
Rede
von Bundesminister
Dr. Thomas de Maizière, MdB
„Grundlagen für eine gemeinsame Netzpolitik der Zukunft“
am 22. Juni 2010 in Berlin

Konrad Zuse schraubte und schraubte – und erfand den Computer. Der Legende nach war er zu faul zum Rechnen und wollte deshalb eine Maschine dafür bauen. Konrad Zuse war ein Pionier des digitalen Zeitalters, ein Vorbild hartnäckigen Strebens. Heute ist sein 100. Geburtstag. Ehren wir einen begnadeten Tüftler, dessen Leben zeigt, dass das Große im Kleinen beginnt.

Und so ist es heute auch in der Netzpolitik. Es geht darum, die Arbeit, die vor uns liegt, anhand einer groben Skizze staatlicher Aufgaben zu beschreiben und zu ordnen, um dann im Kleinen zu beginnen.

Das Phänomen Internet haben wir lange genug erst ignoriert, dann teils unterschätzt, teils überschätzt und vor allem bestaunt.

## A. BEDEUTUNG DES INTERNETS

Das Internet ist Innovationsmotor, Kreativschmiede, Kaufhaus, Arbeitsmittel, Kontaktbörse und vieles mehr. Es ist ein fragmentierter Raum des persönlichen, sozialen, geschäftlichen und öffentlichen Lebens. Ich könnte noch viele weitere Merkmale

nennen, und meine Beschreibung bliebe doch unvollständig. Dampfmaschinen lassen sich besser beschreiben. Sie haben aber auch weniger Funktionalitäten.

Schlüsselfragen unseres Zusammenlebens stellen sich mit dem Internet in neuer Dringlichkeit: Wie nutzen wir die große, weltumspannende Freiheit, die uns das Internet bietet? Wie steht es dabei um den Schutz der Privatsphäre in einem Medium, in dem Privates und Öffentliches ineinanderfließen? Wie weit darf die digitale Erfassung unseres Lebens und unserer Persönlichkeit gehen? Wie sichern wir persönliche Daten vor unerlaubtem Zugriff? Wie schützen wir die Freiheit des Internet und auf welche neuen Gefährdungen müssen wir uns in der digitalen Welt einstellen? Hier sind – nicht nur, aber auch – Antworten von der Politik gefragt, um die ich mich heute bemühen will.

Die netzpolitische Debatte wird nicht selten von Spannungsverhältnissen und scheinbaren Widersprüchen dominiert. Einerseits wollen wir immer mehr Dienste und Möglichkeiten nutzen, andererseits haben wir Angst vor unkontrollierbarer Datenmacht. Einerseits ist der Nutzen globaler Vernetzung allgemein anerkannt, andererseits geht die Angst vor dem Ausverkauf deutscher Datenschutzstandards um. Einerseits soll sich der Staat heraushalten, andererseits einmischen.

## B. GRUNDWERTE EINER GEMEINSAMEN NETZPOLITIK

Bei allem, was wir tun, müssen und wollen wir uns an den Grundwerten unserer Gesellschaft orientieren. Der Einzelne soll frei, selbstbestimmt und eigenverantwortlich handeln, auch im Internet. Dazu gehört auch die Freiheit, Dummheiten begehen zu dürfen, wenn andere dadurch nicht zu Schaden kommen. Der Staat ist – bei allen Schutzpflichten, die er hat – nicht verantwortlich für Art und Umfang der Freiheitsausübung des Einzelnen. Übertriebener Schutz bedeutet zugleich Bevormundung.

Freiheit darf aber nicht als Ellbogenfreiheit missverstanden werden. Zu den zentralen Werten, die wir alle im Netz beachten sollten, gehören deshalb gegenseitiger Respekt und Rücksichtnahme. Der Staat kann für diese Werte werben und sie befördern. Anordnen kann er sie nicht.

Auch im Netz sind rechtlich alle Menschen gleich. Neue „Hohepriester“ der Internetwelt sollte es nicht geben. Nicht alle verfügen über die gleichen Kenntnisse und Fähigkeiten. Wir sollten aber versuchen, einander im Sinne von Chancengleichheit und Solidarität nach Kräften zu unterstützen.

## C. PRINZIPIEN FÜR DIE GESTALTUNG UND WEITERENT-WICKLUNG DER ORDNUNG IM NETZ

Diese Grundwerte sind wichtig für unser Miteinander, egal ob online oder offline. Für die Gestaltung unseres Zusammenlebens im Netz sollten wir darüber hinaus vier Prinzipien beachten, die die Weiterentwicklung unserer Rechtsordnung betreffen.

Erstens: Die Anwendung und Durchsetzung bestehenden Rechts hat Vorrang vor neuer Rechtsetzung.

Viele Phänomene des Internets sind durch das bestehende Recht bereits zufriedenstellend geregelt. Wir sollten daher stets versuchen, zunächst eine Analogie zur „Offline-Welt“ zu bilden.

Regelungsbedarf entsteht erst dort, wo das Internet eine grundlegend andere Wertung verlangt oder die Anwendung des bestehenden Rechts zu Vollzugsdefiziten führt, zum Beispiel wegen der internationalen Dimension des Internets. Wo Regelungslücken bestehen, können wir häufig Analogien bilden, um auf die Wertungen des bestehenden Rechts zurückzugreifen. Wir müssen unsere Rechtsordnung wegen des Internets nicht komplett neu erfinden.

Zweitens: Selbstregulierung hat Vorrang vor neuer Rechtsetzung.

Bevor wir an neue gesetzliche Regelungen denken, sollten wir in einer freiheitlichen Ordnung die Selbstregulierungskräfte von Gesellschaft und Wirtschaft nutzen und einfordern. Erst wo dies nicht zu gesellschaftsverträglichen Lösungen führt oder starke Partikularinteressen das Gemeinwohl überlagern, muss der Staat aktiv werden.

Drittens: Unsere Rechtsordnung muss entwicklungsoffen bleiben und vollziehbar sein.

Die Erfahrung lehrt uns, dass umwälzende technische Entwicklungen in der Regel auch einen Bedarf an neuer Rechtssetzung hervorbringen. Dabei gehorchen Technik und Recht einer jeweils eigenen Rationalität und Geschwindigkeit

Das Recht hinkt der Technik meist hinterher. Das wird oft beklagt. Dies sollten wir aber nicht als Nachteil sehen. Bevor 1835 die erste Eisenbahn in Deutschland fuhr, warnten Ärzte vor den „unerhörten Geschwindigkeiten" von bis zu 40 km/h, die die Menschen angeblich krank machen und gar zu einem "Delirium furiosum" führen sollten. Hätte der Gesetzgeber auf sie gehört und sofort reagiert, stünden wir heute vielleicht nicht in diesem schönen Lokschuppen, sondern auf einem Ponyhof.

In solchen Fällen kommt perspektivisch zum Tragen, was Bernhard Schlink einmal die katechontische, d.h. „aufhaltende“ oder „raumschaffende“ Funktion des Rechts genannt hat. Indem das Recht sich der jeweiligen wissenschaftlichen und technischen Entwicklung nicht nur einfach anpasst, sondern sie manchmal verzögert, schafft es der Gesellschaft und der Politik Raum zum Bedenken und Entscheiden. Momente des Innehaltens bringen nicht selten eine verborgene Vernunft zum Vorschein. Natürlich darf man nicht so lange warten, bis eine rechtliche Regelung gar nicht mehr wirksam werden kann.

Wichtig ist aber, dass die Rechtsordnung entwicklungsoffen bleibt. Sie kann nicht für jede technische Neuerung geändert werden. Gesetze sind daher technikneutral auszugestalten, damit dieses Bedürfnis gar nicht erst entsteht.

Manchmal ist der Gesetzgeber auch gut beraten, Einzelfragen zu technischen Entwicklungen zunächst durch die Rechtsprechung anhand konkreter Fälle klären zu lassen.

