

**Positionspapier
des CSU-Netzrates**

In Freiheit und Fairness.

www.csu.de



Impressum

CSU-Landesleitung
Dr. Bernhard Schwab
Hauptgeschäftsführer
Nymphenburger Straße 64
80335 München

Stand: Januar 2011

Vorwort der Vorsitzenden des CSU-Netzrates



Sehr geehrte Damen und Herren,

die Netzpolitik ist bis heute ein weitgehend weißer Fleck in der deutschen Parteienlandschaft. Bisher hat noch keine große politische Kraft in Deutschland ihre Einzelpositionen rund um das Internet zu einem geschlossenen Bild zusammengefasst. Die CSU will hier eine Vorreiterrolle übernehmen. Wir haben deshalb einen Netzrat mit unabhängigen Experten eingerichtet, der ein wegweisendes Positionspapier zur Netzpolitik erarbeitet hat.

Die CSU stand schon immer an der Spitze des technischen Fortschritts. Es war aber immer auch unsere Position, dass dieser Fortschritt den Menschen dienen und ethisch verantwortbar sein muss. Das gilt auch für das Internet. Unsere Netzpolitik fußt deshalb auf dem Gedanken von „Freiheit und Fairness“, wie ihn der Netzrat eindrucksvoll formuliert hat. Es entspricht unserer Überzeugung, dass Freiheit und Verantwortung auch im Internet ein Geschwisterpaar sein müssen.

**Wir wollen die Themen der Zukunft gestalten.
Wir vertrauen dem mündigen Bürger.
Wir wollen eine lebendige Mediendemokratie.**

Wir alle müssen uns fragen, was das Internet für uns in 5 oder 10 Jahren leisten soll. Wir müssen gemeinsam das Bild schärfen, was wir von diesem Medium erwarten. Erst dann kann die Politik an Hand der „roten Linie“ dort den politischen Rahmen vorgeben, wo dies notwendig ist.

Dieses Positionspapier ist eine Grundlage für diese Diskussion. Das Papier stellt weder einen Beschluss noch einen Endpunkt der Gespräche dar. Denn: Ich wünsche mir, dass Sie sich aktiv einbringen und Ihre Meinung dazu, was das Internet für uns als Bürger leisten soll, äußern.

Mit unserem Positionspapier und dem netzpolitischen Kongress Ende Januar 2011 wollen wir der parteiinternen und öffentlichen Debatte zur Netzpolitik neuen Schwung geben und einen Beitrag zur Meinungsfindung leisten.

Vielen Dank für Ihr Interesse!

Mit freundlichen Grüßen

A handwritten signature in blue ink that reads 'Dorothee Bär'.

Dorothee Bär, MdB

Stv. Generalsekretärin und Vorsitzende des CSU-Netzrates

In Freiheit und Fairness.

Dem CSU-Netzrat gehören an:



Dorothee Bär (Vorsitzende) gehört seit 2002 dem Deutschen Bundestag an und vertritt den Bundeswahlkreis Bad Kissingen. Seit Februar 2009 ist sie stellvertretende Generalsekretärin der CSU und leitet den CSU-Netzrat.



Prof. Andreas Bönnte ist Programmbeauftragter für das Bayerische Fernsehen und Leiter des Programmbereichs Planung und Entwicklung. Zugleich ist Bönnte Honorar-Professor für TV-Journalismus an der Fachhochschule Würzburg-Schweinfurt.



Dr. Reinhard Brandl ist CSU-Bundestagsabgeordneter aus dem Wahlkreis Ingolstadt. Im Jahr 2010 wurde Brandl in die neu gegründete Enquete-Kommission „Internet und digitale Gesellschaft“ des Deutschen Bundestages berufen.



Bertram Brossardt ist Hauptgeschäftsführer der Vereinigung der Bayerischen Wirtschaft (vbw) sowie der Verbände der bayerischen Metall- und Elektroindustrie. Zuvor war Brossardt Leiter der Abteilung Außenwirtschaft und Standortmarketing im Bayerischen Wirtschaftsministerium.



Prof. Dr. Dirk Heckmann ist Inhaber des Lehrstuhls für Öffentliches Recht, Sicherheitsrecht und Internetrecht an der Universität Passau sowie Leiter des Center for IT-Compliance and Trust an der Zeppelin University Friedrichshafen.



Walid Nakschbandi ist Journalist, Fernsehproduzent und Manager in der Verlagsgruppe Georg von Holtzbrinck. Seit 1999 ist der in Afghanistan geborene Nakschbandi Geschäftsführer und Chefredakteur der AVE Gesellschaft für Fernsehproduktion mbH mit Sitz in Berlin und Düsseldorf.

In Freiheit und Fairness.

I. Das Internet als Ort der Freiheit

Das Internet ist das wichtigste und mittlerweile ein selbstverständliches Informations- und Kommunikationsmedium für Jedermann. Es ist aus dem gesellschaftlichen, wirtschaftlichen und politischen Alltag nicht mehr wegzudenken. Für die Menschen als Bürger, Kunden und private Nutzer, aber auch für die Unternehmen, Verbände oder den Staat bietet das Internet erhebliche **Chancen für eine Verbesserung und Erweiterung ihrer Entfaltungs- und Handlungsmöglichkeiten**. Das Internet ist so, wie es sich entwickelt hat und wie es zurzeit jedermann zur Verfügung steht, Ausdruck von Freiheit und soll auch weiterhin ein Ort freier Entfaltung persönlicher, wirtschaftlicher und politischer Interessen bleiben. Soweit diese Freiheit – gewollt – durch unfairen Gebrauch oder – ungewollt – durch systembedingte Risiken gefährdet ist, soll dem durch **Schaffung freiheitssichernder Regeln** begegnet werden. Der Staat hat bei der Freiheitssicherung im Internet eine wichtige Rolle, nicht zuletzt in Erfüllung grundrechtlicher Schutz- und Gewährleistungspflichten. Er kann diese Rolle aber nur gemeinsam mit der Gemeinschaft der Internetnutzer und den Anbietern von Internetdiensten ausfüllen; **zur Freiheit gehört auch (Selbst-) Verantwortung**. Neben seiner Schutzfunktion hat der Staat – soweit er selbst Internetnutzer ist – eine Vorbildfunktion.

Leitmotive seiner Netzpolitik sollten **Freiheit und Fairness** sein. Dies wird realisiert durch

- Zurückhaltung (Grundsatz der Subsidiarität)
- Interessenausgleich (Gebot der Rücksichtnahme) und
- Vorsorge (Schaffung einer sicheren IuK-Infrastruktur).

Vor diesem Hintergrund ergeben sich konkrete Chancen für den Einzelnen (II.), die Wirtschaft (III.) und den Staat (IV.). Um diese langfristig zu erhalten, bedarf es der Gewährleistung von IT-Sicherheit, Rechtssicherheit und Dispositionssicherheit mit Hilfe von Wettbewerb, Transparenz, Verlässlichkeit und Vertrauen (V.).

