

*Lawrence Lessig*  
ARCHITEKTUR DER KONTROLLE  
Internet und Macht

Wir lernen, die Dinge auf eine bestimmte Weise zu sehen, und dann sehen wir sie nur auf diese Weise. Wir sehen nur, was uns diese Sichtweise enthüllt – nichts darüber hinaus, nichts, was ihr widerspricht. Unsere Welt ist nach diesen Schemata eingeteilt. Darüber hinaus sehen wir nichts.

Wir haben bereits ein gutes Stück der Geschichte unserer Zukunft hinter uns; eine Dekade ist vergangen, seit der Begriff des World Wide Web erstmals auftauchte; fünf Jahre, seit der führende Betriebssystemhersteller das Web in sein Betriebssystem eingebaut hat. Heute verbringen Millionen von Menschen ihr Leben zu großen Teilen im Cyberspace<sup>1</sup>. Die Wirtschaft hat den Cyberspace entdeckt und gibt Milliarden aus um herauszufinden, wie er in die Wirtschaft der realen Welt eingepasst werden könnte.

Dennoch haben wir kaum einen Begriff davon, wie diese Zukunft funktionieren wird. Wir betrachten die Fragen von Macht und internationalem Einfluss durch dieselbe Linse wie unsere Väter; wir stellen die gleichen Fragen zu Souveränität und internationaler Politik; dieselben Akteure haben dieselbe Bedeutung; nichts hat sich in der Geschichte, die wir erzählen, geändert, außer natürlich das Jahr und die Zusammensetzung der Regierung.

Ich möchte hier eine andere Sichtweise skizzieren, indem ich zwei Fragen nachgehe: Wie hat der Cyberspace unsere Welt verändert? Und was heißt das für das Verhältnis von Internet und Macht? Im Internet ist derzeit eine Revolution im Gange, und diejenigen, die sich theoretisch mit der Macht und ihrer Rolle bei der Schaffung von Gerechtigkeit auseinandersetzen, werden sich mit dieser Revolution und den Veränderungen, die sie mit sich bringt, befassen müssen.

Regierungen denken stets über Regulierung nach. Sie denken einerseits nach über ihre Macht, Verhalten, das ihnen genehm ist, herbeizuführen, und andererseits über ihre Macht, Verhalten zu unterbinden, das ihnen missfällt. Sie glauben, dass sie diese Macht in erster Linie durch Gesetze

ausüben: durch die Androhung von Gewalt als Anreiz dafür, dass bestimmte Verhaltensweisen an den Tag gelegt werden.

Aber offensichtlich wird Verhalten auf mehrere Weisen reguliert – Gesetze sind nur eine davon. Normen regulieren unser Verhalten, wie dies Gesetze tun. Ich habe drei wunderbare Jahre in Cambridge verbracht. Es waren drei Jahre, in denen ich gelernt habe, wie sehr die englischen Normen von den amerikanischen differieren können und wie hart man bestraft werden kann, wenn man darüber stolpert. Normen regulieren auf ähnliche Weise wie Gesetze – sie bestrafen Verstöße *ex post*. Dennoch funktionieren Normen anders als Gesetze: Die Bestrafung wird von einer Gemeinschaft vorgenommen, nicht vom Staat.

Entsprechend können wir darüber nachdenken, auf welche Weise der Markt reguliert. Der Markt reguliert über den Preis. Er bestimmt den Zugang zu Ressourcen dadurch, dass dafür etwas von entsprechendem Wert angeboten werden muss. Lohn für Arbeit – *quid pro quo*. Der Zwang funktioniert auf mehreren Ebenen gleichzeitig; er wird von einer Gemeinschaft auferlegt, wobei Abweichungen unter Berufung auf Gesetze und Normen korrigiert werden.