Wo der Staat im Internet gesetzgeberisch handelt, muss er den damit verbundenen Anspruch tatsächlich erfüllen können. Er sollte sich daher auf Maßnahmen konzentrieren, die in der digitalen Welt wirklich halbwegs umgesetzt werden können.

Viertens: Entwicklungen des nationalen und internationalen Rechts müssen Hand in Hand gehen.

Bei der Entwicklung unserer Rechtsordnung müssen wir die internationale Dimension immer mit in den Blick nehmen. Gerade das Internet wirft Fragen auf, die sich einfachen nationalen Regelungen entziehen. Die Entwicklung nationalen und internationalen Rechts muss daher Hand in Hand gehen.

## D. ROLLEN DES STAATES

Der Staat hat drei Funktionen rund um das Thema Internet:

1. eine Freiheits- und Ausgleichsfunktion,
2. eine Schutz- bzw. Gewährleistungsfunktion und
3. eine Angebots- und Innovationsfunktion

### I. FREIHEITS- UND AUSGLEICHSFUNKTION

Ich beginne mit der Freiheits- und Ausgleichsfunktion. Die Freiheitsfunktion des Staates im Internet bedeutet, dass der Staat einen Rahmen für die Freiheitsausübung des Einzelnen setzen muss. Die Freude der Freiheitsausübung des einen kann das Leid des anderen sein. Der Staat muss konkurrierende Freiheiten gleichermaßen zur Geltung und manchmal zum Ausgleich bringen – dies meint die Ausgleichsfunktion.

#### 1. PERSÖNLICHKEITSENTFALTUNG DURCH KOMMUNIKATION UND TEILHABE

Das Internet bietet dem Bedürfnis nach freier Entfaltung schier endlose Möglichkeiten. Es mag nicht alles sinnvoll sein, aber Freude macht es den meisten doch.

Die freie Entfaltung der eigenen Persönlichkeit bewirkt, dass wir Informationen über uns, Freunde und Dritte sammeln, nutzen und verbreiten. Wir tun dies auch im Internet.

Das stets wachsende und pulsierende Internet scheint unserem bisherigen Datenschutzrecht, das auf Datenvermeidung und -sparsamkeit angelegt ist, durch Freiheitsausübung zuwiderzulaufen. In diesem Zwiespalt steckt eine gewaltige Herausforderung.

Zunächst: Jeder ist frei, sich im Netz zu entfalten und das Netz zu gestalten. Wir müssen anerkennen, dass es ein „Recht auf persönliche Datenverarbeitung“ gibt und dass es genutzt wird. Es ist in der Offline-Welt so selbstverständlich, dass es keine besondere Beachtung findet. Bei jedem Gespräch im Freundeskreis, bei jedem Kaffeekränzchen reden wir über persönliche Dinge und auch über anwesende oder abwesende Personen. Zwangsläufig verarbeiten wir dabei Daten Dritter. Wäre es anders, wären wir asoziale Wesen.

Bei unseren privaten und sozialen Aktivitäten im Netz müssen wir ebenfalls zunächst einmal von einem Recht auf Persönlichkeitsentfaltung durch Kommunikation und soziale Teilhabe ausgehen. Klatsch und Tratsch sind online nichts anderes.

Diese Erkenntnis ist nicht so trivial, wie sie klingt. Sie bedeutet, dass wir die Verarbeitung von Daten Dritter im Internet nicht nur als Eingriff in deren Rechte, sondern – zumindest im persönlichen und familiären Bereich – zugleich als Ausübung grundrechtlicher Freiheit und Entfaltung sehen müssen.

Zum anderen müssen wir aber die Besonderheiten des Mediums anerkennen. Denn mit dem Internet gewinnt der Einzelne nicht nur neue Möglichkeiten der Kommunikation und sozialen Vernetzung. Er erhält zugleich eine enorme Datenmacht, die er so in der Offline-Welt des persönlichen Miteinanders nicht hat.

Nehmen wir das Beispiel Google Street View. Der Bundesrat berät hier gerade über einen Gesetzentwurf. Der Ansatz dieses Entwurfs ist aller Ehren wert, aber nach meiner Überzeugung falsch:

Wir sollten gesetzgeberisch nicht den Weg einschlagen, dass wir für jeden neuen Dienst ein neues und eigenes Gesetz schaffen. Bei einer solchen Einzelfallgesetz-

gebung würden wir bald hoffnungslos hinterherhinken. Das Recht wäre dann weder technikneutral noch entwicklungsoffen.

Ein anderer Punkt ist aber noch viel interessanter: das Gesetz könnte sich schnell als wirkungslos erweisen. Privatpersonen könnten nämlich die Lücken schließen, die ein Gesetz in Googles Straßenzüge reißen würde. Ein Blogger, der eine lückenlose Darstellung der Straßenzüge in Street View fordert, kündigte bereits an, jedes Haus, das ausgeblendet wird, zu fotografieren und zu geotaggen.

Tatsache ist, dass er und Millionen anderer Privatbürger im Internet durch Veröffentlichung und Vernetzung von Inhalten gemeinsam über nicht viel weniger Datenmacht verfügen, als Google selbst. Bisher hatten nur die Goliaths der automatisierten Datenverarbeitung – der Staat und die Wirtschaft mit ihren teuren Großrechnern – Datenmacht. Das Internet gibt potentiell jedem die Möglichkeit, Daten Dritter zu vernetzen und Datenmacht auszuüben – spätestens seit Web 2.0.

Eine der fundamentalen Veränderungen der Netzgesellschaft ist, dass der Einzelne „Nutznießer“ und „Opfer“ digitaler Persönlichkeitsentfaltung und persönlicher Datenmacht zugleich sein wird. Beides ist Ergebnis gewollter Freiheitsausübung.

Wie soll nun der Staat damit umgehen? Wenn kollidierende Freiheiten aufeinandertreffen, hat der Staat eine Ausgleichsfunktion. In der gegenständlichen Welt bedarf es dazu wenig staatlicher Reglementierung. Das wichtigste Mittel ist das Zivilrecht. Wer durch die Datenverarbeitung anderer einen Schaden erlangt, kann Unterlassungs- und Schadensersatzansprüche geltend machen. Das schärfste Schwert ist das Verbot mit strafrechtlicher Sanktion bei Verleumdung, Beleidigung und übler Nachrede.

In der Offline-Welt wird von diesen Mitteln sehr sparsam Gebrauch gemacht. Sie reichen dennoch v.a. aus zwei Gründen aus:

1. Wir folgen im realen Leben allgemeinen Anstandsregeln und unterliegen einer gewissen sozialen Kontrolle.
2. Wir wissen, dass Klatsch und Tratsch in der Regel kurzlebig sind und die Verbreitung meist auf das private und soziale Umfeld begrenzt ist.

Auch das Internet kennt Formen der sozialen Kontrolle. Wer bei YouTube ein Video für anstößig oder verletzend hält, kann dies melden. Ist die Beschwerde berechtigt, wird es entfernt. Doch sind die Anstandsregeln, gerade was die Grenzen der Verarbeitung von Daten anderer angeht, insgesamt weniger ausgeprägt. Die Zivilgesellschaft selbst muss hier ihr Bewusstsein schärfen. Den Nutzern muss klar sein, dass ihre Entfaltung im Netz in die Freiheiten anderer eingreifen kann. „Was Du nicht willst, das man Dir tut, das füg‘ auch keinem anderen zu“. Diese Verantwortung für eine digitale Rücksichtnahme müssen wir lernen, und zwar von Kindesbeinen an.

Eine Verantwortung für eine gelebte Rücksichtnahme tragen aber auch die Diensteanbieter. Sie dürfen Rücksichtslosigkeit nicht fördern, indem sie die Nutzer durch entsprechende Angebote und Grundeinstellungen dazu verleiten, achtlos Daten Dritter zu vernetzen.

