Regulating Code

Rupert Schneider
Betreuer: Heiko Niedermayer
Seminar Innovative Internettechnologien und Mobilkommunikation SS2013
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: rupert.schneider@in.tum.de

KURZFASSUNG

Motivation: Die fortlaufende Entwicklung des Internets erfordert besondere Maßnahmen für dessen Regulierung. *Zu lösendes Problem:* Von anderen Gebieten bekannte Regulierungsmaßnahmen erweisen sich für das Internet aufgrund dessen Charakteristika oft als ungeeignet. *Lösungsansatz:* Regulatorische Maßnahmen müssen unter Berücksichtigung der technischen Rahmenbedingungen entwickelt werden. *Ergebnisse:* Diese Arbeit gibt eine Einführung in die Regulierung und untersucht verschiedene Maßnahmen auf ihre Wirkung in den Bereichen der Wahrung von Privatsphäre und Datenschutz sowie der Internetzensur. Dabei liegt der Fokus auf der Darstellung der technischen Hintergründe. *Fazit:* Regulierung des Internets durch technische Maßnahmen ist in vielen Bereichen ein wirksames Mittel, hat aber auch Schwächen vorzuweisen. Es empfiehlt sich daher eine Ergänzung von technischen mit legislativen Regulierungsmaßnahmen.

Schlüsselworte

Regulierung, Code, Internet, Privatsphäre, Datenschutz, Zensur

1. EINLEITUNG

Das Internet hat sich über die Jahrzehnte von einer Einrichtung für eine begrenzte Anzahl von Spezialisten zu einer Infrastruktur entwickelt, die von Milliarden von Nutzern, Unternehmen und staatliche Institutionen für private, kommerzielle, politische und weitere Zwecke verwendet wird. Gleichzeitig besitzen diese Akteure sehr verschiedene und oft gegenläufige Interessen, die sie mit den zur Verfügung stehenden technischen Möglichkeiten umzusetzen suchen. Um einen Ausgleich zwischen den verschiedenen Interessen zu erwirken und zu gewährleisten, dass dabei die Rechte der einzelnen Parteien gewahrt werden, etwa das Recht auf freie Meinungsäußerung oder Privatsphäre, ist eine Regulierung des Internets unabdingbar.

Obwohl bereits aus anderen Gebieten Erfahrungen mit vielfältigen Regulierungsmaßnahmen vorhanden sind, beispielsweise zur Wahrung fairen Wettbewerbs in der Wirtschaft, sind diese durch die speziellen Eigenschaften des Internets auf dieses nur sehr beschränkt übertragbar. Durch seine verteilte Struktur und, daraus folgend, dem Fehlen einer eindeutigen Zugehörigkeit von Akteuren zur Gerichtsbarkeit eines Staates, uneindeutigen Verantwortlichkeiten, der Möglichkeit anonymen Agierens und seine speziellen technischen Gegebenheiten sind klassische Ansätze oft nicht anwendbar. Vielmehr sind maßgeschneiderte Lösungen von Nöten, die insbesondere die zugrundeliegenden technischen Eigenschaften - den „Code“ des Internets - berücksichtigen und mit dem rapiden Entwicklungstempo in diesem Bereich mithalten können. Daneben kommt der Frage nach ausreichender Legitimation und Repräsentation relevanter Stakeholder ein hoher Stellenwert zu.

Diese Arbeit gibt einen Überblick über verschiedene Regulierungsansätze und untersucht ihre Anwendbarkeit auf das Internet. Ziel ist dabei nicht, die Überlegenheit einer bestimmten Lösung herauszustellen. Vielmehr wird die Notwendigkeit von Trade-Offs zwischen verschiedenen Zielsetzungen anerkannt und die jeweiligen Vor- und Nachteile verschiedener Ansätze dargelegt. Als konkrete Anschauungsbeispiele werden die Problemfälle der Wahrung von Privatsphäre und Datenschutz sowie der Internetzensur herangezogen. Dabei wird besonderes Augenmerk auf die zugrundeliegenden technischen Hintergründe und die Möglichkeiten für Regulierung „by design“ gelegt. Als Ausgangspunkt der Betrachtungen dient dabei das Buch ”Regulating Code”[2] von Brown und Marsden, von dem auch der Titel dieser Arbeit stammt.

