Johann Wolfgang Goethe – Universität
Frankfurt am Main

Fachbereich Rechtswissenschaft
Wiss. Assistent Dr. Johann Bizer
Institut für Öffentliches Recht
Johann Wolfgang Goethe-Universität

Postfach 11 19 32
D-60054 Frankfurt am Main
E-Mail: bizer@jur.uni-frankfurt.de
http://www.jura.uni-frankfurt.de//bizer.html

An den
Deutschen Bundestag
Enquete-Kommission „Globalisierung der Weltgesellschaft“
Herrn Prof. Ulrich von Weizsäcker
Platz der Republik 1
11011 Berlin

Schriftliche Stellungnahme zur Anhörung vor der Enquete-Kommission des Deutschen Bundestages am 10. Dezember 2001 im Berliner Reichstag

e-Demokratie versus Sicherheit in der Wissensgesellschaft

4. Teilhabe am Wissen: Demokratische Repräsentation, Demokratie und Sicherheit in der globalen Wissensgesellschaft

4.1. Welche spezifischen Probleme und auch Chancen ergeben sich aus der wachsenden Relevanz elektronischer Kommunikation für die demokratische, öffentliche wie individuelle Meinungs- und Willensbildung? Welche Folgen ergeben sich insbesondere für den zentralen Begriff der Öffentlichkeit, der individuellen Privatsphäre und des Rechts auf hinreichende Information?

Chancen

IuK-Techniken bieten gegenüber konventionellen Medien der Massenkommunikation mindestens folgende Vorteile:

Individualisierung des Angebots an Informationen. Auf einer *Website* kann jeder als Anbieter selbst Informationen und Meinungen sammeln und darstellen (offene Kommunikation). Daneben bieten Mailinglisten und Newsgroups (auch geschlossene Websiten) die Möglichkeit, an einen definierten Kreis von

Teilnehmern Informationen aktuell und zeitgleich auszusenden (geschlossene Kommunikation).

Interaktion mit den Nutzern. Das *Internet-Medium* bietet die Möglichkeit der unmittelbaren Interaktion über bestimmte Inhalte über das Medium selbst und damit wegen der Reziprozität eine größere Intensität und Dichte der Kommunikation selbst. Aufgrund ihrer Unmittelbarkeit der Reaktionsmöglichkeiten wird interaktive Internetkommunikation häufig auch als authentischer wahrgenommen, was sich wiederum positiv auf die Teilnahme auswirkt.

Aufgrund ihrer Digitalisierung und der angebotenen Bandbreiten (einschließlich Kompressionsverfahren) ermöglicht Internet-Kommunikaton eine ***multimediale*** Darstellung und Aufbereitung von Informationen und Kommunikation, wodurch ihre Attraktivität und Rezeption gegenüber reinen Text oder Tondarstellungen erhöht wird.

Soweit die ***globalen TK-Netze*** reichen, können Internet-Angebote prinzipiell von jedem Standort in der Welt angeboten oder abgerufen werden. Das Internet bietet damit das ideale Medium für einen weltweiten Informationsaustausch zwischen den Bürgern dieser Welt. Zugespitzt formuliert bietet sich das Internet als Medium der Weltbürger an und wird als solches von den akademischen Eliten auch bereits genutzt.

Die beiden genannten Formen medialer Kommunikation erweitern das Verständnis der Öffentlichkeit. *Neben* die veröffentliche Meinung in einem Medium der Massenkommunikation (Rundfunk, Fernsehen, Presse) tritt das individualisierte Informationsangebot zur Kommunikation. Die Möglichkeiten der IuK-Techniken lässt sich als eine Ebene veröffentlichter Individualkommunikation skizzieren, die zwischen Massenkommunikation (Rundfunk, Fernsehen, Presse) und Individualkommunikation tritt. Das Internet wird auf diese Weise zu einer technischen Plattform einer interaktiven Teilöffentlichkeit einer prinzipiell unbegrenzten Zahl von Teilnehmern. Elektronische Kommunikation fördert und erweitert die **Öffentlichkeit** um „virtuelle Räume“ aus Information und Interaktion.

Elektronische Kommunikation bietet gegenüber den konventionellen Medien der Massen- und Individualkommunikation die Chance einer um Inhalte und Interaktion erweiterten individuellen und öffentlichen Meinungsbildung und begünstigt in diesem Sinne die Entwicklung einer gesellschaftlichen Demokratisierung.

Beispiel: Ein anschauliches Beispiel für den Prozess der zunehmenden Nutzung elektronischer Kommunikation für Zwecke der Information, aber auch für „jedermann“ Anhörungen bietet die europäische Kommission, die mit Hilfe des Internet gleichsam eine virtuelle politische Teilhabe elektronischer Unionsbürger entwickelt hat.

Privatanschrift: Max-Planck-Str. 2 * 63454 Hanau * Tel.: 06181 / 234 32 Fax: 06181 / 91 93 74

Implikationen

Allerdings impliziert der Prozess einer zunehmenden Bedeutung elektronischer Kommunikation für Willensbildungsprozesse auch eine Reihe von Implikationen.

Ungehinderter Zugang zu Informationen

Ein Schlüsselbegriff für die Willensbildung über elektronische IuK-Medien ist die Gewährleistung eines ungehinderten Zugangs zu Informationen. Von Bedeutung ist der Zusammenhang von Willensbildung und Informationszugang, weil über die Beherrschung und Monopolisierung von Informationen auf die Prozesse der öffentlichen und individuellen Meinungs- und Willensbildung eine steuernde Wirkung ausgeübt werden kann.

Ein ungehinderter Informationszugang muss gegenüber **Informationen in der Hand des Staates** – unter Wahrung des Schutzes personenbezogener Daten sowie schützenswerter Betriebs- und Geschäftsgeheimnisse – auch gewährleistet sein. Während in Deutschland einige Bundesländer (Brandenburg, Berlin und Schleswig-Holstein und jüngst auch Nordrhein-Westfalen) bereits Informationszugangs- bzw. -freiheitsgesetze erlassen haben, fehlt eine solche Regelung immer noch für den Bund und die überwiegende Zahl der Landes- und Kommunalverwaltungen. Von Bedeutung ist im Zusammenhang mit der elektronischen Willensbildung, dass die ohnehin häufig ohnehin elektronisch verfügbaren Informationsunterlagen nicht lediglich offline, sondern auch online angeboten werden. Eine gewisse Änderung bahnt sich zumindest für die Nutzung öffentlicher Register (Handelsregister, Vereinsregister) an, die nach den letzten Rechtsänderungen im Registerrecht auch online abgerufen werden können sollen.

Von völlig unterschätzter Bedeutung ist die Tendenz, mit Mitteln des **Urheberrechtes** Informationen dem free flow of information zu entziehen. Die für einen ungehinderten Prozess der öffentlichen Meinungsbildung bedrohliche Entwicklung des Urheberrechts kann hier nur an Hand von zwei prominenten Beispielen angedeutet werden. Nach § 5 UrhG sind „Gesetze, Verordnungen, amtliche Erlasse und Bekanntmachungen“ gemeinfrei, das heißt sie genießen keinen urheberrechtlichen Schutz. Eine entsprechende Regelung für die elektronische Fassung amtlicher Dokumente fehlt sowohl im deutschen als auch im europäischen Recht. Bereits heute kann der Nutzer im Internet Gesetzestexte aus dem Bundesgesetzblatt nicht kostenlos ausdrucken, sondern nur gegen Entgelt.

Das zweite Beispiel gilt der **Domestizierung elektronischer Inhalte durch die Inhaber von Urheber- und anderer Nutzungsrechte**. Ohne Frage ist die kommerzielle Verwertung elektronischer Urheberrechte prinzipiell legitim – sie darf aber nicht die Regel, sondern muss insbesondere im Fokus von Meinungs- und Willensbildungsprozesse die Ausnahme darstellen. Ein Beispiel ist der urheberrechtliche Schutz von elektronischen Pressespiegel, deren elektronische Nutzung über § 49 UrhG und die Rechtsprechung einer Rezeption im Prozess der öffentlichen Willensbildung weitgehend entzogen ist. Auf diese Weise wird das elektronische Kommunikationsmedium um eine seiner besonderen Stärken geschwächt, nämlich in ein

elektronisches Dokument Originaltexte, Zitate und Quellen unmittelbar einzubinden und auf diese Weise im Internet „mit Gründen und Nachweisen“ zu argumentieren.

Die Problematik eines durch Urheber- und andere vergleichbare Rechte domestizierten elektronischen Willensbildungsprozesses wird sich für die Bevölkerung in den Staaten der Dritten und Vierten Welt in Zukunft verschärft stellen. Die ökonomische Monopolisierung der Rechte an Informationen droht die Bevölkerung der Dritten und Vierten Welt von der Informationsgesellschaft auszuschließen.

Handlungsempfehlung: In Bund und Ländern sind Informationsfreiheitsgesetze zu verabschieden. Amtliche Dokumente müssen elektronisch für einen kostenlosen Abruf zur Verfügung stehen. Urheber- und vergleichbare Rechte dürfen das Recht auf ungehinderten Informationszugang zur politischen Willensbildung nicht blockieren. Eine kostenlose Grundversorgung an Informationen zur politischen Willensbildung aus elektronischen Datenbanken ist eine staatliche Aufgabe zur Informationsvorsorge und über öffentliche Einrichtungen zu gewährleisten.

Als Bestandteil der Entwicklungshilfe- und Kulturpolitik ist elektronische Selbstdarstellung und Interaktion der Netzbürger in Entwicklungs- und Schwellenländern zu fördern. In internationalen Abkommen ist das Recht auf ungehinderten Informationszugang der Bürger gegenüber ihren Staaten und internationalen Organisationen zu gewährleisten. Der kostenlose Zugang zu den Dokumenten staatlicher und internationaler Organisationen sollte als Menschenrecht verankert werden. Gegenüber einem free flow an Informationen zur politischen Willensbildung sollten die Rechte der Urheber und vergleichbarer Rechteinhaber die Ausnahme sein.

Privatsphäre

Nutzung von Informationsabrufen

Es gehört zu den Eigenschaften der elektronischen Kommunikationangebote im Internet, dass ihre individuelle Nutzung mit Hilfe von zusätzlichen Werkzeugen („tools“) in der Hand des Informationsanbieters („servers“) personenbezogen erhoben werden kann. Zum Einsatz kommen Werkzeuge wie Cookies oder aktive Programme, die der Rechner des Anbieters auf dem Rechner des Nutzers speichert und zur Erhebung von Nutzerinformationen verwendet. In Verbindung mit Anmeldungen, der Vergabe von Kennwörtern und vergleichbaren Mechanismen werden derartige Techniken im E-Commerce vornehmlich verwendet, um Informationen über den Nutzer auch ohne seine ausdrückliche Zustimmung zur besseren Kundenbindung einzusetzen. Entsprechende Mechanismen – vor allem Cookies – werden häufig auch von Online-Anbietern des öffentlichen Bereiches gesetzt.

Privatanschrift: Max-Planck-Str. 2 * 63454 Hanau * Tel.: 06181 / 234 32 Fax: 06181 / 91 93 74

Gegenüber dieser Praxis zeigen repräsentative Umfragen, dass der Datenschutz ***einen sehr hohen Stellenwert*** genießt. Nach einer im Jahr 2001 in Deutschland durchgeführten Umfrage wünschen 53 % der Befragten, dass dem Datenschutz künftig mehr Bedeutung zukommen solle.[1] Hintergrund dieser Erwartungshaltung sind zumindest zum Teil eigene Erfahrungen. Immerhin 29 % der Befragten nahmen an, dass ihre Daten mehrmals (20 %) oder einmal (9 %) missbraucht wurden. Diese Haltung ist keine nationale Besonderheit wie eine Umfrage unter US-Bürgern vom August 2000 zeigt. Danach sind in den USA bspw. 84 % der Einwohner besorgt, wenn Geschäftsleute oder Unbekannte Informationen über sie oder ihre Familie bekommen.[2]

Diese Ergebnisse spiegeln einen ***internationalen Trend*** wieder wie eine internationale Studie mit einem Vergleich zwischen den USA, Großbritannien und Deutschland aus dem Jahr 1999 bereits erkennen lässt.[3] Während die Vertrauenswürdigkeit der Banken in Sachen Datenschutz in den USA (77 %) und Deutschland (70 %) überwiegend positiv bewertet wird, schneidet der Versandhandel in der Bewertung des Datenschutzes deutlich schlechter ab: Nur 45 % der in den USA Befragten sowie 42 % in Großbritannien und Deutschland kommen zu einer positiven Bewertung dieser Anbieter. Geradezu vernichtend lautet das Urteil der Nutzer und Verbraucher über die ***kommerziellen Internetanbieter***: Nur 21 % USA, 13 % Großbritannien und 10 % Deutschland bringen in Sachen Datenschutz den kommerziellen Internetanbieter Vertrauen entgegen.

