

Code is Law Law is Code

Der Code ist das Gesetz des Cyberspace, so hat das William Mitchell 1995 formuliert. Lawrence Lessig (1999) macht diesen Gedanken zum Gegenstand eines ganzen Buches, das weltweit Aufsehen erregt hat. Der Code, so Lessig, ist das Gesetz. Wenn das stimmt, so muss sich der Satz auch umdrehen lassen. Das Gesetz ist der Code. Nach meiner Meinung, das will ich gleich vorweg sagen, stimmt beides nicht. Aber man kann eine ganze Menge über die Grundstrukturen unseres Rechtssystems als Entscheidungssystem lernen, wenn man sich einmal mit diesem etwas merkwürdigen Thema auseinandersetzt.

Man kann zum Beispiel lernen, welche Ziele wir mit Rechtssystemen verfolgen und welche Mittel wir einsetzen um diese Ziele zu erreichen. Man kann ferner die Frage stellen, ob das Rechtssystem dem Code überlegen ist oder ob es umgekehrt nahe liegt, Teile der Architektur des Cyberspace in das Rechtssystem zu übertragen. Schließlich kann man einige Grundaussagen über *Aktualität in der Informationsgesellschaft* machen, die zeigen, wie sich Rechtssysteme in einer netzbasierten Welt durch Gerichtsentscheidungen verändern. Diese Veränderungen betreffen alle Rechtssysteme der Welt, nicht nur Common Law und Civil Law, sondern auch die religiös basierten – etwa islamischen oder buddhistischen – Rechtssysteme oder Mischformen, wie etwa das chinesische Rechtssystem, solange nur der Zugang zum Netz gewährleistet ist.

Der Code, so Lessig, ist für den Computerwissenschaftler Gesetz (Lessig 1999, S. 383) »und wenn der Code Gesetz ist, sollten wir zunächst einmal fragen: Wer ist der Gesetzgeber? Wer verfasst das Gesetz, das uns reguliert? Welche Rolle spielen wir bei der Festlegung dieser Regulierung? Welches Recht haben wir über diese Regulierung Bescheid zu wissen? Und wie können wir sie gegebenenfalls überprüfen?« (Lessig 1999, S. 383). Diesen Fragen hat die Computerwissenschaftlerin Jean Camp, die an der Kennedy School of Harvard lehrt, entgegen gehalten, dass das Problem nicht darin liege, dass der Code Gesetz ist, oder dass der Code reguliert. Das Problem liege vielmehr darin »dass wir uns nicht darüber unterhalten, wie der Code reguliert« (bei Lessig 1999, S. 382).

Was ist der Code?

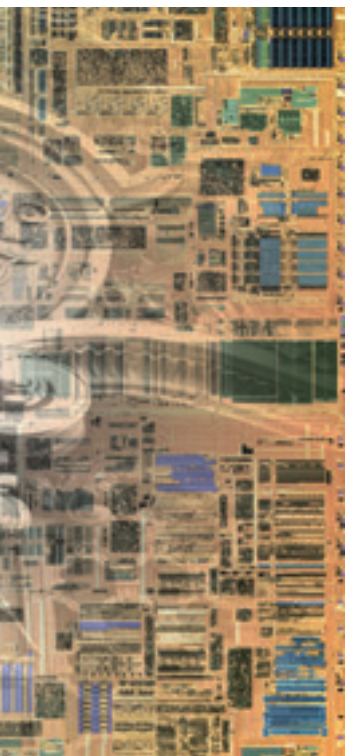
Damit ist zunächst einmal die Frage gestellt, was der Code eigentlich ist. Lessig meint, es sei die *Architektur* des Cyberspace. Er unterscheidet zwischen Recht, sozialen Normen, Markt und Architekturen, als den vier Faktoren, die das Verhalten von Menschen und Systemen regulieren. Meist wird die Netzarchitektur mit dem Begriff *Software* übersetzt – an einigen wenigen Stellen wird aber deutlich, dass es in Wahrheit um das Zusammenspiel von Hardware, Netz, Netztechnik und Software geht. Vereinfacht kann man sagen: Es geht um die Netztechnik, also darum, wie das Netz funktioniert, wie es beschaffen ist und damit über die Anwendungsmöglichkeiten und die Anwendungsgren-



zen des Netzes. Die Anwendungsmöglichkeiten und die Anwendungsgrenzen wirken dann zurück auf das Recht, den Markt und die sozialen Normen. Der Netztechniker wird – so Lessig – zum Gesetzgeber (Lessig 1999, S. 383 und öfter).