2. AUFBAU

Die vorliegende Arbeit ist folgendermaßen aufgebaut: Kapitel 3 gibt eine Einführung in verschiedene Arten von Regulierung. Kapitel 4 behandelt die Problemfelder Privatsphäre und Datenschutz sowie Internetzensur. Dabei werden zunächst die zu lösenden Herausforderungen und verschiedene Möglichkeiten der Regulierung erläutert, während anschließend besonders auf technische Maßnahmen eingegangen wird. Kapitel 5 interpretiert die Ergebnisse hinsichtlich ihrer Wirksamkeit. Abschließend liefert Kapitel 6 eine Zusammenfassung der Arbeit.

3. REGULIERUNG

3.1 Begriff

Der Begriff der Regulierung, wie er in dieser Arbeit verwendet wird, bezieht sich nicht allein auf legislative Maßnahmen von staatlicher Seite. Vielmehr kann Regulierung durch unterschiedliche Akteure, wie zum Beispiel auch Unternehmen oder gewöhnliche Internetnutzer, erfolgen, deren Motivation sich ebenso auf unterschiedlichen Zielsetzungen gründen kann. Zudem bestehen Unterschiede in der Art der Umsetzung. So kann Regulierung über rechtliche oder informelle Maßnahmen erfolgen, über die Zusammenarbeit von mehreren Akteuren und mit unterschiedlich stark ausgeprägter Unterstützung durch technische Mittel. „Regulierung“ wird

doi: 10.2313/NET-2013-08-1_14

hier im weiteren Sinne der Ausübung einer „Kontrolle auf die Online-Umgebung“ verwendet. [2]

3.2 Arten von Regulierung

Im Folgenden werden verschiedene Arten von Regulierung, so wie sie von Brown und Marsden in [2] unterschieden werden, erläutert. Die Klassifikation soll einen Überblick über verschiedene Herangehensweisen an das Feld der Internetregulierung bieten. Wichtig ist vorab die Feststellung, dass Mischformen möglich sind und sich ebenso verschiedene Regulierungsarten gegenseitig ergänzen können.

3.2.1 Selbstregulierung

Selbstregulierung ist eine Art der Regulierung, bei der eine Gruppe von Personen oder Institutionen die Normen ihres Verhalten selbst festlegt [8]. Im Kontext der Internetregulierung sind dies zumeist Unternehmen sowie zivile Personen oder Gruppen. Dahinter steht die Auffassung des Internets als ein dynamischer und innovativer Industriezweig, dessen technische und wirtschaftliche Entwicklung bei minimaler staatlicher Einmischung seine maximale Effizienz erreicht [2]. Besonders in den USA ist dieser Ansatz traditionell sehr populär, während in Europa eine kritischere Anschauungsweise vorherrscht. Kritikpunkte beinhalten insbesondere die immanenten sozialen Auswirkungen technologischer Entwicklungen sowie die Tendenz zur Wettbewerbskonzentration aufgrund von Netzwerk- und Skaleneffekten gerade in der Informationsbranche, was zur Notwendigkeit staatlicher Intervention führt [2].

3.2.2 Staatliche Regulierung

Der entgegengesetzte Extremfall zur Selbstregulierung ist die staatliche Regulierung, bei der Regulierungsmaßnahmen mit legislativen Mitteln durchgesetzt werden. Ihr Legitimitätsanspruch gründet sich zum einen auf den fehlenden Kontrollmechanismen bei reiner Selbstregulierung, insbesondere der richterlichen Kontrolle mit der Möglichkeit des Einspruchs gegen Regulierungsmaßnahmen seitens der Bürger. Zum anderen basiert er auf der staatlichen Aufgabe, die Grundrechte seiner Bürger zu beschützen. Kritiker bemängeln teils Überregulierung, die zu Zensur ausarten kann, Befangenheit von Gesetzgebern durch den Einfluss von Lobbygruppen und mangelnde Mitsprachemöglichkeiten für nichtwirtschaftliche Interessensgruppen, etwa Nutzerverbände.
Des Weiteren hängt die Effektivität staatlicher Regulierung stark davon ab, in welchem Maße beschlossene Gesetze und Verordnungen vollzogen werden. Die Strafverfolgung kann sich aufgrund der im Internet möglichen Anonymität ebenso schwierig gestalten. [2]

