Inhaltsverzeichnis

3. Elemente einer akzeptanzstiftenden Internetregulierung
    - Verfassungsrechtliche Grenzen beachten
    - Sachverständigengutachten: beachten - oder widerlegen
    - Gesellschaftlichen Konsens suchen, Abweichungen erklären
    - Pflicht zur Abschätzung der Technikfolgen und sozialen Folgen
    - Innovationsförderung für freiheitsschützende Technologien
    - Kontrolle der Kontrolleure
4. Fazit

IV. Thesen zur Netzpolitik - Netzpolitik als Querschnittsthema und Aufgabe für einen Internetstaatsminister

Epilog Bär/Heckmann

Vorwort der Vorsitzenden des CSU-Netzrates

Sehr geehrte Damen und Herren,
liebe Freundinnen und Freunde,

im Januar 2011 startete die CSU mit dem ersten Netzkongress, an dem das erste Positionspapier des CSU-Netzrates vorgelegt wurde. Wir haben damit einen breit beachteten Erfolg erzielt und ich freue mich über das große Interesse und die vielfache Zustimmung, die die CSU für diese Positionen in der Öffentlichkeit erhalten hat. Im Verlauf der letzten 14 Monate hat sich diese Aufmerksamkeit, die der **Netzpolitik** als **Querschnittsthema** entgegen gebracht wird, weiter erhöht. Die anstehenden Aufgaben, von Sicherheitsfragen über das Urheberrecht bis hin zur Medien- und Informationskompetenz, sind vielfältig. Deshalb legt der CSU-Netzrat nun das zweite Positionspapier vor.

Sarkozys Bestrebung, „das Internet zivilisieren" zu wollen, fand breiten Diskurs. Ohne das Internet geht heute (fast) nichts mehr. Innerhalb weniger Jahre hat sich das Internet zum **wichtigsten Informations-, Kommunikations- und Unterhaltungsmedium für Jedermann** entwickelt und ist aus unserem Alltag – v.a. aber auch aus unserem Berufsleben - nicht mehr wegzudenken. Das Netz ist eine Bereicherung für unser Leben und ist so, wie es sich entwickelt hat und jetzt jedermann zur Verfügung steht, ein Symbol für die **persönliche** aber auch **sozialphilosophische** und **verfassungsrechtlich verankerte Freiheit** in unserer Gesellschaft.
Ich meine: **Das Internet muss ein Ort der freien Entfaltung persönlicher, wirtschaftlicher und politischer Interessen bleiben.**

Warum aber schaffen wir es in den letzten Jahren nicht, wo mittlerweile dem letzten Kritiker klar geworden sein muß, daß er es nicht schaffen wird, das Internet wieder loszuwerden, vor allem über die **Chancen** zu diskutieren, die es unserer **Gesellschaft** bietet? Warum wirft sich jeder Journalist mit größtem Vergnügen auf

jede noch so halbkritische Aussage eines uninformierten Politikers, um jenen dann genußvoll am Nasenring durch die Arena zu ziehen und vorzuführen?

Die Antwort ist einfach. Weil wir längst eine **digitale Spaltung** unserer Gesellschaft haben, die sich ganz unterschiedlich auswirkt. Wobei die Konfliktlinie entlang derer sich die Spaltung vollzieht eine neue ist. Weder die Generationenfrage, die Stadt/Land-Problematik oder ein politisches Links-Rechts-Schema eignen sich als Erklärung für die digitale Spaltung. Sie verläuft vielmehr zwischen denjenigen, die die Chancen erkannt haben und das Internet als Segen betrachten und denjenigen, die noch im irrigen Glauben leben, das Internet sei nur eine temporäre Modeerscheinung und meinen, daß durch bloßes Ignorieren der Spuk schneller vorbei gehen könnte. Im schlechtesten Fall agieren Schwarzmaler, die im Internet die größte Gefahr der Menschheitsgeschichte sehen und glauben, man könnte es durch Verbote in den Griff bekommen. Im politischen Raum finden sich interessanterweise in jeder Partei Vertreter der einen oder anderen Gruppe.

Der CSU-Netzrat versteht sich als **unabhängiges Expertengremium**, daß wohlüberlegte Positionen zu verschiedenen, das Internet betreffenden, Fragestellungen vorlegt. Klar ist, dass nicht der Anspruch bestehen kann, alle Themenbereiche abzudecken. So steht beispielsweise, neben der Initiative Faires Urheberrecht (www.faires-urheberrecht.de), eine dezidierte Positionierung zur Neugestaltung des Urheberrechts noch aus. Der Netzrat wird sich damit gesondert befassen.

Auch finden sich hier keine neuen Positionen zur Vorratsdatenspeicherung, weil ich mich als Vorsitzende des CSU-Arbeitskreises CSUnet bereits hinlänglich positioniert habe (http://www.csu.de/dateien/csunet/oeffentlich/Antraege/CSUnet_Positionpapier_VDS.pdf).

Der CSU-Netzrat greift mit diesem Papier zwei zentrale Themenkomplexe auf, die ein **freiheitliches** und **faires Internet** ermöglichen: **Bildung** und **Sicherheit**.

Wir wollen damit **Brücken bauen** und integrativ wirken.

Ich setze mich dafür ein, daß die Bürgerinnen und Bürger unseres Landes die Chancen nutzen können – und um die Risiken wissen.

Ich will, daß das Querschnittsthema Internet, das alle betrifft, entsprechend wahrgenommen wird und sehe dem Diskurs über das Für und Wider mit Spannung entgegen.

In diesem Sinn: **Informieren Sie sich! Beteiligen Sie sich! Engagieren Sie sich!**
Denn: Freiheit braucht Fairness. Freiheit bedeutet Verantwortung.

Herzliche Grüße,

Dorothee Bär, MdB
Stv. Generalsekretärin der CSU
Vorsitzende CSU-Netzrat und CSUnet

I. Die spezifische Rolle der Netzpolitik

Der CSU-Netzrat versteht sich als unabhängiges Beratungsgremium verschiedener Experten aus Politik, Wirtschaft und Wissenschaft, das durch Veröffentlichungen und Veranstaltungen Sachverstand, Ideen, Impulse und Visionen für die netzpolitischen Aspekte der unterschiedlichen Ressorts in der Bundes- und Landespolitik einbringen möchte.

Was aber bedeutet eigentlich **Netzpolitik** für uns? Aus unserer Sicht ist Netzpolitik **kein eigenes, abgegrenztes Politikfeld**, sondern eine **Querschnittsmaterie**, die sich quer durch alle politischen Ressorts zieht. Einen Ausschnitt daraus haben wir am Ende dieses Positionspapiers in **10 Thesen** genannt. Dort wird am Ende auch ein eigenes netzpolitisches Amt innerhalb der Bundesregierung gefordert, in Form eines **Staatsminister**s / einer Staatsministerin für **Internet und Digitale Gesellschaft** (in der Denomination in Anlehnung an die gleichnamige Enquete Kommission des Deutschen Bundestages). Ein solches Amt für besondere Aufgaben ist nicht gleichbedeutend mit einem Ministerium, hebt sich aber auch von speziellen Ämtern wie dem eines CIO oder Datenschutzbeauftragten ab. Ein eigenes Internetministerium wäre vor die Frage gestellt, wie sich dieses Ressort von den anderen Ressorts abgrenzt. Die Existenz vieler drängender Herausforderungen, die das Internet mit seinen technischen Neuerungen, wirtschaftlichen Implikationen und sozialen Folgen aufwirft, ändert nichts an der Zuständigkeit und Verantwortung der einzelnen Ministerien für ihre jeweiligen politischen Aufgaben.

Netzpolitik trägt dem Umstand Rechnung, dass es um eine sehr komplexe und dynamische Materie mit einem dezidierten Technikbezug, neuartigen Querbezügen, langfristigen Folgenabschätzungen, grundlegenden Wertungsfragen und neuen Aktions-, Reaktions- und Beteiligungsformen geht, für deren vollständige Durchdringung den Ressorts vielfach Zeit und Ausstattung fehlt. Vor allem aber sind diese Ressorts in festen Zuständigkeitsgrenzen verhaftet, die eine übergreifende Politikgestaltung erschwert. Der CSU-Netzrat greift dieses Phänomen auf und versteht

sich als **Berater** und **Ideengeber** der Ressorts. Dabei macht er sich die Netzwerke zunutze, die seinen Vertretern aus Politik, Wirtschaft und Wissenschaft zur Verfügung stehen. Aber auch eine transparente Rückbindung an die Bürgerinnen und Bürger, die sich ihrerseits über die sozialen Netzwerke, Blogs, Foren und auch E-Mails einbringen, gehört zum Selbstverständnis des CSU-Netzrates.

Der alljährliche Netzkongress zeigt die Offenheit dieser Diskussion, die auf faire Weise zur kritischen Reflexion der vorgestellten Positionen beiträgt. Dabei kann schon aus Kapazitätsgründen immer nur ein kleiner Ausschnitt thematisiert werden. Das betrifft dieses Mal die Themen Bildung und Sicherheit.

II. BILDUNG mit Hilfe eines freien und fairen Internets

Innerhalb weniger Jahre hat sich das Internet zum **wichtigsten Informations-, Kommunikations- und Unterhaltungsmedium** für Jedermann entwickelt. Wir müssen dafür Sorge tragen, dass die Bürger fit gemacht werden im Umgang mit den neuen Medien und der stetig wachsenden Menge von Informationen. Wir plädieren ausdrücklich dafür, die **Medien- und Informationskompetenz** auszuweiten und freien Zugang zu Wissen als staatlichen Kulturauftrag im Internet zu verstehen. Denn: Wenn Menschen gelernt haben, verantwortungsvoll und fair mit anderen umzugehen, bedarf es weniger Regeln. Gerade bei Jugendlichen wird Medienerziehung zu einem immer wichtigeren Gebiet. Medienkompetenz ist der „**edukative Rechtsschutz**" für das digitale Zeitalter. Inbegriffen sind hier die umfassende Vermittlung von IT-Kompetenz durch Gesellschaft, Staat, Schule und Familie, sodass das Internet ganz von alleine zur „**vierten Kulturtechnik**" nach Rechnen, Schreiben und Lesen wird. Es ist unsere Aufgabe, nicht nur die junge Generation, sondern alle Bürger besser für den Umgang zu schulen, damit sie aus den angebotenen Informationen auch die richtigen Schlüsse ziehen kann. Medien- und Informationskompetenz ist Wissen. Und Wissen ist der beste (Daten-) Schutz.

Um Freiheit und Fairness im Netz zu gewährleisten, müssen wir den Menschen aller Altersgruppen ihren Vorkenntnissen und Lebensrealitäten entsprechend die **Fähigkeit zur Eigenverantwortung** vermitteln. Eigenverantwortliches Handeln steht bei uns auch im Netz im Mittelpunkt menschlichen Miteinanders. Nur wer das Netz versteht und die Folgen seines Handelns richtig einschätzen kann, kann die Chan-

cen wahrnehmen und davon beruflich wie privat profitieren. Mit den unzähligen Möglichkeiten des digitalen Alltags erhöhen sich auch die Anforderungen an das Bewusstsein und Selbstverständnis der Userinnen und User.

Statt Freiheit im Internet einzuschränken, sprechen wir uns dafür aus, den Menschen die Kompetenzen zu vermitteln, verantwortungsvoll und (selbst-) bewusst mit dieser Freiheit umzugehen.

1. Medien- und Informationskompetenz als Hüter der Freiheit im Netz

Die digitale Welt bietet ganz neue Möglichkeiten der Partizipation für Bürgerinnen und Bürger: Beispielsweise wird sowohl der politische Meinungsbildungsprozess erleichtert als auch die Möglichkeit, sich über die Arbeit der Regierungen zu informieren. E-Government und Open Government bieten den Menschen an, Behördengänge online zu tätigen oder sich direkt an kommunalen Projekten zu beteiligen und einzubringen. Nur wenn die Nutzer die technischen wie persönlichen Voraussetzungen erfüllen können, stärkt das Internet damit demokratische Prozesse und vereinfacht die Beteiligung der Bürgerinnen und Bürger auf allen Ebenen.