II. Chancen freier Internetnutzung für den Bürger

1. Das Internet als Bereicherung des Alltags

Das Internet gibt den Menschen die Chance, selbstbestimmt und selbstbewusst ihr modernes Leben zu gestalten. **Innovative Nutzungsmöglichkeiten** prägen den heutigen Alltag und stellen sich oft als Bereicherung oder praktische Hilfe dar. Das betrifft etwa die Erweiterung der Möglichkeiten zur Information (z.B. Wikis, Blogs, Foren, Beratungs- und Bewertungsportale), Kommunikation (z.B. E-Mail, Instant Messaging, mobile Kommunikation, soziale Netzwerke) und

Interaktion (z.B. Online-Shopping, E-Partizipation, E-Government). Durch asynchrone Kommunikation kann der Alltag flexibler gestaltet werden. Globale kollaborative Wissensvermehrung („user generated content“, z.B. Wikipedia) und effiziente Wissensverteilung (frei zugängliche Online-Datenbanken, Wertschöpfung über Applikationen, z.B. apps4democracy) schaffen neue und erweiterte Möglichkeiten für die **Teilhabe des Einzelnen an den Schätzen der Welt**. Der virtuelle Raum ist Weltbibliothek und globaler Supermarkt.

2. Das Internet als Chance für Benachteiligte

Der Staat des Grundgesetzes ist zugleich aber auch **Sozialstaat**. Dieses verfassungsrechtlich verankerte Staatsziel kann durch die neuen Möglichkeiten der IuK-Technologien eine Aufwertung und Bereicherung erfahren. Besonders benachteiligten Menschen (Behinderte, Ärmere, Menschen in strukturschwachen Regionen u.a.m.) kann die neue Technik helfen, Hindernisse in ihrem Alltag zu überwinden und damit noch aktiver als bisher am gesellschaftlichen Leben teilzunehmen.

3. Vermittlung von Medienkompetenz als Antwort auf neue Gefährdungen

All diese erheblichen Chancen und Vorteile gehen einher mit der Speicherung, Verarbeitung und Übermittlung zahlreicher Daten. Informations- und Kommunikationsdienste benötigen **Daten als Grundlage ihrer nützlichen Funktionen**. Sie sind aber auch **missbrauchsanfällig**, sei es, dass aus sachfremden Erwägungen mehr Daten als erforderlich gespeichert werden, sei es, dass Nichtberechtigte Zugang zu sensiblen Daten erlangen. Wer welche Daten in welchem Kontext erheben, preisgeben oder nutzen darf, bestimmt (von bestimmten Auskunftspflichten abgesehen) der Betroffene – als Ausdruck seines Grundrechts auf informationelle Selbstbestimmung – selbst. Es bleibt Aufgabe des (staatlichen) Rechts, sicher zu stellen, dass der Einzelne auch unter den **Bedingungen einer freiheitlichen und freizügigen Informationsgesellschaft** von seinen Grundrechten Gebrauch machen kann. Hierfür ist unter anderem IT-Sicherheit zu gewährleisten und Datenmissbrauch zu unterbinden. Vorbedingung hierfür ist aber – mit hoher politischer Priorität – die Vermittlung eines ausreichenden Maßes an **Medienkompetenz**, und zwar für alle Akteure. Die sachgerechte und kritisch reflektierte Nutzung des Internets muss zur **vierten Kulturtechnik** nach Rechnen, Schreiben und Lesen avancieren. Die Wirkungsweise der Internetnutzung darf nicht nur faktisch (im Sinne eines „plug and play“) nachvollzogen, sondern muss im Hinblick auf Chancen und Risiken richtig verstanden werden (siehe näher unten V. 1).

4. Das Recht der Schwächeren im Internet

Nicht jeder muss, will oder kann das Internet (souverän) nutzen, dessen Chancen wahrnehmen und den Risiken adäquat begegnen. Das (staatliche) Recht hat auch die Aufgabe, den **Schwächeren zu schützen**. Wie im realen Raum gibt es auch im virtuellen Raum zahlreiche Rechtsverletzungen, sei es die Übervorteilung des Verbrauchers im Zuge übermäßigen

In Freiheit und Fairness.

Gewinnstrebens oder „virtueller Vandalismus“ im Sinne gezielter Beeinträchtigung des Persönlichkeitsrechts Dritter. Die rechtsstaatlichen, freiheitssichernden Mittel des Staates zur Unterbindung solcher nachteiligen Erscheinungsformen menschlichen Zusammenlebens **sind hier wie dort begrenzt**. In dieser Hinsicht ist die Inkongruenz zwischen virtueller und realer Welt vielleicht nicht so groß wie bisher angenommen, denn Recht ist in beiden Handlungs-zusammenhängen stets nur ein „bedingt taugliches“ Steuerungsinstrument. Das ist keine Kapitulation des Rechts oder des Staates vor den neuen Herausforderungen des 21. Jahrhunderts. Es ist vielmehr die Feststellung, dass es einer Zusammenführung alter und neuer Instrumente des (Rechts-) Schutzes bedarf, gerade deshalb, damit das Internet als Raum erweiterter Freiheit nicht in Frage gestellt wird. Die Anonymität, Schnelligkeit (Flüchtigkeit) und Internationalität laden nicht nur zu fairer Internetnutzung ein, sondern regen auch die Fantasie der Internetkriminellen an. Es müssen adäquate Formen eines freiheitssichernden Rechts-schutzes entwickelt werden, der als **Rechtsschutz im Internet und nicht gegen das Internet** konzipiert werden soll. Neben die bereits vorhandenen Gebote, Verbote und Sanktionen, die im Internet genauso gelten wie in konventionellen Handlungszusammenhängen, treten technische Instrumente (Internetfunktionen mit „eingebautem Rechtsschutz“ wie zum Beispiel Meldebuttons in sozialen Netzwerken) und Elemente der Selbstregulierung (Wachsamkeit der Nutzergemeinschaft etwa in Sachen Jugendschutz).

5. Der Umgang mit globalen IT-Unternehmen

Das bedeutet auch: Staat und Politik müssen sich bei der Bewertung ihrer Handlungsoptionen viel mehr als bisher den **tiefgreifenden gesellschaftlichen Umwälzungen** stellen, welche die fortschreitende Digitalisierung mit sich bringt. Dazu gehört gerade die Erkenntnis – und Akzeptanz –, dass in mancher Hinsicht das staatliche, ordnungsstiftende Gewaltmonopol in der virtuellen Welt schwerer durchsetzbar ist. Die Organisation der Menschen als soziale Einheiten hat sich zu einem nicht unerheblichen Teil virtualisiert und vom realen Leben entkoppelt. Wesentliche Charakteristika des sozialen und gesellschaftlichen Lebens, die bisher fest im Ordnungsrahmen des jeweiligen Nationalstaates verortet waren, spielen sich jedenfalls auch im virtuellen Raum ab: die Pflege sozialer Beziehungen, die Organisation politischer oder sonstiger gesellschaftsrelevanter Aktivitäten, mediale Unterhaltung oder die Information über aktuelle Ereignisse. Für diese virtuellen Aktivitäten besitzen aber einzelne Unternehmen wie **Facebook oder Google** zum Teil ein durchsetzungsmächtiges Ordnungskonzept. Die Entgrenzung des Internet befördert die Verlagerung der Verhaltenssteuerung weg vom Staat hin zu den mit „IT-Herrschaft“ ausgestatten Privatunternehmen. Mit inzwischen über 500 Millionen Mitgliedern weltweit ist Facebook das Paradebeispiel nicht nur für einen global agierenden Konzern im digitalen Zeitalter. Es ist vielmehr auch ein Beispiel für die Neuorganisation der Menschen in virtuellen Handlungszusammenhängen. Der Staat muss diese soziale Realität im Auge behalten und neue Konzepte entwickeln, eine freie und zugleich faire Internetnutzung zu ermöglichen: Dazu zählen etwa die Förderung von „technischem Datenschutz“ sowieso Selbstschutz (Privacy by Design und Privacy by Default, siehe unten V. 6.), aber auch die Unterstützung der Wirtschaft bei der Entwicklung angemessener Alternativangebote. Ordnungspolitik hat im Internet nur dann eine Durchsetzungschance, wenn Staat, Wirtschaft und Gesellschaft stärker als bisher „am gleichen Strang“ ziehen.