3.2.3 Koregulierung

Koregulierung bildet eine Zwischenlösung zwischen Selbst- und staatlicher Regulierung und beinhaltet eine Zusammenarbeit staatlicher Instanzen mit beteiligten Stakeholdern unter Einbeziehung zivilgesellschaftlicher Gruppen. Dadurch sollen die Legitimitätsprobleme anderer Regulierungsarten vermieden werden. Probleme bestehen dennoch bei den Fragen, wie gut zivilgesellschaftliche Gruppen das öffentliche Interesse repräsentieren können und wie effektive Entscheidungsprozesse gewährleistet werden können. Letzteres hat sich in der Vergangenheit als besonders schwierig erwiesen und ist neben anderen Fragestellungen Gegenstand aktueller Forschung. Koregulierung spielt in europäischen Ländern eine zunehmende Rolle, während sie in den USA eher zögerlich angenommen wird. [2]

3.2.4 Regulierung durch technische Mittel

Eine weitere Möglichkeit ist die Ausübung von Regulierung durch Nutzung der zugrundeliegenden Technologien [2]. Beispiele dafür finden sich in Kapitel 4. Ein Vorteil einer solchen Regulierung „by design“ ist - eine entsprechende Verbreitung der Technologie, die zur Regulierung genutzt wird, vorausgesetzt - dass die Maßnahmen teils unabhängig von Ländergrenzen Wirkung zeigen können und somit der Einfluss durch verschiedene Jurisdiktionen gemindert wird. Außerdem erfordert ein derartiges Vorgehen im ersten Moment keine aktive Berücksichtigung durch Benutzer, wenn Verstöße gegen Regulierungsmaßnahmen bereits durch die technische Implementierung ausgeschlossen sind. Gleichzeitig kann es aber für Nutzer mit ausreichendem technischen Wissen auch möglich sein, die Maßnahmen zu umgehen (siehe etwa 4.2.2). Dazu stellt das Erzeugen von Akzeptanz und Unterstützung der notwendigen Technologien eine weitere Herausforderung dar, ohne deren Bewältigung die Regulierung nicht ihren Effekt entfalten kann. Dies wird am Falle des de facto gescheiterten ICRA-Labelingsystems sichtbar (siehe 4.2.2).

4. FALLBEISPIELE

In diesem Kapitel werden die verschiedenen Arten von Regulierung anhand der Fallbeispiele „Privatsphäre und Datenschutz” und „Internetzensur“ veranschaulicht. Dabei werden ihre Vor- und Nachteile im jeweiligen Kontext dargestellt. Besondere Aufmerksamkeit wird der Darstellung von Möglichkeiten zur Regulierung auf technischem Wege gewidmet.

4.1 Privatsphäre und Datenschutz

Das Internet und insbesondere der Trend zum „Mitmach-Internet“ im Zuge des Web 2.0 haben neue Möglichkeiten zur Überwachung und Analyse von Nutzerverhalten geschaffen. Verwertbare Daten werden unter anderem durch Cookies, IP-Adressen, Suchhistorien oder auch die Zeitdauer zwischen dem Anklicken von Links geliefert und ermöglichen die individuelle Profilerstellung und Überwachung großer Mengen von Personen [2, 10]. Dieser Trend wird durch weitere Entwicklungen noch verstärkt. Darunter fällt der Wandel zu einem „Internet der Dinge“, in dem unter anderem durch den Einsatz von RFID-Chips Daten von Objekten aus der realen Welt - wie zum Beispiel Guthabenkarten für öffentliche Verkehrsmittel - automatisiert gesammelt und weitervermittelt werden, auch ohne dass dies für betroffene Personen unmittelbar ersichtlich ist [2]. Dadurch können beispielsweise Bewegungsprofile zu Personen erstellt werden, selbst wenn diese nicht im Internet aktiv sind.

Es gibt eine Vielzahl von Akteuren, die von den gegebenen Möglichkeiten profitieren können und deshalb ein Interesse an ihrer Nutzung haben [2]: Werbe-Netzwerke und Unternehmen erhalten präzise Informationen über die Wirkung von Marketing-Maßnahmen im Internet auf das unmittelbare Konsumenten-Verhalten und können ihre Angebote über die Erstellung von Profilen individuell auf die Präferenzen des Nutzers zuschneiden. Autoritäre Regierungen nutzen die Möglichkeiten zur Identifikation von Dissidenten und

doi: 10.2313/NET-2013-08-1_14

Strafverfolgungsinstitutionen und Geheimdienste versuchen, Straftäter und mögliche Terroristen aufzuspüren. Ein aktuelles Beispiel hierfür sind die Medienberichte über die Überwachung des Datenverkehrs der Kunden mehrerer großer Internetfirmen - unter anderem Google, Facebook, und Youtube - durch den amerikanischen Militärgeheimdienst NSA (National Security Agency) im Rahmen des „Prism"-Programms [1]. Kurzum, es gibt eine Vielzahl von Parteien, für die die privaten Daten und das Verhalten von Personen im Internet von großem Interesse sind.