Aber die Regulierungsinstanz, auf die wir uns konzentrieren müssen um zu verstehen, was der Unterschied im Hinblick auf den Cyberspace ist, ist das, was ich »Architektur« nennen möchte: eine Regulierung, die daraus resultiert, wie die physische Welt ist, wie sie geschaffen wurde, wie sie vorgefunden wird. Architektur reguliert Verhalten; auch ihre Zwänge funktionieren gleichzeitig; aber sie werden nicht durch den Willen des Staates oder einer Gemeinschaft durchgesetzt, sondern durch die physische Macht eines Kontexts bzw. einer Umgebung. Die Idee, dass Architektur regulierend wirkt, ist nicht neu, insbesondere nicht im Zusammenhang mit dem Cyberspace.

David Hackett Fisher beschreibt, wie die Gründer von Neuengland die zukünftigen Städte im Detail planten, um die Verhältnisse der Gebäude zueinander und zum Stadtplatz so zu gestalten, dass das Verhalten in der Stadt reguliert werden konnte.

Berühmt ist Benthams Beschreibung eines Gefängnisses, bei dem alle Zellen von einer zentralen Position aus sichtbar sind, so dass die Gefangenen niemals wissen, ob sie gerade beobachtet werden, aber immer unter Beobachtung stehen und damit reguliert werden.

Napoleon III. ließ in Paris breite Boulevards anlegen, die es Revolutio-

nären unmöglich machen sollten, Barrikaden zu bauen. So konnten die Pariser Bürger reguliert werden.

Robert Moses baute die Autobahnbrücken über den Straßen, die zu den Stränden von Long Island führen, so niedrig, dass Busse nicht unter ihnen durchfahren konnten. Damit stellte er sicher, dass nur Personen mit Autos (vor allem also Weiße) die öffentlichen Strände benutzen konnten, Personen ohne Autos (größten Teils Schwarze) hingegen gezwungen waren, andere Strände zu benutzen. So konnten die sozialen Beziehungen reguliert werden.

In allen diesen Fällen verändern die Zwänge eines Kontexts das Verhalten. Man kann sich darauf verlassen, dass diese Zwänge das Verhalten regulieren – im gleichen Maße wie Gesetze, wenn auch auf andere Weise.

Architektur, Gesetze, Normen und der Markt zusammen regulieren unser Verhalten. Gemeinsam formulieren sie die Bedingungen, unter denen man frei ist zu handeln oder nicht; gemeinsam setzen sie die Zwänge, die vorgeben, was möglich ist und was nicht. Diese vier Modalitäten der Regulierung bestimmen, wie Individuen und Staaten in ihrem Einflussbereich reguliert werden.

Es ist wichtig, diese Modalitäten zusammenzudenken, weil sie miteinander konkurrieren; eine kann die andere verstärken; die andere kann die eine unterminieren. Der Markt kann durch bestimmte Geschäftsregeln gestärkt werden; soziale Normen können durch den Markt untergraben werden.

Der Cyberspace konfrontiert uns mit einer besonders heftigen Wechselwirkung zwischen den verschiedenen Modalitäten. Je nach seiner Konstruktion kann der Cyberspace die Macht sozialer Normen stärken oder schwächen. Je nach seiner Konstruktion kann er Marktmechanismen fördern oder hemmen. Je nach seiner Konstruktion kann er staatliche Regulierung zulassen oder das Verhalten im Cyberspace »unregulierbar« machen.

Je nach seiner Konstruktion.

Der Bauplan, die Konstruktion (*design*) ist der Aspekt, auf den man sich konzentrieren muss, wenn man Macht in diesem Raum verstehen möchte. Der Cyberspace ist zunächst eine Architektur. Er ist eine Plattform, die konstruiert wird. Er wird durch einen bestimmten Code konstituiert – durch Software und Hardware, die den Cyberspace zu dem machen, was er ist. In diesem Code sind bestimmte Werte verankert; er ermöglicht bestimmte Praktiken; er macht die Vorgaben, unter denen das Leben im

Cyberspace abläuft, genauso wie dies die Naturgesetze für das Leben in der Wirklichkeit tun.