Der Klatsch und Tratsch bleibt in der gegenständlichen Welt schon alleine deshalb in seiner Wirkung begrenzt, weil er in der Regel auf dem flüchtigen gesprochenen Wort beruht und auf einen kleinen Kreis von Zuhörern nicht verlässt.

Anders als in der gegenständlichen Welt ist jede Äußerung im Internet aber potentiell weltweit öffentlich, nichts wird bisher vergessen, alles kann den vertrauten Bereich hinter sich lassen. Das macht die soziale Rehabilitierung eines Geschädigten ungleich schwerer. Umso wichtiger wäre es, dem Internet in Zukunft in bestimmten Bereichen das Vergessen oder zumindest das „Nichtwiederfinden“ beizubringen.

Ziel wären ein „digitales Radiergummi“ und ein Verfallsdatum, das ich an meine Daten anbringen kann. Möglicherweise sollten wir über ein „Recht, vergessen zu lassen“ nachdenken, wie es der EU-Kommission vorschwebt. Hilfreich wäre in vielen Fällen schon ein sog. Indexierungsverbot, bei dem Suchmaschinenbetreiber verpflichtet werden, bestimmte markierte Einträge bei den Sucherergebnissen nicht anzuzeigen.

Angesichts der Datenmacht Dritter, sollten wir dem Einzelnen mehr Mittel an die Hand geben, um sich selbst zur Wehr zu setzen.

Wir könnten beispielsweise das Gebot der Rücksichtnahme von Diensteanbieter so konkretisieren, dass sie ihre Angebote mit „rücksichtsvollen Grundeinstellungen“ im Sinne eines „Respect by default“ ausstatten. Die Diensteanbieter müssten dann selbst ein gewisses Haftungsrisiko tragen, wenn sie ihre Kunden durch Voreinstellungen dazu verleiten, Daten über Dritte preiszugeben und zu vernetzen.

Wir sollten auch die Möglichkeiten zur Durchsetzung von Unterlassungs- und Schadensersatzansprüchen verbessern, ohne damit neue Geschäftsmodelle für Abmahnungen zu ermöglichen.

In der Presse kennen wir das Recht auf Gegendarstellung. Wir brauchen etwas Ähnliches im Internet – ein privates Darstellungsrecht, mit dem sich der Einzelne zur Wehr setzen kann, wenn etwas Falsches oder Ehrenrühriges über ihn im Internet kursiert. Man könnte dies mit einem Anspruch des Betroffenen gegenüber Betreibern von Suchmaschinen verbinden, die eigene Darstellung auf Platz eins einer Trefferliste zu setzen.

Bei anonymen Schmähungen sollte der Geschmähte einen Anspruch auf Löschung gegen den Provider erhalten. Wer sich nicht zu erkennen gibt und öffentlich verletzende Äußerungen verbreitet, darf sich über eine Löschung nicht beschweren.

## 2. INFORMATIONELLE SELBSTBESTIMMUNG IM INTERNET

Betrachten wir nun denjenigen, dessen Daten im Netz durch Unternehmen oder den Staat verarbeitet werden. Hier geht es nicht mehr um Klatsch und Tratsch, sondern um die Kontrolle der eigenen Daten und die Begrenzung und Abwehr von Datenmacht im klassischen Sinne.

### a. HERAUSFORDERUNGEN DURCH DAS INTERNET

Ein Kontrollverlust über die eigenen Daten droht aus verschiedenen Richtungen. Ich möchte drei Phänomene herausgreifen.

Erstens: Mit dem Cloud-Computing speichern Nutzer ihre Daten außerhalb der eigenen Festplatte. Das geht schon los mit dem persönlichen Postfach bei web.de, T-Online oder einem anderen Anbieter. Zunehmend werden ganze Festplatten und Datenbestände von Firmen in Clouds ausgelagert, weil es kostensparender ist.

Solche Speicherplätze müssten eigentlich wie Schließfächer ausgestaltet sein. Sie befinden sich aber im „virtuellen Nebel“ und können wie an der Börse verkauft, kombiniert, untervermietet, nochmals ausgelagert und wieder miteinander verbunden werden. Aus diesem Grunde gibt es nicht „die“ Cloud, sondern zahlreiche Geschäftsmodelle von öffentlichen, privaten und gemischten Clouds mit unterschiedlichen Anbietern und Verantwortlichkeiten. Die Bandbreite reicht bis zu Modellen, wo die Infrastruktur, das Betriebssystem und die Anwendungen komplett ausgelagert und auf unterschiedliche Anbieter verteilt sind – im Extremfall weltweit.

Natürlich werden hier auch jede Menge sensible Daten gespeichert. Die Firmengeheimnisse von Coca Cola und Pepsi könnten an einem gemeinsamen Ort gespeichert sein, den keines der beiden Unternehmen kennt. Datenschutz und Datensicherheit in einer Cloud sind deshalb eine gewaltige Herausforderung. Die Datensicherheit wird dabei eine immer stärkere Rolle für die Gewährleistung des Datenschutzes spielen.

Wir brauchen klare Regeln und Verantwortlichkeiten sowie solide Geschäftsmodelle für Clouds, denen wir umfangreiche und sensible Datenbestände anvertrauen.

Der Unternehmer trägt die Verantwortung, den Dienst sicher anzubieten. Dazu kann auch gehören, dass er dem Nutzer eine einfach anzuwendende Verschlüsselung mit auf den Weg geben muss, so dass am Ende nur dieser Zugang zu den Daten hat. Der Nutzer trägt die Verantwortung, auf seinen Schlüssel aufzupassen.

Solche Regelungen sollten mindestens auf europäischer Ebene verankert werden.

Die zweite große Herausforderung ist die sichere Steuerung von Identitäten im Netz. Bei Cloud-Computing, Online-Festplatten oder Online-Banking ist die sichere digitale Identität der Schlüssel zur Kontrolle der eigenen Daten. Der Cloud-Anbieter muss

wissen, dass derjenige, der Zugang zum virtuellen Schließfach oder zu persönlichen Diensten begehrt, dazu auch wirklich berechtigt ist. Eine sichere Identität brauchen wir auch überall dort, wo wir im Internet am Rechtsverkehr teilnehmen, etwa zum Abschluss eines Geschäfts oder bei Verwaltungsvorgängen.

Entscheidend ist dabei, dass das Gegenüber so viel identitätsbestätigende Daten erhält wie gerade in Bezug auf die jeweilige Rechtsbeziehung nötig sind – aber eben auch nicht mehr. Beim neuen Personalausweis ist dies möglich.

Die dritte große Herausforderung für die informationelle Selbstbestimmung ist die Kontrolle der zunehmenden IT-Systeme und -Verfahren, die unseren Alltag prägen, vom Fernseher, Kühlschrank bis zum Auto. Autos können zum Beispiel dank internetbasierter Technik erkennen, wo Staus oder Gefahren drohen. Dazu muss das Auto mitteilen, wo es sich befindet. Mit der immer weiter voranschreitenden Digitalisierung des täglichen Lebens können Prozesse intelligenter, zeit- und kostensparender, umweltschonender etc. gestaltet werden. Der Einzelne muss jedoch die Kontrolle über die Technik behalten.

Sein Auto sollte im Netz nur dort Spuren hinterlassen, wo es zwingend nötig ist. Und der Einzelne sollte vor allem wissen, welches Gerät über das Internet kommuniziert. Bereits eine schlichte Kennzeichnung wäre hilfreich. Wir sollten auch vorsehen, dass zumindest vor der erstmaligen Kontaktaufnahme eines Geräts mit dem Netz eine aktive Einwilligung erforderlich ist.

In diesen drei Bereichen sehe ich eine Verantwortung des Staates.