So ganz revolutionär scheint diese Erkenntnis nicht zu sein. Dass Gegenstände unserer Alltagswelt von Technik bestimmt und beeinflusst sind, ist nun wirklich nichts Neues. Ein Auto hat die Eigenschaft, sich zu bewegen und damit kinetische Energie zu entfalten. Um das Energiebündel zu bändigen, müssen Autos über Bremsen, Scheinwerfer, Blinker, Knautschzone, Luftsäcke, Sicherheitsgurte und vieles andere mehr verfügen. Das Zusammenrücken zwischen Technik und Recht ist stark. Die Straßenverkehrszulassungsordnung ist voll von technischen Regeln. Es kann überhaupt keine Rede davon sein, dass der Techniker der alleinige *Gesetzgeber* bei der Konstruktion eines Autos ist. Werfen wir einen Blick auf die Maschinenparks und Produktionsanlagen in unseren Fabriken. Wir finden technische Normen in Hülle und Fülle, daneben Umweltvorschriften, Unfallverhütungsstandards und DIN-Normen, ohne die es die Industrie in der ganzen Welt überhaupt nicht gäbe. Nun wissen wir alle, dass DIN-Normen durch privatrechtlichen Konsens entstehen, während ein Großteil der Umweltschutz- und Unfallverhütungsvorschriften vom staatlichen Gesetzgeber vorgegeben werden. Aber aus der Perspektive der Techniker kann überhaupt kein Zweifel daran sein, dass sie nicht die *Gesetzgeber* bezüglich der Technik, also der Architektur von Maschinen und Netz, sind. Ganz im Gegenteil, Regeln und Technik sind aufeinander angewiesen, wie zwei kommunizierende Röhren, die gemeinsam nach dem Anwendungsoptimum für menschliche Bedürfnisse suchen.

Das gilt alles auch für netzbasierte Techniken. Schauen Sie auf die Strom-, Gas- oder Wassernetze und Sie



finden dort ausdifferenzierte Formen, die etwa im grid code, distribution code oder metering code zusammengefasst sind. (abgedruckt bei Schwintowski / Dannischewski 2002). Überlagert werden diese technischen Regeln durch rechtliche Normen, etwa im Energiewirtschaftsgesetz oder im Gesetz gegen Wettbewerbsbeschränkungen oder im Energieeinspeisegesetz, um nur einige wenige Regelwerke zu nennen.

Das Gleiche findet man im Bereich der Telekommunikation. Dem TKG als normativem Grundwerk sind eine Fülle von Ausführungs- und Ergänzungsgesetzen beigegeben, die technische Regeln und Standards enthalten. Gemeint sind etwa Zugangsregeln, Regeln über die Nummernportabilität oder über den Universaldienst oder die Vergabe von UMTS-Lizenzen.

Wie kann man angesichts dieses Zusammenwirkens von Technik und Recht auf die Idee kommen, dass die Techniker im World Wide Web machen können was sie wollen, dass sie zum Gesetzgeber werden, dass sie diejenigen sind, die die Standards vorgeben, und sich damit der demokratischen Kontrolle weitgehend entziehen?

Die Antwort hierauf hat zunächst einmal damit etwas zu tun, dass das World Wide Web und die ihm immanente Anwendungsmöglichkeiten noch sehr jung sind und, dass die Fragen aus der Perspektive eines amerikanischen Verfassungsrechtlers gestellt werden. Das amerikanische Verfassungsrecht ist – gemessen am deutschen Verfassungsverständnis – außerordentlich konservativ. Gegenstand der Entscheidungen des amerikanischen Supreme Court ist *staatliches Handeln*. Im World Wide Web handeln aber nicht der Staat, sondern private Unternehmen wie etwa AOL oder T-Online. Die von diesen privaten Akteuren im Netz verwendeten *Architekturen* beschränken in vielen Fällen die Verhaltensspielräume der Kunden. Dies bereitet einem amerikanischen Verfassungsrechtler Sorgen, weil er nicht sicher ist, ob der Supreme Court wohl bereit ist, die von den privaten Dienstleistern im Internet aufgestellten Schranken verfassungsrechtlich zu überprüfen. Interessanterweise verweisen die amerikanischen Verfassungsrechtler für dieses Schutzproblem auf die vorbildliche deutsche Verfassungstradition. Sie meinen die Lehre von der Drittwirkung der Grundrechte im

Privatrecht und sie müssten ergänzend auf die Rechtsprechung des Europäischen Gerichtshofes zur Wirkung der Grundfreiheiten des Europäischen Vertrages gegenüber den nationalen Rechtsordnungen hinweisen. Nur zwingende Gründe des Allgemeininteresses vermögen Schranken der Grundfreiheiten in Europa nationalstaatlich zu legitimieren.