Soziales Engagement, beispielsweise ehrenamtliche Tätigkeiten, auf deren weite Verbreitung wir besonders stolz sind, werden durch den Einsatz des Internets erheblich erleichtert. Organisatorisch wie in Belangen der Öffentlichkeitsarbeit, eröffnen sich hier Chancen, die ohne erheblichen finanziellen und personellen Aufwand früher nicht denkbar gewesen wären.

Politische Partizipation und soziales Engagement im Netz sind unterdessen nur wirkungsvoll, wenn die Menschen, die sich auf diese Weise für die Belange der Gemeinschaft einbringen möchten, Informationen im Internet sinnvoll gewinnen und bewerten können, Online-Kommunikation sicher pflegen und die Möglichkeiten digitaler Einflussnahme kennenlernen. Deshalb ist es wichtig, möglichst vielen Menschen Medien- und Informationskompetenz zu vermitteln. Selbstbestimmtes und selbstbewusstes Handeln der Internetnutzer ist ein Garant für Freiheit.

2. Schutz und Verantwortung der Internetnutzer

Das Bundesverfassungsgericht hat in seiner Entscheidung zur Online-Durchsuchung darauf hingewiesen, dass die IT- und Internetnutzer in einem besonderen Maße schutzbedürftig sind. Zwar hat der Staat einen gewissen Gestaltungsspielraum bei der Realisierung dieser Schutzpflicht. Diesen würde er aber verletzen, wenn er überhaupt nichts unternehmen würde, um die Nutzer in die Lage zu versetzen, das Internet eigenverantwortlich mit einem Mindestmaß an Sicherheit und Vertraulichkeit zu nutzen. Diese **Mindestsicherung** gelingt etwa im Rahmen solcher Bildungskonzepte, wie sie im Folgenden in diesem Positionspapier skizziert werden. Dass der Staat wiederum keine Garantien dafür abgeben kann, dass der Einzelne nicht auch Risiken bei der Internetnutzung ausgesetzt ist, versteht sich von selbst. Neben staatlichen Schutzpflichten und einer etwaigen Produkthaftung der IT-Hersteller und Dienstleister ist auf die Eigenverantwortung des Nutzers hinzuweisen.

Informationskompetenz

Im digitalen Zeitalter kann man in der Regel in Sekundenschnelle an jede erdenkliche Information gelangen. Open Data und Open Source – Projekte katalysieren diese Entwicklung und offenbaren den Schatz am Wissen der Welt für nahezu alle Bürgerinnen und Bürger. Informationen und Meldungen gelangen nahezu ohne Verzögerung zu den Usern und werden nicht mehr ausschließlich von den klassischen Gatekeepern produziert und verbreitet, sondern auch von den Usern selbst generiert. Sender und Empfänger überwinden jede Distanz in Bruchteilen einer Sekunde - ein unschätzbarerer Mehrwert moderner Kommunikation. Die Nutzer müssen dabei aber gute von schlechter, glaubwürdige von unglaubwürdiger Information unterscheiden und die Verlässlichkeit einer Quelle einschätzen können. Ebenso ist es notwendig Fähigkeiten zu vermitteln, den eigenen Informationsbedarf zu erkennen, Informationen zu lokalisieren, selektieren sowie organisieren und letztendlich in Wissen zu verwandeln.

Diskussionen um eine Reformierung des **Urheberrecht**s zeigen, dass der Gesetzgeber unter **Berücksichtigung** möglichst aller **Interessenvertreter** die Rahmenbedingungen liefern muss, die den modernen Lebensgewohnheiten entsprechen. Zudem muss gewährleistet werden, dass alle Bürgerinnen und Bürger die gleichen Möglichkeiten haben, online an Informationen und Content zu kommen und die Netzneutralität garantiert werden kann. Das Internet gehört für uns zur Grundversorgung wie Strom und fließend Wasser.

Verantwortungsvoller Umgang mit neuen Technologien zeigt sich aber nicht nur bei der sicheren elektronischen Kommunikation oder dem fairen Zugang zu Informationen für Alle. Es geht auch darum, die Informationen richtig zu verarbeiten. Wann ist die Grenze zur informationellen Überflutung erreicht und wie ordnet man wertvolles von weniger wertvollem Wissen? Aber auch: wie viel an Mediennutzung mutet man sich zu? Nur wer sich sicher im Netz bewegt, kann einschätzen, worauf er achten muss, um einer Internet- und Mediensucht vorzubeugen. Dazu ist es nötig, das **Internet nicht** als eine **Parallelwelt** mit eigenen Gesetzen wahrzunehmen, sondern es sinnvoll und selbstverständlich in den Alltag zu integrieren. Online und Offline ergänzen sich gegenseitig und nur wenn man mit dieser Tatsache umgehen kann, stehen beide im richtigen Verhältnis zueinander. Wir müssen dafür Sorge tragen, dass der unschätzbare Nutzen des Internets erhalten und nicht zu neuen Abhängigkeiten führt.

Nur, wenn man die Antworten auf diese Fragen kennt, ergibt sich aus den technischen Möglichkeiten auch ein gesellschaftlicher Mehrwert. Dabei muss der freie Zugang zu Informationen ebenso gewährleistet, wie praktikable und verständliche Regelungen zur Weiterverarbeitung und Verbreitung der Inhalte geschaffen werden.

3. Schule2.0 und Lehrerbildung

Schule

Heute ist das Internet wesentlicher Bestandteil der Schule und muss daher auch als Kernkompetenz angesehen werden. Die Vermittlung von Medien- und Informationskompetenz muss deshalb bereits möglichst früh beginnen, sich aber immer den Bedürfnissen des jeweiligen Alters anpassen. Das Internet muss fest und nachhaltig in den Schulalltag integriert werden.
In einem **eigenen Schulfach** sollen die Grundlagen gelehrt werden. Hier geht es darum, die Möglichkeiten des Internets aufzuzeigen und dabei darauf hinzuweisen, welche Gefahren und welche Chancen und Vorteile damit verbunden sein können. Den Schülern muss zum einen eine **grundsätzliche Sensibilität** im Umgang mit ihren persönlichen Daten gegeben und zum anderen ein **digitaler Instinkt** vermittelt werden, der seriöse von unseriösen Inhalten unterscheidet. Dazu gehört auch der geschulte Umgang mit Computertauschbörsen und die Einbeziehung externer Experten. Tutoringmodelle (unter Gleichaltrigen) unterstützen den versierten Umgang mit dem Netz.

Es genügt allerdings nicht, das Thema „Internet" auf eine Schulstunde zu reduzieren, quasi als „Feigenblatt". Dies gelingt einerseits durch den schulischen Einsatz des Internets als Informations- und Kommunikationsquelle, so wie das bereits an den meisten Universitäten praktiziert wird und auch an bayerischen (Pilot-) Schulen zum Beispiel mit einem Online-Portal geschieht (Up- und Download von Schulmaterialien, kollaborative Arbeit unter Mitschülern, Online-Vertretungsplan, Diskussionsforen etc.). **Schulinterne Netzwerke** erleichtern den Informationsfluss zwischen Schule und Schülern ebenso wie zwischen Schule und Eltern. Andererseits kann man inhaltliche Themen der digitalen Gesellschaft in zahlreichen Schulfächern (wie Deutsch, Englisch, Sozialkunde, Informatik, Recht und Wirtschaft etc.) an passenden Stellen einbinden. Wenn man bedenkt, wie viele Schulstunden kurzfristig ausfallen und in denen Schüler mangels adäquater Vertretung zu „Eigenarbeit" angehalten werden: Dort könnte ein Konzept zur gemeinsamen Erarbeitung von Internetthe-

men greifen, dass jede zur Aufsicht eingesetzte Lehrkraft mit geringer Vorbereitung anzustoßen und zu koordinieren vermag. Der Sachverstand geht hier nämlich zu einem großen Teil von den Schülern aus.

Dass ein **Verbot von Smartphones** und ähnlichen Geräten auf dem Schulgelände als abzuschaffender Anachronismus zu betrachten ist, verstehen wir als Selbstverständlichkeit. Zwar erlaubt Art. 56 Abs. 5 Satz 1 BayEUG die Nutzung („Einschaltung") von Mobilfunkgeräten und digitalen Speichermedien zu Unterrichtszwecken. Dies ist aber keineswegs im Schulalltag angekommen. Dort ist nach wie vor pauschal von Handyverboten die Rede, die Erlaubnis wird kaum thematisiert, geschweige denn genutzt. Wir müssen aber in unserer Gesellschaft dahin kommen, dass die Chancen dieser Geräte vor allem unter Lern- und Kommunikationsgesichtspunkten gesehen wird und lediglich Mißbrauch unterbunden wird, und zwar im Rahmen eines umfassenden IT-Nutzungskonzepts unter fachlichen und pädagogischen Gesichtspunkten, nicht einfach durch Verbote. Darüber hinaus ist Art. 56 Abs. 1 Satz 3 BayEUG („Bei Zuwiderhandlung kann ein Mobilfunktelefon oder ein sonstiges digitales Speichermedium vorübergehend einbehalten werden.") vor dem Hintergrund der Rechtsprechung des Bundesverfassungsgerichts verfassungsrechtlich problematisch, zumindest aber restriktiv anzuwenden: Die Vorschrift betrifft nicht nur „Telefone", sondern mit den heutigen Smartphones umfassende Speichermedien, auf denen private E-Mails, SMS, Fotos, Videos, Kalendereinträge, Applikationen sozialer Netzwerke u.v.a.m. gespeichert sind, die dem Kernbereich privater Lebensführung und damit Art. 1 Abs. 1 iV.m. Art. 2 Abs.1 GG zuzuordnen sind. Beim Einzug und der Aufbewahrung solcher Geräte muss gleichermaßen sichergestellt werden, dass ein Zugriff auf diese Inhalte ausgeschlossen ist.

Durch digitale Medien werden **Lerninhalte** anschaulicher und dadurch besser verständlich. Die Schülerinnen und Schüler erhalten eine intensivere Beziehung zu den Inhalten, da sie durch den Einsatz moderner Medien einen praktischeren und unmittelbaren Zugang erhalten. Die Vielzahl an Möglichkeiten des Umgangs mit den Lernmaterialien und der zu lernenden Materie erhöht die Kreativität und wirkt sich

auf die Innovationsfähigkeit der jungen Menschen aus. Außerdem bietet sich die Möglichkeit, besser auf individuelle Fähigkeiten und ein entsprechendes Lerntempo Rücksicht zu nehmen.

Durch den Einsatz von digitalen Schulbüchern werden Aktualität und die Vollständigkeit der Lernmittel gewährleistet und Qualitätsverlust durch Abnutzung der Lernmittel wird minimiert. Hohe Anschaffungskosten für Bücher und Ähnliches werden damit vermieden und es führt zu einer Entlastung der Eltern wie der Schulen. Der sowohl physische wie auch psychische Vorteil, Kindern stets aktuelle Lernmittel zur Verfügung zu stellen statt sie mit antiquaren Schulbüchern auszustatten, darf hierbei nicht unterschätzt werden. Der Netzrat vertritt daher die pointierte Forderung: **Für jedes Kind einen Tablet-PC**. Zeitpunkt und Umfang für die Realisierung dieser Forderung sind im Kontext eines umfassenden Bildungs-IT- und Schulmodernisierungskonzepts mit Finanzierungsplan zu ermitteln, bei dem die heutigen Kosten für Schulbücher und sonstige Lernmaterialien, aber auch die Vorteile einer Effektuierung der Schulverwaltung zu berücksichtigen und gegenzurechnen sind.