Darüber hinaus müssen wir weitere Möglichkeiten nutzen, um die informationelle Selbstbestimmung des Einzelnen zu stärken, indem wir,

- über mögliche Gefahren besser aufklären,
- bestehende Betroffenenrechten einfacher und auch Online ausüben können – zum Beispiel den Widerspruch per Mausklick –
- und die Abhängigkeit von Anbietern mit marktbeherrschender Stellung reduzieren.

Wir brauchen auch mehr echte Verfügungsgewalt über unseren virtuellen Hausrat. Es gibt zum Beispiel in sozialen Netzwerken meist keine Möglichkeit, „seinen Datenbestand mitzunehmen“. Bin ich mit einem Anbieter nicht mehr zufrieden, weil ich den Eindruck habe, dass Datenschutz und Datensicherheit bei ihm nicht gewährleistet sind, muss ich die Möglichkeit haben, zu wechseln und meine Daten mitzunehmen.

Bei der Aufklärung müssen wir früh ansetzen. Kinder und Jugendliche brauchen unsere besondere Aufmerksamkeit. Das von Ministerin Schröder geplante Forum Internet zum Kinder- und Jugendschutz unterstütze ich ausdrücklich.

Bei der Aufklärung sind wir beispielsweise auch mit Kampagnen für die Nutzung sicherer Passwörter bereits auf einem guten Wege. Zur Aufklärung kann und soll auch die einzurichtende Stiftung Datenschutz beitragen.

Ungeachtet der noch zu klärenden organisatorischen Details wollen wir die Durchführung und Veröffentlichung von Vergleichstests zu einer zentralen Aufgabe der Stiftung Datenschutz machen.

Ohne Wettbewerb gibt es dauerhaft keine Freiheit und Selbstbestimmung. Das Netz wird in vielen Bereichen von wenigen, in manchen Bereichen de facto auch nur von einem großen Anbieter beherrscht. Durch ihre marktbeherrschenden Stellungen schaffen sie Abhängigkeiten, die wir auf Dauer nicht akzeptieren können. Wir brauchen mehr Wettbewerb im Netz.

Insbesondere brauchen wir neben der Netzneutralität mehr Verfügungsgewalt über unseren virtuellen Hausrat. Sie ist eingeschränkt, wenn Dienste oder Dateien von einer bestimmten Plattform oder Software abhängig sind. Wenn ich Musiktitel Online kaufe, erwarte ich, dass ich ihn auf den unterschiedlichen Geräten, die ich im Wohnzimmer, im Badezimmer und im Auto habe, abspielen kann.

Die Geschichte des Bürgerlichen Gesetzbuchs zeigt, dass der Staat nicht nur eine freiheitssichernde Funktion hat. Er muss auch für Chancengleichheit Sorge tragen, wenn das freie Spiel der Privatautonomie versagt. Die Verwendung von allgemeinen Geschäftsbedingungen, Haustür- und Internetgeschäfte sind Beispiele für Rechtsbe-

ziehungen, in denen sich Verbraucher und Verkäufer nicht von vornherein auf Augenhöhe begegnen. Durch Einwilligungen und Widerrufsrechte haben wir die Position der Verbraucher gestärkt. Ich unterstütze daher Vorschläge des Verbraucherschutzministeriums, Betroffenenrechte wie den Widerspruch „per Mausklick“ auszuüben. Wir sollten die Ausübung der bestehenden Betroffenenrechte insgesamt vereinfachen, indem wir hierfür die Online-Angebote verbessern. Ein großes Problem, dass wir hierbei in der Vergangenheit hatten, werden wir in Zukunft mit dem neuen Personalausweis besser lösen, nämlich die Identifikation der Betroffenen.

Auch die Ideen vom Datenbrief verfolgt ein richtiges Ziel. Seine Nachteile – weitere Bürokratisierung und Datenzusammenführung – müssen jedoch vermieden werden. Ich habe daher Experten eingeladen, gemeinsam ein praxistaugliches Konzept zu erarbeiten.

Unabhängig vom Datenbrief sollten wir die Transparenz durch bessere allgemeine Informationen im Internet verbessern. Es gibt bereits eine Meldepflicht im Bundesdatenschutzgesetz. Sie gilt für bestimmte Arten der Datenverarbeitung. Der Verarbeitende muss unter anderem angeben, welche Daten er erhebt, zu welchen Zwecken er sie verarbeitet und wem er sie übermittelt. Die Angaben sind in der Regel leicht zu machen und sollten in allgemein verständlicher Form wie das Impressum auf der eigenen Homepage einsehbar sein. Wir müssen hierfür nicht gleich das Gesetz ändern. Wem Datenschutz und Transparenz am Herzen liegen, der kann diese Angaben auch leicht freiwillig machen und noch einen Schritt weiter gehen.

Man könnte diese Information im Internet mit der Möglichkeit verbinden, dass ich als Betroffener mein bestehendes Auskunftsrecht geltend machen kann. Die Ausübung dieses Rechts wäre deutlich erleichtert. Am besten wäre es, wenn das Formular hierfür bereits an die allgemeine Datenverarbeitungsbeschreibung des Unternehmens angehängt wäre.

Der Einzelne verfügt bereits über gute Beschwerde- und Rechtsschutzmöglichkeiten gegen datenschutzrechtliche Verstöße. Sie lassen sich jedoch noch weiter verbessern. Ich habe auf die Bedeutung der Rechtsprechung bereits hingewiesen. Der Bundesgerichtshof hat im März 2010 entschieden, dass gegen Persönlichkeitsverlet-

zungen durch Internetveröffentlichungen im Ausland auch vor deutschen Gerichten geklagt werden kann, wenn die Inhalte typischerweise im Inland abgerufen werden. Dies ist ein großer Schritt in die richtige Richtung. Das könnte der Gesetzgeber übernehmen.

## 3. GARANTIE DER ABWEHRRECHTE GEGENÜBER DEM STAAT

Der Staat unterstützt nicht nur den Einzelnen bei der Wahrnehmung seiner Freiheiten im privaten Bereich. Er hat auch eine die Freiheit sichernde Funktion, die sich gegen sein eigenes Handeln richtet. Das Recht auf informationelle Selbstbestimmung ist als klassisches Abwehrrecht gegen den Staat entstanden, zur Begrenzung staatlicher Datenmacht. Diese Funktion ist auch im Zeitalter des Internets von Bedeutung.

Es wäre rein technisch nicht ausgeschlossen, dass ein Staat das Internet als totalitäres Überwachungsinstrument missbraucht und ohne Rechtsgrundlage breitflächig, anlasslos und heimlich in sämtliche Räume des Internets vordringt. Es mag Staaten geben, die dies tun oder planen. Man kann sich das auch vom Ausland aus vorstellen.

Unser demokratischer Rechtsstaat gehört nicht dazu. Jeder Verdacht in dieser Richtung ist unerhört.

Eine Kriminalisierung des Internets, d.h. eine Herangehensweise, die das Internet ausschließlich als Sicherheitsrisiko betrachtet und in erster Linie Misstrauen gegen den Bürger hegt, kann nicht Ausgangspunkt unseres staatlichen Handelns sein.

Dies gesagt, höre ich bereits den Vorwurf, mit der Vorratsdatenspeicherung hätten wir genau dies getan.

Ich will mich in dieser Frage weder hinter dem Bundesverfassungsgericht noch hinter Europa verstecken. Beide Instanzen geben den Weg vor, wie und in welchem Umfang wir Verbindungsdaten künftig speichern und staatlich nutzen dürfen, ich füge hinzu: und sollten. Doch ich möchte an dieser Stelle ganz deutlich machen:

Eine schrankenlose Anonymität kann es im Internet nicht geben. Für Raubritter und echte Piraten wären das paradiesische Zustände. Aller Freibeuterromantik zum Trotz werden sich aber die wenigsten wünschen, allein auf hoher See Piraten zu begegnen, die nach dem Entern garantiert unerkannt davon segeln.