So gesehen ist es im ersten Augenblick zumindest verständlich, wenn sich ein amerikanischer Verfassungsrechtler darüber Sorgen macht, ob die Gestaltungsmacht privater Dienstleister im www wohl hinreichend auf Fairness und Freiheit kontrolliert wird. So ganz überzeugt bin ich von den Bedenken der amerikanischen Verfassungsrechtler aber trotzdem nicht, denn immerhin verfügt das amerikanische Recht mit dem Sherman-Act aus dem Jahre 1892 über das älteste und mächtigste Kartellrecht überhaupt. Daneben stehen eine Vielzahl von Fairness-Rules in ganz unterschiedlichen Kodifikationen. Die amerikanischen Kartellbehörden und -gerichte haben in der Vergangenheit immer wieder gezeigt, dass sie mit diesem Instrumentarium gegen private Machtentfaltung auf Märkten hervorragend umzugehen in der Lage sind. Die Verfahren gegen IBM und Microsoft mögen als Beispiel genügen. Hinzu kommt, dass die amerikanischen Gerichte die Grundsätze des amerikanischen Kartellrechts schon immer extra territorial angewandt haben. Jedenfalls haben sie dies dann getan, wenn sich kartellrechtsrelevantes Verhalten in den Vereinigten Staaten *auswirkte*, ganz gleichgültig, an welchem Ort der Welt es veranlasst war. Dieser mit dem Begriff *Auswirkungstheorie* erfasste Rechtssatz ist heute fester Bestandteil des *Kartellvölkerrechts* geworden. Wir finden ihn im Deutschen Kartellrecht im § 130 Abs. 2 GWB.

Diese Hinweise zeigen, dass es bei der ganzen Diskussion um *Code is Law* möglicherweise nicht nur um das Aufzeigen von Schutzlücken im System, sondern auch um einen kleinen Machtkampf zwischen dem Verfassungsrechtler auf der einen Seite und den Kartellrechtlern auf der anderen Seite in den USA geht. Aber hiervon abgesehen: Wo liegen eigentlich die Probleme?

Schutzlücken im Code

Um es gleich vorweg zu sagen – die Schutzlücken im Code entstehen nicht durch die einem Computer und einem Netz eigentümliche Vermittlungstechnik. Information ist bekanntlich aus Bits zusammengesetzt, mit denen herkömmliche Computer rechnen. Dort kann ein Bit den Wert Null oder Eins haben und es wird repräsentiert durch den Ladungszustand eines Schaltelements. Information wird umgeformt in »Strom fließt« oder »Strom fließt nicht« und bei dem Empfänger ent-

sprechend entschlüsselt. Der Satz »Code is Law« hat informationstechnisch folgende Struktur:

```
01000011011000100110010001100101010
00000011010010111001101000000010011
00011000010111011000101110
```

