöglichen. Zudem können – mangels Verifizierung der Angaben – auch Profile unter fremden Namen angelegt werden[15].

Dennoch: Anonymität ist in vielen Fällen keine Grundvoraussetzung für die Beteiligung an Cyber-Mobbing-Aktionen. Teils scheint es schon zu genügen, in der Masse aufzugehen, wie sich an der massenhaften Beteiligung personenbezogener Shit-Storms zeigt[16]. 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.

3.2.1.2. Cyber-Mobbing und das Verhalten der Anbieter

Das Problem, wie Anbieter von Kommunikationsnetzwerken mit Cyber-Mobbing 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 wür-

[14] 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.“*

[15] 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 solange Gebrauch gemacht werden, wie sie nicht systematisch vom Anbieter unterbunden werden.

[16] In den vergangenen Monaten sind der Schauspieler Jan Josef Liefers, der Sportler Mario Götze und die Politiker Horst Seehofer und Claudia Roth massiven Angriffen auf Facebook ausgesetzt gewesen.

den 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 zugeschrieben werden kann. Fraglich ist jedoch, ob und in welchem Maß dies effizient und v. a. 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[17].

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.

[17] Ein Beispiel hierfür sind die Mohammed-Karikaturen, die 2010 erstmals in der dänischen Zeitung *Jyllands Posten* erschienen waren. Trotz Anforderungen 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.

3.2.1.3. Cyber-Mobbing und das Verhalten des Staates

Cyber-Mobbing zu unterbinden wäre, sofern hierbei rechtswidrige, v. a. 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[18]. 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 Cyber-Mobbing, 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 keineswegs 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 Cyber-Mobbing 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[19].

3.2.2. Zweites Phänomen: Umgang mit personenbezogen 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

[18] Vgl. hierzu Weitzmann, Cyber-Mobbing, Cyberbullying und was man dagegen tun kann, http://irights.info/cyber-mobbing-cyberbullying-und-was-man-dagegen-tun-kann-2.
[19] http://www.bmfsfj.de/cybermobbing.

bei der Gestaltung ihres Profils und bei ihrer Kommunikation zahlreiche private Informationen preis in der Annahme, 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.

3.2.2.1. Fehlverhalten beim Umgang mit personenbezogen 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 preisgegeben Daten und persönlichen Informationen[20].

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, „The Strength of Weak Ties“, 1973) zur Diskussion[21]. 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 – z. B. 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.

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 Prozent der Nutzer auch nach neuen Kontakten. In der Regel wird es sich hierbei um die Suche nach Kontakten mit schwacher Bindung handeln. Entspre-

[20] Vgl. nächster Abschnitt.
[21] Einführend zu Granovetter der Eintrag in Wikipedia: http://de.wikipedia.org/wiki/Mark_Granovetter.

chend 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, z. B. 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.

3.2.2.2. Umgang mit personenbezogen Daten und persönlichen Informationen auf Seiten der Anbieter

Auf Seiten der Anbieter sind in puncto Datenschutz zumindest zwei Aspekte von Belang: (a) zum einen der Umgang der Anbieter mit den Daten und personenbezogenen Informationen, die die Nutzer hinterlassen, (b) zum anderen die Frage danach, welchen Einfluss die Anbieter auf das Nutzerverhalten hinsichtlich ihres Umgangs mit ihren eigenen Daten haben.

(a) 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[22]. Um solche Ef-

[22] 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 z. B. Transparenz in monopolisierten Märkten – insbesondere wenn das Produkt oder der Dienst für die Zielgruppe von großer Bedeutung ist – ein wenig wirksames Mittel.

fekte zu verringern, enthält der Entwurf für eine EU-Datenschutzverordnung ein „Recht auf Datenübertragbarkeit“[23].

Solche Geschäftsmodelle führen schnell zu Konflikten mit Rechts- und sozialen Normen. Auch stoßen sie häufig auf Unverständnis und führen zu weit gehenden 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 (z. B. personenbezogene Informationen) etwas anfangen, z. B. 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 u. U. verlorengegangene 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?