Die meisten nehmen aber diese Architektur – den Code, über den der Cyberspace definiert ist – als gegeben an. Sie behandeln diesen Code, als ob er definitiv wäre, als ob er eine bestimmte, unveränderliche Natur hätte. Als ob Gott uns den Cyberspace geschenkt hätte und wir nur verstehen müssten, wie er funktioniert. Diese vorgebliche Natur wird in Slogans beschrieben: Der Cyberspace, sagt man, könne nicht reguliert, das Verhalten dort könne nicht kontrolliert werden. Regierungen seien hilflos gegenüber der Natur dieses Raums.

Aber es geht darum zu sehen, dass dieser Auffassung von der Natur des Cyberspace oder vom Cyberspace als Naturgegebenheit gar kein natürliches Objekt entspricht. Wenn irgend etwas ein soziales Konstrukt ist, dann der Cyberspace. Die gängige Auffassung des Cyberspace spiegelt in Wahrheit nur eine spezifische Konstruktion wider, genauer: die Bauweise des Cyberspace zu der Zeit, als er in den Blickpunkt der Öffentlichkeit geriet.

Diese ursprüngliche Konstruktion verunmöglichte Kontrolle, insbesondere Kontrolle durch den Staat, und schuf so eine gewisse Freiheit im Cyberspace. Sie verunmöglichte ebenso Kontrolle durch andere Akteure oder Konkurrenten und förderte dadurch Wettbewerb und Innovation im Cyberspace.

Dafür waren bestimmte Charakteristika dieses Raums verantwortlich, Charakteristika seiner Konstruktion. Konzentrieren wir uns zunächst auf jene Charakteristika, die Freiheit schaffen – die Konstruktionsaspekte, denen wir nach verbreiteter Auffassung die ursprüngliche Freiheit des ursprünglichen Netzes verdanken.

Das ursprüngliche Netz schützte beispielsweise die freie Rede. Kraft seiner Architektur konnte jeder einfach sagen, was er wollte, ohne dass seine Aussagen von anderen kontrolliert werden konnten. China konnte Kritik an China nicht zensieren; Nachrichten über den Terror in Bosnien konnten ungehindert die Staatsgrenzen passieren.

Das ursprüngliche Netz schützte auch die Privatsphäre. Man konnte durch das Internet surfen, ohne dass irgend jemand wusste, wer man war. Man konnte dort weitgehend anonym leben, denn die Netzprotokolle und -technologien machten es einfach, die eigene Identität zu verbergen. Man konnte daher sein, wer immer man sein wollte, oder auch überhaupt niemand.

Das ursprüngliche Netz schützte den freien Informationsfluss. Man konnte kostenlos perfekte Kopien von Texten, Bildern und Musik machen und sie überall im Netz weiterverbreiten.

Und schließlich schützte das ursprüngliche Netz Individuen vor lokaler Reglementierung. Kein Staat konnte das Leben im Netz irgendwelchen Regeln unterwerfen. Weil lokale und auswärtige Aktivitäten ununterscheidbar waren, lag das Verhalten im Internet außerhalb der Reichweite staatlicher Kontrolle.

Jede dieser Freiheiten basierte auf einem bestimmten Charakteristikum des ursprünglichen Netzes und war an eine bestimmte Konstruktion gekoppelt. Wer jemand war, woher er kam, welche Inhalte er verschickte – nachdem alle diese Informationen nicht leicht zu gewinnen waren, war es unmöglich, das Verhalten im Cyberspace zu regulieren.

Was aber, wenn die Konstruktion des ursprünglichen Netzes verändert würde? Was, wenn es einfacher würde, jemanden zu identifizieren? Was, wenn Inhalte leichter überprüfbar würden? Was geschähe dann mit der ursprünglichen Freiheit des Netzes?

Die freie Rede wäre in Gefahr, weil Andersdenkende aufgespürt werden könnten. Die Privatsphäre wäre nicht mehr geschützt, weil Identitäten offenliegen würden. Inhalte könnten nicht mehr ungehindert verbreitet werden, weil Kontrolle möglich wäre. Das Verhalten wäre reglementierter, weil Staaten den Zugang über den Zwang zur Anpassung an ein bestimmtes Verhalten regulieren könnten.