Um die neuen Medien und technischen Geräte sinnvoll einsetzen zu können, sind auch hier entsprechende **urheberrechtliche Vereinfachungen und Anpassungen** von Nöten, um auch den Lehrerinnen und Lehrern die Sicherheit zu geben, Lerninhalte digital vermitteln zu können, ohne sich in rechtlichen Grauzonen zu bewegen. Darüber hinaus halten wir es für unerlässlich, dass z. B. Kinderlieder, die der sprachlichen wie räumlichen Verankerung in der Heimat dienen, GEMA-frei für den Gebrauch in Kindertagestätten, Kindergärten und Schulen vervielfältigbar sind.

Um die Schulen entsprechend mit den nötigen technischen Geräten auszustatten, sind Finanzierungsmodelle zu schaffen. Es sind, neben dem staatlichen Engagement, auch Modelle denkbar, die die freie Wirtschaft integrieren, wenn es beispielsweise um die Frage nach der Ausstattung der Schülerinnen und Schüler mit mobilen Endgeräten geht.

Lehrerbildung

Nicht nur Schülerinnen und Schüler müssen im Hinblick auf das digitale Zeitalter bestens vorbereitet sein, sondern auch die Lehrerinnen und Lehrer, in deren Kompetenz es fällt, zu entscheiden, wann, wie, welche und in welchem Maße digitale Lernmittel im Unterricht zum Einsatz kommen. Neben dem eigenen Schulfach muss das Internet fächerübergreifend eingesetzt und als selbstverständliche Arbeitsmethode angesehen werden.

Lehrerinnen und Lehrer müssen um den **digitalen Alltag** Ihrer Schülerinnen und Schüler wissen und sich im Bereich Social Media auskennen, um beispielsweise in Fällen von Cybermobbing eingreifen oder zumindest als Vertrauensperson beratend agieren zu können.

Die Gegebenheiten einer digitalen Welt müssen auch in der **Aus- und Weiterbildung** der Lehrer ihren Niederschlag finden. Dabei ist wichtig, zum einen selbst eine umfassende Medien- und Informationskompetenz zu erlangen und diese zum anderen entsprechend vermitteln zu können. Es ist darauf zu achten, dass Lehrerinnen und Lehrer immer wieder an Weiterbildungsmaßnahmen teilnehmen, damit sie den Neuerungen der schnelllebigen digitalen Welt gewachsen sind und diese für sie ebenso selbstverständlich werden, wie für die Schülerinnen und Schüler.

Neue Lehr- und Lernkonzepte können den gewandelten Verhältnissen Rechnung tragen, nach denen Schüler in IT-Fragen oftmals ein besseres Wissen und eine größere Erfahrung haben als ihre Lehrkräfte. Bestimmte Fertigkeiten und Inhalte können auf diese Weise gemeinsam erarbeitet werden. Während die Schüler ihr technisches Wissen einbringen, werden die Lehrkräfte mit ihrem analytischen Verstand, Lebenserfahrung und allgemeinem Problembewusstsein punkten können. Ein solcher Unterricht „auf Augenhöhe" wird nicht nur effektiver sein als Frontalunterricht, er dürfte von den Schülern auch besser akzeptiert werden. So verbinden sich Technologien und Werte.

Eigenmotivation

Die Vermittlung von Medien- und Informationskompetenz fordert auch die **Menschen aller Altersgruppen**. Wir müssen den Bürgerinnen und Bürger verdeutlichen, dass sich auch die digitale Welt immer weiter entwickelt und es neben Eigenverantwortlichkeit auch einem gewissen Maß an Eigenmotivation bedarf, sich selbst immer wieder weiter zu bilden und sich auf Veränderungen und Neuerungen in einer schnelllebigen Welt einzulassen.

Unser Ziel ist es, durch die Vermittlung von Medien- und Kommunikationskompetenz an alle Bevölkerungsgruppen die sog. „**Digitale Spaltung**" zu überwinden und die Menschen an den Chancen des digitalen Zeitalters gleichermaßen teilhaben zu lassen. Es darf in unserer Gesellschaft keine Benachteiligungen geben.

Umfassende Vermittlung

Kinder, Eltern und Großeltern, sie alle müssen mit der nötigen Medien- und Informationskompetenz ausgestattet sein. So ist es unerlässlich, dass Eltern **den digitalen Alltag ihrer Kinder verstehen** und sie bereits im Vorschulalter auf den Umgang mit modernen Medien vorbereiten und sie begleiten. Die Frage, welche Lerninhalte wann und in welchem Maße außerhalb der Schule zum Einsatz kommen sollten, darf nicht der Staat, sondern müssen die Eltern (auch auf Basis von Expertenurteilen) entscheiden können.

Nur so erhalten wir ein **hohes Bildungsniveau**, eine **hohe Wettbewerbsfähigkeit** und ein **Höchstmaß an Freiheit**. Auf all dies können und wollen wir keinesfalls verzichten.

4. Wirtschaft und Bildung im digitalen Zeitalter

Um in der modernen Arbeitswelt bestehen zu können, muss man beruflich wie privat mit dem Internet umgehen können. Die Aufhebung der Trennung zwischen Online und Offline ist inzwischen hinlänglich bekannt. Kommunikation, Projektpla-

nung und Informationssuche ist in der Arbeitswelt selbstverständlich und findet vor allem online statt. Auch hier wird von den Betreffenden Eigenverantwortlichkeit erwartet. Viele Unternehmen erarbeiten Social Media-Richtlinien für Ihre Mitarbeiterinnen und Mitarbeiter und schließen damit diese Form des Austauschs und der Kontaktpflege ganz bewusst nicht aus. Die Zeiten, in denen Arbeitgeber das Internet als Privatangelegenheit angesehen haben, sind vorbei. E-Recruiting ist an der Tagesordnung; das Wissen um die Regeln des Netzes werden als selbstverständlich betrachtet.

Nur wenn es uns gelingt, die Grundlage zu schaffen, die Schüler, Studenten oder Auszubildende dafür benötigen, sich im Bereich IT zurecht zu finden, können sich auch Experten und Fachkräfte ausbilden und unsere wirtschaftliche Stärke sichern und ausbauen. **Wettbewerbsfähigkeit** zu erhalten, ein wirtschaftspolitisches Kernziel, gelingt nur, wenn man die **nötige Infrastruktur** schafft und die Bürgerinnen und Bürger mit dem nötigen Grundwissen ausstattet, das sie dann zur **Expertise** ausbauen können. Gleichermassen müssen wir dafür Sorge tragen und Konzepte entwickeln, wie auch ältere Arbeitnehmerinnen und Arbeitnehmer mit den neuen Technologien arbeiten können; sofern sie dies nicht bereits tun. Wir dürfen nicht zulassen, dass der unglaubliche Wert dieser älteren Generationen der Wertschöpfung verloren geht, nur weil sie keine „digital natives" sind.

Nicht nur die Vermittlung der nötigen Kompetenzen, sich in der digitalen Welt sicher zu bewegen, die als solche nicht mehr alleine existiert, sondern ein Teil des privaten wie beruflichen Alltags ist, gehört zu den Kernaufgaben der Politik. Auch die **Erfüllung der technischen Voraussetzungen** ist eine Hauptaufgabe von Staat und Regierung. Die Versorgung der Menschen mit der nötigen Infrastruktur, der **flächendeckende Breitbandausbau**, die **Sicherung und Gewährleistung der Netzneutralität**, all das sind unverzichtbare Bausteine, die uns helfen, Brücken zu bauen, um die „Digitale Spaltung" zu überwinden. Erst wenn die Menschen auch die technischen Mittel haben, können sie das nötige Wissen erlangen und von den Möglichkeiten des digitalen Zeitalters profitieren.

Wir müssen sicherstellen, dass eine lückenhafte Internetversorgung nicht zum Standortnachteil wird.

Kleine und mittelständische Unternehmen, tragende Säulen unserer Gesellschaft, dürfen in ihrem Unternehmertum nicht dadurch eingeschränkt werden, dass ihnen die technischen Voraussetzungen fehlen. **Forschung, Innovation und Unternehmergeist** sind nur dann möglich, wenn sie sich frei von infrastrukturellen Einschränkungen entfalten können. Abwanderungen von etablierten Unternehmen aufgrund von **Fachkräftemangel** im IT-Bereich oder aufgrund fehlender Internet- und Breitbandversorgung müssen wir mit aller Kraft und v. a. zügig entgegenwirken.

Für die Arbeitnehmerinnen und Arbeitnehmer ergeben sich Möglichkeiten, die nur durch die Integration des Internets in den Arbeitsalltag denkbar sind. Projektplanung und interne Kommunikation ebenso wie die Kommunikation mit Geschäftspartnern und Kunden werden orts- und zeitungebunden. So werden Arbeitszeiten flexibler und Homeoffice-Lösungen erleichtern beispielsweise für Väter und Mütter gleichermaßen die Vereinbarkeit von Familie und Beruf.

5. Journalismus2.0 und die Rolle der Medien

Im Grundgesetz (Art 5.) heißt es: "Jeder hat das Recht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten. Die Pressefreiheit und die Freiheit der Berichterstattung durch Rundfunk und Film werden gewährleistet. Eine Zensur findet nicht statt."
Dies gilt selbstverständlich und uneingeschränkt auch im digitalen Zeitalter (*Christoph Neuberger* hat dies in *„Journalismus im Internet"* (Media Perspektiven 1/2012) betrachtet). Man kann sogar sagen: Mehr denn je - wie die weltweiten politischen Umwälzungen in der arabischen Welt des letzten Jahres gezeigt haben. Jeder weiß um die Rolle von Social Media und der Möglichkeit der anonymen Meinungsäußerung und ihrer Wirkung.

Das bisher gültige **Kommunikationsmodell hat sich verändert** und entwickelt sich immer weiter: Die früheren Empfänger sind heute nicht mehr nur Rezipienten, sie sind gleichzeitig auch die Sender, Produzenten von Nachrichten und Meldungen. Sie senden Fotos, Kommentare und Statements in die Welt und geben sich nicht mehr mit der Rolle der reinen (Informations-) Konsumenten zufrieden.

Die klassischen Medien und der Journalismus müssen sich auf diese neuen Gegebenheiten besser und schneller einstellen: Die isolierte Forderung nach einem **Leistungsschutzrecht** zum Beispiel, also die Suche nach einfachen Lösungen und bequemer Sicherung des Status Quo mit Hilfe des Gesetzgebers, ist der falsche Weg. Stattdessen ist Kreativität im Hinblick auf neue Geschäftsmodelle und einer modernen Inhaltspräsentation gefragt. Informationsanbieter wie Journalisten und Verlage müssen die Kanäle, über die sie Ihre Zielgruppe erreichen können, zu nutzen wissen. Der Dialog mit dem Nutzer ist dabei eine entscheidende Komponente.

Gerade jüngere Internetnutzer (zwischen 14 und 19 Jahren) entwickeln aufgrund ihrer Mediensozialisation **andere Ansprüche an den Journalismus** im Allgemeinen oder journalistische Berichterstattung im Speziellen. Ansprüche wie Aktualität, Sachlichkeit, Regelmäßigkeit und Glaubwürdigkeit sind im Hinblick auf Medienberichterstattung nicht neu. Sie erlangen aber durch das Internet eine neue Dimension, können Informationen doch nun viel schneller eruiert und verbreitet, aber auch in effizienter Weise überprüft, verifiziert oder falsifiziert werden, wozu die sog. Schwarmintelligenz bzw. das Crowd Sourcing beiträgt.

Nutzer von Nachrichtenangeboten im Internet legen großen Wert auf **Quellentransparenz** und bewerten bspw. Wikipedia in dieser Hinsicht besser als Presse-Websites. Die Transparenz des Ursprungs einer Information wird auch in Zukunft an Bedeutung gewinnen und sollte daher als wichtiges Qualitätsmerkmal journalistischer Informationen und Websites betrachtet werden.