(b) 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

[23] Siehe Art. 18 des Entwurfs unter: http://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 http://www.collaboratory.de/w/Interviewzusammenfassung_Peter_Schaar#Datenportabilit.C3.A4t.

basales Vertrauensverhältnis mit den Nutzern aufrechtzuerhalten. Immerhin sind die Nutzer und ihre Inhalte ihr hauptsächliches – vielleicht sogar einziges – Kapital. Solange sich aber z. B. ein etwaiger Vertrauensrückgang bei jugendlichen Nutzern[24] 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.

3.2.2.3. Umgang mit personenbezogen Daten und persönlichen Informationen und das Verhalten des Staates

Wie im Strafrecht ist die staatliche Gestaltungsmacht gegenüber zentralen Kommunikations-Plattformen auch in Bezug auf den Datenschutz beschränkt. Dies zeigt sich z. B. daran, dass die Versuche des Gesetzgebers, bei Datenschutzerklärungen der Anbieter mehr Transparenz zu erreichen, bislang kaum erfolgreich waren[25]. 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[26].

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[27]. Zum anderen wäre es den Anbietern auch in diesem Fall u. U. 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.

[24] Einen solchen diagnostiziert z. B. die Jim-Studie 2012 (Jugend, Information Multimedia) des medienpädagogischen Forschungsverbundes Südwest, www.mpfs.de/index.php?id=527.
[25] Vgl. Weitzmann (2013), Seite 8.
[26] Vgl. die Pressemitteilung des ULD vom 24. April 2013, www.datenschutzzentrum.de/presse/20130424-facebook-klarnamen-ovg.htm.
[27] Siehe http://www.telemedicus.info/article/2584-EU-Datenschutzverordnung-vorerst-auf-Eis-gelegt.html.

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[28]. 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 Plattformbetreibern positiv zu beeinflussen? Wie können Anreize aussehen, die die Anbieter dazu bringen, ihr Verhalten – u. U. entgegen der 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?

3.2.3. 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, s. o. zum Cyber-Mobbing) 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.

3.2.3.1. 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

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

Songs Lizenzgebühren verlangen. Auch das Einbinden von YouTube-Videos kann Ärger nach sich ziehen, denn der Nutzer haftet für die Inhalte des Filmschnipsels. Verletzt es bestehende Rechte, kann der Profilinhaber Post von Anwälten bekommen.“[29]

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 u. a. an Beispielen, in denen Unternehmen oder auch Politiker – im Zweifel unbewusst – gegen Urheberrechte verstoßen haben. Beispielsweise wurde dem derzeitigen Vorsitzenden des Bundestags-Rechtsausschusses Siegfried Kauder vorgeworfen, auf seiner Webseite unautorisiert Fotos zu verwenden[30].

Das Urheberrecht ist ein äußerst komplexes Rechtsgebiet, das ursprünglich ausschließlich für professionelle Adressaten (professionelle Künstler, Plattfirmen, 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.

3.2.3.2. 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 solange 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 soweit 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.

[29] Siehe www.stern.de/digital/online/urheberrechtsverletzungen-bei-facebook-eine-pinnwand-fuer-15000-euro-1715257.html.
[30] Siehe http://www.spiegel.de/netzwelt/netzpolitik/angebliche-foto-vergehen-copyright-kaempfer-kauder-hat-urheberrechte-verletzt-a-789073.html.

3.2.3.3. Urheberrechtsverletzungen und das Verhalten des Staates

Ähnlich wie beim Datenschutz entziehen sich zentrale Kommunikationsplattformen weitgehend den traditionellen Werkzeugen staatlicher Lenkung, v. a. 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[31].

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 z. B. daraus, dass die Dienstanbieter häufig im Ausland sitzen und daher schwer in die Verantwortung genommen werden können.

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 z. B. Schadensersatz- oder andere Kompensationsansprüche in Anspruch genommen werden[32]. 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.

3.3. 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

[31] Siehe z. B. http://www.netzpiloten.de/bundeswirtschaftsministerium-verhandelt-warnhinweismodell-unter-ausschluss-der-offentlichkeit/.
[32] 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.