6. Neuorientierung im Urheberrecht: Wirksamer Schutz von Kreativität und Innovation

In solcher Weise differenzierend (und nicht durch bloße Verbote und Vollstreckung) sind auch die **Herausforderungen im Urheberrecht** anzugehen. Auch im Web 2.0 muss die „Selbstbestimmung des Kreativen“ ein geschütztes Gut bleiben. Die gelegentlich zu hörende Forderung, den Urheberrechtsschutz und damit das geistige Eigentum für die virtuelle Welt abzuschaffen, ignoriert die **fundamentale Bedeutung des (geistigen) Eigentumsschutzes für die freiheitlich-demokratische Gesellschaftsordnung**. Allerdings wird eine Beibehaltung des gegenwärtigen Urheberrechtssystems den Interessen der Gesellschaft und der Kreativen ebenso wenig gerecht, wie ein grundsätzlicher Verzicht auf jede Art vernünftiger Regelung. Vordringliche Aufgabe der Politik muss es sein – fernab ideologisch überhöhter Debatten – das System einer **grundlegenden Neubewertung** im Zeitalter digitaler Verwertung zu unterziehen. Dabei sollte ein Ausgangspunkt der Überlegungen sein, dass das bisherige Modell der Vermarktungsintermediäre (z.B. Musikindustrie) im Internet um ein zusätzliches Element der Selbstvermarktung seitens der Kreativen ergänzt und bereichert wurde. Das Internet hat zu einer deutlichen Diversifizierung der Vertriebswege und zu einer Vielzahl neuer Kommunikationsakteure geführt.

7. Angemessener Umgang mit Urheberrechtsverstößen

Das bestehende Urheberrechtssystem nicht an diese gewandelten Verhältnisse anzupassen, hieße, einen sich neu etablierenden gesellschaftlichen Konsens über die Teilhabe an den kulturellen Schätzen der Welt zu ignorieren. Eine solche Neubewertung ist auch deshalb erforderlich, weil die Inkongruenz zwischen Lebenswirklichkeit und rechtlichen Rahmenbedingungen **unlauteren Geschäftsmodellen** zusätzlich Vorschub leisten kann. So legitim Abmahnungen bei Urheberrechtsverstößen sein können, gilt dies doch nicht für „Massenabmahnungen als Geschäftsmodell“. Denn dieses konterkariert gerade, wofür Recht auch und ausschließlich in der virtuellen Welt nutzbar gemacht werden soll – die Wahrung *berechtigter* Interessen Dritter. Solche Praktiken leisten damit einer Mentalität Vorschub, die das Recht in der virtuellen Welt stets nur als Eindringling und Störfaktor wahrnimmt, ohne seine friedensstiftende und auf Interessenausgleich zielende Wirkung zu berücksichtigen. Es ist daher notwendig, mit entsprechenden Mitteln diesen Entwicklungen Einhalt zu gebieten. Insbesondere der erhebliche Interpretationsspielraum betreffend das **Merkmal des „gewerblichen Ausmaßes“** bei Urheberrechtsverletzungen könnte durch den Gesetzgeber zielführend konkretisiert werden. Darüber hinaus wäre auch zu überlegen, ob unter Berücksichtigung der Erfahrungen im anglo-amerikanischen Rechtsraum der Grundsatz des „Notice and take down“ gesetzlich verankert werden sollte. Danach wäre in leichteren Fällen zunächst eine kostenfreie Abmahnung vorzuschalten, die dem Betroffenen die Chance gibt, schnell und ohne weitere Belastung einen rechtmäßigen Zustand herzustellen.

8. Freier Zugang zu Wissen als staatlicher Kulturauftrag im Internet

Wir leben in einer Gesellschaft, in der der Zugang zum Wissen unserer Zeit für die Chancen des beruflichen Fortkommens entscheidend ist. **Open Access** im Sinne eines weitgehend kosten-

In Freiheit und Fairness.

freien Zugangs zu öffentlichen Informationen über das Internet dient der Chancengerechtigkeit. Informationen, deren Entstehung bereits über Steuergelder (etwa im Rahmen öffentlicher Wissenschaftsförderung) finanziert wurden, sollen im Kern frei zugänglich sein. Dies ist Teil des staatlichen Kulturauftrags im Internet. Im Einzelfall ist zu prüfen, ob Kosten zur Sicherstellung des Angebots, für den notwendigen Aufwand einer Aufbereitung oder einer besonderen Bereitstellung erhoben werden dürfen.

9. Wirksamer Schutz von Kindern und Jugendlichen im Internet

Das Internet wird in besonderem Maße von **Kindern und Jugendlichen** genutzt. Das ist prinzipiell zu begrüßen, gibt es doch zahlreiche Angebote für alle Altersgruppen, sowohl für Information und Kommunikation, als auch zum Lernen und Spielen. Durch die Einbeziehung des Internet in das private und schulische Leben lernen die Kinder und Jugendlichen den Umgang mit diesem Medium. Vor Gefahren sind sie allerdings auch wirksam zu schützen (zum Thema Netzsperrungen zur Bekämpfung des Kindesmissbrauchs durch Kinderpornografie unten V. 3). **Adäquater Jugendschutz** ist aber nicht gleichzusetzen mit Verboten, weil bestimmte Angebote und Funktionen dadurch erst recht interessant werden und trotz solcher Verbote für Minderjährige erreichbar sind. Vorrangig sind daher Maßnahmen der Aufklärung und Sensibilisierung, die wiederum „auf Augenhöhe“ kommuniziert werden sollten, damit sie akzeptiert werden. Das betrifft zum Beispiel auch den Umgang mit **gewalthaltigen Computerspielen**. Statt eines pauschalen Verbots bieten sich hier eine bessere Aufklärung und die Entwicklung von Alternativen an. Wenn über die Vergabe der bisherigen Computerspielpreise hinaus die Entwicklung jugendgerechter und attraktiver Online- und Computerspiele gefördert würde (ähnlich wie die Filmförderung), wäre nicht nur der Jugendschutz verbessert, sondern zugleich ein Beitrag zur Förderung der heimischen Wirtschaft geleistet.