Ähnliche Strukturen findet man auch in der Quantenmechanik. Dort gibt es Zustände, die Null oder Eins entsprechen, etwa der Anregungszustand eines Atoms oder die Achsrichtung eines rotierenden Teilchens, SPIN genannt. Hiervon ausgehend sind Mathematiker wie *Peter Shor* derzeit dabei *Quantencomputer* mit Anwendungsmöglichkeiten zu entwickeln, die bei der Bewältigung sehr großer Datenmengen den herkömmlichen Bit gesteuerten Computern weit überlegen sind (Röthlein 2004, S. 133 ff). Gemeint sind zum Beispiel Identifizierungstechniken. Dahinter verbirgt sich das Problem der Sicherheit im Netz, etwa wenn man mit seiner Kreditkarte bezahlt oder wenn man vertrauliche Informationen austauschen will. Wie kann man sicherstellen, dass die Daten nur von demjenigen empfangen werden können, für den sie bestimmt sind und wie kann man sicher sein, dass die Daten von demjenigen kommen, der behauptet, der Absender zu sein? Um das Problem der Netzsicherheit in den Griff zu kriegen, arbeitet man heute an *Biometrischen Verfahren*, die es möglich machen sollen, einen Menschen mit einem Computer zu verknüpfen. Bei Compaq etwa entwickelte man ein Lesegerät für den Daumenabdruck. Man kann auch den Computer mit der Iris des menschlichen Auges verknüpfen und auf diese Weise sicherstellen, dass bestimmte Daten nur von demjenigen empfangen werden können, der mit den richtigen Augen in den Bildschirm schaut. Die Frage, die – zu Recht – gestellt wird, lautet, ob man die Entwicklung solcher Identifizierungstechniken ohne rechtliche Begleitung zulassen darf oder ob der *Staat darauf ein Auge haben muss*, wenn AOL, T-Online und andere Giganten im www zum *Big Brother is watching you* mutieren. (Lessig 1999, S. 111 ff) Die Mitglieder der AOL-Gemeinde können sich darauf verlassen, dass AOL niemandem, auch nicht der Staatsanwaltschaft, der Steuerbehörde oder dem Militär die Möglichkeit eröffnet, das von ihnen gewählte Pseudonym mit ihrem realen Namen zu verbinden. Folglich kann man im Netz, erheblich leichter als im realen Leben, problematische Inhalte, wie beispielsweise Gewaltverherrlichung oder Kinderpornographie, verstecken. Umgekehrt ist die Meinungsfreiheit der AOL-Mitglieder begrenzt. Die Besitzer von AOL können zwar zu allen Mitgliedern sprechen, die Mitglieder haben aber untereinander keinen öffentlichen Raum, in dem sie sich im Netz versammeln könnten. Selbst in einen Chatroom können nur 23 Mitglieder gleichzeitig anwesend sein. (Lessig 1999, S. 131) Gegen diese *Begrenzung der Meinungsfreiheit* – wenn es denn



eine ist – gibt das amerikanische Verfassungsrecht keine Handhabe. Im Deutschen Recht würde man fragen, ob diese Begrenzungen nicht den Charakter einer *Allgemeinen Geschäftsbedingung* tragen und möglicherweise unangemessen sind (§ 307 BGB).

AOL kann die Aktivitäten der Mitglieder im Netz verfolgen und Daten über ihr Verhalten sammeln. An diesen Daten können Mitglieder partizipieren, wenn sie auf einer *Buddy-Liste* stehen. Wenn beispielsweise Ihr Partner auf der Buddy-Liste steht, dann hören Sie auf Ihrem Rechner eine Tür zufallen, wenn er oder sie online geht. Sie können dann auf Ihrem Rechner verfolgen – ohne dass der Partner dies weiß – in welchen Chatroom er sich gerade begibt, oder mit wem er gerade sonst kommuniziert. Da können sehr delikate Daten bei dem Falschen landen. Das Deutsche Recht würde eine solche Netzarchitektur nur zulassen, wenn der Nutzer in die Datenweitergabe vorher eingewilligt hätte (§ 4a BDSG).

Befürchtet wird auch, dass das Netz einen zu starken Urheberrechtsschutz gewährt. Die Urheber können den Zugang zu ihren Texten mit einem *trusted system* verbinden und haben so die Möglichkeit, sich die Nutzung bezahlen zu lassen. (Lessig 1999, S. 231 f.) Die *trusted systems* erreichen genau dasselbe wie der Copyright Schutz, allerdings ohne dass das Gesetz die Beschränkung vornimmt. Was das Urheberrecht durch Strafandrohung und Schadensersatz zu erreichen versucht, das verwirklichen *trusted systems* mithilfe des Codes. Das Urheberrecht verpflichtet andere, die Rechte des Urheberrechtinhabers zu achten, wenn sie sein Eigentum nutzen. Die *trusted systems* gewähren nur dann Zugang, wenn diese Rechte beachtet werden. Die erforderlichen Kontrollmechanismen sind in das System integriert. Der Code ersetzt das Recht, indem er die Gesetze in sich aufnimmt und gewährleistet deren Einhaltung sehr viel wirkungsvoller als dies bisher der Fall war. In einer solchen Situation sind die Urheber sehr viel stärker durch den Code geschützt, als dies bisher über das Gesetz der Fall war. Es könnte in Zukunft nicht mehr um Urheberrechte gehen, sondern um Urheberpflichten – um die