Während das Internet in seiner Anfangszeit noch eine verhältnismäßig kleine Nutzerbasis hatte, von der ein hoher Grad an Wissen über zugrundeliegende Technologien erwartet werden konnte, ist mit der Öffnung des Internets für die breite Bevölkerung kaum noch von derartigen Voraussetzungen auszugehen. Dementsprechend ist auch das Wissen und das Bewusstsein des durchschnittlichen Internetnutzers für potentielle Gefährdungen der eigenen Privatsphäre, die mit der Benutzung einhergehen können, erwartungsgemäß gering ausgeprägt. Selbiges gilt für den Einsatz von Gegenmaßnahmen, wie etwa den Einsatz von Verschlüsselung.

Aus diesen Gründen ist davon auszugehen, dass es regulatorischer Maßnahmen bedarf, um auch im Internet die Rechte auf Privatsphäre und Datenschutz gewährleisten zu können. Im nächsten Abschnitt werden dahingehende Regulierungsansätze erläutert.

4.1.1 Klassische Regulierungsansätze

Der klassische Ansatz, mit dem im Internet den Problemen von Privatsphäre und Datenschutz begegnet wird, ist das sogenannte „Notice-and-Consent"-Modell. Dieses besteht schlichtweg darin, Besucher von Webseiten und Nutzer anderer Dienste über die jeweiligen Informationsverarbeitungspraktiken in Kenntnis zu setzen. Diese haben dann die Option, das Angebot in Anspruch zu nehmen oder nicht.

Dieses Vorgehen ist teils starker Kritik ausgesetzt. So hat Nissenbaum in [10] eine Reihe von Schwächen herausgearbeitet. Zunächst resultiert Notice-and-Consent typischerweise in langen, in juristischem Stil abgefassten Datenschutzerklärungen, die zudem häufig geändert werden. Ohne entsprechenden fachlichen Hintergrund sind sie damit für den durchschnittlichen Internetnutzer kaum verständlich, zudem wird der Zeitaufwand oft als zu groß empfunden. Dies führt dazu, dass ein großer Teil der Bevölkerung Datenschutzerklärungen nur selten oder gar nicht liest [9]. Zwar ließe sich das Problem durch Zusammenfassungen und leichter verständliche und kürzere Erklärungen einschränken, Nisselbaum argumentiert aber, dass relevante Sachverhalte oft in Details versteckt liegen, beispielweise mit welchen Geschäftspartnern unter welchen Bedingungen Daten ausgetauscht werden. Eine Verringerung der Komplexität könnten somit sehr leicht den Verlust relevanter Informationen nach sich ziehen.

4.1.2 Gesetzgeberische Regulierungsmaßnahmen

Basis für die meisten regulierenden Eingriffe im Bereich von Privatsphäre und Datenschutz durch den Gesetzgeber bildet deren Festschreibung als grundlegendes Recht in vielen nationalen und supranationalen Verfassungen. Hervorzuheben sind vor allem die Aufnahme der Privatsphäre in die UN-Menschenrechtscharta und die Charta der Grundrechte der Europäischen Union. Letztere enthält auch explizit das Recht auf Datenschutz und hat zusammen mit der Datenschutzrichtlinie (95/46/EC) und der Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EC) für einen großen Einfluss der europäischen Bestimmungen gesorgt. Gründe hierfür sind zum einen die Festlegung von Richtlinien zur Verarbeitung persönlicher Daten, zum anderen Einschränkungen bezüglich der Weitergabe persönlicher Informationen in Länder, die keinen ähnlichen Schutz gewährleisten. Dadurch geraten andere Staaten in Zugzwang, ähnliche Regelungen zu treffen. In der Gesetzgebung der USA wird dagegen in erster Linie auf das Notice-and-Consent-Modell vertraut, weswegen sie im Vergleich zur europäischen keinen großen Einfluss zeigt. [2]

