Christiane Schultz-Haddouti

Bürgerrechte im Netz. Zwischen Informationsfreiheit und Datenschutz

2007

https://doi.org/10.25969/mediarep/11874

Veröffentlichungsversion / published version

Sammelbandbeitrag / collection article

Bürgerrechte im Netz
Zwischen Informationsfreiheit und Datenschutz

Christiane Schulzki-Haddouti

Demokratie kann nur auf der Basis eines ausgewogenen Spiels der Kräfte funktionieren. Öffentlichkeit ist hierbei ein ausgezeichnetes Mittel, dieses Spiel am Laufen zu halten. Medien, die Öffentlichkeit herstellen, werden deshalb sogar als »vierte Macht« bezeichnet. Sie werden dann zur Macht, wenn sie nicht nur als Vermittler der öffentlichen Meinung auftreten, sondern durch ihr Agieren selbst Gesellschaft gestalten.

Hauptaufgabe der Medien ist es, eine Öffentlichkeit durch Transparenz herzustellen. Je mehr relevante Informationen Bürger erhalten, desto eher sind sie in der Lage, sich eine Meinung zu bilden. In den USA wird das Recht der Bürger auf Information umschrieben mit dem »Recht der Öffentlichkeit, zu wissen«, »the public's right to know«. Informationsfreiheit ermöglicht Bürgern, sich zu informieren, sich zu bilden und mündig Entscheidungen zu treffen. Die Medien stehen damit im Dienste des öffentlichen Interesses auf Wissen und Bildung.

Gefährdete Informationsflüsse

Computernetze als Kommunikationsmedium wurden in den USA von Anfang an in den Dienst der Wissenschaft, und damit auch der Öffentlichkeit gestellt. Der Eigenschaft des Internet, Angriffe auf seine technische Infrastruktur durch das mehrfache Vorhandensein seiner Netzknoten abzufedern, schrieben Netzpioniere wie John Gilmore auch Demokratie sichernde Fähigkeiten zu. Da das Ganze durch den Ausfall einiger seiner Teile nicht nachhaltig beschädigt werden könne, müssten folglich auch Versuche scheitern, einzelne Inhalte zu zensieren. In der Praxis verfügt das Internet leider nicht durchgehend über ausfallsichere Netzstrukturen. Teilnetze wie das chinesische oder saudi-arabische Internet können daher missliebige Inhalte erfolgreich ausblenden oder entfernen. Auch sorgen standortbezogene Internetdienste mittlerweilen dafür, dass bestimmte Inhalte nur noch in ausgesuchten geografischen Regionen überhaupt zugänglich sind. So war die Webkampagne des US-Präsiden-

ten George W. Bush im Wahlkampf 2004 nur für US-Wähler erreichbar [@1]. Internettechnik per se kann keine demokratischen Verhältnisse einführen. Gleichwohl erleichtert und beschleunigt sie den Informationsaustausch zwischen Menschen enorm. Damit prägt sie auch entsprechende Erwartungen und Ansprüche. Wenn ein Bürger etwa Informationen von einer ausländischen Behörde schneller erhalten kann als von einer inländischen, werden deren Arbeitsweise und -prinzipien über kurz oder lang hinterfragt werden. Als deutsche Bürger merkten, dass in anderen Ländern nicht das Prinzip des Amtsgeheimnisses, sondern das der Informationsfreiheit die Politik der Behörden bestimmt, begannen sie diese auch für deutsche Institutionen einzufordern. Inzwischen haben in Deutschland vier Bundesländer die Informationsfreiheit eingeführt, auf Bundesebene steht dank hartnäckiger Lobbyarbeit seitens Journalistenvereinigungen und Verlagen ein entsprechendes Gesetz vor seiner Verabschiedung.