Das alles ist freilich keine Vision, sondern bereits Wirklichkeit. Denn was machbar ist, wird gemacht. In den vergangenen fünf Jahren wurden die Voraussetzungen für die ursprüngliche Freiheit des Cyberspace systematisch untergraben. Es wurden Technologien auf die ursprüngliche Architektur des Web aufgesetzt, die der Identifikation von Personen und Inhalten dienen.

Diese Technologien sind derzeit im wesentlichen in privater Hand. Die Wirtschaft setzt sie ein, um Informationen über ihre Kunden zu gewinnen. Natürlich würden dieselben Identifikationstechnologien auch staatlicher Regulierung und Kontrolle zupass kommen.

Wir alle haben von diesen Technologien schon in verschiedenen Zusammenhängen gehört. Auf der einfachsten Ebene handelt es sich um »Cookies«, die es Websitebetreibern erlauben, jemandes Fährte aufzunehmen; auf einer etwas komplexeren Ebene sind es digitale Zertifizierungstechni-

ken, die persönliche Daten kombinieren, um es einer Person im Netz zu ermöglichen, ihre Identität gegenüber anderen auszuweisen. Die kurz vor der Marktreife stehenden biometrischen Technologien erlauben eine eindeutige Identifikation von Personen mittels der Erfassung unverwechselbarer Körpermerkmale. Wenn Identifikation möglich ist, ist auch Regulierung möglich. Damit wird der ursprüngliche Charakter des Netzes, seine Freiheit, preisgegeben.

\*

iCraveTV zum Beispiel war ein Internet-Sender in Kanada. Gemäß kanadischem Recht war es ihm erlaubt, Sendungen des kanadischen Fernsehens aufzuzeichnen und sie in jedem beliebigen Medium wieder auszustrahlen. iCraveTV beschloss, die TV-Sendungen über das Internet wieder auszustrahlen.

In den USA jedoch ist Free TV nicht erlaubt. Nach US-Recht muss der wiederausstrahlende Sender mit dem Erstsender über die Rechte verhandeln. Daher setzte iCraveTV Technologien ein, die verhindern sollten, dass US-Amerikaner die Website von iCraveTV besuchen können. Kanadier sollten Zugang zu Free TV haben, Amerikaner nicht.

Es ist aber ein Charakteristikum der – noch – bestehenden Architektur des Netzes, dass kaum lückenlos kontrollierbar ist, wer welche Websites aufrufen kann. Daher gab es einige Amerikaner, die trotz der gegenteiligen Bemühungen der Firma Zugang zu iCrave TV erlangten.

Hollywood war darüber nicht begeistert. Also reichte man umgehend Klage bei einem Bundesgericht in Pittsburgh ein, um die Einstellung der kanadischen Website zu erwirken. Das Argument war: egal, ob Free TV in Kanada legal ist, in den Vereinigten Staaten ist es nicht legal; daher sollte, nachdem manche in den USA Zugang zu Free TV bekommen könnten, das US-Gericht Free TV abstellen. Weil Copyright-Gesetze in den USA verletzt wurden, wurde eine massive und rasche Reaktion des Bundesgerichts gefordert.

Halten wir kurz inne und stellen wir uns vor, dass eine vergleichbare Forderung anderswo erhoben wird. Nehmen wir beispielsweise an, ein deutsches Gericht fällt ein Urteil gegen Amazon.com, das die Firma zwingt, den Verkauf von *Mein Kampf* auf der ganzen Welt einzustellen, weil irgend jemand in Deutschland es geschafft hat, das Buch über Amazon.com zu bestellen. Oder stellen wir uns ein Gericht in China vor, das

einem amerikanischen Internet-Provider vorschreibt, die Website eines Dissidenten vom Netz zu nehmen, weil die fraglichen Aussagen in China illegal sind. Ein Amerikaner braucht nur eine Sekunde, um zu dem Schluss zu kommen, dass solche Urteile das Recht auf freie Rede verletzen, dass sie den freien Informationsfluss behindern und dass sie einen unzulässigen Eingriff der Staatsmacht in den Cyberspace darstellen.