Deshalb brauchen wir eine vernünftige Balance zwischen Anonymität und Identifizierbarkeit. Das Grundprinzip des Unbeobachtseins der alltäglichen privaten Lebensgestaltung muss dabei im Internet ebenso gewahrt sein wie Sanktionen gegen schwere Rechtsverletzungen. Und dazu braucht es Möglichkeiten, jemanden als konkreten Menschen zu erkennen.

Wir müssen allerdings an eine Identifizierung mit Hilfe von gespeicherten Verbindungsdaten hohe Anforderungen stellen. In einem grundsätzlich öffentlichen Raum wie dem Internet kann die Identifizierbarkeit praktisch nicht ausgeschlossen werden. Aus Sicht des Betroffenen muss aber sicher gestellt sein, dass die Anforderungen an die faktische Identifizierung unter Wahrung der Verhältnismäßigkeit danach ausgestaltet sind, welchem Zweck sie dient, welche Grundrechte betroffen sind, ob er sich im privaten, sozialen oder öffentlichen Bereichen des Internets bewegt und ob er einen Anlass für die Identifizierung gegeben hat.

Die Frage des Beobachtetseins oder Unbeobachtseins lässt sich indessen oftmals schwer beantworten. Was ist der Maßstab für ein „diffus bedrohliches Gefühl des Beobachtetseins (…), das eine unbefangene Wahrnehmung der Grundrechte in vielen Bereichen beeinträchtigen kann“? Das Bundesverfassungsgericht argumentiert in seiner Entscheidung zur Vorratsdatenspeicherung mit diesem Gefühl. Der Gesetzgeber tut eigentlich gut daran, sich bei seinen Entscheidungen nicht auf „diffus bedrohliche Gefühle“ zu verlassen. Er sollte sich an Fakten orientieren.

Vielleicht brauchen wir – auf allen Seiten – ein wenig mehr Vertrauen in die Normalität. Die Erfahrung lehrt, dass unsere Polizei nicht an jeder Ecke steht, und unbescholtene Bürger nicht ständig ihre Unschuld gegenüber übereifrigen Staatsanwaltschaften beweisen müssen.

Wir müssen dafür werben, dass diese Erfahrungen und das darauf basierende Vertrauen in unseren Rechtsstaat auch im Internet gelten. Dieses Vertrauen wird nicht dadurch hergestellt, dass wir das Internet sich selbst überlassen und auf Verbindungsdaten verzichten. Können wir bestimmte schwere Delikte und Gefahren nicht mehr wirksam bekämpfen, weil sie nicht mehr Offline, sondern nur Online passieren, wird dies weder das Vertrauen in den Staat noch ins Internet stärken.

Das Recht des Stärkeren – die Lichthupe des Rasers, der IT-Wissensvorsprung von Kriminellen gegenüber einfachen Nutzern – es wäre sonst die goldene Regel in einer völlig anonymen Netzwelt. Wir müssen daher grundsätzliche Möglichkeiten der Identifizierbarkeit bereit halten. Maßnahmen wie Quick Freezing ermöglichen keine Identifizierung, wenn eine Tat bereits stattgefunden hat und erst später bemerkt wird.

Ich bin überzeugt, dass die Lücke, die wir ohne Verbindungsdaten in die Gefahrenabwehr und Strafverfolgung reißen würden, zu groß ist, als dass man auf dieses Mittel verzichten könnte. Wir dürfen möglicherweise auch gar nicht darauf verzichten.

Der Europäische Gerichtshof für Menschenrechte hat jüngst entschieden, dass der Staat auch ein Untermaßverbot zu beachten hat und seine Schutzpflichten verletzt, wenn er keine Befugnis zum Abruf von Verbindungsdaten bereitstellt. In dem Fall ging es um die Identifizierung eines Pädophilen, der Kontakt zu einem Kind aufnehmen wollte.

### 4. WEITERE ASPEKTE DER FREIHEITSSICHERNDEN FUNKTION DES STAATES

Neben der freien Entfaltung der Persönlichkeit, dem Recht auf informationelle Selbstbestimmung und dem Hinweis auf die Abwehrrechte gegenüber dem Staat, gibt es weitere Aspekte, die der Freiheits- und Ausgleichsfunktion des Staates zuzuordnen sind. Hierzu gehört der Schutz des geistigen Eigentums bzw. das Urheberrecht. Es ist ein wichtiger Bereich, auf den ich jedoch heute nicht näher eingehen möchte. Die Bundesjustizministerin hat sich hierzu jüngst umfassend geäußert.

## II. SCHUTZ- UND GEWÄHRLEISTUNGSFUNKTION DES STAATES

Ich komme zur zweiten Hauptfunktion des Staates neben der Freiheits- und Ausgleichsfunktion. Es ist die Schutz- und Gewährleistungsfunktion. Sie betrifft in erster Linie eine Verantwortung des Staates für das Internet als Infrastruktur, die für alle zugänglich sein muss und die zuverlässig funktionieren muss.

## 1. GEWÄHRLEISTUNG EINER DIGITALEN GRUNDVERSORGUNG

Die Eisenbahn und das Internet haben sich eigenständig durchgesetzt, weil sie wirtschaftlich und gesellschaftlich einen Mehrwert haben.

Der Staat hat in der Vergangenheit regelmäßig Verantwortung übernommen, wenn es um Infrastrukturen und Dienste ging, für die es ein besonderes allgemeines Interesse gibt. Er hat dies etwa bei Eisenbahn und Post getan, indem er sie lange Zeit in eigener Regie betrieb. Nach ihrer Privatisierung stellt der Staat eine flächendeckende Grundversorgung zu angemessenen Preisen sicher.

Das Internet ist wegen seiner herausragenden Bedeutung für das Gemeinwesen mittlerweile eine grundlegende Infrastruktur, wofür auch der Staat Verantwortung übernehmen muss. Er muss die Grundversorgung sicherstellen.

Bei der Wahl der regulatorischen Mittel sollte der Staat mit Augenmaß agieren. Er muss die Innovationsfähigkeit des Internets erhalten. Drei zentrale Anforderungen zeichnen sich bereits heute ab: die Netzneutralität, ein flächendeckender Zugang auch für Menschen fern der Ballungszentren und eine Grundversorgung mit sicheren Basisdiensten wie De-Mail.

Die Netzneutralität besagt, dass grundsätzlich alle Inhalte gleichberechtigt im Internet transportiert werden. Das ist gut und richtig. Die Bundesregierung will die Netzneutralität bewahren. Dafür setzen wir uns auch im europäischen Rahmen ein.

Mit der Breitbandstrategie der Bundesregierung setzen wir uns intensiv dafür ein, dass auch in ländlichen Räumen bald flächendeckend hochleistungsfähige Internetanschlüsse zur Verfügung stehen. Die Verantwortung hierfür trifft aber nicht den Staat allein. Es sind zuvörderst die TK-Unternehmen, die aus wirtschaftlichen Motiven nur

in Ballungsräumen, die sich gut erschließen lassen, Infrastrukturen breitstellen. Sie müssen auch dort investieren, wo der Aufwand größer und Gewinne geringer sind.

Der Staat kann auch eine Grundversorgung an sicheren Basisdiensten sicherstellen. Wir werden dies mit dem neuen Personalausweis und De-Mail tun. Sie ermöglichen eindeutige Authentifizierungen im Rechts- und Geschäftsverkehr sowie eine sichere Kommunikation. Beides sind Schlüsselfunktionen. Sie kommen auch zum Tragen, wenn wir subjektive Rechte wie das datenschutzrechtliche Auskunftsrecht über das Internet wahrnehmen wollen.