Über das Internet werden auch andere Wertvorstellungen vermittelt. Vor allem das Grundrecht auf Meinungsfreiheit erhielt unter dem Eindruck der nahezu absoluten Meinungsfreiheit, die die US-Verfassung garantiert, eine gewisse Aufwertung (Schulzki-Haddouti 2003). So kritisierten Internet-Nutzer staatliche Bestrebungen, Prinzipien des Jugendschutzes im Internet durchzusetzen, mit dem Verweis auf die Meinungs- und Informationsfreiheit. Jugendschützer hatten dafür plädiert, Schutzmechanismen einzuführen, die analog wie im Fernsehen und Radio mit zeitlichen Begrenzungen oder speziellen Zugangscodes für nichtjugendfreie Angebote funktionieren sollten. Auch erwogen sie, Internet-Provider zur Installation von Filtern gesetzlich zu verpflichten. Letztlich setzte man zu Gunsten der technischen Beherrschbarkeit auf die freiwillige Kooperation aller Beteiligten: Wer Kinder und Jugendliche schützen will, muss entsprechende Software bzw. Browsereinstellungen aktivieren. Mit diesem Kompromiss setzte sich eine wenig regulative Lösung durch. Gleichwohl herrscht noch immer eine ähnlich gelagerte Auseinandersetzung mit gesetzeswidrigen Inhalten: So bleiben etwa rechtsradikale Publikationen, die illegale, weil volksverhetzende Symbole verwenden, in Deutschland verboten, während sie über US-amerikanische und kanadische Websites verfügbar sind. Deutsche Provider müssen deshalb den Zugang zu solchen Sites sperren, wenn es ihnen »technisch möglich und zumutbar« ist. Als die Bezirksregierung Düsseldorf plante, Tausende ausländische Internetseiten zu sperren, wurde sie allerdings wegen der damit verbundenen Einschränkung der Informationsfreiheit kritisiert [@2].

Gefährdete Bildungsfreiheit

Aber nicht nur staatliche Eingriffe können Informationsfreiheit einschränken. Durch die Internationalisierung des Rechts und Digitalisierung des Wissens werden Urheber zunehmend weniger, die Vermarktung durch die Verlage immer mehr geschützt. In Brüssel beschäftigt sich die Europäische Kommission seit Sommer 2004 mit einer Beschwerde des Börsenvereins des Deutschen Buchhandels gegen den wissenschaftlichen Dokumentenlieferdienst Subito. Der vom Bundesforschungsministerium und den Bibliotheken ins Leben gerufene Dienst stellt per E-Mail Kopien von Zeitschriften gegen rund fünf Euro zur Verfügung, Wissenschaftsverlage verlangen für die gleichen Veröffentlichungen im Schnitt 33 Euro. Die Verlage geben an, dass ihnen durch Subito in den letzten sechs Jahren 113 Millionen Euro Umsatz entgangen seien. Dies führe, so die Verlage in ihrer Beschwerde, »unweigerlich weltweit zu einer Erhöhung der jährlichen Abonnementpreise« und müsse daher gestoppt werden. Gleichwohl betreibt der Verlegerverband *International Association of STM Publishers* eine gezielte Preiserhöhungspolitik: So stiegen in den letzten zehn Jahren die Abonnementpreise für Zeitschriften des größten naturwissenschaftlich orientierten Verlags, dem Elsevier-Verlag, zwischen 85 und 560 Prozent. Marktbeherrschende Verlage wie Springer und Riley werben bei ihren Shareholdern mit Renditen bis zu 40 Prozent.