III. Chancen freier Internetnutzung für die Unternehmen

1. Marktchancen und Wertschöpfung

Das Internet bietet nicht nur einen elektronischen Marktplatz, auf den etablierte Unternehmen ihren Geschäftsverkehr verlagern können. Es fördert auch die Entwicklung neuer, **innovativer Geschäftsmodelle**, erschließt neue, **grenzüberschreitende Märkte** und ermöglicht einen **raschen und unkomplizierten Markteintritt**. Unabhängig davon, ob man dies überhaupt wollte, wäre es sowohl volkswirtschaftlich als auch wirtschaftspolitisch verfehlt, Geschäftstätigkeit im und über das Internet und die damit verbundene Innovationskraft durch staatliche Maßnahmen mehr als notwendig einzuschränken. Im Gegenteil: Das Internet ist zu einem wesentlichen und unverzichtbaren **Multiplikator in der globalen Wertschöpfungskette** avanciert. Dessen innovative und prozessoptimierenden Potentiale einzuschränken hieße, der Weltwirtschaft (und damit zugleich der heimischen Wirtschaft) enorme Wachstumsmöglichkeiten zu verwehren. Staatliche Regulierung

sollte deshalb insbesondere die **Gewährleistung des Wettbewerbs und der Chancengleichheit** zum Ziel haben, um die Freiheit aller Marktteilnehmer zu gewährleisten.

2. Notwendigkeit der Dispositions- und Planungssicherheit

Geschäftliche Aktivitäten verlaufen unterdessen zuweilen an der Grenze zwischen Geschäftstüchtigkeit und Betrug. Zum Ausgleich der **Interessen der schutzbedürftigen Verbraucher** einerseits und freier **unternehmerischer Entfaltung** andererseits sollte die Entwicklung neuer Geschäftsmodelle sorgfältig beobachtet und durch frühzeitige Grenzziehung **Dispositions- und Planungssicherheit** gewährleistet werden. Systematischer Missbrauch von (vermeintlichen) Rechtspositionen (wie etwa bei den sog. AboFallen) sollte durch gesetzliche Grenzziehung unterbunden (und nicht der Rechtsprechung überlassen) werden. Verbraucherschutz ist im Interesse sowohl der Verbraucher als auch der (seriösen) Unternehmen. Unklarheiten über seine Reichweite nutzen unterdessen beiden nicht.

3. Unternehmen im Wettbewerb mit globalen und staatlichen Anbietern

Umgekehrt sollte auch zugunsten deutscher Unternehmen, die sich strikt an europäische und nationale Anforderungen des Datenschutz- und Urheberrechts halten, überlegt werden, wie sich diese im strengen Wettbewerb mit globalen, weniger datenschutzsensiblen Unternehmen besser behaupten können, ohne das erwünschte Datenschutzniveau dabei abzusinken.

Zudem stehen deutsche Unternehmen (etwa als mittelständische E-Government-Lösungsanbieter) vielfach auch im Wettbewerb mit staatlichen IT-Dienstleistern, die sich mit Softwareentwicklung und IT-Dienstleistungen auf dem Markt bewegen, dabei aber Privilegien (z.B. Umsatzsteuerbefreiung, Insolvenzunfähigkeit, mittelbare Finanzierung über Steuergelder) genießen. Insofern sind **faire Wettbewerbsbedingungen** herzustellen. Ebenso sind staatliche Technologievorgaben, insbesondere im Bereich der IT-Standardisierung, sowie die zentrale IT-Steuerung durch staatliche Gremien wie den IT-Planungsrat vor dem Hintergrund grundrechtlicher Unternehmensfreiheiten zu sehen. Staatliche IT-Steuerung muss innovationsfreundlich und marktorientiert ausgerichtet sein, um zukunftsfähig zu bleiben.

IV. Chancen freier Internetnutzung für den Staat

1. Die elektronische Verwaltung: bürgernah und serviceorientiert

Nicht nur Bürger und Unternehmen, sondern auch der Staat profitiert vom Internet. Vielfältige Einsatzmöglichkeiten internetbasierter Dienste in der Verwaltung machen E-Government zum

In Freiheit und Fairness.

Motor der Verwaltungsmodernisierung. Damit einher geht eine effizienzsteigernde Geschäftsprozessoptimierung. Der Interneteneinsatz führt zur Flexibilisierung der Kontakte zwischen Bürgern und Behörden, Beschleunigung der Verwaltungsvorgänge, Zeitersparnis und Ressourcenschonung. Für Unternehmen bedeutet die optimierte Aufstellung der deutschen Verwaltung einen **Standortvorteil**, weil zum Beispiel Genehmigungen schneller erteilt werden und die Servicequalität steigt. Insgesamt kann die Verwaltung **bürgerfreundlicher** agieren, weil sie neue Zugänge für Verwaltungsdienstleistungen schafft, Verwaltungsverfahren einfacher und verständlicher gestalten kann und dem Bürger „auf Augenhöhe“ gegenüber tritt. Neue Technologien zur Authentifizierung und rechtsverbindlichen Kommunikation sollen für eine **sichere und vertrauenswürdige Abwicklung elektronischer Prozesse** sorgen.

2. Blended Government: Mischung aus elektronischem und persönlichem Service

Die skizzierten Vorteile eines umfassenden IT- und Interneteneinsatzes in der staatlichen Verwaltung werden unterdessen durch rechtliche und tatsächliche Rahmenbedingungen relativiert. So ist die Verwaltung mittelfristig gezwungen, **hybride Verwaltungsverfahren** anzubieten, also konventionelle Kommunikation neben elektronische Kommunikation zu stellen („blended government“); jedenfalls solange bis die neuen Kommunikationsformen über flächendeckende Internetzugänge für jedermann erreichbar und in der Handhabung zumutbar sind. Hierfür bedarf es sowohl einer **konsequenten Breitbandversorgung** (besonders in ländlichen Gegenden) als auch der Vermittlung der notwendigen Medienkompetenz. Auch zukünftig wird die persönliche Betreuung durch Verwaltungsmitarbeiter eine wichtige Rolle bei der Aufgabenerledigung spielen, zumal diese dank höherer Verwaltungseffizienz mehr Zeit für den Bürger haben sollten (und sie nicht „wegrationalisiert“ werden).

3. E-Government erfordert akzeptanzstiftende Begleitmaßnahmen

Zu berücksichtigen ist auch, dass Innovationen gegenüber retardierenden Kräften nur dann durchsetzbar sind, wenn ein **Mindestmaß an Akzeptanz** bei den Betroffenen erzeugt wird (Notwendigkeit des „change management“). Den Bürgern, aber auch den Verwaltungsmitarbeitern soll vermittelt werden, welche Vorteile der IT- und Interneteneinsatz auch in ihrem Umfeld hat. Deren Sorgen sind ernst zu nehmen und, soweit möglich, zu zerstreuen. Das gelingt am ehesten, wenn Prozesse des E-Government einen unmittelbaren, hohen Nutzen für die Anwender haben, wenn sie anwenderfreundlich und sicher gestaltet werden und Hilfe bei der Umstellung auf neue Systeme angeboten wird. Verbleibende artikulierte Sorgen der Anwender können unter Umständen aber auch Anlass geben, Gefahren oder Risiken neu einzustufen.