Eine erwähnenswerte Bestimmung aus der europäischen Datenschutzrichtlinie für elektronische Kommunikation ist, dass zunächst das Einverständnis des Nutzers eingeholt werden muss, bevor Daten auf dessen Gerät gespeichert oder auf solche zugegriffen werden darf. Außerdem müssen klare und verständliche Informationen zur Verwendung der Daten gegeben werden. Damit werden insbesondere Cookies eingeschlossen, die zur Nachverfolgung von Nutzeraktivitäten verwendet werden könnten. [2]

4.1.3 Regulierung durch technische Maßnahmen

Nachfolgend werden einige technische Regulierungsmaßnahmen beschrieben:

P3P: Die „Platform for Privacy Preferences" (P3P) wurde 2002 ein offizieller Standard des World Wide Web Consortium (W3C). P3P soll Nutzern den Umgang mit Datenschutzrichtlinien erleichtern, wozu diese in maschinenlesbarer Form angeboten werden. Beispielsweise über Browsereinstellungen sind dann Kriterien konfigurierbar, die Webseiten erfüllen müssen, damit ihnen persönliche Daten unmittelbar gesendet werden dürfen. Bei Nichterfüllung werden dem Nutzer bei Aufruf einer Webseite die relevanten Abweichungen angezeigt, sodass dieser eine informierte Entscheidung über den Besuch treffen kann, ohne aber die gesamten Datenschutzrichtlinien durchlesen zu müssen. Aufgrund mangelnder Verbreitung und zu komplexer Bedienung für Benutzer wurde die Weiterentwicklung des Standards zwar 2006 eingestellt, einige Browser unterstützen ihn aber dennoch. [11]

Do-Not-Track: Die „Do-Not-Track"-Option wurde auf Initiative der amerikanischen Federal Trade Commission (FTC) entwickelt und wird derzeit am W3C standardisiert. Sie beinhaltet eine in Internetbrowsern aktivierbare Option, um Webseitenbetreibern mitzuteilen, dass der Benutzer nicht wünscht, dass sein Verhalten etwa zum Ziele personalisierter Werbung mitverfolgt wird. Dies kann unter anderem durch ein Feld im HTTP-Header geschehen. [2, 12]

Zertifizierungen: Hersteller können sich durch bestimmte Zertifizierungen bescheinigen lassen, dass ihr Produkt besondere Datenschutzbestimmungen erfüllt. Ein Beispiel hierfür ist das mit europäischen Mitteln geförderte EuroPrise-Siegel, das durch das Unabhängige Landeszentrum für Da-

[1] Wernick, Christian: US-Geheimdienst zapft Internet an. In: Süddeutsche Zeitung (08.06.2013), Nr. 130, S. 1

doi: 10.2313/NET-2013-08-1_14

tenschutz Schlesweig-Holstein ausgestellt wird. Als Bedingung für dessen Ausstellung müssen Software und Entwicklungsprozesse durch zugelassene Prüfer auf ihre Eigenschaften im Hinblick auf Privatsphäre und Datenschutz untersucht werden. Zertifizierte Produkte dürfen von deutschen Regierungsinstitutionen bevorzugt eingekauft werden. [2, 6]

4.2 Internetzensur

Ebenso wie es bei klassischen Medien der Fall war, gibt es auch im Internet Bestrebungen zu einer Zensur bestimmter Inhalte. Dahinter steht als Zielsetzung typischerweise die Einschränkung des Zugangs zu Informationen und Daten, die von der regulierenden Partei als kriminell oder unmoralisch erachtet werden oder deren Verbreitung aus sonstigen Gründen unerwünscht sind. Dabei ist Zensur häufig umstritten, da sie meist der Meinungsfreiheit zuwiderläuft und dem Vorwurf der Intransparenz ausgesetzt ist. [2]

4.2.1 Formen der Zensur

Die wohl bekanntesten Fälle von Zensur erfolgen von staatlicher Seite. Dazu zählt beispielsweise die Einschränkung des Zugriffs auf kinderpornographische Seiten in europäischen Ländern [2]. Daneben gibt es Zensur durch autoritäre Regierungen in Ländern wie China, das bekanntermaßen eines der ausgereiftesten Zensursysteme der Welt besitzt. So wird dort unter anderem Datenverkehr geblockt, in dem bestimmte Schlüsselbegriffe vorkommen (z.B. „Falun Gong“) und der Zugriff auf Seiten wie Twitter und Facebook gesperrt [1, 5]. Somit wird der Zugang der chinesischen Bevölkerung zu Inhalten geblockt, die die Regierung als problematisch ansieht, wie etwa bestimmte politische Ideologien und historische Ereignisse [4].