Musterprozesse und Beschwerden sind der jüngste Höhepunkt eines erbittert geführten Feldzugs der großen internationalen Verlage gegen die Verbreitung digitaler Kopien. Im Bundesjustizministerium, das im Herbst 2004 die zweite Stufe der Urheberrechtsreform vorstellte, fanden die Verlagslobbyisten Gehör – zum großen Entsetzen der Vertreter von Bildung und Wissenschaft. Bildungs- und Forschungseinrichtungen müssen sich mit Brosamen begnügen: Wenn ein Verlag den Beitrag nicht selbst vertreibt, soll der Versand von Kopien nur noch per Post und Fax oder digital in einem nicht durchsuchbaren Grafik-Format legal sein. Außerdem sollen Bibliotheken an Bildschirmen nur so viele Exemplare digital zugänglich machen dürfen, wie im Papierbestand vorhanden sind. Denn nur dort, wo keine technischen Schutzmaßnahmen eingesetzt werden, bleibt die Privatkopie nach dem neuen Gesetz zulässig.

Angesichts der zunehmenden Digitalisierung kommt dies einem gewaltigen Einschnitt in die Informations- und Bildungsfreiheit gleich. Dabei liegt der Sinn von Wissenschaft darin, dass man Wissen erzeugt und es anderen mitteilt. Ähnlich wie Softwareentwickler mit Linux auf das Microsoft-Monopol reagierten, setzen die Wissenschaftler nun auf »Open Access«. Sie veröffentlichen ihre Beiträge auf einer wachsenden Anzahl hochschuleigener Server. Das Konzept des »Open Access« geht zu-

rück auf den Engländer Steven Harnad, der 1994 den Vorschlag unterbreitete, das traditionelle Peer-Review-Publishing über eine über das Internet kostenlose Verbreitung und ein nachträgliches Begutachtungsverfahren zu revolutionieren. Inzwischen gibt es allein in der Physik 75 kostenlose Open-Access-Zeitschriften. Der Anreiz für die Wissenschaftler liegt in der höheren Aufmerksamkeit, die die Online-Dokumente erfahren: Dokumente, die online verfügbar sind, werden bis zu zehnmal öfter von Kollegen zitiert als Dokumente, die nur in Papierform vorliegen. Der weltweit operierende Wissenschaftsverlag Springer hat die laufende Debatte um »Open Access« auf seine Weise aufgegriffen: Autoren bezahlen im so genannten »Open-Choice-Modell« 3000 Dollar, wenn ihr Beitrag parallel zur Printausgabe kostenlos im Internet zugänglich sein soll. Eine vom Medizin-Nobelpreisträger Harold Varmus gegründete medizinische Open-Access-Zeitschrift verlangt für einen Beitrag immerhin nur 1500 Dollar.

Ob und wie Informationen fließen dürfen, ist von fundamentaler Bedeutung für die Wissensgesellschaft. Ob Informationen frei verfügbar, verkäuflich oder gar geheim gehalten werden, bestimmt das Gefüge der Gesellschaft. Regulierungsmechanismen sind Machtmechanismen. Doch wie das Gemeingut Wissen geschützt und gepflegt werden kann, ist immer noch eine weitgehend offene Frage. Eine Maßnahme könnte darin bestehen, nicht nur Bibliotheken, sondern auch Museen und Archive für die Archivierung und Zugänglichmachung von digitalem Wissen zu erweitern. Ein anderes Gegenmittel besteht im Selbermachen: Freie Software, freie Enzyklopädien, frei zugängliche Systeme, freie Datei-Sharing-Systeme, quelloffene Content-Management-Systeme. [@3]

Kryptografie soll Privatheit schützen

Schon der Chaos Computer Club verschrieb sich sowohl der Informationsfreiheit wie dem Datenschutz mit seinem Grundsatz »Öffentliche Daten nützen, private Daten schützen«. Demokratie kann ohne Informationsfreiheit und ohne Transparenz nicht funktionieren. Ebenso sehr sind Menschen in einer Demokratie auf Privatheit, ja auf die so genannte »informationelle Selbstbestimmung« angewiesen. So stellte das Bundesverfassungsgericht 1983 in seinem Volkszählungsurteil fest:

»Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, dass etwa die Teilnahme an einer Versammlung oder einer

Bürgerinitiative behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8,9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.«