Weblogs eignen sich besonders für Diskussionen, Twitter für Informationsverbreitung und Beziehungspflege, soziale Netzwerke für beides. Die Nutzungsmotive der einzelnen Plattformen und Netzwerke sollten bei deren Einsatz im Blick behalten werden. Soziale Netzwerke, Weblogs und Twitter sollten nicht als zweite „Verwertungsstation" für bereits publizierte Nachrichten und Informationen genutzt werden, ohne diese erneut medienspezifisch anzupassen und aufzuarbeiten.

Während es Rezipienten immer leichter fällt, gesuchte Informationen im Internet zu finden, wird es für sie zunehmend schwieriger, die **Authentizität und Richtigkeit einer Nachricht** zu bewerten. Dies stärkt den Wunsch nach Transparenz bei der Informationsverbreitung. Da die Komplexität bei der Nutzung von Informationen im Internet aus Sicht der Rezipienten stetig zunimmt, steigt die Bedeutung komplexitätsreduzierender, klarer Nachrichten und Webseiten.

In einer Welt, in der jeder Konsument von Informationen selbst zum Produzenten von Nachrichten wird, müssen wir uns vom gelernten **Selbstverständnis des Gatekeepers** verabschieden. Das Wertegerüst, auf dem Selbstverständlichkeiten wie die Pressefreiheit in ihrer Definition stehen, bleibt unverändert. In vielen Bereichen merken wir aber, dass die Implikationen grundlegender Begriffe sich erweitern und Gesetze auf ihre heutige Tauglichkeit überprüft werden müssen.

Die **Pressefreiheit** bleibt - wie die Freiheit selbst - auch und gerade im Internet unantastbar.

6. Freier und fairer Informationszugang: Mehr Bandbreite!

Eine schnelle Anbindung an das Internet ist in allen Teilen Bayerns eine wesentliche Voraussetzung für Wachstum und Wohlstand in der Zukunft. Die Erfahrung zeigt: Ohne einen breitbandigen Anschluss können Kommunen nahezu keinen Baugrund mehr verkaufen, geschweige denn ein Gewerbeunternehmen ansiedeln. Ist dagegen eine besonders schnelle Verbindung vorhanden, zum Beispiel über ein

Glasfasernetz, werden plötzlich auch Standorte für Unternehmen interessant, die eher abseits der klassischen Verkehrswege gelegen sind. Für viele Kommunen im ländlichen Raum ist dies die Chance, wieder Anschluss an die wirtschaftliche Entwicklung zu finden und attraktive Arbeitsplätze vor Ort zu schaffen. Selbst wenn der Arbeitgeber nicht am Ort ist, erleichtert eine schnelle Internetanbindung gut ausgebildeten Fachkräften, sich außerhalb der Ballungsräume im ländlichen Raum niederzulassen. Darüber hinaus ist auf die zunehmende Verbreitung von Telearbeitsmöglichkeiten hinzuweisen.

Grundrecht auf adäquate Internetnutzung

Der Zugang zu schnellem Internet ist aber nicht nur eine wirtschaftliche Frage. In der modernen Gesellschaft sind mit dem Internet auch unzählige Bildungs- und Teilhabechancen verbunden, von denen kein Mensch ausgeschlossen werden darf. Ein schmalbandiger Zugang, beispielsweise über eine ISDN-Verbindung, schränkt die Nutzung der heute schon im Netz zur Verfügung stehenden Angebote deutlich ein. In absehbarer Zukunft werden viele Medienangebote nur noch mit breitbandigen Verbindungen zu nutzen sein, und das keineswegs nur zu Unterhaltungszwecken. Es geht auch um die Anbindung der Menschen zu den virtuellen Rathäusern und elektronischen Behördenservices (E-Government und Open Government), die Nutzung moderner Gesundheitstechnologien (E-Health) oder die effiziente Steuerung von Verkehr und Energiehaushalten (Smart Traffic, Smart Metering), die zunehmenden webbasierten Bildungsangebote, insbesondere über Lernvideos und Live-Streaming u.v.a.m. Diese überragende Bedeutung einer adäquaten Internetnutzung heute und morgen im Blick, brauchen wir aber kein neues Grundrecht auf Internetnutzung: Es gibt bereits ein solches Grundrecht auf Internetnutzung. Und zwar in Auslegung des Grundgesetzes. Dort sind neben dem expliziten Grundrecht, „seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten" (Art. 5 Abs. 1 Satz 1 GG) zahlreiche Freiheitsrechte (besonders die Berufsfreiheit, aber auch die Eigentumsgarantie, das Recht auf informationelle Selbstbestimmung, der schulische Bildungs- und Erziehungsauftrag sowie weitere politische und soziale Teilhaberechte)

normiert, aus deren Gesamtschau sich eben dieses Grundrecht auf adäquate Internetnutzung ergibt. Daraus ergibt sich zwar kein direkter Anspruch der Bürger auf Finanzierung von Hardware, Software und Services aus öffentlichen Geldern, jedoch eine Infrastrukturschaffungspflicht des Staates mit dezidierten Regulierungsgrenzen (keine Netzsperren, keine Internetnutzungsverbote wie z.B. Three-Strikes-out). Der Staat muss bei der Konkretisierung seines Gestaltungsauftrages der herausragenden Bedeutung der Internetnutzung Rechnung tragen. Er trägt damit eine Mitverantwortung für den Netzausbau.

Flächenland Bayern

In einem Flächenland wie Bayern kann ein rein marktorientierter Ansatz, in dem jeder Netzabschnitt für sich rentabel sein soll, die vollständige Versorgung der Bevölkerung mit breitbandigem Internet nicht leisten. Über 77 Prozent der bayerischen Kommunen haben deshalb zwischen 2008 und 2011 am **Förderprogramm** des Freistaates teilgenommen, um, in Verbindung mit eigenen Mitteln, die Rentabilitätslücke der privaten Unternehmen auszugleichen. Einige Kommunen, wie zum Beispiel die Gemeinde Oberhausen im Landkreis Neuburg-Schrobenhausen, sind sogar einen Schritt weiter gegangen und haben selbst ein Providerunternehmen gegründet und darüber alle Ortsteile mit Glasfaserkabeln erschlossen. An vielen Stellen stehen aber nur Verbindungen in der Größenordnung von 1 Mbit/s zur Verfügung. Das stellt zwar eine gewisse Grundversorgung dar, ist aber bei weitem nicht ausreichend.

Förderung Breitbandausbau

Der Netzrat fordert deswegen die Bundesregierung auf, die Kommunen auch in Zukunft zu fördern, die noch bestehenden Versorgungslücken zu schließen und ein Folgeprogramm aufzulegen, dass den **flächendeckenden Ausbau von Hochleistungsnetzen mit Downloadraten von mindestens 50 Mbit/s bis zum Jahr 2015** als Gegenstand hat. Der bereits heute absehbaren digitalen Spaltung bei den Netzen der nächsten Generation zwischen den Ballungszentren und dem ländlichen Raum muss frühzeitig entgegengewirkt werden.

Der Bund hat mit der jüngsten Novelle des Telekommunikationsgesetzes einige begrüßenswerte Maßnahmen zur Förderung des Breitbandausbaus in die Wege geleitet. Leider wurde versäumt, die Möglichkeit zu schaffen, in unterversorgten Gebieten eine Universaldienstverpflichtung für die Anbieter auszusprechen. Dies sollte nachgeholt werden. Ein breitbandiger Anschluss an das Internet hat heute für viele Menschen einen ähnlichen Stellenwert wie der Anschluss an Strom, Wasser oder Telefon. Das spiegelt sich aber in der Gesetzgebung bisher nicht wieder.

Die vollständige Erschließung Deutschlands mit Breitbandanschlüssen ist eine der großen Infrastrukturherausforderungen unserer Zeit. In einem Flächenland wie Bayern entscheidet sich auch daran die Gleichwertigkeit der **Lebensverhältnisse in Stadt und Land**. Der Bund hat sich richtigerweise dafür in seiner **Breitbandstrategie** ehrgeizige Ziele gesetzt. Er ist jetzt gefordert, die Länder und Kommunen auch finanziell so zu unterstützen, dass sie diese Ziele tatsächlich umsetzen können.

7. Fazit

In Deutschland sind 98 Prozent der Jugendlichen und zwei Drittel der Gesamtbevölkerung online. Das bedeutet aber noch nicht, dass der größte Teil der Bevölkerung bereits heute selbstbewusst, selbstständig und souverän im und mit dem Internet agieren würde. Ganz im Gegenteil: Die im Februar 2012 veröffentlichte DIVSI Milieu-Studie zu Vertrauen und Sicherheit im Internet (https://www.divsi.de/divsi-milieu-studie) unterscheidet insgesamt sieben Internet-Milieus: Die **Digital Natives** mit den Digital Souveränen (15 %), Effizienzorientierten Performern (14 %) und Unbekümmerten Hedonisten (12 %), die **Digital Immigrants** mit den Verantwortungsbedachten Etablierten (10 %) und Postmateriellen Skeptikern (10 %) sowie die **Digital Outsiders** mit den Ordnungsfordernden Internet-Laien (12 %) und den Internetfernen Verunsicherten (27 %). Dieses heterogene Bild unterstreicht die Aufgabe und Herausforderung der (Netz-) Politik, sowohl Chancen- als auch Problembewusstsein zu vermitteln und allen Menschen einen ihren Kenntnissen, Erfahrungen, Einstellungen und Wünschen entsprechenden Zugang zur Digitalen Chancenrepublik

Deutschland zu ermöglichen. Denn das lohnt sich nicht nur, es ist essentiell für Freiheit, Wohlstand und Wohlbefinden in der Informationsgesellschaft des 21. Jahrhunderts.

Kein anderes Medium hat in dieser Schnelligkeit zuvor das Leben der Menschheit so gewaltig verändert. Die **Trennung zwischen realem und virtuellem Leben** wird immer schwieriger und ist bereits heute teilweise **obsolet**. Die innovativen Nutzungsmöglichkeiten des Internets prägen unser Leben und stellen meist eine enorme Bereicherung, Erleichterung oder praktische Hilfe dar. Der virtuelle Raum ist vieles: Weltbibliothek und Jobmaschine, globaler Supermarkt und weltumspannende Versammlungsmeile. Das Internet macht unser Leben vorurteilsfreier und demokratischer.

Das Internet ist ein Gewinn für die Menschheit. Das Internet und seine Chancen sind Megathemen für unsere Gesellschaft. Aufgabe der Politik ist es hierbei, die Rahmenbedingungen zu schaffen, die die Menschen für die Teilhabe benötigen. Ganz konkret heißt das: Medien- und Informationskompetenz vermitteln, Schulen ausstatten und Lehrer ausbilden, Erfordernisse der Wirtschaft in ihrer Vielfalt berücksichtigen und die notwendige Infrastruktur zu schaffen. Auch die Debatte über unseren gesellschaftlichen Blick auf die virtuelle Welt, in der jeder in Freiheit und Fairness von den Chancen profitieren kann, darf dabei nicht zu kurz kommen.

III. SICHERHEIT mit Hilfe eines freien und fairen Internets

Wir sehen die unendlichen **Chancen**, die dieses Medium uns bietet und vergleichen es deshalb gerne mit dem größten Fortschritt in der Geschichte der Menschheit seit Erfindung der Kunst des Buchdruckes. Das Internet bietet neue Möglichkeiten der **Partizipation**. Das Internet bietet **Transparenz**. Das Internet bietet weltweite Kommunikationsmöglichkeiten und prägt unser alltägliches Leben. Aber eben wegen dieser Realität ist das Internet zugleich Tatort, Vertriebskanal für illegale Inhal-

te und immer wieder selbst Angriffsziel. Bei allen Chancen, Vorteilen und Möglichkeiten kann man die **Risiken**, die mit der Internetnutzung (und darüber hinaus: mit der Nutzung von Informations- und Kommunikationstechnologien) verbunden sind, nicht außen vor lassen. Man denke etwa - ohne wertende Reihenfolge - an das Phishing von Kontozugangsdaten, Industriespionage, Ehrverletzungen in den verschiedenen Formen, Mobbing, Stalking, die Verbreitung von rechts- oder linksextremistischer Propaganda, Verbrechensplanung via Webkommunikation, aber auch die Verbreitung von Schädlingen wie Viren und Würmern oder die Botnetzkriminalität, wonach Rechner über Schwachstellen im System „gekapert" werden, um sie zum Beispiel für Spamming oder DOS-Attacken zu missbrauchen. Auch gewisse Formen des „Cyberwar" oder „Cyberterrorismus" werden diskutiert, wenngleich hier zum Teil belastbare empirische Erkenntnisse fehlen.