## 2. SCHUTZ DES INTERNETS UND SEINER DIENSTE DURCH ANGEMESSENE VERANTWORTUNGSÜBERNAHME

Zur Schutz- und Gewährleistungsfunktion des Staates gehört der Schutz des Internets als Infrastruktur. Wir haben bereits eine nationale Strategie für Cyber-Sicherheit. Die Bedrohung ist sehr real: Große Botnetze könnten das Internet regional und national lahmlegen, vielleicht auch andere Staaten. Das Beispiel Estland zeigt, wie gravierend die Auswirkungen eines solchen Angriffs sein können.

Würde das Internet über Tage oder gar Wochen in Deutschland ausfallen, wäre der volkswirtschaftliche Schaden immens. Teile des wirtschaftlichen und gesellschaftlichen Lebens und der Verwaltung würden zum Erliegen kommen.

Wir haben ein Gesetz, das eine ausreichende Versorgung mit Post- und Telekommunikationsdienstleistungen etwa bei Naturkatastrophen, besonders schweren Unglücksfällen oder im Spannungs- oder Verteidigungsfall sicherstellt. Dies muss grundsätzlich auch für das Internet gelten, und es ist zu klären, welcher speziellen Regelungen es hierfür bedarf.

Der Staat ist beim Schutz des Internets als Infrastruktur aber auch auf die Mitwirkung der Nutzer und Anbieter angewiesen. 35 Prozent der Nutzer geben an, dass ihr Computer bereits infiziert wurde. Dennoch surfen weiterhin 20 Prozent ohne Virenschutz. Jeder Einzelne hat eine Verantwortung, zur Sicherheit des Netzes beizutra-

gen. Hierzu gehört an erster Stelle ein wirksamer Schutz gegen Viren, Schadprogramme und Trojaner, mit denen Botnetze ferngesteuert werden.

Der Einzelne trägt dabei eine größere Verantwortung, je mehr er selbst gefahrgeneigte Dienste einrichtet oder anbietet. Wer eine Homepage bastelt und damit ein öffentliches Angebot schafft, muss sicher stellen, dass sich hierüber keine Schadprogramme und Viren verbreiten. Wer über einen WLAN-Anschluss verfügt, muss dafür Sorge tragen, dass er die marktüblichen Sicherungen gegen unbefugte Nutzung vornimmt.

Der Bundesgerichtshof hat hier meines Erachtens zu Recht auf die allgemeinen Grundsätze der sog. Störerhaftung abgestellt. Er hat dabei auch beschrieben, was für den Einzelnen an Sicherungsmaßnahmen zumutbar ist und was nicht. Insbesondere hat der BGH darauf hingewiesen, dass dem privaten Betreiber eines WLAN-Netzes nicht zugemutet werden kann, seine Netzwerksicherheit fortlaufend dem neuesten Stand der Technik anzupassen.

Aber nicht alles ist dem Einzelnen an Sicherungsmaßnahmen zumutbar. Hersteller von Hard- und Software sowie Diensteanbieter stehen daher ebenfalls in der Verantwortung, und zwar um so mehr, als sie erstens in der Regel besser wissen, wie man sich gegen Angriffe schützen kann und weil zweitens ihre Angebote zum Teil grundsätzlich mehr oder weniger gefahrgeneigt sind.

Wir sollten darüber nachdenken, ob nicht für bestimmte gefahrgeneigte Angebote eine Gefährdungshaftung oder eine Beweislastumkehr bezüglich des Verschuldens in Betracht kommt.

Provider sollten etwa dafür haften, wenn sie keine ausreichenden Vorkehrungen gegen den Transport von Viren und Schadprogrammen treffen. Eine solche Verkehrssicherungspflicht gegen Viren und Schadsoftware sowie Datendiebstahl ist keine Kontrolle von Inhalten. Eine Kontrolle von Inhalten durch die Provider hielte ich für falsch, um das klar zu sagen.

Hier müssten gegebenenfalls noch passende technische Lösungen entwickelt werden. Umgekehrt sollten diejenigen Anbieter bei der Haftung privilegiert werden, die anerkannt sichere Basisdienste nutzen oder integrieren, etwa die Identifikation mit dem neuen Ausweis oder die sichere Kommunikation mit De-Mail.

## 3. ABWEHR VON GEFAHREN UND BEKÄMPFUNG DER KRIMINALITÄT IM INTERNET

Zur Schutz- und Gewährleistungsfunktion des Staates gehören natürlich auch die Gefahrenabwehr und die Kriminalitätsbekämpfung im Internet. Der Staat hat das Recht, in manchen solcher Fälle sogar die Pflicht, in Internetdienste und -nutzungen einzugreifen.

Er muss sich dabei an den Eingriffsbefugnissen der realen Welt orientieren. Das klassische Eingriffsinstrumentarium des Staates zur Gefahrenabwehr und Strafverfolgung muss auch im Zeitalter des Internets zur Verfügung stehen.

Es darf keine Privilegierung und es darf keine Benachteiligung der Strafverfolgung im Internet geben.

Dies setzt freilich voraus, dass dieses Instrumentarium im Internet de jure und de facto einsetzbar ist. Und es setzt voraus, dass unsere Beamten so gut ausgebildet und ausgestattet sind, dass sie es bei Einsätzen im virtuellen Raum auch tatsächlich anwenden können. Hier müssen wir noch besser werden.

Zum Schutz der Sicherheit müssen wir auch unsere technologische nationale Souveränität wahren, nationale Kernkompetenzen erhalten und ausbauen. Hierzu braucht unser Land Forscher und Unternehmer, die strategische IT- und Internetkompetenzen erhalten und ausbauen. Ohne eine starke eigene IT-Industrie geraten wir in Abhängigkeiten, die unsere Freiheiten und unsere Verfassungsidentität gefährden können.

Auch eine verbesserte Ausbildung und Konzentration von IT-Sachverstand innerhalb von Behördenzweigen, wie etwa die Stärkung des BSI, die Bildung von Polizei-

Spezialeinheiten, die Schaffung von Schwerpunktstaatsanwaltschaften und spezialisierten Gerichten, ist wichtig. In bestimmten Bereichen bietet sich auch eine enge partnerschaftliche Zusammenarbeit mit Privaten an. An Maßnahmen im Polizeibereich arbeiten meine Innenministerkollegen und ich bereits mit hoher Intensität. Dabei haben wir zwischenzeitlich auch schon deutliche Erfolge zu verzeichnen. Allerdings liegt auch noch ein erhebliches Stück zur Optimierung des Kampfes gegen die Computerkriminalität vor uns.

Ebenso wichtig ist ein guter Schutz gegen die verbreiteteste Form von Internetkriminalität – den Betrug mittels gestohlener oder falscher Identitäten.

Wenn wir im Internet kommunizieren oder handeln, müssen wir uns auf die identitätsbezogenen Angaben unseres Gegenübers verlassen können. Umgekehrt müssen wir uns darauf verlassen können, dass unsere eigene elektronische Identität akzeptiert wird.

Sie sind eine Schlüsseltechnik für das Internet. Einrichtung, Schutz, Auflösung und Zusammenführung von elektronischen Identitäten müssen solide geregelt sein. Wir müssen uns dem Schlüsselthema der Datensicherheit und des Datenschutzes in Zukunft gemeinsam noch stärker widmen. Denn ohne sichere und transparente elektronische Identitäten kann es kein vertrauensvolles Miteinander im Netz geben. Mit dem neuen Personalausweis und De-Mail werden wir einen großen Schritt vorangekommen.

Offline steht uns zur Gefahrenabwehr die ganze Bandbreite des Ordnungsrechts zur Verfügung. Online kann es grundsätzlich nicht anders sein.

Das Ordnungsrecht setzt in vielen Bereichen, die stark gefahrgeneigt sind, bereits an, bevor eine konkrete Gefahr auftaucht. Dies kann zum Beispiel durch Erlaubnisvorbehalte der Fall sein. Wer Auto fahren will oder eine Gaststätte eröffnet, erhält erst eine Erlaubnis, wenn er über die Kenntnisse oder Zuverlässigkeit verfügt.