Privatheit ist also eine Grundbedingung demokratischen Handelns und damit ein schützenswertes Grundrecht. Unter dem Primat der Meinungsfreiheit wurde in den USA in den 90er Jahren die Diskussion um die Verfügbarkeit von Verschlüsselungstechniken geführt. Hierzulande wurde die Kryptofrage eher unter dem Aspekt des Fernmelde- und Betriebsgeheimnisses diskutiert, denn mit Hilfe von Verschlüsselungstechniken können Nutzer die Inhalte ihrer Kommunikation geheim halten – und damit vor Dritten schützen. Es geht hier also weniger um ein Mehr an Transparenz, sondern um ein Mehr an Privatheit. Im Zentrum der Auseinandersetzungen stand die von dem Amerikaner Phil Zimmerman entwickelte Verschlüsselungssoftware *Pretty Good Privacy*, kurz PGP. Sie beruht auf einem asymmetrischen Verschlüsselungssystem, das US-Wissenschaftler schon in den 70er Jahren entwickelt hatten, um das Problem des sicheren Schlüsselaustausches in Computernetzen zu lösen.

Kryptografisches Wissen war allerdings lange Zeit die Domäne staatlicher Sicherheitsbehörden. Eingesetzt wurden und werden Verschlüsselungstechniken etwa von Diplomaten im Ausland, um Botschaften gesichert ins Heimatland zu überbringen, aber auch vom Militär, das seine Pläne vor der Kenntnisnahme durch den Gegner schützen will. Mit dem preiswerten und allgemein verfügbaren PGP drohte das staatliche Hoheitswissen um die Verschlüsselungskunst an Bürger und Unternehmen weitergegeben zu werden, die sich ihrerseits damit gegen private und staatliche Abhörversuche schützen konnten. Deshalb versuchte die US-Regierung von Anfang an die Entwicklung und später den Export asymmetrischer Verschlüsselungssysteme zu reglementieren. Kryptografische Systeme wurden beispielsweise als Waffen eingestuft, um ihren Export einschränken zu können. Deutsche Behörden verwiesen wiederum auf ihre gesetzlich verbrieften Rechte, in besonderen Fällen Abhörmaßnahmen durchführen zu dürfen. Eine Verschlüsselung von Telefongesprächen würde dieses Recht jedoch erheblich behindern, ein beschränkter Zugang zu dieser Technik wäre daher sinnvoll.

Als Ende der 90er Jahre immer mehr Hinweise auf Wirtschaftsspionage unter befreundeten Staaten publik wurden, erwies sich diese Argumentaion als wenig hilfreich. Die Recherchen des neuseeländischen

Friedensaktivisten Nicky Hager und des britischen Autors Duncan Campbell hatten die Existenz eines globalen, satellitengestützten Abhörnetzwerkes enthüllt, das Staaten wie Großbritannien, Australien, Neuseeland und Kanada unter der Führung der USA seit Ende des 2. Weltkrieges aufgebaut hatten. Wie später ein Untersuchungsausschuss des Europäischen Parlaments bestätigte, wurde das System nicht nur zur militärischen Aufklärung, sondern auch zum Gewinn wirtschaftlich relevanter Informationen verwendet. Der einzige Schutz der Wirtschaftsunternehmen vor diesen Lauschangriffen bestand im Schutz ihrer Kommunikation – mittels Verschlüsselung. Eine wie auch immer staatlich regulierte Kryptotechnik würde jedoch nie das uneingeschränkte Vertrauen der Unternehmen genießen können. Die deutsche Regierung entschloss sich daher 1999 unter dem argumentativen Druck von Cyberrights-Gruppen und Wirtschaftsverbänden in ihren Kryptoeckpunkten zu einer liberalen Handhabung. Sie bekräftigte ihre Haltung wenig später mit der Entscheidung, die Weiterentwicklung von GnuPG, der Open-Source-Variante von PGP, zu unterstützen und eigene, hardwaregestützte Kryptoprodukte zu entwickeln. Vor allem die Entscheidung, eine Open-Source-Variante eines mächtigen Verschlüsselungssystems zu fördern, zeigte der US-Regierung deutlich, dass ihre restriktive Exportpolitik nicht länger erfolgreich sein konnte. Kurz darauf lockerte sie ihre Restriktionen beträchtlich.