Die meisten dieser Straftaten gab und gibt es auch ohne das Internet. Das Internet schafft vielfach aber neue Tatgelegenheiten, trägt zur „Modernisierung" der Informations- und Kommunikationsstrukturen krimineller Kreise bei und hat eine größere Reichweite, so dass der Begriff Internetkriminalität durchaus berechtigt ist. Die **Antwort der Rechtsordnung** darf natürlich nicht sein, die Internetnutzung einfach einzuschränken, weil dadurch die überwiegend legitimen, nützlichen Nutzungsformen und die damit verbundenen Chancen und Vorteile leiden würden. Vielmehr besteht die Herausforderung darin, Kriminalität im und über das Internet zu unterbinden, um damit letztlich die Freiheit der Internetnutzer zu gewährleisten. Es soll verhindert werden, dass Menschen Foren fernbleiben, weil sie dort beleidigt oder belästigt werden, oder den Online-Handel meiden, weil sie Angst vor Betrug und Ausbeutung haben. **Der Staat muss gleichzeitig Freiheit und Sicherheit im Internet gewährleisten**. Das kann er aber nur bedingt. Zur Internetsicherheit müssen alle Akteure, Staat, Wirtschaft und Gesellschaft beitragen.

1. Dilemmata

Die Gewährleistung der (inneren) Sicherheit kollidiert mit den Freiheitsgrundrechten. Die zur Sicherheitsgewährleistung berufenen staatlichen Stellen müssen (nicht nur, aber auch) bei der Regulierung des Internets bestimmte Dilemmata auflösen, um den teilweise divergierenden Interessen Rechnung tragen zu können. Sie stehen dabei vor disparaten Herausforderungen: So kommt die aktuelle DIVSI-Studie (https://www.divsi.de/divsi-milieu-studie) zu dem Ergebnis, dass einerseits „fast drei Viertel der deutschen Bevölkerung staatliche Maßnahmen zur Gewährleistung von Sicherheit im Internet" fordern. Andererseits lehnt „die von solchen staatlichen Maßnahmen am stärksten betroffene Gruppe der Digital Natives staatliche Reglementierungen mehrheitlich ab und hat zum Teil kein Verständnis für die Probleme und Bedürfnisse der anderen Bevölkerungsgruppen in Bezug auf das Internet und dessen Nutzung".

Technische Innovationen können auch Kriminalität erleichtern

Politik und Gesellschaft müssen sich darüber bewusst werden, dass das Internet, die Digitalisierung und die Entwicklung innovativer Technologien - neben allen ihren positiven freiheitserweiternden Wirkungen - neue Mittel, Gelegenheiten und Wege für Kriminalität und terroristische Aktivitäten eröffnen. Dieses Phänomen ist nicht neu. Mit der Entwicklung des Automobils ging ebenso dessen Missbrauch einher, seien es die Erleichterung grenzüberschreitenden Menschen- und Drogenhandels oder rücksichtslose Fahrweisen, die auch Menschenleben kosten. Ein freies Internet wird zu einem Teil immer auch ein kriminelles Internet sein, genauso wie Kriminalität und Rechtsverletzungen Teil unserer Lebenswirklichkeit sind. Damit ist das Internet nicht „böse". Es ist nur ein Medium.

Es ist Ausdruck von Freiheit, Menschen in Selbstbestimmung agieren zu lassen. Dass solches selbstbestimmtes Handeln immer nur in **fairer Abgrenzung zu Rechten und Interessen Dritter** erfolgte, mag in der Tendenz erstrebenswert sein; es wäre in dieser Absolutheit aber illusorisch. Was aber erwarten die Menschen: Möchten sie vor diesen Kriminalitätsformen geschützt oder bei ihrer Internetnutzung in Ruhe gelassen werden? Soll der Staat sich einmischen oder heraushalten?

Schutz der Freiheit erfordert auch Eingriffe

Die Debatte um etwaige Eingriffsbefugnisse staatlicher Ermittlungsbehörden ist stark geprägt durch die **Grenzziehung grundrechtlicher Freiheiten** der (unbescholtenen) Bürger, deren **Privatsphäre** durch technische Überwachungsmaßnahmen betroffen ist. Umgekehrt wird seitens der staatlichen Ermittlungs- und Verfolgungsbehörden auch ein großes Maß an Eingriffsbefugnissen verlangt, um bestehenden, aber auch antizipierten, gravierenden Gefahren Herr werden zu können. Ein freies Internet fordert zum Schutz eben jener Freiheit auch staatliche Eingriffe - vor allem gegenüber den tatsächlichen Störern. Wüsste man immer, dass eine belastende Ermittlungsmaßnahme alleine den Täter bzw. Störer trifft, wäre die Akzeptanz solcher Eingriffsbefugnisse wohl sehr hoch: Der unbescholtene Bürger ist nicht betroffen, der Betroffene hat die Ursache des Eingriffs durch seine eigene Tat gesetzt. Es liegt aber im Wesen **polizeilicher Gefahrenabwehr und Strafverfolgung**, dass die Sachverhalte nicht immer eindeutig sind, weswegen zuweilen auch umfangreich ermittelt wird. Würde man etwa einer Anschlagsdrohung nicht nachgehen, weil auch Personen kontrolliert werden müssten, die sich als unschuldig erweisen, könnten die Opfer bzw. ihre Angehörigen ineffizientes Handeln der Behörden beklagen. Das Dilemma – auch und gerade für „Ermittlungen im Netz" – besteht darin, das rechte Maß an „zu viel" und „zu wenig" zu finden: Die **staatliche Schutzpflicht zur Sicherheitsgewährleistung** ist kein Freibrief für unverhältnismäßige Maßnahmen gegenüber Unbescholtenen; einen „Generalverdacht" lehnen über zwei Drittel aller Bundesbürger ab. Genauso wenig rechtfertigt es die **grundrechtlich** geforderte **Freiheitsgewährleistung**, Täter oder Störer zu verschonen. Was erwarten also die Menschen: Möchten sie vor Kriminalität, die im oder über das Internet stattfindet, geschützt oder bei ihrer Internetnutzung in Ruhe gelassen werden? Soll der Staat sich einmischen oder heraushalten?

Anonymität ist notwendig und kritisch zugleich

Staatlichen Zugriffen könnte sich „jedermann" größtenteils dadurch entziehen, dass er digitale Spuren auch dadurch vermeidet oder beseitigt oder deren Ermittlung erschwert, dass er technische Möglichkeiten zur Anonymisierung seiner Inter-

netnutzung wahrnimmt. Eine solche Anonymisierung erschwert auch polizeiliche Ermittlungen. Das kann so weit gehen, dass ein Täter nicht mehr ermittelbar ist, wenn das Einzige, das zu ihm führen würde, die IP-Adresse wäre, die aber entweder gelöscht oder bereits vom Betreffenden verschleiert wurde. Umgekehrt ist Anonymisierung (bzw. Pseudonymisierung) zum Schutz der Privatsphäre zugleich datenschutzrechtlich erlaubt und - für Diensteanbieter - sogar geboten (§ 13 Abs. 6 TMG). Bei bestimmten Diensten (etwa Ärztebewertungen, prekären politischen Meinungsäußerungen oder Suizidforen) ist Anonymität unverzichtbar. So stellt sich die Grundsatzfrage: Wie viel Anonymität braucht, wie viel Anonymität verträgt unsere (digitale) Gesellschaft? Gibt es ein „**Grundrecht auf Anonymität**" und wie weit geht sein **Schutz**? Sollen sich Menschen im Internet völlig anonym bewegen können? Ein letztes Mal: Was erwarten die Menschen? Möchten sie vor Anonymitätsmissbrauch geschützt oder bei ihrer anonymen Internetnutzung in Ruhe gelassen werden? Soll der Staat sich einmischen oder heraushalten?

Das so beschriebene Dilemma ist weder ein Grund gegen, noch einer für die sog. Vorratsdatenspeicherung. Es zeigt nur den Hintergrund auf, vor dem diese politisch hochumstrittene und rechtlich bislang nicht vollständig geklärte Thematik (auch vor dem Hintergrund von iPv6) zu diskutieren ist.

2. „Baustellen" der netzpolitischen Sicherheitsdiskussion

Vor dem Hintergrund der sicherheitspolitischen Herausforderungen zur Bekämpfung von Kriminalität und der beschriebenen Dilemmata ergeben sich mehrere „Baustellen", auf denen Netzpolitik Vorschläge zur **Errichtung einer Sicherheitsarchitektur für ein freies und faires Internet** liefern kann. In all diesen Fällen geht es um bestimmte Instrumente oder Methoden der Kriminalitätsbekämpfung, welche in der Sicherheitspolitik immer wieder genannt oder gefordert werden oder gar bereits zum Einsatz kommen.

Keine Wiederbelebung von Netzsperren

Bereits im ersten Positionspapier des CSU Netzrates 2011 haben wir uns klar gegen Netzsperren ausgesprochen. Sie sind technisch leicht umgehbar und kontraproduktiv. Vor allem sind sie so unverhältnismäßig wie die Verhängung einer pauschalen Ausgangssperre zur Vermeidung von Straftaten im öffentlichen Raum. Wenn dieses Instrument danach nicht einmal zur Bekämpfung eines Verbrechens wie der Dokumentation von Kindesmissbrauch durch Bilder und Videos im Internet taugt, gilt im **Erst-recht-Schluss: Keine Netzsperren** gegen **Urheberrechtsverletzungen** oder andere **Gesetzesverstöße**. Deren Unzulässigkeit haben mittlerweile auch der Europäische Gerichtshof und weitere Gerichte bestätigt.

Damit wird das darin liegende Unrecht nicht gutgeheißen. Es wird nur der Blick auf wirksamere und besonders verhältnismäßige Methoden der Kriminalitätsbekämpfung gelenkt, wie etwa das Löschen krimineller „Angebote", effektive Auswertung öffentlich zugänglicher Informationen oder das direkte Vorgehen gegenüber den Tätern.

Verfassungswidrigkeit von „Three Strikes out"

In ähnlicher Weise lehnen wir auch den Plan ab, einer zweifachen erfolglosen Ermahnung die **Sperrung** des **Internetzugangs** für einen **Rechtsverletzer** folgen zu lassen. Auch dieses Instrument ist unverhältnismäßig und letztlich untauglich. Wenn das Verbot zur Nutzung eines bestimmten Anschlusses (Rechners) ausgesprochen, die Leitung etwa beim heimischen Rechner gekappt wird, sind zugleich „Unschuldige" mitbetroffen, weil eben auch Familienangehörige Zugriff haben. Wie will man eine solche „Sippenhaft" rechtfertigen? Kinder könnten nicht mehr für die Schule recherchieren, günstiges Online-Shopping zur Entlastung der Familienkasse wäre gestrichen. Bezieht man ein solches Internetnutzungsverbot hingegen alleine auf die Person: Dann müsste man jeglichen Kontakt des Betroffenen zu Online-Rechnern unterbinden. Man müsste quasi „verbieten", dass sich der Delinquent im Internetcafé im Urlaub, bei Freunden oder im Hotel ins Internet einloggt. Streng genommen dürfte er nicht einmal eine Fahrkarte an einem mit dem Bahnserver verbundenen Automaten im Bahnhof ziehen, soweit er damit „das Internet nutzen"

würde. Überdies ist es verfassungsrechtlich fragwürdig, wenn der Betroffene dann auch nicht mehr die Internetfunktion des „File Transfer Protocol" nutzen dürfte, um etwa Geschäftsdaten zu transferieren.