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 z. B. langfristigen Geschäftsinteressen dienen, obwohl er kurzfristig wirtschaftliche Einbußen bedeutet[33].

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?

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

[33] So mag es die Attraktivität eines sozialen Netzwerks steigern und Vorbehalte verringern, wenn Persönlichkeitsrechtsverletzungen und Cyber-Mobbing 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 Cyber-Mobbing anziehen würde, ist z. B. kaum zu ermitteln.

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 herzustellen, 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 o. g. 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 Lehrerpersonal. Ganz generell werden Themen zur Medienpraxis und Medienkritik nicht in einem eigenem Fach behandelt, sondern tauchen eher bruchstückhaft im Deutsch- oder Informatikunterricht auf.

Hiervon abgesehen stellt sich die Frage, ob der Staat seiner Akteurs-Rolle 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?

4. „Kodex“ – ein Begriffsvorschlag

Die hierzu angestellten Beobachtungen münden in einem ersten Vorschlag, wie der Terminus „Kodex“ begrifflich angelegt sein könnte. Dieser Vorschlag soll u.a. 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, das die Etablierung eines Digitalen Kodex anvisiert, 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[34].

Kodizes wären 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 noch 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 weitergehende 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.

[34] Ausnahmen bilden Kodizes für spezielle kulturelle Gruppen. Solchen Verhaltenskataloge (etwa ein Samurai-Kodex) richten 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 irrelevant.

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 professionelle Akteure – Ärzte, Journalisten, Wissenschaftler oder Plattformanbieter – großen Einfluss auf diese gesellschaftlichen Aspekte oder moralischen Güter haben. Zu überlegen, 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 z. B. 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.

4.1. 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 werden sich jedoch als Regelungsadressaten aus Effizienzgesichtgründen 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.

4.2. „Die Nutzer“ sind kein stabiles soziales Gebilde

Eine Charakterisierung von Nutzern steht generell vor der Schwierigkeit, dass Nutzer kein dauerhaftes, stabiles soziale 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 ei-

nes 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.

5. Literatur

Baran, Paul (1964), On distributed communications networks, RAND Publications, USA 1964, http://www.rand.org/pubs/research_memoranda/RM3420.html.

BITKOM (2011), Soziale Netzwerke - Eine repräsentative Untersuchung zur Nutzung sozialer Netzwerke im Internet, 2. Auflage 2011, http://www.bitkom.org/files/documents/SozialeNetzwerke.pdf.

Deterding, Sebastian (2010), Das Internet ist dezentral, Präsentation Berlin 2010, http://codingconduct.cc/Das-Internet-ist-dezentral.

Esguerra, Richard (2011), An Introduction to the Federated Social Network, https://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

Granovetter, Mark. S. (1973): The Strength of Weak Ties, The American Journal of Sociology 78 (6): 1360–1380. http://www.jstor.org/stable/2776392.

Kreutzer, Till (2012): Auf dem Weg zu einem Urheberrecht für das 21. Jahrhundert, Wirtschaftsdienst Berlin 2012, Heft 10, S. 699-705, http://www.wirtschaftsdienst.eu/archiv/jahr/2012/10/2863/.

Kreutzer, Till (2013): Verantwortung im Internet, Themenaufriss im Projekt „Braucht Deutschland einen Digitalen Kodex?“, https://www.divsi.de/sites/default/files/Themenpapier_Verantwortung%20im%20Internet_final_2013_06_18.pdf

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

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

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, http://truecenterpublishing.com/psycyber/psytextrel.html.

Weitzmann, John H. (2013), Plattformen und die Rolle ihrer Betreiber in Bezug auf Verantwortung im Internet, Themenaufriss im Projekt „Braucht Deutschland einen Digitalen Kodex?“, https://www.divsi.de/sites/default/files/Themenpapier_Plattformen_final_2013_06_18_0.pdf

Zittrain, Jonathan L. (2008), The Future of the Internet -- And How to Stop It, Yale University Press & Penguin UK 2008, http://dash.harvard.edu/handle/1/4455262.