Auch für besonders gefahrgeneigte Online-Dienste sollten wir in manchen Fällen eine staatliche Erlaubnis bzw. Zulassung in Betracht ziehen. Es geht mir nicht darum,

flächendeckend Erlaubnispflichten für Internetdienste einzuführen, was nach EU-Recht auch gar nicht zulässig wäre. Hierzu gehören für mich internetbasierte Kreditvermittlungsplattformen. Einer besonderen Genehmigung bedarf es auch für den Internet-Versandhandel von Medikamenten. Auch potentiell freiheitsgefährdende Dienste, wie Ortungsdienste zum Beispiel zur ununterbrochenen Beaufsichtigung von Kindern und Jugendlichen, sind eines eingehenden Blickes wert. Wir sollten eine öffentliche Debatte darüber führen, bei welchen Diensten eine nationale oder europaweite Erlaubnispflicht im Interesse der Bürgerinnen und Bürger eingeführt oder verbessert werden sollten.

Eine Art von Diensten, die mir besondere Sorgen bereiten, sind die anonymen Finanzdienste, mit denen weltweit und ohne Nachvollziehbarkeit Gelder verschoben werden können. Im Internet wird für anonyme Finanzdienste unter anderem mit solchen Verheißungen geworben:

„Sie diktieren die Bedingungen, Sie haben die Kontrolle und sonst niemand – ev. Abmahnungen gehen sofort in die Ablage P (Papierkorb) – Sie sind nicht greifbar – Sie machen Geschäfte praktisch vom „Niemandsland“ aus – Sie kassieren ohne „Big Brother“ weltweit virtuell.“

Hier sollten wir nicht nur über eine Erlaubnispflicht und Auflagen, sondern sogar – in bestimmten Fällen, etwa bei höheren Beträgen – über ein Verbot nachdenken.

Das Internet kann durch die Ordnungsbehörden auch genutzt werden, um klassische ordnungsrechtliche Maßnahmen durch neue, „weiche“ Steuerungsinstrumente zu ersetzen oder zu ergänzen. Beispiele sind behördliche Warnungen oder Veröffentlichungen von Ergebnissen ordnungsbehördlicher Kontrollen. Im Bereich des Lebensmittelrechts kennen wir derartige Warnmeldungen schon länger. Sie können – auch ökonomisch – sehr wirksam sein.

Ein Punkt, der noch weiterer Diskussion bedarf, ist der Umgang mit illegalen Inhalten, zum Beispiel Kinderpornografie. Der Staat kann es unter keinen Umständen dulden, wenn die Schwächsten und Schutzbedürftigsten missbraucht werden.

Eine generelle Verpflichtung zur inhaltlichen Kontrolle durch die Provider lehne ich, wie gesagt, ab. Ist dem Provider allerdings bekannt, dass er solche Inhalte zum Abruf bereit hält, muss auch er dafür Sorge tragen, dass sie gelöscht werden.

Mit dem Zugangserschwerungsgesetz ist nun die rechtliche Möglichkeit geschaffen worden, kinderpornografische Inhalte zu sperren, wenn eine Löschung – aus welchen Gründen auch immer – nicht erfolgreich ist. Wie bekannt ist, wird dies erst einmal nicht gemacht. Der Gesetzgeber hat damit ein mittleres Erdbeben in der Netzgemeinde ausgelöst.

Ich gestehe, dass die Politik damit nicht gerechnet hat. Viele im Ausland verstehen die Deutschen dabei auch nicht. Die Vernichtung kinderpornografischer Schriften müsste eigentlich gegenüber einer Maßnahme, die lediglich die Nichtverbreitung sicherstellen soll, der schwerere Eingriff sein. Im Internet wird dies aber anders und umgekehrt empfunden.

Im Koalitionsvertrag haben wir vereinbart, das Löschen deutlich in den Vordergrund zu rücken. Ich habe daher mit dem Bundeskriminalamt ein Maßnahmenbündel geschnürt, um das Löschen von Kinderpornografie gerade im Ausland zu verbessern und weitere Maßnahmen zu ergreifen, um die Konsumenten stärker zu verfolgen. Dies werde ich in Kürze im Einzelnen vorstellen.

## III. ANGEBOTS- UND INNOVATIONSFUNKTION

Ich komme zur dritten Funktion des Staates von grundlegender netzpolitischer Bedeutung: seine Angebots- und Innovationsfunktion.

Es ist Aufgabe des Staates, Innovationen gezielt zu fördern. Ich bin überzeugt davon, dass dies dem Wirtschaftsstandort Deutschland unmittelbar zugutekommt, auch Arbeitsplätze sichert.

Wir sollten gemeinsam mit der Wirtschaft wesentliche, wachstumsbestimmende technologische Trends rund und das Internet identifizieren und verfügbare öffentliche und unternehmerische Ressourcen auf die zukunftsweisendsten Bereiche lenken.

Wir erhalten und stärken damit Kernkompetenzen, die unserem Wirtschaftsstandort zugutekommen und uns international weniger abhängig machen

Die Bundesregierung bekennt sich längst zu einer Förderung innovativer Informationstechnik aus Deutschland. Das Projekt THESEUS ist mit rund 100 Mio. Euro Fördermitteln durch das Bundeswirtschaftsministerium eines der derzeit größten IT-Vorhaben der Bundesregierung. Mit THESEUS wollen wir neue Technologien für das Internet der Dienste entwickeln und erproben, wir wollen den Zugang zu Informationen vereinfachen, Daten zu neuem Wissen vernetzen und die Grundlage für die Entwicklung neuer Dienstleistungen im Internet schaffen. Wir fördern auch innovative IT-Sicherheitsprodukte aus Deutschland, sei es durch ein entsprechendes Forschungsprogramm der Kollegin Schavan, sei es durch unsere Investitionen im Rahmen des Konjunkturpaketes II.

Neben dem Fördern ist es Aufgabe des Staates, eigene Angebote zu machen, vor allem im Bereich seiner eigenen Verwaltung, an der Schnittstelle zwischen Amt und Bürgern, beim E-Government.

Gute elektronische Behördendienste sind weltweit gefragt. Die Verwaltung in Deutschland genießt international hohes Ansehen. Mit innovativen und anwenderfreundlichen Angeboten können wir international eine Vorreiterrolle einnehmen. Als rohstoffarmes und wissensorientiertes Land sollten wir diese Chance nutzen. Elektronische Behördendienste können jedoch nur erfolgreich sein, wenn einige Voraussetzungen erfüllt sind.

E-Government ist kein Selbstzweck. Nicht jedes Angebot ist geeignet und sinnvoll. Zudem sollten elektronische Behördendienste im Verhältnis zum Bürger noch sehr lange als Zusatzangebote ausgestaltet sein und den konventionellen Behördenkontakt nicht vollständig ersetzen.

Anders sieht es in Bezug auf die Wirtschaft aus. Hier können elektronische Behördendienste durchaus verpflichtend ausgestaltet werden, wie wir es bei der Umsatzsteuervoranmeldung und dem Handelsregister bereits kennen. Letztlich profitieren beide Seiten davon, weil es viel Aufwand und Geld spart. Mit Wirtschaft und Wissen-

schaft entwickeln wir derzeit ein neues Modell und pilotieren es beim Austausch von Umweltdaten.

Das Vertrauen in die öffentliche Verwaltung beruht darauf, dass sie dem Bürger gegenüber integer, verlässlich und an Recht und Gesetz gebunden, auftritt. Elektronische Behördendienste müssen entsprechend gestaltet sein.

Die IT muss den Anforderungen der Verwaltung und der Bürger folgen und nicht umgekehrt. Es darf nicht sein, dass bei einer Ermessensentscheidung ein bestimmtes Kriterium nur deshalb nicht berücksichtigt wird, weil das von der Verwaltung genutzte Programm kein Feld dafür vorsieht.