Neben Zensur von staatlicher Seite gibt es auch Selbstzensur, bei der der Nutzer seine eigenen Handlungen einschränkt. Dies kann durch die Benutzung von Filtersoftware auf dem Endsystem geschehen oder aber durch gewohnheitsmäßige Verhaltensweisen, die beispielsweise aus Angst vor staatlicher Überwachung an den Tag gelegt werden [2].
Daneben sind auch Institutionen wie Schulen oder auch Unternehmen dafür bekannt, den Zugriff auf bestimmte Seiten einzuschränken.

4.2.2 Zensur auf technischer Ebene

Im Folgenden werden verschiedene Möglichkeiten der Zensur auf technischer Ebene sowie ihre jeweiligen Vor- und Nachteile erläutert:

Labeling-Systeme: Das Prinzip hinter Labeling-Systemen ist, dass Anbieter ihre bereitgestellten Inhalte durch eine Reihe von Schlüsselbegriffen kategorisieren. Dies ermöglicht Anwendern, durch das Betreiben von Filtersoftware auf ihren Endsystemen Zugriffe auf bestimmte Klassen von Inhalten einzuschränken. Ein bekanntes System dieser Art wurde durch die Internet Content Rating Association (ICRA, heute Teil des Family Online Safety Institute) für den Jugendschutz bereitgestellt. Dabei klassifizieren Anbieter ihre Inhalte anhand eines vorgegebenen Fragenkatalogs und ergänzen diese dann durch entsprechende Kennzeichnungen, anhand derer Filterentscheidungen etwa durch entsprechende Einstellungen in Webbrowsern getroffen werden können. Allerdings hat das System keine breite Verwendung gefunden. [2, 7]

Adressbasierte Filterung: Bei adressbasierter Filterung werden IP-Pakete anhand ihrer Zieladresse gefiltert. Der Ort, an dem dies geschieht, können etwa Router - typischerweise von Internet Service Providern (ISP) - oder Firewalls sein, wo dies zur Standardfunktionalität zählt. Pakete zu Zielen, die in einer entsprechenden Blacklist aufgeführt sind (respektive: nicht in einer Whitelist), werden nicht weitergeleitet („gedroppt“). Ein Problem dieses Vorgehens ist, dass es leicht zur unbeabsichtigten Sperrung von weiteren „harmlosen“ Inhalten führen kann, da unter einer IP-Adresse in der Regel mehrere Webseiten (oder andere Dienste) bereitgestellt werden. Zudem müssen die zugrundeliegenden Listen verwaltet und aktuell gehalten werden. Eine Umgehung der Filterung ist durch den Einsatz von Proxy-Servern leicht zu bewerkstelligen. [4]

DNS-Poisoning: Beim DNS-Poisoning werden Anfragen auf das Domain Name System (DNS) genutzt, das dazu verwendet wird, Domainnamen in IP-Adressen aufzulösen. Anhand einer Blacklist (oder Whitelist) wird festgestellt, ob der Zugriff auf die angeforderte Domain gesperrt werden soll. Falls ja, wird entweder keine Antwort zurückgegeben oder aber eine modifizierte, die statt der angeforderten z.B. die Adresse einer generische Seite mit Informationen über den Grund der Sperrung zurückliefert. Ein Vorteil gegenüber der Filterung auf Adressbasis ist, dass ungewollte Sperrungen von anderen Domains mit der gleichen IP-Adresse vermieden werden. Schwierigkeiten entstehen aber dennoch, wenn eine feinere Filterung gewünscht ist. Zum Beispiel könnte nur die Sperrung von Webseiten, nicht aber des Maildienstes einer Domain gewollt sein. Insofern ist auch DNS-Poisoning für übertriebene Sperrungen anfällig. Weiterhin kann eine Sperre leicht umgangen werden, falls die IP-Adresse des zur Domain gehörigen Servers bekannt ist oder auf einem anderem Wege als DNS ermittelt wird: In diesem Fall erübrigt sich die DNS-Anfrage, da an Stelle der Domain unmittelbar die IP-Adresse genutzt werden kann. [3, 4]