IT-Einsatz ist Vertrauenssache. Die Unmerklichkeit und (buchstäbliche) Unbegreiflichkeit elektronischer Prozesse rückt die Vertrauensbildung in das Zentrum jeder technikgetriebenen Innovationsbemühung. Der Staat hat in Bezug auf IT-Einsatz und Internetnutzung unterdessen viel Vertrauen verloren, nicht zuletzt aufgrund gescheiterter IT-Projekte, Datenpannen und verfassungswidriger Gesetze (Online-Durchsuchung, Vorratsdatenspeicherung, Computerwahlen

u. a. m.). Neben den Herausforderungen einer fundamentalen, wegweisenden und visionären Verwaltungsreform muss der Staat zugleich **akzeptanzstiftende Begleitmaßnahmen** treffen, über die er Vertrauen zurück gewinnen und die Legitimität seiner Reformpolitik steigern kann.

4. Modernisierung und Vertrauensstiftung durch eine neue Offenheit

Eine besondere Chance, die Verwaltungsmodernisierung mit Hilfe elektronischer Medien voranzutreiben und Vertrauen beim Bürger zurück zu gewinnen, bietet das Konzept **Open Government/Open Data**, wonach sich die Verwaltung gegenüber dem Bürger mehr und mehr öffnet und solche Informationen zum internetbasierten Abruf über web 2.0-Technologien (Portale, social web) bereithält, die für den Bürger (aber auch Unternehmen) nützlich sind. Ein solches Konzept wird derzeit weltweit diskutiert und kommt teilweise bereits (etwa in den USA) zur Anwendung. Es dient als Ausprägung des **Transparenzprinzips** der Verstärkung der Demokratie, hilft zur Vereinfachung der Verwaltungsabläufe und hat akzeptanzstiftende Wirkung beim (zuweilen politik- und staatsverdrossenen) Bürger. Open Government ist Erfolg versprechend. **Verwaltungsinformationen sollen strukturiert online verfügbar** gemacht werden. Wichtig ist auch, dass die relevanten Informationen durch den Urheber hinreichend erklärt werden. Scheintransparenz muss vermieden werden. Schutzwürdige personenbezogene Daten und geheimhaltungsbedürftige Sachdaten sind ausgenommen. Die hierdurch auf lange Sicht erreichbare effiziente Bürgerbeteiligung am Verwaltungsgeschehen, durch die der **Bürger zur Ressource** avanciert, unterstützt den Gedanken der Verwaltungsmodernisierung durch E-Government (E-Partizipation). Der virtuelle Raum verbindet Amtsstube und Wohnzimmer und vermag die oft als obrigkeitlich empfundene Distanz der Behörden zu den Bürgern ein Stück weit aufzuheben. Umgekehrt stärkt das Internet den Gedanken des Ehrenamtes; der Bürger avanciert zur Ressource. Dadurch entsteht responsive Demokratie, nämlich **repräsentative Demokratie** mit dem Ohr am Puls der Zeit. Ein willkommener Nebeneffekt ist die Wertschöpfung durch „Veredelung der Rohdaten“, wenn diese nämlich in neue Geschäftsmodelle, Produkte und Dienstleistungen einfließen.

V. Technische, organisatorische und rechtliche Rahmenbedingungen für freie Internetnutzung

1. Nachhaltiger Schutz durch Befähigung zur Risikovorsorge

Das Internet bietet eine Vielzahl an Chancen für die Menschen, für Unternehmen und für den Staat. Es birgt aber auch Risiken. Das Konzept der „Internetnutzung in Freiheit und Fairness“ beruht auf der Leitidee, dass die Akteure im Social Web, E-Commerce, E-Business und E-Government den beschriebenen Chancen am ehesten zur Geltung verhelfen, wenn sich der Staat auf die Gestaltung und Regulierung eines freiheitssichernden Rahmens für die Internetnutzung beschränkt und insbesondere den **Bürger befähigt, selbstbestimmt und selbstbewusst zu entscheiden**, ob, in welchem Maße und mit welcher Zwecksetzung er das Internet für seine Belange

In Freiheit und Fairness.

nutzt. Die hierfür erforderliche **Medienkompetenz** muss in den Schulen vermittelt werden, aber nicht nur dort. Im Rahmen einer **Qualifizierungsoffensive** sollen innovative Ideen (auch und gerade mit Hilfe der Internetgemeinschaft) entwickelt werden, um das notwendige technische, aber auch funktionale Basiswissen schnell zu allen Bürgern zu bringen (unabhängig vom Alter, von der Vorbildung oder dem Standort des Betroffenen). Medienkompetenz im Sinne einer vierten Kulturtechnik bedeutet weit mehr als nur technisches Computerwissen oder Omnipräsenz in sozialen Netzwerken. Vielmehr geht es auch und besonders um eine selbstbestimmte und selbstbewusste, reflektierte und sensible Mediennutzung in Kenntnis der immanenten Chancen und Möglichkeiten, Risiken und Gefahren. Eine solche Medienkompetenz kann nicht statisch erworben werden, sondern ist geradezu das Paradebeispiel für die **Notwendigkeit „lebenslangen Lernens“**.

2. Der Staat als „Schiedsrichter“

Der **Appell an die Fairness** soll die Internetnutzer daran erinnern, dass mit dem Gebrauch von Freiheitsrechten in einer Gemeinschaft auch Verantwortung gegenüber jenen Personen übernommen wird, für die die freie Internetnutzung auch nachteilig und sogar verletzend sein kann. Wie im „realen“ Leben kann der Staat (schon wegen seiner verfassungsrechtlichen Schutzpflichten) Gefährdungen und Rechtsgutverletzungen nicht tatenlos hinnehmen, diese umgekehrt aber auch nicht vollständig unterbinden, will er am Prinzip der Freiheit festhalten. Er kann aber – bildlich gesprochen – wie ein „Schiedsrichter“ das freie „Spiel“ der Internetnutzer beobachten, ab und zu lenkend, ermahnend oder auch sanktionierend eingreifen, ohne den „Spielfluss“ übermäßig zu stören. „Spielregeln“ entwirft der Staat – soweit erforderlich – unter Berücksichtigung der „Spielerinteressen“. Dieser **subsidiär wahrzunehmende Gestaltungsauftrag** bedeutet – in Verbindung mit der Erfüllung von Schutzpflichten und der Gewährleistung von Rechtsschutz für die Schwächeren im Internet – eine Mammutaufgabe für den Staat. Die Schaffung, Erhaltung und permanente Weiterentwicklung einer **sicheren IT-Infrastruktur** ist notwendige Voraussetzung für die freie Internetnutzung. **Internetkriminalität** muss so bekämpft werden, dass Gefahren so weit wie möglich vermieden, abgewehrt oder minimiert werden. Der Balance von Freiheit und Sicherheit willen müssen polizeiliche Befugnisse aber so gestaltet sein, dass sie nicht unverhältnismäßig in Freiheit und Privatsphäre der Bürger eingreifen.