Vom Ende der Anonymität

Mit den Terroranschlägen vom 11. September 2001 wurde diese liberale Politik zwar nicht offiziell rückgängig gemacht, doch andere, nicht weniger wichtige Entwicklungen begannen eine wichtige Rolle zu spielen. Die Empfehlungen des Echelon-Untersuchungsausschusses zeigten in der europäischen Politik keine spürbare Wirkung. Die Entwicklung von kryptografischen Techniken und deren Einsatz in Unternehmen wurde nicht, wie gefordert, aktiv weiterbetrieben. Das Bundeswirtschaftsministerium fror nach wenigen Jahren die Unterstützung der Entwicklung von GnuPG ein, deutsche Kryptohersteller gerieten im Zuge der Weltwirtschaftskrise stark unter Druck. 2004 wurden sogar die ersten Stimmen aus der Politik vernehmbar, die erneut eine Regulierung von Kryptografie forderten – bislang allerdings ohne Erfolg. Denn mit PGP und GnuPG stehen Bürgern wie Kriminellen längst mächtige Werkzeuge zur Verfügung. Die Entwicklung kann vorerst nicht mehr gestoppt werden. Auch gab und gibt es keine begründeten Klagen von Strafverfolgern, dass Verschlüsselungstechnik ihre Ermittlungen erschweren würde.

Polizei und Geheimdienste setzen auf andere Aufklärungsinstrumente, die aus bürgerrechtlicher Sicht jedoch nicht weniger bedenklich sind. Jeder Kommunikationsteilnehmer erzeugt digitale Spuren – dies ist bereits seit der Entwicklung von ISDN in den 80er Jahren bekannt. Angerufene können anhand der Nummer des Anrufenden erkennen, mit wem sie es zu tun haben. Internet-Provider wissen anhand der Nummer, welcher Kunde im Netz ist und was er dort macht. Strafverfolger können mit Hilfe dieser Verbindungsdaten herausfinden, wer mit wem in Kontakt steht und auf diese Weise Beziehungsgeflechte ausforschen. Anhand standortbezogener Verbindungsdaten, wie sie GSM-Handys oder auch GPS-Sender regelmäßig generieren, können sie auch Bewegungen von Personen mit Hilfe von digitalen Geoinformationssystemen aufzeichnen. Die Auswertung der Verbindungsdaten kann so wertvolle Hinweise darauf geben, ob eine Person verdächtig ist oder nicht. Mittels mächtiger Data-Miningsysteme können Strafverfolger diese großen Datenmengen intelligent auswerten. Die rechtlichen Hürden hierfür liegen sehr niedrig.

Nachdem der US-Präsident im Herbst 2001 seine europäischen Amtskollegen aufgefordert hatte, die Speicherung von Verbindungsdaten zwingend vorzuschreiben, wurde in der Europäischen Union eine Debatte befeuert, die bis heute nicht beendet ist. Die allermeisten Mitgliedstaaten sind davon überzeugt, dass eine Speicherung von Verbindungsdaten sinnvoll ist. Inzwischen spricht sich nur mehr Deutschland gegen eine Zwangsspeicherung aus. Zwar setzten Datenschützer im deutschen Recht durch, dass diese Daten grundsätzlich nicht gespeichert werden müssen. Falls dies aber doch zu Abrechnungszwecken nötig sei, in gekürzter Form. Dies galt allerdings nur bis Sommer 2004. Seit der Novelle des Telekommunikationsgesetzes werden die Nummern grundsätzlich in voller Länge gespeichert – außer der Kunde wünscht es anders. Dies soll nicht zuletzt die Strafverfolger bei der Identifizierung von Kommunikationsteilnehmern unterstützen.