Dass dieses Misstrauen gegenüber dem Internethandel auf einer durchaus ***realistischen Einschätzung*** des Verhaltens der Anbieter beruht, lässt sich einer Untersuchung der Federal Trade Commission aus dem Jahr 2000 entnehmen.[4] Untersucht wurde bspw., in welchem Unfang es selbst bedeutende Dienstanbieter zulassen, dass Dritte Cookies auf dem Rechner ihres Nutzers setzen können. Dabei handelt handelt es sich um eine besonders raffinierte Erhebungstechnik im Internet, um Informationen über das Nutzerverhalten nicht nur dem Anbieter zur Verfügung zu stellen, den der Nutzer besucht hat, sondern auch Dritten, von denen der Nutzer praktisch keine Kenntnis hat und mit denen er auch nicht willentlich in Kontakt treten will.[5] Untersucht wurde das Verhalten von Web-Anbietern mit über 39.000 Besuchern im Monat (visitors each month) unterteilt nach einer Gruppe der 100 populärsten Seiten und einer nach dem Zufallsprinzip zusammengestellten Vergleichsgruppe. Das Ergebnis: 57 % der

---

[1] Opaschowski, Der gläserne Konsument, B.A.T Forschungsinstitut 2001; ders. DuD 11/2001, 678 ff.

[2] 59 % very bzw. 25 % somewhat concerned. The Pew Internet & American Life Project, Trust and privacy online. Why americans want to rewrite the rules, August 2000, pg 25 Question 3.

[3] IBM Multi-National Consumer Privacy Survey, October 1999. pg 24.

[4] Ftc, Privacy Online: Fair Information Practices in the Electronic Marketplace. A Report to Congress, May 2000.

[5] Bizer, Web-Cookies – datenschutzrechtlich, DuD 1998, 277-281.

zufällig ausgesuchten Anbieter ließen Cookies Dritter zu, aber nur 78 % dieser Anbieter haben ihre Nutzer darüber auch unterrichteten. Unter den Top Anbietern ließen sogar 78 % Cookies Dritter zu, wovon die Hälfte (49 %) ihre Nutzer – gleichwie in welcher Form und an welchem Ort – *nicht* in Kenntnis gesetzt wurden.

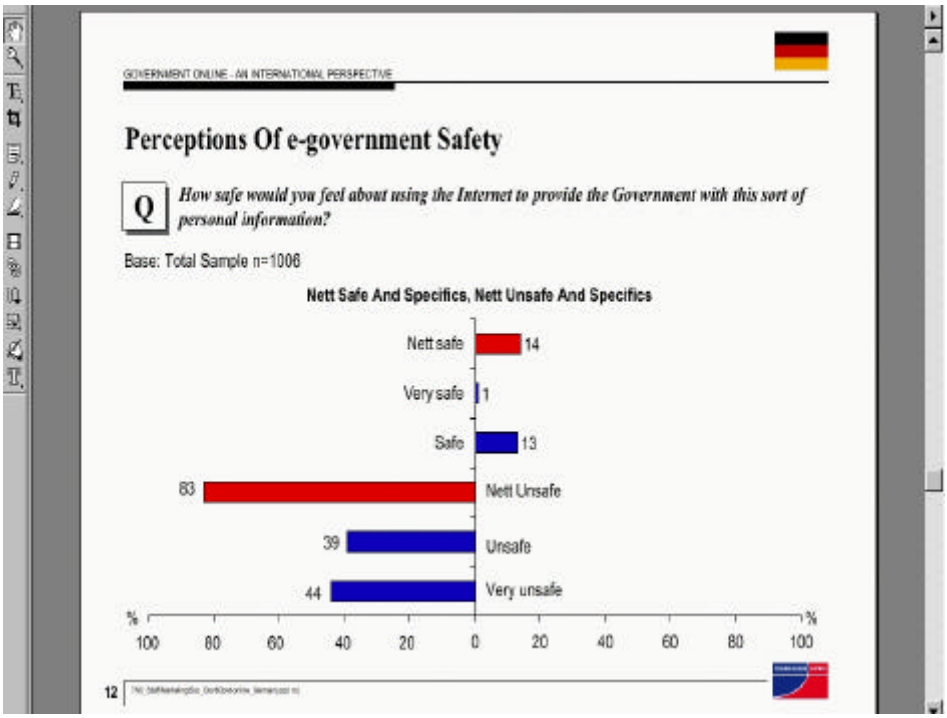
Die Zustimmung zum und die Erwartung an den Datenschutz sind im nicht-öffentlichen Bereich vor allem auch deswegen von Bedeutung, weil ein deutlicher ***Zusammenhang zwischen*** der Einschätzung des ***Datenschutzes*** einerseits und dem ***Kaufverhalten*** andererseits nachgewiesen werden kann. Datenschutz ist ein Akzeptanzfaktor für die Entwicklung von Märkten. Bereits die IBM–Studie aus dem Jahr 1999 belegt einen Zusammenhang zwischen dem Vertrauen der Kunden in den Datenschutz eines Anbieters und seinem Kaufverhalten. In der ***Offline-Welt*** zeigte sich, dass 54 % in den USA, 32 % in Großbritannien und 35 % in Deutschland wegen fehlender Sicherheit über die Verwendung ihrer Daten auf die Nutzung oder den Kauf eines Angebots verzichtetet hatten. Bei den kommerziellen ***Internetanbietern*** zeigte sich eine noch stärkere Angleichung im internationalen Vergleich, nämlich 57 % in USA, 41 % in Großbritannien und 56 % in Deutschland.[6] Dass dieses Ergebnis keine Eintagsfliege ist, beweist eine Umfrage vom Oktober 2000 der Mannheimer Forschungsgruppe Wahlen im Auftrag des Bundesverbandes der Banken. Danach erklärten 62 % der Internetnutzer in Deutschland, sie hätten im Internet noch nicht online bestellt oder gekauft, weil ihrer Meinung nach der Datenschutz unzureichend gewährleistet sei. Zu vergleichbaren Ergebnissen kommt die Opaschowski-Studie[7] im Jahr 2001 für den Internethandel: Nur 23 % gehen davon aus, dass ihre Daten bei der Nutung im Internet hinreichend geschützt sind und halten eine Nutzung für unbedenklich. Hingegen gaben 46 % an, wegen Mängeln bei Datenschutz und Datensicherheit das Internet nicht zu nutzen. Noch 26 % sahen sich nicht in der Lage, zu dieser Frage Stellung zu beziehen („weiß nicht"). 5 % war diese Frage „egal".

Vergleichbar differenzierte Umfrageergebnisse für die *Nutzung von E-Government-Anwendungen* liegen nicht vor. Dass aber gleichwohl die Nutzer hinsichtlich der Verwendung ihrer personenbezogenen Daten in E-Government Anwendungen erhebliches Misstrauen aufbringen, zeigt die folgende Untersuchung: 83 % der Deutschen sind der Ansicht, der Regierung personenbezogene Daten über Internetanwendungen zu verschaffen, sei unsicher – nur 14 % halten es für sicher.

---

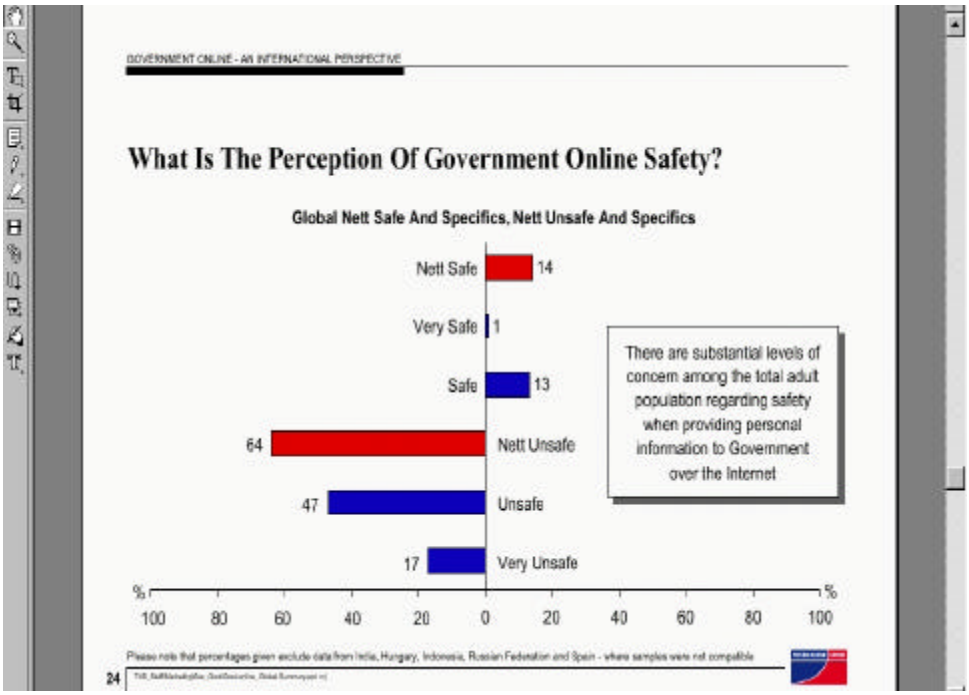
[6] IBM 1999 (Fn. 3), pg. 23, 27.

[7] Opaschowski 2001 (Fn. 1) = DuD 11/2001,

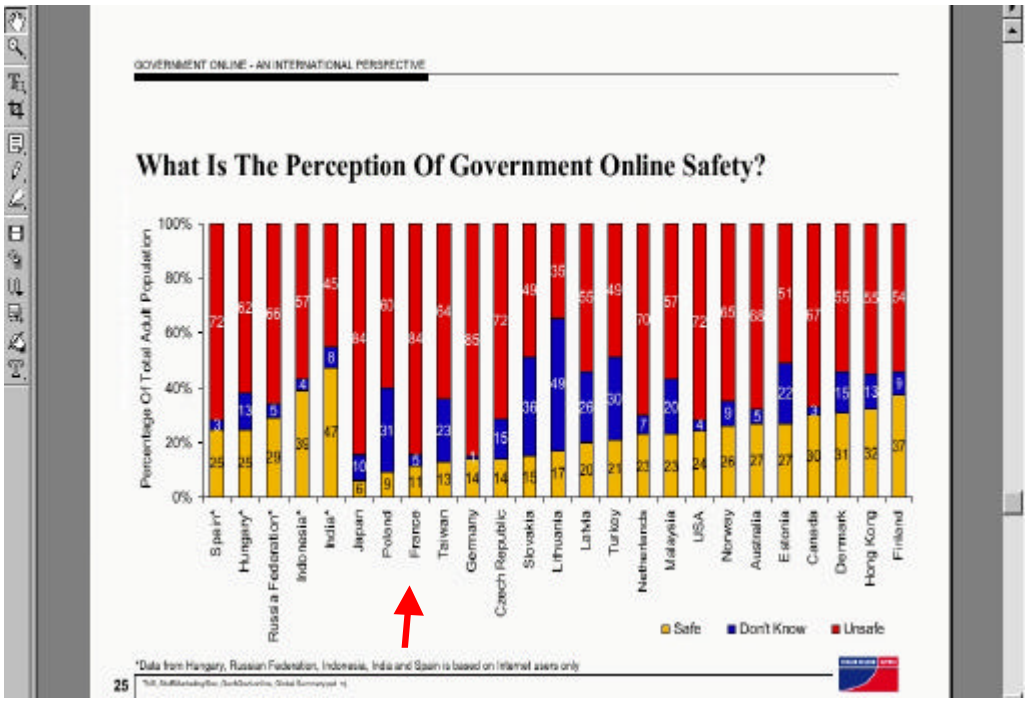


NFO im Auftrag BMWi 1

Im internationalen Vergleich liegt Deutschland zwar mit diesem hohen Anteil über dem Durchschnitt – jedoch zeigt die übernächste Abbildung, dass in so wichtigen Staaten wie Frankreich und Japan eine ähnliche hohe Rate des Misstrauens besteht, die nicht ohne Bedeutung bleiben kann.