Für das Gericht in Pittsburgh zählte die freie Rede dagegen nicht. Die Tatsache, dass Kanadier ein Recht auf Free TV haben, spielte keine Rolle. Das Gericht ordnete die vorläufige Schließung der Website an, bis die Betreiber beweisen konnten, dass sie in der Lage sind, den Zugriff von Nicht-Kanadiern zu verhindern. iCraveTV fügte sich und entwickelte rasch Technologien, mit denen die Unterteilung des Cyberspace in geographische Zonen möglich wurde.

Das Muster sollte jetzt klar sein. Obwohl Nationen wie die USA die Wichtigkeit der freien Rede im Cyberspace predigen, fallen alle Werte in sich zusammen, sobald es um Fragen der nationalen Sicherheit – und dazu zählen alle Copyrightangelegenheiten – geht. Der Trend geht dahin, das Internet in Zonen zu unterteilen, um lokale Regulierung zu ermöglichen. Die Technologien für diese Segmentierung stehen schon bereit.



Die Zukunft des Netzes wird sich grundlegend von seiner Vergangenheit unterscheiden. Sie wird Kontrollmöglichkeiten bieten, die seiner ursprünglichen Konstruktion fremd waren. Die Zukunft gehört einem Netz mit lokalen, von Einzelstaaten auferlegten Regulierungen. Diese Regulierungen werden auf technologischer Ebene funktionieren: indem sie in die Architektur des Cyberspace selbst eingebaut werden. Damit wird sich der Charakter des ursprünglichen Raums – seine Freiheit – verändern.

Aber es ist eine zweite Form von Kontrolle, auf die ich mich hier konzentrieren möchte. Es ist nicht die Kontrolle des Staates über unser Verhalten im Cyberspace – diese Geschichte ist mittlerweile hinreichend bekannt. Es geht mir vielmehr um die Kontrolle, die der Cyberspace selbst Akteuren in diesem Raum über andere Akteure zugesteht. Eine Geschichte, die John Naughton in seinem außergewöhnlichen Buch *A Brief History of the Future* erzählt, soll diesen Punkt illustrieren.

1964 präsentierte ein Wissenschaftler aus dem RAND-Team<sup>2</sup> namens

Paul Baran dem US-Verteidigungsministerium den Entwurf eines Telekommunikationsnetzwerks, das dem heutigen Internet sehr ähnlich war. Es hatte nicht genau die Architektur des Internet, und Baran war vielleicht auch nicht der erste, der einen solchen Entwurf vorstellte, aber die Idee war radikal und bedeutend genug, dass das Verteidigungsministerium seine Experten um eine Beurteilung des Entwurfs bat.

Als Experte fungierte die Firma AT&T. Ihr gefiel der Plan nicht. AT&T-Geschäftsführer Jack Osterman meinte: »Erstens kann es nicht funktionieren, und wenn doch, wären wir doch verrückt, wenn wir die Schaffung eines Konkurrenten zulassen würden.«

Das amerikanische Telefonnetz hatte eine besondere Architektur, in der bestimmte Prinzipien verankert waren. Der Inhaber des Netzes – AT&T – konnte entscheiden, wie es genutzt werden durfte. Das Netz zentralisierte diese Entscheidung, und diese Konstruktion wurde von der zuständigen staatlichen Behörde, der FCC<sup>3</sup>, unterstützt. Bis in die späten 60er Jahre – und teilweise sogar bis zur Aufteilung von AT&T 1984 – hatte der Netzbetreiber die Macht zu entscheiden, welche Innovationen in seinem Telekommunikationsnetzwerk zulässig waren.<sup>4</sup> Diese Entscheidungsmacht war in der Architektur verankert.