Pflicht der Inhaber geistigen Eigentums, dieses Eigentum anderen zugänglich zu machen. (Lessig 1999, S. 227)

Mag sein, dass es so kommt. Die Urheber würden dann über eine ähnlich starke Stellung ver-

fügen, wie die Inhaber von Patenten. Das Patentrecht eröffnet in dieser Situation die Einräumung von Zwangspatenten. – Über etwas Ähnliches müssten wir wohl dann auch bei Urheberrechten nachdenken. Außerdem wird der Markt über angemessene Preise automatisch dafür sorgen, dass die Urheber ihre Texte freigeben. Hiervon abgesehen dürften die meisten Probleme spätestens nach der Erstveröffentlichung gelöst sein, wenn nämlich der Text allgemein zugänglich geworden ist. Wie auch immer, auch diese Probleme der Netzarchitektur scheinen auf dem Boden des derzeit geltenden Rechts ohne weiteres lösbar zu sein. Schwieriger scheint es nach wie vor zu sein, den Schutz der Urheber – insbesondere im Bereich der Musikindustrie – weltweit zu gewährleisten.

Schließlich wird auf Lücken beim Verbraucherschutz hingewiesen. (Lessig 1999, S. 343) Der Verbraucher werde im Netz veranlasst, fremde Rechtsordnungen zu wählen, die er nicht beurteilen und einschätzen könne. Dieses Problem ist in der Tat ein wichtiges und vielbeachtetes. Es hat nun aber wirklich nichts mit der Netzarchitektur oder der Netztechnik zu tun. Es geht ausschließlich um die verbraucherschützende Ausgestaltung des nationalen IPR und die Anwendung dieser Regeln auf jeden Anbieter im Netz, ganz gleichgültig, welche Rechtsordnung er als Referenzordnung durchzusetzen versucht. Man muss in der Tat aus der Perspektive der nationalen Rechtsordnung über die Frage nachdenken, welche Klauseln missbräuchlich sind. Dabei ist es sinnvoll, zwischen Klauseln zu unterscheiden, die nur im Netz verwendet werden können (netzspezifische Klauseln) und solchen, die im Netz besonders häufig angetroffen werden (netzübliche Klauseln). (Friske 2005) Gerade aber dieses Beispiel zeigt besonders gut, dass das Recht in der Lage ist, mit den Herausforderungen der Netztechnik Schritt zu halten und etwaige Schutzlücken auch angemessen zu schließen. Es mag sein, dass die Entwicklung neuer rechtlicher Kategorien gelegentlich etwas länger dauert, als es sich manche wünschen – aber die Befürchtung, der Netztechniker könnte zum Gesetzgeber werden, ist beim besten Willen nicht aufrechtzuerhalten. Was können wir trotzdem von der Behauptung *Code is Law – Law is Code* lernen?

Recht als Anwendungssoftware

Die erste interessante Erkenntnis aus dem Gedanken, dass der Code so etwas wie ein Gesetz sein könnte, ist, dass Recht umgekehrt gedacht *Anwendungssoftware* ist. Diese Erkenntnis scheint mir fundamental zu sein. Sie zeigt zunächst einmal, dass Recht *ein System* ist und dass es sich in einer permanenten dynamischen Selbstorganisation befindet. Wie bei jeder anderen Anwendungssoftware auch, kann der einzelne Bürger die eine oder andere Regel ohne weiteres begreifen und verstehen. Problematisch wird das Anwenden der Regeln im Gesamtzusammenhang, unter Berücksichtigung aller Systembausteine, die miteinander verwoben sind und aufeinander wirken. Wenn es z. B. in §144a VAG heißt, dass ein Versicherungsvermittler Verträge nur an im europäischen Wirtschaftsraum zugelassene Versicherer vermitteln darf, so ist das eine klare und jedem einsichtige Regelung. Schwieriger werden die Dinge, wenn man die europäische Dienstleistungsfreiheit hinzudenkt und fragt, ob man die Freiheit einer Dienstleistung überhaupt von einer Zulassung abhängig machen kann? Wenn ja, muss es dann nicht reichen, wenn die Zulassung in einem einzigen Staat der Europäischen Union erfolgt ist? Angenommen, die spanische Aufsichtsbehörde hat die Zulassung ordnungsgemäß erteilt – darf der Vermittler nun Verträge anbieten oder muss er warten, bis das Unternehmen in seinem Heimatland *notifiziert* ist? Möglicherweise bestehen gegenüber der Notifizierungspflicht Zweifel. Darf ein nationales Gesetz trotz solcher Zweifel eine Geldbuße verhängen? Ist da nicht der Bestimmtheitsgrundsatz von Art. 103 GG verletzt?