NFO im Auftrag BMWi 2



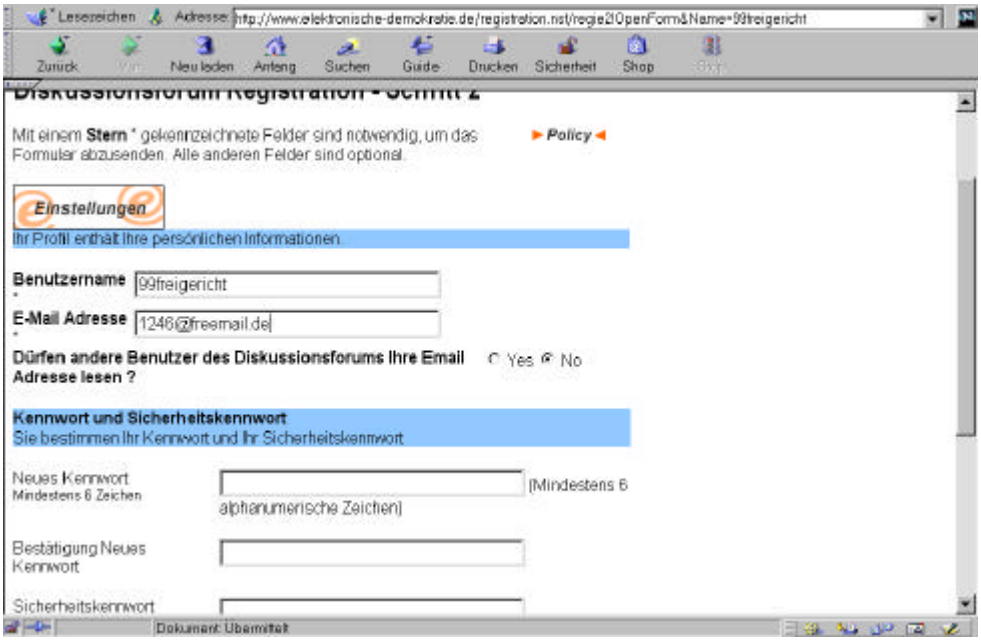
NFO im Auftrag BMWi 3

Schlussfolgerung: Die Werte liefern den empirischen Beleg für den hohen Stellenwert einer anonymen – bzw. als milderes Mittel – pseudonymen Nutzung von Informationsangeboten im Internet. Vor dem Hintergrund der genannten Untersuchungen liegt die Schlussfolgerung nahe, dass die Bürger Informationsangeboten, deren Nutzung Rückschlüsse auf ihre politische Haltung vermitteln könnten und die offen oder verdeckt ohne jede weitere Rechtfertigung Nutzungsdaten erheben werden, mit größter Zurückhaltung begegnet wird. Dies gilt für Informationsangebote politischer Parteien ebenso wie für die Angebote elektronischer Medien und Datenbanken. Nicht nur wegen ihrer fehlenden öffentlichen Transparenz, sondern auch unter dem Gesichtspunkt der Nutzerakzeptanz ist die im Entwurf des Terrorismusbekämpfungsgesetzes in § 8 Abs. 8 E-BVerfSchG enthaltene Regelung, wonach das Bundesamt für Verfassungsschutz unter näher bestimmten Voraussetzungen von den Anbietern die Auskünfte über Teledienstnutzungsdaten verlangen kann, eine höchst problematische Regelung. Sie ist dies im übrigen auch in Hinblick auf die Risiken, die sich für die Nutzer aus einer Übermittlung an Nachrichtendiensten in Drittstaaten ergeben können.

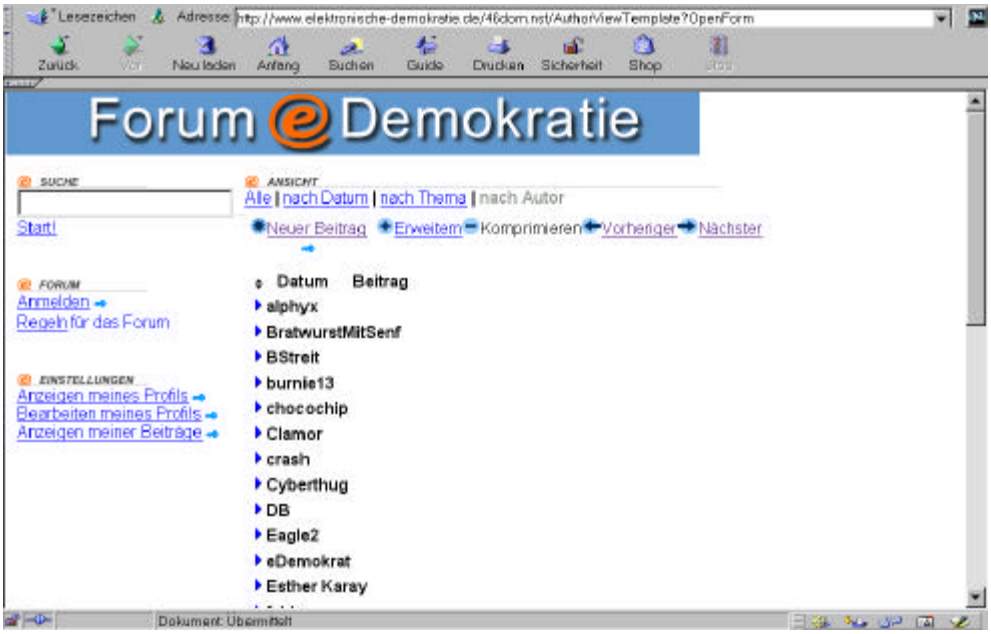
Nutzung interaktiver Medien

Die Tendenz zur Anonymität und Pseudonymität hat im übrigen auch für die Akzeptanz der Nutzung interaktiver Medien eine überragende Rolle. Insbesondere in öffentlichen Foren politischer Parteien und Vereinigungen sowie öffentlicher Medienangebote äußert sich der überwiegende Teil der Nutzer unter einem selbstgewählten Namen anonym bzw. unter Pseudonym. Soweit die Anbieter eine Registrierung für die Teilnahme in dem öffentlichen Forum voraussetzen, können die Teilnehmer sich für die Nutzung im Forum ein Pseudonym zulegen, unter dem sie sich dann öffentlich äußern können. Im Form http://www.elektronische-demokratie.de/ des Deutschen Bundestages haben sich bspw. über 70 % der registrierten

Teilnehmer ein Pseudonym für die Mitwirkung im öffentlichen Forum zugelegt. Teilweise agieren die Teilnehmer auch unter pseudonymen Email-Adressen („123@freemail.de“).



www.elektronische-demokratie.de 1



www.elektronische-demokratie.de 2

Das Handeln im Internet unter einem Pseudonym ist ein fester Bestandteil der Kommunikationskultur des Internet. In der Regel konzentriert sich die öffentliche Debatte in der politisch orientieren Internetkommunikation zwischen Personen unter Pseudonym auf die Qualität der geäußerten Meinung. Mangels personenbezogener Fixierung kann die Bewertung eines Beitrages nicht vom Status einer bestimmten Person abhängig gemacht werden. Die

Verwendung eines Pseudonyms versteht sich als eine angemessene Reaktion der Teilnehmer, auf eine für sie völlig unübersichtliche Zahl von Lesern. Anstatt auf seine Meinungsäußerung zu verzichten, äußert sich der Internetnutzer mit Hilfe einer Selbstschutzmaßnahme und nimmt auf diese Weise am Prozess der öffentlichen und individuellen Meinungs- und Willensbildung teil.

Befürchtungen die Nutzer würden unter der „Tarnkappe“ ihres Pseudonyms verbal „über die Stränge schlagen“ oder das Forum für ihre privaten Zwecke missbrauchen, erweisen sich meist als völlig unbegründet. Ausnahmen wird im Zweifel dadurch begegnet, dass der inkriminierte Beitrag vom Moderator oder Veranstalter nachträglich gelöscht wird und dem Teilnehmer die Zulassung zum Forum entzogen wird.

Handlungsempfehlung: Informationsangebote zur politischen Willensbildung sollten auf die Erhebung personenbezogener Daten verzichten. Das Setzen von Cookies und die Verwendung aktiver Programme zur verdeckten Erhebung personenbezogener Daten sollte von den Informationsanbietern unterlassen werden.

Interaktive Internetkommunikation setzt die Möglichkeit zur Äußerung unter Pseudonym voraus. Öffentliche Foren zur politischen Willensbildung sollten die Verwendung von Pseudonymen zulassen.

Nationale Leitfäden wie das in der Entwicklung befindliche E-Government Handbuch des Bundesamtes für die Sicherheit in der Informationstechnik sollten sich ihre Empfehlungen an den Zielen der Datensparsamkeit sowie dem Grundsatz der anonymen und pseudonymen Nutzung orientieren. Entsprechende Empfehlungen sind in die internationale Aktivitäten bspw. der EU und der OECD aufzunehmen.

4.2. Welche neuen Formen gesellschaftlich relevanter politischer Kommunikation werden sich herausbilden und welche Folgen ergeben sich daraus für die politisch Willensbildung und das politische System sowie für deren Akteure und Institutionen? Welche Entwicklungsmöglichkeiten bietet die Wissens- und Informationsgesellschaft für die parlamentarische Demokratie?

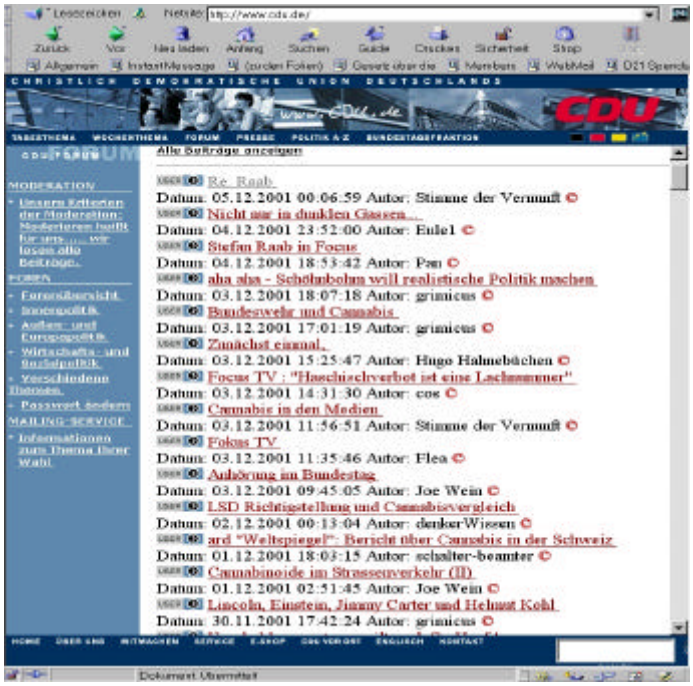
Neue Formen der politischen Kommunikation

Bereits heute zeichnet sich das Bild fragmentierter interaktiver Teilöffentlichkeiten, die ergänzend neben die Medien der Massenkommunikation treten und in denen Bürger jenseits einer für die Inhalte verantwortlichen Redaktion Informationen und Meinungen austauschen. Die interaktiven Formen intensivieren die politische Kommunikation, denn sie ermöglichen eine unmittelbare Form des Austausches, der wegen seiner Öffentlichkeit transparent und nachvollziehbar für andere Nutzer bleibt.

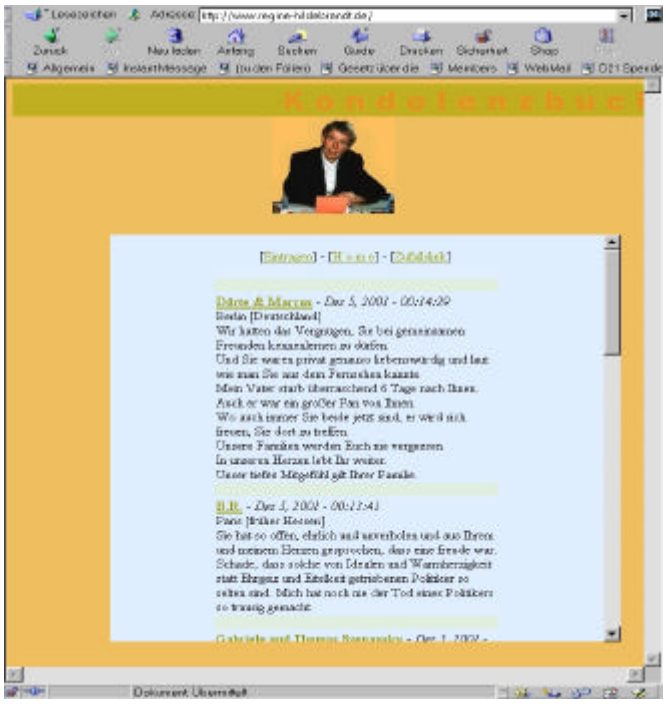
Die neuen Formen der politischen Kommunikation werden teilweise durch die Institutionen der parlamentarischen Demokratie organisiert – überwiegend werden sie aber schon heute jenseits dieser Institutionen durch Medien der Massenkommunikation oder durch Bürgervereine (NGO) als autonome Form der politischen Willensbildung initiiert und ermöglicht.

Das Internet wird bereits von allen politischen Parteien, Ministerien sowie zahlreichen Behörden und Kommunen zur Selbstdarstellung und Information genutzt. Die Strategien orientieren sich weitgehend an den für Zwecke des E-Commerce entwickelten Instrumenten der Kundenbindung. Den Nutzer werden Grundinformationen angeboten, deren Vertiefung oder Aktualisierung gegen Hinterlegung einer Email-Adresse bspw. über das Abonnement eines elektronischen Newsletters oder die Angabe seiner postalischen Adresse möglich ist.

Die interessanteste Entwicklung vollzieht sich derzeit auf der Ebene der Interaktion. Einige Parteien und Fraktionen bieten die Möglichkeit, sich in Foren zu gestellten oder selbstgewählten Themen zu äußern.