Dieses Prinzip hatte Auswirkungen auf Innovationen. Wer eine neue Technologie zur Nutzung des Telekommunikationsnetzwerks anzubieten hatte, wusste, dass AT&T die Idee gutheißen musste, bevor sie realisiert würde. Neue Ideen waren auf jemandes Erlaubnis angewiesen, bevor sie umgesetzt werden konnten, und jeder wusste, dass dieser Jemand ein massives Interesse am bestehenden Modell der Telekommunikation hatte. Innovationen, die mit diesem Modell vereinbar waren, hatten gute Chancen übernommen zu werden. Aber neue Ideen, die sich nicht ohne weiteres mit ihm vertragen würden, hatten nicht die geringste Chance. Jeder vernünftige Innovator würde seine kreative Energie anderswo einsetzen.

Zentral für den ursprünglichen Bauplan des Internet ist aber ein anderes architektonisches Prinzip mit anderen Auswirkungen auf Innovationen. Erstmals 1981 von den Netzwerkarchitekten Jerome Saltzer, David P. Reed und David Clark beschrieben, regt dieses Prinzip – »end-to-end«-Prinzip oder kurz »e2e« genannt – Programmierer an, Intelligenz an den jeweiligen Enden zu plazieren und das Netzwerk selbst dumm zu halten. Dumme Netzwerke, kluge Anwendungen.



Zunächst unter dem Aspekt der Effizienz beschrieben, wurde schnell klar, dass dieses Prinzip eine wichtige Implikation hat: wettbewerbsfördernde Neutralität. End-to-end bedeutet, dass das Netzwerk selbst nicht in der Lage ist, irgendwelche Unterscheidungen zu machen. Es ist nicht fähig zu entscheiden, welche Anwendungen laufen sollten oder welche Inhalte zuzulassen sind. Ein solches Netzwerk ist dumm; es verarbeitet die Datenpakete blind. Es kann genauso wenig unterscheiden, welche Pakete »Konkurrenten« sind, wie das Postamt erkennen kann, in welchen Briefen es kritisiert wird.

Diese Architektur fördert Innovationen. Programmierer können davon ausgehen, dass jede neue Anwendung und jeder neue Inhalt in diesem Netzwerk laufen werden. Sie müssen nicht mit allen möglichen Betreibern verhandeln, bevor sie ihre Programme in deren Netzwerken einsetzen. Selbst wenn eine neue Anwendung die bis dahin dominierende Netzwerk-anwendung konkurrenziert, kann sie in diesem Netzwerk laufen.

Der Prüfstein des Erfolges einer Innovation ist hier nicht, ob sie in die Geschäftspolitik des Netzbetreibers passt, sondern ob der Markt sie verlangt. E2e ist damit ein Prinzip, das Innovation auf der Ebene der Architektur hervorbringt. Dieser Wert war in das ursprüngliche Netz eingebaut, was in der Folge außergewöhnliche Innovativität und Kreativität garantierte.

E2e ist nicht das einzige Prinzip der ursprünglichen Architektur des Internet. Es ist nicht die einzige Art und Weise, wie Innovationen begünstigt wurden – andere Strukturen im ursprünglichen Modell leisten Vergleichbares. Ein Großteil des ursprünglichen Internets war nach dem Open Source-Prinzip konstruiert; Open Source-Software ist Software, deren Quellcode jedermann zur Verfügung steht und die nach Wunsch verwendet und weiterentwickelt werden kann. Das bedeutet zweierlei: dass die bestehenden Ressourcen von anderen für Innovationen genutzt werden können; und dass das System – weil es offen, also nicht unter der Kontrolle irgendeiner Firma, ist – neue Verwendungsweisen nicht diskriminieren kann. Genau wie bei e2e bleibt die Plattform eines Open Source-Systems neutral, und lädt so zu Innovationen ein.