3. Internetsperren als untaugliches Instrument

Technische Instrumente sind auf ihre Eignung für die Erfüllung legitimer öffentlicher Aufgaben zu überprüfen. In diesem Zusammenhang bestehen insbesondere **erhebliche Bedenken gegen Internetsperren** als Instrument im Kampf gegen inkriminierte Inhalte wie Kinderpornografie. Zwar mögen entsprechende Stoppschilder im Netz die Erreichbarkeit solcher Webseiten auf den ersten Blick erschweren. Auch der Appell an das Rechtsbewusstsein potentieller Konsumenten wirkt auf den ersten Blick rechtfertigend. Der Netzrat der CSU erkennt dabei das Bestreben all derjenigen an, die sich im Glauben an die Wirksamkeit im Kampf gegen Kinderpornografie für Internet-Sperren eingesetzt haben.

Sperren können (von Anbietern und Konsumenten) leicht umgangen werden und schießen über ihr Ziel hinaus, weil durch sie auch der Zugang zu legalen Inhalten gesperrt werden kann. Außerdem sind sie kontraproduktiv: Die Sperrlisten können durch spezielle Suchstrategien nachgebildet werden und bieten – einmal ins Netz gelangt – gleichsam „Surftipps“ für die interessierten Kreise. Schließlich stellt sich die Frage, wie man wirksam verhindern kann, dass eine einmal etablierte Sperrinfrastruktur zukünftig auch für andere Inhalte verwendet wird. Ob dies aktuell auf der politischen Tagesordnung steht, ist insoweit nicht relevant. Meinungs- und Informationsfreiheit, die nach der Rechtsprechung des Bundesverfassungsgerichts für die Demokratie „schlechthin konstituierend“ sind, fordern im Internetzeitalter eine freiheitssichernde Infrastrukturgestaltung. Vor allem aber wird durch solche Sperren kinderpornografisches Material nicht entfernt, sondern der trügerische Eindruck erweckt, dass der damit zugrundeliegende Markt, beruhend auf tausendfachem Kindesmissbrauch, eingedämmt werde. Das verstellt den Blick auf notwendige Ermittlungsmaßnahmen. Das **vorzugswürdige Prinzip „Löschen statt Sperren“** ist demgegenüber frei von „schädlichen Nebenwirkungen“. Es setzt allerdings voraus, dass stärker als bisher grenzüberschreitend versucht werden muss, Kindesmissbrauch nicht nur unter Strafe zu stellen, sondern auch wirksam mit allen zur Verfügung stehenden Mitteln zu bekämpfen. In praktisch keinem der relevanten Staaten mit entsprechenden Serverstandorten genießen Hersteller und Vertreiber kinderpornografischen Materials einen rechtlichen Schutz, durch den eine wirksame Löschung verhindert würde. Beschränkt man eine solche konzertierte Aktion auf weltweit geächtete Verbrechenformen wie eben Kindesmissbrauch, könnte ein Konsens hergestellt werden, ohne die Freiheit der Internetnutzung in Frage zu stellen. Wobei sich die Alternative, das Kindeswohl zu Lasten freier Internetnutzung zu stärken, ohnehin nicht stellt, weil die Einschränkung dieser Freiheit wie gesehen sowohl den Kindesmissbrauch als auch dessen Dokumentation nur (kurzfristig) unsichtbar, aber nicht ungeschehen machen würde. Solche Verbrechen müssen verstärkt an der „Quelle“ bekämpft werden. Je stärker der reale Kindesmissbrauch unterbunden wird, um so weniger Bildmaterial entsteht, das diesen im Internet dokumentiert. Und umgekehrt: Wenn man den Online-Vertrieb ausdünn, könnte dies auch Auswirkungen auf „bestellten Kindesmissbrauch“ haben. Die Kriminalitätsbekämpfung ist in diesem Bereich in der Tat schwierig. Es müssen auch neue Wege erforscht und diskutiert werden. Internetsperren haben sich nach vorherrschender Expertenmeinung aber als falscher Weg erwiesen.

4. Internetkriminalität und Terrorismus wirksam bekämpfen

Politik und Gesellschaft müssen sich darüber bewusst werden, dass die Digitalisierung **neue Mittel und Wege für Kriminalität und Terrorismus** eröffnet. Die Debatte um etwaige Eingriffsbefugnisse staatlicher Ermittlungsbehörden ist stark geprägt durch die Grenzziehung grundrechtlicher Freiheiten der (unbescholtenen) Bürger, deren Privatsphäre durch technische Überwachungsmaßnahmen betroffen wird. Umgekehrt wird seitens der staatlichen Ermittlungs- und Verfolgungsbehörden auch ein großes Maß an Eingriffsbefugnissen verlangt, um bestehenden, aber auch antizipierten Gefahren Herr werden zu können. 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 – Gefährdungs-**

In Freiheit und Fairness.

potentiale in einer globalisierten und digitalisierten Welt treten. Ebenso wie der Staat Inlands-kriminalität 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 und einer verbesserten internationalen Zusammenarbeit könnte die Entwicklung neuer freiheitsschonender Technologien zur Früherkennung krimineller Bedrohungen einen Beitrag zur Balance von Freiheit und Sicherheit im Internet bieten.

5. Gewährleistung von Netzneutralität

Von besonderer Bedeutung für eine Internetnutzung in Freiheit und Fairness ist auch die **Gewährleistung von Netzneutralität** in dem Sinne, dass eine gleichberechtigte Übertragung aller Datenpakete erfolgt, unabhängig davon, woher diese stammen, welchen Inhalt sie haben oder welche Anwendungen die Pakete generiert haben. Die Ende 2009 verabschiedete EU-(Änderungs)Richtlinie (2009/136/EG) über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen hat die Netzneutralität als politisches Ziel und als von den nationalen Regulierungsbehörden zu fördernden Regulierungsgrundsatz festgeschrieben. Sie ist damit der Ausgangspunkt für **verhältnismäßige und wettbewerbsfördernde nationale Maßnahmen** in diesem Bereich.

6. Smarte Technologien erfordern ein „Smart Privacy Management“

Die Politik muss sich aber auch in verstärktem Maße darüber bewusst werden, dass die Gesellschaft erst am Anfang der digitalen Revolution steht. Was heute das Web 2.0 ist, wird in nicht allzu ferner Zukunft in eine umfassende Digitalisierung und Vernetzung des Alltags münden. **Smarte Technologien** werden den Einzelnen dann in fast jedem erdenklichen Handlungszusammenhang begleiten. Dieses innovative Zukunftsmodell ist mit enormen Potentialen verbunden, nicht nur um die Lebensqualität des Einzelnen zu erhöhen, sondern auch für das Gemeinwesen insgesamt. Unter den Stichworten „Smart Grid“ (intelligente Energienetze) und „Smart Metering“ (digitale Stromzähler) zeichnen sich zum Beispiel außerordentliche Möglichkeiten für eine effiziente Energienutzung ab.