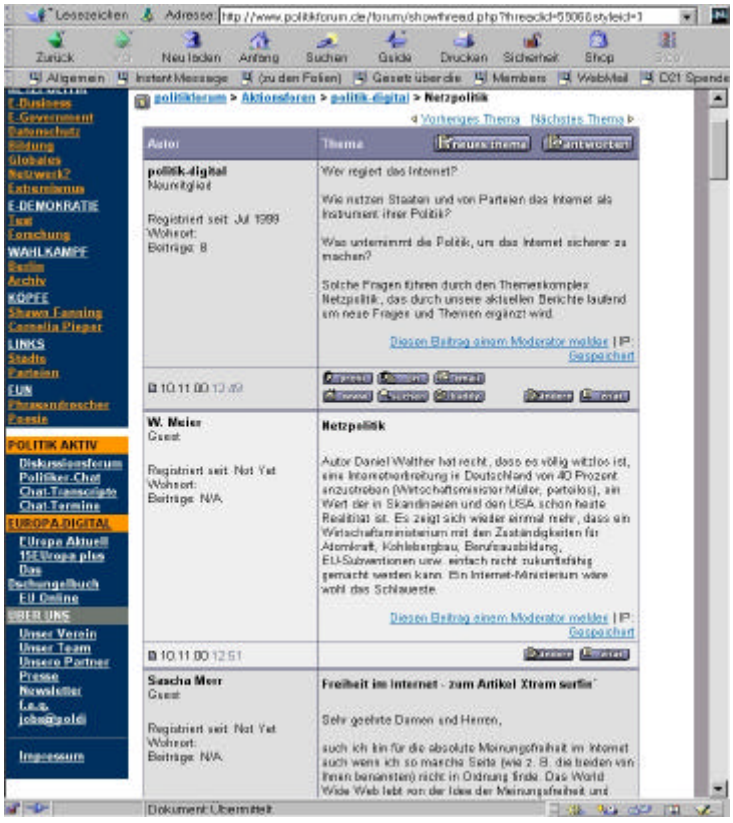
Forum der CDU 1



SPD Trauer um Regine Hildebrandt 1

Neben dieser Mitwirkung an der politischen Willensbildung der Parteien (Art. 21 GG) wird das Internet aber auch von nicht-staatlichen Organisationen NGO zur Selbstdarstellung politischer Ziele sowie zur politischen Kommunikation genutzt, indem jedermann die Möglichkeit zur Äußerung geboten wird. Im folgenden dokumentiere ich als Beleg für die Vielfältigkeit das Angebot von http://www.politik-digital.de/, das stellvertretend für andere stehen kann.

www.politik-digital 1



webforum www.politik-digital 2

Chat in www.politik-digital 3

Den institutionalisierten politischen Akteuren bieten die Möglichkeiten zur elektronischen Interaktion eine intensivere Rückkoppelung zum Bürger. Umgekehrt vermitteln die interaktiven Optionen des elektronischen Mediums dem Bürger die Chance, sich unmittelbar an die politisch institutionalisierten Akteure als Person mit ihrem Anliegen oder ihrer Meinung zu wenden.

Allerdings lässt sich bereits heute absehen, dass die interaktiven Möglichkeiten des Internets die institutionalisierten politischen Akteure auch zu zusätzlichen und neuen medienspezifischen kommunikativen Leistungen herausfordert.

- Das Angebot zur unmittelbaren Interaktion in *Webforen* setzt voraus, dass die Beiträge der Bürger zur Kenntnis genommen werden und die institutionalisierten politischen Akteure auf diese auch mehr oder weniger direkt reagieren. Andernfalls droht das Angebot zur Interaktion auf einer nur symbolischen Ebene zu verharren, was den Nutzern früher oder später auch nicht verborgen bleibt. Letztlich erfordert das Angebot zur Interaktion seitens der institutionalisierten politischen Akteure

- Herausgefordert werden die politischen Akteure in den *Webforen* vor allem auch hinsichtlich ihrer Ausdrucksweise: Elektronische Beiträge erfordern eine eigene Art der Mitteilung in Form einer präzisen gesprochenen Schrift, die experimentell gelernt werden muss (Medienkompetenz). Erwartet wird weder ein Interview noch eine Pressemitteilung.

- Reaktionen auf elektronische Interaktion in *Webforen* sind zeitintensiv. Sie sind für den institutionalisierten politischen Akteur öffentliche Rede, die aber schriftlich im Netz

fixiert „sein muss“. Ohne zusätzliche personelle Kapazitäten oder die Unterstützung von Moderatoren werden beispielsweise Abgeordnete die Möglichkeiten der Kommunikation in Webforen nicht wirksam für ihre politische Kommunikation nutzen können.

- Möglicherweise erklärt der Aufwand für Kommunikation in Webforen die zunehmende Attraktivität des *Chattens* mit Politikern: Das Chatten ist zeitlich begrenzt und erzeugt durch das im Netz veröffentlichte Transskript gleichwohl einen gewissen massenkommunikativen Multiplikationseffekt.

Folgen für die parlamentarische Demokratie

Die Konsequenzen der Internetkommunikation für die parlamentarische Demokratie lassen sich noch nicht abschließend überblicken. Folgende Tendenzaussagen lassen sich jedoch bereits schon heute treffen:

- Zahlreiche Abgeordnete nutzen die Möglichkeiten des Internets bereits auf eigenen Homepages für ihre ***Selbstdarstellung*** neben der institutionell vermittelten Darstellung durch http://www.bundestag.de.

- Die elektronische Kommunikation bietet dem Parlament als Volksvertretung die Chance einer intensiveren ***Rückkoppelung mit dem Bürger*** sowohl auf der Meinungs- als auch auf der Sachebene durch Foren der Interaktion wie sie bspw. im Projekt http://www.elektronische-demokratie.de erprobt wird.

- Vor allem auf der Informationsebene bietet das Internet die Möglichkeit, die parlamentarischen ***Beratungen in den Ausschüssen*** transparent zu gestalten.

- Bei einem strategisch geschickten Einsatz der Möglichkeiten elektronischer Kommunikation kann das Parlament insbesondere strategische Nachteile gegenüber der Regierung ausgleichen, indem es die ***politische Kommunikation*** sowohl innerhalb des Parlaments zwischen Regierungskoalition und Opposition als auch mit Bürgern und Verbänden im Netz „***zelebriert***“. Hierzu muss das Parlament die Möglichkeiten der elektronischen Kommunikation einer virtuellen Bühne vergleichbar punktuell auch einzusetzen verstehen, d.h. es bedarf eines entsprechenden Konsenses unter den Abgeordneten.

- Ungenutzte Potentiale bestehen für das Parlament insbesondere bei der Anhörung von Sachverständigen. So könnten die Ausschüsse bspw. die an die Sachverständigen gerichteten Fragen zeitgleich im Internet veröffentlichen und jeden Bürger zur Beantwortung und Diskussion auffordern. Eine elektronische ***Bürgeranhörung*** könnte als Ergänzung und Gegengewicht zu den Anhörungen häufig dominierenden Vertretern der Verbände und der Wissenschaft bilden. Durch gezielte Fragestellungen könnten insbesondere Anwendungserfahrungen der Bürger in Erfahrung gebracht werden. Das Instrument ***virtueller Hearings*** mit Jedermann-Beteiligung wird bereits heute von der

EU-Kommission genutzt. Wirksam unterstützen kann dieses Instrument die parlamentarischen Beratungen allerdings erst, wenn die Bürgerbeiträge in einem gesonderten Bericht zusammengefasst und für die Beratungen aufbereitet werden.

Handlungsempfehlung: Virtuelle Bürgeranhörungen sollten an drei ausgewählten Beispielen erprobt und ihre Erfahrungen ausgewertet werden. Die Ausschussberatungen sollten punktuell über das Internet zugänglich gemacht werden. Die Möglichkeiten der Interaktion im Projekt www.elektronische-demokratie.de des Deutschen Bundestages sind zu nutzen.

4.3. Welche demokratischen Potentiale ergeben sich aus den spezifischen Eigenschaften der neuen IuK-Möglichkeiten für die Mitwirkungsmöglichkeiten der Bürger? Welche praktischen Erfahrungen gibt es und welche besonderen Maßnahmen sind für die weitere Förderung der Demokratisierungsziele sinnvoll?

Die Möglichkeiten der IuK-Techniken erlauben eine

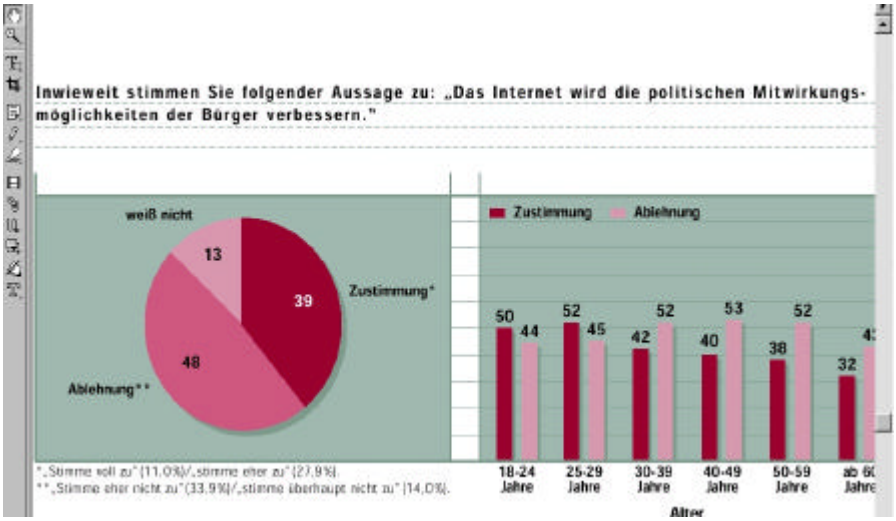
- Teilhabe an parlamentarischen Entscheidungsprozessen durch Meinungsäußerung und Sachinformationen (siehe oben zu 4.2).
- Elektronische Wahlentscheidungen zu Selbstverwaltungskörperschaften und elektronische Abstimmungen.[8]
- Teilhabe an Verwaltungsentscheidungen in öffentlichen Planungsprozessen durch elektronische Anhörungsverfahren (Bauleitplanung, Verkehrsplanung etc.).
- Teilhabe an der politischen Willensbildung durch Meinungsbildung und -äußerung jenseits förmlich verlaufender parlamentarischer Entscheidungsprozesse in Vereinen und Verbänden.
- Politische Selbstorganisation „Betroffener“ bzw. spontaner oder kulturell verfestigter Protestkulturen.

Seitens der Bürger werden die Möglichkeiten des Internets überwiegend noch zurückhaltend bewertet. Überwiegende Zustimmung kommt vornehmlich von Jüngeren. Andererseits ist offensichtlich, dass viele Bürger den Neuen Medien mit dem Gefühl der Überforderung begegnen. Die Werte geben Anlass zu zwei Einschätzungen

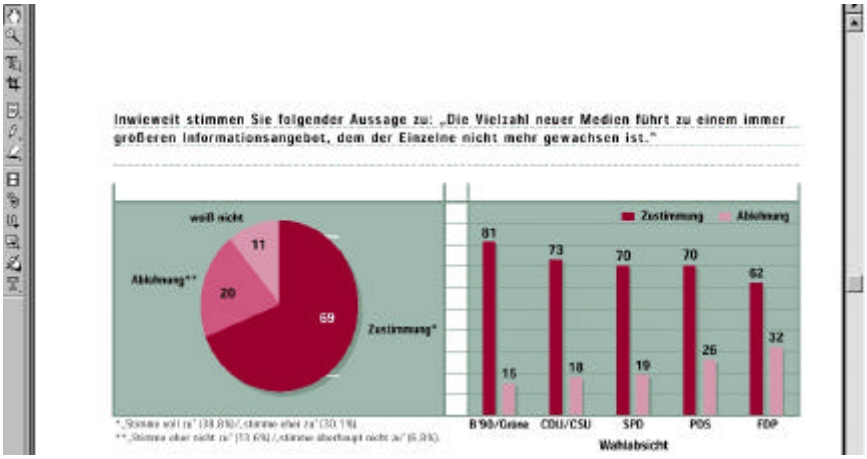
- Ohne Medienkompetenz der Nutzer und Anbieter werden sich nur geringe demokratischen Potentiale der IuK-Techniken entfalten können.

[8] Aus Zeitgründen kann dieser Aspekt in diesem Zusammenhang nicht näher vertieft werden.

- Die Entfaltung demokratischer Potentiale der neuen IuK-Techniken bedarf ausreichender Zeit für ihre Gestaltung und Aneignung.