Datenschutz in der Telekommunikation wird damit zu einem Recht, das aber nicht selbstverständlich gewährt wird, sondern das Nutzer ausdrücklich einfordern müssen. So wie der Schutz des Fernmeldegeheimnisses für E-Mail nur dann existiert, wenn Nutzer ihre E-Mails selbst verschlüsseln. Auch kann sich ein Internet-Surfer nur dann anonym im Netz bewegen, wenn er einen Anonymisierungsdienst nutzt. All diese Selbstschutz-Werkzeuge sind allerdings noch nicht so gestaltet, dass sie jeder Nutzer verwenden könnte. Sie setzen ein gewisses Maß an technischem Verständnis voraus – und bleiben damit denjenigen praktisch vorenthalten, die das Internet nutzen möchten, ohne viel davon zu verstehen. Erst wenn die Nutzung dieser datenschutzunterstützenden Werk-

zeuge sehr einfach wird, wird auch der von ihnen gewährte Schutz selbstverständlich.

Von entscheidender Bedeutung scheint deshalb heute die Entwicklung der Web-Services zu sein. Diese Dienste, die die nahtlose Nutzung mehrerer, vorwiegend kommerzieller Internetdienste ermöglichen, werden erst dann breit genutzt, wenn sie das so genannte Identitätsmanagement in den Griff bekommen. Erst wenn das System weiß, mit wem es zu tun hat, wird es für seine Betreiber verwendbar. Doch die Identität des Nutzers kann auch pseudonym oder anonym sein. Nicht in jedem Fall ist die Offenlegung der wahren Identität nötig. Die Anforderung des Datenschutzes, mit personenbezogenen Daten sparsam und zweckgebunden umzugehen, sollte möglichst frühzeitig, noch in der Entwicklungs- und Standardisierungsphase umgesetzt werden, um die informationelle Selbstbestimmung nachhaltig im Internet zu verankern. Doch Unternehmen denken bei der technischen Ausgestaltung solcher Systeme nicht immer an den Datenschutz, obgleich er die Akzeptanz bei den Nutzern wesentlich steigern könnte. Datenschützer und Bürgerrechtler müssen sich daher in diese Entwicklungsarbeit aktiv einbringen und vor Ort in den Gremien ihre Standpunkte darlegen.

Gelingen kann eine datenschutzfreundliche Technikgestaltung nur, wenn Diskussions- und Gestaltungsprozesse offen und transparent sind. Doch gerade in sicherheitsrelevanten Bereichen ist dies selten der Fall. Bis heute sind Datenschützer weder in den internationalen Gremien zur Entwicklung abhörfähiger Telekommunikation, noch in den Gremien zur Standardisierung biometrischer Reisepässe vertreten. Da ein offener Austausch von Ideen und Ansichten so nicht stattfinden kann, ist zu bezweifeln, dass die auf diese Weise entstehende Technik überhaupt gesellschaftlich legitimiert ist. Gleichwohl gedeiht die verführerische Kraft des technisch Machbaren besonders gut in einer Atmosphäre der Angst, wie sie seit dem 11.9.2001 gepflegt wird. Grundrechte lassen sich in solcher Atmosphäre nur mühsam vermitteln und durchsetzen.