Unter den Bedingungen einer weitgehenden (auch politisch erwünschten) Durchdringung von Staat, Wirtschaft und Gesellschaft mit Internetdiensten ist es unverständlich, deren Nutzung pauschal verbieten zu wollen. Nimmt man in naher **Zukunft das Internet der Dinge**, die elektronische Vernetzung von Alltagsgegenständen hinzu, wäre für den Adressaten eines Internetnutzungsverbots das digitale Leben (Smart Health, Smart Metering etc.) vorübergehend beendet. Eine solche Sanktion ist keineswegs vergleichbar mit einem Fahrverbot oder etwa einem Gewerbeverbot, weil diese – anders als die Internetnutzung in der Informationsgesellschaft – eine nur sektoriell begrenzte Wirkung haben.

Defizite bei ACTA

Wie verfehlt eine streng sanktionsorientierte Regulierung (gerade zur Durchsetzung des Urheberrechts) sein kann, zeigt auch die Entwicklung bei ACTA, dem internationalen Handelsabkommen zur Bekämpfung von Urheberrechtsverletzungen und Produktpiraterie. Auch ACTA ist im Kontext der (Rechts-) Sicherheit zu betrachten, der Frage also, wie eine Rechtsordnung mit Rechtsverletzungen umgeht. Wir lehnen das Abkommen in seiner jetzigen Form ab, obwohl es inhaltlich weitestgehend dem entspricht, was im deutschen Urheberrecht schon heute geregelt ist. Es weist nämlich drei erhebliche Defizite auf:

Zunächst beim **Regelungsgegenstand**: Das Urheberrecht ist als magna carta der Informationsgesellschaft keine politisch beliebige Verfügungsmasse. Die Internetnutzer, und das ist in naher Zukunft jedermann, haben ein spezifisches und berechtigtes Interesse daran, mitzuentscheiden, wie Informationen geschützt, zugänglich gemacht und verbreitet werden. Es gibt ein dringendes Interesse an einer **baldigen und vor allem fairen Urheberrechtsreform**, die den gewandelten technischen und sozialen Bedingungen, der Rolle des Urhebers mit den neuen Vertriebswegen und

Wertschöpfungsketten, dem Phänomen einer „**Abmahnindustrie**" und den **begrenzten Kontrollmöglichkeiten der Provider** Rechnung trägt. Ansätze gibt es hierzu bereits viele, wie etwa die vielen Ideen für ein neues Urheberrechtskonzept oder die Initiative www.faires-urheberrecht.de. Das erste Defizit liegt bei ACTA schlicht darin, dass es dieser Herausforderung überhaupt keine Rechnung trägt. Statt einer neuen **Austarierung der Interessen der Urheber, Rechteverwerter und Nutznießer** bleibt es bei dem überkommenen Schutz-und-Schranken-Modell, für das sich kein gesellschaftlicher Konsens mehr findet.

Des Weiteren bei der **Regelungsintention**: Der eigentliche Zweck des Abkommens liegt in einer Harmonisierung der Schutzstandards mit einem Schwerpunkt auf (rechtsstaatlichen) Zwangsmaßnahmen. Das genügt angesichts technischer Umgehungsmaßnahmen oder einer Überforderung der Normadressaten durch eine unzeitgemäße, komplexe und komplizierte Rechtslage nicht. Das zweite Defizit äußert sich bei ACTA in einer gewissen **Unbeholfenheit** bei den **Schutzmaßnahmen**. Durchaus typisch für überkommene politische Denkmuster werden Maßnahmen wie das Three-Strikes-Out-Modell, Sperr-, Filter- und Kontrollzwänge erwogen, die sich vielfach bereits als technisch untauglich, unverhältnismäßig und wenig akzeptanzstiftend erwiesen haben. Dass diese mittlerweile aus dem Entwurf des Abkommens gestrichen wurden, erscheint wenig beruhigend. Das Gesamtkonzept ist nämlich in einem Geiste verfasst, der solche Maßnahmen als „ultima ratio" provozieren könnte, wenn und weil sich die vereinbarten Schutzmaßnahmen als unzureichend erweisen. Dieser Zwangsmühle entkommt man nur mit der Herstellung eines breiten gesellschaftlichen Konsenses.

Geradezu kontraproduktiv erweist sich schließlich das **Regelungsverfahren**: Die Art und Weise, wie das Abkommen im Vorfeld zwischen den Vertragspartnern verhandelt wurde - intransparent und unter Ausschluss der Betroffenen -, mag völkerrechtliche Gepflogenheit sein. Ebenso mag die letztverbindliche Entscheidung durch parlamentarische Ratifizierung dem Modus einer repräsentativen Demokratie entsprechen. Dies bewirkt jedoch bestenfalls **Legalität** (im Sinne formaler Rechtmäßigkeit), nicht **Legitimität** (im Sinne von inhaltlicher Anerkennungswürdigkeit) der

daraus hervorgehenden Normen. Das Urheberrecht, das im digitalen Zeitalter unstreitig reformbedürftig ist, sollte durch keine staatlich veranlasste Maßnahme vorab verfestigt werden. Das dritte - und größte - Defizit von ACTA liegt also in der fehlenden **Bürgerbeteiligung**. Die Informationsgesellschaft verlangt, gerade in Bezug auf ihre identitätsstiftenden Normen (wie eben dem Urheberrecht) so etwas wie empathische Kooperation. Empathie durch ein echtes (nicht taktisches) **Verständnis der Bürgerinteressen in Zeiten des Wandels**. So entsteht eine responsive Demokratie, in der die Repräsentanten ihr Ohr am Puls der Bürger haben, deren Empfindsamkeit spüren und um Zustimmung und Akzeptanz werben.
Urheberrechte sollen auch weiterhin geschützt, Produktpiraterie soll bekämpft werden. Die Reformbedürftigkeit des Urheberrechts betrifft weniger die Wirtschaftskriminalität, sondern vielmehr den Schutz von und den Zugriff auf Informationen und Inhalte, wie sie zum digitalen bürgerlichen Alltag gehören.

Keine Online-Durchsuchung durch die Hintertür

Die Erkenntnisse des Chaos Computer Clubs in der Analyse des sog. Staatstrojaners haben den Zugriff von Ermittlungsbehörden auf IT-Systeme in ein neues Licht getaucht. Zwar setzen die neuen gesetzlichen Regelungen zur Online-Durchsuchung im BKA-Gesetz und in manchen Landespolizeigesetzen die strengen Vorgaben des Bundesverfassungsgerichts um. Es ist aber fraglich, ob das genügt, um letztlich auch **verfassungskonforme Maßnahmen** ergreifen zu können. Nach derzeit geltendem Recht obliegt es nämlich der Exekutive, Maßnahmen zum Zugriff auf informationstechnische Systeme in eigener Regie zu gestalten, ggf. also auch Trojanersoftware „auf dem Markt" zu beschaffen und ohne weitere Kontrolle einzusetzen, nachdem ein Richter den Einsatz generell erlaubt hat. Das wiederum kann zu einer unverhältnismäßigen Umsetzung der gesetzlichen Erlaubnis führen, so wie dies in den kürzlich offen gelegten „Trojaner-Fällen" diskutiert worden ist. Daraus sind Konsequenzen zu ziehen: Zum einen darf es **keine intransparente, unkontrollierte Beschaffung bzw. Herstellung von Software** geben, die für schwerwiegende Grundrechtseingriffe eingesetzt werden kann. Auch und gerade bei staatlichem IT-Einsatz muss Transparenz und Qualitätssicherung höchstes Gebot sein. Zum anderen muss

technisch sichergestellt sein, dass eine solche (Trojaner-) Software tatsächlich nichts anderes bewirkt als gesetzlich präzise vorgegeben ist. Dass die Software nicht alles darf, was sie tatsächlich kann, ist keine hinreichende Vorkehrung. Sollte eine technisch wirksame Beschränkung auf das erlaubte Maß nicht möglich sein, muss auf ihren Einsatz verzichtet werden. Das „Kompetenzzentrum Informationstechnische Überwachung" (CC ITÜ), in dem Qualitätssicherung bei der Herstellung einer Trojanersoftware geleistet werden soll, ist insoweit ein erster Schritt in die richtige Richtung. Ein weiterer Aspekt ist die Anregung, zur Ausfüllung des Richtervorbehalts nur speziell ausgebildete, auch mit technischen Feinheiten betraute Richterinnen und Richter einzusetzen. Die Trojaner-Diskussion zeigt ein weiteres Mal, dass beim Zusammenspiel von rechtlichen Befugnissen und technischen Maßnahmen **größte Sorgfalt** erforderlich ist. Ob auf diese Weise überhaupt eine „gerichtsfeste" Online-Durchsuchung künftig möglich ist, bleibt aus unserer Sicht abzuwarten. Dies gilt auch hinsichtlich einer sog. Quellen-Telekommunikationsüberwachung. Zwar ist diese der Online-Durchsuchung schon deshalb vorzuziehen, weil sie das mildere Mittel darstellt. Hier wird nicht gezielt eine Festplatte bzw. sonstiges Speichermedium durchsucht, sondern „nur" die laufende Kommunikation überwacht (so wie die klassische Telefonüberwachung im Gegensatz zur Wohnungsdurchsuchung einschließlich Lauschangriff). Dennoch gelten für die Infiltration des Zielsystems vergleichbare Anforderungen (keine „Zuschaltung" einer Webcam oder eines Keyloggers etc.). Und was definitiv zu beachten ist: Sollte eine „Quellen-TKÜ" richterlich erlaubt sein (was derzeit ohnehin nur zur Gefahrenabwehr zulässig wäre und nach der Strafprozessordnung umstritten ist), muss sich die Maßnahme auch auf die Überwachung der laufenden Kommunikation beschränken.

3. Elemente einer akzeptanzstiftenden Internetregulierung

Die Ablehnung bestimmter Instrumente zur Gefahrenabwehr und Kriminalitätsbekämpfung bedeutet keineswegs, dass man die Gefahren und Delikte im Netz geringschätzt und die Sicherheit einem „freien Internet" opfern müsste. Vielmehr ist

der Gedanke der Fairness nicht nur als Appell an die Rechtstreue der Internetnutzer, sondern zugleich auch als **Verfahrensmodus** in der **Gestaltung von Sicherheitspolitik** (aber auch in anderen Politikfeldern) heranzuziehen. Der Netzrat versteht sich – wie eingangs geschildert - als Beobachter und Ideengeber für solche Themen, bei denen das Internet Gegenstand staatlicher Regulierung oder Deregulierung ist. Wir schlagen weniger konkrete Gesetze oder Maßnahmen vor, sondern unterstützen die Ressorts in netzpolitischer Hinsicht.

Verfassungsrechtliche Grenzen beachten

Es mag eine Selbstverständlichkeit sein, dass der Gesetzgeber bei seinem Wirken, auch und gerade bei der Begründung freiheitseinschränkender Sicherheitsinstrumente die verfassungsrechtlichen (und natürlich auch europarechtlichen) Grenzen beachtet. Leider hat es in den letzten Jahren eine Vielzahl von Entscheidungen des Bundesverfassungsgerichts gegeben, in denen das höchste Gericht eben solche Gesetze für verfassungswidrig erklärt hat: Telekommunikationsüberwachung, Online-Durchsuchung, automatisierte Kfz-Kennzeichenerfassung, Vorratsdatenspeicherung u.a.m. Bei Letzterer hat Karlsruhe dem Gesetzgeber gar aufgegeben, **hinreichend „anspruchsvolle" (und normenklare) Regelungen** zu schaffen. Dies wurde in den Medien als „schallende Ohrfeige" für den Gesetzgeber interpretiert und hat auch das Vertrauen der Bevölkerung in eine Angemessenheit der Sicherheitsgesetze, gerade in Abwägung mit den bürgerlichen Freiheitsinteressen, beeinträchtigt. Es wäre wichtig, dass gesetzgeberischer Tätigkeit, besonders zu informationstechnischen polizeilichen Mitteln, wieder einmal Verfassungskonformität bescheinigt werden kann.