Forschungsgruppe Wahlen Telefonfeld GmbH 2001



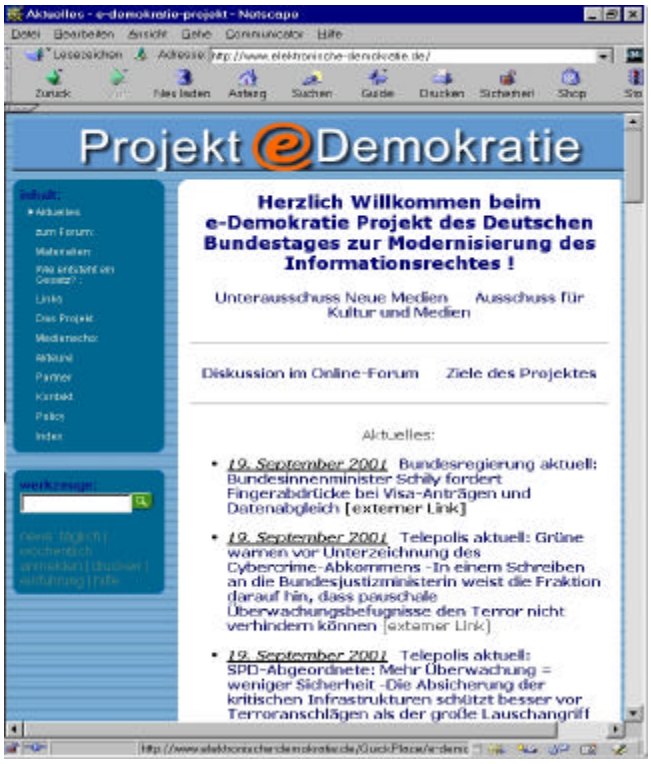
Forschungsgruppe Wahlen Telefonfeld GmbH 2001

Praktische Erfahrungen im Bereich des Deutschen Bundestages

Erste experimentelle Erfahrungen im Bereich der Interaktion versucht der Deutsche Bundestag derzeit durch zwei verschiedene Formen. Zum einen durch ein sporadisches Forum zu aktuellen Themen, deren Beiträge redaktionell betreut werden,

www.bundestag.de/forum 1

sowie durch das Projekt http://www.elektronische-demokratie.de, in dem die Beiträge redaktionell unbearbeitet von den Teilnehmern zu Fragen der Modernisierung des Informationsrechts eingestellt werden können.



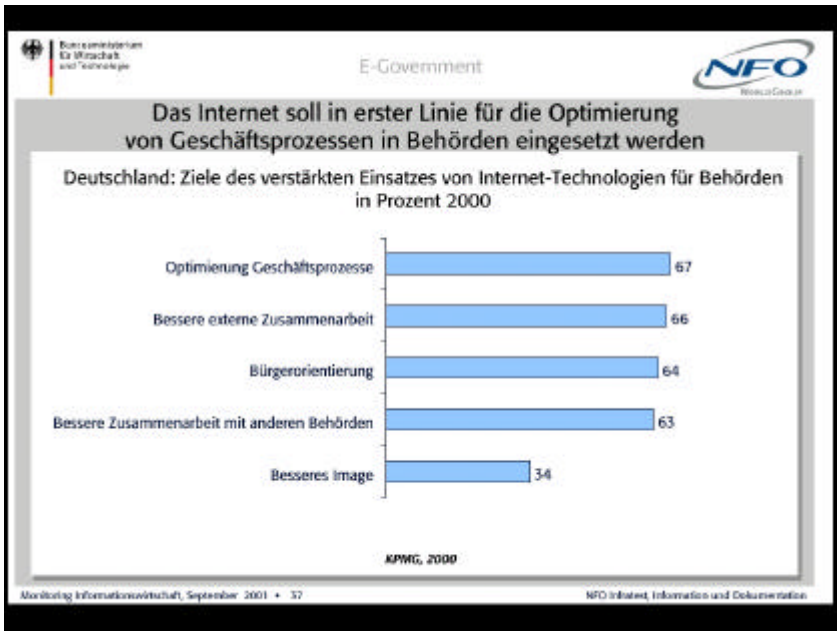
Erste Schlussfolgerungen aus den Erfahrungen aus dem Projekt http://www.elektronische-demokratie/ sind bereits oben dargestellt worden: Interaktivität im Internet erfordert eine besondere Medienkompetenz sowie einen gewissen Zeitaufwand seitens der Abgeordneten. Die Erwartungshaltung der Teilnehmer an eine Beteiligung der Abgeordneten in einem solchen Forum sind hoch. Häufig ist festzustellen, dass die Teilnehmer im Forum nur über geringe Vorstellung von der Arbeitsweise der Abgeordneten haben.

Für interaktive Kommunikationsforen ist die Existenz eines Moderators als Vermittler sowie der Umstand, dass dieser über „ein Gesicht verfügt", von großer Bedeutung. Dem Moderator wächst die Rolle der Autorität über die Einhaltung der Kommunikationsregeln zu. Das „Gesicht" ist wichtig, um den in Internetkulturen gegenüber staatlichen Institutionen latenten (Vor-)Zensurverdacht glaubwürdig ausräumen zu können. Gleichzeitig muss der Moderator für die Teilnehmer prinzipiell angreifbar sein, d.h. allein die Möglichkeit, sein Rollenverhalten in Frage stellen und diskutieren zu können, ist eine vertrauensbildende Maßnahme in der elektronischen Kommunikation.

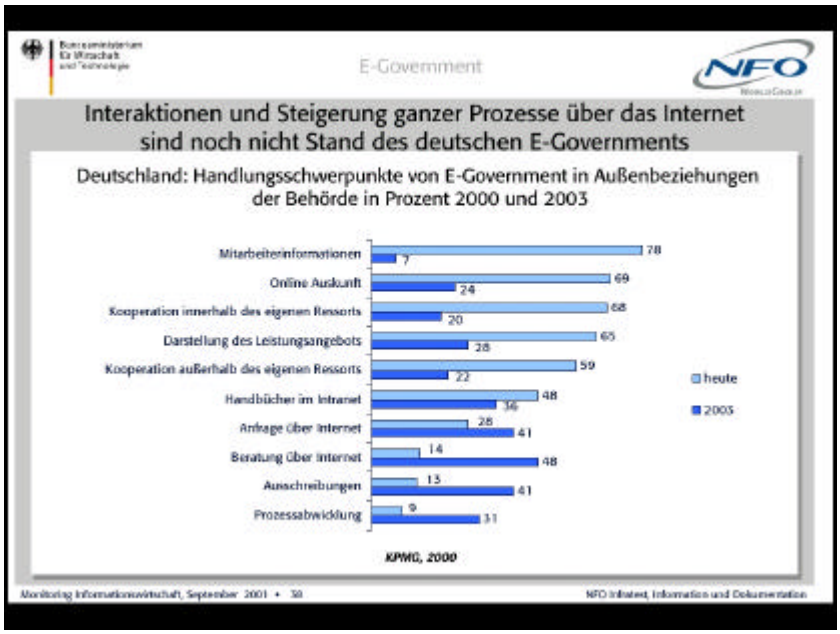
Förderung der Demokratisierung

Die Aneignung der elektronischen Kommunikationstechniken verläuft als ein Lernprozesse, in dem Konzepte entwickelt, ausprobiert und verworfen werden. Das derzeitige Stadium ist eine Phase des Lernens und des Experimentierens mit den Möglichkeiten der neuen Medien.

Die Bedeutung der elektronische Interaktion mit dem Bürger in E-Government-konzepten wird allerdings durch Einschätzungen der Strategen erheblich relativiert. Im Vordergrund der derzeitigen Überlegungen zum E-Government steht in erster Linie die Nutzung der IuK-Technik zur Optimierung der Geschäftsprozesse innerhalb der Verwaltung. Insbesondere die Information und Beratung der Bürger mit Mitteln des Internets stellt sich aus dieser Perspektive vor allem als eine Optimierung der Sprechzeiten in den Verwaltungen dar, die als Sekundärnutzen auch bürgerfreundlich ist. Die Nutzung des Internets für die Beteiligung der Bürger an verwaltungspolitischen Entscheidungsverfahren steht alles andere als im Vordergrund der E-Government-Strategen.



NFO im Auftrag BMWi 4



NFO im Auftrag BMWi 5

Handlungsempfehlung: Anwendungen und Nutzungsmöglichkeiten des Internets für Formen der politischen Willensbildung ausprobieren: Entwerfen, Testen, Beobachten, Auswerten.

4.4. Inwieweit sind wichtige Aspekte einer hinreichenden demokratischen Repräsentation von gesellschaftlichen Interessen und Gruppen auch in globalisierten IuK-Netzen zu

verwirklichen?
Welche besonderen Probleme ergeben sich und welche Folgen erwachsen für Ansätze zur weiteren Demokratisierung sowohl der technischen Verwaltungen als auch der politischen Gestaltung der weltweiten IuK-Netzwerke ?

Das Internet steht als über die Welt gespanntes Netz einzelner Rechner als Synonym für eine globalisierte elektronische Welt. Die Gestaltungsvorgaben globaler Netzwerke richten sich nach

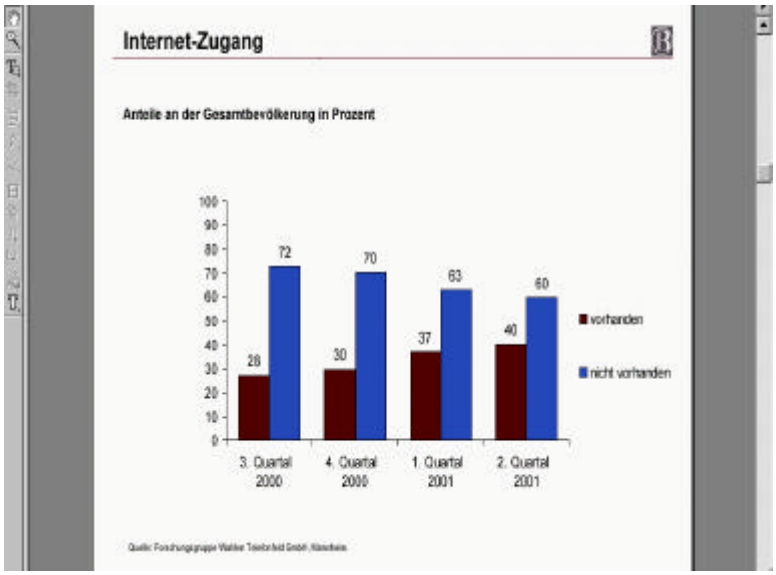
- den Ergebnissen einer internationalen technischen Standardisierung, die teilweise transparent für alle über das Internet (RFC-Standards), zum Teil auch geschlossen innerhalb der klassischen Normungsorganisationen (bspw. ETSI) verläuft
- Die Internationale Fernmeldeunion (ITU)
- Industriekonsortien wie W3C oder Global Buisiness Dialogue
- Selbstorganisation des Internets wie bspw. ICANN (Internet Corporation for Assigned Names and Numbers), einer privaten Internet-Organisation mit Sitz in Marina del Rey, Kalifornien, die bestimmte zentrale Koordinierungsaufgaben für die Verwaltung von Domain-Namen und Adressen für das Internet übernimmt.

Lediglich das ICANN sieht eine Wahl zumindest einiger Positionen seines Leitungsgremiums („Direktorium“) durch registrierte Internetnutzer vor. Das ITU verfügt über eine völkerrechtliche Grundlage.

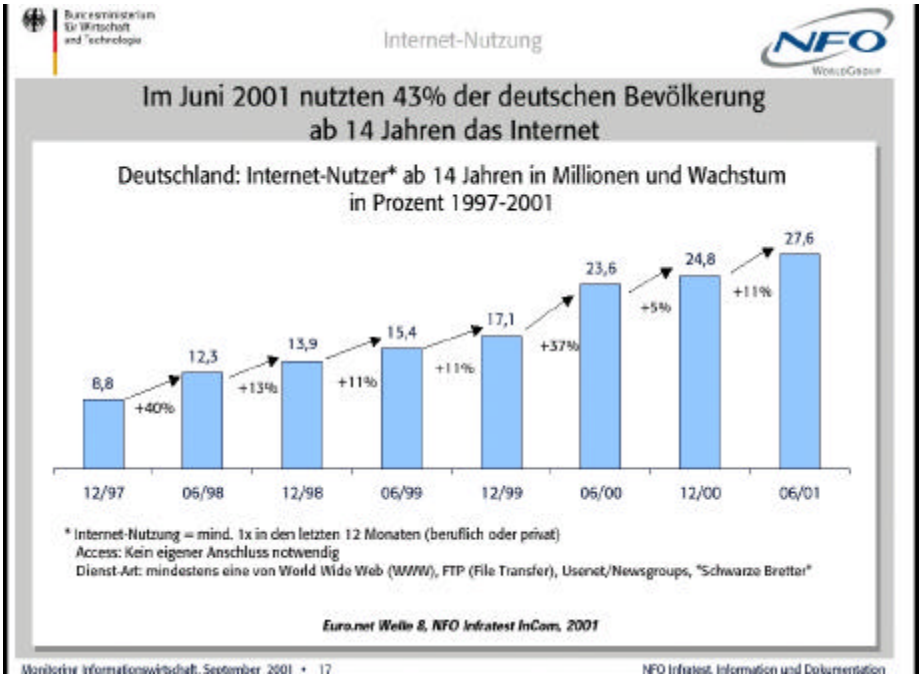
Handlungsempfehlung: Die defizitäre demokratische Legitimation der Normung des globalen Netzwerkes bedarf einer gesonderten Untersuchung, in deren Rahmen ein Konzept einer völkerrechtlichen Legitimation zu entwerfen ist.