Content Inspection: Content-Inspection-basierte Systeme treffen Filterentscheidungen über die Blockierung von Paketen nicht anhand deren Quelle oder Ziel, sondern durch die Untersuchung ihres Inhalts auf bestimmte Kriterien. Dabei wird häufig auf Komponenten von Intrusion-Detection-Systemen zurückgegriffen. Je nach Ergebnis der Untersuchung werden Maßnahmen initiiert, um die Kommunikation zu verhindern. Dies kann zum Beispiel durch einfaches „Droppen“ der Pakete geschehen. Clayton et al. haben bei ihrer Untersuchung der „großen Firewall von China“ (GFC) in [4] noch eine weitere Möglichkeit entdeckt: Die hier eingesetzte Methode benutzt TCP-Reset-Nachrichten, um bei Bedarf einen Verbindungsabbruch zu erzielen. Die Autoren waren jedoch in der Lage, diesen Mechanismus durch einfaches Ignorieren der TCP-Reset-Nachrichten zu umgehen.
Die Filterung per Content Inspection ist im Vergleich zu den beiden vorigen Methoden sehr präzise. Dennoch kommt es auch hier zu „Kollateralschäden“. Im Falle der GFC wird z.B. nach Schlüsselwörtern wie „rfa“ (Abkürzung für „Radio Free Asia“) gefiltert, was 2010 auch zur Sperrung der Google-Suche in Hong Kong führte, die „rfa“ als Teil ihrer Suchparameter enthielt [1]. Daneben ist das Verfahren verhältnismäßig aufwändig und entsprechend teuer in der Umsetzung. Bei verschlüsselten Verbindungen ist es nicht anwendbar, wobei prinzipiell die Möglichkeit zur generellen

doi: 10.2313/NET-2013-08-1_14

Erkennung und Blockierung von verschlüsseltem Datenverkehr bestünde. Wie in [5] für die GFC beschrieben, lässt sich zudem speziell die Filterung anhand von Schlüsselwörtern dadurch vermeiden, dass IP-Pakete so fragmentiert werden, dass sich die Schlüsselwörter jeweils auf zwei Pakete aufteilen. Eine Erkennung von solchen Schlüsselwörtern würde es erfordern, dass der Zensor die Pakete wieder zusammensetzt, was aufwändig und teils gar nicht möglich ist, da Pakete über unterschiedliche Zwischenstationen geroutet werden können. [4]

4.2.3 Schlussfolgerungen

Die weiter oben beschriebenen technischen Zensurmöglichkeiten weisen unterschiedliche Stärken und Schwächen auf. Als Fazit lässt sich festhalten, dass jede der Maßnahmen von technisch versierten Nutzern umgangen werden kann, auch wenn sie für den Großteil der Internetnutzer ein ausreichendes Hindernis darstellen. Eine größere Sicherheit vor Umgehung kann durch die Kombination mehrerer Methoden erzielt werden, wie es auch Clayton et al. an der GFC beobachteten [4]. Dies könnte aber zu vermehrten unbeabsichtigten Sperrungen führen.

Wichtig ist auch die Feststellung, dass die gesellschaftliche Akzeptanz von Zensurmaßnahmen neben ihrem Einsatzzweck stark von ihrer Genauigkeit abhängt: Beispielweise waren übermäßige Sperren einer der Hauptgründe, aus denen 2004 im amerikanischen Bundesstaat Pennsylvania verabschiedete Zensurmaßnahmen gegen Kinderpornographie als verfassungswidrig abgelehnt wurden [4]. Dies kann als gutes Beispiel für die gegenseitige Beeinflussung von „Code“ und Gesetzgebung gesehen werden.

5. INTERPRETATION

Abschnitt 4.1 behandelte das Problemfeld von Privatsphäre und Datenschutz im Internet. Die vorgestellten technischen Regulierungsmaßnahmen in diesem Bereich hatten nur begrenzten Effekt und Änderungen konnten eher auf legislativer Ebene erzielt werden. Abschnitt 4.2 zeigte dagegen für das Gebiet der Internetzensur auf, wie technische Maßnahmen effektiv für Regulierung verwendet werden können.

Insgesamt lässt sich somit keine eindeutige Überlegenheit einer bestimmten Art von Regulierung ableiten. Vielmehr können je nach Gebiet unterschiedliche Maßnahmen geeignet sein.

6. ZUSAMMENFASSUNG

In Kapitel 3 dieser Arbeit wurde der Begriff der Regulierung erklärt und verschiedene Arten von Regulierung vorgestellt: Es gibt Selbstregulierung, staatliche Regulierung, Koregulierung und daneben noch die Regulierung „by design“ mit technischen Mitteln. Jede dieser Arten hat unterschiedliche Eigenschaften hinsichtlich ihrer Legitimität und Wirksamkeit.