Die Urform des Internet ist eine neutrale Plattform, eine Art Gemeingut<sup>5</sup>, von dem alle zehren können. Es ist eine öffentliche Ressource, die ein öffentliches Gut hervorbringt, es ist ein Erbe, das das größte Ausmaß an Kreativität und Innovation hervorgebracht hat, das die Welt je gesehen hat.

Diese Neutralität, dieses Gemeingut wird mittels einer bestimmten Art von Technologie, die das Netz regiert, geschaffen, sie wird konstruiert. Sie ist ein Prinzip, das gewählt wird.

Dieses Prinzip der Neutralität verändert sich derzeit, besser gesagt: Wir verändern es. Mit dem Umstieg von Telefonverbindungen auf Breitbandtechnologien wird das Netz so umgebaut, dass das e2e-Prinzip verletzt wird. Es wird in einer Weise umgebaut, die den Netzbetreibern Macht über die zulässigen Verwendungsweisen des Netzes gibt. Es wird so konstruiert, dass es die Eigentümer der Verbindungswege – gleich, ob Kabel oder Funk – ermächtigt zu entscheiden, welche Inhalte über das Netz verbreitet werden. Es wird so umgebaut, dass es strategische Entscheidungen der Netzbetreiber ermöglicht. Die ursprüngliche Neutralität wird damit untergraben.

In den Vereinigten Staaten ist diese Umstellung im Zuge des Ausbaus der Breitbandtechnologien bereits in vollem Gange. Die großen Player sind AT&T, das so viele Kabelmonopole aufkauft wie es nur kann, und AOL, das eben Time-Warner geschluckt hat. Beide Firmen waren einmal Befürworter einer offenen und neutralen Internet-Plattform. Aber kaum waren sie selbst Eigentümer von Kabelnetzen, war jeder von ihnen an einer Kontrolle der Inhalte interessiert, die über ihre Leitungen liefen.

Nehmen wir zum Beispiel die Videoübertragung. Die Kabelmonopolisten übertragen Videoinhalte derzeit auf Fernsehgeräte. Das Internet (denken wir nur an iCraveTV) ermöglicht die Übertragung solcher Inhalte auf Computer. Aber die Kabelbetreiber in den USA haben diese Übertragung eingeschränkt (während sie für die Übertragung auf Fernsehgeräte Gebühren verlangen). Und auf die Frage, ob Computer-Videoübertragung über das Kabelnetz überhaupt jemals zugelassen würde, antwortete der Leiter der AT&T Internet Services: »Wir haben nicht 56 Milliarden für ein Kabelnetzwerk ausgegeben, damit uns jetzt das Blut aus den Adern gesaugt wird.«

\*

Es geht um das Prinzip – das Prinzip, das wir aufgeben. Wenn wir den Netzbetreibern erlauben, das Netzwerk unter Umgehung des e2e-Prinzips auszubauen, erlauben wir ihnen auch, die Innovationsanreize, die das ursprüngliche Netz bot, abzubauen. Die Entscheidung für einen bestimmten Code ist auch eine Entscheidung über die Innovationen, die der Code zu fördern oder zu hemmen imstande ist.

Die vorgeführten Beispiele sollten zeigen, worum es heute geht. Sowohl im Hinblick auf Freiheit als auch auf Innovation verändert sich der Cyberspace. Beide Male werden Grundprinzipien des ursprünglichen Internet ausgehöhlt. Die Zukunft wird nicht wie die Vergangenheit sein.

Alle diese Veränderungen geschehen, weil sich die Architektur des Netzes verändert, weil sie verändert wird und wir dies zulassen. Die ursprüngliche Architektur wird weiterentwickelt, um sich ihrer Prinzipien zu entledigen und den Cyberspace immer mehr an die wirkliche Welt anzugleichen – um ihn reguliert und konzentriert, kontrolliert und farblos zu machen.

Sowohl im Hinblick auf das Prinzip der Freiheit als auch auf das der Innovation ist der Ursprung dieser Veränderung in der Wirtschaft zu suchen. Ihr widerstrebt das Unregulierte, sie strebt nach einem gesicherten Monopol – nach Macht. Und dieses Streben hat Folgewirkungen.