Die Rechte des „digital citizen“ dürfen unterdessen nicht mit dem Verweis auf eine unvermeidliche Veränderung der äußeren Umstände in den Hintergrund treten. Das informationelle Selbstbestimmungsrecht als unbedingter Garant individueller Freiheit muss ein integraler Bestandteil der Systeme des virtuellen Alltags der Zukunft werden. Das ist eine Aufgabe, der sich alle Beteiligten – Staat, Unternehmen und Zivilgesellschaft – in gemeinsamer Verantwortung stellen müssen. Das „Smart Life“ muss den Menschen Rechtssicherheit – insbesondere auf dem Gebiet des Datenschutzes - bieten können. Hilfreich kann hier ein **„Smart Privacy Management“** sein. Rechtsschutz in diesem Sinne wird sich insbesondere durch eine adäquate – das heißt rechtssichere – Gestaltung der Technik herstellen lassen. Die wesentlichen Prinzipien des Rechts

müssen schon bei der Ausgestaltung der Systeme in deren technische Abläufe integriert werden (Privacy by Design). So sollen datenschutzfreundliche Voreinstellungen Nutzerinteressen bereits bei der Softwareentwicklung berücksichtigen (Privacy by Default), sollen Anbieter smarterer Technologien Eingriffe in die Privatsphäre offen legen (Privacy by Transparency) und den Nutzern wirksame Hilfe bei der datenschutzkonformen Anwendung bieten (Privacy by Assistance). Schließlich soll es die Möglichkeit zur Feinabstimmung und Anpassung an den eigenen Bedarf der IT-Nutzung geben (Privacy by Adjustment). Weil selbst solche Maßnahmen und Instrumente gewisse Risiken bei der Digitalisierung des Alltags nicht ausschließen können, sorgen weitere vertrauensbildende Maßnahmen (u. a. in der Gestaltung der Geschäftsmodelle) für die Vereinbarkeit von Unternehmens- und Verbraucherinteressen (Privacy by Trust). Auf diese Weise entsteht ein umfassendes, integriertes Datenschutzkonzept („made in Germany“), das sogar neue Geschäftsfelder erschließen kann (Datenschutz als Geschäftsmodell).

VI. Ausblick: Technik für Menschen

Internetnutzung in Freiheit und Fairness kann das Leitbild der Informationsgesellschaft sein, die innovative Technologien als Motor der Modernisierung von Staat und Verwaltung, Wirtschaft und Gesellschaft sieht, sich dabei aber einer Werteordnung besinnt, die ein gedeihliches Zusammenleben der Menschen fernab von reinen Nützlichkeitsabwägungen ermöglicht. Die Errungenschaften des demokratischen Rechts- und Sozialstaates mit seiner Freiheitsordnung sind dort, wo sie – auch durch moderne Technologien – gefährdet sind, zum Wohle Aller zu bewahren. Das Internet und die mit ihm korrespondierende IT sind ein hilfreiches Medium zur Erfüllung von Aufgaben und Befriedigung von Bedürfnissen – aber auch nicht mehr. IT-Einsatz „um jeden Preis“ darf es nicht geben. Automatisierte Prozesse sollen dem Menschen Freiheit geben, ihn aber nicht ersetzen oder seiner Individualität berauben. **IT soll den Menschen dienen, nicht umgekehrt.**

Internetnutzung in Freiheit und Fairness.

10 Positionen für Staat, Wirtschaft und Gesellschaft

1. Das Internet ist so, wie es sich entwickelt hat und wie es zurzeit jedermann zur Verfügung steht, Ausdruck von Freiheit und soll auch weiterhin ein Ort freier Entfaltung persönlicher, wirtschaftlicher und politischer Interessen bleiben. **„Freiheit und Fairness“ als Leitbild der Netzpolitik** werden vor diesem Hintergrund realisiert durch staatliche Zurückhaltung (Grundsatz der Subsidiarität), Interessenausgleich (Gebot der Rücksichtnahme) und Vorsorge (Schaffung einer sicheren IuK-Infrastruktur).
2. Internet und Informationstechnologie durchdringen zunehmend Staat und Wirtschaft und letztlich alle Lebensbereiche der Menschen. **Allgegenwärtige IT** verändert auch die Rolle des Rechts, weil das menschliche Verhalten zunehmend in globalen, fremdgesteuerten Netzwerken stattfindet. IT-Herrschaft kann nur zum Teil durch den Staat und nur zum Teil durch gesetzliche Regulierung ausgeübt und gewährleistet werden. Global agierende IT-Unternehmen und mächtige Netzwerke schaffen Bedingungen, unter denen neue Wege der IT-Steuerung begangen werden müssen.
3. Schon aufgrund seiner **verfassungsrechtlichen Schutzpflichten und Ordnungsaufgaben** darf der Staat das Internet aber nicht „sich selbst“ überlassen. Vielmehr obliegt ihm die Schaffung eines Ordnungsrahmens zur Gewährleistung von Wettbewerb und Chancengleichheit, IT-Sicherheit und Dispositionssicherheit, Transparenz, Verlässlichkeit und Vertrauen. Zudem hat er für jene Wertordnung einzutreten, die das Grundgesetz der Gemeinschaft sowohl im realen als auch im virtuellen Raum vorgibt.
4. Zur Freiheit gehört auch (**Selbst-**) **Verantwortung**, die die Nutzer im Internet tragen, soweit staatlicher Schutz als Konsequenz einer freien Internetnutzung nicht gewollt ist oder nicht in Anspruch genommen wird. Es müssen adäquate Formen eines **freiheitssichernden Rechtsschutzes** entwickelt werden, der als Rechtsschutz *im* Internet und nicht *gegen* das Internet konzipiert werden soll. Rechtliche Regulierung muss auch die technischen Bedingungen und die funktionale Wirkungsweise des Internet beachten. Neben Gebote, Verbote und Sanktionen treten technische Instrumente und Elemente der Selbstregulierung.
5. Der **Schutz der Schwächeren und von Minderheiten** ist unabhängig davon – soweit möglich – zu gewährleisten. Die Vermittlung eines ausreichenden Maßes an **Medienkompetenz** (im Sinne eines reflektierten und sorgfältigen Umgangs mit neuen Medien und besserem Verständnis der Chancen und Risiken der Informationstechnologien) hat hohe politische Priorität. In diesem Sinne ist Bildungspolitik ein wesentlicher Bestandteil von Sicherheitspolitik und Risikomanagement im Internetzeitalter.
6. Das **Urheberrecht** bedarf einer Neuorientierung, bei der der berechnete Schutz von Kreativität und Innovation unter den Bedingungen eines anonymen und flüchtigen Netzes einerseits und neuer Distributionsformen für digitalisierte geistige Schöpfungen andererseits zu

betrachten ist. Der „einfache Nutzer“ braucht eine verständliche Anleitung, welche Nutzungsformen insoweit von vorneherein gesetzlich erlaubt sind oder zumindest vertraglich ermöglicht werden.