Hightech als gesellschaftlicher Machtfaktor

Besonders attraktiv für Sicherheitspolitiker und Strafverfolger ist derzeit die Idee der Prävention: Mit Hilfe von Hightech sollen Straftaten und Verbrechen verhindert werden, bevor sie geschehen. Um die Absicht eines potenziellen Täters zu erkennen, wollen Strafverfolger möglichst frühzeitig so viele Daten wie möglich auswerten können. Nicht zuletzt der »11. September« hatte gezeigt, dass Sicherheitsbehörden einige Attentäter bei einer gründlichen Datenüberprüfung rechtzeitig aus dem

Verkehr hätten ziehen können. Mit der Ausstattung sämtlicher Reisepässe mit biometrischen Daten sollen potenzielle Attentäter schon bei der Identitätsfeststellung erkannt werden. Bei dieser Art von Prävention spielt der Einsatz von Hightech die Hauptrolle. Er suggeriert, man könne mit seismografischer Genauigkeit eine Art Wetter- und Erdbebenfühligkeit für Terroranschläge entwickeln. In Wahrheit rücken mit dem Ruf nach einer Früherkennung künftiger Gewaltexzesse das Prognostische und das Imaginäre ins Zentrum des politischen Denkens. Man erwartet von denjenigen, die von Staats wegen mit Sicherheitsfragen befasst sind, dass sie sich alle erdenklichen Bedrohungen ausmalen und reagieren, bevor die Gewalt ihren Lauf nimmt (vgl. Schulzki-Haddouti 2004).

Inzwischen sind in der deutschen Politik alle Mittel der Prävention diskussionsfähig – von der Abschiebung von Ausländern, die politisch inkorrekte Äußerungen wagen, über das präventive Abhören bis hin zur Sicherungsverwahrung verdächtiger Mitbürger. Attraktiv scheint das Sammeln personenbezogener Reisedaten bei Fluggesellschaften und die Zusammenführung und Auswertung dieser und anderer Daten in einer gemeinsamen Datenbank von Polizei und Geheimdiensten. Diese Art von Rasterfahndung soll möglichst europaweit durchgesetzt werden. Computersysteme sollen zudem die unterschiedlichsten Bedrohungsszenarien durchexerzieren und die Menschen auf die – imaginären – Schreckensszenarien vorbereiten. Dabei verleihen komplexe Computer- und Visualisierungssysteme den Szenarien Glaubwürdigkeit und den Verfechtern der sicherheitstechnischen Aufrüstung und bürgerrechtlichen Abrüstung die argumentative Munition. Freiheit wird dabei zu einem gesellschaftlichen Gut, das scheinbar nur durch ein Mehr an Sicherheit erreicht werden kann. Datenschützern bleibt oft nur ein Beklagen der Entwicklung, von der Gestaltung sind sie weitgehend ausgeschlossen. Auch eine entsprechende Technikfolgenabschätzung kann der rasanten Entwicklung nur mehr hinterherhinken. Grundrechte drohen so nachhaltig beschädigt zu werden.

Letztlich können nur Transparenz und Dialog unsere Grundrechte wahren. Nur ein funktionierender Interessenausgleich kann Demokratie garantieren. Interessensgruppen in aller Welt können sich mit Hilfe des Internet vernetzen, um Fakten auszutauschen, Hintergründe zu erarbeiten und nationale wie internationale Strategien auszuarbeiten. In dem Maße, wie staatliche Einrichtungen und private Unternehmen die neuen Technologien nutzen, müssen auch Bürger das Medium Internet für ihre Interessen nutzen lernen. Zwar sind die Kräfteverhältnisse hinsichtlich Finanzierung und technischer Infrastruktur denkbar unterschiedlich, doch die gesellschaftliche Entwicklung spricht für die Macht der Bürger: In der demokratischen Wissens- und Informationsgesellschaft wird letzt-

lich der Interessensvertreter mit dem besseren Argument und gesellschaftlichen Nutzen die größere Akzeptanz finden.

Literatur

Christiane Schulzki-Haddouti (Hg.) (2003): *Bürgerrechte im Netz*. Bundeszentrale für politische Bildung.

Christiane Schulzki-Haddouti (2004): *Im Netz der inneren Sicherheit*. Hamburg: Europäische Verlagsanstalt.

Digitale Verweise

[@1] www.georgewbush.com
[@2] www.odem.org/informationsfreiheit
[@3] www.urheberrechtsbuendnis.de