Das Beispiel zeigt, wie Rechtsordnungen funktionieren. Sie sind Systeme, die miteinander verschachtelt sind und aufeinander wirken. Sie sind durch bestimmte Rangregeln strukturiert, die im Gesetz nicht ohne weiteres zu finden sind. Für die Auslegung der unterschiedlichen Rechtsbegriffe sind bestimmte Methoden leitend. Und ganz grundsätzlich sind Prinzipien, die etwas mit der Verhältnismäßigkeit von Regeln zu tun haben, in jedem Falle zu beachten.

Das Rechtssystem beinhaltet also eine *Anwendungssoftware*, die sich dem Anwender nicht ohne weiteres erschließt. Sein Verhalten wird durch diese Art der Anwendungssoftware nicht quasi automatisch geändert – ganz im Gegenteil. Das Rechtssystem nimmt in Kauf, dass die Anwender die Strukturen und die Inhalte des Systems erst einmal lernen und begreifen müssen.

Bei einem technischen Code, wie er bei der Konfiguration des Internets gebräuchlich ist, ist dies ganz anders. Die Anwendungssoftware verändert die Be-



Prof. Dr. Hans-Peter Schwintowski

Jg. 1947. Im Anschluss an eine mehrjährige berufliche Tätigkeit studierte H.-P. Schwintowski Rechtswissenschaft an der Universität Göttingen. Nach Abschluss der beiden Juristischen Staatsexamina promovierte er 1982 über ein Thema aus der Fusionskontrolle. 1986 habilitierte H.-P. Schwintowski über Deregulierungsfragen auf Versicherungsmärkten. Es folgten Lehrstuhlvertretungen an den Universitäten Münster, München, Tübingen, Bielefeld und Passau. 1988 wurde er zum Prof. auf Zeit (C2) an der Universität Göttingen ernannt. Es folgten Berufungen an die Universitäten Würzburg (C3) und Passau (C4). 1993 nahm er einen Ruf (C4) an die Humboldt-Universität zu Berlin an, wo er seine Lehrtätigkeit im August 1993 aufnahm.

Kontakt

Humboldt-Universität
zu Berlin
Juristische Fakultät
Unter den Linden 9
D-10117 Berlin
Tel.: +49 30 2093-3329
Fax: +49 30 2093-3412
E-Mail:
hps@rewi.hu-berlin.de
www.rewi.hu-berlin.de/
jura/1s/swt

schaffenheit des Netzes automatisch und in jedem Einzelfall sofort. Niemand kann sich dieser Software mehr entziehen. Wenn erst einmal ein bestimmter Zugangscodes, eine bestimmte Zertifizierung, netztechnisch umgesetzt ist, müssen diejenigen, die Zugang begehren, den dafür erforderlichen Schlüssel benutzen und besitzen.

So gesehen erweist sich der technische Code im Netz als *starr*, während das Rechtssystem anpassungsflexibel und dynamisch ist. Rechtssysteme sind selbstlernende Systeme, sie organisieren sich über die ihnen immanenten Refferenzprinzipien täglich neu und täglich anders. Eine gewisse Ähnlichkeit mit einem Rechtssystem hat allenfalls der *offene Code*, also das, was die Netztechniker Open source-Software oder Quellcodes nennen. Bei diesen offenen Codes, die etwa von LINUX oder Netscape ins Netz gestellt wurden, können die Nutzer, die dem Code zugrunde liegende Architektur erkennen und umgestalten. Damit allerdings hat der Code für keinen Nutzer mehr Verbindlichkeit. Jeder kann ihn so umgestalten, wie er es wünscht. Es gibt keine Gerichte oder Instanzen, die darüber entscheiden würden, ob es zweckmäßig oder vernünftig ist, eine Umgestaltung zuzulassen. Der Quellcode ist somit ein offenes evolutorisches System, aber kein Rechtssystem, weil Letzteres seine Dynamik aus dem offenen Diskurs, den gerichtlichen Instanzen und der bindenden Endentscheidung gewinnt.