4.5. Welche Folgen ergeben sich aus der weiterhin zu konstatierenden elektronischen Abstinenz großer Teile der Bevölkerung, insbesondere auch in den Schwellen- und Entwicklungsländern? Welche Maßnahmen sind notwendig, um eine breitere und aktive Teilnahme und Teilhabe zu fördern?

Die Zahlen über steigende Nutzerzahlen im Internet dürfen nicht darüber hinwegtäuschen, dass selbst in Deutschland der überwiegende Anteil der Bevölkerung noch über keinen Internetanschluss verfügt. Zu berücksichtigen ist ferner, dass die Angabe von 40 % der Bevölkerung mit Zugang zum Internet. noch keine Aussage über die tatsächliche Nutzungsfrequenz enthält.



Forschungsgruppe Wahlen 2001



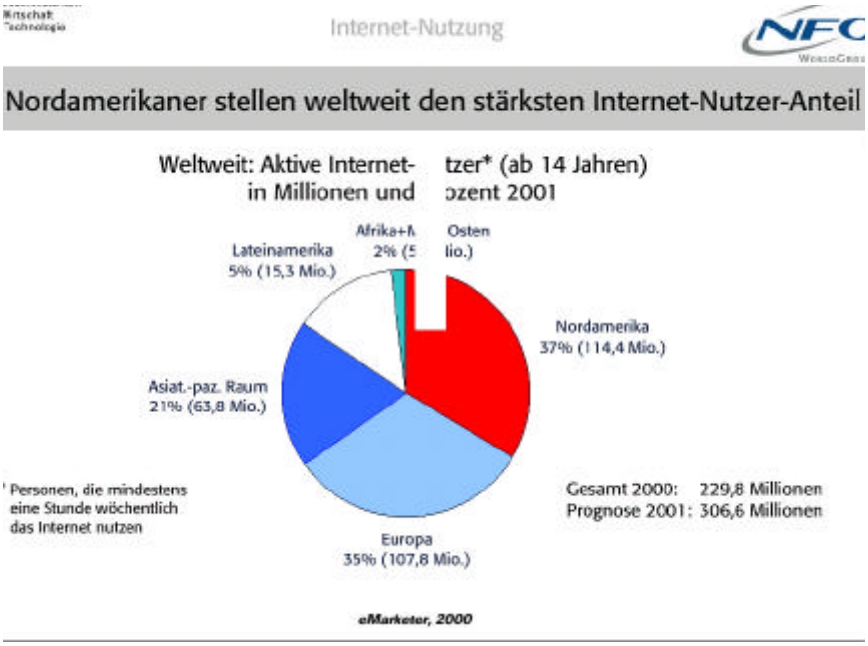
NFO im Auftrag BMWi 6

Innerhalb der Gruppe der Internetnutzer ist eine deutliche Differenzierung nach Bildungsschicht und Einkommen festzustellen. Je höher die Schulbildung und Einkommen desto stärker die Internetnutzung.

NFO Infratest InCom 9/2001 1

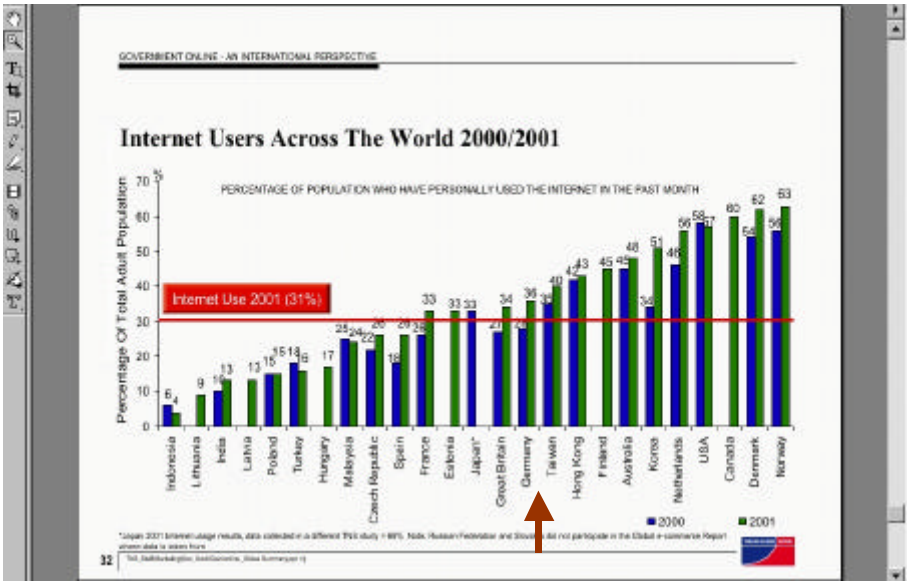
NFO Infratest InCom 9/2001 2

Dramatisch fällt die Anschlussdichte im Weltmaßstab aus – wie das folgende Chart zeigt. Die Prozent-Angaben beziehen sich auf die Gesamtgröße der Internetnutzer. Die Differenzen würden noch erheblich stärker auseinander klaffen, wenn als Bezugsgröße die Bevölkerung gewählt worden wäre.



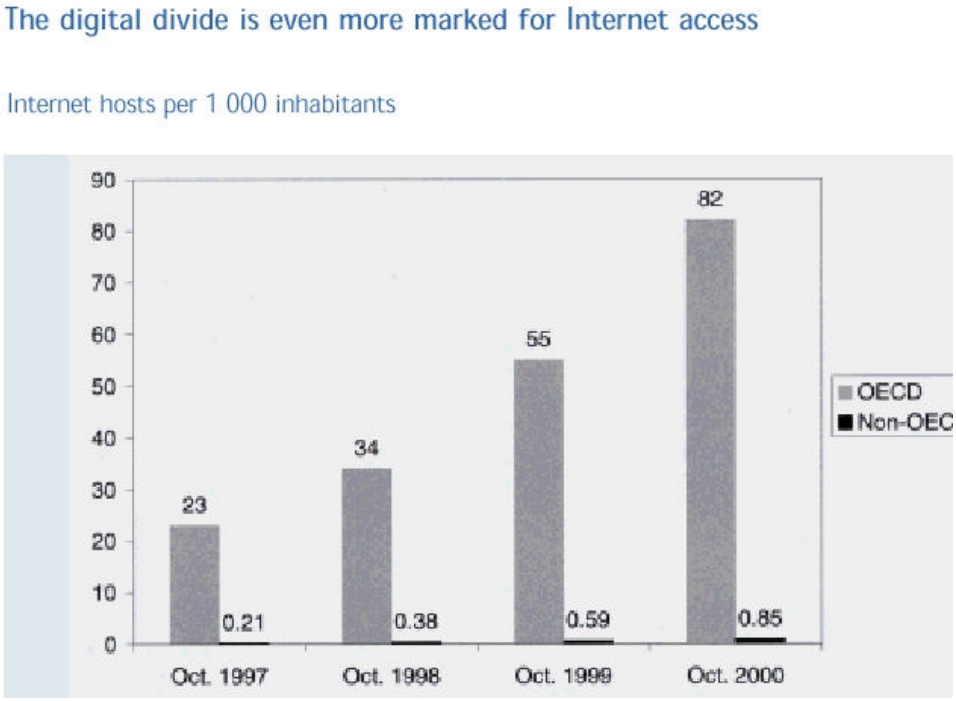
Taylor Nelson Sofres 11/2001 1

Die folgende Grafik belegt die These, dass auch innerhalb der entwickelten Industriestaaten große Unterschied in der Internetnutzung auszumachen sind.



Taylor Nelson Sofres 11/2001 2

Das folgende Chart entstammt einer Untersuchung der OECD und verdeutlicht den Abstand zwischen den „entwickelten Staaten“ der OECD und dem Rest der Welt.



OECD Understanding Digital Divide 2001 1

Die Erläuterung der Studie verdeutlicht, dass innerhalb der Nicht-OECD-Länder die Anteile der Internet-Hosts ebenfalls nicht gleichmäßig verteilt sind.[9] Sie verteilen sich auf wenige Schwellenländer der Nicht-OECD-Staaten.

- In October 2000, there were just over 94 million Internet hosts in the world, with 95.6% in the OECD area and 4.4% outside the OECD area. Growth in non-member countries, mostly those with relatively high GDP per capita, has matched growth rates in the OECD area.
- Chinese Taipei, Singapore, Hong Kong (China) and Israel account for 52% of all Internet hosts outside the OECD area and Argentina, Brazil, Malaysia and South Africa for a further 24%.
- On a regional basis, North America and Europe account for 89% of all Internet hosts. The regional share of Internet hosts
- is very low in Central and South America and in Africa.
- Africa has only 0.25% of all Internet hosts and its share has been decreasing. The overwhelming majority of these Internet hosts are in South Africa, where the growth rate is slow. The shares of Central and South America have grown, owing to much higher growth rates in Argentina, Brazil and Chile.

[9] OECD, Understanding the Digital Divide, 2001.

Zusammenfassend ist festzuhalten:

> National können wegen ihrer sozio-technischen Voraussetzungen an der Willensbildung über elektronische Kommunikationsmedien (Internet) derzeit nur Bevölkerungsteile mit hoher Schulbildung und Einkommen partizipieren.
>
> Zwischen den Staaten der westlichen Welt bestehen erhebliche Unterschiede in der Nutzung des Internets. Im Weltmaßstab ist die Bevölkerung ganzer Kontinente von der Teilhabe an der elektronischen Kommunikation buchstäblich ausgeschlossen.

Handlungsempfehlung: Die Grundversorgung mit elektronischen Kommunikationsmedien ist Voraussetzung für die Entwicklung einer zivilen Informationsgesellschaft und daher staatlich zu gewährleisten. Eine breitere und aktive Teilnahme lässt sich in Europa *erstens* durch Kostensenkung im Bereich von Telekommunikation und Internetnutzung (flatrate) und *zweitens* durch Maßnahmen zur Förderung der Medienkompetenz insbesondere im Rahmen der beruflichen Aus- und Weiterbildung erreichen.

Die Versorgung der Bevölkerung in Staaten der Dritten und Vierten Welt mit einer Grundversorgung an Möglichkeiten der elektronischen Kommunikation zur elektronischen Selbstdarstellung und Interaktion sollte Bestandteil der Entwicklungshilfe- und Bildungspolitik sein. Es bedarf erheblicher Anstrengungen, damit zumindest die Bildungseliten in Entwicklungs- bzw. Schwellenländern die Chance haben, den Anschluss an die globale Informationsgesellschaft der Industriestaaten nicht vollständig zu verpassen.

4.6. Inwieweit erfordert die zunehmende gesellschaftliche Bedeutung elektronischer Kommunikation eine Neugewichtung oder Erweiterung des Grundrechtsverständnisses? Welche neue Bedeutung kommt beispielsweise dem Recht auf informationelle Selbstbestimmung, dem Recht auf Privatsphäre sowie den Schutzrechten hinsichtlich der individuellen Kommunikation zu ?

Von Bedeutung für die elektronische Kommunikation sind u.a.

- Schutz der Meinungsäußerungsfreiheit
- Schutz personenbezogener Daten, die bei der Nutzung der Telekommunikation sowie der Internetdienste[10] anfallen.

---

[10] Nach deutschem Recht: Tele- und Mediendienste – bei entsprechender Bandbreite nicht auszuschließen auch Rundfunkdienste. Nach EU-Recht „Dienste der Informationsgesellschaft“.

- Schutz der Vertraulichkeit der kommunizierten Inhalte und ihrer Umstände.
- Schutz der Integrität und Authentizität elektronischer Dokumente.
- Verfügbarkeit elektronischer Informationen.
- Zugang zu elektronischen Informationen.

Die Liste ist nicht abschließend.

Grundrechte sind Abwehrrechte gegen staatliche Gewalt. Sie wirken jedoch mit ihren objektivrechtlichen Schutzgehalten auch auf die Rechtsordnung ein und verpflichten den Gesetzgeber, den geschützten Rechtsgütern auch in der privaten Kommunikation Geltung zu verschaffen. Ein wirksamer Schutz individueller Kommunikationsrechte hat unter zwei Gesichtspunkten besondere Bedeutung:

1. Wirksamer Schutz ist eine zentrale Voraussetzung für die Entwicklung einer zivilen Informations- und Wissensgesellschaft freier, wenngleich rechtlich gebundener Netzbürger.
2. Der wirksame Schutz der individuellen Kommunikation ist eine *zentrale Akzeptanzvoraussetzung für die Entwicklung der zivilen Informationsgesellschaft*.