Sachverständigengutachten: beachten - oder widerlegen

Es mag konzediert werden, dass Regelungen im IT-Bereich nicht immer leicht zu begreifen sind. Umso mehr ist es bedeutsam, dass der Gesetzgeber Sachverständige heranzieht, deren Beurteilung durchaus beachtlich ist, solange sie nicht konkret widerlegt wird. Eine einfache Ignorierung übereinstimmender Sachverständigenaussagen (wie bei den Netzsperren als untaugliches Instrument geschehen) sollte

vermieden werden. Genau jene Sachverständigen werden möglicherweise auch vom Bundesverfassungsgericht gehört. Ihre Expertise findet dann Eingang in dessen Entscheidungen. Diesen „Umweg über Karlsruhe" könnte man zuweilen vermeiden. Dabei ist es nicht nur der Erlass verfassungswidriger Gesetze, der die **Normakzeptanz** verringert. Problematisch ist es auch, wenn der Gesetzgeber solche Ursachen und/oder Wirkungen der Informationstechnik zugrunde legt, die sich leicht widerlegen lassen. Man darf davon ausgehen, dass die wachsamen Bürger Mittel und Wege finden, solcher Politik gebündelten Sachverstand entgegen zu setzen.

Gesellschaftlichen Konsens suchen, Abweichungen erklären

Wir verstehen die repräsentative Demokratie – wie gesehen - als responsive Demokratie. Das Parlament sollte, gerade wenn es um wichtige Weichenstellungen im Verhältnis von Freiheit und Sicherheit geht, einen breiten Konsens suchen. Und zwar in einem Dialog mit den gesellschaftlichen Kräften - auch denen, die gemeinhin als „Netzgemeinde" bezeichnet werden. Dafür sollen geeignete **Beteiligungsformen** gesucht bzw. gestaltet werden, die eine Interessenvertretung der „Gesamtbevölkerung" ermöglichen. Nicht jedes Interesse wird am Ende ganz berücksichtigt werden können. Jedoch muss dies einer **Akzeptanz** nicht entgegenstehen, wenn die **Entscheidungen plausibel erklärt** werden. Das geschieht seit 2010 (mit dem durch den damaligen Bundesinnenminister de Maizière initiierten Netzdialog, aber auch dem Verbraucherschutzdialog durch Bundesministerin Aigner oder die Mitwirkung bestimmter Experten in der Enquete Kommission Internet und Digitale Gesellschaft u.a.m.) verstärkt, sollte aber ausgebaut werden.

Pflicht zur Abschätzung der Technikfolgen und sozialen Folgen

Informationstechnische Eingriffe haben nicht nur kurzfristige Folgen, etwa beim Zugriff auf bestimmte personenbezogene Daten. Sie wirken auch langfristig. Das Bundesverfassungsgericht hat in einem solchen Kontext von dem „**diffusen Gefühl permanenten Überwachtseins**" gesprochen. Solche sozialen Folgen, aber auch Konsequenzen zum Beispiel für die Vertraulichkeit und Integrität informationstechnischer Systeme sollen erkannt, bewertet und bei den Gesetzen und ihren Umsetzungsakten berücksichtigt werden. Ähnlich wie die obligatorische „Umweltverträglichkeitsprüfung" könnte es eine „**Privatsphärenverträglichkeitsprüfung**"

geben. Dabei ist der von *Alexander Roßnagel, Staatsrechtler und Sachverständiger im Verfahren zur Vorratsdatenspeicherung vor dem Bundesverfassungsgericht*, zutreffend entwickelte Gedanke einer „**Überwachungsgesamtrechnung**" zu berücksichtigen: Einzelne Maßnahmen mögen für sich noch verhältnismäßig und vertretbar sein. In der Summe kann aber ein Eingriffs- und Belastungspotential entstehen, das mit einem nachhaltigen Grundrechtsschutz unvereinbar ist. Das muss auch in einem übergreifenden Be- und Entlastungskonzept geprüft werden, weil einzelne Gesetzgebungsvorhaben möglicherweise damit überfordert wären.

Innovationsförderung für freiheitsschützende Technologien

Der Staat muss zur Bekämpfung schwerer Kriminalitätsformen zuweilen in Grundrechte der Bürger eingreifen. Der Einsatz moderner Technik gehört auch auf Seiten der Sicherheitsbehörden dazu. Es gehört aber ebenso zur **Verhältnismäßigkeit** solcher staatlichen **IT-Eingriffe**, dass mildere Mittel nicht nur vorzuziehen sind, wenn sie bereits existieren. Nach ihnen ist auch gezielt zu suchen. Deshalb hat der Staat die Pflicht zur Innovationsförderung für **freiheitsschützende Technologien**. Davon macht er durchaus bereits Gebrauch. So werden etwa durch das Programm „Trusted Cloud" des Bundeswirtschaftsministeriums zwölf Forschungsprojekte gefördert, die sich der Entwicklung vertrauenswürdiger Cloud-Strukturen widmen. So sollen die Vorteile dieser Innovation mit den Risiken für Datenschutz und Datensicherheit in Einklang gebracht werden. Solche Ansätze sind auch in der IT-relevanten Sicherheitspolitik zu verstärken. Zwar gibt es sowohl auf Bundes-, als auch auf EU-Ebene **Forschungsförderung** im Bereich der **IT-Sicherheit**. Diese ist bislang aber weniger auf **Privatsphären- und Persönlichkeitsschutz bei informationstechnischen Ermittlungsinstrumenten** gerichtet. Dies hätte auch positive Effekte für die Akzeptanz und die Wiedergewinnung verlorenen Vertrauens in der Bevölkerung. Damit kann letztlich dem Kerngedanken von „Freiheit und Fairness" Rechnung getragen werden.

Ein freies Internet braucht Fairness im Umgang der Akteure: nicht nur zwischen Privatpersonen, sondern auch zwischen Staat und Bürger. Staatliche Instanzen sollen zeigen, dass sie schwerwiegende Eingriffe nur als „ultima ratio" vornehmen und

technische Eingriffsmittel so entwickeln und einsetzen, dass **Neben- und Fernwirkungen** so gering wie irgend möglich gehalten werden. Wissenschaft und Forschung können einen erheblichen Beitrag für innovative Technologien leisten, die sich der Vertraulichkeit und Integrität der IT-Systeme und damit verbunden dem Schutz von Privatsphäre und Persönlichkeit widmen. Sie müssen aber auch gefördert und unterstützt werden.

Kontrolle der Kontrolleure

IT-Eingriffe sind - teilweise unvermeidbar - diffus und komplex. Es muss kein böser Wille der Anwender sein, wenn sich technische Mittel nachteiliger auswirken, als dies zunächst intendiert ist. Umso mehr muss gewährleistet sein, dass demokratische (Sicherheits-) Gesetze nur in verhältnismäßiger Weise in die Freiheitsbereiche der Bürger einwirken. Hierfür bedarf es auch einer **(rechtsstaatlichen) Kontrolle** der **eingesetzten Sicherheitskräfte**. Dies geschieht zum Teil - präventiv - durch Richtervorbehalt, muss aber auch fortwährend im Laufe von Eingriffsmaßnahmen gewährleistet werden.

4. Fazit

Angesichts der Einschränkungen, die das Bundesverfassungsgericht etwa in Fällen der Online-Durchsuchung oder der Vorratsdatenspeicherung dem Gesetzgeber aufgetragen hat, muss der Staat mit dem Bürger auch in einen Dialog über die veränderten – und zum Teil nur begrenzt kontrollierbaren – Gefährdungspotentiale in einer globalisierten und digitalisierten Welt treten. Ebenso wie der Staat Inlandskriminalität nur bis zu einem bestimmten Maß bekämpfen kann, wird er auch nicht jede Form der globalen Kriminalität oder des globalen Terrorismus vollumfänglich unterbinden können, unabhängig von der Intensität seiner Eingriffsbefugnisse.

Neben der permanenten Wachsamkeit der Gemeinschaft gegenüber Bedrohungssignalen, der behutsamen Anwendung der verfassungskonformen Ermittlungsinstrumente, einer quantitativ und qualitativ verbesserten **Ausstattung** der **Sicher-**

heitsbehörden mit Personal und Knowhow und einer verbesserten internationalen Zusammenarbeit könnte die Entwicklung neuer, möglichst wenig eingreifender **Technologien zur Früherkennung krimineller Bedrohungen einen Beitrag zur Balance von Freiheit und Sicherheit im Internet** bieten. Daneben spielen die Bedingungen, unter denen neue Eingriffsbefugnisse und Ermittlungsinstrumente entstehen, eine wichtige Rolle für die Akzeptanz. Staatliche Akzeptanzstiftung ist eine wichtige Gegenleistung für die Solidarität der unbescholtenen Bürger, polizeiliche Eingriffe hinzunehmen.

IV. Thesen zur Netzpolitik - Netzpolitik als Querschnittsthema und Aufgabe für einen Internetstaatsminister

1) Netzpolitik ist Bildungspolitik. Die Aus- und Fortbildung in den Schulen, Hochschulen, Berufsschulen, den zahlreichen Fortbildungsstätten etc. wird bereits heute zum Teil und künftig noch stärker durch die neuen Medien unterstützt. Sei es durch das digitale Klassenzimmer, E-Learning, Blended Learning, durch den E-Campus, die Virtuelle Hochschule Bayern u.v.a.m. Wir leben in einer Informationsgesellschaft, die schnell und flexibel verfügbare Informationen und ihre weitere Verarbeitung im täglichen Leben, sei es für private, berufliche oder gesellschaftliche Zwecke, benötigt. Das digitale Zeitalter bietet hierfür die Chancen, Mittel und Wege. Dies zu nutzen setzt aber Grundkenntnisse und Grundfertigkeiten im Umgang mit den neuen Medien voraus (Medien- und Informationskompetenz). Es ist eine zentrale Aufgabe aller Bildungseinrichtungen, dies zu vermitteln, am besten ganz praktisch mit dem Einsatz von IT. Bildungspolitik muss dies fördernd und steuernd berücksichtigen.

2) Netzpolitik ist Familien- und Jugendpolitik. Die Digitalisierung der Kommunikation, die zunehmende Bedeutung der sozialen Netzwerke und die Integration von Internet und IT in den Lebensalltag (Smartphones, Online-Spiele, webbasierte Lernsoftware usw.) werfen auch neue Fragen für die Erziehung und das Familienleben auf. Die „Verweildauer" im Internet übersteigt längst den klassischen Fernseh-

konsum. Außerdem werden Kinder und Jugendliche „im und durch das Netz" immer selbständiger; sie sind dort aber zugleich gewissen Gefährdungen ausgesetzt. Bemerkenswert ist auch, dass sich die natürliche Autorität der Eltern in Netzfragen relativiert. Vieles wird in den Familien zu lösen sein. Soweit die Politik aber gefordert ist, müssen deren Antworten und Konzepte auf jeden Fall technisch sinnvoll sein und dürfen sich nicht etwa in einem „Abschalten des Netzes nach 20.00 Uhr ...." und ähnlichen Verboten darstellen.