Kapitel 4 behandelte als Fallbeispiele die Gebiete „Privatsphäre und Datenschutz“ und „Zensur“.
Im ersten Teil wurde zunächst das „Notice-and-Consent“-Modell als klassischer Regulierungsansatz erläutert und seine Schwachstellen diskutiert. Anschließend wurden verschiedene gesetzgeberische Maßnahmen zur Stärkung von Privatsphäre und Datenschutz erklärt, wobei die Rolle der Europäischen Union als Wegbereiter betont wurde. Im nächsten Schritt wurden einige technische Regulierungsmaßnahmen erläutert.
Der zweite Teil ging zunächst auf Gründe und Formen von Zensur ein. Anschließend wurden verschiedene technische Realisierungen mit ihren jeweiligen Stärken und Schwächen behandelt. Es wurde das Fazit gezogen, dass keine der vorgestellten Methoden eine absolute Sicherheit gewährleisten kann, aber für die meisten Internetnutzer ausreichend ist, als auch, dass die Akzeptanz von Zensurmaßnahmen stark von ihrer Präzision abhängt.

Kapitel 5 schloss mit dem Fazit, dass prinzipiell keine eindeutige Überlegenheit einer bestimmten Art von Regulierung festzustellen ist und ihre Eignung vom jeweiligen Einsatzgebiet abhängt.

7. LITERATUR

[1] Anderson, D. : Splinternet Behind the Great Firewall of China. In: *ACM Queue* 10 (2012), Nov., Nr. 11, S. 40:40–40:49. `http://dx.doi.org/10.1145/2390756.2405036`. – DOI 10.1145/2390756.2405036. – ISSN 1542–7730

[2] Brown, I. ; Marsden, C. T.: *Regulating Code: Good Governance and Better Regulation in the Information Age*. Cambridge, Massachusetts : The MIT Press, 2013. – ISBN 9780262018821

[3] Clayton, R. : Anonymity and traceability in cyberspace / University of Cambridge, Computer Laboratory. 2005 (UCAM-CL-TR-653). – Forschungsbericht

[4] Clayton, R. ; Murdoch, S. ; Watson, R. : Ignoring the Great Firewall of China. In: Danezis, G. (Hrsg.) ; Golle, P. (Hrsg.): *Privacy Enhancing Technologies* Bd. 4258. Springer Berlin Heidelberg, 2006. – ISBN 978–3–540–68790–0, S. 20–35

[5] Crandall, J. R. ; Zinn, D. ; Byrd, M. ; Barr, E. ; East, R. : ConceptDoppler: a weather tracker for internet censorship. In: *Proceedings of the 14th ACM conference on Computer and communications security*. New York, NY, USA : ACM, 2007 (CCS '07). – ISBN 978–1–59593–703–2, S. 352–365

[6] EuroPrise: *EuroPriSe – European Privacy Seal*. `https://www.european-privacy-seal.eu/about-europrise/fact-sheet`. – aufgerufen am 09.06.2013

[7] Family Online Safety Institute: *About ICRA*. `http://www.fosi.org/icra/`. – aufgerufen am 08.06.2013

[8] Kokswijk, J. van: Social Control in Online Society–Advantages of Self-Regulation on the Internet. In: *Proceedings of the 2010 International Conference on Cyberworlds*. IEEE Computer Society (CW '10). – ISBN 978–0–7695–4215–7, 239–246

[9] Moores, T. : Do consumers understand the role of privacy seals in e-commerce? In: *Commun. ACM* 48 (2005), März, Nr. 3, S. 86–91. `http://dx.doi.org/10.1145/1047671.1047674`. – DOI 10.1145/1047671.1047674. – ISSN 0001–0782

[10] Nissenbaum, H. : A contextual approach to privacy online. In: *Daedalus* 140 (2011), Nr. 4, S. 32–48

[11] Reay, I. ; Dick, S. ; Miller, J. : A large-scale empirical study of P3P privacy policies: Stated actions vs. legal obligations. In: *ACM Trans. Web* 3 (2009), Apr., Nr. 2, S. 6:1–6:34. http://dx.doi.org/10.1145/1513876.1513878. – DOI 10.1145/1513876.1513878. – ISSN 1559–1131

[12] World Wide Web Consortium (W3C): *Tracking Preference Expression (DNT)*. http://www.w3.org/TR/tracking-dnt/. Version: Apr. 2013. – aufgerufen am 09.06.2013