7. Freie Internetnutzung bedeutet auch Freiheit zum Missbrauch und explizite Freizügigkeit. Deshalb ist ein besonderer **Schutz der Kinder und Jugendlichen** erforderlich, weil deren Zugang zum Netz nur eingeschränkt kontrolliert werden kann. Im Vordergrund stehen Bildungs- und Erziehungskonzepte, Selbstregulierung, technische Vorkehrungen und die Schaffung attraktiver jugendschutzkonformer Alternativangebote (besonders im Bereich der Online-Spiele).

8. Soweit sich die freie Internetnutzung in der Planung und Durchführung von Straftaten oder gar extremistischer oder terroristischer Umtriebe äußert, sind **Ermittlungs- und Verfolgungsmaßnahmen** der zuständigen Behörden auch im virtuellen Raum erforderlich. Dabei ist – auch in Ansehung der Rechtsprechung des Bundesverfassungsgerichts – auf die Verhältnismäßigkeit der Mittel und Methoden zu achten, damit weder die Privatsphäre der (unbescholtenen) Internetnutzer übermäßig eingeschränkt noch die freiheitliche Infrastruktur des Internet in Frage gestellt werden.

9. Das Internet bietet sowohl etablierten Unternehmen als auch Unternehmensgründern attraktive Möglichkeiten für **innovative Geschäftsmodelle**. Soweit hier im Verbraucherschutz, Datenschutz oder Wettbewerbsrecht juristisches Neuland betreten wird (z.B. beim Cloud Computing), benötigen Unternehmen Dispositions- und Planungssicherheit, damit sich die Rechtsunsicherheit nicht investitionsfeindlich auswirkt. Der Staat sollte die freie und faire Bereitstellung und Nutzung innovativer Dienste fördern und formaljuristische Hürden nur dort errichten, wo dies das Gemeinwohl oder überwiegende Rechtsgüter erfordern.

10. Dem Staat bieten die elektronischen Medien die Chance zu mehr **Bürgernähe, Service und Transparenz**. E-Government und „Open Government/Open Data“ unterstützen den Prozess der Verwaltungsmodernisierung. Die eingesetzte Technik muss dabei sicher, vertrauenswürdig und für die Anwender nützlich sein. Das Internet bietet zahlreiche Möglichkeiten, Demokratie zu (er-)leben und bürgernah zu gestalten, sei es, dass der Bürger auf elektronischem Wege Zugang zu Verwaltungsinformationen bekommt (Open Government) oder der Staat seinen Bürgern dort begegnet, wo diese sich als „Netizen“ aufhalten (government 2.0). Open Government im Sinne einer kontextbezogenen Aufbereitung und Erläuterung wesentlicher Entscheidungen und Fakten stärkt die Demokratie: Es macht hoheitliches Handeln für den Bürger begreifbar und ermöglicht ihm Teilhabe am staatlichen Geschehen. Responsive Demokratie hilft Staat, Verwaltung und Politik, Vertrauen beim Bürger zu gewinnen und Akzeptanz für ihre Entscheidungen zu stiften.

Epilog

Sehr geehrte Damen und Herren,

Ziel dieses Positionspapiers ist es, der Politik – und damit letztlich den demokratisch legitimierten Entscheidungsträgern –, einen Kompass für die gegenwärtigen und zukünftigen netzpolitischen Herausforderungen in der Informationsgesellschaft des 21. Jahrhunderts an die Hand zu geben. Einzelne Fragestellungen der aktuellen Diskussion werden exemplarisch zur Erläuterung der vorgeschlagenen Weichenstellungen dargestellt. Der CSU-Netzrat versteht sich insoweit als ein unabhängiges Dialogforum von Wissenschaft, Wirtschaft und Politik, um die parteiinterne politische Willensbildung und Positionsbestimmung in diesem Bereich sachverständig zu unterstützen. Die in diesem Papier vertretenen Positionen bieten Handlungsoptionen mit Empfehlungscharakter auf der Grundlage der aktuellen netzpolitischen Diskussion und der rechtlichen Rahmenbedingungen, deren konkrete Umsetzung den politisch Verantwortlichen auf EU-, Bundes- und Landesebene verbleibt. Wissenschaft und Praxis können – und sollen – in diesem Zusammenhang eine beratende, mitunter auch mahnende, Rolle einnehmen. Ihre Aufgabe ist es, Probleme zu benennen und mögliche Lösungsansätze zu formulieren. Die konkrete Umsetzung bleibt Aufgabe der Politik.

Dabei ist auch zu beachten, dass die netzpolitische Diskussion – auch und gerade von Seiten des Staates und der Parteien – im Jahr 2010 erst richtig aufgenommen wurde. So hat der Bundesminister des Innern, Dr. Thomas de Maizière, mit seinem Netzdialog und seiner Grundsatzrede zur Netzpolitik am 22. Juni 2010 einen ersten Anstoß gegeben, überkommene politische Positionen zu überdenken und ggf. neu zu bewerten. Einen ähnlichen Dialog führte die Bundesverbraucherschutzministerin Ilse Aigner (Verbraucher im Netz - Welche Regelungen brauchen die Verbraucher? Was sollten die Anbieter tun?) am 11. Januar 2011 durch.

In ebenso offener Weise im Dialog mit Wirtschaft, Wissenschaft und Verbänden erfolgt die Diskussion um „Verantwortung und Schutzrechte in der vernetzten Gesellschaft“ innerhalb der von Bundesministerin der Justiz Sabine Leutheusser-Schnarrenberger geführten AG 5 auf dem Nationalen IT-Gipfel der Bundesregierung. Diese (und weitere) Entwicklungen gilt es weiter zu verfolgen und inhaltlich zu berücksichtigen. Dies fällt insofern leicht, als das CSU-Netzratmitglied Professor Heckmann in alle genannten Initiativen involviert ist bzw. war.

Schließlich muss auch die sachverständige Aufbereitung der Problemfelder innerhalb der Enquete Kommission „Internet und digitale Gesellschaft“ beachtet werden, die die aufgeworfenen (Rechts-) Fragen innerhalb von 2 Jahren mit einer Vielzahl von Beratungen und Gutachten unter Einbeziehung zahlreicher externer Experten beantworten soll. Der CSU-Netzrat ist demgegenüber ein kleines Gremium, das erstmals auf Parteiebene erste Orientierungspunkte herausgearbeitet hat. Die Arbeit der Enquete Kommission, für die Dr. Reinhard Brandl, MdB aus der CSU berufen wurde, wird damit weder substituiert noch konterkariert.

Netzpolitik ist ein Politikfeld von hoher Komplexität und hoher politischer Priorität angesichts der erheblichen gesellschaftlichen Veränderungen und rasanten technologischen Entwicklung zu Beginn des 21. Jahrhunderts.

Die parteiinterne und öffentliche Diskussion ist aus Sicht des Netzrates hiermit eröffnet.

München und Passau, den 31.1.2011

Für den Netzrat: Dorothee Bär, Vorsitzende und Prof. Dr. Dirk Heckmann

CSU-Landesleitung

Franz Josef Strauß-Haus
Nymphenburger Straße 64
80335 München
servicecenter@csu-bayern.de

www.csu.de