3) Netzpolitik ist Haushaltspolitik. Die Konsolidierung der öffentlichen Haushalte ist nach wie vor ein Ziel mit höchster Priorität. Gerade die Modernisierung von Staat, Verwaltung, Wirtschaft und Gesellschaft durch IT-Einsatz (etwa im Rahmen des E-Government, aber auch bei E-Health oder beim E-Learning) kann auch der Einsparung von Haushaltsmitteln ohne Qualitätsverlust dienen (solange man die beteiligten Menschen dazu befähigt, IT-Verfahren professionell einzusetzen). Dabei sind zwischenzeitliche Mehrkosten durch Investitionen und hybride Verfahren sorgfältig zu kalkulieren, damit sich diese in der Gesamtbilanz nicht negativ auswirken.

4) Netzpolitik ist Umweltpolitik. Digitale Mobilität durch Videokonferenzen und intelligente Verfahren spart Zeit und Energie und schont die Umwelt, wenn für Sitzungen nicht mehr zahlreiche Kilometer auf Straßen verbracht werden. Hinzukommt das wichtige Thema Elektromobilität, das einen spezifischen Bezug zu IT-Verfahren hat, etwa bei der Navigation und der Gestaltung und Nutzung des Versorgungsnetzes.

5) Netzpolitik ist Wirtschaftspolitik. Schon heute wird ein großer Teil der Wirtschaftskraft unmittelbar oder mittelbar durch den Einsatz von Informations- und Kommunikationstechnologien erbracht. Die IT-Branche war in der Finanzkrise ein regelrechter (Job-) Motor. E-Business und E-Commerce zeigen die Chancen des Handels und der Dienstleistungsunternehmen in einem globalen Wettbewerb. Moder-

ne Wirtschaftspolitik muss die Herausforderungen aufnehmen, die durch diese veränderten Geschäftsmodelle, Vertriebswege und Wertschöpfungsketten entstehen. Sei es durch angemessene Regulierung oder Deregulierung oder durch gezielte Wirtschaftsförderung, z.B. von Startups. Gerade im Freistaat Bayern gibt es in dieser Hinsicht, nicht zuletzt durch die Ausgründungen der Forschungsprojekte der exzellenten bayerischen Hochschulen, viel Potential.

6) Netzpolitik ist Verbraucherschutzpolitik. Der Internetnutzer ist schutzbedürftiger Verbraucher, besonders im Online-Handel, aber auch bei der Nutzung zahlreicher weiterer Online-Dienste. Noch mehr als etwa im Haustürwiderrufsrecht bedarf es adäquater Schutzstandards. Das Fernabsatzrecht bietet bereits zahlreiche Instrumente des Verbraucherschutzes, etwa durch das Widerrufsrecht oder zuletzt durch die Button-Lösung zur Vermeidung von Abo-Fallen. Hierzu gehören aber auch die Datenschutz- und Privatsphärenschutzregeln, für die durch die Besonderheiten global agierender Dienste wie Facebook und Google große Herausforderungen bestehen.

7) Netzpolitik ist Sozialpolitik. Das Internet ermöglicht die Teilhabe an der Bürgergesellschaft. Natürlich bietet es eine neue Anbindung benachteiligter Menschen, deren Behinderungen oder sonstigen Benachteiligungen kein Hinderungsgrund mehr sein müssen, am beruflichen oder sozialen Leben durch die Möglichkeiten der Barrierefreiheit beteiligt zu sein. Aber Sozialpolitik geht weiter: Die Partizipation an Petitionen ist beispielsweise genauso über das Netz möglich wie die Unterstützung durch Mitmenschen bei der Bewältigung persönlicher Probleme in Foren. Die Sozialpolitik sollte das Internet als Chance sehen und Strategien zur „digitalen Hilfestellung" entwickeln.

8) Netzpolitik ist Sicherheitspolitik. Das Internet mag von manchen als „Gefahr" angesehen werden, gibt es doch bestimmte Kriminalitätsformen, die sich im Netz

entfalten. Umgekehrt bietet das Internet mit seinen Netzwerken Chancen zur Kriminalitätsbekämpfung und Gefahrenvorsorge, wenn etwa die Polizei in sozialen Netzwerken zur Suche nach vermissten Kindern auffordert oder dort Fahndungen ausschreibt u.v.a.m.

9) Netzpolitik ist Rechtspolitik. Der elektronische Rechtsverkehr, E-Justice, digitale Willenserklärungen etc. sind längst Justizalltag. Rechtsverbindliches Handeln im Netz muss ein widerspruchsfreier Teil der Rechtsordnung sein. Wie professionell die Justizministerien mit diesen Herausforderungen umgehen, sieht man seit 20 Jahren auf dem Deutschen EDV-Gerichtstag. Darüber hinaus ist es aber auch eine wichtige Aufgabe der Rechtspolitik, die Rechtsordnung mit ihrer Rechtsdogmatik auf die Besonderheiten der Digitalisierung und Vernetzung einzustellen: Welche Regelungen passen noch in die heutige Welt, wo besteht Reformbedarf? Welcher verfassungsrechtliche Rahmen gilt für Rechtsänderungen und Eingriffe?

10) Netzpolitik ist Zukunftspolitik. Man könnte diese Liste verlängern. So betrifft das Internet auch die Netzphilosophie, die Netzkultur oder die IT-Steuerung. Es geht - auch und gerade in politischer Hinsicht - auch darum, zu ermitteln, mit welchem Werteverständnis, in welchen Umgangsformen und mit welchen technischen Voraussetzungen und Wirkungen die neuen Medien genutzt werden. Schon hierfür bedarf es besonderer Anstrengung, nicht zuletzt um nicht den Anschluss an die „digital Natives" zu verlieren, die sich in ihrem digitalen Leben von überkommenen politischen Positionen unzureichend verstanden fühlen. Netzpolitik ein Querschnittsthema über praktisch alle Politikfelder. Deshalb wäre es auch zu begrüßen, wenn der Stellenwert der Netzpolitik seine Entsprechung in politischen Ämtern findet. Angemessen wäre deshalb die **Schaffung des Amtes eines Staatsministers / einer Staatsministerin für Internet und Digitale Gesellschaft auf Bundesebene**. Ein Internetstaatsminister muss als Schnittstelle zwischen den verschiedenen politischen Ressorts fungieren. Das Querschnittsthema Netzpolitik findet unter seinem Dach eine Sammelstelle. Der Internetstaatsminister ist damit der Ingenieur, der die

Architekten - also die klassischen politischen Ressorts - in Fachfragen berät. Ein Internetstaatsminister soll Ansprechpartner für rechtliche wie gesellschaftliche Fragen im digitalen Zeitalter sein. Er muss darauf achten, dass Gesetze und Regelungen bereits in ihrer Entstehungsphase im Hinblick auf Praktikabilität und Umsetzbarkeit in einer digitalen Lebenswirklichkeit tauglich sind. Ein Internetstaatsminister würde im Vorfeld Gesetzesvorhaben auf ihre Auswirkungen auf das Internet prüfen und die beteiligten Ressorts beraten. ACTA hätte dann heute vielleicht einen anderen Status. Ein Internetstaatsminister soll Garant für die Freiheit des Internets sein. Seine Aufgabe und seine Kompetenz besteht darin, darauf zu achten, ein Höchstmaß an Sicherheit zu gewährleisten, dabei aber unverhältnismäßige Einschränkungen für die Nutzer zu vermeiden.

Auch die Abstimmung mit den einzelnen Stellen auf Bundes- wie auf Länderebene (wie zum Beispiel mit den Landesdatenschutzbeauftragten) fällt in sein Aufgabengebiet, um möglichst einheitliche und länderübergreifende Regelungen zu finden. Konkret bedeutet das beispielsweise auch die enge Zusammenarbeit mit dem Kulturstaatsminister, der Bundesbeauftragten für die Informationstechnik oder dem Bundesbeauftragten für Datenschutz und Informationsfreiheit. Um innerhalb der EU und auf internationaler Ebene im Diskussionsprozess teilhaben zu können und ernst genommen zu werden, ist ein Internetstaatsminister als Sprachrohr und Verantwortlicher der Bundesregierung unerlässlich. In Abstimmung mit den zuständigen Kultusministern kann ein Internetstaatsminister auch dabei unterstützend tätig sein, bundesweite Standards für die Vermittlung von Medien- und Informationskompetenz zu erarbeiten.

Der Internetstaatsminister schafft damit - was Expertise und Zuständigkeiten angeht - Klarheit im derzeit noch unübersichtlichen Feld der Netzpolitik. Er bietet als konkreter Ansprechpartner somit Lösungsansätze und Sicherheit in einem Bereich, in dem die Politik in den letzten Monaten leider auch einiges an Vertrauen einbüßen musste und gestaltet durch Integration der relevanten Themen der Zukunft.

Epilog

Sehr geehrte Damen und Herren,

Netzpolitik ist Zukunftspolitik. Diese 10. These, mit der wir das 2. Positionspapier des CSU Netzrates abgeschlossen haben, ist so etwas wie die Quintessenz, die wir im letzten Jahr aus all unseren Überlegungen, Diskussionen und Erkenntnissen gewonnen haben. Wir sind überzeugt, dass das Internet als umspannendes Netzwerk von Menschen, Dingen, Ideen und Inhalten entscheidend dazu beitragen wird, wie wir unser privates, berufliches und gesellschaftliches Leben in den nächsten Jahren gestalten können und gestalten wollen. Manches lässt sich schlicht nicht mehr aufhalten oder umdrehen, wie der Siegeszug der sozialen Netzwerke, der Einsatz smarter Technologien oder die politische Forderung nach Transparenz und Partizipation. Die soziale Funktion der Gefällt-mir-Komplimente, der Demokratisierungsprozess durch besseren Informationszugang aller Bevölkerungsschichten und deren Beteiligungsmöglichkeiten oder die Wertschöpfung durch Wissensteilung bringen die Werte unserer Verfassung erst richtig zur Geltung.

Freiheit und Fairness, das gilt auch und erst recht in diesem 2. Positionspapier. Dass wir dieses Mal die Attribute Bildung und Sicherheit in den Vordergrund gerückt haben, ist kein Zufall. Sie stehen wie kaum ein anderes Thema für die These der Netzpolitik als Zukunftspolitik. Das Internet verändert alles. Aber alles ist nichts ohne entsprechende Bemühungen um bessere Bildungschancen und ein angemessenes Sicherheitsdenken in und mit einem freien und fairen Internet.

Dafür bedarf es aber auch eines grundlegenden Umdenkens. Pointiert ausgedrückt: Schulen sollten nicht so selten, Ermittlungsbehörden nicht zu schnell Informationstechnik zur Erledigung ihrer Aufgaben einsetzen. Bislang ist staatlicher IT-Einsatz aus Sicht der Bürger durchaus negativ besetzt: Während Bildungschancen mittels IT eher zu wenig in den Blick genommen werden, verbindet sich IT auf Seiten des Staates oftmals mit unverhältnismäßigen, verfassungswidrigen Instrumenten. Faire Internetnutzung bedeutet in diesem Sinne auch Augenschein und Augenmaß.

Nach dem Netzkongress ist vor dem Netzkongress. Wir machen weiter, stellen uns der Diskussion und leisten Überzeugungsarbeit für unsere digitale Chancenrepublik Deutschland. Themen wie Open Government Data und Informationsfreiheit, datenschutzkonformes Cloud Computing oder die notwendige Urheberrechtsreform werden uns in den nächsten Monaten wieder begegnen, nachdem wir uns in Ansätzen hierzu bereits positioniert haben. Spannend erscheint auch die Diskussion um einen konsensfähigen Wertekanon zur Absicherung grundrechtlicher Freiheiten bei der Internetnutzung. Wir freuen uns auf Anregungen und konstruktive Kritik. Folgen Sie uns auf Twitter oder werden Sie Mitglied im Arbeitskreis CSUnet. In jedem Fall gilt: Engagieren Sie sich. Bringen Sie sich ein.

München und Passau, den 16. März 2012

Dorothee Bär, MdB
(@DoroBaer)

Prof. Dr. Dirk Heckmann
(@elawprof)