Wenn wir heute über Macht und ihre Auswirkungen nachdenken; wenn wir über den Staat nachdenken, der seine Macht einsetzt, um bestimmte Effekte zu erzielen; wenn wir über internationale und lokale Politik nachdenken – dann müssen wir einen anderen Schwerpunkt setzen.

Statt uns allein auf die Machtkonstellation zwischen den Staaten zu konzentrieren, sollten wir uns zuallererst mit der Machtverschiebung auseinandersetzen, die die Entstehung der »Cyberspace« genannten Architektur mit sich gebracht hat: wie weit dieser Raum eine neue Quelle der Macht darstellt, deren Wesen von seiner Konstruktion abhängt. Und als nächsten Schritt sollten wir uns überlegen, wie sich der spezifische Charakter der ursprünglichen Macht dieses Raums heute verändert. Wie wir zulassen, dass er sich verändert, weil die Wirtschaft den Code verändert.

Auf der Bühne, die die Architektur des Cyberspace bietet, werden Machtkämpfe ausgetragen: Es geht darum, ob Staaten Macht haben, und wenn ja, wieviel; ob Mitbewerber Macht haben über andere Mitbewerber, und wenn ja, wieviel. Eine Analyse internationaler Beziehungen, die diese Bühne ignorierte, wäre genauso unvollständig wie eine, die China ignoriert.

Aber wenn wir den Stellenwert des Cyberspace ernst nehmen – seine Rolle bei der Regulierung all dieser Beziehungen, sein Potential, neue Formen der Regulierung einzuführen – dann werden wir erkennen, wie er sich verändert. Dann wird uns klar, dass wir zulassen, dass er sich verändert; dass wir dastehen und zusehen, wie dieser neue Raum und seine Ökologie umgemodelt, ausgehöhlt, zerstört werden – durch die Verän-

derung einer Architektur, die einen Freiraum definierte, ein Gemeingut, das die größte Revolution der Kreativität hervorgebracht hat, die wir je gesehen haben.

*Aus dem Englischen von Klaus Nellen und Anita Traninger*

*Anmerkungen der Redaktion*

- 1 Der Begriff wurde dem Roman *Newromancer* des amerikanischen Science-Fiction-Autors William Gibson entlehnt und bezeichnet einen virtuellen Raum, der nur in der Computerwelt existiert. Inzwischen wird »Cyberspace« als Synonym für das Internet verwendet.
- 2 RAND (ein Akronym aus den Begriffen »research and development«) ist eine seit dem Ende des 2. Weltkriegs bestehende Non-Profit-Organisation mit dem Ziel, als Think tank politische Entscheidungsfindungen durch Forschung und Analyse zu unterstützen.
- 3 Die FCC (*Federal Communications Commission*) ist eine Regierungsbehörde, die für die Förderung des Wettbewerbs in allen Sektoren der Kommunikationsindustrie zuständig ist.
- 4 Als Nachfolgerin der *Bell Telephone* hatte die *American Telephone and Telegraph Company* von Anfang des 20. Jahrhunderts bis 1983 das – staatlich geduldete – Telefonmonopol innerhalb der USA. Der Anschluss von Fremdgeräten war verboten, mit dem Argument, dass sie das Gesamtsystem stören könnten. So war es unmöglich, neue Technologien in das AT&T-System einzuführen. Angesichts dieser Firmenpolitik und der Fortschritte auf dem Gebiet der Datenübertragung sah sich die US-Regierung schließlich dazu veranlasst, ein Kartell-Verfahren gegen AT&T einzuleiten. 1982 kam es zu einer Einigung, in deren Folge AT&T in kleinere Firmen (»Baby Bells«) zerlegt wurde.
- 5 Im Original »commons«, ein Begriff aus dem anglo-amerikanischen Eigentumsrecht, der ein Stück Land bezeichnet, das von der Allgemeinheit genutzt werden kann.