Der Wert, den dieses diskursive System für die Stabilität unserer sozialen Ordnungen hat, scheint mir auf der Hand zu liegen. Aber trotzdem ist immerhin die Frage erlaubt, ob das Rechtssystem möglicherweise unteroptimal organisiert ist, ob es eventuell Anleihen beim geschlossenen oder womöglich beim offenen Code nehmen sollte. Ein Rechtssystem, das so funktionieren würde wie ein geschlossener Code, würde sämtliche ihm immanenten Ge- und Verbote unmittelbar und sofort durchsetzen. Wir wissen alle, dass dies faktisch technisch nicht möglich ist. Aber selbst wenn wir die Köpfe der Menschen so vernetzen könnten, wie wir dies mit Computern tun, würden wir eine interessante Feststellung machen. Die materiellen Regeln des Rechtssystems würden sich bei sofortiger Um- und Durchsetzung aller Ge- und Verbote aufgrund der dem Rechtssystem immanenten Verhältnismäßigkeitsregeln sofort ändern. An die Stelle eines Rechtes für den Verzug würden Regeln treten, die es in bestimmten Fallkonstellationen erlauben, erst später zu bezahlen. An die Stelle des Rechtes für Leistungsstörungen würde ein Recht für Preisnachlässe treten, je nachdem, wie die Qualität der gelieferten Sachen tatsächlich ist. Für die vielen Übertretungen und Vergehen würde es eine

Fülle von Straffreistellungsgründen geben, die nach Kriterien gestaffelt wären, die wir heute noch gar nicht kennen. Kurz: Das Rechtssystem würde seine Wirkweise den Zielen anpassen, die wir mit dem heute gebräuchlichen Rechtssystem und seiner Wirkweise im Wesentlichen verbinden. Wir würden uns allerdings erstmals der Tatsache bewusst werden, welche Wirkung eigentlich Rechtsregeln haben, wenn sie flächendeckend sofort und unmittelbar umgesetzt werden. Immerhin zeigt dieses Gedankenexperiment, dass wir bei der Konstruktion unserer Rechtssysteme deren Wirkweise sehr wohl in unsere Überlegungen einbeziehen, ohne dies allerdings immer sehr offen zu machen. Vielfach wissen wir auch nicht ganz genau, wie das System wirken wird. Deshalb schaffen wir Normen, die den Gerichten zur Ausfüllung und Auslegung zugewiesen werden. Die Gerichte werden auf diese Weise zum Gesetzgeber, und zwar innerhalb des Rahmens und Spielraums, der ihnen durch die Offenheit der Rechtsbegriffe vom parlamentarischen Gesetzgeber zugewiesen wird.

Literatur

- Friske, Lars* (2005): Allgemeine Geschäftsbedingungen, Berliner Juristische Universitätsschriften, Bd. 47.
Lessig, Lawrence (1999): Code and other Laws of Cyberspace, New York; deutsche Ausgabe Code and andere Gesetze des Cyberspace, Berlin 2001,
Mitchell, William (1995): City of bits: Space Place, and the Infobahn, Cambridge, Mass., S. 111; ähnlich wie *Ethan Kartsh*, Software Worlds and the First Amendment: Virtual Doorkeepers in Cyberspace, University of Chicago Legal Forum 1996, S. 335, 338; *Joel Reidenberg*, Lex Informatica: The Formulation of Information Policy, Rules Through Technology, Texas Law Review 1976 (1998), S. 553; *James Boyles*, Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors, University of Cincinnati Law Review 66 (1997), S. 177; *Andrew Shapiro*, The Control Revolution, New York 1999.
Röthlein, Brigitte (2004): Die Quantenrevolution, Neue Nachrichten aus der Teilchenphysik, München, S. 133 ff.; vgl. für die klassische Codierung eines Computers, *Hans-Joachim Flechtner*, Grundbegriffe der Kybernetik, München 1984, S. 77 ff.; aus der Perspektive des Nervensystems; *Humberto R. Maturana*, Erkennen: Die Organisation und Verkörperung von Wirklichkeit, 2. Aufl., 1985, S. 230.
Schwintowski, Hans-Peter/Dannischewski, Johannes (2002): Deutsches und Europäisches Energie- und Netzrecht, EWeRK-Schriftenreihe, Band Nr. 7.