Wirksam („effektiv“) kann und wird individuelle Kommunikation durch Maßnahmen auf mindestens zwei verschiedenen Ebenen geschützt:

- ***Ebene 1: Mit Hilfe des Rechts*** werden Kommunikationsrechte durch eine risikoadäquate (d.h. an den durch die Anwendung der IuK-Technik induzierten Risiken) Anwendung, Weiterentwicklung und Reformulierung des Schutzgehaltes bestehender Rechte sowie die Gewährleistung einer sicheren Infrastruktur als Voraussetzung einer ungehinderten Kommunikation geschützt.

Beispiel 1: Nachdem mit der Privatisierung des Telekommunikationsmarktes das Fernmeldegeheimnis aus Art. 10 GG gegenüber privaten TK-Dienstanbietern keine unmittelbare Geltung mehr beanspruchen konnte, hat der Gesetzgeber 1996 diesem über § 85 TKG einfachgesetzlich Geltung verschafft. Flankiert wird der Schutz der Vertraulichkeit der Kommunikation durch die Verpflichtung der Dienstanbieter zur technisch-organisatorischen Sicherung dieses Geheimnisses in § 87 TKG sowie durch einen strafrechtlichen Schutz des § 206 StGB. Eine entsprechende Verpflichtung findet sich auch im EG-Recht in der sogenannten TK-Datenschutzrichtlinie 97/66/EG.

Beispiel 2: Der Schutz personenbezogener Daten aus der Nutzung von Internetangeboten hat der nationale Gesetzgeber durch das Teledienstdatenschutzgesetz (TDDSG) und den Mediendienstestaatsvertrag (MD-StV) sicherzustellen versucht. Von Bedeutung ist hier die international beachtete Verpflichtung der Dienstanbieter, Angebote zur pseudonymen oder anonymen Nutzung anzubieten.

Beispiel 3: Den Schutz der Willenserklärungsfreiheit vor Verfälschung hat der Gesetzgeber zu gewährleisten versucht, indem er dem dem Signaturgesetz Anforderung an technisch-organisatorische Voraussetzungen sicherer elektronischer Signaturen vorgegeben hat.

Beispiel 4: Durch die Gewährleistung von Zugangsrechten zu staatlichen Informationen wird versucht, nicht nur ein informationelles Gleichgewicht zwischen Staat und Bürgern herzustellen, sondern vor allem Voraussetzungen für die politische Willensbildung zu gewährleisten. Besondere Probleme wirft die Gewährleistung der Nutzungsrechte der Bürger gegenüber (bspw. urheberrechtlich geschützten) Nutzungsrechten auf.

- ***Ebene 2: Mit Hilfe der Technik*** können die Grundrechtsträger ihre Kommunikationsrechte selbst gegen unberechtigte Zugriffe und Angriffe schützen. In der Diskussion werden solche Maßnahmen auch als **Selbstschutzmaßnahmen** bezeichnet. Schutzmaßnahmen können aber auch von den Dienstleistern der technischen TK-Infrastruktur sowie der Angebote im Internet ergriffen werden.

Beispiel 1: Die Vertraulichkeit der Kommunikation kann mit Hilfe von Verschlüsselungsverfahren von den Kommunikationsteilnehmern selbst geschützt werden. Der Anbieter von Inhalten im Netz (Tele- und Mediendienste) kann die Kenntnis der Nutzung bestimmter Webseiten durch die Einrichtung mit Hilfe von Verschlüsselung geschützter Kanäle gewährleisten (bspw. SSL-Verschlüsselung).

Beispiel 2: Durch die Verwendung von Pseudonymen können Nutzer Informationsangebote gegen unberechtigte Kenntnis ihrer personenbezogenen Daten geschützt nutzen. Perspektivisch ermöglicht die Verwendung vorbezahlter Wertkarten im Internet ihre anonyme Inanspruchnahme, ohne die Rechte des Anbieters auf Bezahlung unangemessen zu verkürzen. TDDSG und MD-StV versuchen die Bedingungen eines angemessenen Selbstdatenschutzes durch die Verpflichtung der Anbieter zu ermöglichen, anonyme oder pseudonyme Nutzung ihrer Dienste im Rahmen der Zumutbarkeit anzubieten..

Beispiel 3: Die Verwendung von elektronischen Signaturen nach Signaturgesetz bietet Voraussetzungen, damit Nutzer je nach Schutzbedürfnis die Integrität und Authentizität ihrer Informationen gegenüber Dritten selbst schützen können.

Schlussfolgerung: Der Schutz der Kommunikationsgrundrechte vollzieht sich einerseits auf einer rechtlichen, zum anderen auf einer technischen Ebene. Die technische Entwicklung ermöglicht es den Nutzern, ihre elektronische Kommunikation gegen Eingriffe Dritter in offenen Netzen technisch selbst zu schützen. Mit dieser Entwicklung verschiebt und erweitert sich die staatliche Aufgabe zur Grundrechtsgewährleistung vom einfachen Rechtsschutz zur Aufgabe, technische Selbstschutzmöglichkeiten zu fördern.

Der Text der Verfassung spiegelt die tatsächliche Bedeutung „elektronischer Individualrechte“ unvollständig oder nur partiell wieder: So sind die Rechte auf informationelle und kommunikative Selbstbestimmung das Ergebnis einer Verfassungsinterpretation aus dem

allgemeinen Persönlichkeitsrecht, nicht aber einer ausdrücklichen Entscheidung des Verfassungsgebers. In anderen Fällen „klebt“ der Verfassungstext an überkommenen Formulierungen wie bspw. dem Begriff des „Fernmeldegeheimnisses“, obwohl weltweit von Telekommunikation die Rede ist. Die mit Blick auf die moderne IuK-Technologien erforderliche Entwicklung der verfassungsrechtlichen Gehalte ist nicht nur eine Frage der Ausgestaltung des Verfassungstextes, sondern eine hermeneutische Aufgabe von Wissenschaft und Anwendungspraxis. Gleichwohl ist die Reflektion und ggf. Fortentwicklung der Verfassungstexte in Hinblick auf die Chancen und Risiken der IuK-Technologien eine zentrale verfassungspolitische Aufgabe des Verfassungsgebers, die er als solche auch nicht negieren sollte.

Aufgrund der Privatisierung der Telekommunikation ist von mindest ebenso großer Bedeutung die wirksame Gewährleistung individueller Kommunikationsrechte gegenüber den privaten Dienstleistern durch ausreichende Gesetze. Da die Informationsflüsse elektronischer Kommunikation über weltweite Netze vermittelt wird, selbst wenn der Informationszugriff von einem im Inland belegenen Client auf einen im Inland belegenen Server erfolgt, müssen die Kommunikationsrechte auch weltweit geschützt und gewährleistet werden.

In Anbetracht der Bedeutung der elektronischen Kommunikationsgrundrechte und ihres Stellenwertes im Austausch von Informationen und Meinungen zwischen Bürgern der Staaten dieser Welt, fehlt es an einer internationalen Kodifizierung von Grund- und Menschenrechte der Netzbürger. Eine solche Kodifizierung ist als Gegengewicht zu den bereits international vielfältig koordinierten und abgestimmten Eingriffsbefugnissen in die Telekommunikation (ILETS, CyberCrime Konvention, Rechtshilfeübereinkommen der EU etc.) überfällig.

Handlungsempfehlung: National ist der Grundrechtskatalog fortzuentwickeln. Im Verhältnis zu den privaten Anbietern der IuK-Infrastruktur sind die Schutzgehalte der Grundrechte vor allem durch einfachgesetzliche Maßnahmen zu gewährleisten.

Auf internationaler Ebene (Europarat, UN) ist eine Charta der elektronischen Menschenrechte zum Schutz der elektronischen Kommunikation der Netzbürger als Gegengewicht zu den nationalen, aber weltweit wirkenden Eingriffsmöglichkeiten von Sicherheitsbehörden einerseits und Dienstanbietern andererseits in diese Rechte zu entwickeln.

4.7. Ergeben sich besondere Gefährdungen für die demokratische Grundordnung aus den spezifischen Eigenschaften der neuen globalen IuK-Möglichkeiten? Falls ja: Welches sind diese und welche Maßnahmen sind für ihre Bewältigung notwendig und sinnvoll?

Im folgenden beschränke ich mich auf die Skizzierung von einigen – aus meiner Sicht – zentralen Gefährdungen.

Download rechtswidriger Dokumente

Ohne Zweifel besteht die Möglichkeit, dass Nutzer im Inland bspw. Informationen von Webservern im Ausland laden können, deren Verbreitung nach deutschem Recht eine Straftat darstellt (Beispiele: Rechtsradikalismus, Volksverhetzung, Auschwitzlüge etc.). Diese Möglichkeit kann je nach Einzelfall eine strafbare Handlung darstellen, sie bewirkt aber nach derzeitigem Kenntnisstand keine „besondere Gefährdung der demokratischen Grundordnung“ in der Bundesrepublik Deutschland. Zu berücksichtigen ist, dass die Verfügbarkeit rechtswidriger Inhalte im Internet nicht identisch mit ihrer Kenntnisnahme durch eine relevante Zahl von Nutzer ist, zumal von denen wiederum eine relevante Zahl für die „Qualität“ dieser Informationen auch empfänglich sei muss. Gleichwohl ist das Angebot extremistischer Inhalte in Internet, insbesondere aber das Interesse an ihrer Rezeption *ein* Indikator (unter anderen) für den Stellenwert bspw. extremistischer oder verfassungsfeindlicher Tendenzen in der Gesellschaft der Bundesrepublik Deutschland. Dieser Indikator gewinnt jedoch erst einen relevanten Aussagewert, wenn er mit anderen Tatsachen, Hinweisen und Indizien in Beziehung gesetzt und gewichtet wird.

Zudem ist zu berücksichtigen, dass aufgrund der durch das Medium Internet hergestellten Öffentlichkeit extremistische Inhalte nicht nur unter dem Gesichtspunkt der Gefährdung durch Rezeption und Massenwirksamkeit ihrer Inhalte zu bewerten sind. Auch umgekehrt kann gelten, dass gerade die Allgemeinzugänglichkeit extremistischer Inhalte eine öffentliche und kritische Rezeption innerhalb der politischen Bildung auslösen kann, der ihrerseits wiederum unter der Voraussetzung einer sensiblen (medialen) Öffentlichkeit und einer gewissen Breitenwirkung eine systemstabilisierende Funktion zukommen kann.

Der Verbreitung rechtswidriger Inhalte kann letztlich durch die Verpflichtung der Provider begegnet werden, im Rahmen der Störerhaftung den Zugang zu derartigen Webseiten zu sperren. Voraussetzung ist allerdings nach deutschen und europäischen Recht, eine positive Kenntnis derartiger Sachverhalte. Die Provider sind nicht verpflichtet, von sich aus aktiv nach rechtswidrigen Inhalten zu forschen. Unter den international wichtigen Bestrebungen ist insbesondere die vom Europarat unter Beteiligung anderer westlicher Staaten (USA, Kanada etc.) Ende November 2001 beschlossene CyberCrime-Konvention zu nennen.

Der BGH hat Ende 2000 entschieden, dass Meinungsäußerungen, die auf ausländischen Servern gehostet sind und den Tatbestand der Volksverhetzung nach § 130 Abs. 3 StGB erfüllen, im Inland verfolgt werden können, wenn die Äußerung konkret zur Friedensstörung im Inland geeignet ist (BGH vom 12.12.2000, Az.: 1 StR 184/00 – MMR 2001, 228).

Verletzlichkeit der Informationsgesellschaft

Eine zunehmende Abhängigkeit der Gesellschaft und ihrer Bürger von elektronischen Kommunikationsmedien erhöht ihre Verletzlichkeit gegenüber gezielten Angriffen auf Einrichtungen der Telekommunikation und zentrale Informationsangebote. Durch den hohen und weltweiten Vernetzungsgrad sind derartige Angriffe bspw. durch Viren, trojanische Pferde etc. („Schneeballeffekt“) auch von Servern aus dem Ausland nicht nur möglich, sondern Realität.

Die Diskussion über die erforderlichen Maßnahmen wird derzeit unter den Stichworten des „information war“ sowie der „***kritischen Infrastrukturen***“ geführt. Derartige Maßnahmen könnten zwar wichtige Einrichtungen in der Bundesrepublik Deutschland zeitlich begrenzt „lahm legen“, jedoch ist die Vermutung abwegig, auf diese Weise könne die „demokratische Grundordnung“ in besonderer Weise gefährdet werden. Zunächst haben die Erfahrungen mit Systemausfällen durch Angriffe von außen, immer auch zu einem erhöhten Sicherheitsbewusstsein bei den Netz- und Internetanbietern geführt. Schließlich ist zu bedenken, dass nicht jede veröffentlichte Information über Angriffe im Internet auf eine böswillige Attacke mit Schädigungsabsicht beruht. Zahlreiche Schwachstellen im Internet werden von Hackern öffentlich gemacht, die auf diese Weise die Sicherheit im Internet erhöhen wollen. Insofern sorgt die Netzkultur bereits in Ansätzen durch Selbstversuche und Transparenz dafür, mögliche Schwachstellen aufzudecken und abzustellen. Unter diesem Gesichtspunkt ist die insbesondere in der CyberCrime Konvention vorgesehene Strafbarkeit des absichtlichen Hackings nicht unproblematisch, weil sie geeignet ist, die fruchtbare Sicherheitskultur des „hacking for checking“ zu blockieren.