Der Staat kann daher nur bedingt auf das Design und die Funktionalitäten marktüblicher und marktbeherrschender Dienste zurückgreifen.

Allerdings ist es für Behörden nicht einfach, Internetangebote eigenständig zu designen. Zur Entwicklung und Einführung elektronischer Behördendienste sind sie vielfach auf die Zusammenarbeit mit Privaten im Rahmen von Public Private Partnerships angewiesen. Diese Zusammenarbeit drückt manchen Angeboten ihren eigenen Stempel auf. Wenn dieser zu stark in den Vordergrund rückt, kann es problematisch werden. Dem können wir entgegenwirken, indem wir staatliche Kräfte und eigenes Know-How bündeln und behördenübergreifend zur Verfügung stellen.

Wenn wir heute neue IT-Systeme in der deutschen Verwaltung einführen, so handelt es sich fast immer um Integrationsprojekte, bei denen wir bestehende Systeme miteinander verbinden, häufig über Bund-, Länder- und Kommunalgrenzen. Diese Zusammenarbeit verschiedener staatlicher Ebenen bei der IT hat für unser Land größte Bedeutung. Mit der Föderalismusreform und der Schaffung des IT-Planungsrates haben wir die Voraussetzungen dafür geschaffen, dass Bund, Länder und Kommunen ihre elektronischen Behördendienste nach gemeinsamen Standards leichter und unabhängiger von privaten Partner ausgestalten und anbieten können.

Wenn der Staat den Menschen gegenübertritt, hat er eine besondere Verantwortung – für Rechtsstaatlichkeit, Transparenz, Verlässlichkeit seines Verhaltens und für den

diskriminierungsfreien Umgang mit allen Bürgern. Staatliche IT-Systeme und Internet-Angebote müssen diese Anforderungen aufnehmen. Sie müssen rechtlich und technisch sicher funktionieren, auf offenen Standards basieren, von allen Menschen plattformunabhängig genutzt werden können, barrierefrei sein und größtmögliche Transparenz bieten. Offene Standards erlauben es den Anwendern, notwendige Daten frei, mit hoher Qualität und bestmöglicher Sicherheit weiterzugeben. Sie verhindern Abhängigkeiten.

Verwaltungsvorgänge, in denen sich Staat und Bürger in einem Rechtsverhältnis gegenüber stehen, verlangen regelmäßig eine eindeutige Identifikation des Bürgers. Der Staat muss sich sicher sein können, wer einen Antrag gestellt oder eine Anzeige erstattet hat. Mit dem Personalausweis schaffen wir ein universell nutzbares, sicheres und datenschutzfreundliches Medium für diese Aufgabe.

Bei staatlichen Angeboten im Internet sollten wir dort investieren, wo auf Seiten der Bürger ein vorrangiges Bedürfnis besteht bzw. eine erheblich Effizienz- und Kostenersparnis auf Seiten der Verwaltung eintritt. Dies ist vermutlich vor allem bei weit verbreiteten Verwaltungsgeschäften, wie der Kfz-Anmeldung, oder anderen Massenvorgängen, wie zum Beispiel der Beantragung von BAföG, der Fall. Für die Einführung eines Online-Antrags beim BAföG hat sich daher auch der Normenkontrollrat ausgesprochen.

Beim Ausbau staatlicher Internet-Angebote sollten wir uns im Übrigen an den klassischen Staatsaufgaben orientieren. Hierzu zählen der Kulturauftrag und der Bildungsauftrag. Einen weiteren Vorrang sehe ich bei Angeboten, mit denen der Staat eine wichtige Aufklärungs- und Warnfunktion erfüllt, die der Sicherheit dient.

Es geht nicht um das Kaufen von Diensten für die Verwaltung, die der Anbieter gerade hat oder anbietet, sondern um die Erarbeitung von Diensten, die Bürger und Staat brauchen.

Der moderne Staat hat auch die Aufgabe der Wirtschafts- und Forschungsförderung übernommen. Wirtschaftliche Innovation kann der Staat fördern, indem er seine nicht-personenbezogenen Datenbestände Online zur Verfügung stellt. Auf der Basis

dieser Daten können neue Geschäftsmodelle entwickelt werden. Das Statistische Bundesamt stellt bereits 166 Mio Datensätze Online zur Verfügung. Diese Form der Bereitstellung wird weltweit unter dem Begriff „Open Data“ bzw. „Open Government“ diskutiert. Open Government ist v.a. für wirtschaftliche Nutzungen sinnvoll und innovativ. In diesem Zusammenhang ist auch der Aufbau der Geodateninfrastruktur in Deutschland zu nennen, der mir besonders am Herzen liegt.

Mit vielen elektronischen Behördendiensten können Kosten in großem Umfang gespart werden. Einige Angebote bedienen indessen vorrangig Einzelinteressen. Wer eine Leistung in Anspruch nimmt und hiervon in besonderer Weise profitiert – etwa durch kommerzielle Nutzung -, sollte dafür durchaus auch zahlen.

Wir sollten uns ohnehin von der Vorstellung verabschieden, dass alles, was im Internet passiert, umsonst ist. Nichts ist umsonst. Die meisten Geschäftsmodelle des Internets finanzieren sich über Werbung und Daten der Nutzer. Staatliche Angebote sind auf andere Finanzierungen angewiesen, und zwar auf Gebühren oder Steuergelder. Gebühren sollten dort erhoben werden, wo wir es normalerweise auch tun, nämlich dann, wenn der Betroffene von der Leistung besonders profitiert. Mit Steuern sollten wir grundsätzlich nur solche Angebote finanzieren, mit denen wir eine staatliche oder kommunale Kernaufgabe erfüllen.

Das Internet hat auch als Medium der politischen Willensbildung viel Potential. Online-Konsultationen können Beteiligungen von Verbänden und Interessengruppen im kommunalen und staatlichen Rechtssetzungsverfahren durch eine zusätzliche Form der Bürgerbeteiligung ergänzen.

Dabei dürfen die Erwartungen freilich nicht überdehnt werden. Die gewählten Entscheidungsträger bleiben letztlich verantwortlich und Online-Konsultationen ohne Quorum und Registrierung sind nur bedingt repräsentativ. Sind sich alle Seiten dessen bewusst, überwiegen die Vorteile gleichwohl bei weitem.

## E. NÄCHSTE SCHRITTE

Was folgt aus dieser ersten Skizze eines Ordnungsrahmens für das Internet? Was sind die nächsten Schritte? Brauchen wir zum Beispiel ein Netzgesetzbuch?

Die Themen sind vielschichtig und vor allem rechtlich völlig unterschiedlich gelagert. Ein Netzgesetzbuch kann es schon deshalb nicht geben, weil es nicht unserer Tradition entspricht, zivilrechtliche, öffentlich-rechtliche und strafrechtliche Regelungen durcheinander zu würfeln und in ein Gesetzbuch zu schreiben.

Wir werden möglichst früh und gemeinsam konkrete Handlungsvorschläge erarbeiten, die wir im Wege der Selbstregulierung und die wir gesetzlich umsetzen wollen. Dazu gehört auch das allgemeine Datenschutzgesetz.

Lassen Sie uns den Ordnungsrahmen einer systematischen Netzpolitik in den nächsten Wochen und Monaten weiter erörtern. Die Thesen, die meine heutigen Ausführungen zusammenfassen, finden Sie ab heute im Internet. Sie können dort nicht nur bewertet, sondern auch mit konkreten Handlungsvorschlägen versehen werden. Ich lade Sie und alle anderen Interessierten zur Teilnahme herzlich ein. Das Bundesministerium des Innern wird Ihre Vorschläge prüfen und gegebenenfalls in den Katalog der Handlungsvorschläge aufnehmen, die wir gemeinsam mit den anderen Ressorts erarbeiten wollen.

Die Zeit des Staunens über das Internet und seine Wirkung ist vorbei.