Maßnahmen zur Verminderung von Verletzlichkeitsrisiken setzen zunächst an der Architektur der Infrastruktur an, die redundant ausgelegt wird. Anbieter und Nutzer im Internet sind im übrigen über ausreichende Schutzmaßnahmen gegen Angriffe zu unterrichten (Firewalls, Virenschutz, Verschlüsselung, elektronische Signaturen). Selbstschutzmöglichkeiten sind zu fördern. Aktivitäten in diese Richtung betreibt die Bundesregierung bspw. mit ihrer Initiative www.sicheres-internet.de.

Mit Hilfe internationaler Abkommen wie bspw. der CyberCrime Konvention des Europarates sollen die rechtlichen Grundlagen zur Bekämpfung von Kriminalität mit Mitteln des Internets sowie gegen das Internet international harmonisiert werden.

Verletzlichkeit der Individualkommunikation

Spezifische Risiken können sich für die demokratische Grundordnung aus der Überwachung und Erfassung der elektronischen Individualkommunikation im öffentlichen und individuellen Meinungsbildungsprozess ergeben. Sie können sich einschränkend auf das Kommunikationsverhalten der Bürger auswirken und auf diese Weise das verfassungsrechtliche Postulat des freien Willensbildungsprozesses unterlaufen. In Staaten unterhalb des europäischen rechtsstaatlich-freiheitlichen Niveaus können derartige Maßnahmen zur Kontrolle und Unterdrückung demokratischer Meinungsäußerungen der Bürger verwendet werden.

- Indikator sind zumindest in Rechtsstaaten die materiellen Eingriffstatbestände, die den Staat zu einer Kommunikationsüberwachung berechtigen. Bereits für den Rechtsstaat Bundesrepublik ist festzustellen, dass erstens die zur TK-Überwachung berechtigenden Tatbestände ständig ausgeweitet werden, und dass allein für den Bereich der Straftatverfolgung jährlich erhebliche Steigerungsraten festzustellen sind. Über den Vorfeldbereich der nachrichtendienstlichen Überwachung sind Informationen nicht einmal im Rechtsstaat Bundesrepublik Deutschland öffentlich bekannt.

- Hinweise auf das Gefährdungspotential liefert vor allem die weltweite Standardisierung im Rahmen von ETSI durch die Vorgabe von technischen Schnittstellen zur Überwachung der Telekommunikation. Während der Einsatz derartig weltweit standardisierter Einrichtungen in Rechtsstaaten westlicher Prägung immerhin durch die materiellen Eingriffsbefugnisse der Sicherheitsbehörden noch gebunden ist, wirft ihre Verwendung in anderen Staaten bereits erhebliche Probleme für die Wahrnehmung individueller Kommunikationsgrundrechte auf. Sie ist aber auch für das Inland nicht ohne Bedeutung, denn die mit den Schnittstellen gebotenen Eingriffsmöglichkeiten wirken angesichts der weltweit vermittelten Internetkommunikation auch auf das Inland zurück. Letztlich erhöht jede Schnittstelle zur Überwachung immer auch das Risiko einer nicht rechtlich gebunden Überwachung.

- Eine weitere Dimension erfährt die prinzipielle Überwachbarkeit der elektronischen Kommunikation schließlich durch die Möglichkeiten der heimlichen Überwachung in privaten Kontexten und hier insbesondere in Abhängigkeitsverhältnissen, in denen der stärkere Teil auch Anbieter der Telekommunikation ist. Beispiele sind die Überwachung der betrieblichen Internetkommunikation, der elektronischen Kommunikation in Hochschulen und Schulen sowie an anderen (teilöffentlichen) Netzknoten der Meinungsbildung. Im Mittelpunkt der Diskussion steht neben der Gefährdung der freien Kommunikation durch staatliche Einwirkungen vor allem die Abwehr von Wirtschaftspionage.

Schutzmöglichkeiten für die individuelle Kommunikation bestehen vor allem in der Verwendung von Selbstschutztechniken in der Hand der Netzbürger. Beispiele sind die Verwendung von Verschlüsselungsverfahren sowie Möglichkeiten der anonymen bzw. pseudonymen Kommunikation.

Handlungsempfehlung: Gefährdungen durch Information über, Angebot und Förderung von Selbstschutzmaßnahmen im Internet verringern. Durch technisch-organisatorische Maßnahmen die Verfügbarkeit elektronischer Informationen und der IuK-Infrastruktur gewährleisten. Kommunikation der Netzbürger in einer zivilen Informationsgesellschaft stärken und absichern.

4.8. Wie beurteilen Sie die Sicherheit der Kommunikation in der Wissens- und Informationsgesellschaft? Berücksichtigen Sie bitte dabei insbesondere den Aspekt innerer und äußerer Gefährdungen sowohl hinsichtlich des Schutzes des demokratischen Systems als auch hinsichtlich der denkbaren Schutzziele Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit der elektronischen Kommunikation

4.9. Welche besonderen Rahmenbedingungen ergeben sich aus den spezifischen Eigenschaften der neuen IuK-Möglichkeiten sowohl für den Schutz von Grundrechten und Bürgerfreiheiten als auch für die effektive Strafverfolgung und Rechtsdurchsetzung in elektronischen IuK-Netzen? Inwieweit ist hier von einem Interessenskonflikt auszugehen und welche Möglichkeiten eines Ausgleichs oder Kompromisses sehen Sie?

4.10. In welchem Zusammenhang stehen hinreichender Grundrechtsschutz, technischer Selbstschutz der Nutzer sowie flächendeckende technische Überwachungs- und Kontrollmöglichkeiten mit den zentralen politischen Ziel, die Sicherheit von IT-Systemen zu verbessern und zu fördern?

4.11. In welchem Verhältnis stehen Sicherheit der öffentlichen, wirtschaftlichen und individuellen Kommunikation und die Sicherung demokratischer Strukturen und Verfahren in einer globalen Informations- und Wissensgesellschaft?

Zu einigen Gesichtspunkten wurde bereits in der Antwort zu Frage 4.7. Stellung genommen.

Elektronische Kommunikation ist prinzipiell gegenüber folgenden Angriffen verletzlich:

1. Einem elektronischen Dokument kann nicht angesehen werden, ob es nachträglich verändert worden ist. Aus diesem Grund ist seine „Integrität“ bspw. mit Hilfe von elektronischen Signaturen zu gewährleisten.

2. Einem elektronischem Dokument kann nicht angesehen werden, von wem es stammt. Zu gewährleisten ist daher seine Authentizität bspw. mit Hilfe elektronischer Signaturen.

3. Der Inhalt eines elektronisches Dokument kann ohne Schutzmaßnahmen in den Datenspeichern der Vermittlungsrechner sowie auf der Übermittlungstrecke von Dritten zur Kenntnis genommen werden. Die Vertraulichkeit der Inhalte elektronischer Dokumente ist daher netzseitig und individuell durch Maßnahmen der Verschlüsselung zu gewährleisten.

4. Aufgrund der Flüchtigkeit elektronischer Informationen ist ihre Verfügbarkeit gegen Verluste durch technische Fehler und Angriffe zu gewährleisten.

Zwischen den Zielen staatlicher Sicherheit und den Grundrechten der Bürger besteht insofern eine Interessenskonvergenz als es Aufgabe des demokratisch freiheitlichen Rechtsstaat ist, die individuellen Freiheiten in ihrer wechselseitigen Beziehung und Abhängigkeit zu schützen und zu fördern. Zielkonflikte ergeben sich jedoch, wenn staatliche Maßnahmen zum Schutz der IuK-Netze sowie zur Aufklärung und Vorbeugung von Cyber Kriminalität Kommunikationsrechte zum Schutz staatlicher Interessen oder individueller Rechte Dritte einschränken. Maßstab für die Auflösung derartiger Zielkonflikte ist das Prinzip der Verhältnismäßigkeit. Maßnahmen zur

Einschränkung der individuellen Kommunikationsrechte sind unverhältnismäßig, wenn sie ungeeignet, nicht erforderlich und unangemessen sind.

- Problematisch sind staatliche Eingriffsmaßnahmen, wenn sie mit kontraproduktiven Nebenwirkungen verbunden sind, die ihrerseits den Schutz der Grundrechte von Bürgern und Wirtschaftssubjekten erheblich gefährden, die sie eigentlich schützen wollen.
  Ein Beispiel: Die Ausrüstung technischer IuK-Anlagen nach den ETSI-Standards mit Schnittstellen für das Überwachen ist eine technische Voraussetzung, um in Deutschland nach den Kriterien des Rechtsstaates des Grundgesetzes Individualkommunikation überwachen zu können. Wird dieselbe Anlagen in ein anderes Land geliefert oder in einem anderen Land hergestellt, dessen Überwachungspraxis den westeuropäischen Maßstäben eines Rechtsstaates nicht genügt, wird nicht nur die Individualkommunikation der Bürger dieser Staaten gefährdet, sondern vor dem Hintergrund der weltweiten Vernetzung auch die der in Deutschland ansässigenBürger und Unternehmen, deren Kommunikation über dieses Land geleitet wird oder die sich in diesem Land befinden und elektronisch miteinander kommunizieren.

- Einen adäquaten Schutz gegen die eben benannten Risiken bieten Verschlüsselungsverfahren in der Hand der Kommunikationspartner. Eine staatliche Einflussnahme auf die Sicherheit verfügbarer Verschlüsselungsverfahren durch rechtliche oder technische („Falltüren, Exportbeschränkungen“) Maßnahmen, gefährdet den Schutz der Grundrechte derjenigen, deren Kommunikation gegen illegitime Eingriffe privater Dritter oder dritter Staaten geschützt werden soll.

Eine Auflösung des Zielkonflikts zu Gunsten der staatlichen Sicherheitsbehörden würde letztlich die Vertraulichkeit der Kommunikation gefährden, die durch Maßnahmen der inneren Sicherheit gerade geschützt werden soll. Eine pragmatische Auflösung des Zielkonflikts wird derzeit international zu Gunsten der Verschlüsselungsfreiheit vorgenommen, weil andernfalls nicht nur die freiheitlichen Rechte, sondern auch die Ausübung der Wirtschaftsfreiheiten der im Inland ansässigen Subjekte erheblich gefährdet wäre (Wirtschaftsspionage). Nach deutschem Verfassungsrecht wäre eine andere Lösung ohnehin unverhältnismäßig, da davon ausgegangen werden kann, dass mit wachsender krimineller Energie und steigenden Gewinnerwartungen (der „organisierten Kriminalität“) auch die Bereitschaft zur Entwicklung und Verwendung verbotener Schutzmaßnahmen steigt.

Maßnahmen der TK-Überwachung sind im übrigen nur zulässig, wenn auch das Verhältnis von Aufwand zu Ertrag Eingriffe in die Telekommunikation Unbeteiligter rechtfertigen kann. Problematisch ist, dass nicht einmal national ausreichende Kenntnisse über Art, Umfang und Ertrag von TK-Überwachungsmaßnahmen im Bereich der Straftatverfolgung bestehen. Bislang hat der Bundestag keinen Wert darauf gelegt, die von ihm beschlossenen Maßnahmen in regelmäßigen Abständen einer kritischen Überprüfung nach Aufwand und Ertrag zu unterziehen. Internationale Übereinkommen über eine derartige Transparenz bestehen nicht.

Privatanschrift: Max-Planck-Str. 2 * 63454 Hanau * Tel.: 06181 / 234 32 Fax: 06181 / 91 93 74

Eine vergleichbare Problematik lässt sich am Beispiel des Rechts auf anonyme bzw. pseudonyme Kommunikation nachvollziehen, kann hier aber nicht näher ausgeführt werden.

Handlungsempfehlung: Den technischen Selbstschutz für elektronische Kommunikation gewährleisten und nicht beschränken. Art, Umfang und Erfolg der Maßnahmen der TK-Überwachung regelmäßig und öffentlich überprüfen. Internationale Verankerung von Kommunikationsrechten.

4.12. Welche Auswirkungen auf Inhalte haben Konzentrationsprozesse bei Herstellern und Medien- und TK-Anbietern ?

Auf die bedrohliche Situation, dass Verwertungsrechte den freeflow of information und damit den politischen Willensbildungsprozess einschränken, ist bereits oben in der Antwort zu Frage 4.1. hingewiesen worden.